Citrix Application Delivery Management サービス

Machine translated content

Disclaimer

Contents

概要

May 7, 2021

Citrix Application Delivery Management（以前の NetScaler Management and Analytics Service）は、Citrix ADC MPX、Citrix ADC VPX、Citrix ADC SDX、Citrix ADC CPX、Citrix ADC CPX、Citrix ADC BLX、Citrix Gateway、Citrix Secure Web Gateway、および Citrix SD-WAN を含むすべての Citrix 環境を管理するための Web ベースのソリューションです。アプライアンスをオンプレミスまたはクラウドにデプロイします。

このクラウドソリューションを使用すると、単一の統合された、一元化されたクラウドベースのコンソールから、グローバルアプリケーション配信インフラストラクチャ全体を管理、監視、トラブルシューティングできます。Citrix Application Delivery Management（ADM）は、Citrix ADC 展開環境でのアプリケーション配信のセットアップ、展開、管理に必要なすべての機能を提供し、アプリケーションの正常性、パフォーマンス、およびセキュリティを豊富に分析します。

Citrix ADM には、次の利点があります。

- 機敏性 — 運用、更新、使用が容易 Citrix ADM のサービスモデルはクラウド上で利用可能であるため、Citrix ADM が提供する機能を簡単に操作、更新、使用することができます。更新の頻度と自動更新機能の組み合わせにより、Citrix ADC 展開が迅速に強化されます。
- タイム・ツ・バリューの短縮 — ビジネス目標の達成を迅速化従来のオンプレミス展開とは異なり、Citrix ADM サービスを数回クリックするだけで使用できます。インストールと構成の時間を節約するだけでなく、潜在的なエラーに対して時間とリソースの無駄を避けることもできます。
- マルチサイト管理 — 複数のサイトデータセンターにまたがるインスタンスを 1 つのペインで管理できます。Citrix ADM を使用すると、さまざまな種類の展開環境にある Citrix ADC を管理および監視できます。オンプレミスとクラウドに展開された Citrix ADC は、ワンストップで管理できます。
- 運用効率 — 運用生産性を向上させる最適化および自動化された方法。Citrix ADM では、従来のハードウェア展開の保守とアップグレードにかかる時間、コスト、リソースを節約し、運用コストを削減できます。

Citrix ADM 仕組み

Citrix ADM は、Citrix Cloud 上のサービスとして利用できます。Citrix Cloud にサインアップしてサービスの使用を開始したら、ネットワーク環境にエージェントをインストールするか、インスタンスに組み込みエージェントを起動します。次に、管理するインスタンスをサービスに追加します。

エージェントは、データセンター内の Citrix ADM と管理対象のインスタンス間の通信を可能にします。エージェントは、ネットワーク内の管理対象インスタンスからデータを収集し、Citrix ADM に送信します。

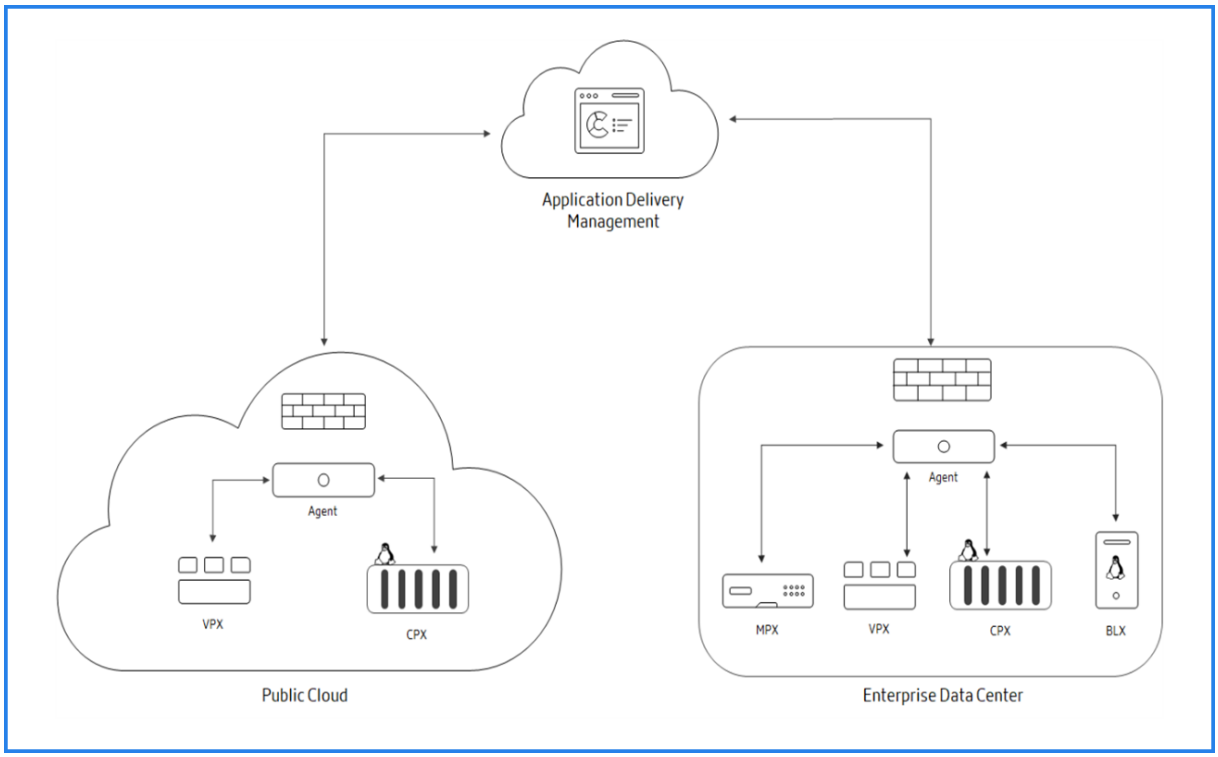
Citrix ADM にインスタンスを追加すると、トラップ先として暗黙的に追加され、インスタンスのインベントリが収集されます。

サービスでは、次のようなインスタンスの詳細が収集されます。

- ホスト名
- ソフトウェアのバージョン
- 実行構成と保存済み
- 証明書
- インスタンス上で構成されたエンティティ、など。

Citrix ADM は、管理対象インスタンスを定期的にポーリングして情報を収集します。

次の図は、サービス、エージェント、およびインスタンス間の通信を示しています。



リリースノート

May 7, 2021

Citrix Application Delivery Management（Citrix ADM）リリースノートでは、サービスリリースで利用可能な新機能、既存機能の強化、修正された問題、既知の問題について説明します。
リリースノートには、次のセクションの 1 つまたは複数が含まれています。

- 新機能: 現在のリリースで利用可能な新機能、既存機能の強化、修正です。
- 既知の問題: 現在のリリースに存在する問題とその回避策 (該当する場合)。
- 以前のリリース: 以前のリリースでリリースされた新機能および機能強化。

新機能

May 7, 2021

このトピックでは、リリースで利用可能な新機能、既存の機能の強化、および修正を示します。

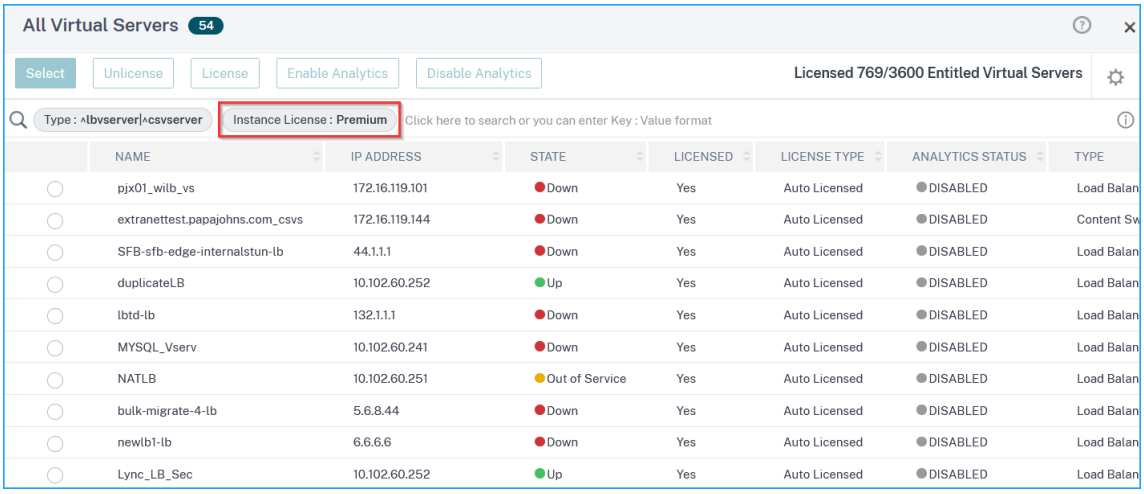
Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで Citrix ADM 最新ビルドに自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

2021 年 **4** 月 **17** 日

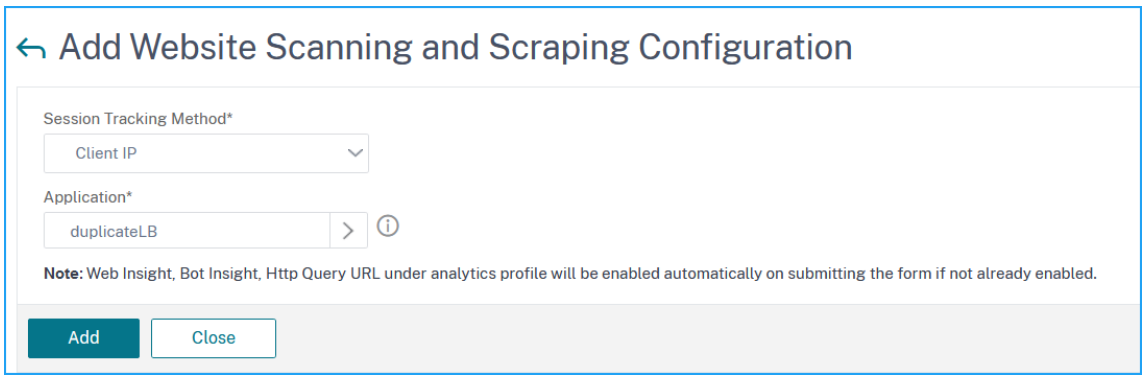
セキュリティ違反の改善

[分析] **>** [セキュリティ] **>** [セキュリティ違反] で、次の改善点を表示できるようになりました。

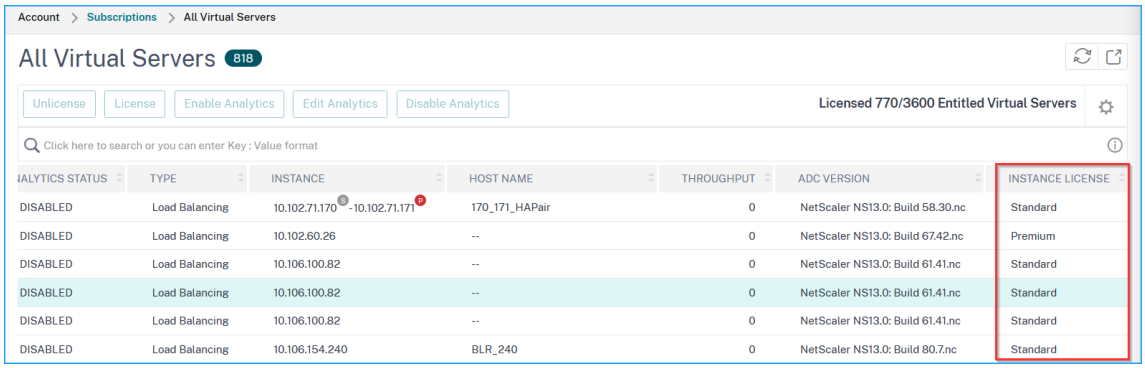
- アカウントの乗っ取り、ウェブサイトスキャン、コンテンツスクレイピング違反の分析を有効にすると、高度なセキュリティ分析と **WebInsight** 設定 も自動的に有効になります。
- [設定] オプションから、アカウント乗継ぎ、**Web** サイトスキャン、コンテンツスクレイピング違反の前提条件設定を構成するアプリケーションを選択すると、Premium ライセンスフィルターが適用されます。この機能強化により、プレミアムライセンスアプリケーションのみを表示および選択できます。



- 設定オプションから、**Web** サイトのスキャンとスクレイピングの前提条件構成ページでは、まずセッショントラッキング方法を選択し、次にアプリケーションを選択できます。



- **[** アカウント**] > [**サブスクリプション**]** の [すべての仮想サーバー] ページに [インスタンスライセンス] オプションが表示され、インスタンスのライセンスタイプを分析できます。



[NSADM-68058]

アプリダッシュボードでセキュリティ違反を表示する

[分析**] > [**セキュリティ**] > [**セキュリティ違反**] > [**アプリケーションの概要] で、WAF と Bot に対して表示できた違反の詳細が [アプリケーションダッシュボード] でも表示されるようになりました。[アプリケーション**] > [**ダッシュボード] に移動してアプリケーションを選択し、[セキュリティ] タブをクリックして、選択したアプリケーションに適用可能な WAF および Bot 違反を表示します。

この拡張機能では、アプリケーションのパフォーマンスと使用状況の可視性とは別に、違反の詳細を単一ペインビューで視覚化することもできます。

[NSADM-66876]

IP アドレスの色コードが動的に変更され、インスタンスの状態が示されます

ADM GUI の［ネットワーク］**>**［インスタンス］**>**［**Citrix ADC**］の［IP アドレス］列で、IP アドレスマークの色コードが動的に変更され、インスタンスの状態が示されます。たとえば、特定のプライマリ・インスタンスが「up」状態の場合、対応する IP アドレスの円形 P マークの色コードが緑色に変わります。また、円形のマークをポイントして、インスタンスのステータスを確認することもできます。以前は、IP アドレスのカラーコードは静的で、プライマリは青、セカンダリは灰色でした。

[NSADM-67681]

修正された問題

SSL 証明書の場合、証明書が **SSL** ダッシュボード設定で構成されている場合でも、ADM GUI には発行者の種類が「推奨されていません」と表示されます。

[NSHELP-26123]

2021 年 **3** 月 **30** 日

ボットインサイト**-**ボット管理用のログメッセージを表示する

[分析**] > [**セキュリティ**] > [**セキュリティ違反**] > [**アプリケーションの概要] の [ボット] で、アプリケーションを選択して [ログ] をクリックしてボットの詳細を表示したときに、署名と署名 ID として識別されたボットカテゴリを表示できるようになりました。シグネチャ ID を使用すると、検出されたボットが良好なボットか悪いボットかを分析できます。その他のボットカテゴリでは、シグニチャ ID には N/A と表示されます。

シグニチャカテゴリと ID の詳細については、ボット署名の更新を参照してください。

[NSADM-63099]

アプリのセキュリティ違反-ボット

[分析] > [セキュリティ] > [セキュリティ違反] > [すべての違反] で、[BOT 違反] カテゴリでキーストロークとマウスの動的ボット検出を表示できるようになりました。詳しくは、「アプリのセキュリティ違反」を参照してください。

[NSADM-61855]

解決された問題

- インフラストラクチャ分析で、SSL 違反カウンタ (PE CPU 制限、PPS 制限、スループット制限、SSL スループット制限、SSL TPS 制限) の UI 用語「パケットドロップ」が「レート制限違反」に変更されるようになりました。

  [NSADM-69007]

- ADM が生成した技術サポートバンドルの解凍に失敗する。

  [NSHELP-26726]

2021 年 3 月 17 日

セキュリティアドバイザリを使用して組織を保護する

Citrix ADM セキュリティアドバイザリは、Citrix の一般的な脆弱性およびエクスポージャス（CVE）の影響を受ける ADC インスタンスを特定し、適切な修復を適用するのに役立ちます。このアドバイザリでは、ADC インスタンスが危険にさらされている Citrix CVE を強調し、緩和策と修復を推奨しています。ADM サービスを使用して緩和策と是正を適用することにより、推奨事項を確認し、適切なアクションを実行できます。

セキュリティアドバイザリ機能は次のとおりです。

- スキャン: デフォルトのシステムスキャンとオンデマンドスキャンが含まれます。
  - システムスキャン: デフォルトで週に 1 回、すべての管理対象インスタンスをスキャンします。システムスキャンの日付と時刻は ADM によって決定され、変更することはできません。
  - オンデマンドスキャン: 必要に応じてインスタンスを手動でスキャンできます。最後のシステムスキャンの後に経過した時間が重要な場合は、オンデマンドスキャンを実行して、現在のセキュリティポスチャを評価できます。または、修正または緩和が適用された後にスキャンして、改訂された姿勢を評価します。
- CVE 影響分析: インフラストラクチャに影響を与えているすべての CVE と、すべての ADC インスタンスが影響を受ける結果を表示し、修復と緩和を提案します。この情報を使用して、緩和と修復を適用してセキュリティリスクを修正します。

- CVE レポート: 最後の 5 つのスキャンのコピーを保存します。これらのレポートをダウンロードして分析できます。
- CVE リポジトリ： Citrix が 2019 年 12 月以降に発表したすべての ADC 関連 CVE の詳細ビューが表示され、ADC インフラストラクチャに影響する可能性があります。このビューを使用して、セキュリティアドバイザリースコープの CVE を理解し、CVE の詳細を確認できます。

詳しくは、「セキュリティアドバイザリ」を参照してください。

[NSADM-69280]

Citrix のロータッチオンボーディングワークフローに追加された新機能

新しい Citrix のロータッチオンボーディングワークフローには、いくつかの新機能と優れたユーザーエクスペリエンスを備えた強化された GUI が付属しています。セキュリティアドバイザリとアップグレードアドバイザリの 2 つの新しいタブが導入されました。Citrix ADM セキュリティアドバイザリは、ADC インスタンスを危険にさらす脆弱性について警告し、緩和策と修復を推奨します。アップグレード・アドバイザリを使用して、エンドオブライフ（EOL）に近づいている ADC インスタンスまたは古いバージョンで確認できます。これらの ADC を最新のリリースにアップグレードし、最新の機能強化と修正の恩恵を受けることができます。詳細については、Citrix ADM サービス接続を使用した Citrix ADC インスタンスのロータッチオンボーディングを参照してください。

[NSADM-69280]

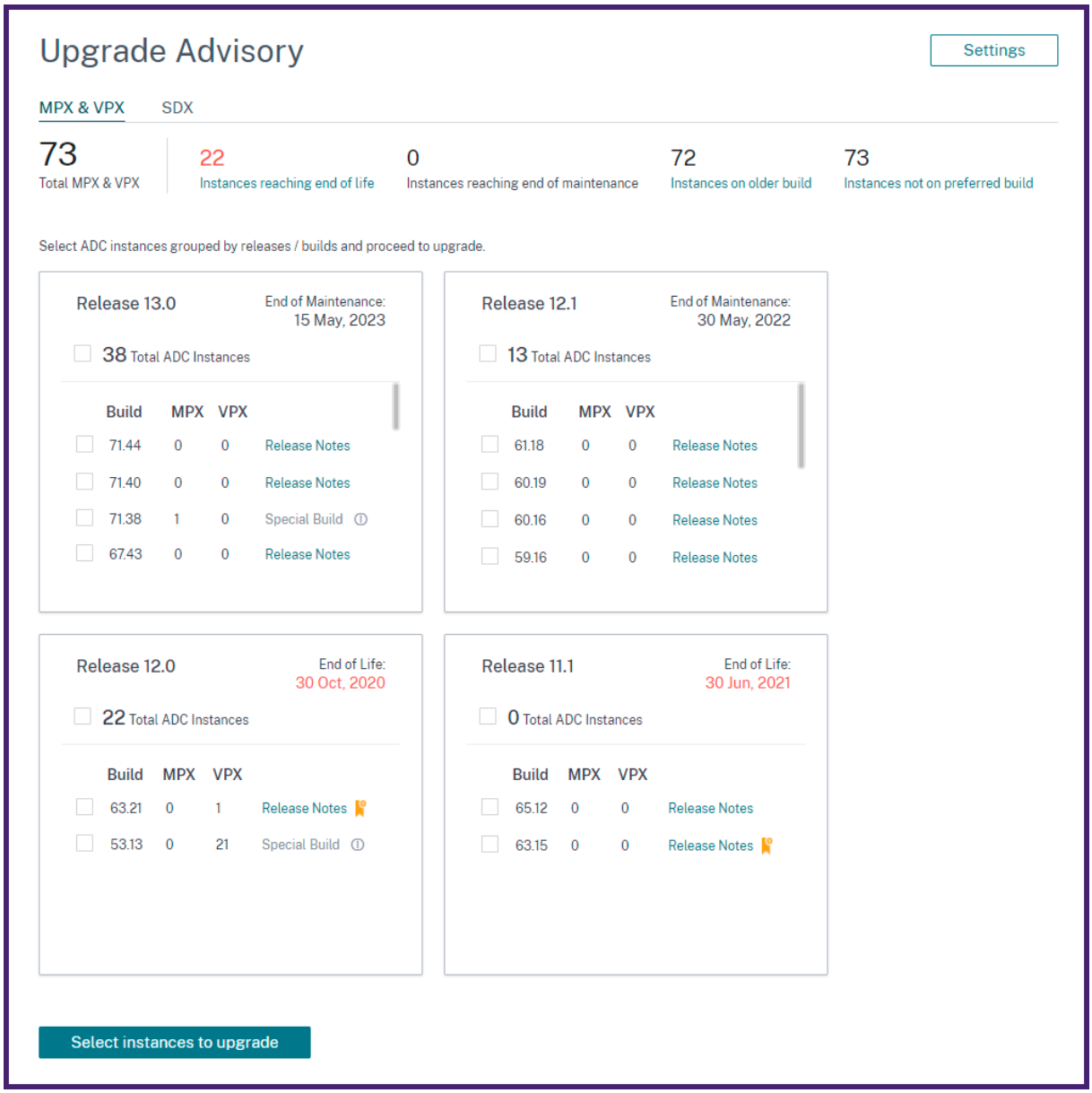
Citrix ADM アップグレードアドバイザリを使用して **ADC** インスタンスのライフサイクルを監視する

Citrix ADM アップグレードアドバイザリは、ADC インスタンスのライフサイクルを監視するのに役立ちます。ネットワーク管理者は、Citrix ADM 異なる ADC リリースで実行されている多数のインスタンスを管理できます。各 ADC インスタンスのライフサイクルの監視は、面倒な作業になります。このプロセスを容易にするために、ADM アップグレードアドバイザリでは、次の情報を提供します。

- EOL または EOM に達または到達したインスタンスを識別します。そのため、EOL または EOM の日付より先に ADC のアップグレードを計画できます。
- 最新のリリースまたはビルドにないインスタンスを強調表示します。これらのインスタンスを最新のリリースまたはビルドにアップグレードして、新機能やバグ修正の恩恵を受けることができます。
- 優先 ADC ビルド上にないインスタンスを強調表示します。組織によっては、インスタンス用に優先 ADC ビルドを使用している場合があります。ADM では、機能、修正された問題、およびその他の考慮事項に応じて、組織に適したビルドを設定できます。次に、優先ビルドにないインスタンスを確認し、アップグレードします。優先ビルドを実行しているインスタンスは、星形のアイコンで示されます。
- 最も人気のあるリリースまたはビルドで実行されているインスタンスを強調表示します。一般的なビルドを実行しているインスタンスは、リボンアイコンで示されます。

上記のポイントを確認したら、「アップグレードアドバイザリ」(Upgrade Advisory) ページから ADC インスタンスをアップグレードするメンテナンス・ジョブを作成できます。

> 重要:
>
> アップグレード・アドバイザリは、ADC ソフトウェア・バージョンの EOM または EOL のみを監視します。ADC ハードウェアアプライアンスの EOL はチェックしません。



詳しくは、「アップグレードアドバイザリ」を参照してください。

[NSADM-56646]

アプリケーションの遅さの根本原因の分析

アプリケーションの遅さは、ビジネスへの影響や生産性につながるため、あらゆる組織にとって大きな懸念事項です。[アプリケーション**] > [Web Insight**] で、新しいメトリック [応答時間の異常のあるアプリケーション] を表示でき

るようになりました。管理者として、このメトリックを使用して、アプリケーションの速度低下が次の原因で発生しているかどうかを分析できます。

- クライアントネットワークの遅延
- サーバーネットワークの待ち時間
- サーバー処理時間

詳しくは、「アプリケーションの遅さの根本原因の分析」を参照してください。

[NSADM-63170]

2021 年 3 月 03 日

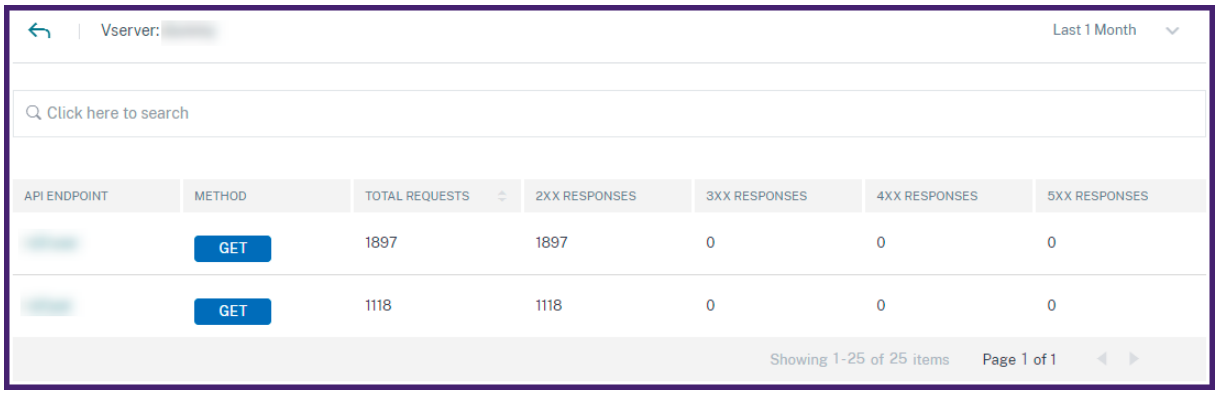
ADM で **API** エンドポイントを検出する

これで、API ゲートウェイを使用して、組織内の API エンドポイントを検出できます。Citrix ADM では、［アプリケーション］**>**［**API** ゲートウェイ］**>**［**API** 検出］ページに、ADC インスタンスおよび API 展開の一部である API エンドポイントが表示されます。

[API Discovery] で、仮想サーバーまたは API 配置を選択すると、ADM GUI に API エンドポイントとその詳細が表示されます。

- メソッド -それは、API エンドポイントで使用されるメソッドを表示します。たとえば、GETおよびPOSTメソッド
- リクエスト合計 -それは、API エンドポイント上の API リクエストの数を表示します。
- 応答ステータス -それは、各応答ステータスのカウントを表示します。たとえば、2xx、3xx、4xx、5xxなどです。
- 仕様で見つかりました -この列は API デプロイにのみ表示されます。場合によっては、API 定義の一部ではない内部 API が外部からのトラフィックを受信することがあります。この列は、API エンドポイントと観測されたメソッドが API 定義の一部であるかどうかを識別するのに役立ちます。

仮想サーバ:

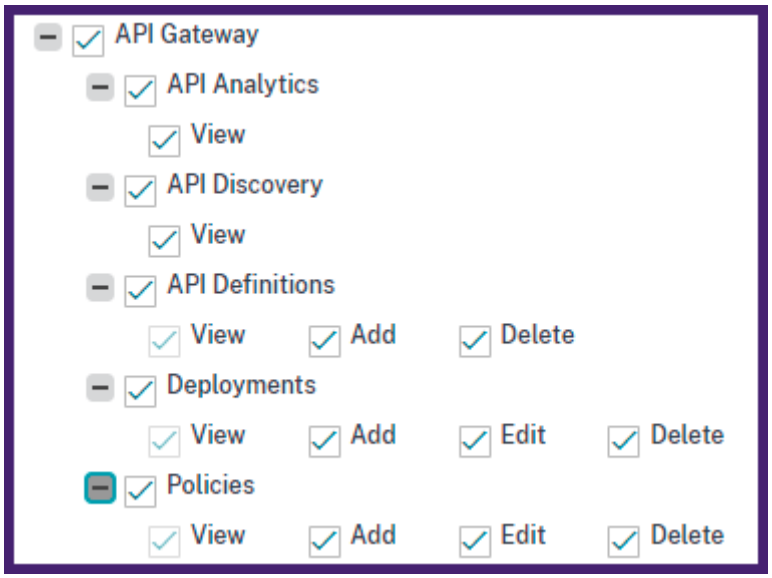


API デプロイ**:**

[NSAPISEC-1234]

API ゲートウェイの設定と管理権限の付与

管理者は、アクセスポリシーを作成して、API ゲートウェイの設定と管理に対するアクセス許可をユーザーに付与できます。ユーザー権限は、表示、追加、編集、および削除できます。これを行うには、[アカウント] **>** [ユーザー管理] **>** [アクセスポリシー] に移動します。



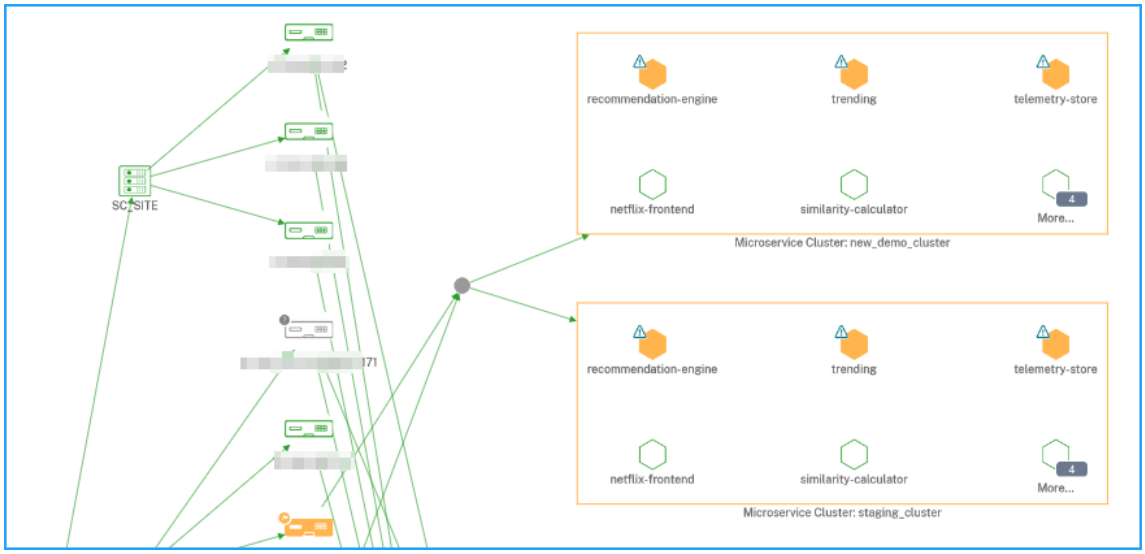
[NSADM-63097]

グローバルサービスグラフの改良

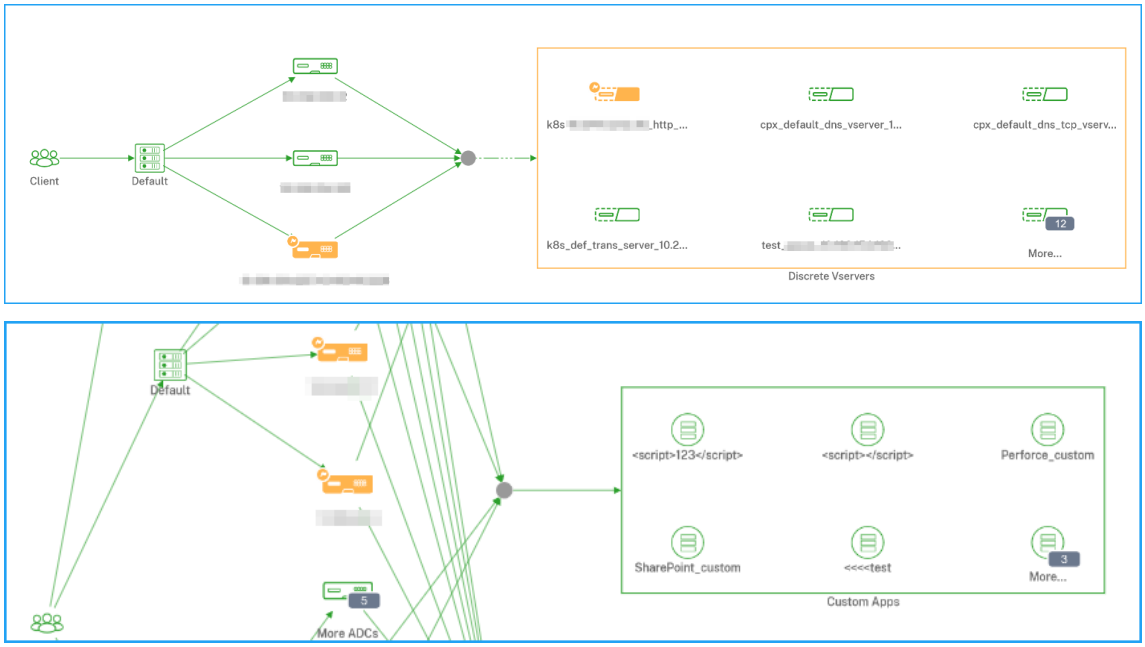
[アプリケーション] **>** [サービスグラフ] **>** [グローバル] で、次の項目を表示できます。

- クラスター名に基づくマイクロサービス。

  > 注
  >
  > 3 つのクラスターのマイクロサービスのみを表示できます。



- 個別の仮想サーバーとカスタムアプリケーションの拡張ビュー



Citrix ADM での **Venafi** 統合

デジタルセキュリティを維持するには、環境内の SSL 証明書の管理を自動化する必要があります。有効期限が切れた SSL 証明書は、セキュリティリスクにつながる可能性があります。これで、Venafi 信頼保護プラットフォームサーバーを構成して、ADM サービス GUI から SSL 証明書を管理できます。

Venafi 統合では、ADM サービスの GUI を使用して、証明書を再発行し、ADC インスタンスにインストールされている証明書の更新を自動化できます。詳しくは、「SSL 証明書管理の自動化」を参照してください。

[NSADM-58047]

解決された問題

- [ネットワーク] > [構成ジョブ] でジョブを作成し、特定の曜日または月の日付として [実行頻度] を選択すると、スケジュールされたジョブは指定された時刻に従って実行されません。

  [NSHELP-26034]

- プロキシサーバが有効になっていて、エージェントがその IP アドレスを取得できない場合、DNS サーバなしで ADM の登録または更新に失敗します。

  [NSHELP-25835]

- 管理者以外のユーザーの場合、ADM GUI の [ネットワーク] > [ネットワーク機能] > [GSLB] の下に **GSLB** サービスデータが表示されるまで 1 分以上かかります。

  [NSHELP-25740]

- ライセンスプールのしきい値が設定されていない場合でも、電子メール通知を受信します。

  [NSHELP-25723]

- **Gateway Insight** で、レポートをスケジュールすると ([レポートのエクスポート] > [エクスポートのスケジュール])、生成されたレポートに [ページが見つかりません] と表示されます。

  [NSHELP-25496]

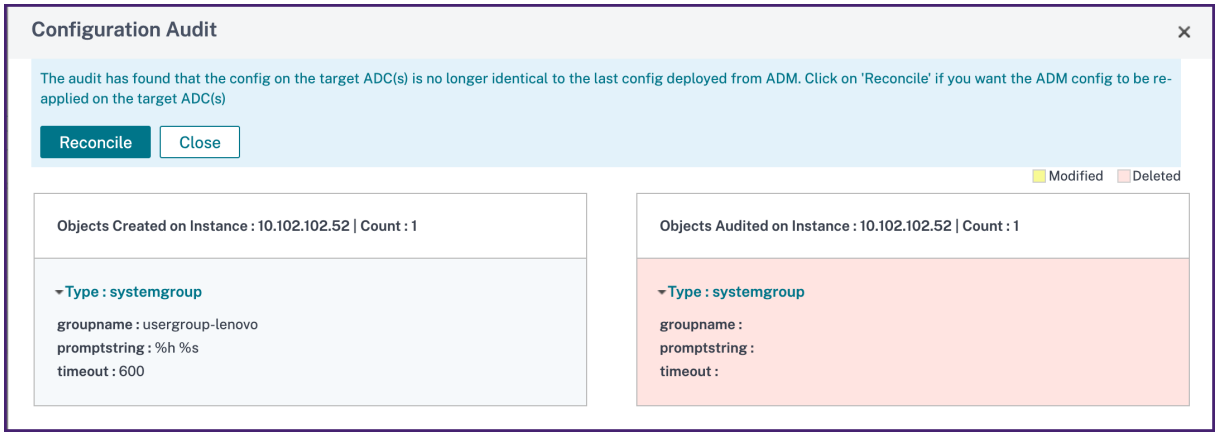
- 場合によっては、ADM GUI でインスタンスライセンスの表示に失敗することがあります。

  [NSADM-67697]

2021 年 2 月 11 日

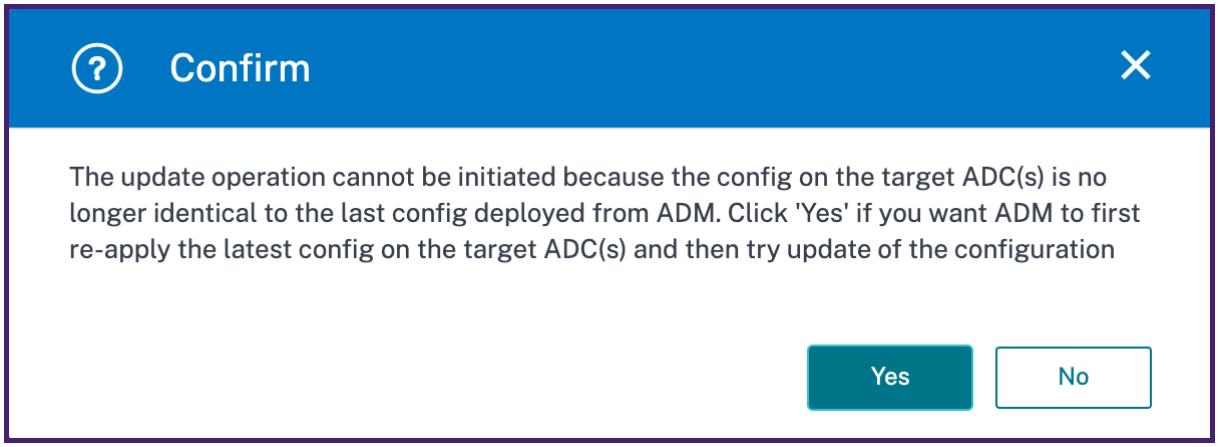
StyleBook の設定を調整する

StyleBook 構成パックを使用して ADC 設定を監査すると、ADC インスタンスで検出された変更またはドリフトを調整できます。この操作により、ADM の設定パックのバージョンに合わせて ADC 設定が復元されます。



StyleBook 設定を使用して、ADC インスタンス上にオブジェクトを作成したとします。そのオブジェクトが ADC インスタンスから削除されると、[**Configuration Audit**] ページに変更が識別され、調整できます。調整アクションは、構成パックで定義されているように、削除したオブジェクトを ADC インスタンス上に復元します。

構成パックの更新中に変更またはドリフトが検出された場合は、変更を調整するための確認メッセージが表示されます。

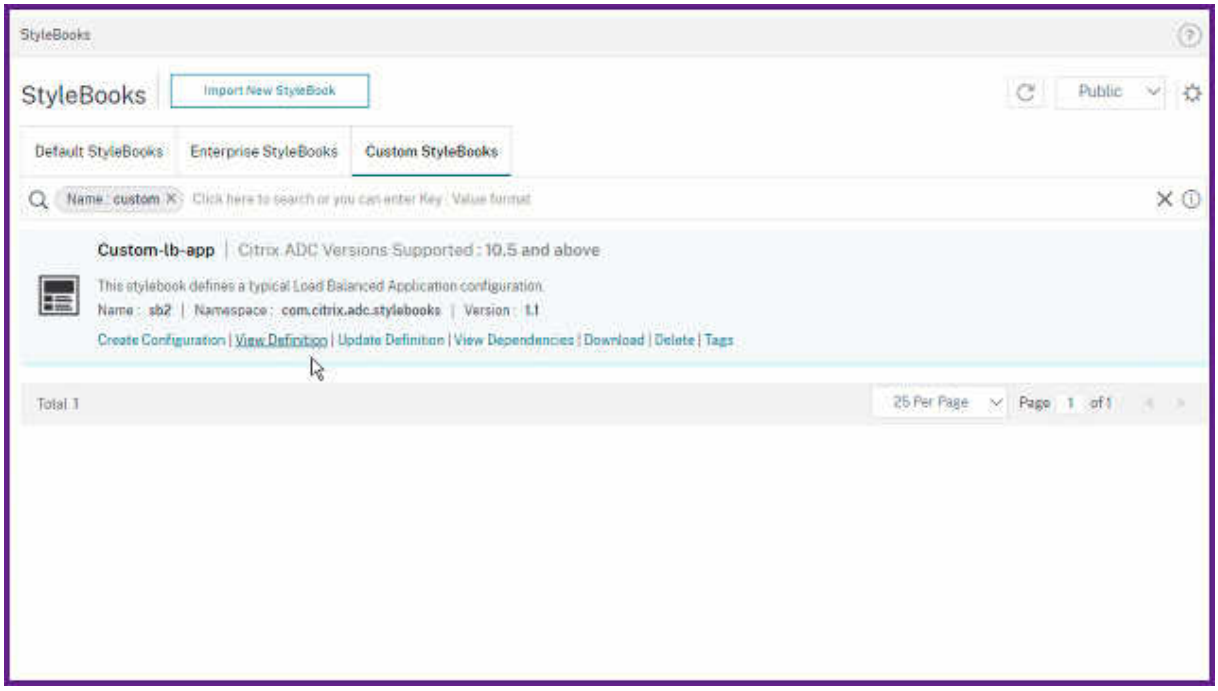


[NSADM-62742]

GUI でカスタム **StyleBook** 定義を更新する

ADM GUI 自体からカスタム StyleBook 定義を更新できるようになりました。

> 注 ADM GUI から StyleBook 定義を更新する前に、次のことを確認してください。
>
> - StyleBook 定義には、依存する StyleBook はありません。
> - StyleBook 定義から作成された構成パックはありません。



以前は、次のことをしなければなりませんでした:

1. StyleBook をダウンロードしてください。
2. ADM から削除します。
3. 定義をオフラインで更新します。
4. それを ADM にインポートし直します。

この機能を使用すると、定義を所定の位置に更新できます。

[NSADM-67726]

StyleBook の定義に新しいデータ型と組み込み **IP** 関数

ADM StyleBooks では、新しい IP 機能を容易にするために、`ipnetwork` データ型がサポートされるようになりました。このデータ型には、2 つの部分があります。最初の部分は IP アドレスで、2 番目の部分はネットマスクです。

ネットマスクは、ネットマスク長（`netmask-len`）またはネットマスクの IP アドレス（`netmask_ip`）を使用して表されます。IPv6 アドレスのネットマスク長は、0 ～32 ～128 の整数です。これは、ネットワーク内の IP アドレスのカウントを決定するために使用されます。

新しい組み込み IP 関数は次のとおりです。

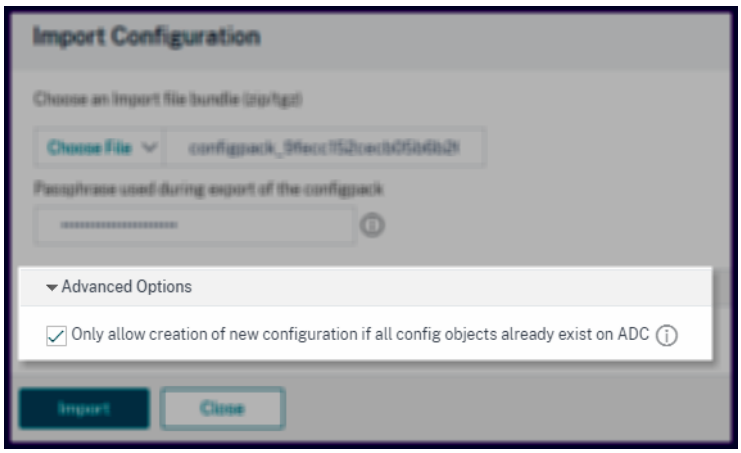
- `ip_network()`: IP アドレスとネットマスク長を入力として受け取ったときに、IP ネットワーク表記を返します。
- `network_ip()`: 指定された IP ネットワークの最初の IP アドレスを返します。
- `subnets()`: 指定した IP ネットワークとネットマスク長からのサブネットのリストを返します。
- `netmask_ip()`: 指定された IP ネットワークのネットマスク IP アドレスを返します。

- broadcast_ip(): 指定された IP ネットワークのブロードキャスト IP アドレスを返します。
- cidr(): 指定された IP ネットワークの CIDR 表記を返します。
- is_cidr(): この関数はipnetworkの値を受け入れます。そして、指定された値が IP ネットワークの CIDR 表記と一致した場合にTrueが返されます。
- is_in_network(): この関数は、ipnetworkおよびipaddressの値を受け入れます。そして、指定された値が IP ネットワークの CIDR 表記と一致した場合にTrueが返されます。

[NSADM-56083]

StyleBook 構成のインポート中に詳細オプションが導入されました

StyleBooks > [構成**]** で、[構成のインポート] オプションに詳細オプションが含まれるようになりました。このオプションは、ADC インスタンス上にすでに設定オブジェクトがある構成パックをインポートする場合に便利です。



同じ ADC インスタンスを 2 つの ADM サーバに追加することを考えてみましょう。また、ADM サーバの 1 つが、その ADC インスタンスに構成パックを展開しています。その構成パックを別のサーバー (または ADM サービス) に移行する場合は、ローカルコンピューターにエクスポートします。次に、構成パックをインポートする ADM サーバーでこのオプションを使用します。このオプションは、設定オブジェクトを ADC インスタンスに再デプロイせずにインポートします。

[NSADM-62743]

すべての **API** トラフィックの **API** 分析の表示

[**API** ゲートウェイ**] > [API** 分析] ページに、すべての API リクエストと応答が表示されるようになりました。以前は、このページには、レート制限または認証ポリシーを設定した API トラフィックのみが表示されていました。

[NSADM-62936]

サービスグラフの改善

マイクロサービスサービスグラフで、管理者として、次の情報を分析できます。

- エッジ幅に基づくサービス間のヒット数。
- レビューまたはクリティカルステータスのサービスの理由。

サービスアイコン	説明
	エッジの幅は、ヒット数を示します。エッジの幅が大きいほど、ヒット数が多くなることを示します。
	警告アイコンが付いたサービスは、サービスにエラーがあることを示します。
	ストップウォッチアイコンが付いたサービスは、サービスにレイテンシーまたは応答時間の問題があることを示します。
	ストップウォッチと警告アイコンの両方があるサービスは、サービスにエラーと遅延/応答時間の問題の両方があることを示します。

> 注:
>
> サービスに警告アイコンまたはストップウォッチアイコンがない場合は、そのサービスに Hits の異常またはしきい値違反があることを示します。

[NSADM-65798]

解決された問題

- **Gateway Insight** で、レポートをスケジュールすると (**[**レポートのエクスポート**] > [**エクスポートのスケジュール**]**)、生成されたレポートに「ページが見つかりません」と表示されます。

  [NSHELP-25496]

- ADM で ADC インスタンスを追加するときに、Citrix ADC プロファイルとして SNMP v2 を選択すると、ADM IP アドレスが SNMP マネージャとして追加されます。

  [NSHELP-26245]

- [ネットワーク**] > [**構成ジョブ] で、[実行頻度**]** が次のように設定されていると、スケジュールされた構成ジョブは指定された時刻に従って実行されません。
  - 特定の曜日です。
  - 月の特定の日付。

  [NSHELP-26034]
- 次の条件が満たされると、DNS サーバーなしで ADM の登録または更新が失敗します。
  - プロキシサーバが有効になっています。
  - エージェントは IP アドレスを取得できません。

  [NSHELP-25835]
- 場合によっては、ADM GUI でインスタンスライセンスの表示に失敗することがあります。

  [NSADM-67697]

2021 年 **1** 月 **29** 日

IPAM は、割り当てられた **IP** アドレスのリソースを表示します

IPAM ネットワークから割り当てられた IP アドレスの詳細を表示できるようになりました。

- **Module**: IP アドレスを予約した ADM モジュールを表示します。たとえば、IP アドレスが StyleBooks によって予約されている場合、この列には StyleBooks がモジュールとして表示されます。
- リソースタイプ: そのモジュールのリソースタイプを表示します。StyleBooks モジュールでは、設定リソースタイプだけが IPAM ネットワークを使用します。したがって、この列の下に [構成] が表示されます。
- リソース **ID**: リンク付きの正確なリソース ID を表示します。このリンクをクリックして、IP アドレスを使用しているリソースにアクセスします。構成リソースタイプの場合、構成パック ID がリソース ID として表示されます。

[NSADM-62751]

解決された問題

インスタンスが FQDN として構成され、名前にハイフン（「-」）が含まれている場合は、Citrix ADM から Citrix ADC SDX インスタンスを削除できません。
[NSHELP-26022]

プロキシサーバが有効になっていて、エージェントがその IP アドレスを取得できない場合、DNS サーバなしで ADM の登録または更新に失敗します。
[NSHELP-25835]

2021 年 1 月 13 日

サービス・グラフ：サービス・キー・メトリック・トレンドの表示

サービスグラフで、表形式ビューを使用して次の項目を確認できるようになりました。

- サービスの主なメトリック
- ソースサービスと宛先サービス間の主要なメトリック

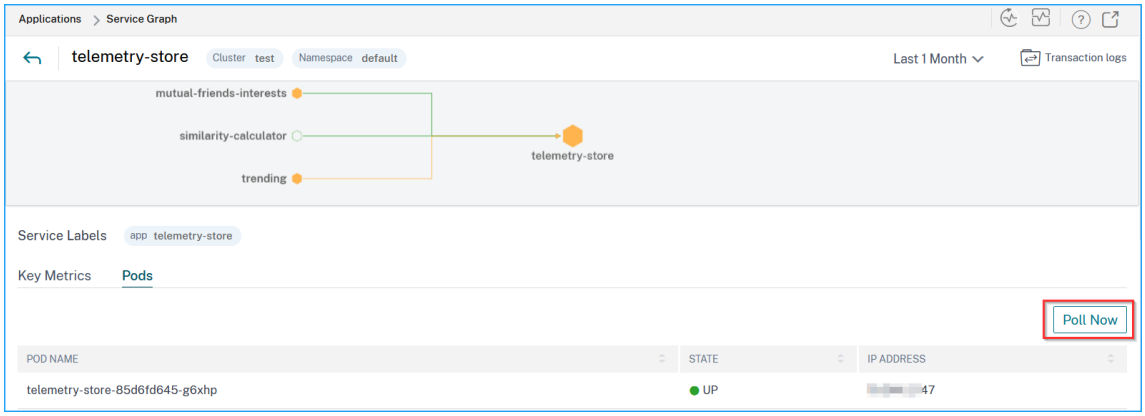
管理者は、これらの主要なメトリックを使用して、選択した期間におけるゴールデンシグナルの傾向を分析できます。詳しくは、「サービス詳細の表示」を参照してください。

[NSADM-65163]

サービスグラフ**-[**今すぐポーリングする**]** オプションを使用して **Pod** ステータスを取得します

サービスグラフで、[今すぐポーリング] オプションを使用して最新の Pod ステータスを取得できるようになりました。[今すぐポーリングする] オプションは、クラスターから最新の Pod ステータスをフェッチします。

1. ノードをクリックし、[詳細の表示] を選択します。
2. [ポッド] タブで、[今すぐ投票] をクリックします



[NSADM-62963]

動的リストを追加するための新しい **StyleBook** 属性

StyleBook 定義で、`allow-new-values` 属性を追加して、パラメータの動的リストを追加できるようになりました。ユーザーがこの StyleBook を選択して構成を作成すると、ユーザーは新しい値をリストに追加できます。

allow-**new**-values属性とallowed-values属性を組み合わせて使用できます。この組み合わせにより、パラメータの有効な値のリストを定義し、新しい値を受け入れることができます。

例:

```
-
      name: port
      type: tcp-port
      allowed-values:
            - 80
            - 81
            - 8080
      allow-new-values: true
<!--NeedCopy-->
```

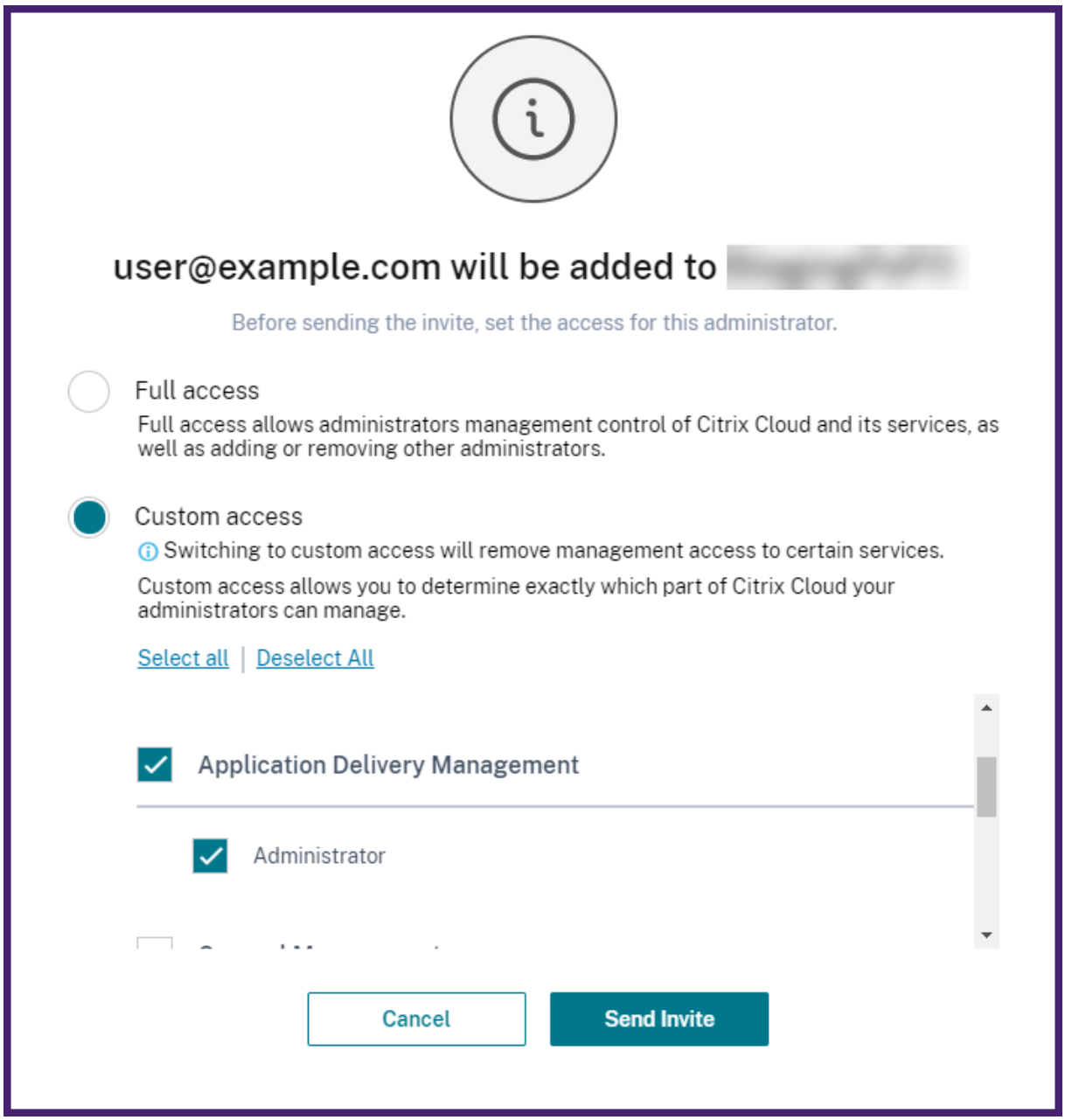
この例では、構成パックの作成/更新中に 80、81、8080 から選択するか、パラメータポートの新しい値を入力できます。詳しくは、「新しい値を許可」を参照してください。

[NSADM-62749]

ADM サービスへのカスタムアクセス権を持つユーザーを招待する

スーパー管理者として、カスタムアクセス権を持つ新しいユーザーを招待して ADM サービスを使用できるようになりました。このオプションでは、Citrix Cloud の ADM サービスにのみユーザーアクセスを制限できます。以前は、ADM サービスのみにアクセスするようにユーザーを招待することができませんでした。だから、フルアクセスで招待状を送らなければなりませんでした。

Citrix Cloud で新しいユーザーを招待するには、[アイデンティティアクセス管理] **>** [管理者] に移動します。[カスタムアクセス] オプションで、[**Application Delivery Management**] を選択します。デフォルトでは、管理者ロールが選択されています。



招待リンクは、指定されたユーザーの電子メールアドレスに送信されます。また、ユーザーは、このリンクを使用して管理者として Citrix ADM にログオンできます。管理者アクセスを使用すると、ユーザーは次の操作を実行できます。

- ADM で ADC インスタンスを追加および管理します。
- StyleBook を使用して、ADC インスタンスに設定をデプロイします。
- ADC インスタンスのプール容量ライセンスを設定します。
- AutoScale グループを作成および設定します。

> 注
>
> 管理者は、Citrix Cloud から ADM GUI にアクセスできます。ただし、[アカウント] > [ユーザー管理] ページ

> は制限されています。スーパー管理者は、必要に応じてこのページへのアクセス権を付与できます。

招待を送信し、ユーザを設定する方法の詳細については、「Citrix ADM でのユーザーの構成」を参照してください。

[NSADM-55384]

解決された問題

- Gateway Insight で、[ゲートウェイ] の下に表示される合計数が正しくありません。

  [NSHELP-25729]

- [ネットワーク] **>** [構成ジョブ] **>** [ジョブの作成] で [構成ソース] の下の [録音と再生] を選択すると、次のエラーメッセージが表示されます。

  ```
  Unable to get config diff for: <instance IP>
  ```

  [NSADM-63986]

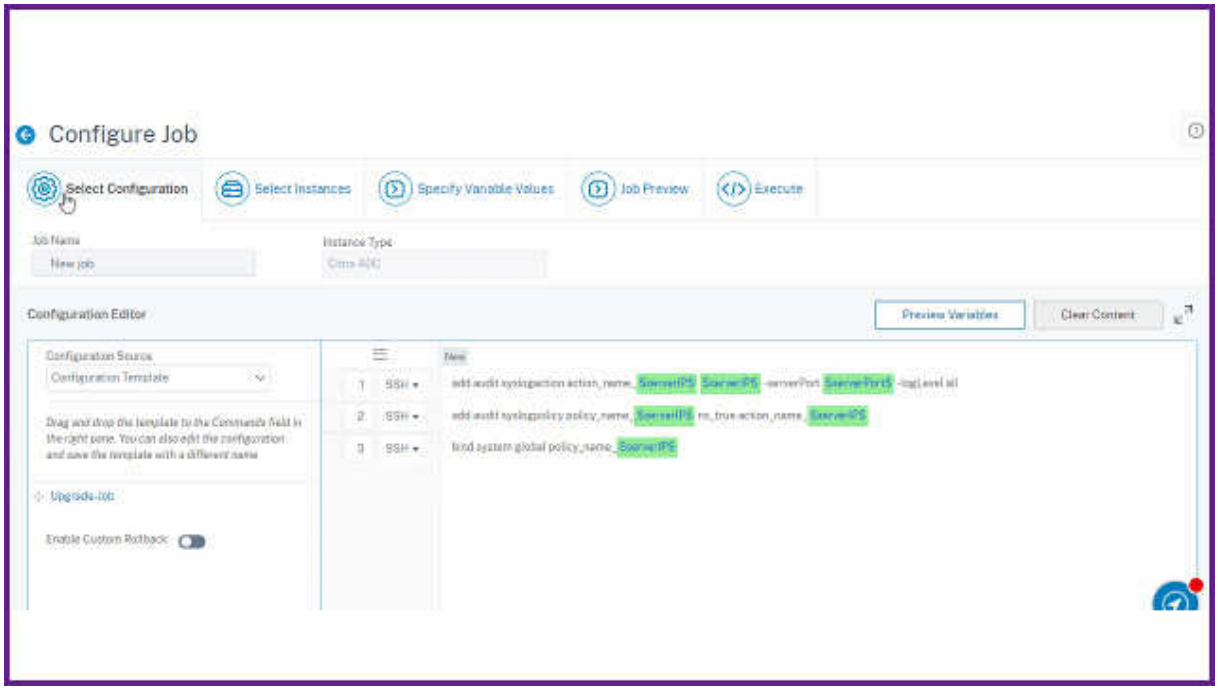
- グループのアプリケーションで無効な正規表現を指定し、手動で少数のアプリケーションを選択すると、正規表現が無効であると、手動で選択したアプリケーションは表示されません。

  [NSHELP-25739]

2020 年 **12** 月 **17** 日

既存の設定ジョブのタブを切り替える

既存の構成ジョブを編集するときに、任意のタブに切り替えることができます。たとえば、[構成の選択] タブが表示されている場合は、[ジョブプレビュー] タブに切り替えることができます。以前は、次のタブに直線的に移動することができました。たとえば、[構成の選択] タブからは、[インスタンスの選択] タブにのみ移動できました。

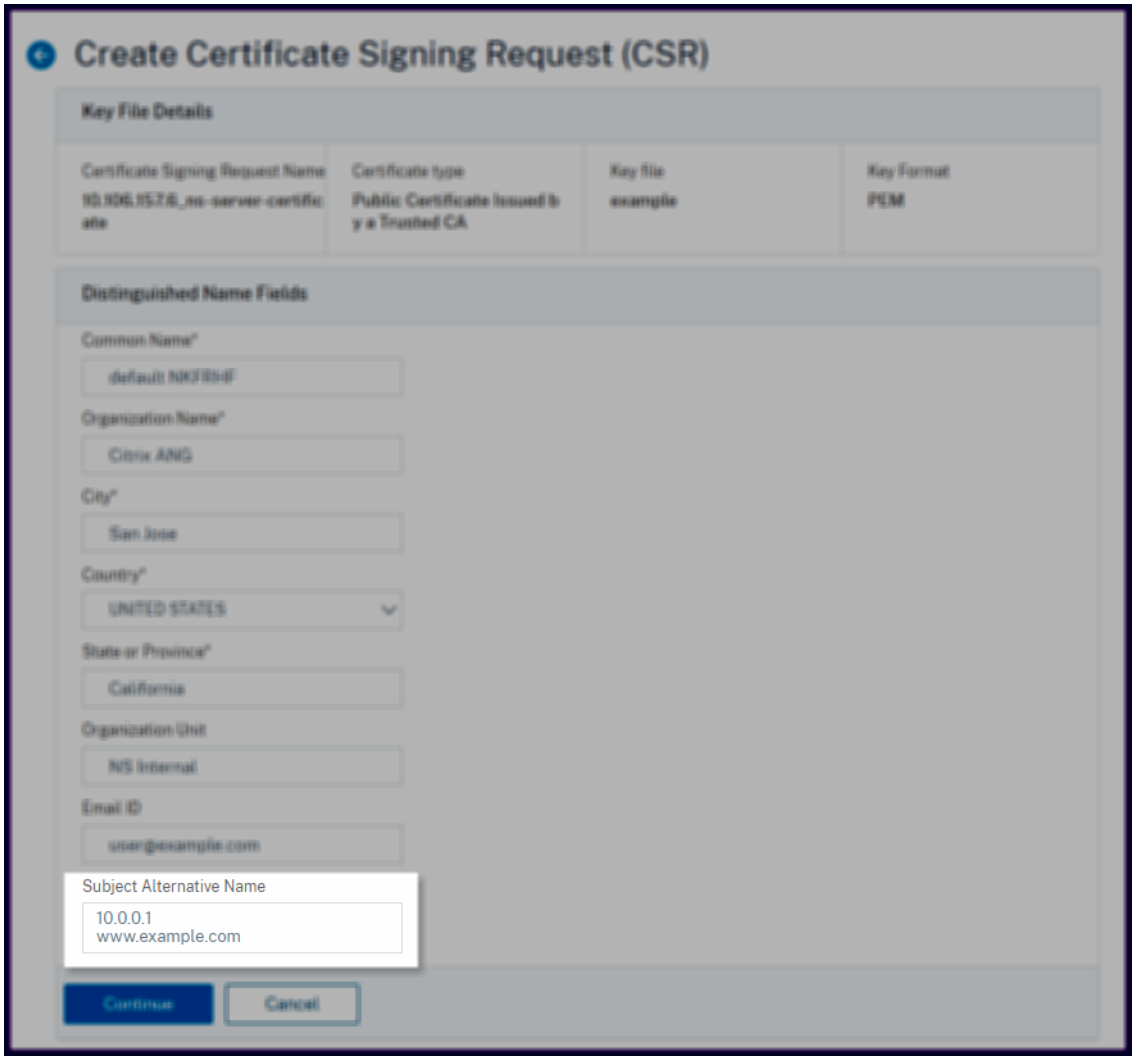


[NSADM-42944]

サブジェクトの代替名を持つ **CSR** の作成

サブジェクト代替名を使用して証明書署名要求 (CSR) を作成できるようになりました。この機能を使用すると、単一の証明書で複数のドメインを保護できます。

選択した SSL 証明書の CSR 作成時に、複数のサブジェクト代替名を含めることができるようになりました。これらの値は、ドメイン名と IP アドレスにすることができます。詳しくは、「証明書署名要求 (CSR) の作成」を参照してください。



[NSADM-51556]

アプリのセキュリティ違反-ボット

［セキュリティ違反］で、［ボット違反］カテゴリで **Citrix Gateway** のアカウント乗っ取りを表示できるようになりました。詳しくは、「違反カテゴリ」を参照してください。

[NSADM-57698]

ボットの洞察-モバイル **(Android)** アプリケーションのボットカテゴリを表示する

ボットインサイトで、モバイルネットワークを介して検出された次のボットカテゴリを表示できるようになりました。

- Web クライアントレート制限
- Android レート制限
- Web クライアントデバイス

- Android 端末

詳しくは、「ボットの洞察」を参照してください。

[NSADM-57724]

解決された問題

- ［ネットワーク］**>**［イベント］**>**［イベントの概要］で、Citrix ADC SDX 関連のイベントをクリックすると、GUI が［イベント］ページにリダイレクトされますが、データは表示されません。

  [NSHELP-25630]

- ADM サービスは、ログインセッションの有効期限タイムアウトおよびログアウト API を使用しません。その結果、ユーザーセッションは有効なままになります。

  [NSADM-63819]

- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。

  [NSADM-5882]

2020 年 **12** 月 **02** 日

アプリケーションの使用状況に関する異常の表示

管理者は、アプリケーションがどのように利用されているかを確認する必要があります。アプリケーションキーメトリックは、アプリケーションの使用状況を特定するのに役立ちます。アプリケーションへのトラフィック範囲は予測できないため、特定の期間において、アプリケーションパフォーマンスの異常な偏差が発生することがあります。このようなシナリオでは、管理者として、このような突然の異常を表示し、直ちにトラブルシューティングが必要な場合に確認することができます。
Citrix ADM は、このような異常を検出し、必要な詳細を提供します。

詳しくは、「アプリケーションの使用状況と異常」を参照してください。

[NSADM-54677]

セキュリティ違反の機密度レベルの選択

過剰なクライアント接続と Web サイトスキャン違反の場合、動作確認プロファイルを作成し、感度レベルを [低]、[中]、[高] として選択できるようになりました。プロファイルを作成することで、これらの違反に対する異常の総数を Citrix ADM で報告する方法を決定できます。

詳しくは、「動作確認プロファイルの設定」を参照してください。

[NSADM-59536]

アプリのスコアを計算するためのアプリケーションの **CPU** 使用率

管理者は、アプリケーションが使用する CPU を監視できます。アプリの CPU 使用率のしきい値を設定して、アプリの最終スコアを決定することもできます。[アプリスコアの構成] ページでは、[アプリ **CPU** 使用率] を選択し、下限および上限しきい値を構成できます。

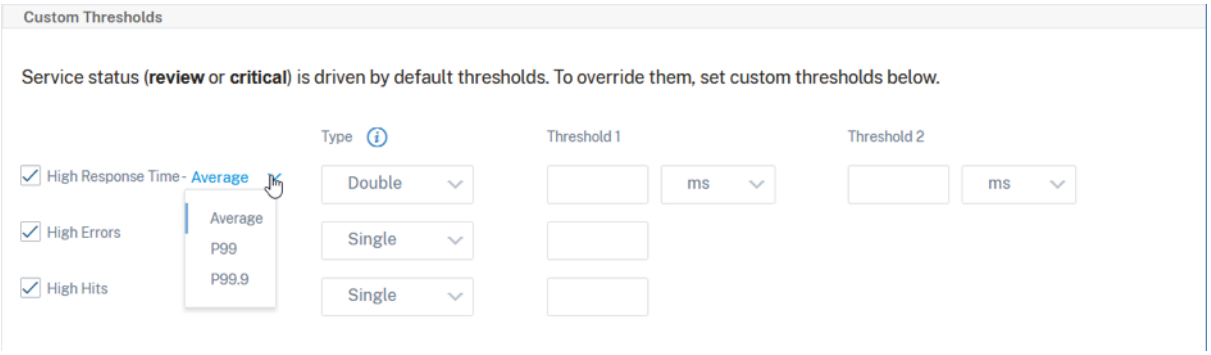
詳しくは、「アプリケーションの平均 CPU 使用率」および「アプリのスコアコンポーネントを選択し、しきい値を設定する」を参照してください。

[NSADM-57468]

サービスグラフでのしきい値の設定

サービスグラフで、次のメトリックのしきい値を選択して設定し、サービスのスコアとステータスを計算できます。

- 高い応答時間（平均、P99、P99.9）
- エラーが高い
- ハイヒット



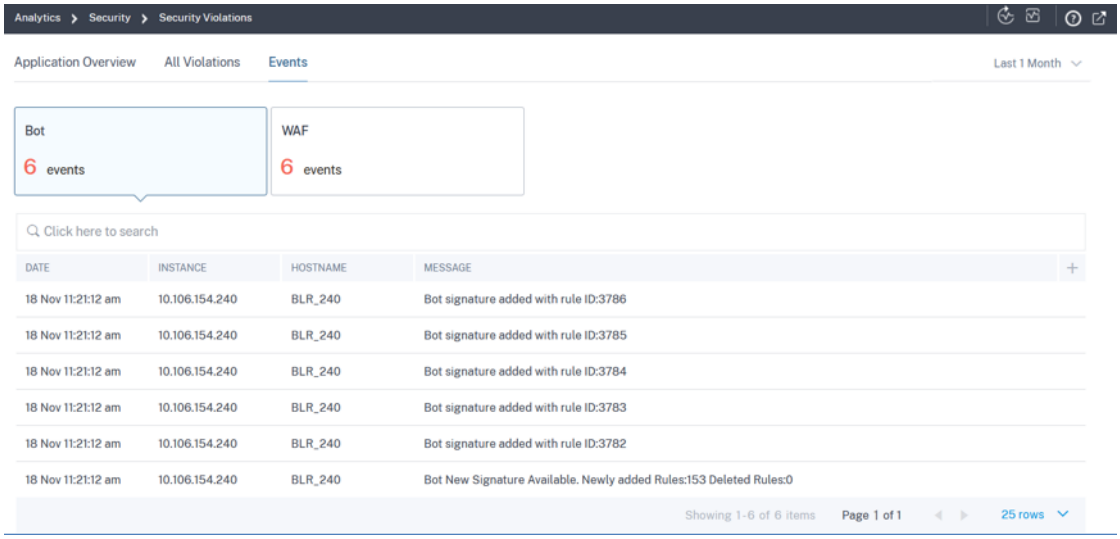
> 注
>
> Citrix ADM は、選択したメトリックに基づいてサービスの最終スコアとステータスを計算します。たとえば、しきい値の構成で［High Hits］のみを選択した場合、Citrix ADM はデフォルトのしきい値（応答時間 = 200 ミリ秒、エラーカウント = 0）と高いヒットを使用してサービススコアを計算します。

詳しくは、「サービスグラフでのしきい値の設定」を参照してください。

[NSADM-59731]

セキュリティ違反のイベント履歴を表示する

セキュリティ違反で、ボットインサイトとセキュリティインサイトのイベント履歴を表示できるようになりました。[分析] **>** [セキュリティ] **>** [セキュリティ違反] に移動し、[イベント] タブをクリックして、ボットと WAF イベントを表示します。



[NSADM-62684]

インフラストラクチャ分析の改善

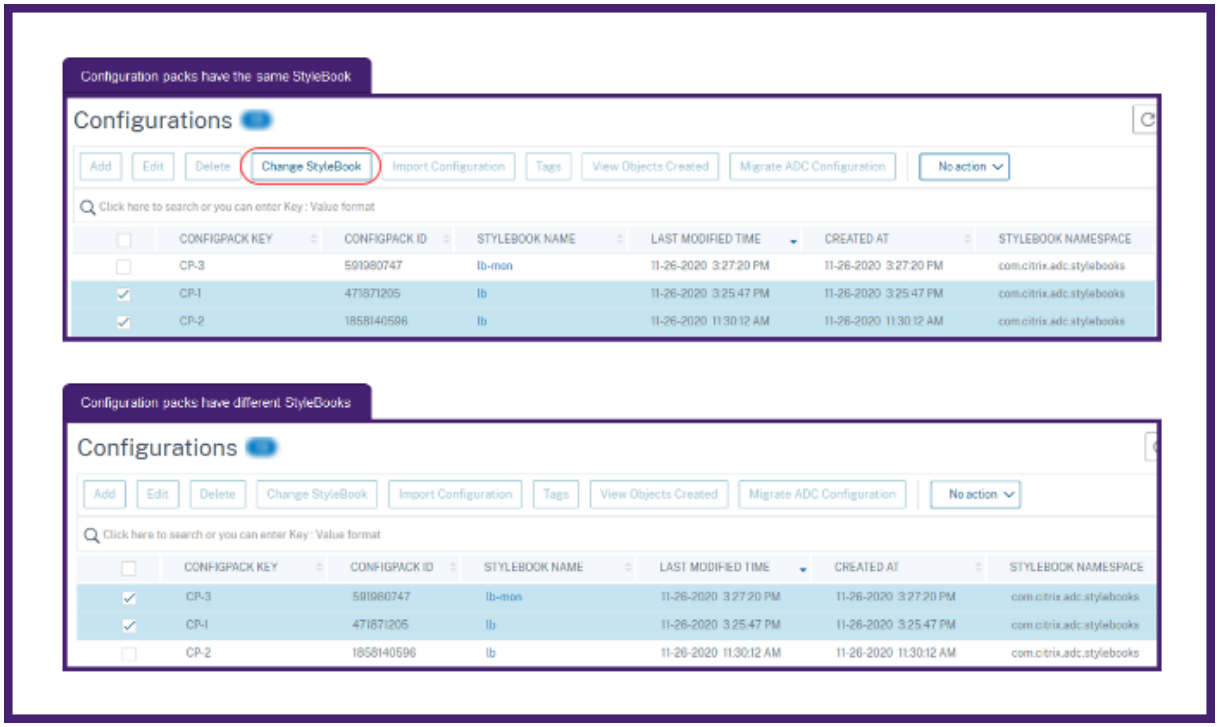
インフラストラクチャ分析では、ユーザーエクスペリエンスを向上させるいくつかのテーマの更新が UI に対して行われます。

[NSADM-57697]

複数の構成パックの **StyleBook** を一度に変更

複数の構成パックの StyleBook を一度に変更できるようになりました。既存の StyleBook を新しい StyleBook に置き換える場合、関連するすべての構成パックまたは複数の StyleBook を 1 つの操作で変更できます。以前は、StyleBook を変更するために、各構成パックを 1 つずつ選択する必要がありました。

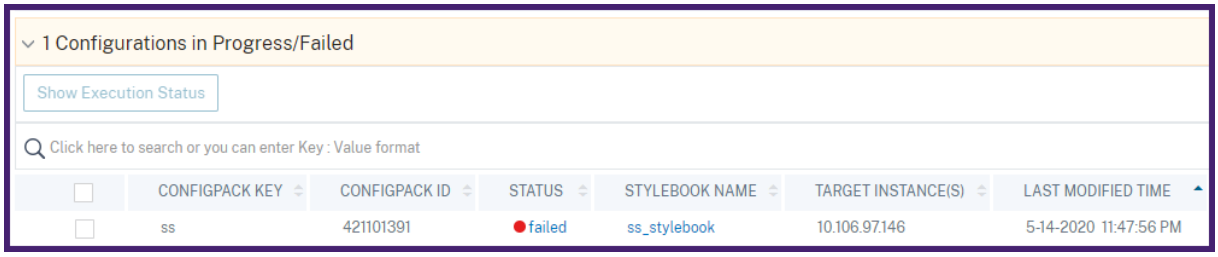
> 注:
>
> 同じ StyleBook に関連付けられている構成パックを選択してください。そうしないと、StyleBook の変更オプションが使用できなくなります。



選択した構成パックについて、次の条件が満たされると、ADM は StyleBook を正常に変更します。

- 既存の StyleBook のすべての構成パラメータが、選択した StyleBook に存在する必要があります。
- 選択した StyleBook の新しいパラメータはオプションです。

選択した構成パックの進行状況を確認するには、[構成] ページの **[**進行中**/**失敗] の [構成] を選択します。



詳しくは、「複数の構成パックがある StyleBook を変更する」を参照してください。

[NSADM-57941]

AutoScale アプリケーションのアクセスタイプを変更する

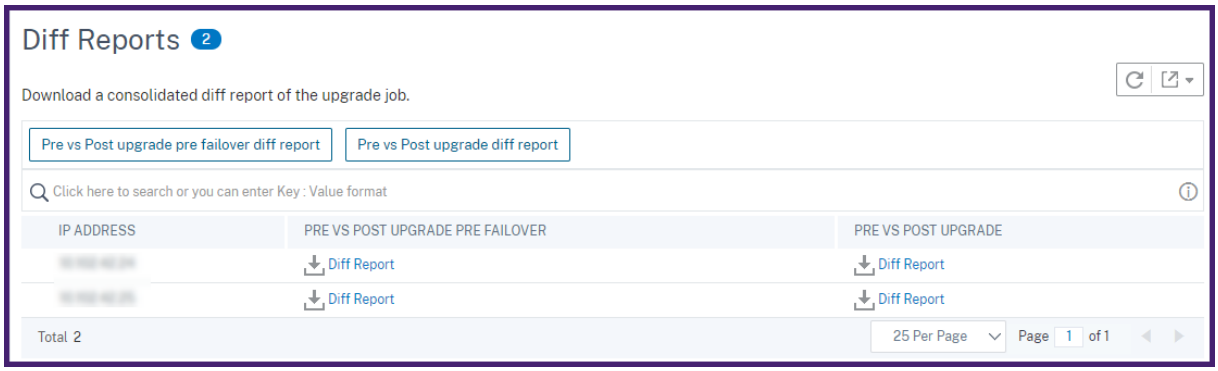
ADM は、DNS または Route 53 トラフィック分散を持つ AutoScale アプリケーションのアクセスタイプの変更をサポートするようになりました。したがって、すべての AutoScale アプリケーションのアクセスタイプを変更できます。
以前は、アクセスタイプの変更は、ALB または NLB トラフィック分散があるアプリケーションでのみサポートされていました。

[NSADM-57029]

ADC アップグレード・ジョブの統合差分レポートのダウンロード

ADC アップグレードジョブの統合差分レポートをダウンロードできるようになりました。このレポートには、アップグレード前スクリプトとアップグレード後のスクリプトの出力の違いが含まれます。したがって、アップグレード後に ADC インスタンスでどのような変更が行われたかを判断できます。

> 注
>
> 相違レポートが生成されるのは、アップグレード前およびアップグレード後の段階で同じスクリプトを指定した場合だけです。したがって、アップグレード後の段階で [アップグレード前のスクリプトと同じスクリプトを使用] を選択してください。



次のタイプの相違レポートをダウンロードできます。

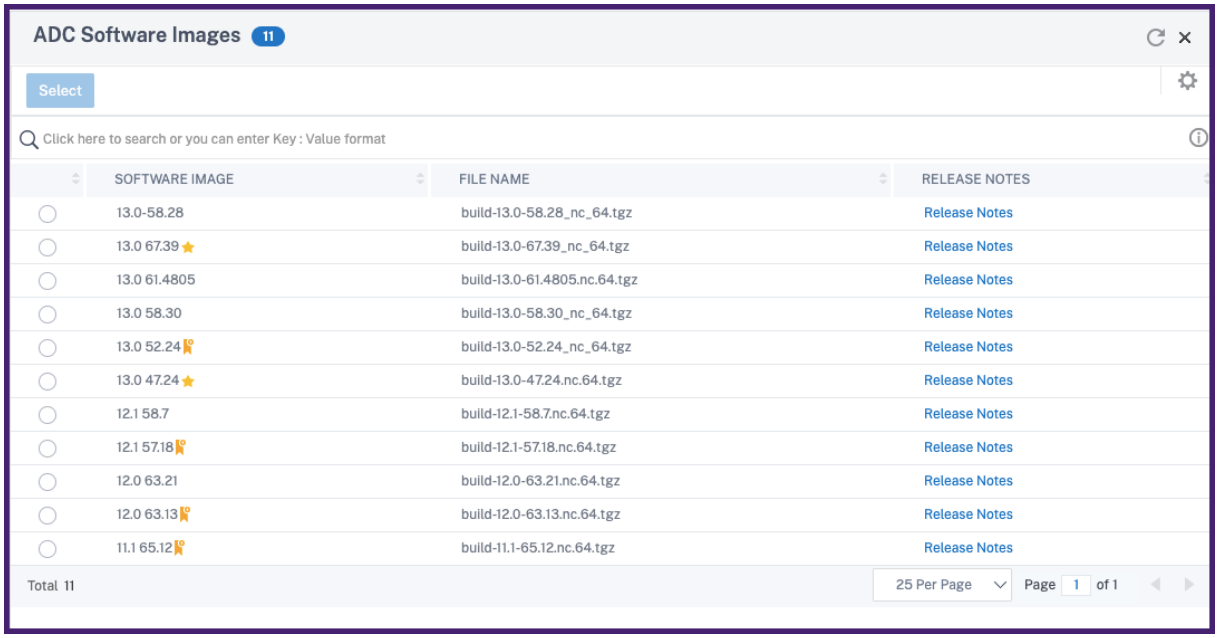
- アップグレード前とポストアップグレード前のフェイルオーバー差分レポート
- アップグレード前対アップグレード後の差分レポート

詳しくは、「ADC アップグレード・ジョブの統合差分レポートのダウンロード」を参照してください。

[NSADM-50200]

アップロードせずに **ADC** イメージを選択する

ADC アップグレードジョブを作成するときに、アップロードせずに ADC イメージを選択できるようになりました。このオプションでは、Citrix ダウンロード Web サイトで使用可能なすべての ADC イメージが一覧表示されます。選択した ADC イメージは、Citrix ダウンロードサービスからダウンロードされます。



詳しくは、「ジョブを使用して Citrix ADC インスタンスをアップグレードする」を参照してください。

[NSADM-52471]

修正された問題

ユーザーが **[** サブスクリプション**]** ページに移動して **[** ライセンス**]** をクリックすると、**[** サブスクリプション**]** ページに対する表示権限または編集権限を持っている場合でも、**[** 認証されていません**]** エラーが表示されます。

[NSHELP-25351]

ADM サービスは、ログインセッションの有効期限タイムアウトおよびログアウト API を使用しません。その結果、ユーザーセッションは有効なままになります。

[NSADM-63819]

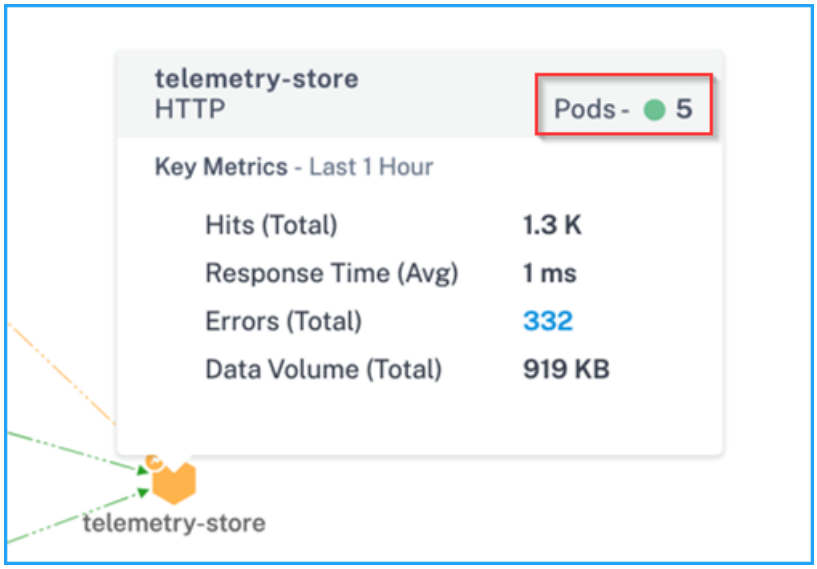
[分析**] > [**セキュリティ**] > [**セキュリティ違反] で、大量のクライアント接続を受信しても、過剰なクライアント接続インジケータに異常が表示されません。

[NSADM-64548]

2020 年 **11** 月 **11** 日

サービスグラフ ― 関連するバックエンドポッドの詳細をすべて表示

サービスグラフで、サービス上にマウスポインタを置くと、サービスに関連付けられた Pod の合計を表示できます。



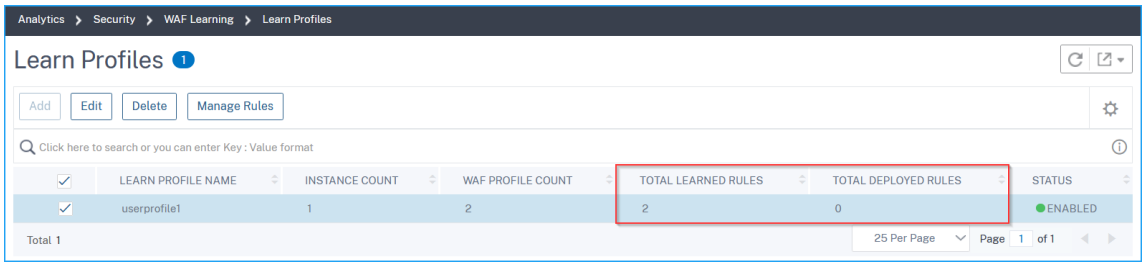
詳しくは、「サービス詳細の表示」を参照してください。

[NSADM-47395]

WAF 学習エンジンの改良

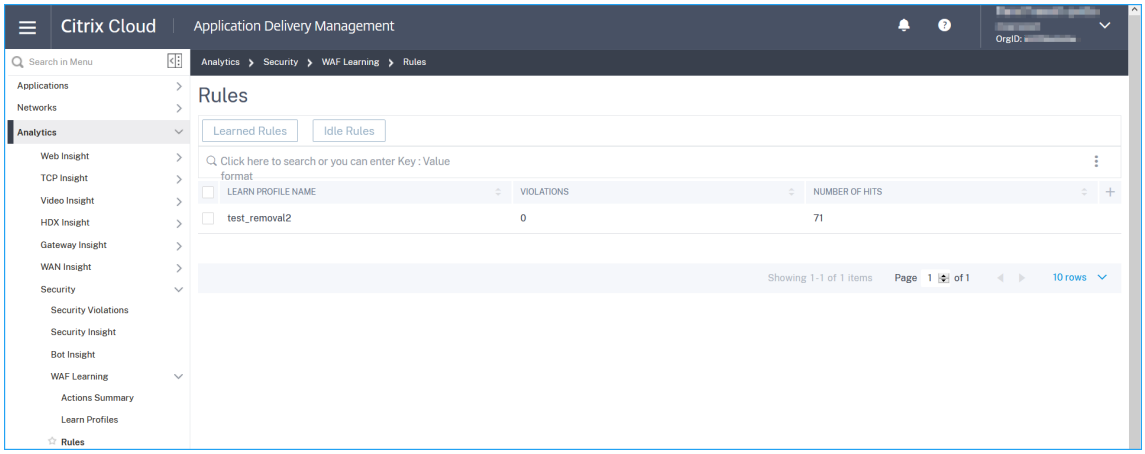
WAF ラーニングエンジンで、次の機能強化を表示できるようになりました。

- 「学習プロファイル」ページでは、学習済ルールの合計と配布済ルールの合計を表示できます。

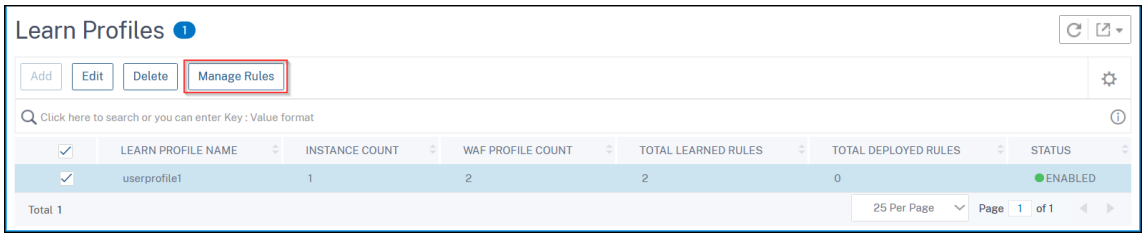


- [ルール] ページは使用できなくなりました。[ルールの管理] オプションが [プロファイルの詳細] ページに追加されます。プロファイル名を選択し、[**Manage Rules]** ボタンをクリックすると、学習されたルール、アイドルルール、および展開されたルールに関する関連情報にアクセスできます。

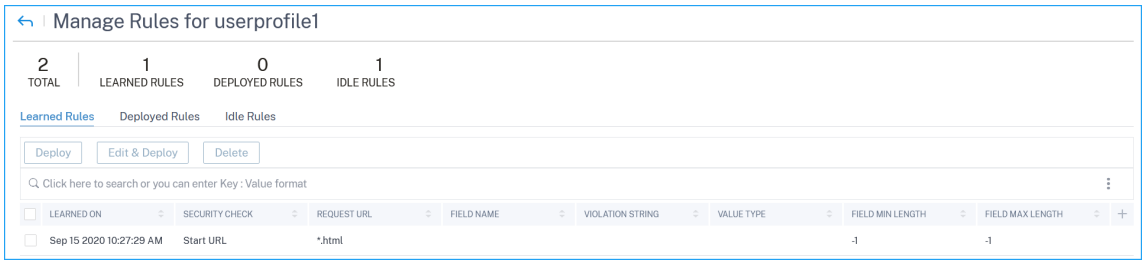
  以前:



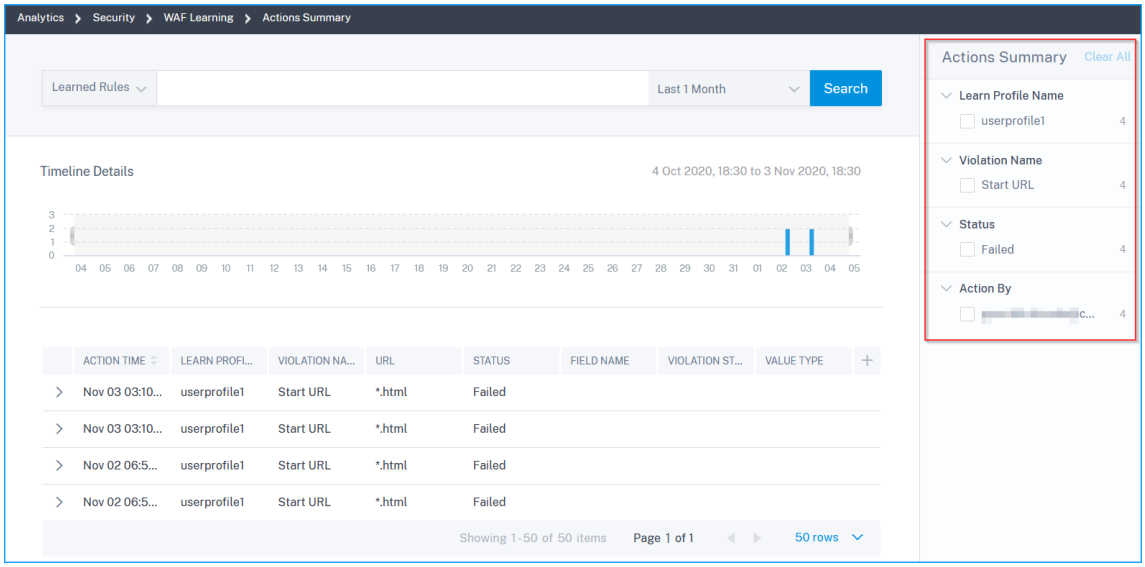
今:



- [**Manage Rules**] をクリックすると、選択したプロファイルのルールの合計、学習されたルールの合計、展開済みルールの合計、およびアイドル状態のルールの合計を表示できます。



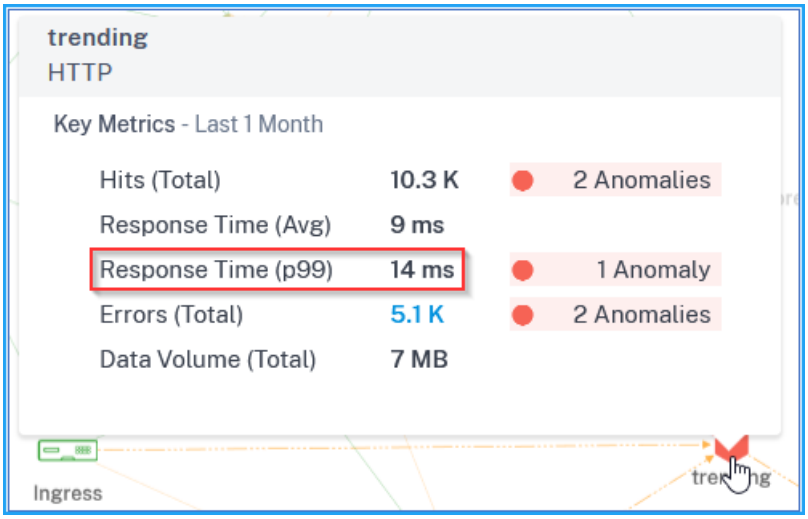
- [アクションの概要] ページで、[アクションの概要] のオプションを選択して、結果をフィルタできます。



詳しくは、「WAF ラーニングエンジン」を参照してください。

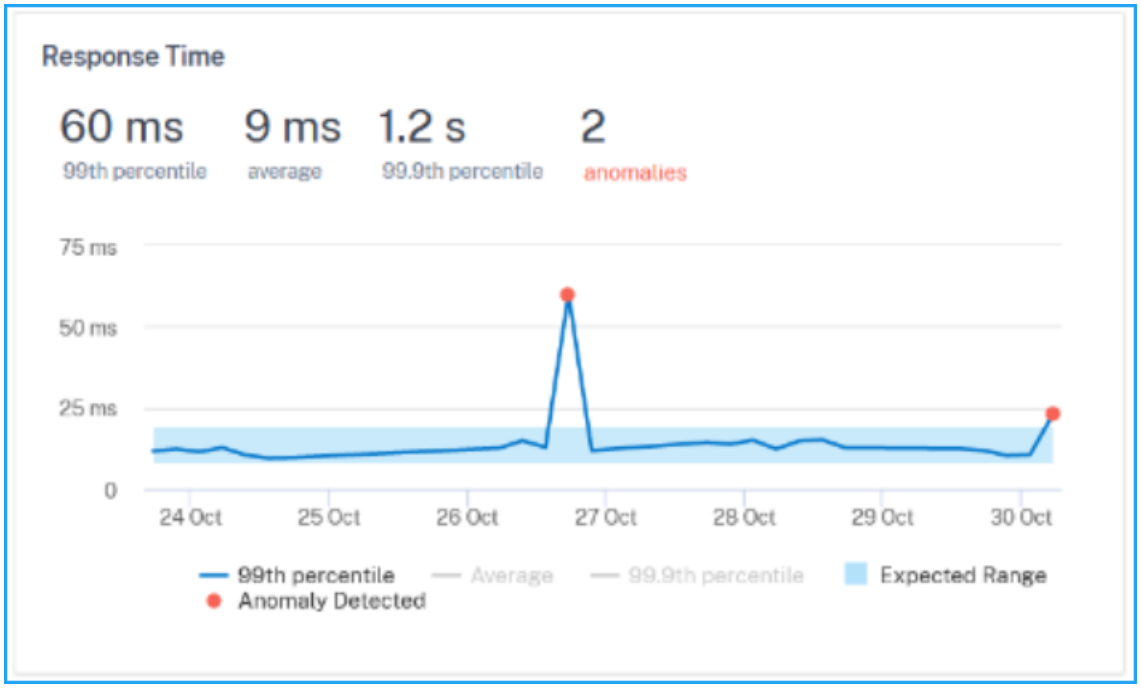
サービスグラフ：サービス応答時間の **Pxx** の値を表示する

サービスグラフで、サービスの上にマウスポイントを置いたときに、応答時間のPxxの値を表示できるようになりました。



[**Response Time**]（**p99**）：選択した期間におけるサービス応答時間の 99% が **p99** の値より小さいことを示します。

ドリルダウンしてサービスの詳細を表示する場合、選択した期間におけるレスポンス時間の 99 パーセンタイルおよび 99.9 百分位数も表示できます。



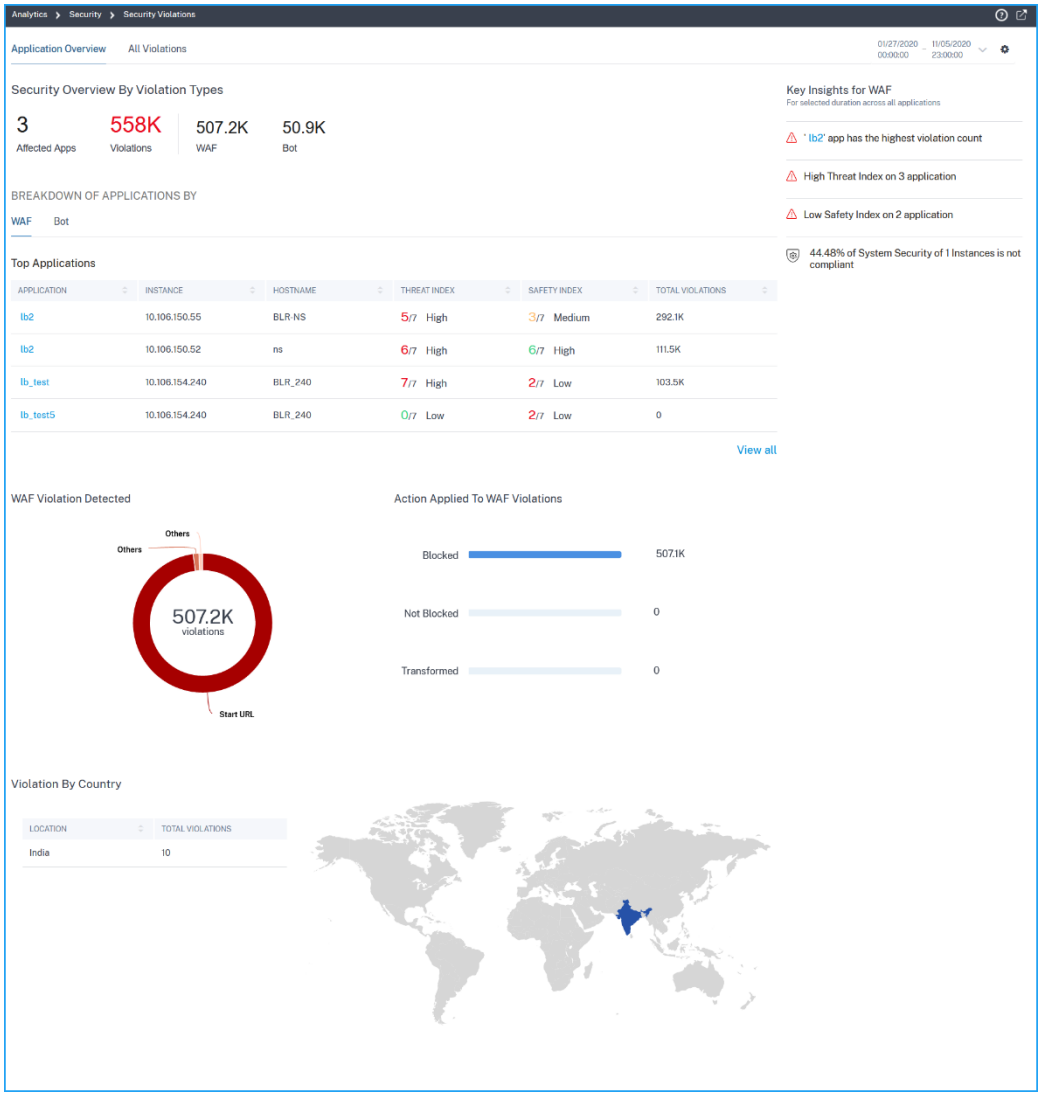
管理者として、pxxの値を使用すると、サービスの応答時間をよりよく理解できます。詳しくは、「サービス詳細の表示」を参照してください。

[NSADM-57729]

アプリのセキュリティ違反 ー セキュリティインサイトとボットインサイトの詳細でアプリケーションを視覚化

[分析] **>** [セキュリティ] **>** [セキュリティ違反] で、セキュリティインサイトとボットインサイトの両方に関連付けられた脅威の詳細を完全に可視化して、アプリケーションを視覚化できるようになりました。「セキュリティ違反」ページには、「すべての違反」および「アプリケーションの概要」オプションが追加されました。

- 「すべての違反」— アプリケーションのセキュリティ違反の詳細を表示します。
- [アプリケーションの概要] — 違反合計、WAF および Bot 違反の合計、上位アプリケーション、国別の違反などの情報を含む概要を表示します。



詳しくは、「アプリケーションのセキュリティ違反の詳細を表示する」を参照してください。

[NSADM-57174]

サービスグラフ-ゴールデンシグナルのメトリックを使用して **Kubernetes** サービスを監視する

Kubernetes クラスターで実行されているサービスのゴールデンシグナルメトリックは、特定の期間における潜在的な異常を検出できる一連のメトリックのことです。Kubernetes クラスターに 100 個のマイクロサービスがある場合、頻繁な問題があるサービスを特定するのは難しい場合があります。次の 3 つの主要なメトリックは、Citrix ADM サービスグラフが Kubernetes サービスの潜在的な異常を特定するのに役立つゴールデンシグナル指標です。

- ヒット数
- 応答時間（平均）と応答時間（P99）
- エラー

管理者は、これらのメトリックを使用して、次の操作を実行できます。

- サービスステータスの識別
  - **Critical** — サービスの複数のメトリックに異常またはしきい値違反がある
  - 確認 — サービスのいずれかのメトリックに異常またはしきい値違反がある
  - 良好 — 異常なし、またはしきい値違反のないサービス
- 各メトリックで識別される異常の数を分析する
- 問題のトラブルシューティングを行い、大きな影響を回避する

詳しくは、「サービス詳細の表示」を参照してください。

[NSADM-56399]

修正された問題

StyleBook

- StyleBooks では、既存の構成パックの [作成日] フィールドに無効な日付が表示されます。

[NSADM-62160]

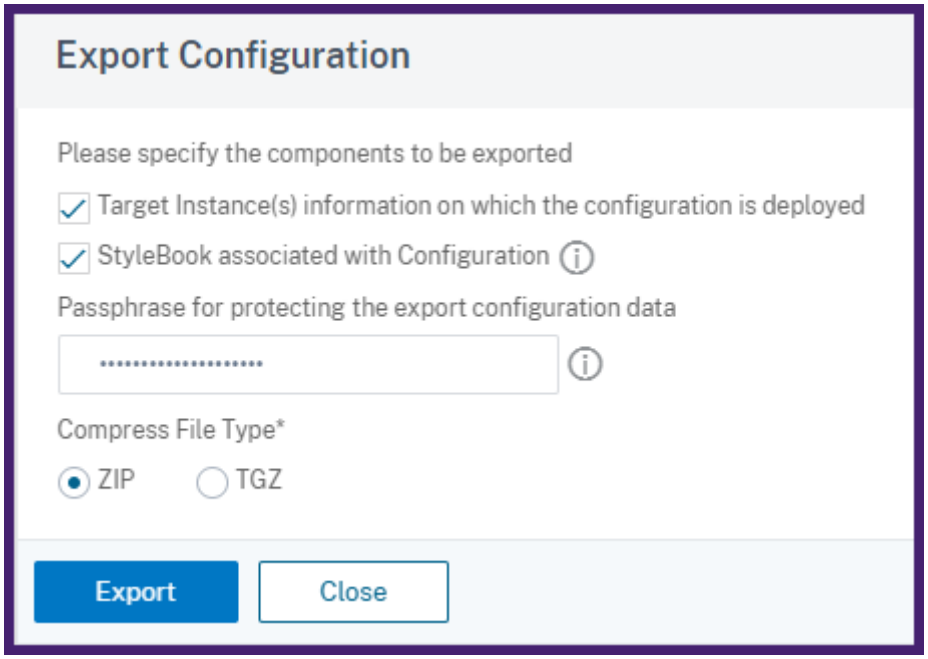
2020 年 10 月 27 日

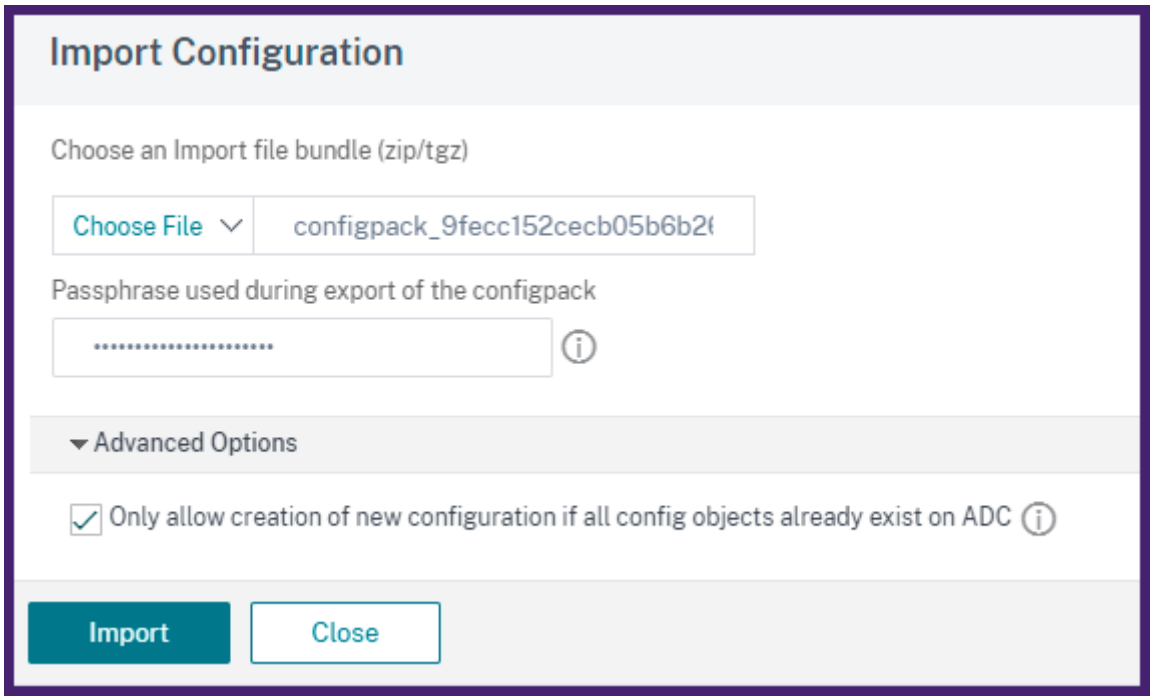
StyleBook 構成パックをエクスポートまたはインポートする

StyleBooks のような構成パックをエクスポートまたはインポートできるようになりました。この機能を使用すると、StyleBook 設定を別の ADM サーバーに簡単に共有できます。以前は、StyleBook をダウンロードして別の ADM サーバーにインポートし、そこから構成を作成する必要がありました。

構成パックをエクスポートすると、`tgz`または`zip`バンドルがローカルコンピュータにダウンロードされます。このバンドルには、設定パックで定義されたすべてのパラメーターを含む JSON ファイルが含まれます。指定されている場合は、ターゲットインスタンスの情報も含まれます。カスタム StyleBook の設定パックでは、StyleBook をエクスポートバンドルに含めることができます。エクスポートバンドルを暗号化するためのパスフレーズを指定します。このパスフレーズは、構成パックの機密データを保護します。

ローカルコンピューターから別の ADM サーバーに構成パックをインポートできます。構成パックをインポートするには、エクスポート時に指定したパスフレーズを使用します。詳しくは、「構成パックのエクスポートまたはインポート」を参照してください。





[NSADM-57935]

プールされたライセンス機能に対してのみ **ADM** サーバを構成する

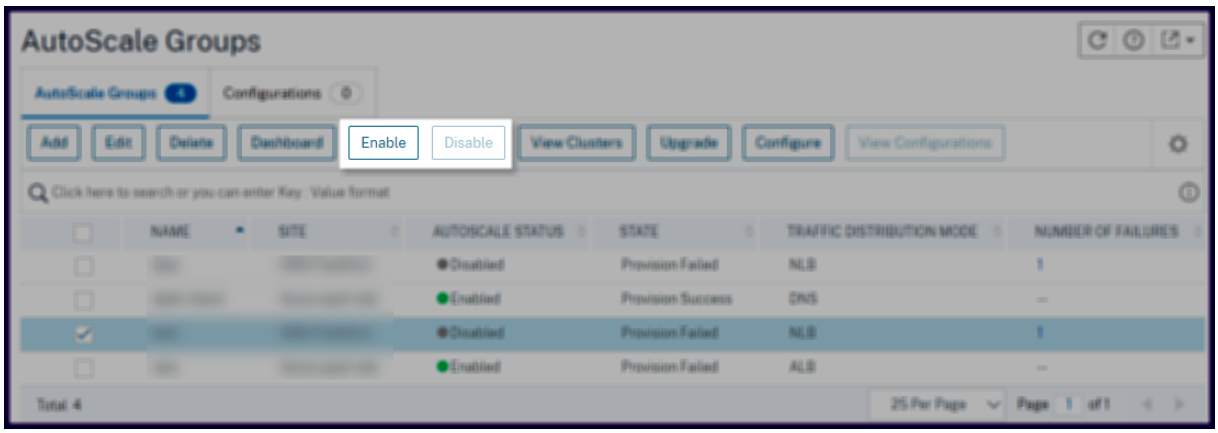
管理者は、プールされたライセンス機能に対してのみ ADM サーバーを構成できるようになりました。この構成は、ゾーン内の ADC データを制限する規制要件がある場合に役立ちます。ADM サービスは、ADC インスタンスからライセンスデータのみを受信します。また、グローバルにデプロイされた ADC インスタンス間で、プールされたキャパシティーライセンスを動的に割り当てることができます。詳しくは、「ADM サービスをライセンスサーバーとしての

み構成する」を参照してください。

[NSADM-47930]

AutoScale グループを編集せずに有効または無効にする

AutoScale グループを編集せずに有効または無効にできるようになりました。[ネットワーク**] > [AutoScale** グループ] ページに [有効または無効化] オプションが表示されます。また、[編集**]** オプションで AutoScale グループを有効または無効にすることもできます。



[NSADM-57802]

さまざまな **ADC** アップグレードステージでカスタム・スクリプトを実行

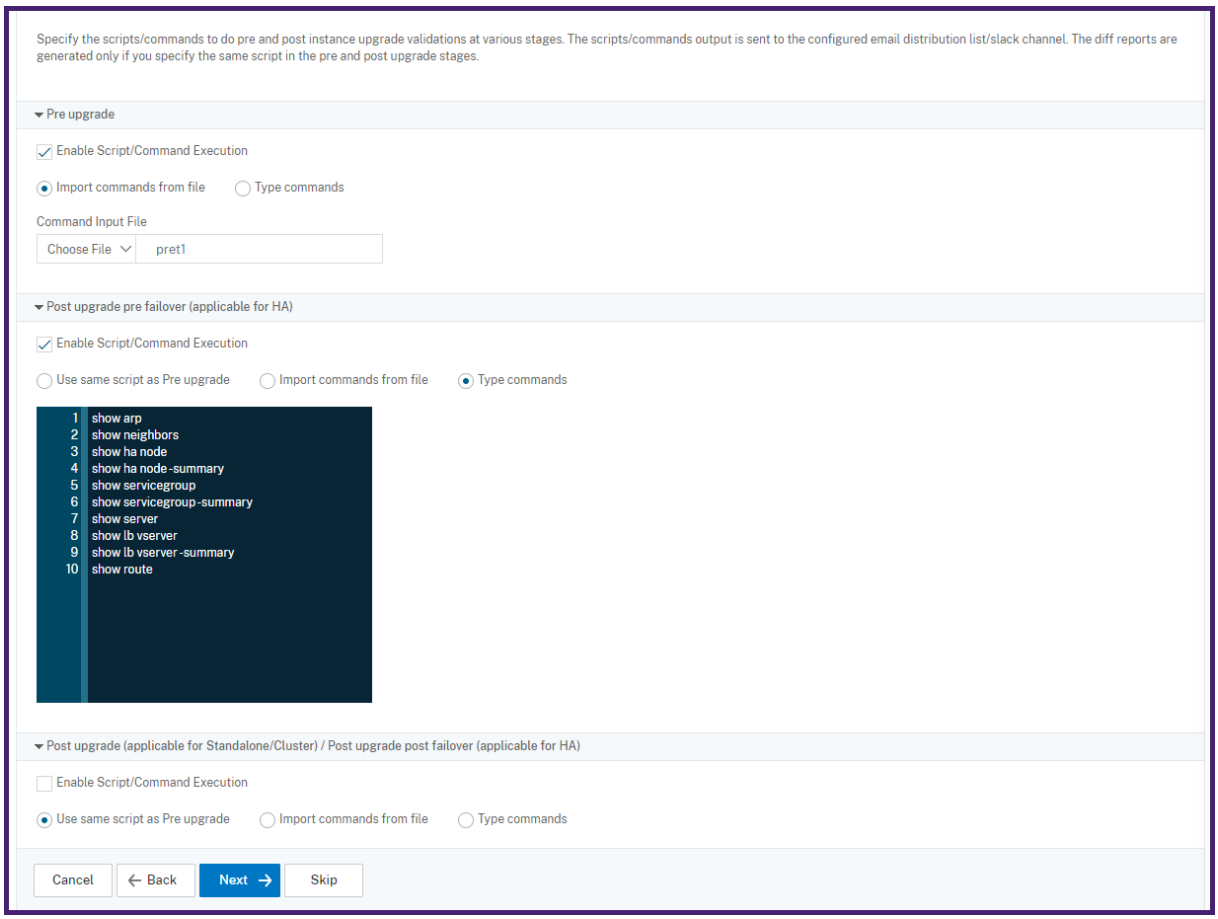
カスタムスクリプトは、ADC インスタンスのアップグレードの前後に変更をチェックするために使用されます。インスタンスのアップグレードには、複数のステージがあります。これで、これらのスクリプトを次の段階で実行するように指定できます。

- アップグレード前: インスタンスをアップグレードする前に、指定されたスクリプトが実行されます。
- アップグレード前のフェールオーバー後（**HA** に適用可能）: このステージは、高可用性配置にのみ適用されます。指定されたスクリプトは、ノードのアップグレード後、フェールオーバーの前に実行されます。
- アップグレード後（スタンドアロンに適用）**/**フェールオーバー後のアップグレード後（**HA** に適用可能）：指定されたスクリプトは、スタンドアロンデプロイでインスタンスをアップグレードした後に実行されます。高可用性展開では、スクリプトはノードとフェイルオーバーをアップグレードした後に実行されます。

この機能を使用すると、インスタンスアップグレードの各段階で発生した変更を確認できます。

> 注:
>
> 必要な段階でスクリプトの実行を有効にしてください。そうしないと、指定されたスクリプトは実行されません。

ADM GUI では、スクリプトファイルをインポートしたり、コマンドを直接入力したりできます。アップグレード後のステージでは、アップグレード前のステージで指定したスクリプトと同じスクリプトを使用できます。詳しくは、「ジョブを使用して Citrix ADC インスタンスをアップグレードする」を参照してください。

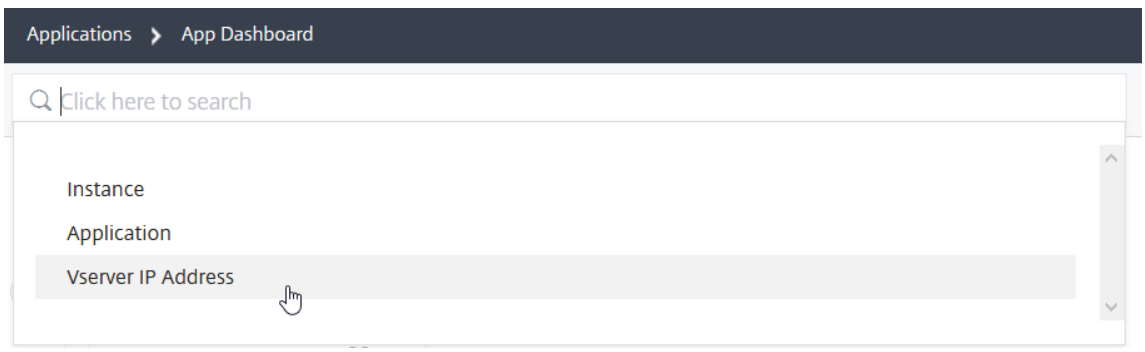


[NSADM-56649]

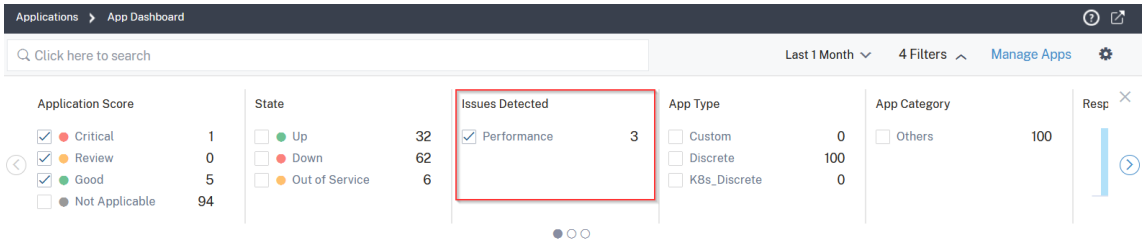
アプリケーションダッシュボードの改善

アプリダッシュボードで次の機能強化を表示できるようになりました。

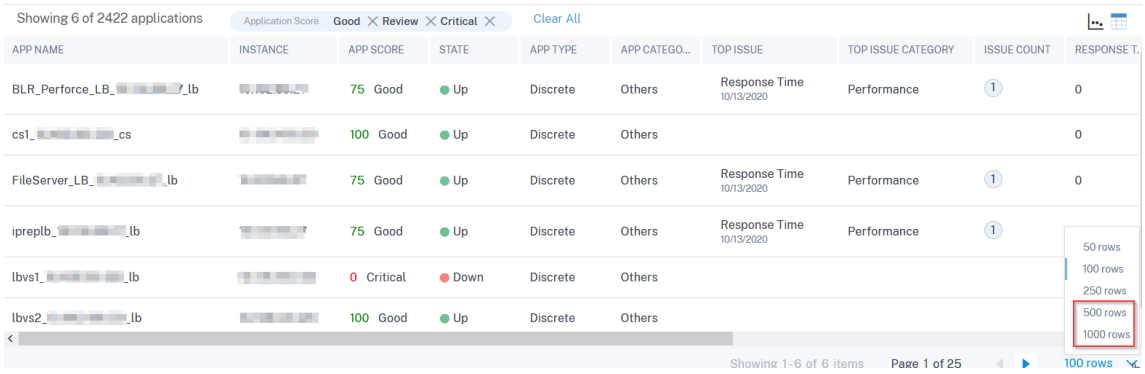
- 検索バーで、仮想サーバの IP アドレスに基づいて結果をフィルタリングできます。



- フィルタから問題の種類（パフォーマンス、インスタンスの健全性、構成、システムリソース）を選択することで、特定の問題の影響を受けるアプリケーションのリストを取得できます。

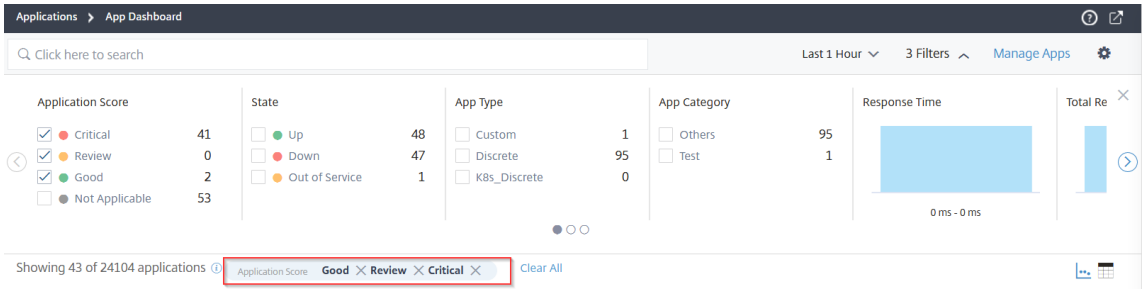


- 表形式ビューでは、500 行および 1000 行オプションを選択して、アプリケーションの最大数を表示できます。



> 注
>
> 500 行または 1000 行のオプションを選択した場合、Citrix ADM はすべてのアプリケーションを表示するのに約 20 秒かかります。
>
> すべてのアプリケーションがロードされたら、グラフビューオプションを選択できます。

- 既定では、[クリティカル]、[レビュー]、および [良好] ステータスのアプリケーションを表示できます。ステータスが「該当なし」のアプリケーションを表示するには、フィルタの下の「適用不可」を選択する必要があります。



- サーバー応答時間の問題では、仮想サーバーを選択した後、異常の詳細を表示できます。

[NSADM-57049]

解決された問題

システム

- [アカウント] > [ユーザー管理] > [グループ] で、外部ユーザーが複数のグループの一部であり、1 つ以上のグループに対してアプリケーションが選択されていない場合、外部ユーザーは仮想サーバーまたは他のエンティティを表示できません。

  [NSHELP-25181]

- アカウント > ユーザー管理 > グループ] で、SDX インスタンスを使用してグループを追加または編集する場合、グループの作成または変更に通常よりも時間がかかります。

  [NSHELP-25081]

ライセンス

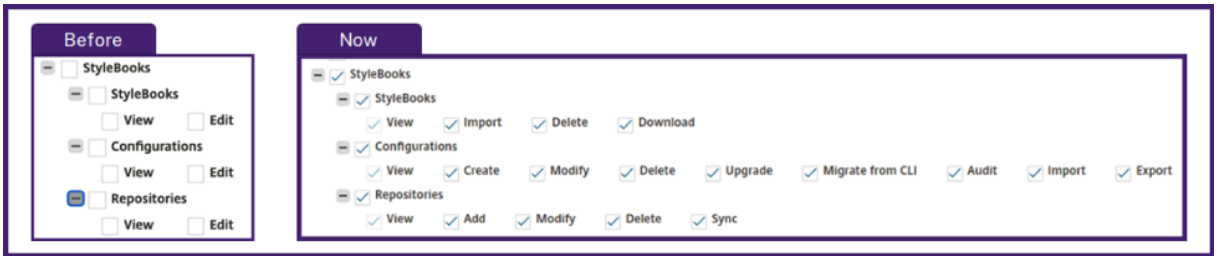
管理対象外のインスタンスにライセンスを割り当てると、ドーナツチャートにライセンス割り当ての割合が正しく表示されません。

[NSADM-60798]

2020 年 10 月 14 日

ユーザーに新しい **StyleBook** 権限を付与する

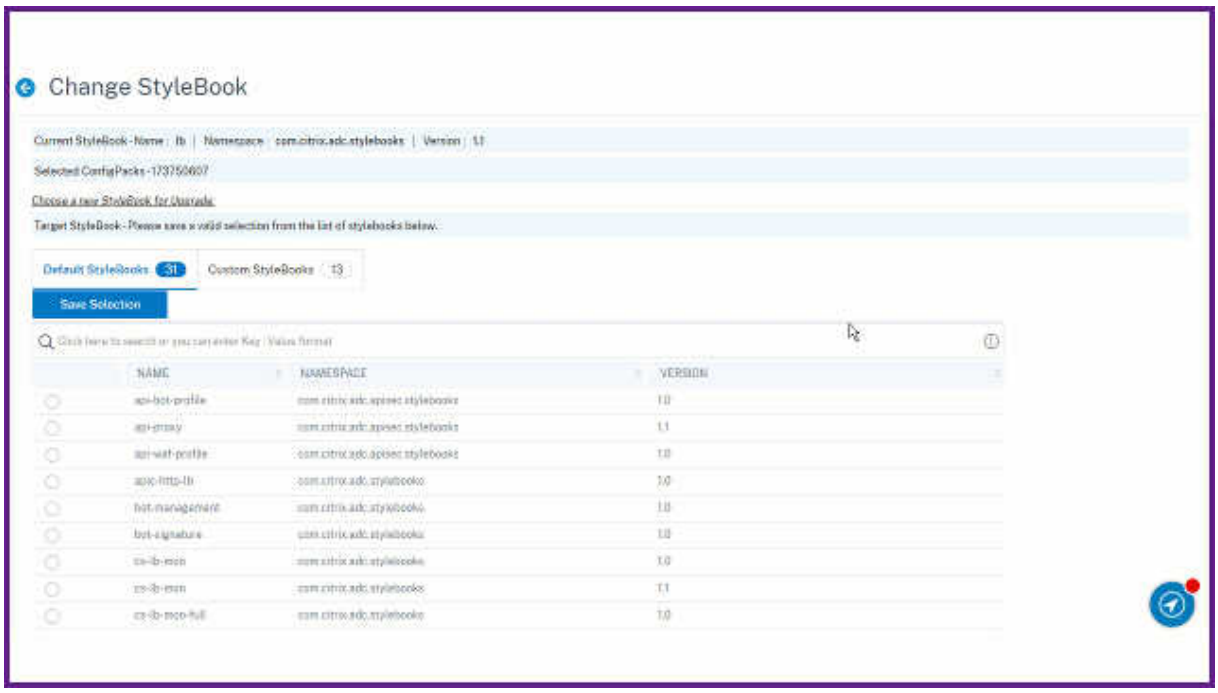
管理者は、アクセスポリシーを作成する際に、インポート、削除、ダウンロードなどの新しい StyleBook 権限をユーザーに付与できるようになりました。これを行うには、[アカウント] > [ユーザー管理] > [アクセスポリシー] に移動し、[追加] をクリックします。以前は、表示および編集権限のみを選択できました。詳しくは、「ユーザーに StyleBook パーミッションを付与する」を参照してください。



[NSADM-57672]

設定パックを編集して **StyleBook** を変更する

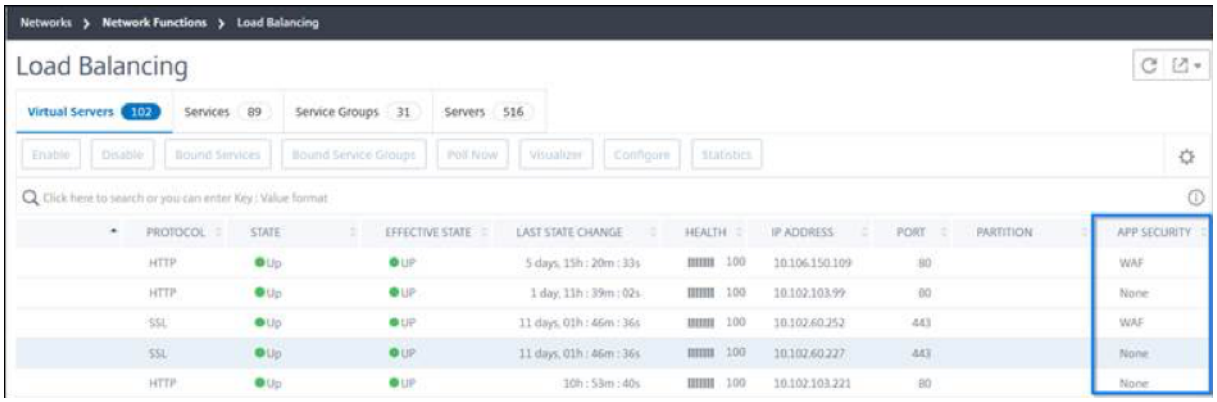
これで、設定パックを編集して StyleBook を変更できます。以前は、[ConfigPack を移行] オプションを使用してこれを行うことができました。詳しくは、「設定パックの StyleBook を変更する」を参照してください。



[NSADM-58245]

ネットワーク機能**:[**アプリセキュリティ**]** 列の追加

[ネットワーク**] > [**ネットワーク機能**] > [**負荷分散とコンテンツスイッチング] で、[アプリのセキュリティ x] 列を表示できるようになりました。



管理者は、仮想サーバーが次のものを使用してバインドされているかどうかを分析できます。

- **WAF** — 仮想サーバはアプリケーションファイアウォールポリシーで設定され、WAF セキュリティ違反を表示します。
- ボット — 仮想サーバーはボットポリシーで設定され、ボットのセキュリティ違反が表示されます。
- ボット、**WAF** — 仮想サーバーはアプリファイアウォールとボットポリシーの両方で構成され、WAF と Bot の両方のセキュリティ違反を表示します。

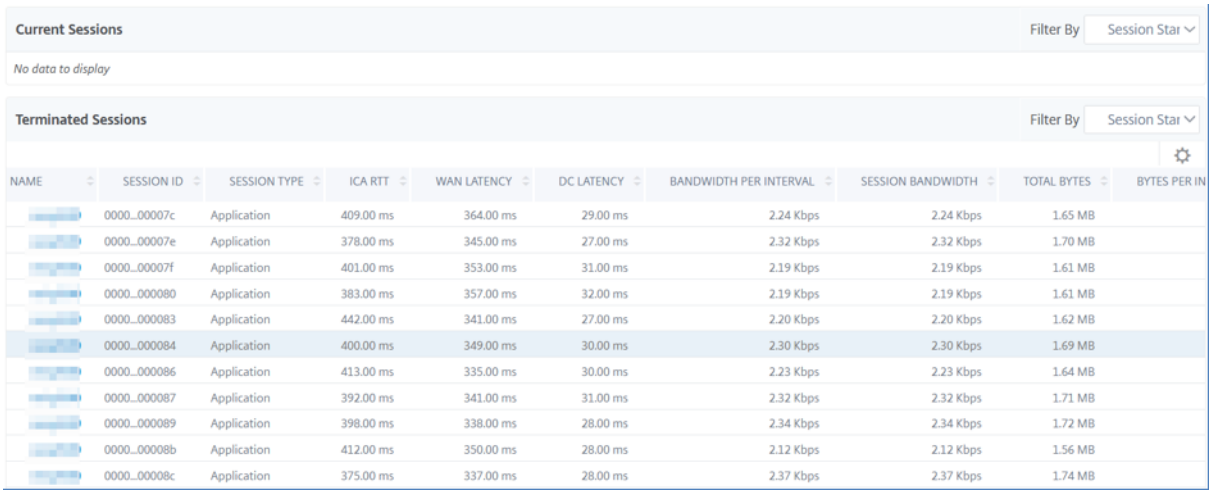
- なし — 仮想サーバーは、アプリファイアウォールまたはボットポリシーを使用して構成されていません。

詳しくは、「アプリケーションのセキュリティ違反の詳細を表示する」を参照してください。

[NSADM-54300]

HDX Insight: アクティブなセッションと終了したセッションをすべて表示する機能強化

[Analytics] > [HDX Insight] > [Users] で、アクティブおよび終了したセッションのすべてのユーザーの統合ビューを視覚化できるようになりました。



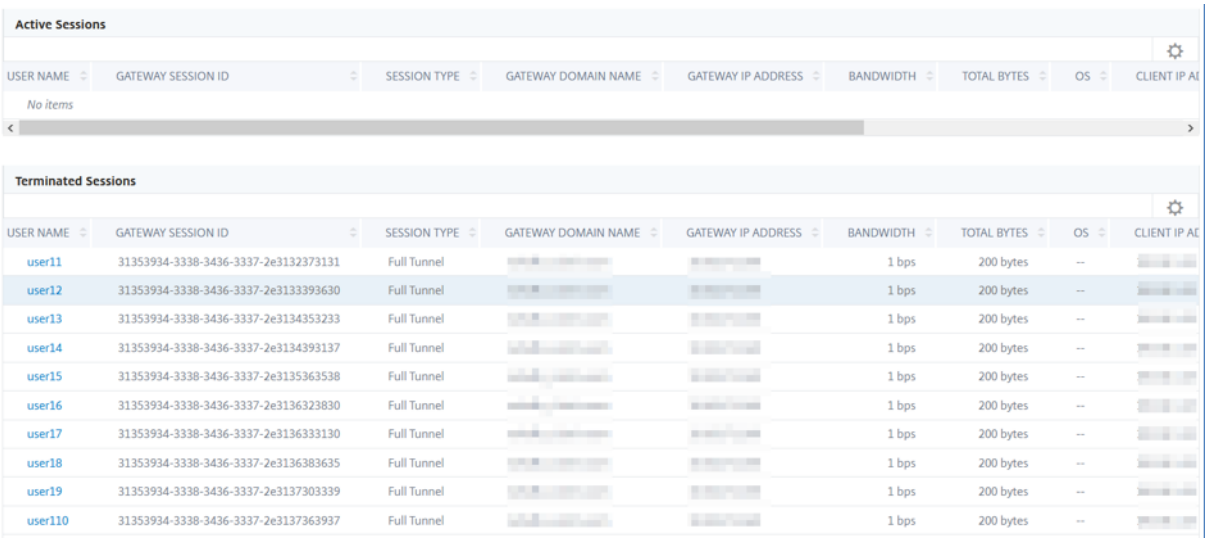
管理者として、この改善により、次のことが可能になります。

- 単一ペインビジュアライゼーションですべてのユーザーの詳細を表示する
- 各ユーザーを選択し、アクティブなセッションと終了したセッションの表示に関する複雑さを排除

[NSADM-57685]

Gateway Insight: アクティブなセッションと終了したセッションをすべて表示する機能強化

[アナリティクス] **> [Gateway Insight] > [**ユーザー**] > [**ゲートウェイユーザー] で、アクティブおよび終了したセッションのすべてのユーザーの統合ビューを視覚化できるようになりました。



管理者として、この改善により、次のことが可能になります。

- 単一ペインビジュアライゼーションですべてのユーザーの詳細を表示する
- 各ユーザーを選択し、アクティブなセッションと終了したセッションの表示に関する複雑さを排除

[NSADM-60800]

Security Insight — SQL インジェクション文法違反の表示

Security Insight で、新しい違反の種類である SQL インジェクション文法を表示できるようになりました。Security Insight で SQL インジェクション文法違反を生成するには、Citrix ADC インスタンスで次のコマンドを構成する必要があります。

1. `add ns ip <IP> <subnet mask> -type SNIP`
2. `add lb vs http_vs http <VS_IP> 80`
3. `add service http_svc <SVC_IP> http 80`
4. `bind lb vs http_vs http_svc`
5. `add appfw profile abc -startURLAction none -SQLInjectionGrammar ON -SQLInjectionType None`
6. `set appfw settings -defaultProfile abc`

詳しくは、「Security Insight」を参照してください。

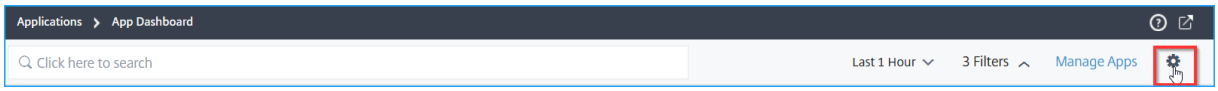
アプリダッシュボード**:App Score** コンポーネントを選択し、しきい値を設定

App Dashboard で、管理者として、コンポーネントを選択し、アプリスコア計算のしきい値を構成できるようになりました。アプリスコアは、次の定義を定義するスコアリングシステムです。

- アプリケーションがどれくらいうまく実行されているか

- アプリケーションが応答性の点でうまく動作しているかどうか

[アプリケーション] **>** [ダッシュボード] に移動し、設定アイコンを選択してアプリのスコアコンポーネントを表示します。



詳しくは、「アプリスコアコンポーネントを選択し、しきい値を設定します」を参照してください。

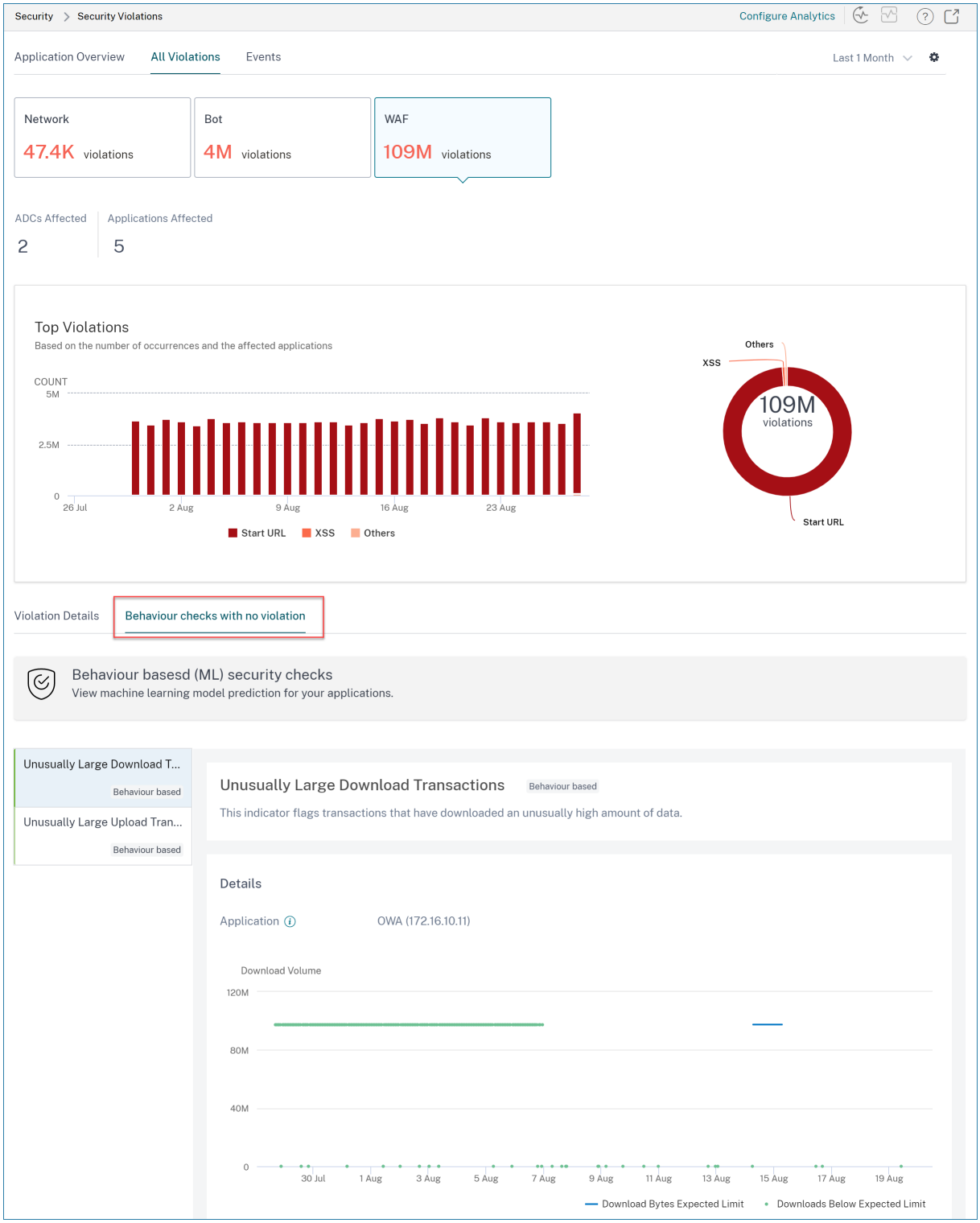
[NSADM-52870]

アプリのセキュリティ違反**:** トラフィックパターンに基づいて予測を視覚化

[分析] **>** [セキュリティ] **>** [セキュリティ違反] で、すべてのセキュリティ違反 (WAF および Bot) について、違反の詳細とは別に、機械学習アルゴリズムに基づいて 3 週間のトラフィック予測を視覚化できるようになりました。管理者として、この 3 週間の予測により、次のことが可能になります。

- 違反が観察されない場合でもトラフィックパターンを分析する
- 予測から観察された異常なトラフィックパターンに対するトラブルシューティングアクションの実行
- Citrix ADM が異常以外のデータを処理していることに注意する

[セキュリティ違反] ページで、[違反のない動作チェック] タブをクリックして、3 週間のトラフィック予測を表示します。



詳しくは、「アプリのセキュリティ違反」を参照してください。

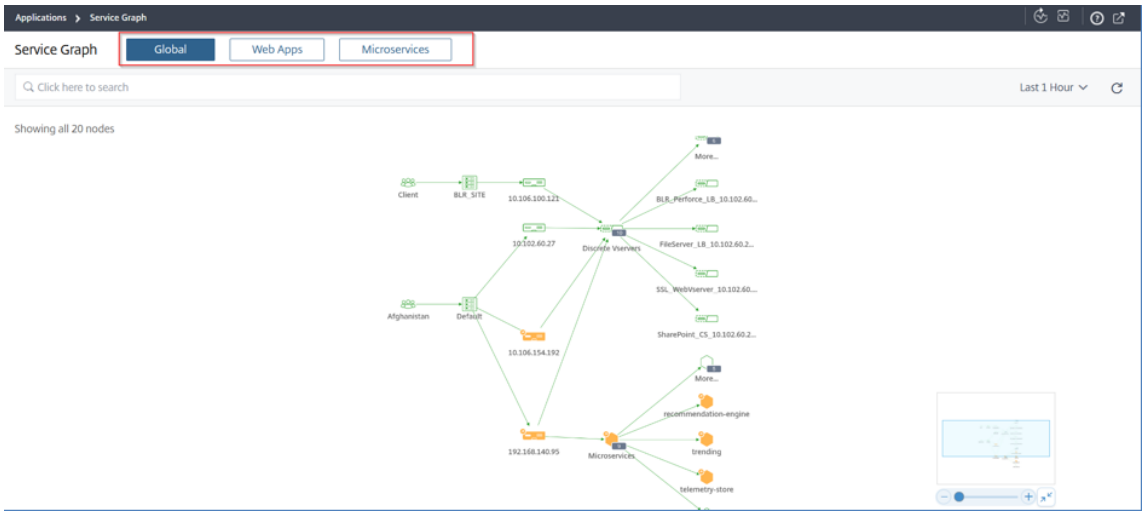
[NSADM-58721]

サービスグラフの改善

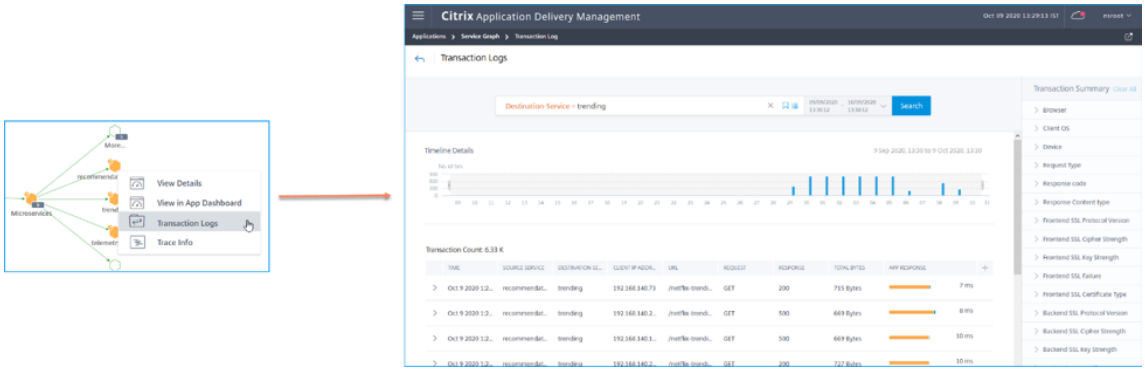
[アプリケーション] **>** [サービスグラフ] で、次の機能強化を表示できるようになりました。

- サービスグラフページには、次の 3 つのタブがあります。
  - グローバル — すべての Citrix ADC インスタンスにおけるアプリケーションのサービスグラフを表示します。
  - **Web Apps** — 3 層 Web アプリケーション (負荷分散、コンテンツスイッチング、および GSLB) のサービスグラフを表示します。
  - マイクロサービス — Kubernetes マイクロサービスのサービスグラフを表示します。

  各タブをクリックして、それぞれのサービスグラフを表示します。



- グローバルサービスグラフから、マイクロサービスの詳細にアクセスできます。サービスをクリックしてオプションを選択すると、それぞれの GUI にリダイレクトされます。



- マイクロサービスサービスグラフには検索バーがあり、マウスポインタを使用して次のカテゴリを選択してフィルタを作成できます。

- [**Client Geo Location**] — クライアントがアクセスしている入力とそのサービスを表示します。
- **ingress-IP**： 入力に関連付けられたすべてのサービスを表示します。

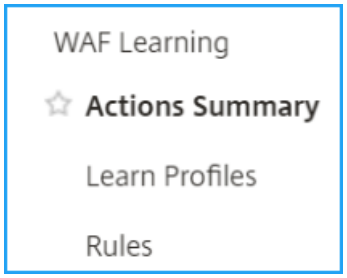
[NSADM-57696]

2020 年 **9** 月 **29** 日

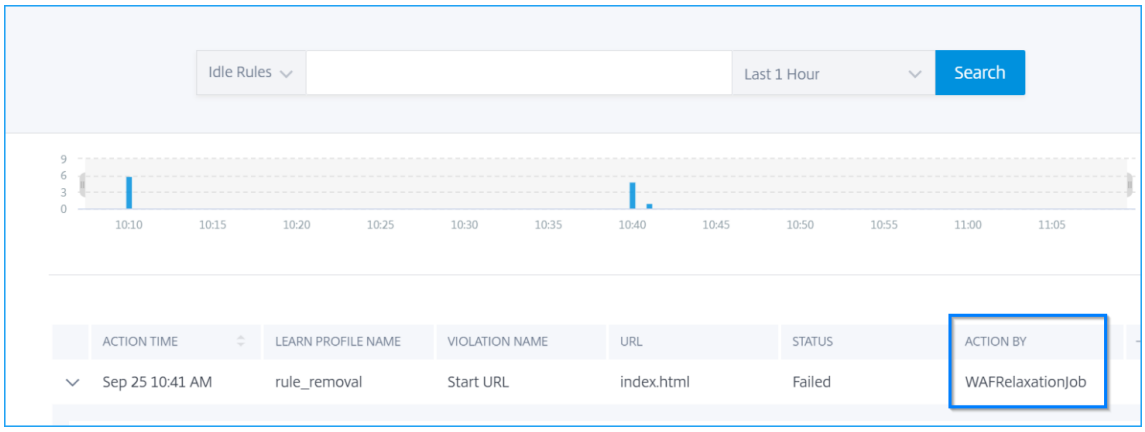
WAF 学習エンジンの改良

WAF ラーニングエンジンで、次の機能強化を表示できるようになりました。

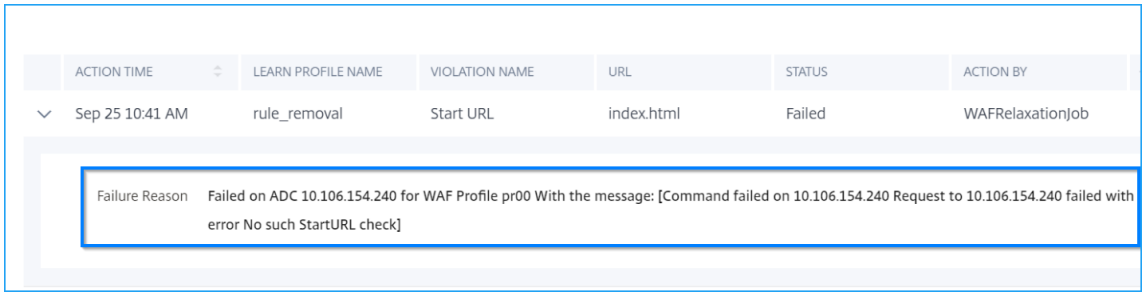
- **WAF** ラーニング **>** ダッシュボードが **WAF** ラーニング **>** アクションの概要に置き換えられました



- ［アクション別］オプションを使用すると、学習したルールが Citrix ADM によって自動展開されているのか、管理者が［展開］または［スキップ］オプションを手動で選択したかを理解できます。



- 展開された学習ルールが失敗した場合は、[アクションの概要] ページで失敗理由を表示できます。

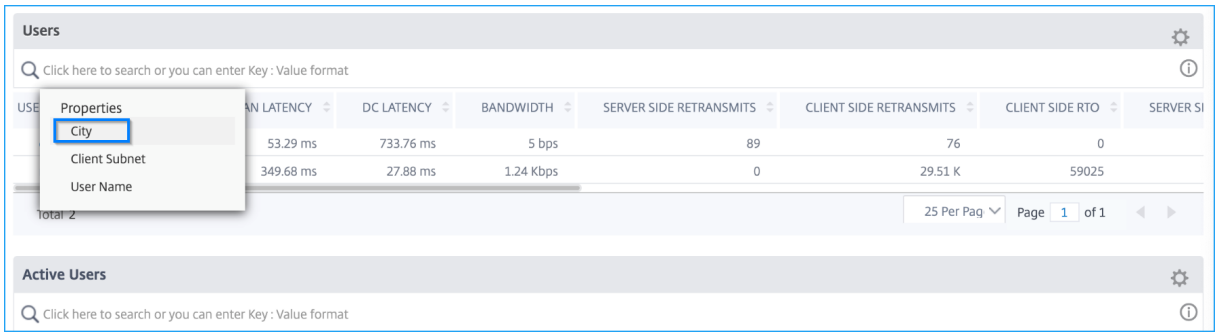


- 設定された学習済みプロファイルごとに、最大 100 万の学習済みルールを表示できます。

  [NSADM-57220]

HDX インサイト — 都市名を使用して検索

HDX Insight で、都市名に基づいて結果をフィルタリングできるようになりました。

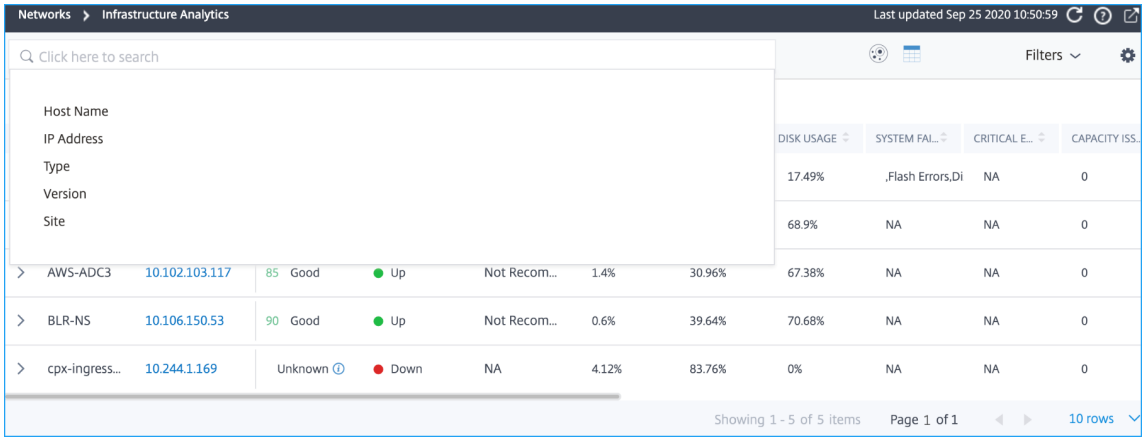


[NSADM-57366]

インフラストラクチャ分析 — 検索属性

Infrastructure Analytics では、検索バーにマウスカーソルを置き、次の検索属性を選択して結果を絞り込むことができます。

- ホスト名
- IP アドレス
- 種類
- バージョン
- サイト

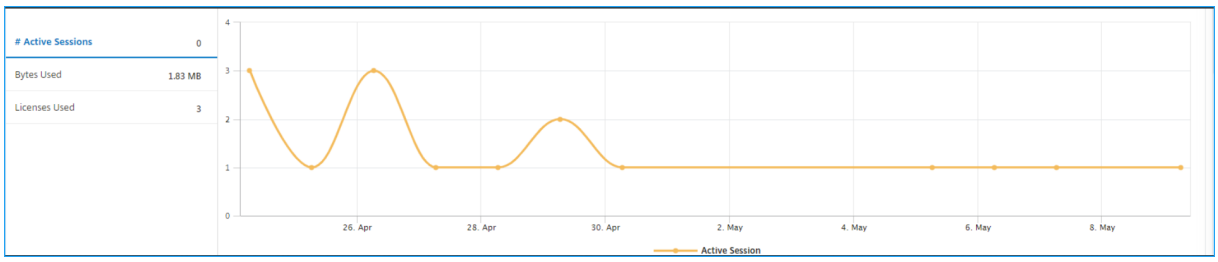


[NSADM-59453]

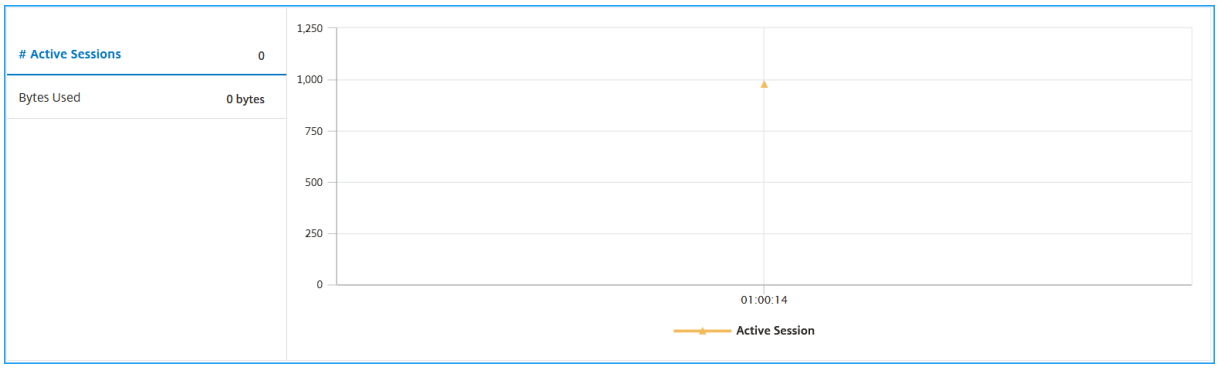
Gateway Insight 改善

[**Gateway Insight] > [**ユーザー**]** で、ライセンス情報が削除されます。

以前:



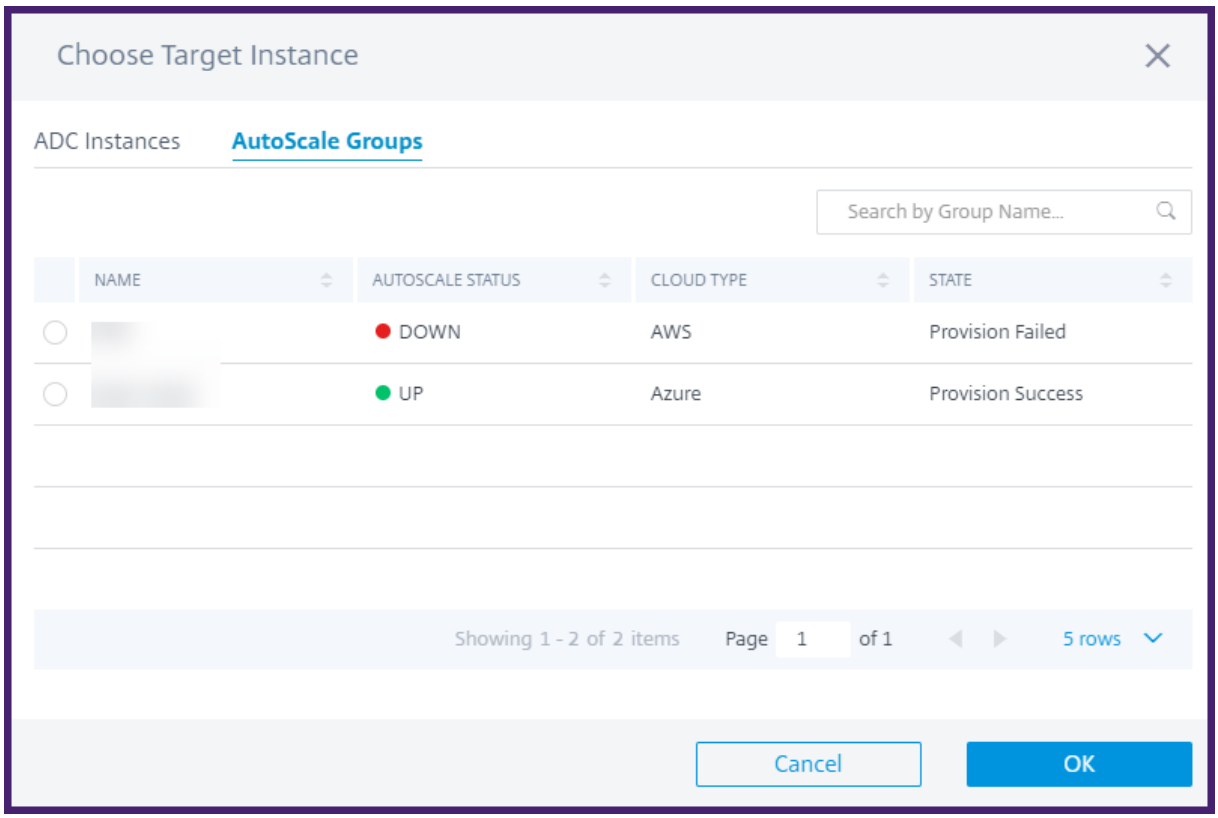
今:



[NSADM-53494]

StyleBook 構成ビルダーを使用して **ADC** 設定を **AutoScale** グループに移行する

StyleBooks 構成ビルダーで、ADC 設定を AutoScale グループに移行できるようになりました。これを行うには、ターゲットインスタンスとして必要な Autosale グループを選択します。



[NSADM-51470]

解決された問題

展開

ADM エージェントイメージは AWS M5 インスタンスタイプでは機能しません。この修正により、ADM エージェントイメージが M5 インスタンスタイプで動作するように、サポートされるドライバーが追加されました。

[NSHELP-24250]

ネットワーク

「<」文字で構成ジョブを実行すると、ジョブは失敗します。

[NSADM-53465]

2020 年 **9** 月 **16** 日

ADM サービス接続を使用した **ADC** インスタンスのロータッチオンボーディング

これで、新しい Citrix ADM サービスのオンボーディングワークフローを使用できます。これにより、ADC インスタンスを ADM サービスにオンボーディングし、ハイブリッドマルチクラウド展開を可視化できます。このワークフロ

ーの自動オンボーディング機能は、ADC インスタンスの新しい ADM サービス接続機能を活用します。これにより、ADC インスタンスを ADM サービスに接続できます。詳しくは、「Citrix ADM サービス接続を使用した Citrix ADC インスタンスのロータッチオンボーディング」を参照してください。

> 注:
>
> このワークフローは、カナリアリリースによって段階的に展開されます (GA)。ADM サービス環境でこの機能が利用可能になると、電子メールが送信されます。

[NSADM-51952]

Kubernetes サービスグラフ**-**クライアントトランザクションの概要

Kubernetes サービスグラフで、特定の場所のすべてのクライアントの詳細なトランザクションログを表示できるようになりました。この機能を使用すると、次の項目を表示できます。

- 応答時間 > 500 ミリ秒
- 5xx エラー

> 注:
>
> 選択したクライアントの 2xx および 4xx トランザクションのサンプルのみを表示できます。

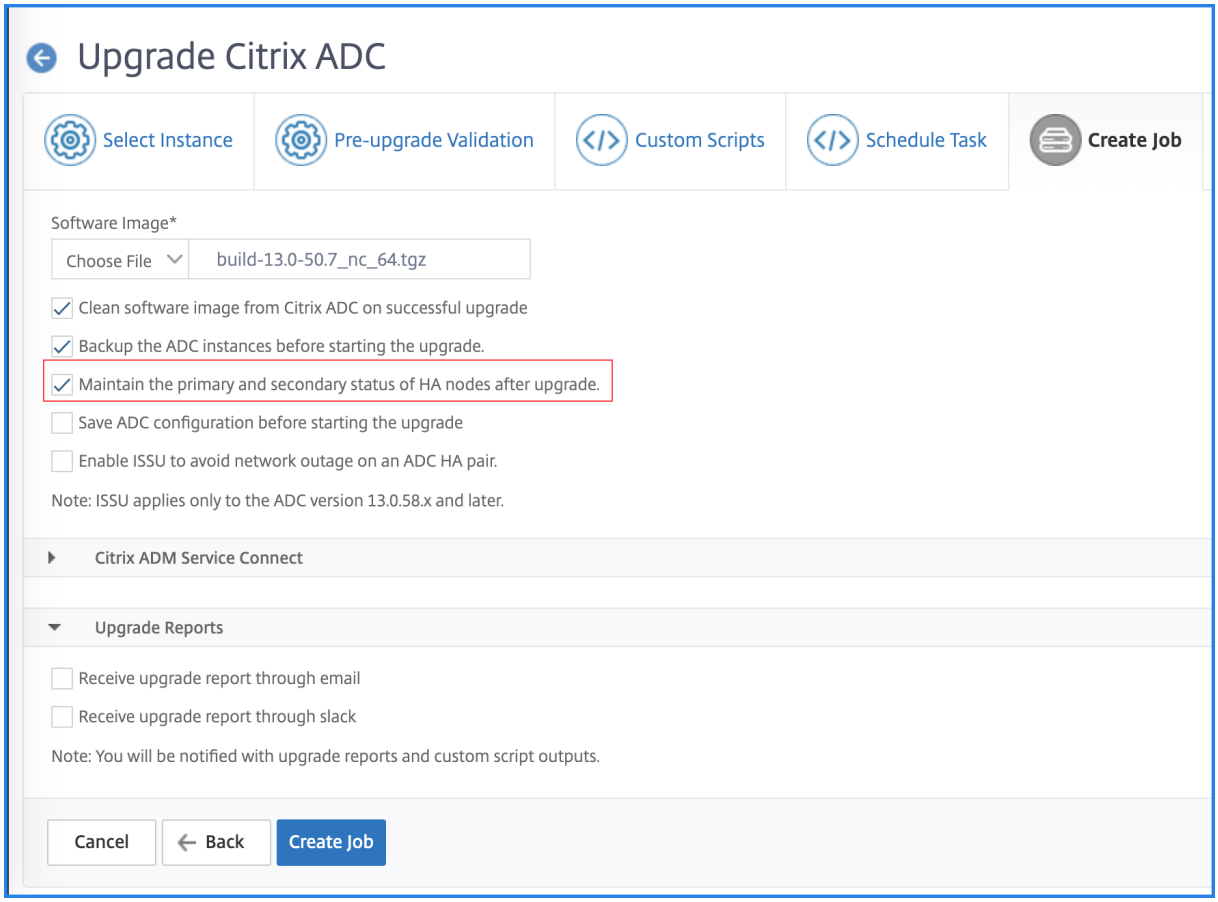
この機能を使用すると、トランザクションの詳細を調べるだけでなく、クライアント、ADC、サーバー間で分割されたメトリック (クライアント RTT、SSL メトリック、サーバーの応答時間など) を視覚的に理解できます。

詳しくは、「クライアントメトリックの表示」を参照してください。

[NSADM-58342]

アップグレード後に **ADC** 高可用性ノードのステータスを維持する

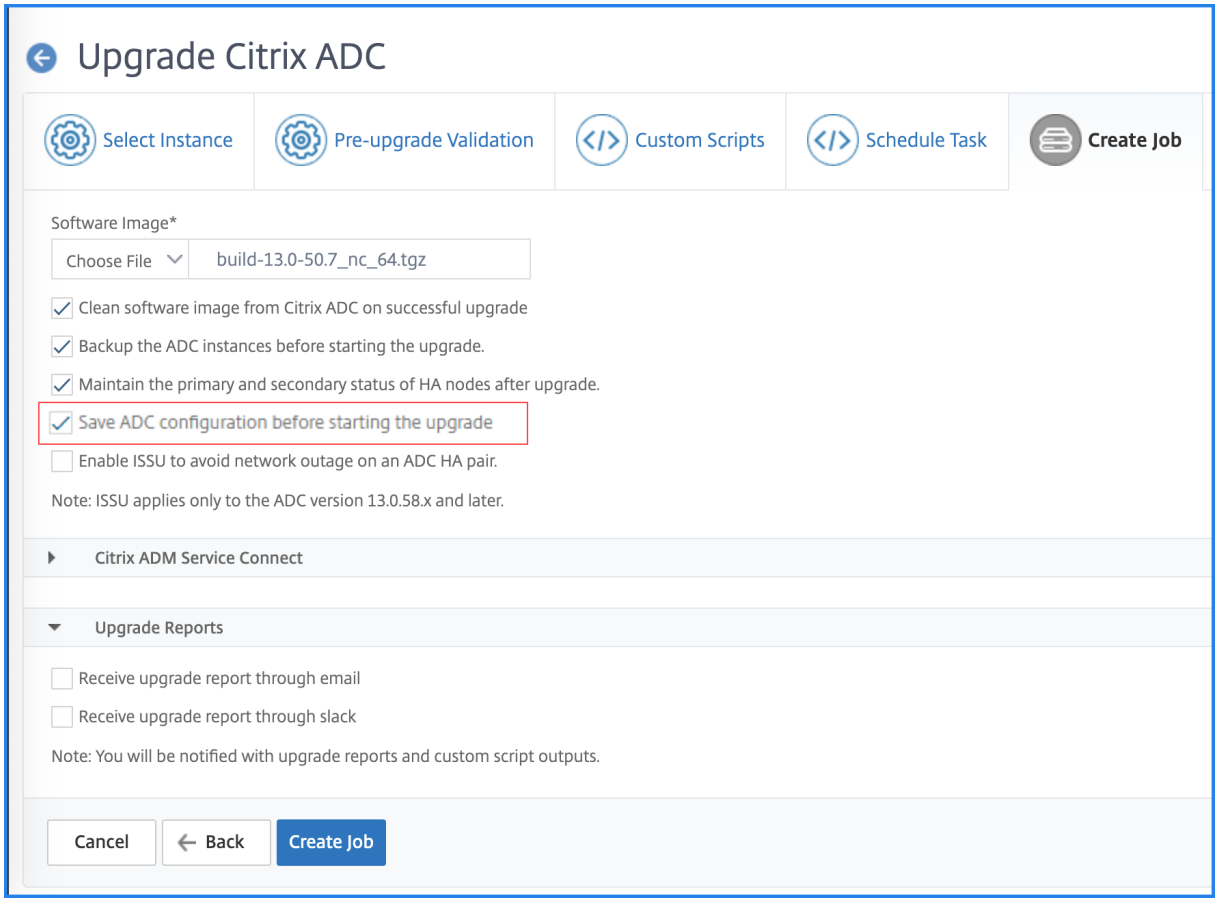
ADC 高可用性ペアのアップグレードジョブを作成すると、新しい [アップグレード後に **HA** ノードのプライマリおよびセカンダリステータスを保持] オプションが表示されます。このオプションは、[ジョブの作成] タブの下に表示されます。各ノードのアップグレード後にアップグレードジョブでフェイルオーバーを開始する場合は、このオプションを選択します。以前は、GUI オプションはなく、各ノードのアップグレード後に、アップグレードジョブがデフォルトでフェイルオーバーを開始していました。



[NSADM-47736]

アップグレードの前に **ADC** 設定を保存する

ADC インスタンスのアップグレードジョブを作成するとき、インスタンスをアップグレードする前に、実行中の ADC 設定を保存できるようになりました。[**Create Job**] タブで 、**[**アップグレードを開始する前に **ADC** 設定を保存] オプションを選択します。



[NSADM-52470]

修正された問題

Analytics

[アナリティクス**] > [HDX Insight] > [**ユーザー**]** ページで列のサイズを変更できません。

[NSHELP-24288]

2020 年 9 月 02 日

AutoScale アプリケーションのアクセスタイプの変更

これで、AutoScale アプリケーションのアクセスタイプを変更できます。アクセスタイプを変更する場合は、次の項目も変更できます。

- FQDN タイプ
- ドメイン名
- ドメインのゾーン。

[NSADM-52810]

API ゲートウェイの改善

API ゲートウェイ機能は、次の機能で改善されました。

- API Analytics: [詳細表示] をクリックしてタイルを展開すると、API インスタンスとエンドポイントを名前の一部で検索できます。API アナリティクスの表示を参照してください。
- デプロイ:API デプロイの分析を有効にします。API アナリティクスを有効にするを参照してください。
- ポリシー:API デプロイの WAF ポリシーと BOT ポリシーを設定します。API 定義へのポリシーの追加を参照してください。

  > 注
  >
  > WAF ポリシーと BOT ポリシーを設定する前に、StyleBooks を使用して ADM でプロファイルを作成してください。次のデフォルトの StyleBooks が新しく追加され、プロファイルが作成されます。
  >
  > `api-waf-profile`
  >
  > `api-bot-profile`

  詳しくは、「StyleBook を使用して WAF と BOT プロファイルを作成する」を参照してください。

[NSADM-52804]

StyleBooks バンドルにアイコンを含める

バンドルから複数の StyleBook をインポートする場合、各 StyleBook にアイコンを追加できるようになりました。アイコンと`icon_mapping.json`ファイルを`resources`フォルダにアップロードします。アイコンファイル名と StyleBook 名が一致する場合、アイコンは自動的に StyleBook にマッピングされます。それ以外の場合は、StyleBooks とアイコンを`icon_mapping.json`ファイルに次のようにマップします。

```
<StyleBook file name> : <icon file name>
```

`defaulticon` エントリのみを指定した場合、バンドル内のすべての StyleBook は指定されたアイコンにマップされます。

```
defaulticon: <icon file name>
```

アプリケーション／ **StyleBooks** では、インポートされた StyleBook がマップされたアイコンとともに表示されます。

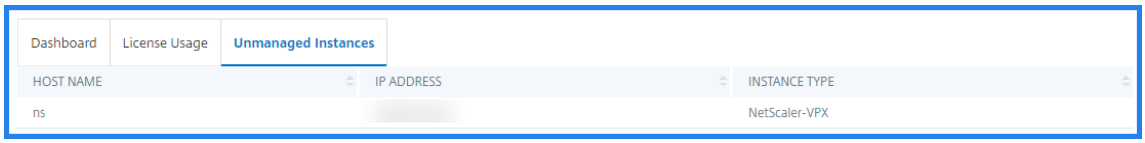
詳しくは、「カスタム StyleBook をインポートする」を参照してください。

[NSADM-52330]

［プールされた容量］ページの改善

次の GUI の変更により、［プールされた容量］ページが改善されました。

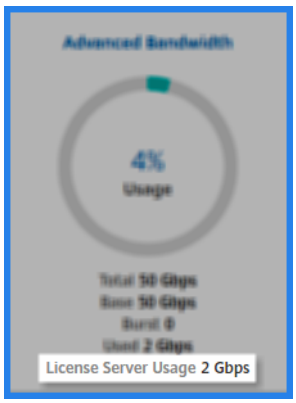
- 管理対象外のインスタンス — これは新しいタブです。Citrix ADM で検出されたが管理されていないインスタンスが表示されます。以前は、これらのインスタンスは [ダッシュボード] タブに [管理対象外] ライセンスステータスで表示されていました。



- ライセンスステータス-この列では、次のステータスが削除されます。
  - 管理されていない
  - 同期中

  これで、[割り当ての詳細] 列がインスタンスリストから削除されます。

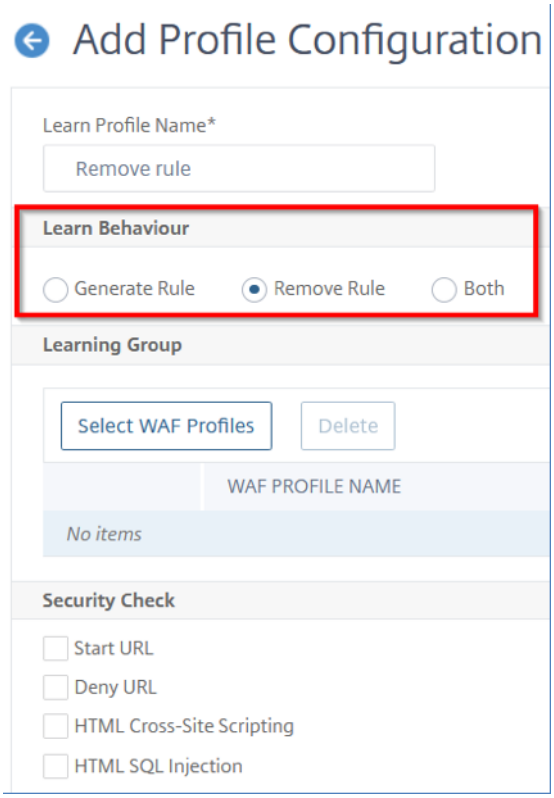
- ライセンスサーバの使用状況-使用状況チャートに追加された新しいインジケーター。ライセンスサーバーのプールされた容量消費量が表示されます。



[NSADM-52770]

WAF 学習エンジン**-**ルールの削除のサポート

セキュリティチェック付きの着信トラフィックが Citrix ADC インスタンスで受信されない場合、学習動作を変更して緩和ルールを削除できるようになりました。**[** 分析**] > [**セキュリティ**] > [WAF** ラーニング**] > [**プロファイルのラーニング**]** に移動し、[追加] をクリックして [学習動作] オプションを表示します。



- 「ルールを生成」— 例外ルールを生成し、管理者がルールを展開またはスキップできるようにします。
- 「ルールの削除」— 設定されたアイドル時間がしきい値を超えたときに、例外ルールを削除します。
- [両方]: 受信トラフィックがない場合に例外ルールを生成し、ルールを削除します。

ルールの削除オプションは、次のセキュリティチェックにのみ適用できます。

- 開始 URL
- URL を拒否する
- HTML クロスサイトスクリプティング
- HTML SQL インジェクション

ルールを削除すると、通知は Slack、SMS、メール、ServiceNow で生成されます。**WAF** ラーニングダッシュボードで詳細を表示することもできます。

詳しくは、「ラーニングプロファイルの設定」を参照してください。

[NSADM-52871]

アプリのセキュリティ違反-ボット

アプリのセキュリティ違反で、BOT 違反カテゴリで **Web** サイトスキャナーを表示できるようになりました。詳しくは、「アプリのセキュリティ違反」を参照してください。

[NSADM-53289]

アプリのセキュリティ違反-ネットワーク

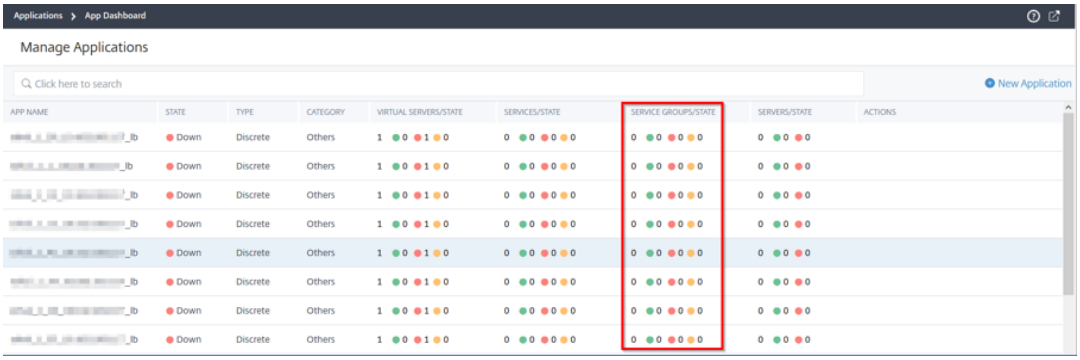
アプリのセキュリティ違反で、ネットワーク違反カテゴリでスモールウィンドウ攻撃を表示できるようになりました。詳しくは、「アプリのセキュリティ違反」を参照してください。

[NSADM-46023]

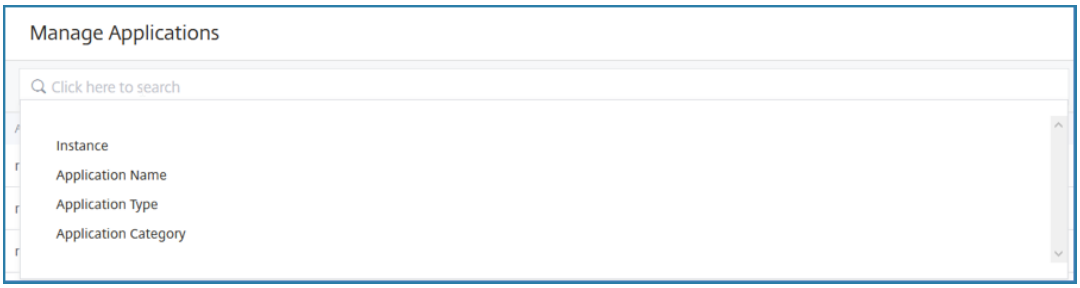
アプリダッシュボードの改善

アプリダッシュボードで、次の機能強化を表示できるようになりました。

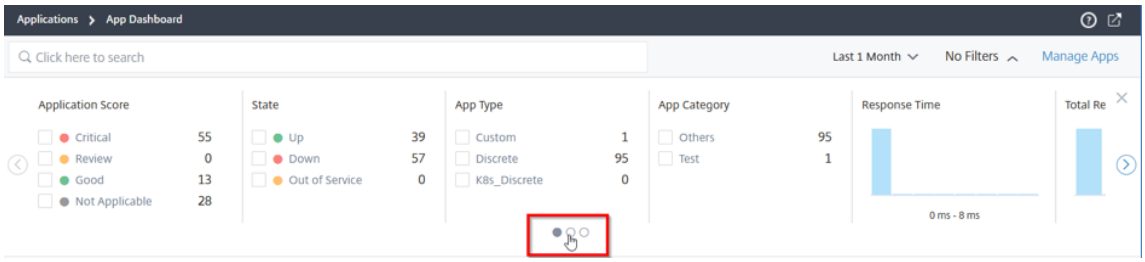
- [アプリケーションの管理] ページで、次の操作を行います。
  - サービスグループの合計と、[Up]、[Down]、または [Out of Status] であるサービスグループのステータスを表示できます。



  - 検索バーにマウスポインタを置き、カテゴリを選択して検索を絞り込むことができます。



- [アプリケーションダッシュボード] ページでは、スクロールバーがカルーセルスライダーに置き換えられ、すべてのオプションに簡単にアクセスできます。



[NSADM-52759]

Web Insight ダッシュボード

ウェブアプリケーション、クライアント、および Citrix ADC インスタンスの詳細なメトリックスを可視化する改善された Web インサイト機能を表示できるようになりました。この改善された Web Insight により、パフォーマンスと使用状況の観点から、完全なアプリ情報を同時に評価および視覚化することができます。管理者は、次の対象 Web Insight を表示できます。

- アプリケーション。[アプリケーション**] > [**ダッシュボード] に移動し、アプリケーションをクリックし、[**Web Insight**] タブを選択して詳細なメトリックスを表示します。詳しくは、「アプリケーション使用状況の分析」を参照してください。
- すべてのアプリケーション。[アプリケーション**] > [Web Insight**] に移動し、各タブ ([アプリケーション]、[クライアント]、[インスタンス]) をクリックして、次のメトリックを表示します。

アプリケーション	クライアント	インスタンス
アプリケーション	クライアント	インスタンス・メトリック
サーバー	ジオ・ラオケーションズ	アプリケーション
ドメイン	HTTP 要求メソッド	ドメイン
地理的場所	HTTP 応答の状態	URL
URL	URL	HHTP リクエストメソッド
HTTP 要求メソッド	オペレーティングシステム	HTTP 応答の状態
HTTP 応答の状態	Web ブラウザー	クライアント
SSL エラー	SSL エラー	サーバー
SSL 使用法	SSL 使用法	オペレーティングシステム
-	-	Web ブラウザー

詳しくは、「Web Insight ダッシュボード」を参照してください。

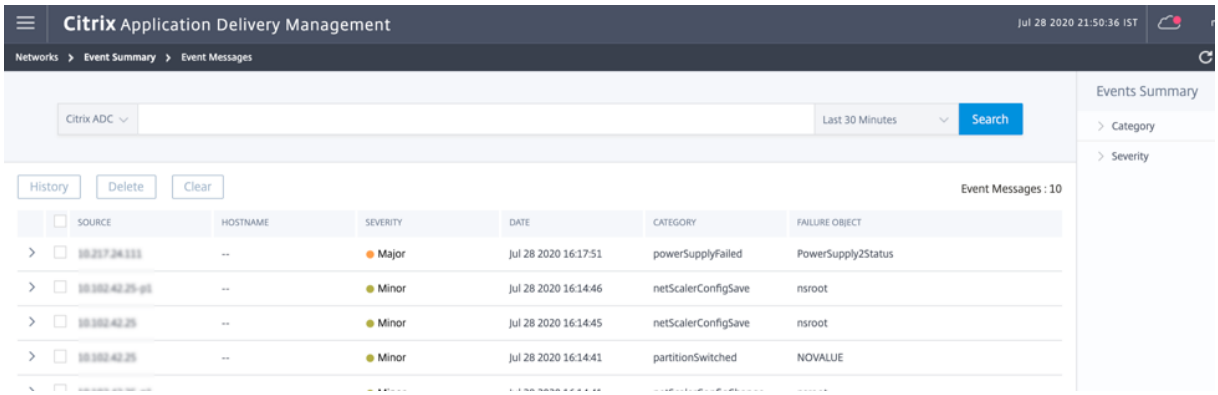
GCP での **ADM** エージェントのサポート

Google Cloud Platform（GCP）では、Citrix ADM エージェントがサポートされるようになりました。詳しくは、「GCP に Citrix ADM エージェントをインストールする」を参照してください。

[NSADM-31980]

イベントメッセージの新しい検索機能

[ネットワーク] > [イベント] > [イベントメッセージ] で、AND/OR などの論理演算子を使用して検索できるようになりました。また、カスタム期間を使用してデータをフィルタすることもできます。また、[Events Summary] パネルには、各イベントカテゴリと重大度が表示されます。



解決された問題

Analytics

Citrix ADM 分析レポートには、期間が 1 か月として選択されても、14～28 日のデータしか表示されません

[NSHELP-23836]

システム

ファイルサイズが大きい場合、ADM はエージェントテクニカルサポートバンドルを生成しません。
[NSHELP-24620]

ライセンス

ライセンスアクセスコード ([ネットワーク] > [ライセンス] > [ライセンスファイルの追加]) を使用して **ADM GUI** にライセンスファイルをインストールすると、「ライセンス情報の解析に失敗しました」というメッセージが表示されます。この問題は、ライセンスファイルがサポートされていない Jazz サーバーに格納されている場合に発生します。この修正により、Jazz サーバーが ADM にライセンスファイルを追加できるようになります。

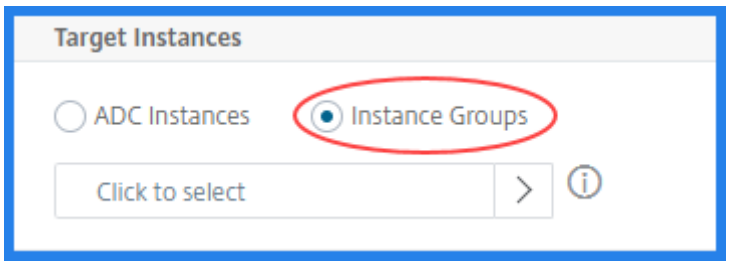
[NSADM-59338]

2020 年 8 月 17 日

構成パックをデプロイするターゲットインスタンスグループの選択

StyleBooks > Configurations ページで新しい設定を追加するときに、ADC インスタンスグループを選択して構成パックをデプロイできるようになりました。また、この設定はグループ内のすべてのインスタンスに適用されます。

これを行うには、[****** ターゲットインスタンス**]** セクションで **[**インスタンスグループ ******] を選択します。



[NSADM-56605]

IPAM ネットワークから **IP** アドレスを指定する

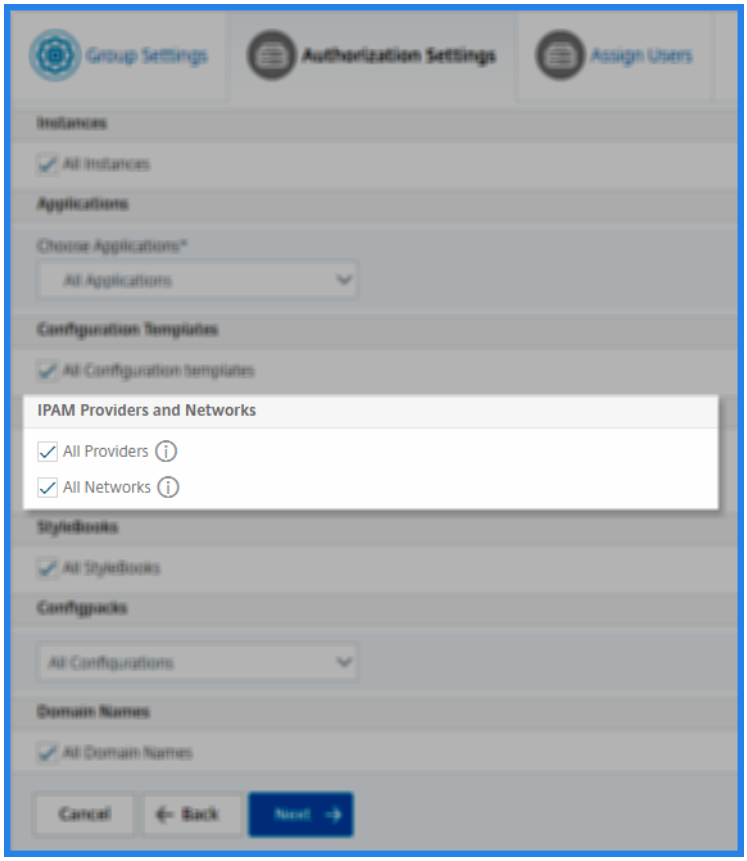
StyleBook 定義で`dynamic-allocation`属性値を true に設定すると、ユーザーは選択した IP アドレスネットワークから IP アドレスを指定できます。ADM は、指定された IP アドレスを仮想サーバに割り当てます。

[NSADM-56068]

IPAM へのユーザー認証の管理

管理者は、**IPAM** プロバイダーとネットワークを選択し、ユーザーまたはグループにアクセス権を付与できます。

1. [システム**] > [**ユーザー管理] ページに移動します。
2. [承認設定] タブで、IPAM プロバイダーとネットワークを追加します。



[NSADM-54377]

StyleBook 組み込み関数の改良

StyleBook 定義を作成するときは、次の組み込み関数を使用して機能を向上させます。

- `replace()` — リストで指定された文字または文字列を置き換えるようになりました。以前は、この関数にリスト入力を提供できませんでした。
- `ip()` — 整数値を受け入れ、それを同等の IP アドレスに変換します。また、IP アドレスの加算と減算もサポートしています。
- **`int`**`()` — IPv4 アドレスを受け入れ、同等の整数値を返すようになりました。

[NSADM-56310], [NSADM-55209]

新しい **StyleBook** 組み込み関数を使用する

StyleBook 定義の作成時に、ADM StyleBooks では次の組み込み関数がサポートされるようになりました。

- `distinct()` -入力リストから一意の項目を抽出します。
- `split()` -入力文字列をリストに分割します。

[NSADM-56103], [NSADM-55958]

StyleBooks を使用しない **AutoScale** グループアプリケーションの設定

StyleBooks を選択せずに、ADC AutoScale グループでアプリケーションを構成できるようになりました。ただし、今後 StyleBooks を使用する場合は、このアプリケーションを編集して再送信し、確認ウィンドウで [はい] を選択します。

以前は、StyleBook の選択は、AutoScale グループアプリケーションを構成するために必須でした。

[NSADM-52814]

Gateway Insight 改善

Gateway Insight で、次の項目を表示できるようになりました。

- ユーザー名に基づいて結果をフィルタリングできる検索バー。[分析] **> [Gateway Insight] > [**ユーザー**]** に移動して、**[**ユーザー**]** と [アクティブユーザー] の検索バーを表示します。検索バーにマウスポインタを置き、[ユーザー名] を選択し、ユーザー名を入力して結果をフィルタリングします。

- ユーザーの地理的位置に基づいてユーザー情報を表示する地理マップ。管理者として、この地理マップを使用すると、特定の場所のユーザー合計、アプリ合計、セッション総数のサマリー、合計セッションを表示できます。

  1. [アナリティクス] **> [Gateway Insight**] に移動して、地域マップを表示します。
  2. 国をクリックします。たとえば、
     米国地理マップには、選択した国のユーザーリスト、アクティブなセッション、終了したセッション、アプリケーションなどの詳細が表示されます。

- 特定の場所に基づいてユーザーをフィルタリングできるゲートウェイの地情報マップ。

  1. [分析] **> [Gateway Insight] > [**ゲートウェイ**]** に移動します。
  2. ゲートウェイドメイン名を選択して geo マップを表示します

3. 国をクリックします。たとえば、米国

   地域マップには、選択した国のユーザーリスト、アクティブなセッション、終了したセッション、アプリケーションなどの詳細が表示されます。

[NSADM-55504], [NSADM-55506]

アプリのセキュリティ違反 ー ネットワーク

[アプリのセキュリティ違反] で、[ネットワーク違反] カテゴリで **SYN** フラッド攻撃を表示できるようになりました。詳しくは、「アプリのセキュリティ違反」を参照してください。

[NSADM-46021]

グローバルサービスグラフの改良

Global Service Graph で、検索バーを使用して結果をフィルタリングできるようになりました。管理者は、次の条件を満たす場合に、この検索バーを使用して、特定のインスタンス/クライアント/アプリケーション/データセンターにすばやく絞り込むことができます。

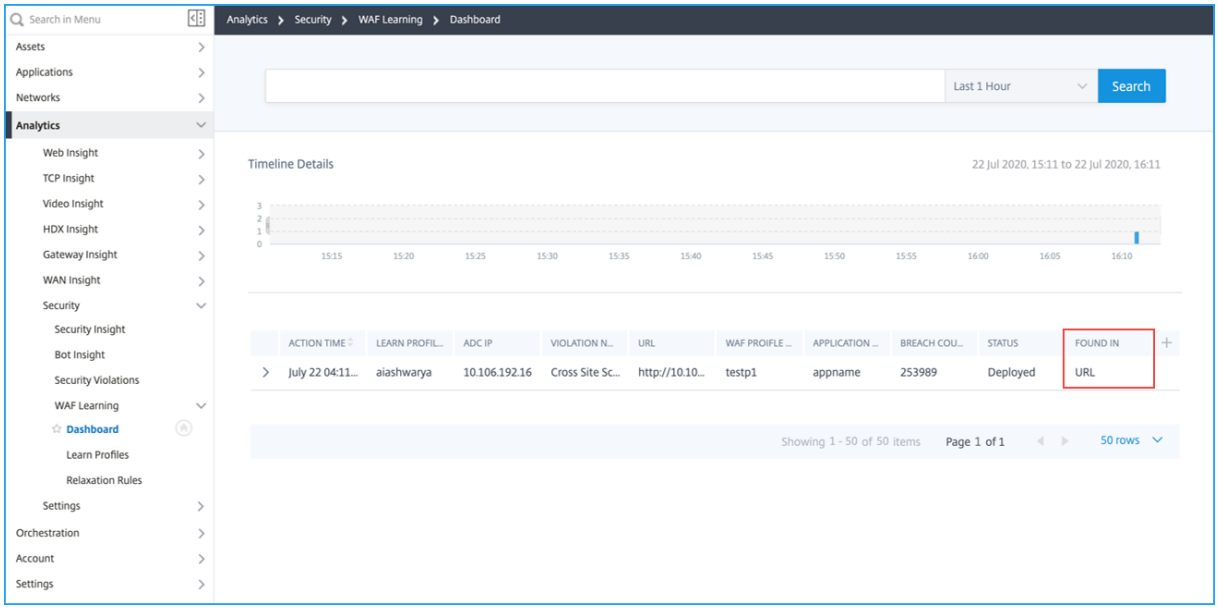
- 多数のデータセンターを持つ大企業
- データセンターごとに多数の Citrix ADC インスタンスを構成しました
- 各 Citrix ADC インスタンス経由で展開またはアクセスされる多数のアプリケーションを構成
- 異なる場所からアプリケーションにアクセスするクライアント

詳しくは、「サービスグラフ-すべてのアプリケーションの全体的ビュー」を参照してください。

[NSADM-52149]

クロスサイトスクリプト違反のログメッセージの拡張

クロスサイトスクリプト違反が展開された **WAF** ラーニングダッシュボードで、新しい属性を表示できるようになりました。この新しい属性は、クロスサイトスクリプト違反の場所を指定します。違反の場所には、フォームフィールド、URL、ヘッダー、Cookie、またはその他の場所を指定できます。



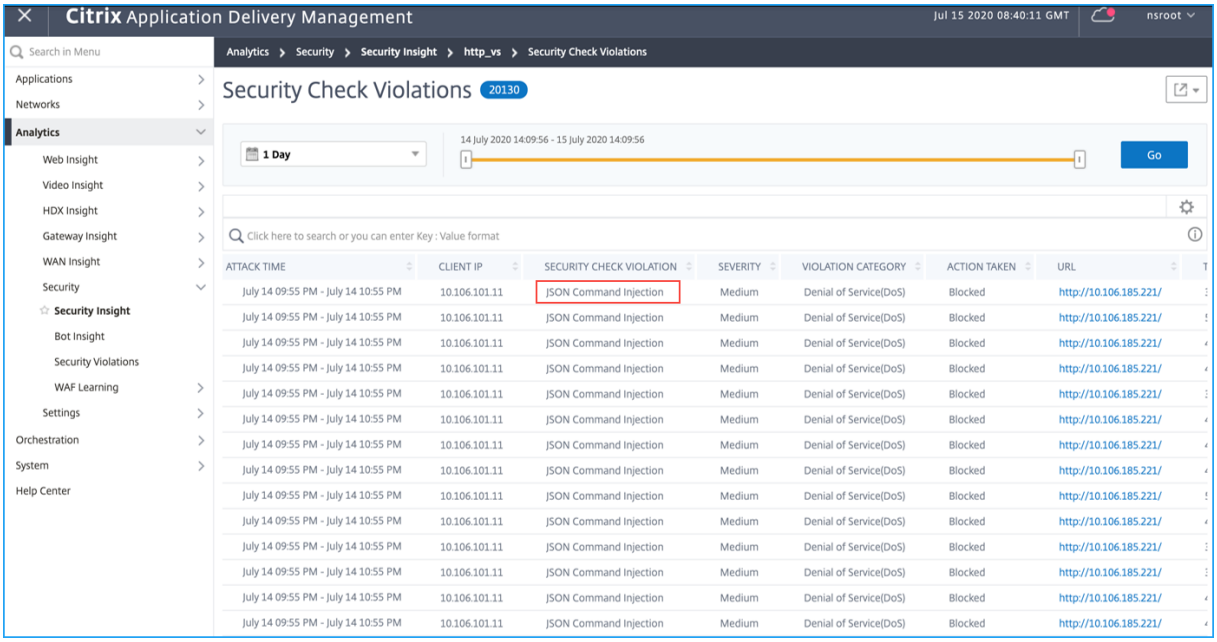
[NSADM-52941]

Security Insight — JSON コマンドインジェクション

Security Insight で、新しい違反の種類である JSON コマンドインジェクションを表示できるようになりました。Security Insight で JSON コマンドインジェクション違反を生成するには、Citrix ADC インスタンスで次のコマンドを構成する必要があります。

```
add appfw profile abc_js -type JSON -startURLaction none -starturlclosure
off -jsoncmdinjectionaction block log stats -jsoncmdinjectiontype cmdkeyword
```

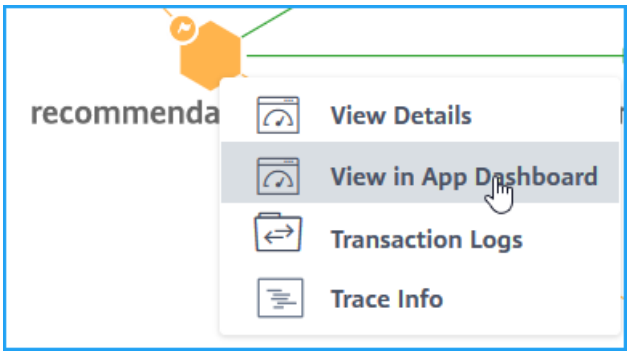
設定後、Security Insight で JSON コマンドインジェクション攻撃を表示できます。



[NSADM-52869]

Kubernetes アプリケーションのサービスグラフ **—** アプリダッシュボードでアプリの詳細を表示

サービスグラフで、サービスをクリックして [**App Dashboard** で表示] を選択すると、選択したアプリの詳細が [**App Dashboard**] に表示されます。



詳しくは、「マイクロサービスアプリケーションのアプリケーションの詳細」を参照してください。

[NSADM-56583]

アプリのセキュリティ違反でセキュリティインサイトとボットインサイト攻撃の詳細を表示する

アプリセキュリティ違反では、****WAF** カテゴリと Bot カテゴリで、セキュリティインサイトとボットインサイト攻撃の詳細をそれぞれ表示できるようになりました。**[**** 分析**] > [**セキュリティ**] > [**セキュリティ違反] に移動して、次の違反を表示します。

WAF	ボット
バッファオーバーフロー	昇降補助具
コンテンツの種類	フィードフェッチャー
クッキーの一貫性	リンクチェッカー
CSRF フォームタグ付け	マーケティング
URL を拒否する	スクレーパー
フォームフィールドの一貫性	スクリーンショットクリエーター
フィールドの書式	検索エンジン
最大アップロード数	サービスエージェント
リファラーヘッダー	サイトモニター
安全な商取引	スピードテスター
セーフオブジェクト	ツール
HTML SQL 注入	未分類
開始 URL	ウイルススキャナー
クロスサイトスクリプティング **(XSS)**	脆弱性スキャナ
XML DoS	DeviceFP 待ち時間を超えました
XML 形式	無効なデバイス EFP
XML WSI	キャプチャ応答が無効です
XML SSL	キャプチャの試行回数を超えました
XML 添付ファイル	有効なキャプチャ応答
XML SOAP 障害	キャプチャクライアントミュート
XML バリデーション	キャプチャ待ち時間を超えました
そのほか	リクエストサイズの制限を超えました
IP レピュテーション	レート制限を超えました
HTTP DOS	ブロックリスト（IP、サブネット、ポリシー式）
TCP スモールウィンドウ	許可リスト（IP、サブネット、ポリシー式）
署名違反	ゼロピクセルリクエスト
ファイルのアップロードタイプ	接続元 IP
JSON クロスサイトスクリプティング **(XSS)**	ホスト
JSON SQL	ジオロケーション

WAF	ボット
JSON DOS	URL
コマンドインジェクション	
コンテンツタイプ XML を推論する	
クッキーハイジャック	

[NSADM-54296]

ピーク使用率とリーン期間の分析-アプリのスケール制限を評価し、上位 **5** つのアプリケーションメンテナンスウィンドウを特定します

管理者は、トラフィックを分析し、次のことを決定する適切な時間を見つける必要があります。

- 本番環境でアプリケーションをスケールアップする場合
- アプリケーションのダウンタイムをスケジュールする場合

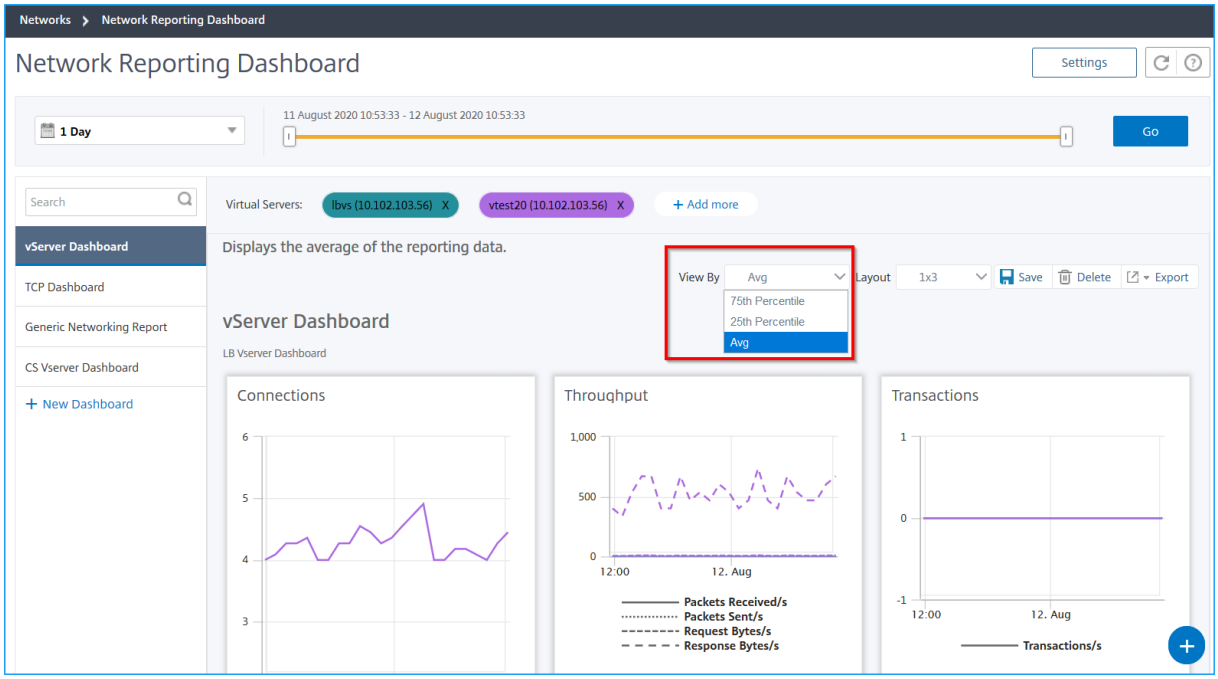
Citrix ADM ピーク使用量とリーン期間分析機能を使用すると、選択した期間の主要なメトリックを分析できます。これらのメトリックから、トラフィックを分析し、ウェブアプリケーションをスケールアップするか、スケジュールされたダウンタイムを計画するタイミングを決定できます。

詳しくは、「アプリケーションのピーク使用率とリーン期間の分析」を参照してください。

[NSADM-52167], [NSADM-52140]

集約を適用してネットワークレポートデータを表示する

ネットワークパフォーマンスデータに集約を適用し、ダッシュボードでアプリケーションのパフォーマンスを表示できるようになりました。要件に基づいて結果をエクスポートすることもできます。データに適用されたこれらの集計を使用して、すべてのリソースを最適に分析し、確実に活用することができます。[ネットワーク**] > [**ネットワークレポート] に移動し、1 日またはそれ以降の期間を選択して [表示方法] オプションを表示します。



既存のデータで、「表示別」(**View** By) リストからオプションを選択して、集計を適用できます。詳しくは、「集約フィルタを適用してネットワークレポートデータを表示する」を参照してください。

[NSADM-56494]

スマート展開での評価ライセンスの種類を選択

これで、評価ライセンスを使用して ADM Autoscale ソリューションを体験できます。[スマートデプロイ] オプションを選択して ADC インスタンスを AWS にデプロイするときに、[評価] ライセンスタイプを選択できるようになりました。このオプションを使用すると、Citrix ADC VPX Express 製品を展開できます。また、最大 3 つのインスタンスまで AutoScale できます。

[NSADM-52143]

解決された問題

ライセンス

エージェントの再起動により、Citrix ADM ライセンスは無効になります。

[NSHELP-23539]

ネットワーク

エージェントの登録が成功した後でも、Citrix ADM エージェントの状態で`reset:requested`が表示されます。

[NSHELP-23413]

StyleBook

デフォルトの StyleBooks を使用して AutoScale グループアプリケーションを構成する場合、DNS および UDP モニタタイプはサポートされません。この修正により、次の AutoScale グループ StyleBooks のバージョンが更新されました。

- lb-mon-autoscale-v1.5
- cs-lb-mon-autoscale-v1.4

[NSADM-55982]

2020 年 7 月 24 日

アプリのセキュリティ違反-ネットワーク

アプリセキュリティ違反のネットワーク違反の一部として、セグメントスマック攻撃を表示できるようになりました。詳しくは、「アプリのセキュリティ違反」を参照してください。

[NSADM-46025]

Kubernetes アプリケーションのサービスグラフ-問題のトラブルシューティングのためのクライアントメトリックの表示

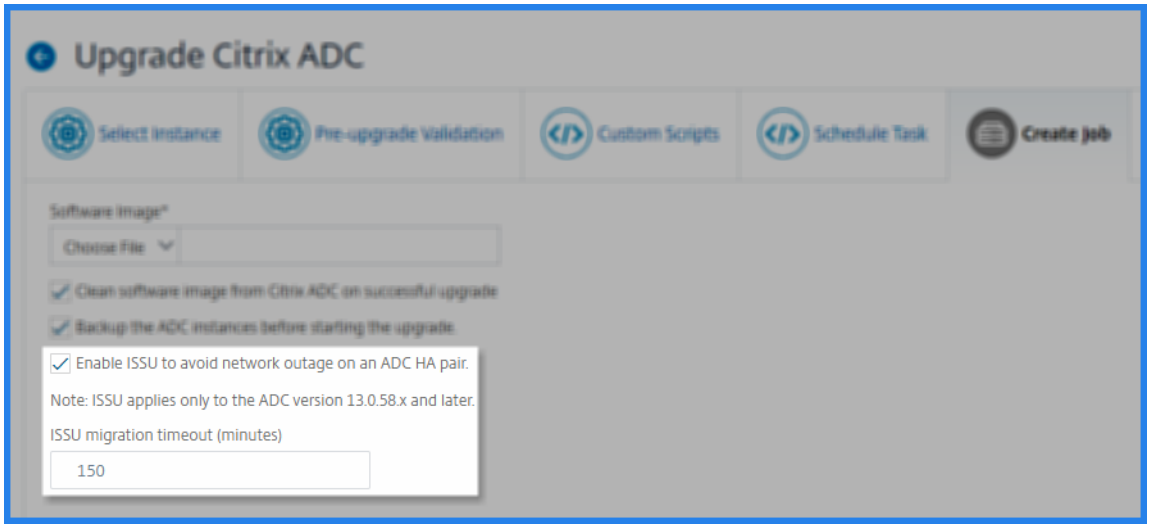
Kubernetes アプリケーションのサービスグラフで、クライアントがサービスにアクセスしている場所を確認できるようになりました。管理者は、クライアントメトリックスを視覚化し、クライアントから発生する問題を分析できます。

詳しくは、「サービスグラフで詳細を表示」を参照してください。

[NSADM-54335]

インサービスソフトウェアアップグレードのサポート

アップグレードジョブの作成時に、インサービスソフトウェアアップグレード（ISSU）オプションを選択できるようになりました。ISSU は、ADC 高可用性ペアでのダウンタイムなしのアップグレードを保証します。ISSU 機能は、アップグレード中に既存の接続を使用する移行機能を提供します。したがって、ダウンタイムなしで ADC HA ペアをアップグレードできます。



[NSADM-43357]

StyleBooks で **ADM IP** アドレス管理（**IPAM**）ネットワークを動的に一覧表示

StyleBook を構築して、ユーザーが IP アドレスを自動割り当てする ADM IPAM ネットワークを選択できるようになります。IPAM ネットワークリストは ADM から動的に取得されます。以前は、**StyleBook** 定義に記載されている IPAM ネットワークを選択できました。

これで、`type:ipaddress`のパラメータ定義に新しい属性`dynamic-allocation`が追加されます。入力として**`true`**または**`false`**を取ることができます。この値を**`true`**に設定した場合、ユーザは ADM 内の IP アドレス管理ネットワークのリストからネットワークを選択できます。次に、ADM は、選択したネットワークから IP アドレスを自動的に割り当てます。

例:

```
  -
    name: virtual-ip
    label: "Load Balancer IP Address"
    type: ipaddress
    dynamic-allocation: true
    required: true
<!--NeedCopy-->
```

この例では、`virtual-ip` フィールドには ADM 内の IPAM ネットワークが一覧表示されます。リストからネットワークを選択して、ネットワークから IP アドレスを自動割り当てます。設定が削除されると、IP アドレスはネットワークに解放されます。

[NSADM-54246]

StyleBooks と構成パックのユーザー認証の改善

管理者は、［アカウント］**>**［ユーザー管理］**>**［グループ］ページで、特定の StyleBook および構成パックをユーザーグループに対して承認するための制御が向上しました。認証設定の **StyleBooks** セクションと **Configpacks** セクションが改善され、次の変更が加えられています。

- **StyleBooks** — 正規表現を含むフィルタ式を使用して、StyleBooks の認可リストを指定できるようになりました。

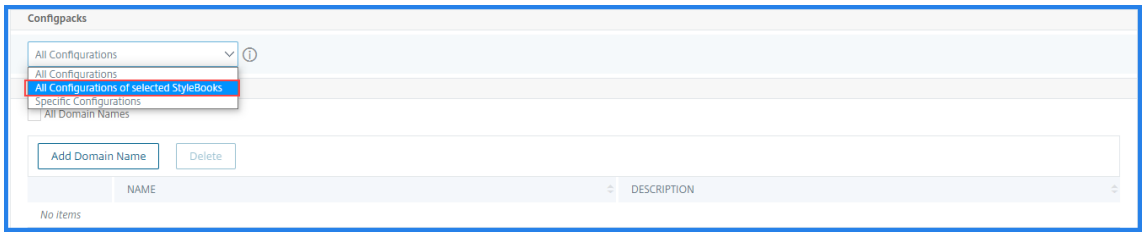
  例:

  ```
  name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND version=1.0
  ```

  このクエリは、次の条件を満たす StyleBook をリストします。

  - StyleBook 名は`lb-mon`または`lb`のいずれかです。
  - StyleBook の名前空間は`com.citrix.adc.stylebooks`です。
  - StyleBook 版は `1.0`です。

- 構成パック — 選択した StyleBooks に属する構成パックについて、ユーザーを認証できるようになりました。これを行うには、[**Configpacks**] セクションの **[**選択した **StyleBooks** のすべての構成] を選択します。

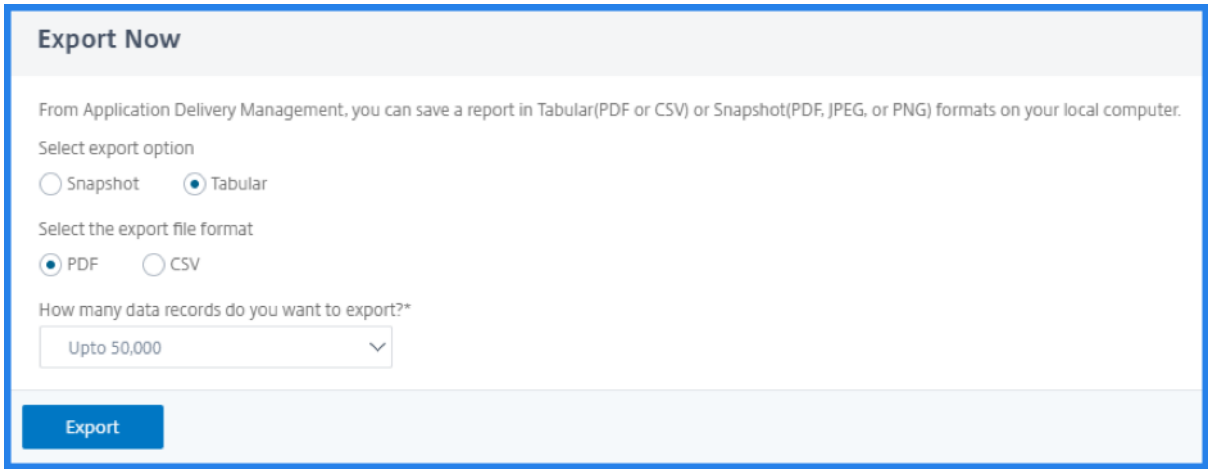


[NSADM-52334]

2020 年 **7** 月 **15** 日

ADM レポートを表形式でエクスポートする

ADM レポートを表形式またはスナップショットでエクスポートできるようになりました。また、表形式でエクスポートするデータレコードの数を選択することもできます。以前は、レポートをスナップショットとしてのみエクスポートできました。

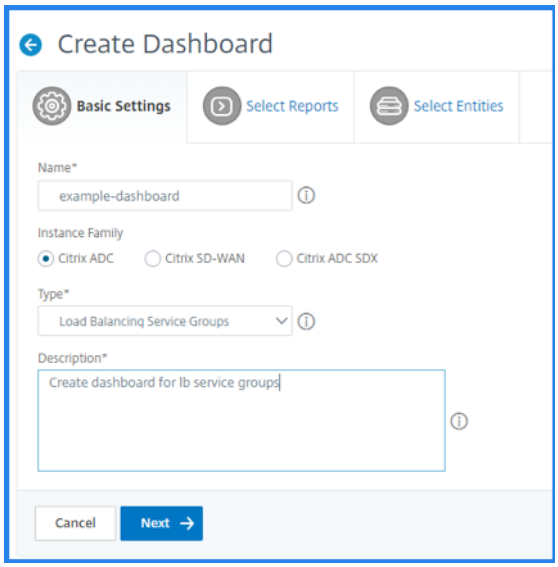


詳しくは、「エクスポートレポートのエクスポートまたはスケジュール設定」を参照してください。

[NSADM-52461]

負荷分散サービスグループのネットワークレポートの生成

負荷分散サービスグループとサービスの両方について、ネットワークレポートダッシュボードを作成できるようになりました。以前は、負荷分散サービスのダッシュボードのみを作成できました。



このダッシュボードには、選択したサービスグループの次のレポートを表示できます。

- 接続: クライアントとサーバーの接続カウンタ。
- スループット: 要求バイト数と応答バイトカウンタ。
- Time to First Byte（TTFB）: 要求パケットをサービスグループに送信し、サービスグループから最初のパケットを受信するのに要した平均時間。この応答時間は TTFB と呼ばれます。

詳しくは、「ネットワークレポート」を参照してください。

[NSADM-51596]

認証、認可、および監査ポーリングおよびネットワークレポートのサポート

Citrix ADM は、ADC インスタンスから認証、承認、監査（Citrix ADC AAA）イベントをポーリングし、ネットワークレポートでその傾向を視覚化できるようになりました。ADM GUI には、ダッシュボードを作成するための次の Citrix ADC AAA ネットワークレポートが含まれています。

- **HTTP** 認証の成功と失敗
- **HTTP** 以外の認証の成功と失敗
- **AAA** セッション
- 現在の **AAA** セッション
- 現在の **ICAOnly** セッション
- 現在の **ICAOnly** 接続
- 現在の **ICA**（**SmartAccess**）接続
- 認証の成功と失敗

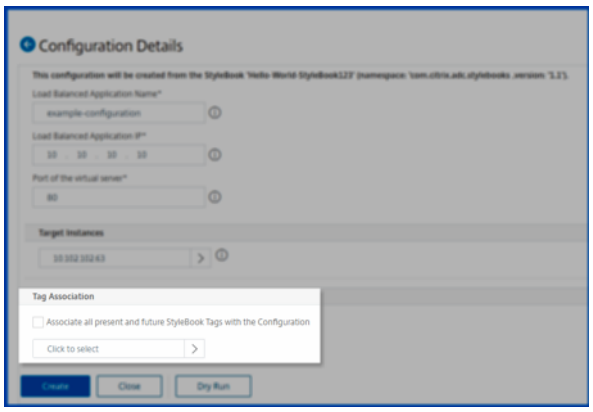
詳しくは、「ネットワークレポート作成」を参照してください。

[NSADM-51372]

StyleBook タグをその構成に関連付ける

StyleBooks では、ラベルの用語は **Tag** に変更されます。これで、StyleBook タグを構成パックに関連付けることができます。そのため、StyleBook タグ自体を使用して構成パックを検索できます。
構成パックを作成するときは、[タグの関連付け] セクションで次のいずれかのオプションを使用します。

- 現在および将来のすべての **StyleBook** タグを構成に関連付ける — このオプションは、すべての StyleBook タグを構成パックに関連付けます。また、今後 StyleBooks に追加する可能性のある新しいタグを必ず関連付けます。
- 「タグの選択」 -このオプションは、選択した StyleBook のタグを表示します。必要な StyleBook タグを選択し、構成パックに関連付けることができます。



詳しくは、「StyleBook のタグを作成する」を参照してください。

[NSADM-53600]

StyleBooks は条件付きパラメータをサポートしています

StyleBook 設定フォームで、別のパラメータで指定された値に基づいて、パラメータの外観または初期値を動的に制御できるようになりました。これを行うには、パラメータ定義で`dependent-parameters`属性を使用します。このアトリビュートは、新しい`gui`サブ属性として新たに追加されます。
フォーム上でのパラメーターの動作を制御するソースパラメーターにこの属性を指定します。この属性には、他のパラメータを制御する複数の条件を含めることができます。
たとえば、ソースパラメータプロトコルは依存パラメータ証明書を持つことができます。証明書は、プロトコルパラメータ値が SSL の場合にのみ表示されます。
各条件は、次の属性を持つことができます。

- `target-parameter`: この条件を適用するターゲットパラメーターを指定します。
- `matching-values`: アクションをトリガーするソースパラメーターの値のリストを指定します。
- `action`: ターゲットパラメーターで次のいずれかのアクションを指定します。
  - `read-only`: パラメーターは読み取り専用になります。
  - `show`: パラメーターが非表示の場合、フォームに表示されます。
  - `hide`: パラメーターがフォームから削除されます。
  - `set-value`: パラメータ値は value 属性で指定された値に設定されます
- `value`: アクションが`set-value`の場合のターゲットパラメーターの値。

ユーザー入力がソースパラメーターの指定された値と一致する場合、ターゲットパラメーターの外観または値は、指定されたアクションに従って変化します。

詳しくは、「依存パラメータ」を参照してください。

[NSADM-52329]

StyleBook 設定を作成または更新したユーザーの表示

StyleBook > Configurations で、構成パックを作成または最後に更新したユーザーを表示する新しい列が追加されます。ユーザーによって構成パックをフィルター処理する場合は、プロパティの一覧から [作成者] オプションを選択して、構成パックをフィルター処理します。

[NSADM-52336]

スクリプトを使用して **AWS** でゼロタッチエージェントを有効にする

AWS で ADM エージェントを起動するときに、ユーザーデータとしてエージェント自動登録スクリプトを指定できるようになりました。スクリプトの例をAWS に Citrix ADM エージェントをインストールするに示します。このスクリプトは、AWS シークレットマネージャーから認証の詳細を取得し、deployment.py スクリプトを実行して、エージェントを ADM サービスに登録します。
または、次のいずれかを実行することもできます。

- 起動時にエージェントを自動登録するユーザーデータに、実際の認証の詳細を指定します。

- エージェントが正常に起動した後、deployment_type.py スクリプトを使用してエージェントを登録します。詳しくは、「AWS に Citrix ADM エージェントをインストールする」を参照してください。

[NSADM-55322]

Citrix ADM での **WAF** 学習

管理者は、学習プロファイルを設定して、緩和規則リストを生成できます。

- 選択した Web アプリケーションのみ
- 選択したプロファイル名のみ

詳しくは、「ラーニングプロファイルの設定」を参照してください。

[NSADM-49494]

アプリのセキュリティ違反-ネットワーク

既存のアプリのセキュリティ違反とは別に、ネットワーク違反の一部として次の違反を表示できるようになりました。

- HTTP desync 攻撃
- ブライヘンバッハー攻撃

詳しくは、「アプリケーションのセキュリティ違反の詳細」を参照してください。

[NSADM-49468], [NSADM-46460]

トラブルシューティングのための入力メトリックと入力の詳細を表示する

サービスグラフで、次の項目を表示できます。

- 入力メトリック
- 進入の詳細（ドリルダウン）
- 使用される進入のタイプ
  - 階層 **1** の入力 — Kubernetes クラスタ内の CitrixIngress Controller は、Kubernetes クラスタ外の Citrix ADC インスタンス（VPX/MPX/SDX/BLX）を構成します。
  - 階層 **2** の入力 — Kubernetes クラスター内の Citrix ADC CPX インスタンスとともにサイドカーとして動作する CitrixIngress Controller です。

    > 注：Kubernetes クラスタで 2 層アーキテクチャ（ADC を MPX/VPX/SDX/BLX として使用、および ADC を CPX として使用した階層 2 入力）を構成している場合にのみ、階層 1 入力と階層 2 入力を表示できます。

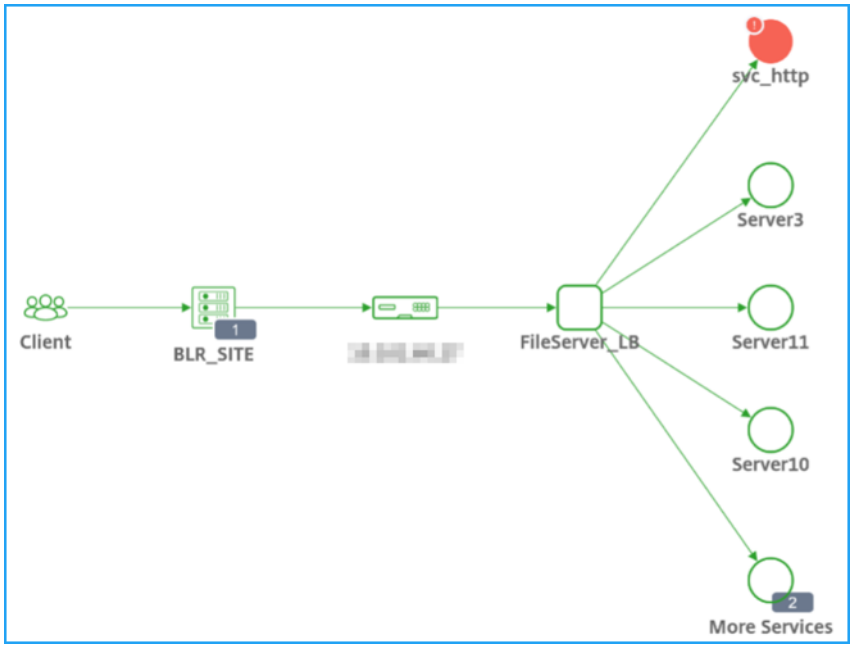
詳しくは、「問題のトラブルシューティングに関する進入の詳細の表示」を参照してください。

[NSADM-53755]

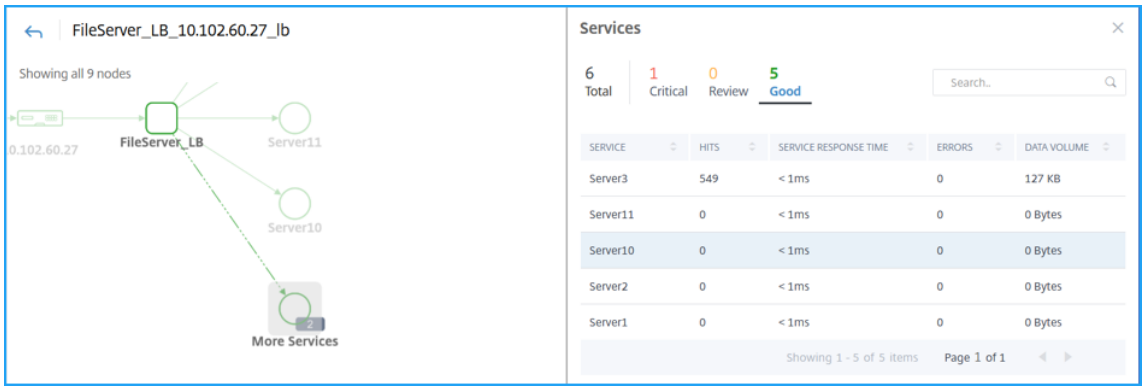
3 層の **Web** アプリケーションサービスグラフの改良

3 層の Web アプリケーションサービスグラフが即興で次のように変更されました。

- サービスはグループ化され、上位 4 つの低スコアサービスのみが表示されます。

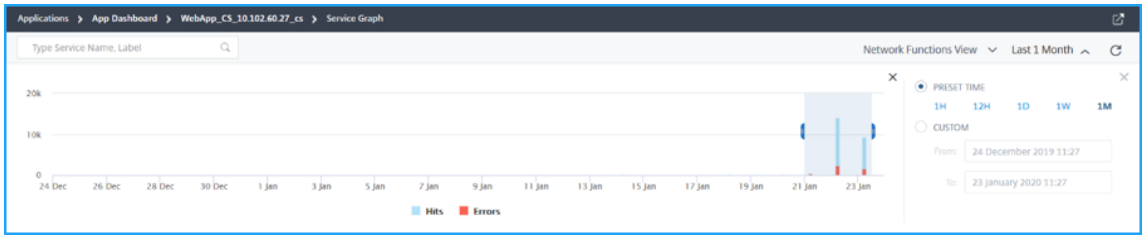


[その他のサービス] をクリックして、[クリティカル]、[レビュー]、[良好] などのステータスに基づいてすべてのサービスを表示します。

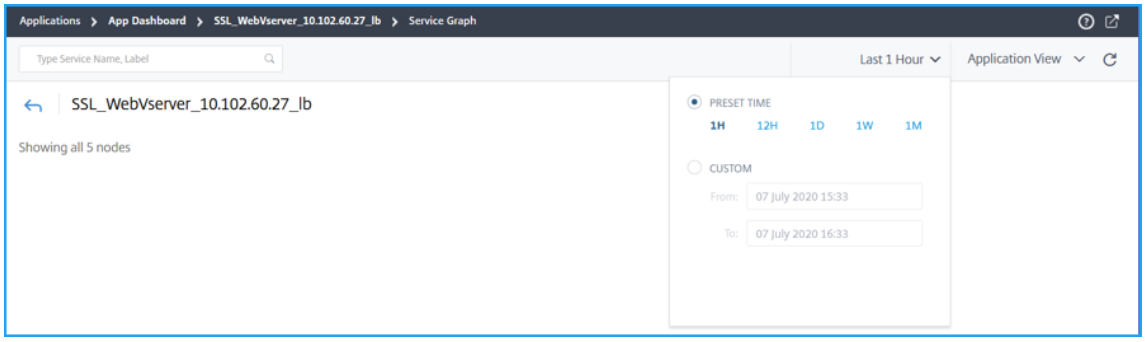


- ヒットとエラーの棒グラフは表示されません。

以前の

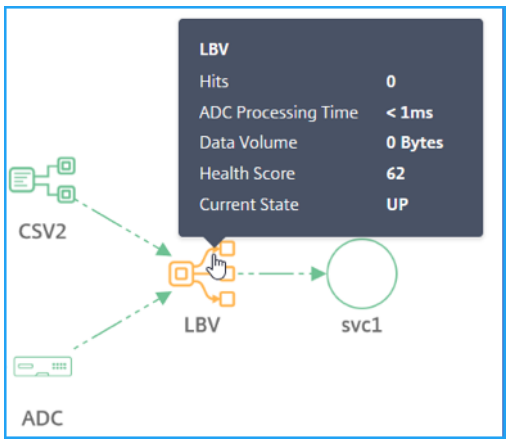


現在

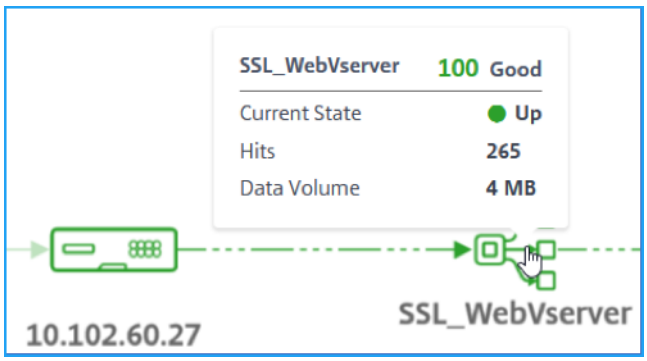


- ネットワーク機能のメトリックが更新されます。

  以前の



  現在

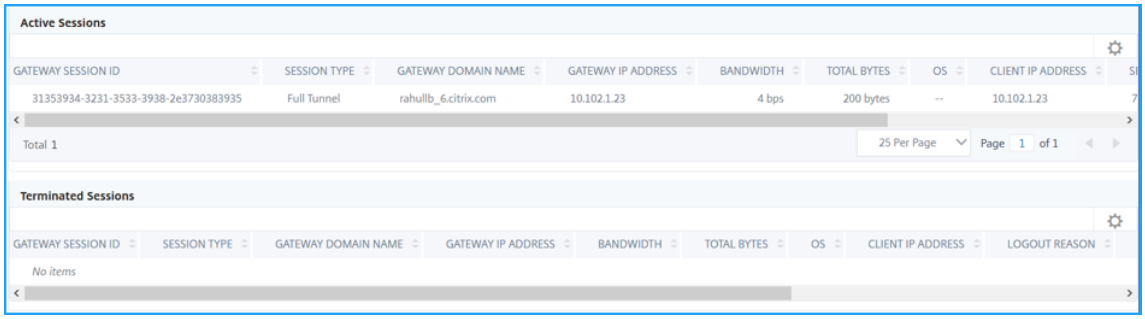


[NSADM-52147]

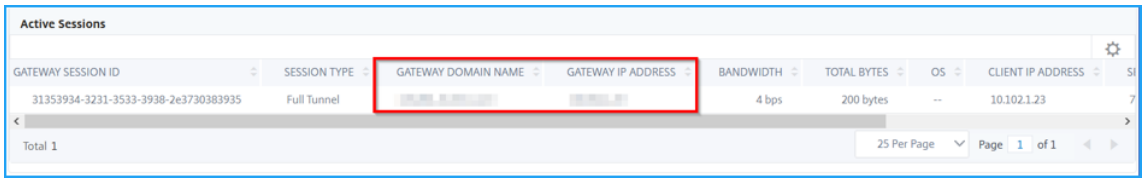
Gateway Insight 改善

Gateway Insight で、ゲートウェイユーザーに対する次の機能強化を表示できるようになりました。管理者として、これらの機能強化により、レポートをエクスポートするときに完全なユーザー情報を取得できます。[アナリティクス**] > [Gateway Insight] > [**ユーザー] に移動し、表示するユーザーを選択します。

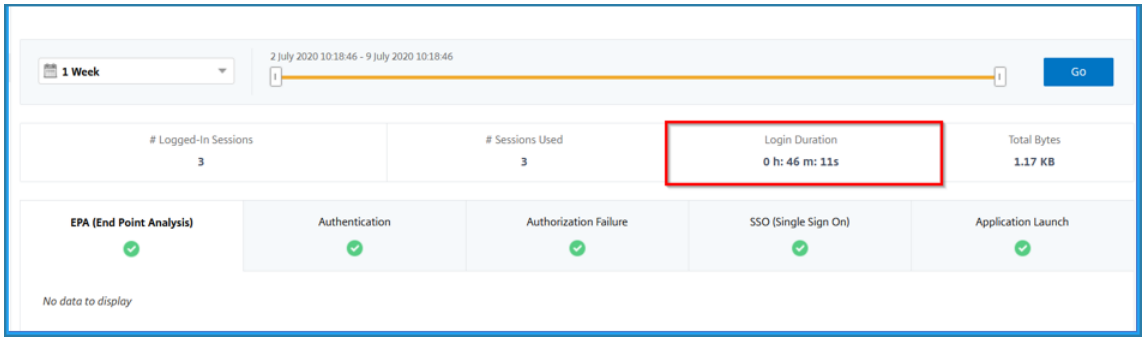
- ユーザーのアクティブセッションと終了したセッション。



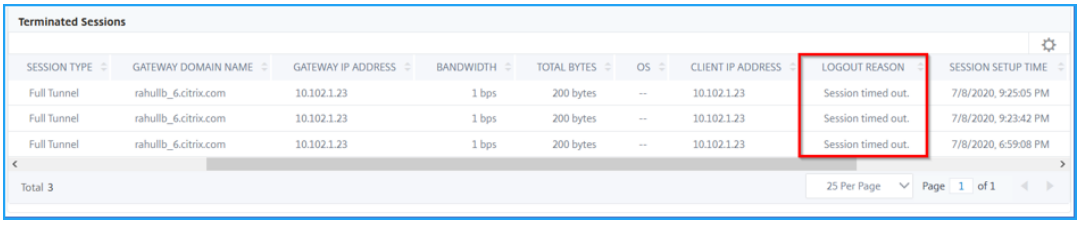
- アクティブセッションのゲートウェイドメイン名とゲートウェイの IP アドレス。



- ユーザーのログイン時間。



- ユーザーのログアウトセッションの理由。ログアウトの理由は次のとおりです。
  - セッションのタイムアウト
  - 内部エラーのためログアウトしました
  - 非アクティブセッションがタイムアウトしたためログアウトしました
  - ユーザーがログアウトしました
  - 管理者がセッションを停止しました



[NSADM-52763]、[NSADM-52767]、[NSADM-52764]、[NSADM-53496]

SDX インスタンス用の組み込みエージェントのサポート

SDX インスタンスで Citrix ADM 組み込みエージェントを使用できるようになりました。さらに、MASToolsを使用して組み込みエージェントを開始できます。詳細については、インスタンスを管理するように ADC 組み込みエージェントを構成するを参照してください。

解決された問題

Analytics

ADM が ADC メトリック情報を収集すると、CPU 使用率が高くなります。

[NSADM-56374]

システム

[システム設定**]** ページで **[**インスタンスログインの認証情報のプロンプト**]** を有効にすると、ADM GUI はインスタンスダッシュボードにライセンス情報を表示しません。

[NSHELP-23944]

ネットワーク

管理対象インスタンスの数が 58 インスタンスの上限を超えている場合、[**Networks] > [Licenses**] の下に、ADM GUI に管理対象インスタンスの不正なライセンス情報が表示されます。この修正により、インスタンスの最大数が 1000 に増加しました。

[NSHELP-23956]

2020 年 6 月 30 日

アプリのセキュリティ違反 — 地域ごとの一意の **IP** の過剰

[地域ごとの過大な **Unique IP**] インジケータでは、リージョンに基づく異常の総数を表示する地理マップを表示できるようになりました。グラフには、選択したリージョンの関連する違反の詳細が表示されます。

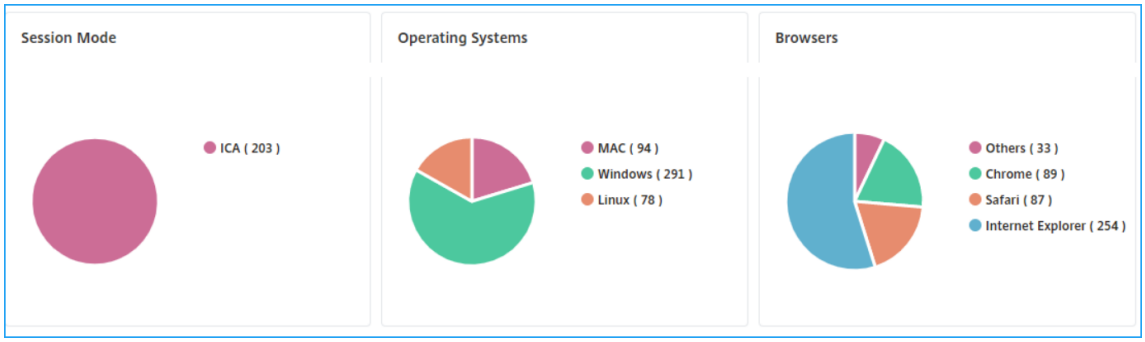
詳しくは、「地域ごとの過度なユニーク IP 数」を参照してください。

[NSADM-52555]

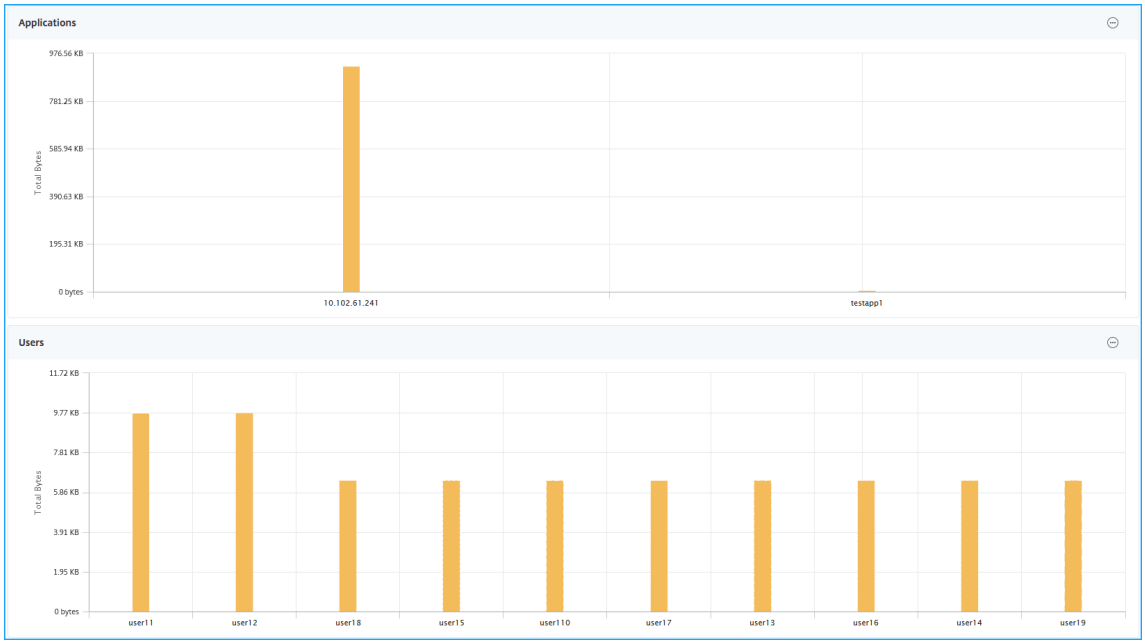
Gateway Insight 改善

Gateway Insight で、次の機能強化を表示できるようになりました。

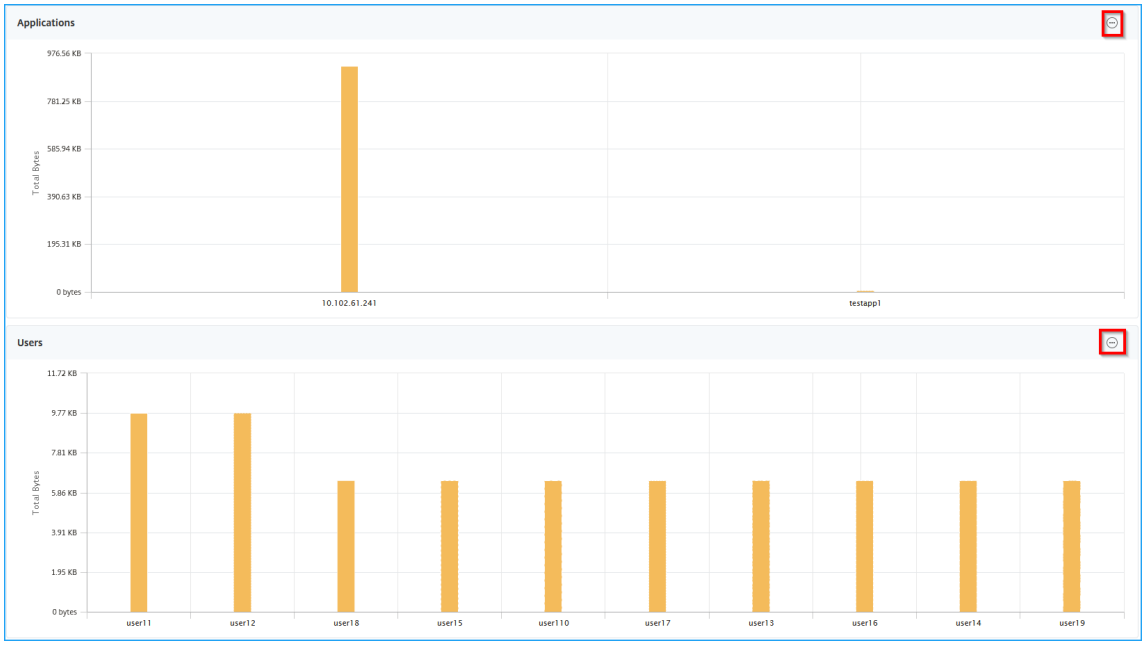
- ユーザーの詳細 -ADC Gateway アプライアンスに関連付けられた各ユーザーのインサイトを表示できます。[分析] > [**Gateway Insight**] >**[ユーザー]** に移動し、ユーザーをクリックして、セッションモード、オペレーティングシステム、ブラウザーなど、選択したユーザーのインサイトを表示します。



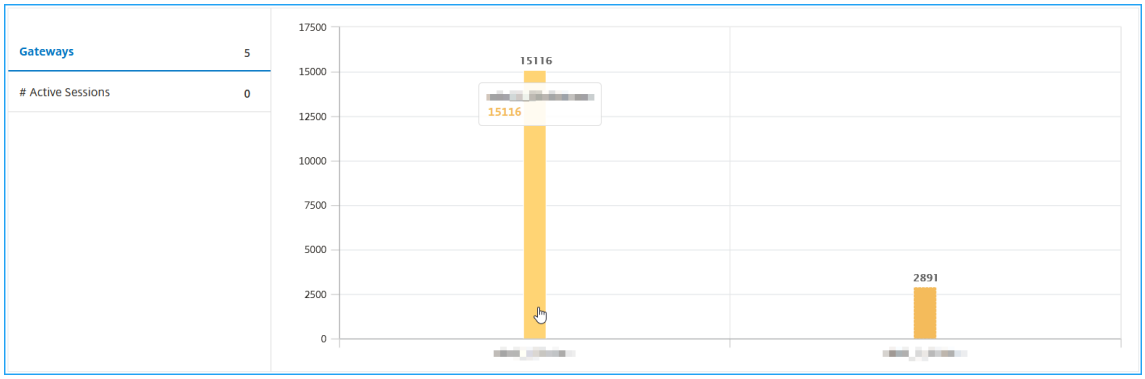
- 選択したゲートウェイのユーザーとアプリケーション-[**Analytics**] > [**Gateway Insight**] >**[Gateway]** に移動し、ゲートウェイドメイン名をクリックして、選択したゲートウェイに関連付けられている上位 10 のアプリケーションと上位 10 人のユーザーを表示します。



- アプリケーションとユーザーの表示オプション — 10 を超えるアプリケーションおよびユーザーの場合、[アプリケーションとユーザー] の [詳細] アイコンをクリックすると、選択したゲートウェイに関連付けられているすべてのユーザーとアプリケーションの詳細を表示できます。



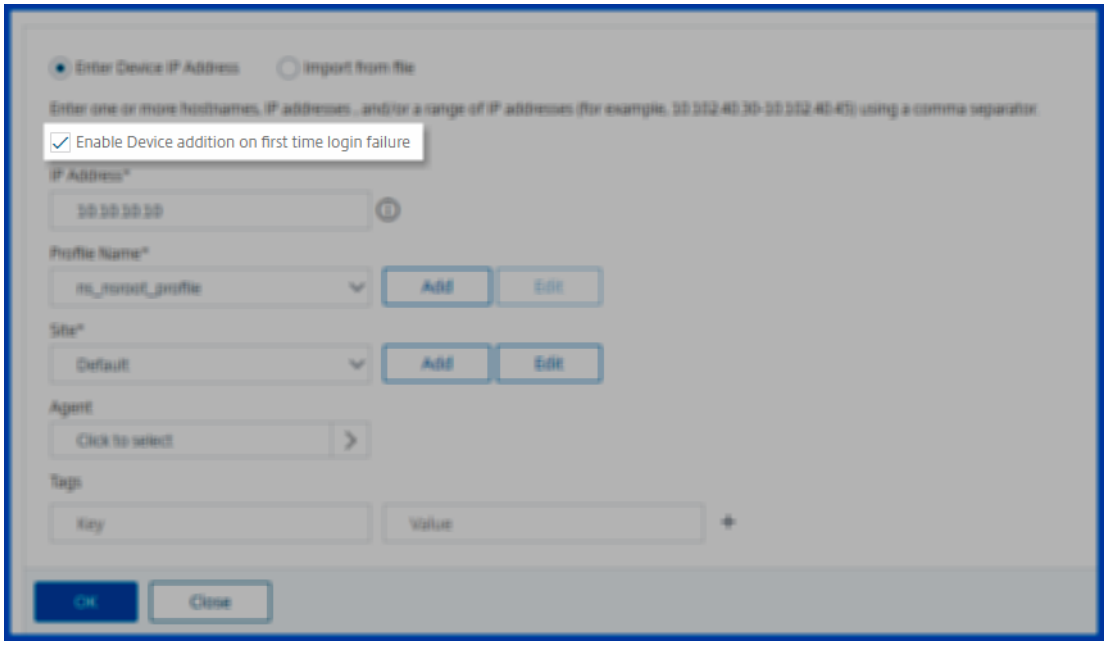
- 棒グラフをクリックして詳細を表示 — 棒グラフをクリックすると、関連する詳細を表示できます。たとえば、[アナリティクス] **> [Gateway Insight] > [**ゲートウェイ] の順に選択し、ゲートウェイの棒グラフをクリックしてゲートウェイの詳細を表示します。



[NSADM-53489]、[NSADM-53508]、[NSADM-53906]、[NSADM-52768]

有効な認証情報なしで **ADC** インスタンスを追加可能

Citrix ADM でインスタンスを初めて追加するときに、有効な資格情報がない場合でもインスタンスを追加できるようになりました。インスタンスが追加されると、［ネットワーク］**>**［インスタンス］**>**［**Citrix ADC** ］ページで［ダウン］状態になり、［ログイン失敗］警告が表示されます。ADM でインスタンスを管理するための正しい認証情報を指定します。



インスタンスがライセンスされていない場合、インスタンスを選択すると [**License**] オプションが表示されます。[**License**] をクリックして、ライセンスプールからインスタンスにライセンスを適用します。

[NSADM-44856]

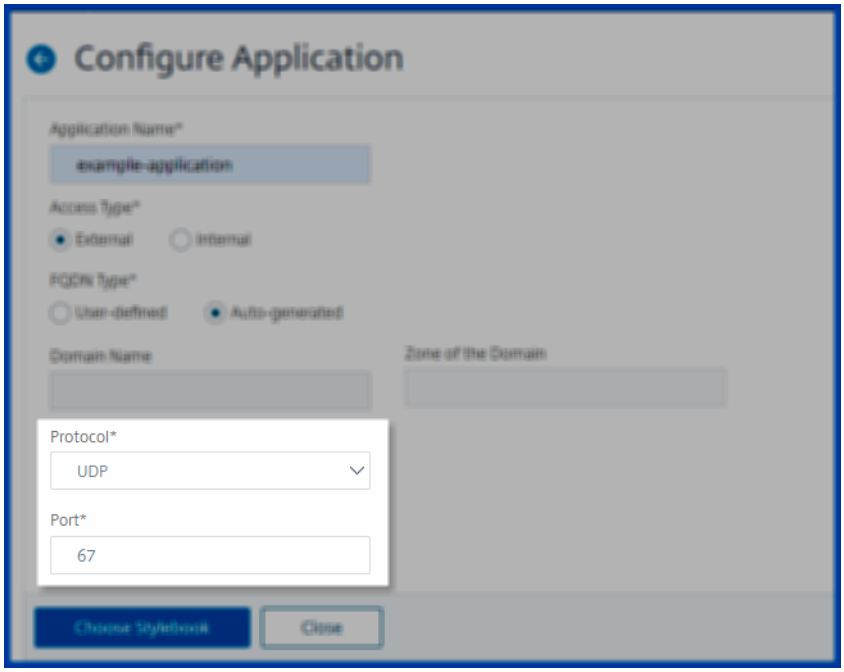
[プールされた容量**]** ページの下に **ADC FIPS** インスタンスプールを表示する

ADC FIPS インスタンスは、FIPS インスタンスプールからライセンスをチェックアウトできるようになりました。したがって、ADM GUI では、[ネットワーク**] > [**ライセンス**] > [**帯域幅ライセンス**] > [**プールされた容量**]** ページの下に、**FIPS** インスタンスに割り当てられたプールライセンスが表示されます。

[NSADM-51207]

Azure での **AutoScale** グループアプリケーションは **UDP** トラフィックをサポートします

Azure 内の AutoScale グループアプリケーションは、UDP トラフィックを受信できるようになりました。アプリケーションを Autoscale グループに設定する場合は、UDP トラフィックを許可する **UDP** プロトコルとポート値を選択します。



この機能により、アプリケーションを構成するために、次の AutoScale グループ StyleBooks が新たに追加されます。

- `lb-mon-autoscale-v1.4`
- `cs-lb-mon-autoscale-v1.3`

[NSADM-53288]

解決された問題

ライセンス

次の条件が満たされると、インスタンスライセンスステータスが [管理] ではなく [**Sync-In-Progress**] として表示されます。

1. 複数のライセンスは、同じエディションとプールに属しています。
2. ADC インスタンスは、プールからライセンスをチェックアウトします。

[NSADM-55928]

システム

- Syslog メッセージは ADM GUI に表示されません。

  [NSADM-55822]

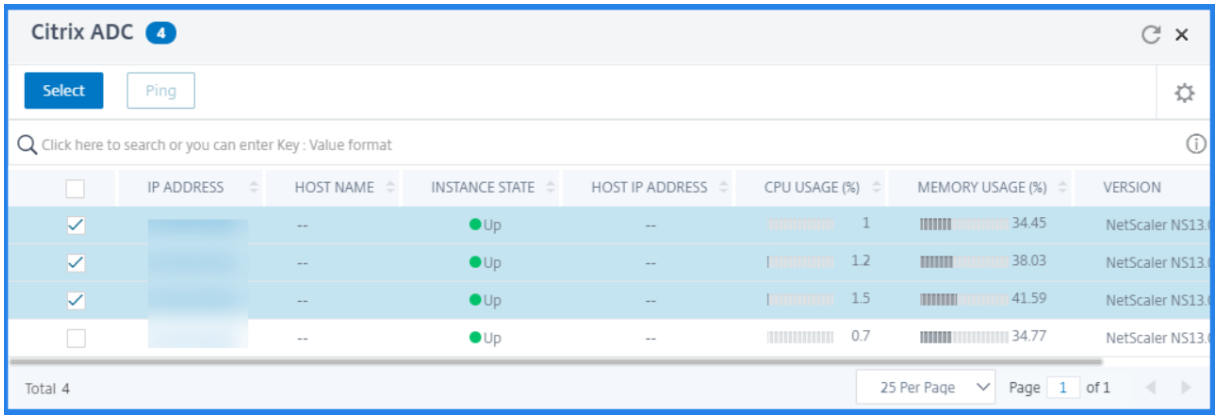
- ユーザーのグループを変更すると、パスワードの複雑さエラーが表示されます。

  [NSHELP-23497]

2020 年 6 月 22 日

一度に複数のターゲットインスタンスを選択

同じ構成パックを複数の ADC インスタンスにデプロイする場合、必要な ADC インスタンスを一度に選択できるようになりました。以前は、構成パックをデプロイするために、インスタンスを 1 つずつ選択する必要がありました。この機能を使用すると、インスタンスをフィルタして、必要なインスタンスを選択することもできます。



[NSADM-50115]

インスタンスの配布をマイナーバージョン別に表示

インスタンスダッシュボードに、管理対象インスタンスの配布がマイナーバージョン別に表示されます。バージョングラフは、すべてのマイナーバージョンのデバイス数を視覚化するのに役立ちます。

[NSADM-42183]

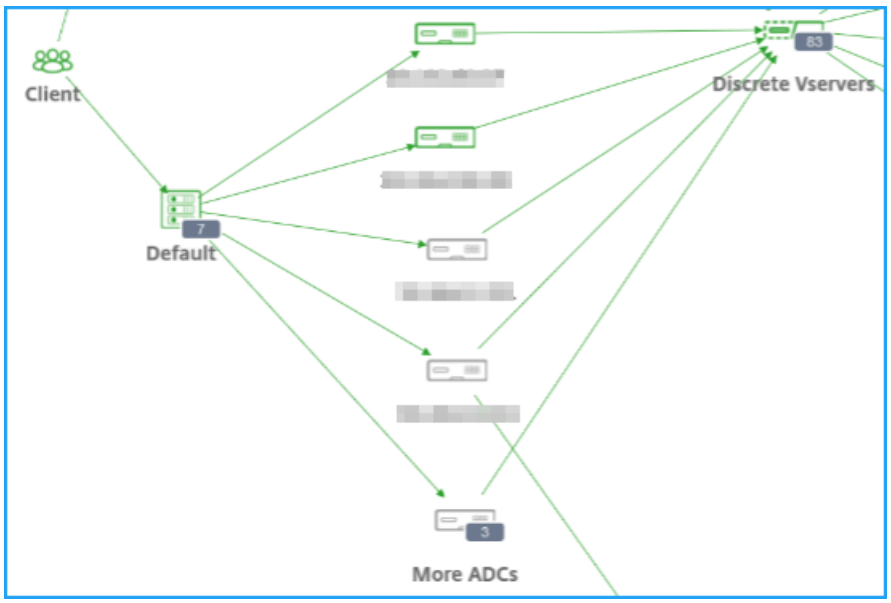
グローバルサービスグラフの改良

管理者として、グローバルサービスグラフ内の単一ペインビューは、次のような場合にインフラストラクチャからアプリケーションビューまで監視するのが難しい場合があります。

- 多数のデータセンターを持つ大企業
- データセンターごとに多数の Citrix ADC インスタンスを構成しました
- 各 Citrix ADC インスタンス経由で展開またはアクセスされる多数のアプリケーションを構成

改善されたグローバルサービスグラフでは、非編成のビューが排除され、次の項目を表示できます。

- Citrix ADC インスタンスの合計でグループ化されたデータセンター
- 各データセンターの上位 4 つの低スコアの Citrix ADC インスタンスのみ



[その他の **ADC**] をクリックして、それぞれのステータス（クリティカル、レビュー、良好および該当なし）タブを選択して、すべての Citrix ADC インスタンスを表示します。インスタンスの IP アドレスをクリックして、インスタンスのスコア、主要メトリック、および ADC インスタンスに関連付けられた問題などのインスタンスの詳細を表示します。

> 注
>
> グローバルサービスグラフからインスタンスをクリックして、Citrix ADC インスタンスの詳細を表示することもできます。

[NSADM-53249]

解決された問題

Analytics

- **Web** トランザクション分析では、保存済みの検索は、ページの更新後に表示されません。

  [NSADM-53722]

- [分析] > [**Web Insight**] では、すべてのメトリックスページ (クライアント、サーバー、URL、要求メソッド、応答ステータス、ユーザーエージェント、オペレーティングシステム) で予想されるデータが表示されない

  [NSADM-53632]

- 適切な RBAC を構成した後でも、[アプリケーション] > [アプリケーションダッシュボード] のアプリケーション、および [ネットワーク機能] > [負荷分散] の仮想サーバーには、グループのユーザーによって新しいスタイルブック/configpack が追加されると、期待されるデータが表示されません。

  [NSHELP-23101]

GUI

- VPN 接続では、ADM は SSO（シングルサインオン）を使用して ADC GUI に接続できません。

  [NSHELP-23099]

2020 年 6 月 04 日

最初のログイン時に **3** つのステップで **AWS** アプリケーションを配信する

ADM GUI に初めてログオンすると、次の 3 つのステップで ADC インスタンスを使用して AWS にあるアプリケーションを配信できます。

1. クラウドアクセスプロファイルを作成して、AWS アカウントを Citrix ADM サービスに登録します。
2. AWS リージョン、VPC の詳細、および ADC ライセンスを指定して AWS 環境を準備します。

   AWS 環境は、AWS インフラストラクチャ、ADM エージェント、および ADM AutoScale グループで構成されます。このステップでは、ADM は次のものを作成します。

   - サブネット、セキュリティグループ、NAT ゲートウェイなどを含む必要なインフラストラクチャを作成する AWS の CloudFormation スタック。
   - ADC インスタンスを管理する VPC 内の ADM エージェント。
   - ADC オートスケール・グループこのグループは、後で [ネットワーク**] > [AutoScale** グループ] ページでカスタマイズできます。

3. 環境準備が成功したら、StyleBook を使用してアプリケーションを構成を実行しアプリケーションを配信します。

最初のログオン後、ADC インスタンスを Autoscale する場合は、Citrix ADM を使用した Citrix ADC 自動スケーリングを参照してください。

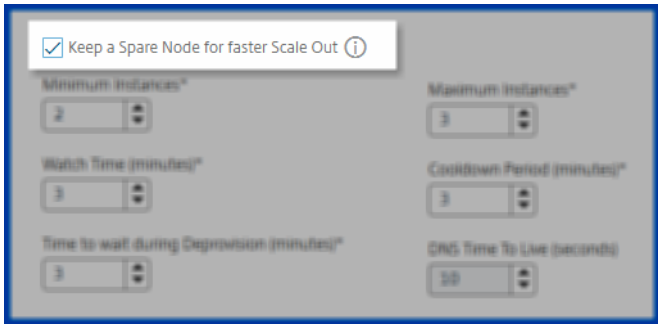
詳しくは、「はじめに」を参照してください。

[NSADM-47626]

AutoScale グループに予備ノードを維持する

AutoScale グループを作成するためにパラメータを指定するときに、より高速なスケールアウトを実現するために、予備ノードを維持することを選択できるようになりました。

ADM は、スケールアウトアクションが発生する前に予備ノードをプロビジョニングし、シャットダウンします。AutoScale グループに対してスケールアウトアクションが発生すると、ADM は、すでにプロビジョニングされているスペアノードを起動します。その結果、スケールアウトにかかる時間が短縮されます。



詳しくは、「Autoscale パラメータの構成」を参照してください。

[NSADM-48191]

自動生成された **FQDN** を使用した **AutoScale** グループアプリケーションの構成

AutoScale グループのアプリケーションを構成するときに、自動生成された FQDN タイプを選択できるようになりました。このオプションでは、ドメインとゾーン名が自動的に生成されます。

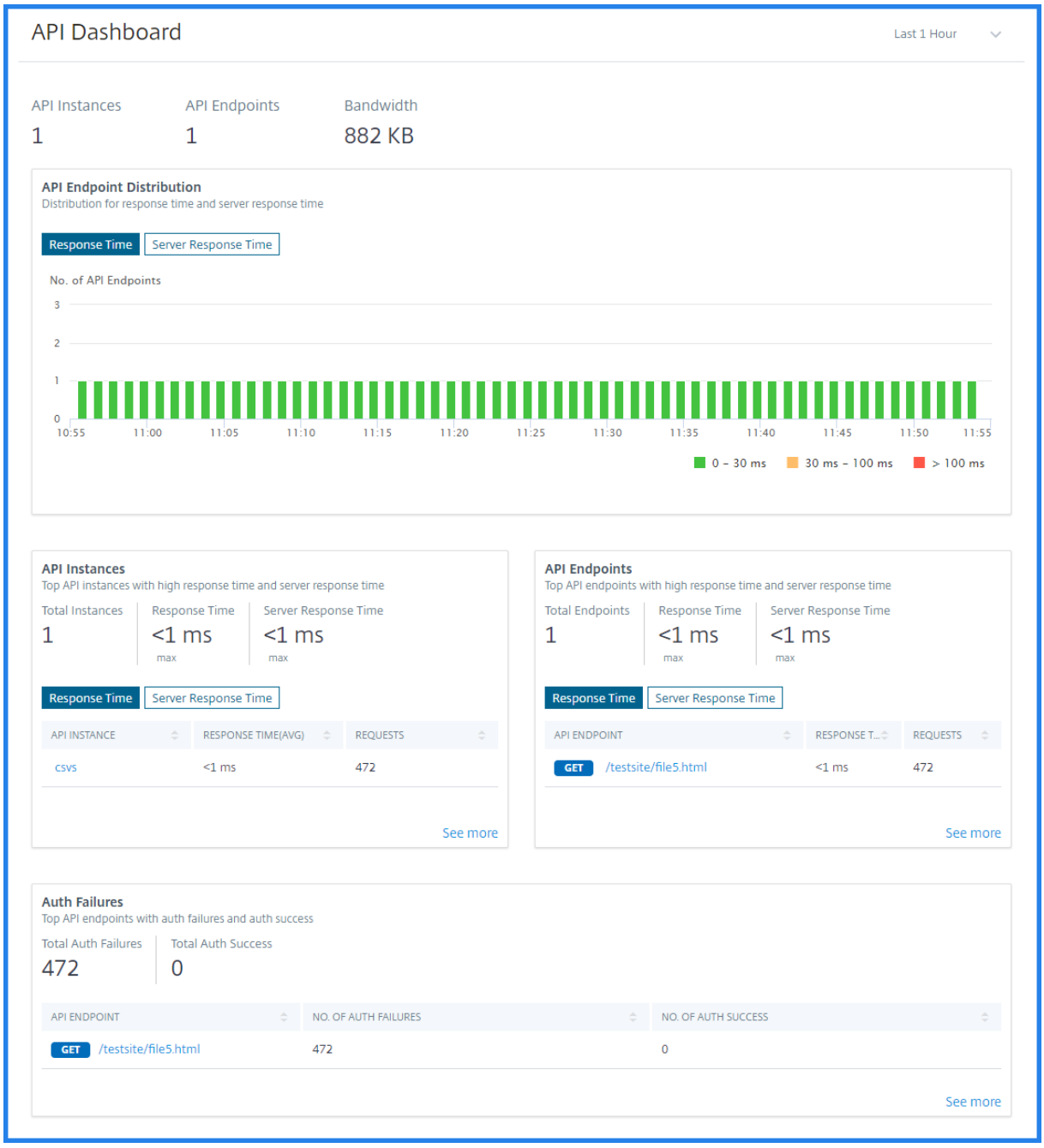
ユーザー定義の FQDN タイプを選択した場合は、アプリケーションを構成するためにドメインとゾーン名を指定する必要があります。詳しくは、「StyleBook を使用してアプリケーションを構成」を参照してください。

[NSADM-51494]

ADM で **API** インスタンスとエンドポイントを監視する

管理者は、Citrix Application Delivery Management（ADM）で API Gateway に API 定義を追加および展開できます。この機能を使用すると、ポリシーを追加して、着信 API 要求を認証するためのトラフィック選択基準を定義できます。
[**API** 分析] ページには、API インスタンスとエンドポイントの次のメトリックスが表示されます。

- API エンドポイントのアプリケーションとサーバーの応答時間の分布
- アプリケーションとサーバーの応答時間が長い API エンドポイント。
- より多くのリクエストと帯域幅を持つ API エンドポイント。
- エンドポイントが API リクエストを受信する場所。
- エンドポイントへの API リクエストの合計およびドロップされた API リクエストの傾向。
- HTTPS 応答ステータス。
- API エンドポイントの帯域幅の消費。
- API エンドポイントでの SSL エラーと使用状況。



詳しくは、「API 定義の管理」を参照してください。

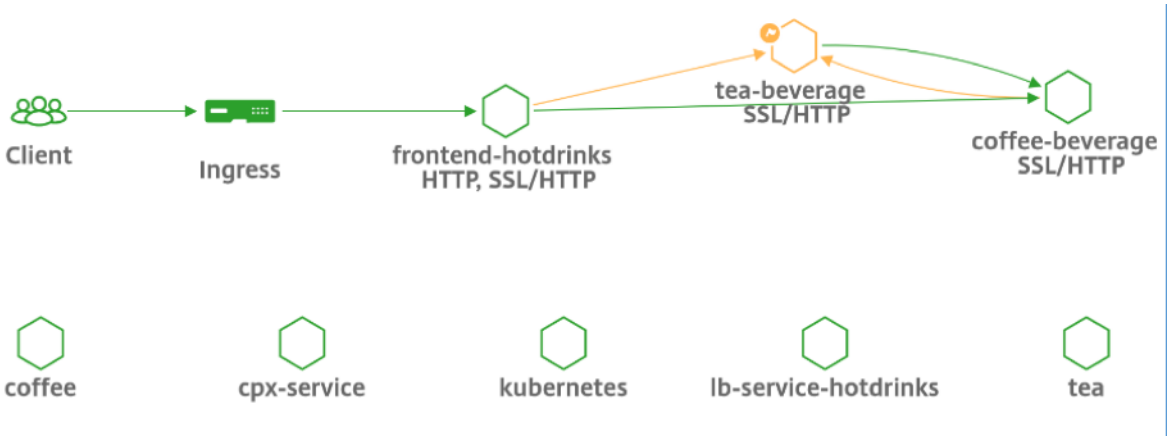
[NSADM-47869]

サービスグラフの改善

サービスグラフは、いくつかのテーマの変更で更新されます。また、いくつかのマイナーな UI 更新を体験できます。

- FAQ のリンク：部分的なデータ問題およびデータ問題のないサービスグラフに関するトラブルシューティングシナリオの詳細を表示します。

- ADC 処理時間メトリックの変化 — このメトリックは、1 ミリ秒未満ではなく、0 と表示されます。この変更は、ステータスが Out of Service または Down の ADC インスタンスにのみ適用されます。
- マイクロサービスアプリケーションを表す Hexagon — サービスグラフでは、マイクロサービスアプリケーションが六角形の記号で表示されます。



- ADC インスタンスの詳細の表示 — アプリケーションのサービスグラフ（アプリケーション **>** **[**アプリケーション名**]** **>** サービスグラフ）から ADC インスタンスをクリックします。このページには、インスタンススコア、主要メトリック、問題など、ADC インスタンスの詳細が表示されます。
- マイクロサービスアプリケーションを表示するグローバルサービスグラフ：マイクロサービスアプリケーションは、設定されたしきい値に基づいて表示されます。

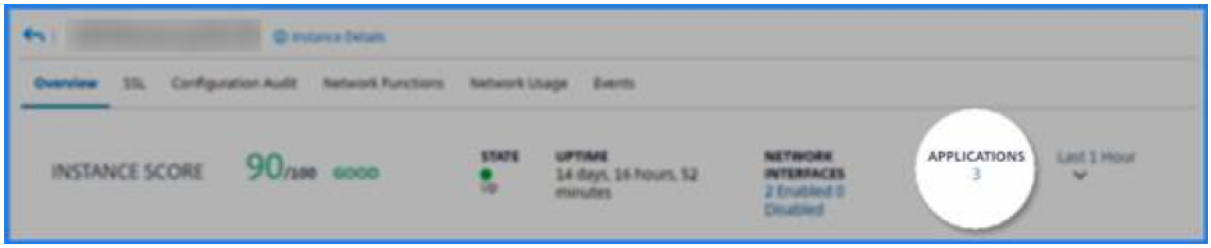
スコアに応じて、赤色（クリティカル）、オレンジ（レビュー）、緑（良好）でマイクロサービスアプリケーションを表示できます。

- 対応するサービスを表示する名前空間フィルタ — サービスグラフには、クライアントおよび入力とともに、対応するサービスが表示されます。

[NSADM-51973]

[インフラストラクチャ分析**]** ページからアプリケーションを表示する

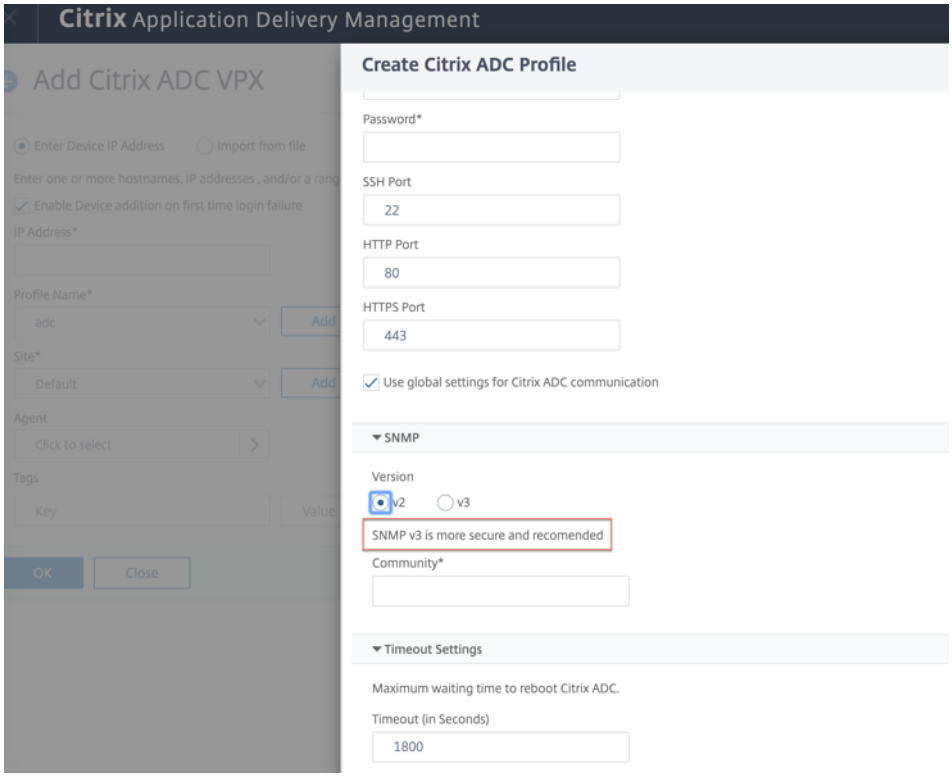
[インフラストラクチャ分析] ページでインスタンスを選択すると、インスタンスにデプロイされているアプリケーションの数を表示できます。[アプリケーション] リンクをクリックして、それらのアプリケーションを表示します。



[NSADM-43848]

SNMP V2 用の新しい **UI** テキスト

ADM GUI で ADC インスタンスを追加するときに、[**SNMP**] で [SNMP V2] を選択すると、次のメッセージが表示されます。「SNMP V3 はより安全で、推奨されます。」デフォルトでは、SNMP V3 が選択されています。

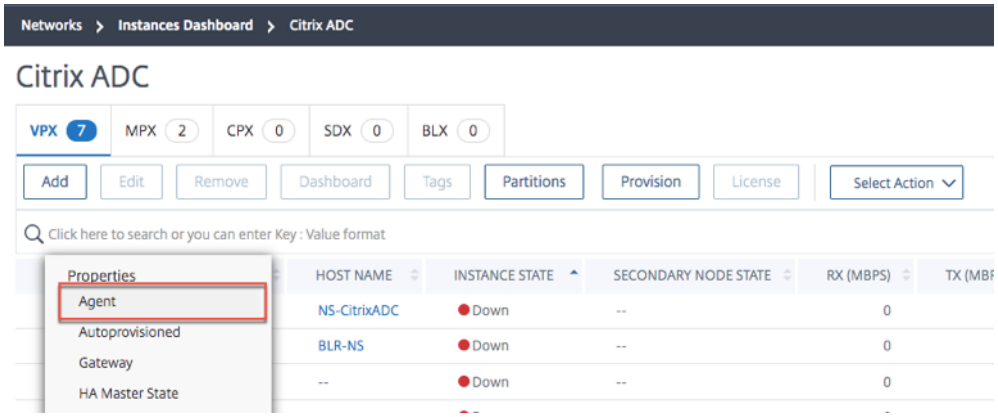


詳しくは、「インスタンスの追加」を参照してください。

[NSADM-51179]

エージェントを新しい検索プロパティとして追加

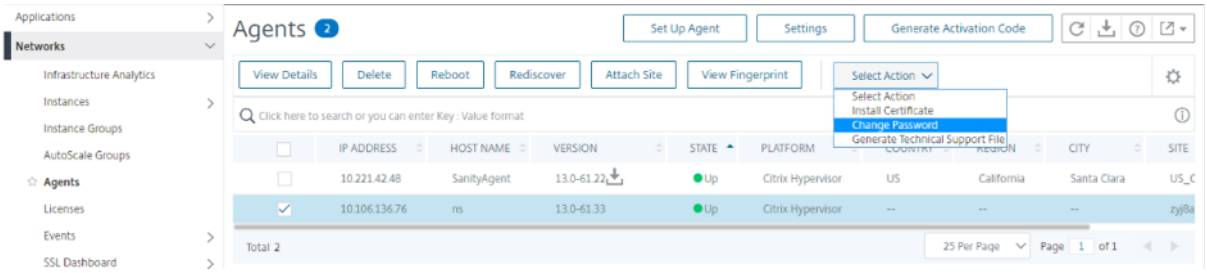
[ネットワーク] **>** [インスタンス] **>** [**Citrix ADC**] で、関連するエージェントでインスタンスを検索できるようになりました。検索アイコンをクリックし、[プロパティ**] > [**エージェント**]** を選択します。



詳しくは、「タグとプロパティの値を使用してインスタンスを検索する方法」を参照してください。
[NSADM-47424]

エージェントのデフォルトパスワードの変更

インフラストラクチャのセキュリティを確保するために、エージェントのデフォルトのパスワードを変更できるようになりました。
パスワードを変更するには、GUI から [ネットワーク] **>** [エージェント] に移動し、[アクションの選択] をクリックし、[パスワードの変更] を選択します。

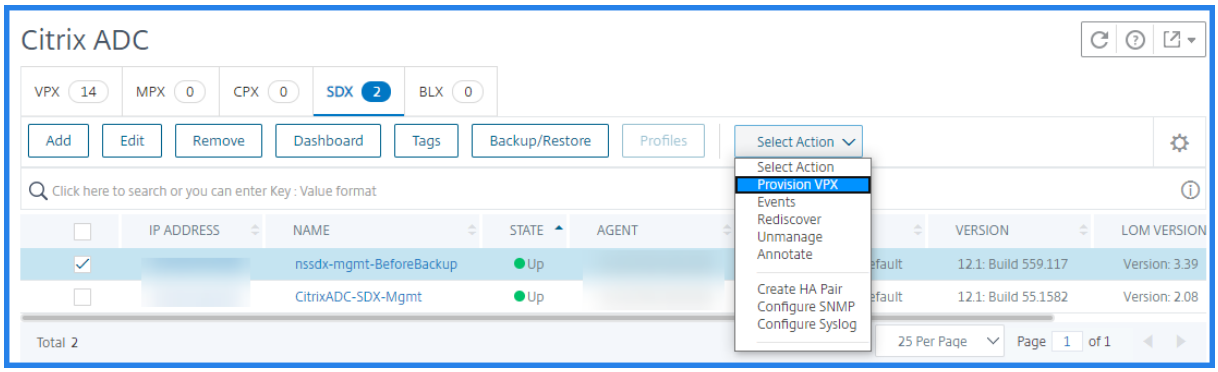


詳しくは、「はじめに」を参照してください。

[NSADM-47521]

ADM を使用して **SDX** で **ADC** インスタンスをプロビジョニングする

これで、ADM を使用して、SDX アプライアンス上に 1 つ以上の Citrix ADC インスタンスをプロビジョニングできます。ADM サービスは、SDX アプライアンスに Citrix ADC インスタンスを暗黙的にデプロイし、インスタンスの構成の詳細をダウンロードします。



詳しくは、「ADM を使用して SDX 上の ADC VPX インスタンスのプロビジョニング」を参照してください。

[NSADM-23845]

解決された問題

Analytics

Gateway Insight では、CSV 形式のエクスポートレポートが期待どおりに機能しません。

[NSHELP-22780]

GUI

お気に入りを保存メニューには、javascript エラーが表示されることがあります。

[NSADM-52856]

ライセンス

未処理のタイムアウト例外とデッドロック状態が原因で、プールされたライセンス機能が期待どおりに動作しません。

[NSHELP-22729]

2020 年 5 月 15 日

サービスグラフで部分的なデータまたはデータがないかの診断詳細の表示

必要なサービスグラフ構成を完了し、Citrix ADM で Kubernetes クラスターを追加すると、サービスグラフのデータ入力が開始されます。状況によっては、サービスグラフに部分的なデータが表示されているか、データが表示されないことがあります。サービスグラフに部分的なデータまたはデータがない理由のいくつかは、次のとおりです。

- スタティックルートが設定されていません
- Kubernetes クラスターのステータスが停止しています
- CPX 登録が失敗しました
- CPX 仮想サーバにはライセンスがありません
- サービスグラフがすべてのデータをロードできないように、必要な分析構成が設定されていません

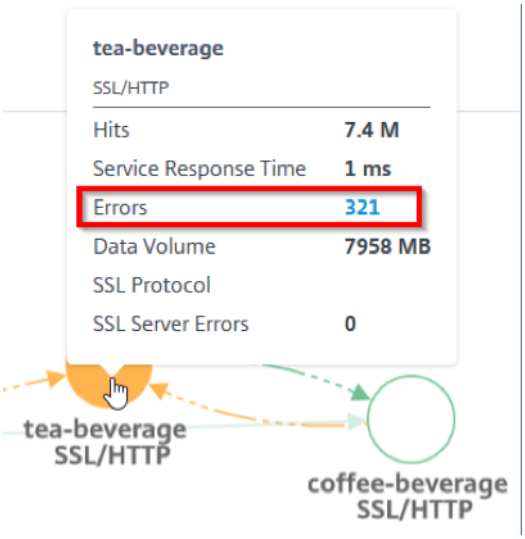
管理者として、サービスグラフ機能に部分的なデータが表示されているか、データが表示されていない場合に、その理由の分析が困難な場合があります。

サービスグラフページでは、データの一部またはデータの問題のない問題のトラブルシューティングに必要な理由と必要なアクションを確認できるようになりました。
詳細については、「診断の詳細を表示する」を参照してください。

[NSADM-47865]

サービスグラフでエラーを表示する簡略化されたプロセス

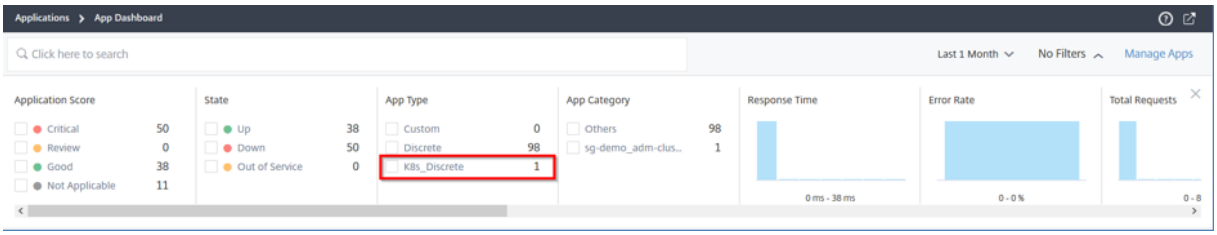
サービスグラフでは、HTTP および SSL エラーを表示するプロセスが簡略化されます。これで、誤ったサービスの上にマウスポインタを置いて、エラーカウントをクリックすることで、エラーの合計を表示できます。



[NSADM-47864]

アプリダッシュボードでマイクロサービスアプリケーションを表示する

アプリダッシュボードでは、Kubernetes クラスターの Citrix ADC CPX インスタンスから構成されたマイクロサービスアプリケーションの詳細を表示できます。アプリの種類フィルターには、新しい **K8S_Discrete** オプションがあり、フィルターを適用してマイクロサービスアプリケーションの詳細を表示できます。



詳しくは、「マイクロサービスアプリの詳細を表示する」を参照してください。

[NSADM-47863]

Citrix ADM での **WAF** 学習

Citrix Web App Firewall（WAF）は、SQL インジェクションやクロスサイトスクリプティングなどの悪意のある攻撃から Web アプリケーションを保護します。データ漏洩を防ぎ、適切なセキュリティ保護を提供するには、トラフィックを監視して、脅威や攻撃に関するリアルタイムの実用的なデータを監視する必要があります。報告された攻撃は偽陽性であり、それらの攻撃を例外として提供する必要がある場合があります。

Citrix ADM 学習エンジンは、WAF が Web アプリケーションの動作（通常のアクティビティ）を学習できるようにする反復パターンフィルターです。エンジンは、モニタリングに基づいて、HTTP トラフィックに適用されるセキュリティチェックごとに推奨されるルールまたは例外のリストを生成します。管理者は、Citrix ADM でこれらの違反リストを表示し、展開するかスキップするかを決定できます。

詳細については、「Citrix ADM での WAF 学習」を参照してください。

[NSADM-44341]

アプリのセキュリティ違反-地域ごとの過度な一意の **IP**

既存のアプリのセキュリティ違反とは別に、ボットカテゴリの一部として、地域ごとの過度な一意の **IP** を表示できるようになりました。[地域ごとの過大な **Unique IP**] インジケータを使用すると、特定の場所から Web アプリケーションへの訪問数を増やす不良ボットを分析およびブロックできます。
詳細については、「地域ごとのユニーク IP の過剰」を参照してください。

[NSADM-43982]

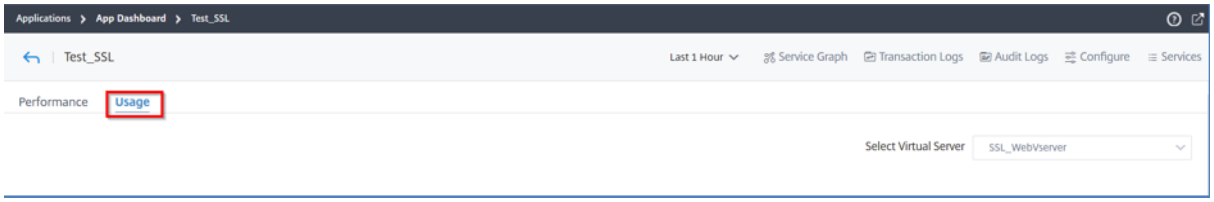
アプリケーション使用状況の分析

アプリケーション所有者は、パフォーマンスと使用の観点からアプリケーション全体を評価し、視覚化する能力を持っている必要があります。

即興の App Dashboard では、すべてのアプリケーションのパフォーマンスと使用状況指標をまとめて表示できます。既存のアプリケーション・パフォーマンス・メトリックとともに、アプリケーションをクリックすると、使用状況タブにメトリックの詳細が表示され、次のことができます。

- アプリケーションの使用状況を理解します。
- パフォーマンスの偏差と使用状況の指標を関連付けます。

アプリケーションに複数の仮想サーバーがある場合は、リストから仮想サーバーを選択します。



管理者として、アプリケーションダッシュボードを使用して、次のメトリックスの単一ペインビューを視覚化できます。

- クライアント
- サーバー
- 地理的位置
- URL
- HTTP 応答の状態
- オペレーティングシステム
- Web ブラウザー
- SSL エラー
- SSL の使用法

詳しくは、「アプリケーション使用状況の分析」を参照してください。

グローバルサービスグラフ**:** ユーザー、インフラストラクチャ、アプリケーションを包括的に視覚化

> 注**:**
>
> この機能はプレビューです。

グローバルサービスグラフ機能を使用すると、`clients to infrastructure to application`ビューの全体的な視覚化を取得できます。この単一ペインのサービスグラフビューでは、管理者として、次の操作を実行できます。

- ユーザーが特定のアプリケーション (3 層の Web アプリとマイクロサービスアプリ) にアクセスしているリージョンを理解する
- クライアント要求が処理されたというインフラストラクチャ（Citrix ADC インスタンス）ビューの視覚化
- 問題がクライアント、インフラストラクチャ、またはアプリケーションから発生しているかどうかを把握
- さらにドリルダウンして、問題のトラブルシューティングを行います。

「アプリケーション」**>**「サービスグラフ」**>**「グローバル・サービスグラフ」の順にナビゲートして、次のように表示します。

- クライアントからバックエンドサーバに接続されたすべてのアプリケーションのエンドツーエンドの詳細。
- 各データセンターに接続されているすべての Citrix ADC インスタンス。注: GSLB アプリがある場合にのみ、データセンターを表示できます。
- クライアントのメトリック情報。
- Citrix ADC メトリックス情報。
- 個別のアプリケーション、カスタムアプリケーション、および個別のマイクロサービスアプリケーションを持つすべての Citrix ADC インスタンス
- カスタムアプリ、個別アプリ、マイクロサービスアプリに属する上位 4 つの低スコアアプリケーション。
- 上位 4 つの低スコア仮想サーバのメトリック情報。
- クリティカル、レビュー、良い、適用できないなどのアプリケーション (個別のアプリ、カスタムアプリ、マイクロサービスアプリ) のステータス。

詳しくは、「サービスグラフ内のすべてのアプリケーションの全体的ビュー」を参照してください。

[NSADM-47425]

StyleBooks フィルターをカスタマイズしてユーザー認証を提供

管理者は、「アカウント」**>**「ユーザー管理」**>**「グループ」ページで、特定の **StyleBook** をユーザーに承認できます。カスタムフィルタクエリを使用して StyleBooks を検索できるようになりました。クエリは、キーと値のペアの文字列です。キーは次のとおりです。

- 名前
- 名前空間
- バージョン

次に例を示します:

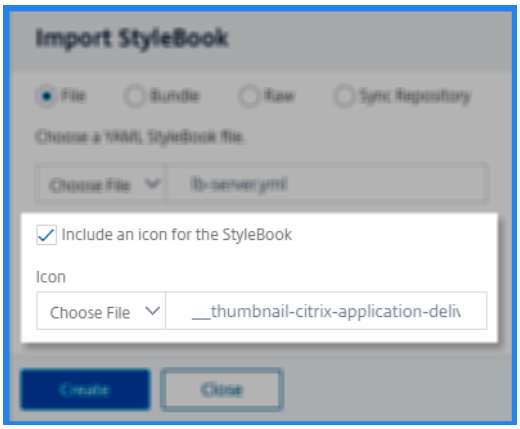
```
name=lb-mon OR namespace=com.citrix.adc.stylebooks OR version=1.0
```


検索結果には、指定されたキーと値のペアに基づいて StyleBooks が一覧表示されます。ADM は、指定されたクエリに基づいて、これらのスタイルブックへのユーザアクセスを提供します。詳細については、Citrix ADM でグループを構成するを参照してください。

[NSADM-49446]

StyleBook をアイコンでインポートする

StyleBook をインポートするときに、アイコンを追加できるようになりました。アプリケーション／ **StyleBook** では、インポートされた StyleBook にアイコンが表示されます。



詳しくは、「カスタム StyleBook をインポートする」を参照してください。

[NSADM-45810]

StyleBooks の新しい組み込み関数を使用する

StyleBook 定義の作成時に、ADM StyleBooks では次の組み込み関数がサポートされるようになりました。

- `startswith()` — 文字列が指定されたプレフィックスで始まるかどうかを調べます。詳細情報。
- `contains()` — 文字列に指定された部分文字列が含まれているかどうかを調べます。詳細情報。
- `endswith()` — 文字列が指定された接尾辞で終わるかどうかを調べます。もっと詳しく。](/en-us/citrix-application-delivery-management-service/stylebooks/stylebooks-grammar/built-in-functions.html #endswith)
- `substring()` — 文字列から部分文字列を抽出します。もっと詳しく。](/en-us/citrix-application-delivery-management-service/stylebooks/stylebooks-grammar/built-in-functions.html #substring)

[NSADM-45889]

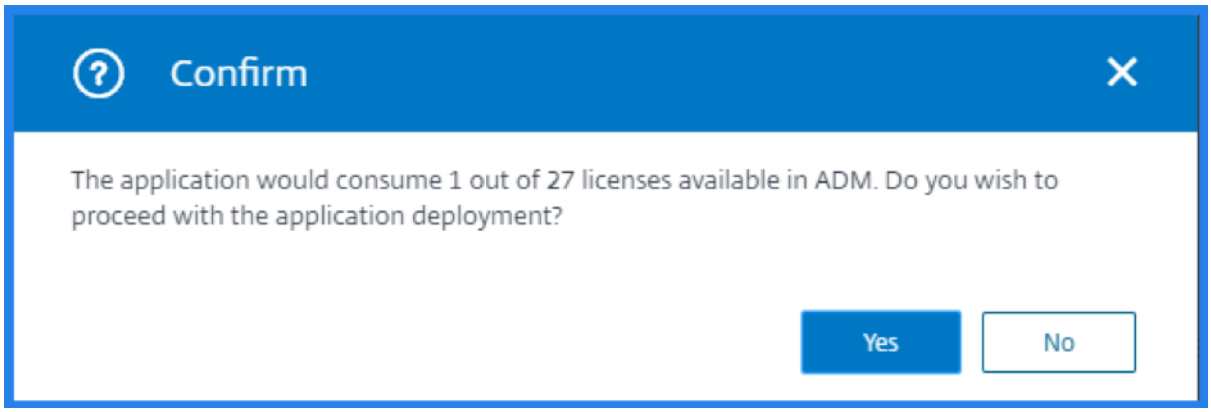
StyleBook 設定ビルダーは **ADC WAF** 機能をサポート

StyleBook 設定ビルダーは、ADC ソース構成の WAF 機能を認識し、サポートするようになりました。サポートされる ADC 機能の詳細については、StyleBooks 構成ビルダーを使用した Citrix ADC アプリケーション構成の移行を参照してください。

[NSADM-48941]

アプリケーションの展開前にライセンス使用を確認する

StyleBooks を使用してアプリケーションを作成する場合、アプリケーションをデプロイする前に、必要なライセンス使用量を確認できます。アプリケーションを作成する手順を完了すると、次のメッセージが表示されます。



確認メッセージが表示されたら、**[**はい] をクリックします。ADM は、必要なライセンスをアプリケーションに割り当てます。
以前は、StyleBooks を使用してアプリケーションを作成するには、自動ライセンス仮想サーバーオプションを有効にする必要がありました。これで、自動ライセンス仮想サーバーオプションが無効になっていても、アプリケーションを作成できます。

詳しくは、「StyleBook を使用してアプリケーションを作成する」を参照してください。

[NSADM-51306、NSADM-47184]

解決された問題

ネットワーク

負荷分散仮想サーバレポートを含むすべてのパフォーマンスレポートの CSV レポートをエクスポートすると、エクスポートされたレポートは空白で表示されます。

[NSHELP-22465]

[ネットワーク**] > [**構成監査**] > [**監査レポート] で、選択した ADC インスタンスに対して、次のアクションは機能しません。

- リビジョン履歴の相違

- アップグレード前対アップグレード後の差分
- 設定のダウンロード

[NSADM-51310]

アップグレードスクリプトのダウンロードに失敗し、「ファイルが見つかりません」というエラーメッセージが表示されます。この問題は、メンテナンスのアップグレードジョブが正常に完了した後、スクリプトをダウンロードするときに発生します。

[NSADM-48809]

Analytics

Citrix ADM GUI のアップロードとダウンロードトランザクションのインジケータが異常に大きい場合、分析データは期待どおりに表示されません。

NSADM-50930]

2020 年 4 月 28 日

アプリケーションのセキュリティ違反の詳細を表示する

既存のネットワーク違反とは別に、ボットカテゴリと WAF カテゴリの違反を表示できるようになりました。Citrix ADM で視覚化できる違反は次のとおりです。

ボット	WAF
過剰なクライアント接続	異常に高いアップロードトランザクション
アカウント乗っ取り	ダウンロードトランザクションが異常に高い
異常に高いアップロードボリューム	過度なユニーク IP
異常に高いリクエスト率	
ダウンロードボリュームが異常に高い	

詳しくは、「アプリケーションのセキュリティ違反の詳細を表示する」を参照してください。

[NSADM-40227]、[NSADM-43969]、[NSADM-43974]、[NSADM-43977]、[NSADM-43980]、[NSADM-43984]

ボット署名の更新に関するレポートを表示する

ボットインサイトで、以下の場合に [イベント履歴] でボット署名の更新を表示できるようになりました。

- 新しいボットシグネチャが Citrix ADC インスタンスに追加されます。
- 既存のボットシグネチャは、Citrix ADC インスタンスで更新されます。

[分析] **>** [セキュリティ] **>** [ボットインサイト] に移動し、[イベント履歴] で署名更新の概要を表示します。

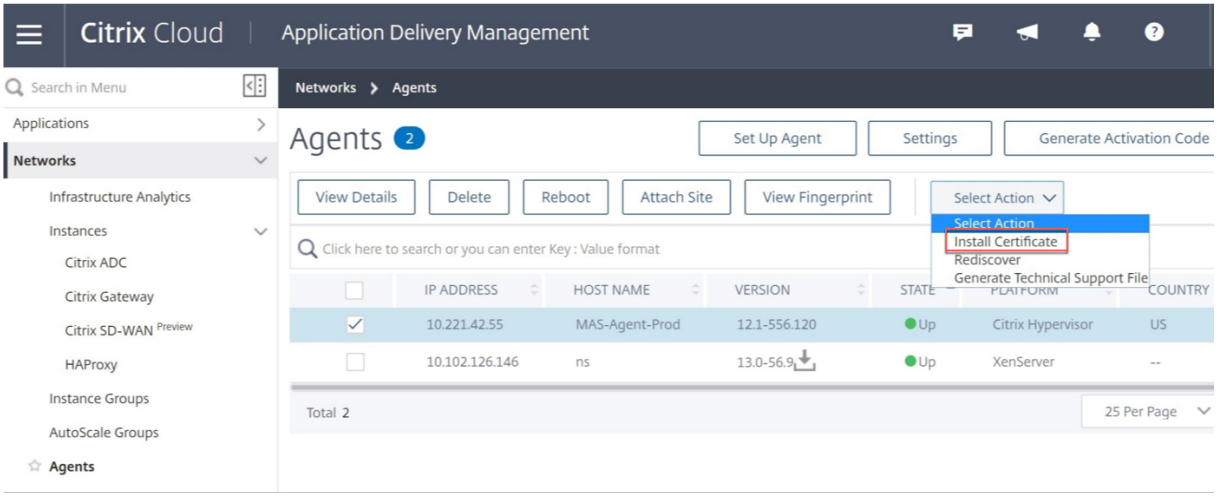
詳しくは、「ボットの洞察」を参照してください。

[NSADM-40228]

エージェント証明書をインストールする

セキュリティ要件を満たすために、ADM GUI を使用して証明書を ADM エージェントにアップロードできるようになりました。証明書をインストールするには、GUI から [ネットワーク] **>** [エージェント] に移動し、[アクションの選択] をクリックし、[証明書のインストール] を選択します。

詳しくは、「はじめに」を参照してください。



[NSADM-47904]

新しい形式で逐語型文字列を指定する

逐語的な文字列は、エスケープ文字 (\\ など) を使用せずに、元の形式で PI 式のような複雑な入力を受け取ることができます。

StyleBook 定義に PI 式を含めて、その形式を出力に保持するには、次の構文を使用して式を指定できます。

- 新しい構文:

```
~{
<pi-expression> }
~

Example:

~{
```



```
8   "HTTP.REQ.COOKIE.VALUE("jsessionid") ALT HTTP.REQ.URL.BEFORE_STR(
        "=").AFTER_STR(";jsessionid=") ALT HTTP.REQ.URL.AFTER_STR(";
        jsessionid=")" }
9   ~
10  <!--NeedCopy-->
```

- 古い構文:

```
1   “ <pi-expression>\” ”
2
3   Example:
4
5   ""HTTP.REQ.COOKIE.VALUE(\\"jsessionid\\") ALT HTTP.REQ.URL.
        BEFORE_STR(\\"=\\").AFTER_STR(\\";jsessionid=\\") ALT HTTP.REQ
        .URL.AFTER_STR(\\";jsessionid=\\")""
6
7   <!--NeedCopy-->
```

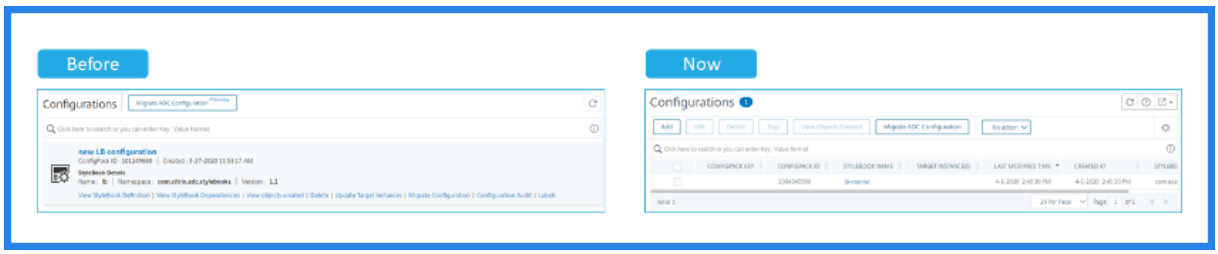
指定した PI 式は、出力内の形式を変更しません。

[NSADM-45888]

StyleBooks 設定**-**リストビュー

ADM GUI では、StyleBooks 設定がリストビューに表示されます。以前は、タイルビューで表示されていました。

この変更により、列ヘッダーで StyleBook 設定を並べ替えることができます。たとえば、構成を LAST MODIFIED TIME でソートできます。

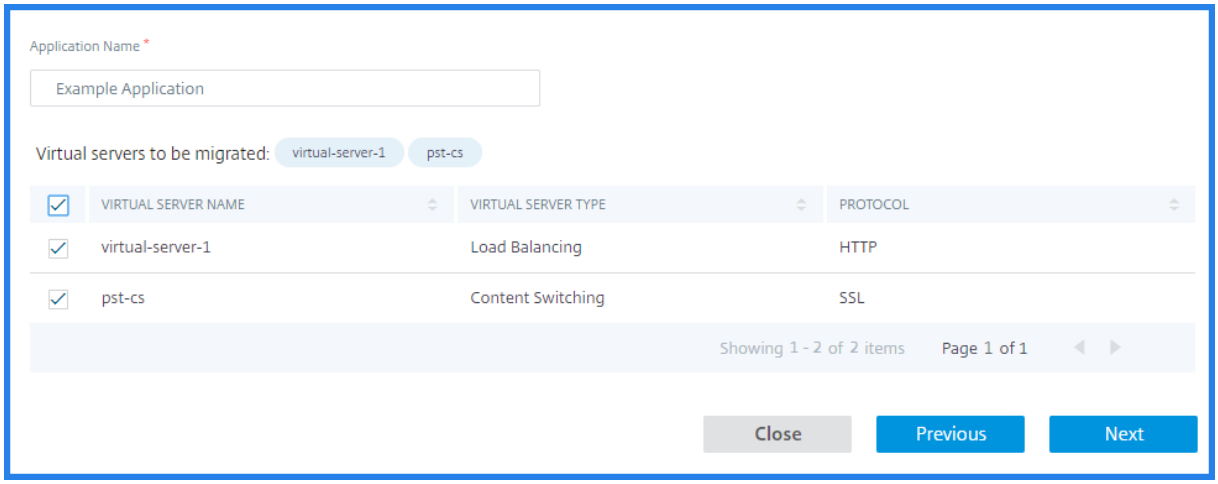


[NSADM-48918]

構成ビルダーを使用した複数の仮想サーバーの移行

StyleBooks 構成ビルダーで、構成ソースからターゲットインスタンスに移行する仮想サーバーを 1 つ以上選択できます。以前は、一度に移行する仮想サーバを 1 つだけ選択できました。

この機能を使用すると、アプリケーションを作成するために必要な仮想サーバーを選択し、ターゲットインスタンスに移行できます。



[NSADM-49602]

解決された問題

Analytics

- **Security Insight** では、タイムスライダーを使用すると、[アプリケーションの概要] が空白で表示されます。

[NSADM-50809]

アプリケーション

- アプリケーションダッシュボードからアプリケーションを選択すると、**[**キーメトリック**]** の下の **[** 応答時間**]** メトリックの値が正しくない形式で表示されます。

  [NSADM-50274]

- 次の場合、「アプリケーションの管理」ページは空白で表示されます。

  - カスタムアプリを削除するとします。[更新] ボタンをクリックした後にのみ、他のアプリが表示されます
  - 表示する行の数を変更します。
  - 複数のページが使用可能な場合は、次のページをクリックします

  [NSADM-50224]

- アプリケーションの Service Graph では、トランザクションが IPv6 のサーバーを介して発生した場合に、クライアントからサービスへのエンドツーエンドのトランザクションの詳細は入力されません。

  [NSADM-50201]

ネットワーク

- **[** 構成ジョブ**]** で、**[** 構成ソース**]** リストから **[** インスタンス**]** を選択し、**[** 実行構成**]** または **[** 保存された構成**]** オプションを選択すると、エラーメッセージ`Please provide Citrix ADC IP Address`が表示されます。

  [NSADM-50810]

- インデントの問題によりエージェント登録に失敗する

  [NSADM-50596]

- **Configuration Audit** では、レポートを CSV 形式でエクスポートすると、データは表示されません。複数のエクスポートを実行すると、Citrix ADM GUI がハングすることもあります。

  [NSADM-48322]

StyleBook

- StyleBook 依存関係のコンパイル中に誤ったエラーメッセージが表示される。

  [NSADM-50466]

インフラ

- Citrix ADM に表示される `mpsgroup`のアクティビティのログ情報。

  [NSHELP-22370]

2020 年 4 月 14 日

ADM での **IPAM** のサポート

ADM は、IP アドレス管理（IPAM）をサポートし、ADM 管理構成で IP アドレスを自動割り当ておよび解放します。次の IP プロバイダーを使用して定義されたネットワークまたは IP 範囲から IP を割り当てることができます。

- ADM 内蔵 IP アドレス管理プロバイダ。
- Infoblox IPAM ソリューション。詳しくは、「インフォブロックス DDI」を参照してください。

現在、ADM IPAM は次の用途で使用できます。

- **StyleBook**s：設定を作成するときに、IP を仮想サーバーに自動割り当てます。
- **Kubernetes** 入力: 仮想 IP アドレスを Kubernetes クラスタ内の入力設定に自動的に割り当てます。

また、ADM によって管理される各ネットワークまたは IP 範囲で、割り当てられた IP アドレスと使用可能な IP アドレスを追跡することもできます。詳しくは、「IPAM の設定」を参照してください。

[NSADM-48377]

AutoScale グループへの内部アプリケーションのデプロイ

AutoScale グループに内部アプリケーションと外部アプリケーションをデプロイして、ADM Auto Scaling ソリューションを使用できるようになりました。以前は、外部アプリケーションのみを展開できました。
Autoscale グループに内部アプリケーションをデプロイするには、AWS での AutoScale 設定およびAzure での AutoScale 構成を参照してください。

[NSADM-47520]

SSL ダッシュボードに追加された新しい列

SSL ダッシュボードの次のタブに新しい列が追加されます。

- [SSL 証明書] — [キー強度] 列が追加されます。[キー強度] の値を使用して SSL 証明書をフィルタリングできます。
- [SSL プロトコル] — [プロトコルタイプ] 列が追加されます。プロトコルタイプを使用して SSL プロトコルをフィルタリングできます。

[NSADM-42191]

アプリケーションのセキュリティ違反の詳細を表示する

インターネットにさらされている Web アプリケーションは、攻撃に対して非常に脆弱になっています。Citrix ADM を使用すると、アクション可能な違反の詳細を視覚化し、アプリケーションを攻撃から保護できます。単一ペインソリューションの [セキュリティ] **>** [セキュリティ違反] に移動し、次の操作を行います。

- 次のアプリケーション・セキュリティ違反にアクセスします。
  - HTTP スローロリス
  - DNS スローロリス
  - HTTP スローポスト
  - `NXDomain` フラッドアタック
- アプリケーションを保護するための是正措置を講じる

詳しくは、「アプリケーションのセキュリティ違反の詳細を表示する」を参照してください。

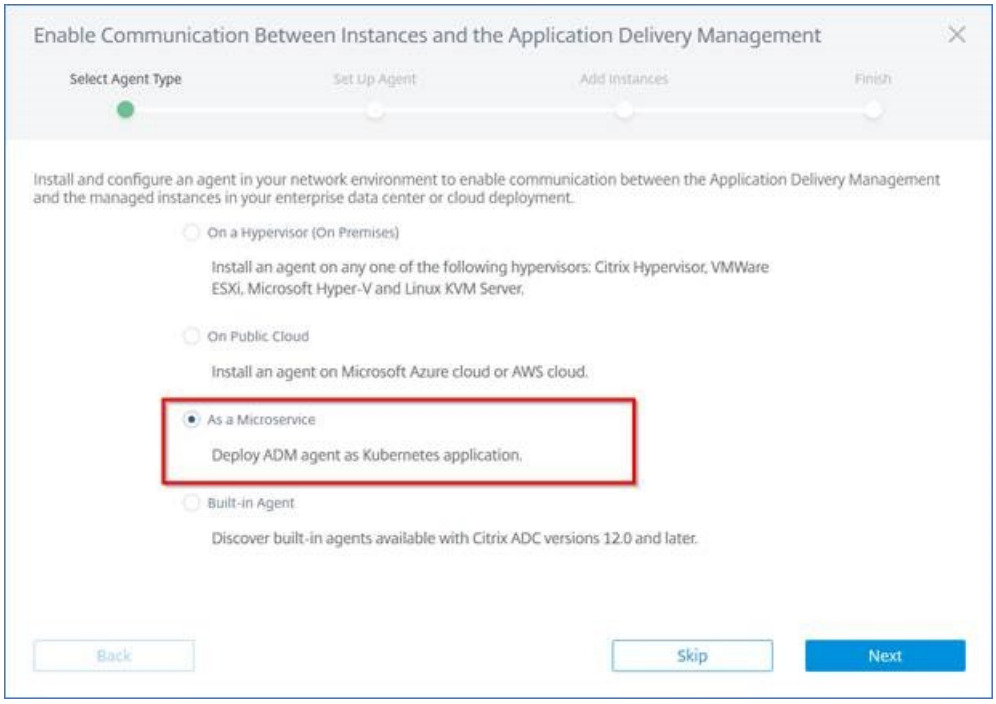
[NSADM-48069]

Citrix ADM エージェントをマイクロサービスとして展開する

これで、Kubernetes クラスターで Citrix ADM エージェントをマイクロサービスとして展開できます。Citrix ADM では、

1. [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] をクリックします。

2. [開始] をクリックし、[マイクロサービスとして] オプションを選択して、[次へ] をクリックします。



3. 次のパラメータを指定します。

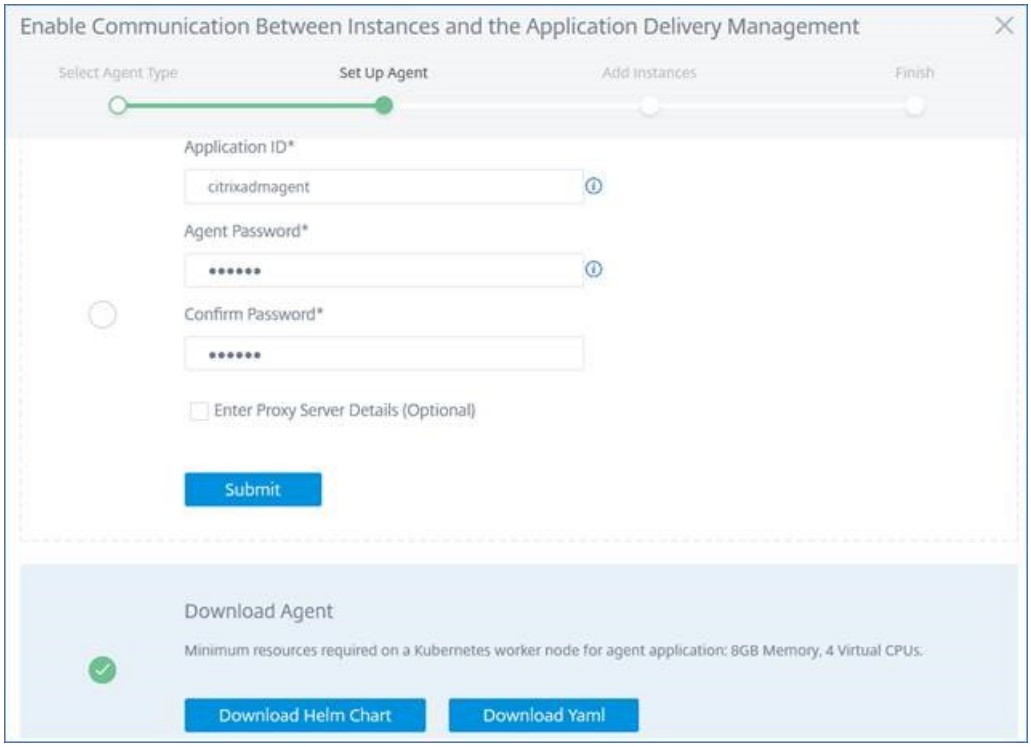
   a) アプリケーション **ID** — Kubernetes クラスタ内のエージェントのサービスを定義し、このエージェントを同じクラスタ内の他のエージェントと区別するための文字列 ID

   b) **Agent Password** — エージェント経由で CPX から ADM サービスへのオンボードにこのパスワードを使用するための CPX のパスワードを指定します。

   c)「パスワードの確認」— 確認のために同じパスワードを指定します

   d) [送信] をクリックします

4. [送信] をクリックすると、YAML または Helm チャートをダウンロードできます



5. Kubernetes マスターで、YAML ファイルを保存し、コマンド`kubectl create -f <yaml file>`

   詳しくは、「はじめに」を参照してください。

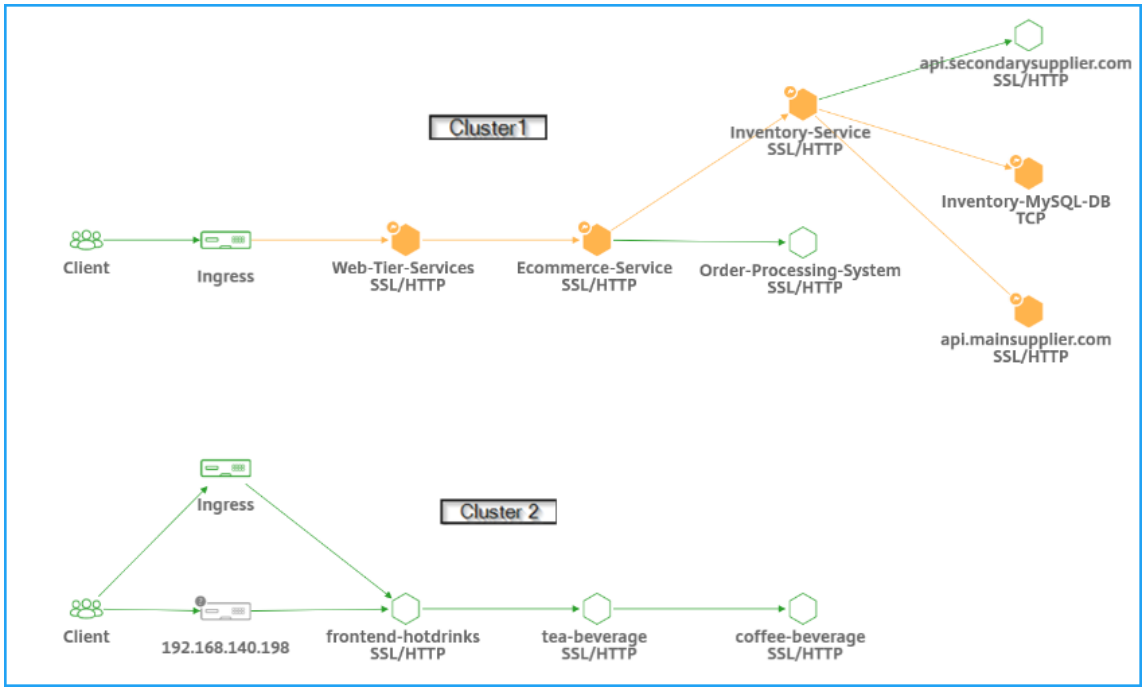
[NSADM-43971]

2020 年 3 月 31 日

サービスグラフで複数のクラスターとその他のフィルターを表示する

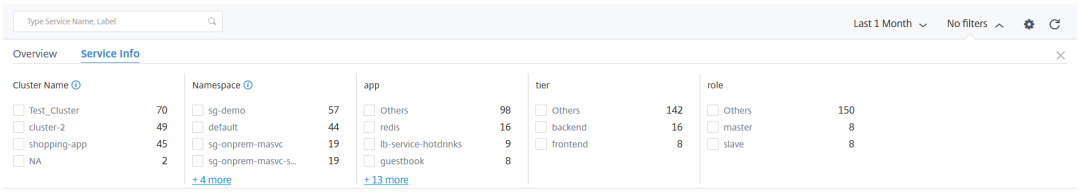
サービスグラフで、次の項目を表示できます。

- 各クラスターに関連付けられているサービス。



- フィルタの詳細:
  - [**Cluster**]: 選択した 1 つまたは複数のクラスタに適用可能なすべてのサービスが表示されます。
  - [**Namespace**]: 選択したネームスペースに適用可能なすべてのサービスが表示されます。

    > 注
    >
    > Kubernetes サービス定義 YAML のサービスに対して構成されたラベルによっては、さらに多くのフィルターオプションが表示される場合があります。



[NSADM-43985]

分散トレース

サービスグラフで、トレース情報を使用して次のことを行えます。

- サービス全体のパフォーマンスを分析する
- 選択したサービスとその相互依存サービス間の通信フローの視覚化
- エラーを示すサービスを特定し、エラーのあるサービスをトラブルシューティングする

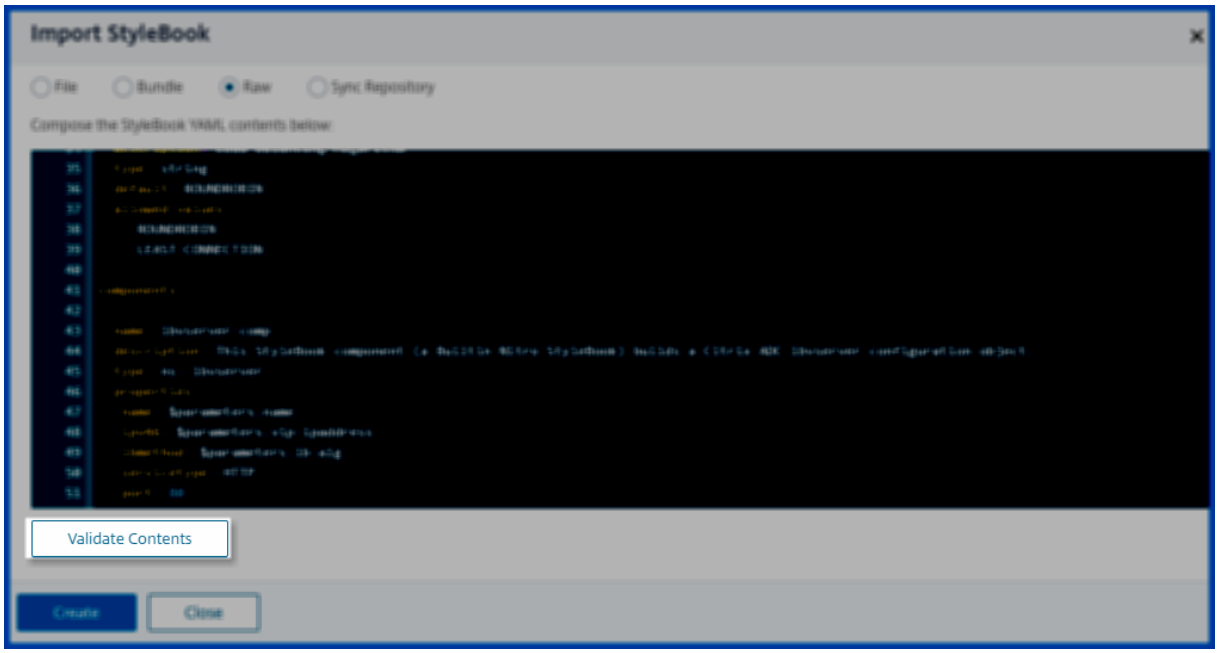
- 選択したサービスとその相互依存サービスの間のトランザクションの詳細を表示します。詳しくは、「分散トレース」を参照してください。

[NSADM-43976]

ADM にインポートする前に、**StyleBook** の内容を検証する

ADM YAML エディタで StyleBook を作成する場合、ADM にインポートせずに StyleBook 文法エラーをチェックできるようになりました。

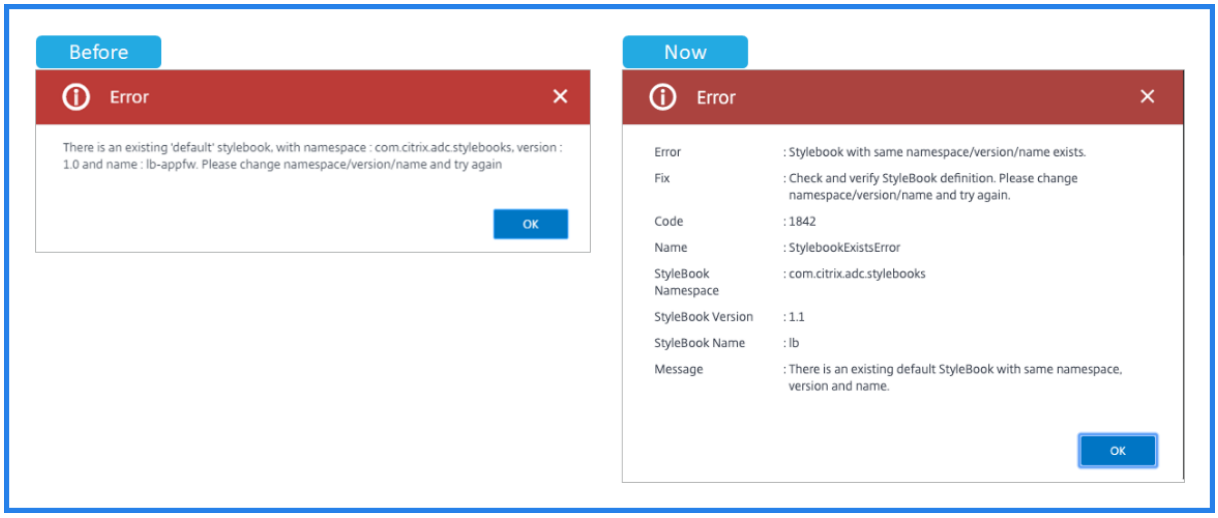
StyleBook のコンテンツにエラーがある場合は、ADM GUI にエラーの詳細が表示されます。表示されたエラーを修正し、StyleBook の編集またはインポートを続行できます。



[NSADM-47978]

StyleBooks エラーメッセージ表示の改善

StyleBook 文法エラーのある StyleBook をインポートすると、ADM GUI にエラーメッセージが表示されます。一部のエラーメッセージは、エラーの詳細を表示するように整理されています。エラーの詳細には、エラーの種類に応じて、エラー、修正、コード、名前などがあります。[修正] フィールドには、問題を解決するための情報が表示されます。



[NSADM-44274]

GitHub リポジトリ内の任意のフォルダから **StyleBook** をインポートする

GitHub リポジトリ内の任意のフォルダから、StyleBook ファイルを ADM に同期できるようになりました。以前は、**GitHub** リポジトリのルートフォルダにある **StyleBook** ファイルのみをインポートまたは同期することができました。

詳しくは、「GitHub リポジトリからのスタイルブックのインポートと同期」を参照してください。

[NSADM-46147]

構成パックに対する **ADC** 構成の監査

StyleBooks> Configuration で、**StyleBook** 設定パックによる変更を現在の **ADC** 構成と明示的に比較できるようになりました。この機能では、以下を実行できます:

- StyleBook 構成パックと ADC 構成間の構成ドリフトを検出します。
- ADC 上で変更または削除されたオブジェクトで、構成パックによって加えられた変更を反映していないオブジェクトを特定します。

構成パックの変更を ADC 設定と比較するには、目的の構成パックで [**Configuration Audit**] をクリックします。

詳しくは、「構成パックに対する ADC 構成の監査」を参照してください。

[NSADM-45866]

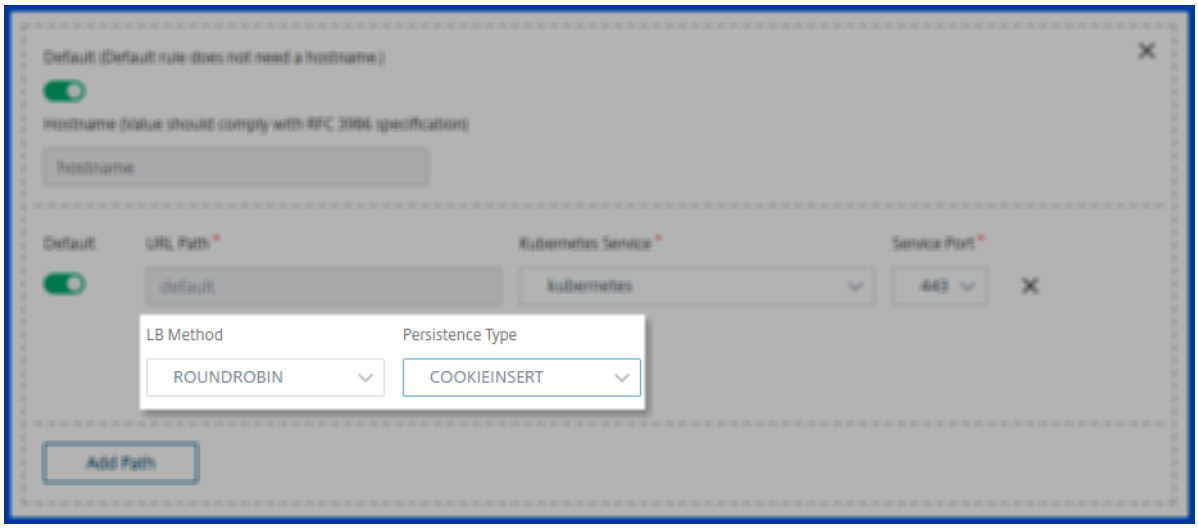
入力構成を展開するための **Citrix** 注釈のサポート

入力構成にコンテンツルーティングルールを追加するときに、ADM GUI に次の Citrix 注釈を含めることができるようになりました。

- 「**LB** メソッド」— 選択した Kubernetes サービスの優先負荷分散方式を選択します。
- 「永続タイプ」— 選択した Kubernetes サービスに対して優先する負荷分散永続性タイプを選択します。

コンテンツルーティングルールを追加したら、選択した LB メソッドと永続タイプを Ingress 仕様で表示できます。入力設定を確認して展開します。

詳しくは、「入力構成の展開」を参照してください。



[NSADM-48414]

インスタンスは、デプロイタイプを表記で示します

ADM GUI では、インスタンスの IP アドレスがデプロイの種類を示すようになりました。次の表記では、展開の種類について説明します。

- 高可用性ペアでは、P — プライマリサーバと S — セカンダリサーバ。
- C クラスタ
- A-Autosale グループ

インスタンスに表記がない場合は、スタンドアロンのデプロイを示します。

[NSADM-41859]

2020 年 **3** 月 **03** 日

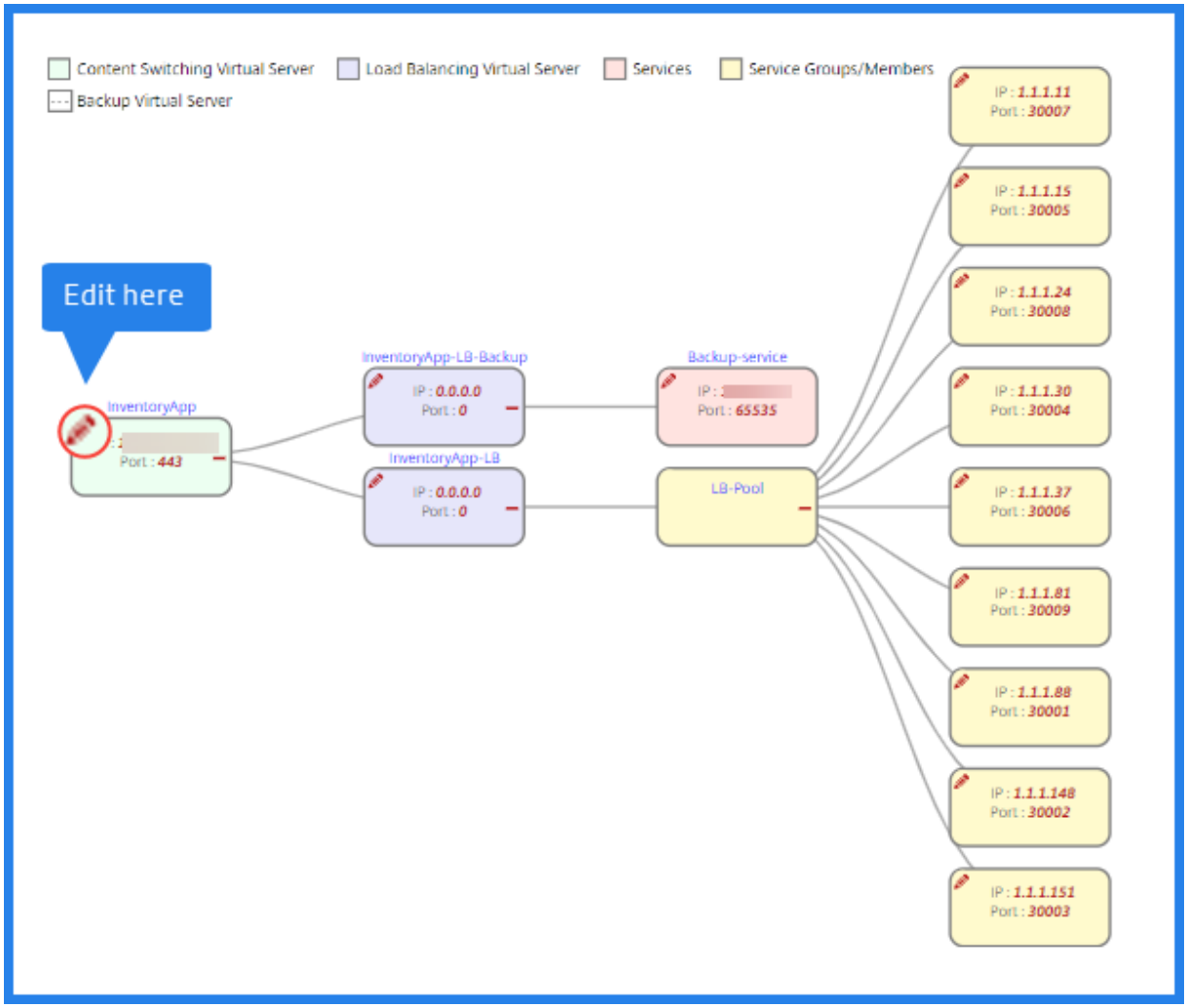
StyleBooks 構成ビルダーでの配置属性の編集

> 注:
>
> この機能はプレビューです。

StyleBooks 構成ビルダーを使用すると、既存の ADC 構成からアプリケーション構成 StyleBook と設定パックを作成できます。また、構成ビルダーは、ある ADC インスタンスから別のインスタンスへのアプリケーション構成の移行も自動化します。

構成ビルダーウィザードでは、StyleBook および構成パックを作成する前に、選択したアプリケーションのデプロイ属性を編集できるようになりました。これで、元の設定で、仮想サーバ、サービス、およびサービスグループメンバーの IP アドレスとポート値を編集できます。

アプリケーションの作成と移行が完了すると、対応する StyleBook とともに Citrix ADM で ConfigPack が作成されます。この構成パックには、新しい IP アドレスとポートの値があります。作成された ConfigPack を表示するには、[アプリケーション] **> [StyleBooks] > [**構成] に移動します。



詳しくは、「StyleBooks 構成ビルダーを使用して ADC アプリケーション構成を移行する」を参照してください。

[NSADM-44197]

すべてのアプリケーションを表示できるが、アプリケーションのサブセットのみを編集可能

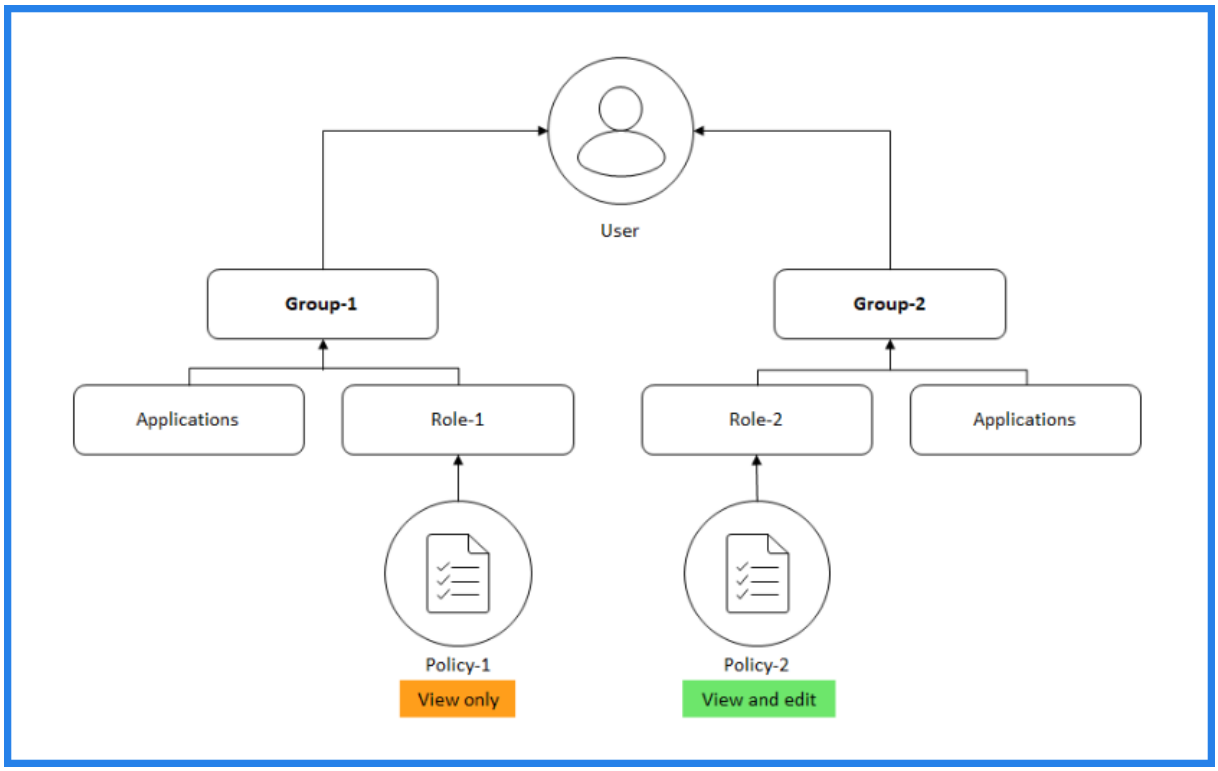
管理者が異なるアクセスポリシー設定を持つグループにユーザーを追加すると、そのユーザーは複数の承認スコープとアクセスポリシーにマップされます。

この場合、ADM は、特定の認可スコープに応じて、アプリケーションへのアクセスをユーザーに許可します。

ポリシー 1 とポリシー 2 の 2 つのポリシーを持つグループに割り当てられているユーザを考えてみましょう。

- Policy-1： アプリケーションに対する権限のみを表示します。
- ポリシー 2： アプリケーションに対する表示および編集権限。

これで、ユーザーは Policy-1 で指定されたアプリケーションを表示できます。また、このユーザーは、Policy-2 で指定されたアプリケーションを表示および編集できます。Group-1 アプリケーションに対する編集アクセスは、Group-1 認可スコープにはないため、制限されます。



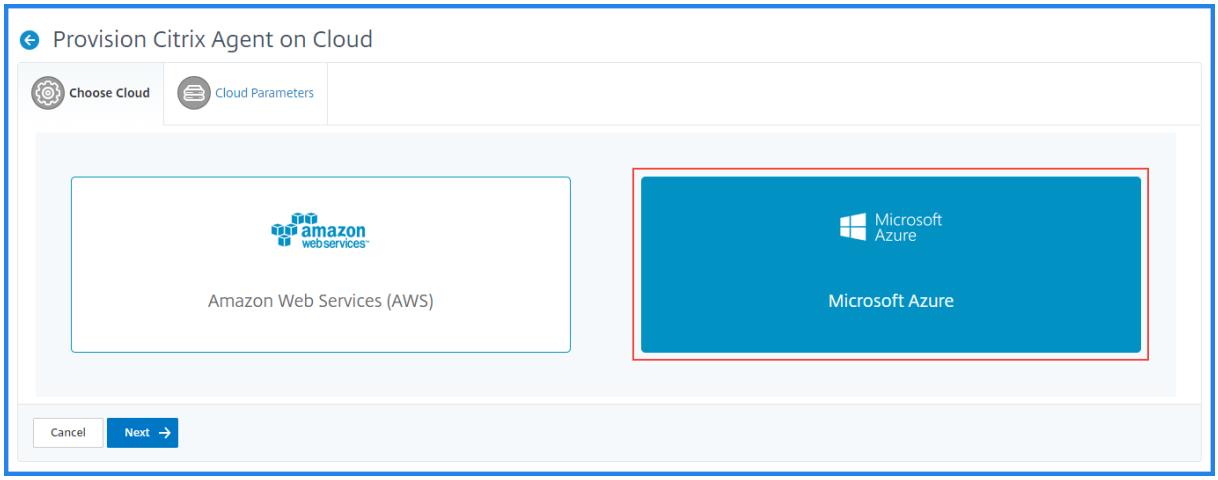
以前は、ADM はすべてのグループ権限の結合を考慮して、ユーザーを承認しました。上記の例に基づいて、ユーザーはグループ 1 とグループ 2 のすべてのアプリケーションを表示および編集することができました。このアクセス許可により、ユーザーはアクセスポリシーによって主に許可されていないリソースを編集することができました。

詳しくは、「承認スコープに基づくユーザーアクセスの変更方法」を参照してください。

[NSHELP-5854]

Azure で **Citrix ADM** エージェントをプロビジョニングする

ADM GUI を使用して Azure で ADM エージェントをプロビジョニングできるようになりました。Azure の ADM エージェントは Citrix ADM に自動的に登録されます。登録済みエージェントは **[ネットワーク] > [エージェント]** ページに表示されます。Azure で ADM エージェントをプロビジョニングする方法については、Azure で Citrix ADM エージェントをプロビジョニングするを参照してください。

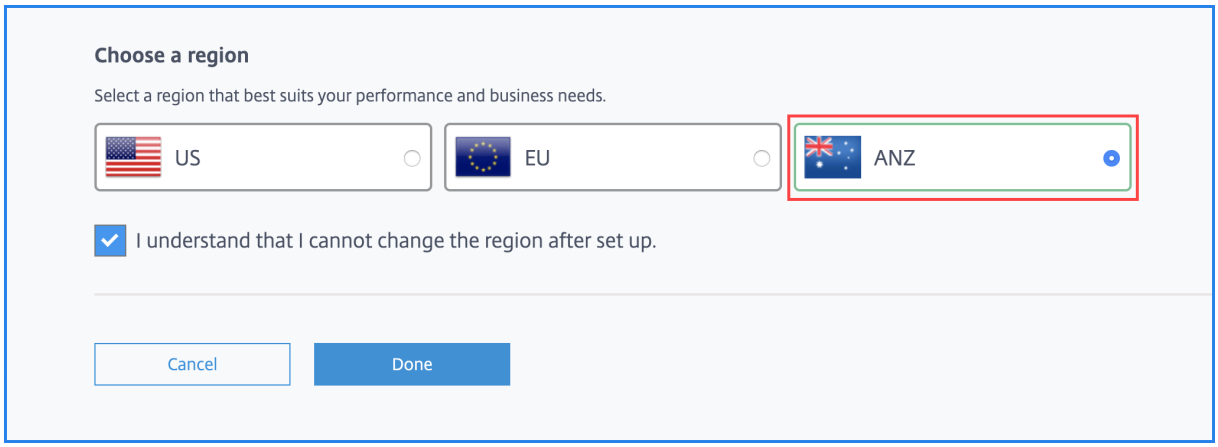


または、Azure マーケットプレイスから Citrix ADM エージェントをインストールすることもできます。詳しくは、「Azure への Citrix ADM エージェントのインストール」を参照してください。

オーストラリアリージョンを選択して **ADM** サービスをセットアップします

これで、オーストラリア (ANZ) リージョンを選択して ADM サービスをセットアップできます。Citrix ADM では、次のリージョンがサポートされるようになりました。

- 米国（米国）
- ヨーロッパ (EU)
- オーストラリア（ANZ）



詳しくは、「はじめに」を参照してください。

[NSADM-44447]

アップグレードメンテナンスジョブの前後にカスタムスクリプトを実行する

メンテナンス・ジョブを作成して ADC インスタンスをアップグレードすると、ADM はアップグレードするインスタンスに対して事前検証チェックを実行します。[アップグレード前の検証] タブでは、選択したインスタンスで次の項目がチェックされます。

- カスタマイズをチェックします。
- ディスクの使用状況をチェックし、ディスク容量が少ない場合はエラーを表示します。
- ディスクハードウェアの問題がないか確認します。

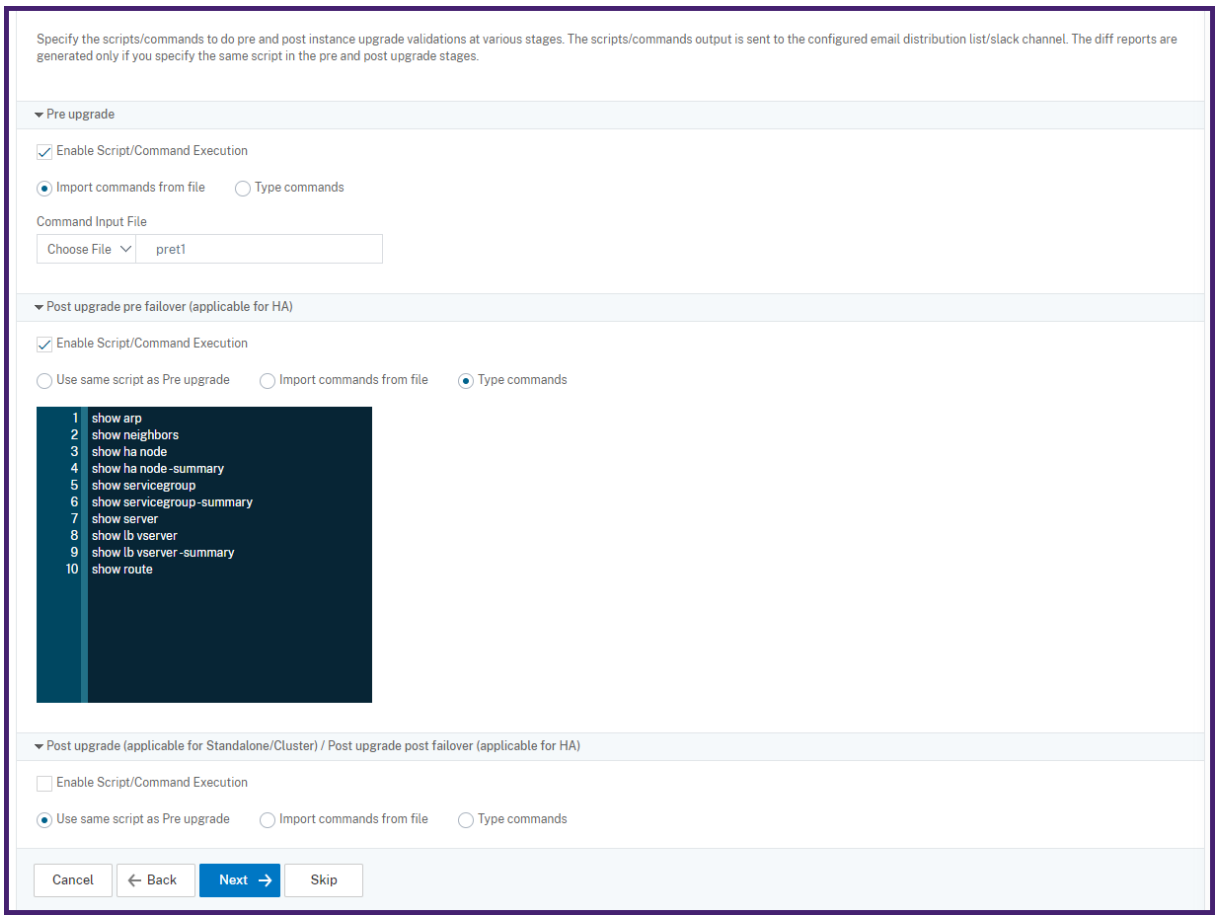
失敗したインスタンスを削除し、アップグレードメンテナンスジョブの作成に進むことができます。

[カスタムスクリプト] で、インスタンスのアップグレードの前後に実行するカスタムスクリプトを指定します。次のコマンドを実行するには、次のいずれかの方法を使用します。

- ファイルからコマンドをインポートします。
- Citrix ADM GUI でコマンドを直接入力します。

これらのスクリプトは、アップグレード前とアップグレード後の変更を確認するのに役立ちます。例:

- アップグレード前とアップグレード後のインスタンスのバージョン。
- アップグレード前後のインターフェイス、高可用性ノード、仮想サーバ、およびサービスのステータス。
- 仮想サーバーとサービスの統計。
- ダイナミックルート。



詳しくは、「ジョブを使用して Citrix ADC インスタンスをアップグレードする」を参照してください。

[NSADM-40534]

ジョブ実行中にアップグレードイメージをインスタンスにアップロードする

アップグレードメンテナンスジョブをスケジュールする場合は、アップグレードイメージを ADC インスタンスにアップロードするタイミングを決定できます。「ジョブの作成」で、次のいずれかを選択します。

- **Upload Now** — このオプションは、イメージをすぐにインスタンスにアップロードします。
- **[** 実行時にアップロード] — このオプションは、ADM がスケジュールされたアップグレード保守ジョブを実行したときに、イメージを ADC インスタンスにアップロードします。

詳しくは、「Citrix ADC インスタンスのアップグレードをスケジュールする」を参照してください。

[NSADM-44855]

ADM オートスケールグループは、**C5**、**M5**、および **C5n** の **AWS** インスタンスタイプをサポートします

AWS クラウドで ADM AutoScale グループを作成する場合、C5、M5、および C5n AWS インスタンスタイプで ADC インスタンスをプロビジョニングできるようになりました。これらのインスタンスタイプを選択すると、高パフ

ォーマンスの ADM 自動スケーリングを実現できます。

> 注:
>
> ADM GUI では、選択した ADC バージョンの推奨 AWS インスタンスタイプが自動的に入力されます。Autoscale グループの作成を参照してください。

AWS インスタンスタイプの詳細については、AWS インスタンスタイプを参照してください。

[NSADM-40089]

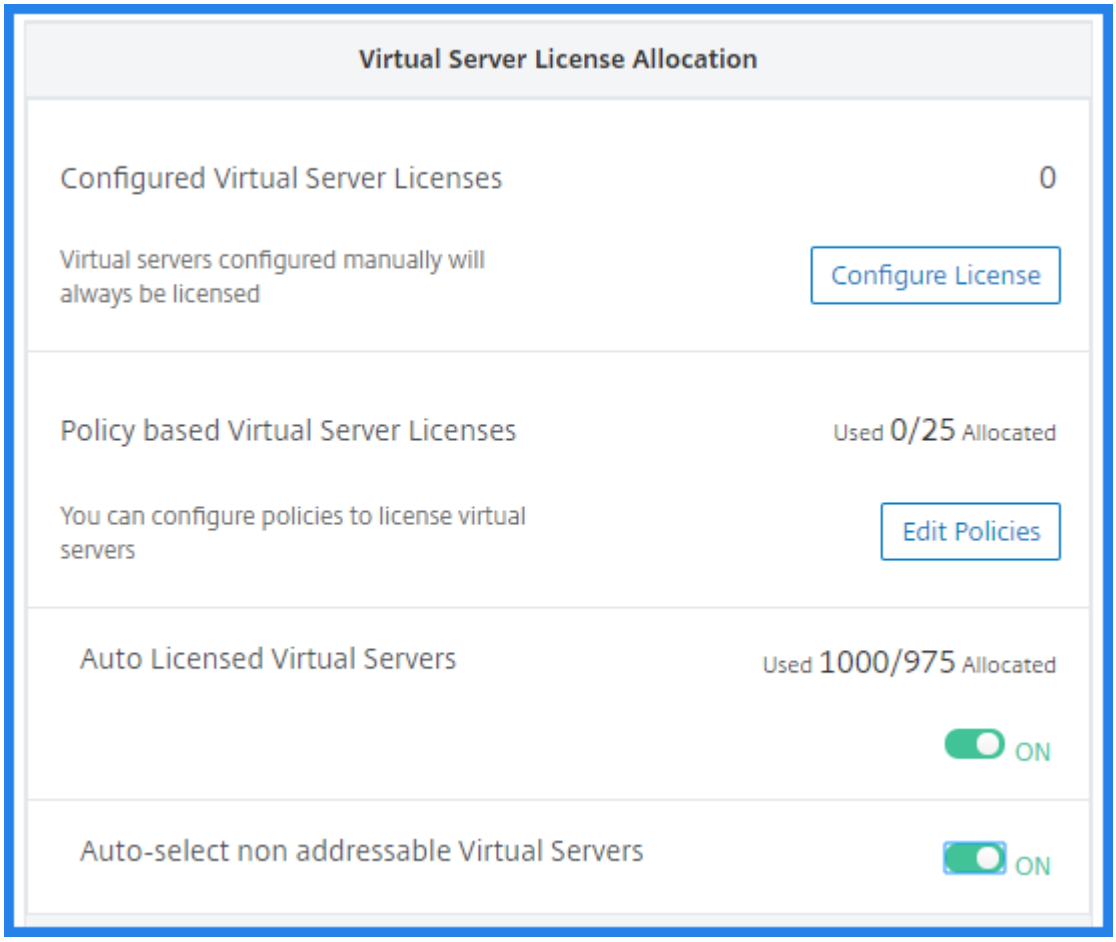
ポリシーを使用した仮想サーバへのライセンスの適用

[サブスクリプション] で、仮想サーバーにライセンスを適用するポリシーを構成できるようになりました。以前は、手動または自動のどちらかの仮想サーバにのみライセンスを適用できました。これで、ポリシーを使用するか、手動または自動を使用してライセンスを適用できます。

ポリシーを使用すると、自動ライセンスを取得する仮想サーバの数を制御できます。また、選択したインスタンスの仮想サーバーにのみライセンスを適用します。

ポリシーを編集するときは、次の項目を指定できます。

- CPX インスタンスに仮想サーバーの制限を個別に設定して、ライセンスを適用します。ADM は、指定された制限まで CPX インスタンス上の仮想サーバーにライセンスを適用します。
- ライセンスを適用するために、選択した ADC インスタンス（MPX/VPX/BLX）に仮想サーバーの制限を設定します。ADM は、指定された制限まで ADC インスタンス上の仮想サーバーにライセンスを適用します。
- 仮想サーバライセンスを適用する優先順位 ADC インスタンスを選択します。したがって、ADM は、選択したインスタンスの仮想サーバーにのみライセンスを適用できます。



[自動ライセンス仮想サーバー] および [アドレス指定できない仮想サーバーの自動選択] オプションは独立しています。以前は、自動ライセンス仮想サーバーを有効にする場合にのみ、アドレス指定できない仮想サーバーの自動選択を有効にできました。

[NSADM-35724]

ADM での **ADC** 容量の問題を表示

ADC インスタンスが使用可能な容量の大半を消費した場合、クライアントトラフィックの処理中にパケット廃棄が発生することがあります。この問題は、ADC インスタンスのパフォーマンスが低下します。このような ADC 容量の問題を理解することで、より多くのライセンスをプロアクティブに割り当て、ADC のパフォーマンスを安定させることができます。

ADC の容量に関する問題を確認するには、

1. [ネットワーク**] > [**インフラストラクチャ分析] に移動します。
2. 容量の問題を表示するインスタンスを展開します。

ADM は、ADC インスタンスから 5 分ごとにこれらのイベントをポーリングし、パケットドロップまたはレート制限カウンタが存在する場合は、その増加を表示します。問題は、次のキャパシティパラメータに分類されます。

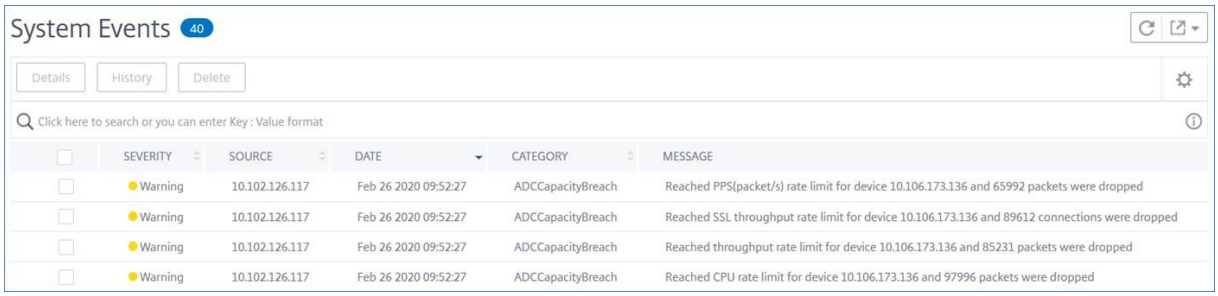
- スループット制限に達しました — スループット制限に達した後、インスタンスでドロップされたパケット数。
- **PE CPU** 制限に達しました -PE CPU 制限に達した後、すべての NIC でドロップされたパケット数。
- **PPS** 制限に達しました — PPS 制限に達した後にインスタンスでドロップされたパケット数。
- **SSL** スループットレート制限 — SSL スループット制限に達した回数。
- **SSL TPS** レート制限 — SSL TPS 制限に達した回数。

ADM は、定義されたキャパシティしきい値に基づいてインスタンススコアを計算します。

- 低しきい値：1 パケットドロップまたはレート制限カウンタ増分
- 高しきい値：10000 パケットのドロップまたはレート制限カウンタ増分

したがって、ADC インスタンスが容量のしきい値に違反すると、インスタンスのスコアが影響を受けます。

パケットがドロップまたはレート制限カウンタが増加すると、`ADCCapacityBreach` カテゴリの下にイベントが生成されます。これらのイベントを表示するには、「アカウント」**>**「システム・イベント」に移動します。



選択した期間（時間/日/週/月）の ADC レート制限統計を表示するには、**[**ネットワーク**] > [**ネットワークレポート] に移動します。

[NSADM-40183]

サービスグラフでのサービスの詳細の表示

[Service Graph] で、サービスの上にマウスポインタを置き、サービスをクリックして、次のオプションを表示します。

- 詳細の表示
- トランザクション・ログ：HTTP および SSL over HTTP トランザクションの詳細を表示できます。詳細については、「Web トランザクションログを表示する」を参照してください。

「詳細の表示」オプションを使用すると、次の項目を表示できます。

- サービスがホストされているクラスター名
- サービスの名前空間とサービスラベル
- 選択したサービスに接続されているすべての関連付けられた着信および発信サービス

- ヒット、サービス・レスポンス時間、**HTTP** エラー、データ・ボリューム、**SSL** フロントエンド・エラー、**SSL** バックエンド・エラー、**TCP** フロントエンド・エラー、**TCP** バックエンド・エラーなどのグラフ形式のサービス・キー・メトリック

これらの主要なメトリックの傾向を使用して、選択した期間におけるサービスのパフォーマンスを分析できます。

詳しくは、「サービス詳細の表示」を参照してください。

[NSADM-41297]

アプリケーションのサービスグラフの表示 **(GSLB)**

> 注
>
> この機能はプレビュー中です。

サービスグラフで GSLB アプリケーションを表示して、次の項目を表示できます。

- アプリケーションの構成方法（GSLB アプリケーション、データセンター、ADC インスタンス、CS、および LB 仮想サーバを使用）
- クライアントからサービスまでのエンド・ツー・エンドのビュー
- クライアント要求が処理されるデータセンターの名前と、関連するデータセンター Citrix ADC メトリック
- GSLB 仮想サーバのステータス（クリティカル、レビュー、良好）。Citrix ADM は、アプリのスコアに基づいて仮想サーバーのステータスを表示します。
- クリティカル（赤） -アプリのスコアが 40 未満であることを示します。
- レビュー（オレンジ） -アプリのスコアが 40 から 75 の間であることを示します。
- **Good**（緑） -アプリのスコアが 75 を超えることを示します。

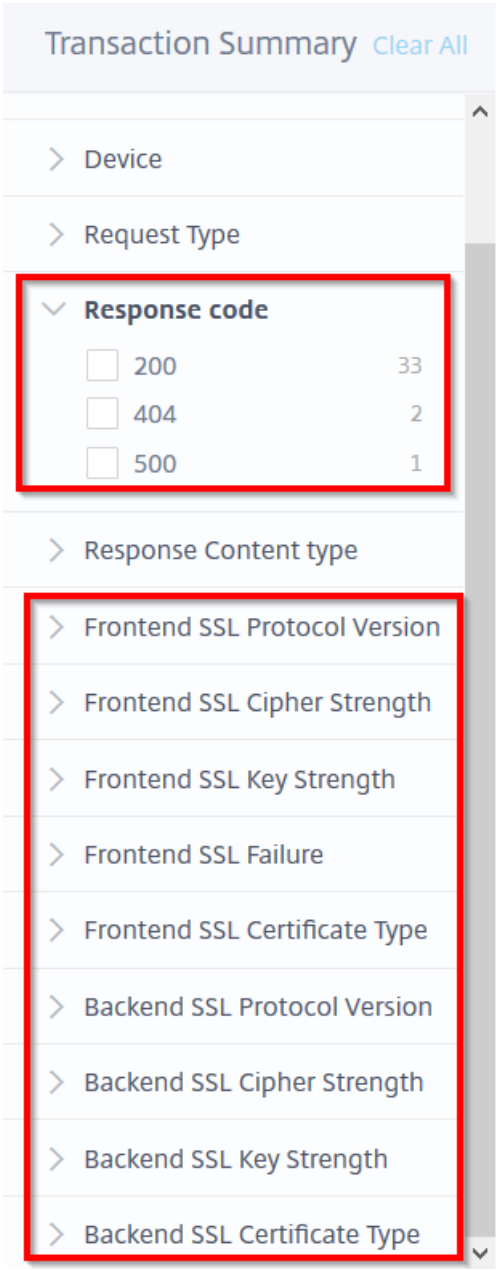
詳しくは、「サービスグラフ」を参照してください。

[NSADM-43967]

[トランザクションのサマリー**]** パネルに **4xx** および **SSL** メトリックの表示

Web トランザクション分析 [トランザクションの概要] パネルでは、次の項目を表示できるようになりました。

- 4xx エラー
- SSL フロントエンドおよび SSL バックエンドメトリック



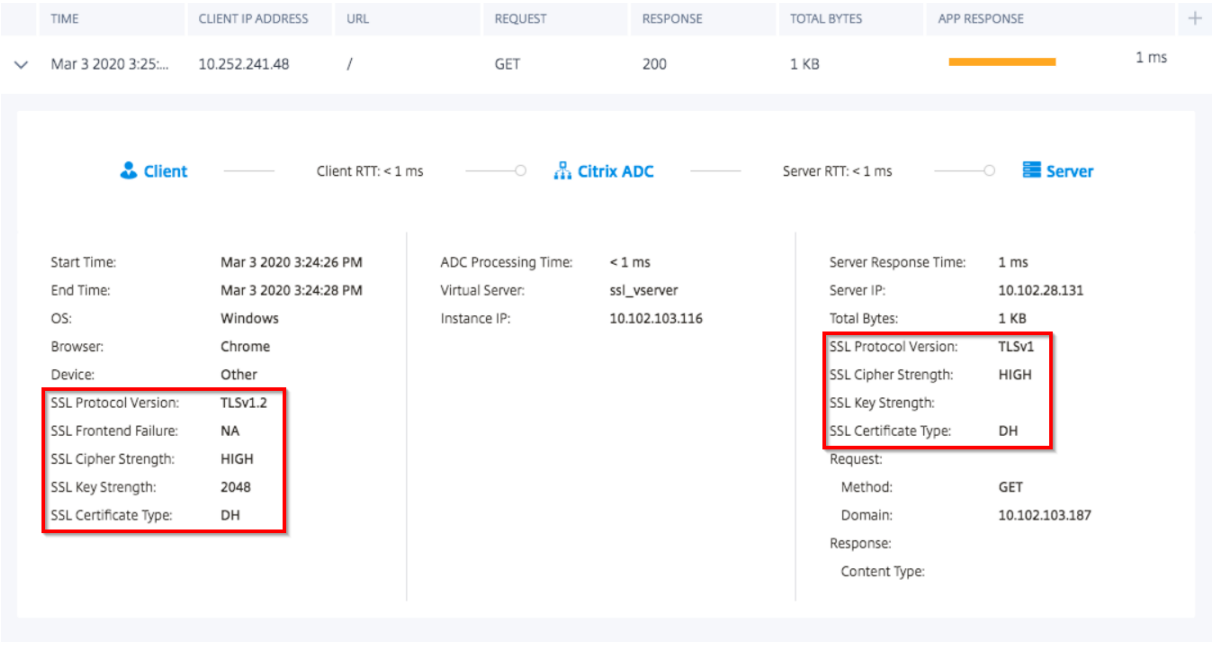
詳しくは、「ウェブトランザクションの分析を表示する」を参照してください。

[NSADM-43841]

ウェブトランザクション分析での **SSL** メトリックの表示

ウェブトランザクション分析でトランザクションをクリックすると、SSL トランザクションのその他のメトリックスを表示できるようになりました。これらのメトリックから、クライアントまたはサーバーから SSL エラーが発生したかどうかを分析できます。

クライアントとサーバーについて、次のメトリックが表示されます。

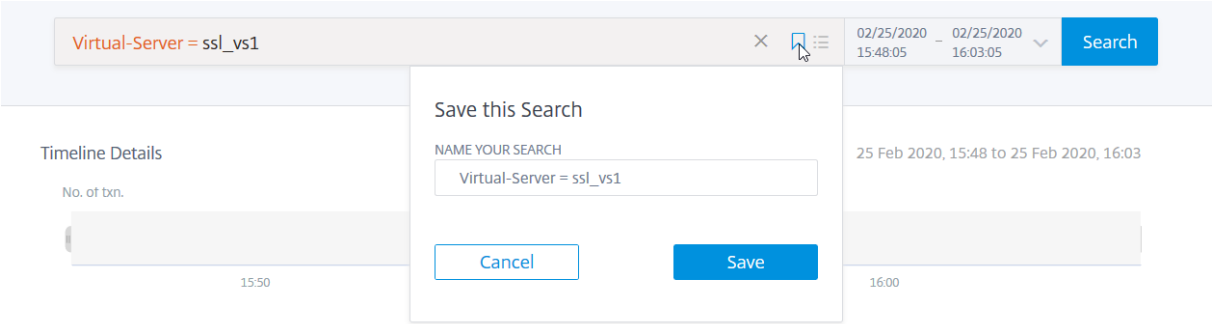


詳しくは、「ウェブトランザクションの分析を表示する」を参照してください。

[NSADM-43844]

ウェブトランザクション分析の詳細検索で検索オプションを保存

ウェブトランザクション分析の高度な検索オプションで、検索クエリを保存できるようになりました。その後、候補と演算子を再度使用する代わりに、一覧から保存された検索クエリをクリックすることができます。
検索クエリを保存するには、ブックマークアイコンをクリックし、任意の名前を指定して、[保存] をクリックします。



詳しくは、「ウェブトランザクションの分析を表示する」を参照してください。

[NSADM-43843]

解決された問題

アプリケーション

- アプリケーションダッシュボードには、ADC HA ペアとクラスタからのアプリケーションが表示されません。

[NSADM-47668]

- エージェントが追加されていない場合、Citrix ADM はアプリケーションダッシュボードにエラーメッセージが表示されます。

[NSADM-47444]

- **IE 11** ブラウザでは、アプリケーションダッシュボードが空白で表示されます。

[NSADM-47812]

Analytics

- ADC インスタンス AppFlow でクライアント側の測定を有効にすると、Citrix ADM AppFlow デコーダログファイルプロセスが失敗します。

[NSHELP-21462]

ネットワーク

- ADC ホスト名は、[ネットワーク機能**] > [GSLB**] に表示されません。

[NSADM-47335]

- ネットワークレポートダッシュボードには、1 か月の間、完全なデータが表示されません。

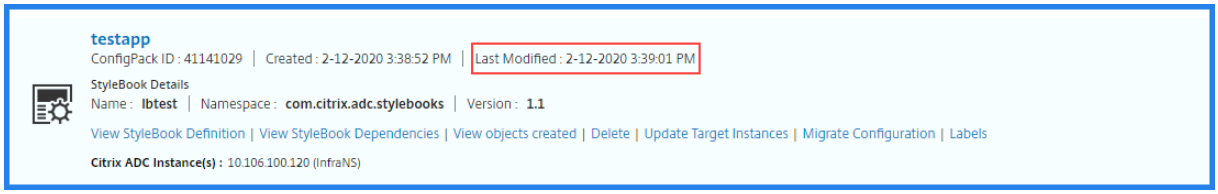
[NSHELP-21731]

2020 年 2 月 11 日

新機能と機能強化

StyleBooks 構成に新しい列が表示される

「アプリケーション」>「**StyleBooks** 」>「構成」で、StyleBook 構成（設定パック）の構成タイルに最終更新時刻が表示されるようになりました。



[NSADM-45811]

解決された問題

Analytics

- Web インサイトと HDX インサイトの週次レポートは表示されません。

  [NSADM-46149]

アプリケーション

- アプリケーションダッシュボードでアプリ分析を表示するデフォルトの期間は 15 分に変更されます。

  [NSADM-46980]

- StyleBook 設定を使用してカスタムアプリケーションを作成すると、編集オプションと削除のオプションが期待どおりに機能しません。

  [NSADM-46821]

ライセンス

- [プールされた容量] オプションは、[帯域幅ライセンスの種類] に初めて表示されません。

  回避策:

  1. [ライセンスタイプ] リストから [仮想 CPU ライセンス] を選択します。
  2. 選択を [帯域幅ライセンス] に変更して、[プールされた容量] オプションを選択します。

  [NSADM-40129]

ネットワーク

- 多数のコマンドで構成ジョブを作成すると、[**Action**] タブに [**Abort**] オプションは表示されません。

  [NSADM-47041]

2020 年 **2** 月 **03** 日

新機能と機能強化

アプリケーションのサービスグラフ

アプリケーションダッシュボードのサービスグラフ機能を使用すると、次の項目を表示できます。

- アプリケーションの構成方法の詳細（コンテンツスイッチング仮想サーバーと負荷分散仮想サーバーを使用）
- クライアントからサービスへのエンドツーエンドのビュー
- クライアントがアプリケーションにアクセスしている場所
- クライアント、サービス、仮想サーバーのメトリックの詳細
- エラーがクライアントまたはサービスからのものである場合
- サービス、仮想サーバ、およびクライアントのステータス（クリティカル、レビュー、良好）。

詳しくは、「サービスグラフ」を参照してください。

[NSADM-41898]

改善されたアプリケーションダッシュボード

アプリケーションダッシュボードを使用して、次の新機能を表示できます。

- アプリケーションのステータス（クリティカル、フェア、良好および該当なし）
- アプリケーション（負荷分散またはコンテンツスイッチング）設定の詳細
- 選択したアプリケーションに関連付けられたサービスの詳細
- 選択したアプリケーションのメトリックの詳細。アプリケーションのレスポンス時間、スループット、1 秒あたりのリクエスト数、エラー率、合計接続数、データ量などのグラフ形式
- 選択したアプリケーションに適用可能なすべての問題

詳しくは、「アプリケーション」を参照してください。

[NSADM-32894]

アプリケーション分析のパフォーマンス指標

Citrix ADM には、Citrix ADC Web アプリケーションで発生する次の新しいアプリケーションパフォーマンス指標が表示されるようになりました。

- 不適切な永続性タイプ
- 不安定なサーバー (5xx)
- セッションの再利用推奨（SSL）
- SSL リアルタイムトラフィック
- 異常に大きな HTTP ヘッダー
- TCP 再構成キュー制限ヒット
- サージキューのビルダップ

「アプリケーション」**>**「ダッシュボード」の順にナビゲートし、アプリケーションを選択することで、これらのアプリケーションの問題を表示できます。

詳しくは、「アプリケーション分析用のパフォーマンス・インディケータ」を参照してください。

[NSADM-39779]

Citrix ADM での **Web** アプリケーションファイアウォールのサポート

Security Insight では、次の新しい Web アプリケーションファイアウォール (WAF) 保護ポリシーが有効になり、WAF の違反パターンが強調されます。

- APPFW_BUFFEROVERFLOW_QUERY
- APPFW_BUFFEROVERFLOW_TOTAL_HDR

[NSADM-43541]

StyleBooks 構成表示 **ADC** インスタンスのホスト名表示

StyleBooks 構成 (設定パック) では、ADC インスタンスのホスト名と IP アドレスが設定タイルに表示されるようになりました。ホスト名または IP アドレスを使用して、StyleBook 構成を検索できるようになりました。

[NSADM-42517]

到達不能な **Kubernetes** クラスターを削除する

クラスターが到達不能または存在しなくなった場合でも、ADM サービスから Kubernetes Ingresses を削除できるようになりました。クラスターの Ingresses を削除した後、到達可能性に関係なく、親クラスターを削除することもできます。

[NSADM-45612]

Citrix 入力クラスで入力イベントを処理する

Citrix ADM ServiceNow は、Citrix Ingress クラス注釈 (`kubernetes.io/ingress.class: Citrix`) を持つ入力イベントのみを処理します。また、ADM サービスによって生成される入力仕様には、Citrix Ingress クラス注釈が含まれています。

[NSADM-45613]

Citrix ADC FIPS インスタンスでプール容量ライセンスを構成する

Citrix ADC MPX および VPX FIPS ライセンスでプール容量ライセンスを構成できるようになりました。詳しくは、「プールされた容量の構成」を参照してください。

[NSADM-31742]

ネットワーク関数エンティティの新しいデフォルトポーリング時間

ネットワーク機能エンティティのデフォルトのポーリング時間は、30 分から 60 分に変更されます。デフォルトでは、Citrix ADM サービスは 60 分ごとに構成されたネットワーク機能エンティティを自動的にポーリングします。

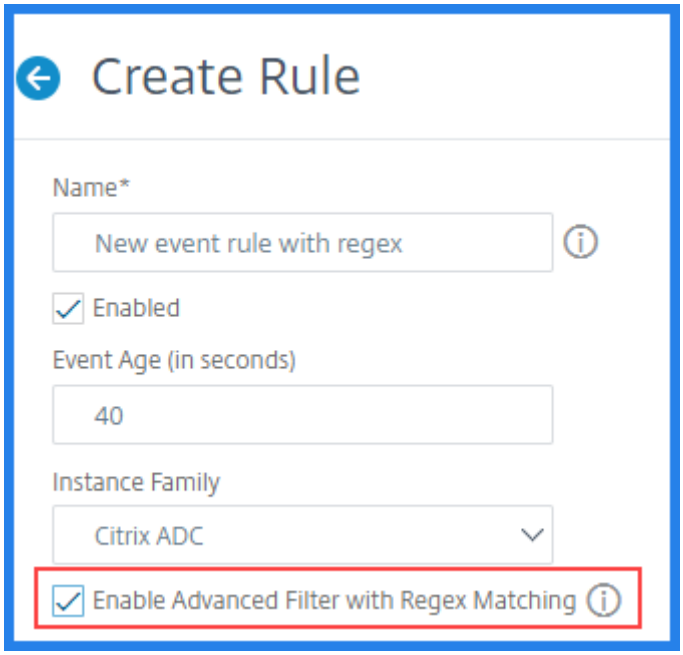
詳しくは、「Citrix ADM が管理対象インスタンスおよびエンティティをポーリングする方法」を参照してください。

[NSADM-44078]

正規表現パターンマッチングを使用した高度なフィルタ

正規表現パターンマッチングを使用して、障害オブジェクト、構成コマンド、およびメッセージをフィルタリングできるようになりました。以前は、イベントをフィルタリングするためにアスタリスク (*) パターンマッチングのみを使用できました。

詳しくは、「イベントルールの定義」を参照してください。



[NSADM-43614]

フィーチャ固有のエクスポートレポートの表示と編集

Citrix ADM は、個別の ADM 機能の下に機能固有のスケジュールエクスポートレポートを表示します。これらのレポートは表示、編集、削除できます。たとえば、Citrix ADC インスタンスのエクスポートレポートを表示するには、［ネットワーク］**>**［インスタンス］**>**［**Citrix ADC** ］の順に選択し、［エクスポート］アイコンをクリックします。[**Export Reports**] ページには、ADC インスタンスのすべてのエクスポートレポートが表示されます。以前は、ADM 定期エクスポートレポートが [アカウント**] > [**エクスポートスケジュール] に表示されていました。

詳しくは、「エクスポートレポートのエクスポートまたはスケジュール設定」を参照してください。

[NSADM-43329]

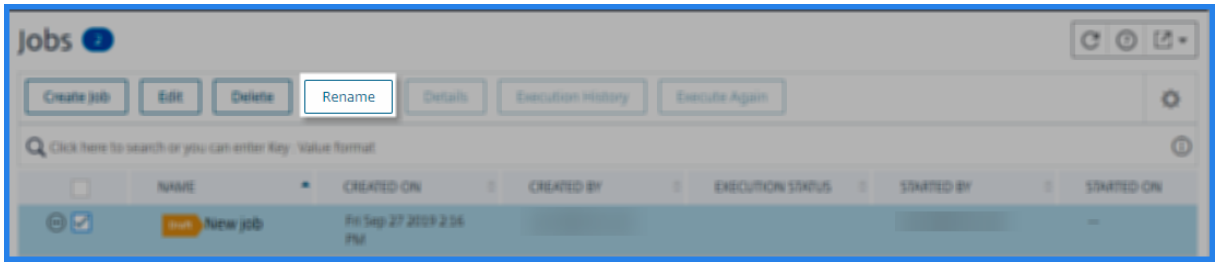
Citrix ADC SSL 証明書の表示とダウンロード

Citrix ADM GUI には、検出された Citrix ADC インスタンスのすべての SSL 証明書が表示されます。ADC インスタンスの SSL 証明書を表示およびダウンロードするには、**Citrix ADC** で［ネットワーク］**>**［**SSL** ダッシュボード］**>**［**SSL** 証明書ファイル］に移動します。

[NSHELP-6556]

構成ジョブとテンプレートの名前変更

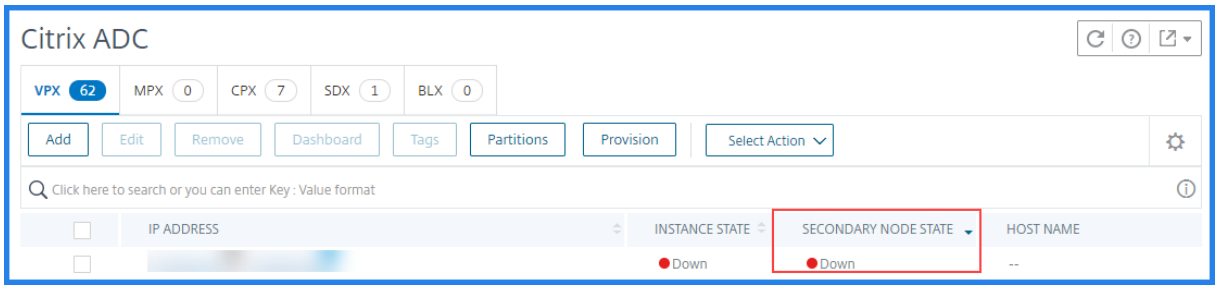
Citrix ADM でカスタム構成ジョブとカスタム監査テンプレートの名前を変更できるようになりました。



[NSADM-42945、NSHELP-6488]

セカンダリインスタンスステータスの新しい列

Citrix ADM GUI で、[ネットワーク] **>** [インスタンス] で、高可用性ペアのセカンダリインスタンスのステータスを確認できるようになりました。たとえば、**Citrix ADC** をクリックすると、セカンダリインスタンスのステータスの新しい列が表示されます。Citrix ADM GUI では、インスタンスの概要ページにセカンダリインスタンスのステータスが表示されます。これで、[セカンダリノードの状態] 列と [ダッシュボード] の下にステータスを表示できます。



[NSHELP-6236]

解決された問題

- アプリダッシュボードでは、StyleBooks を使用してカスタムアプリケーションを定義すると、StyleBooks はページの下部に表示され、ナビゲートするのが困難でした。

  この修正により、StyleBooks は新しいページに表示されます。選択した StyleBook の詳細を指定すると、新しいアプリケーションがアプリケーションダッシュボードに表示されます。

  [NSADM-45241]

- ファイル名に複数のピリオド（.）を含むファイルをアップロードして構成ジョブを作成すると、Citrix ADM GUI にエラーが表示されます。その結果、設定ジョブは作成されません。

  [NSADM-45748]

2019 年 **12** 月 **17** 日

新機能と機能強化

Citrix ADM エージェントのフェイルオーバーのサポート

エージェントのフェールオーバーは、2 つ以上の登録済みエージェントがあるサイトで発生する可能性があります。サイト内でエージェントが非アクティブ（DOWN 状態）になると、Citrix ADM サービスは、非アクティブなエージェントの ADC インスタンスを他のアクティブなエージェントに再配布します。

エージェントのフェイルオーバーを実現するには、必要な Citrix ADM エージェントを 1 つずつ選択し、同じサイトに接続します。詳しくは、「マルチサイト展開用に Citrix ADM エージェントを構成する」を参照してください。

[NSADM-30048]

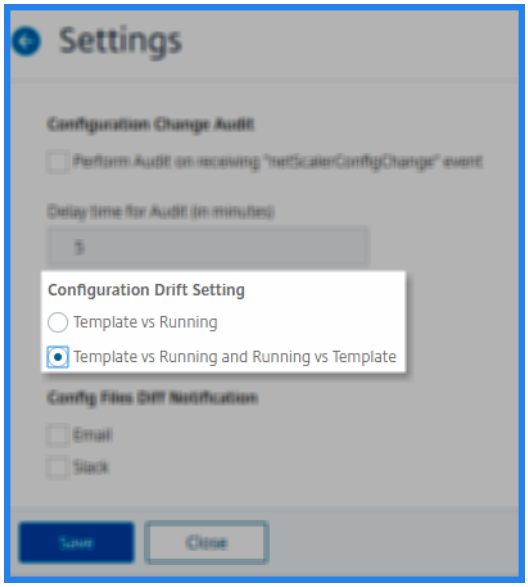
Citrix ADC 構成のドリフトを **2** つのモードで表示

Citrix ADM GUI で、2 つのモードで構成のドリフトを表示できるようになりました。

1. テンプレートと実行中: ADM サービスは、監査テンプレート設定をインスタンスの実行構成と比較します。
2. テンプレートと実行中および実行とテンプレート: ADM サービスは、次の両方の方法で構成を比較します。
    - 監査テンプレート設定と、インスタンスの実行設定を比較します。
    - インスタンスの構成実行と監査テンプレートを比較します。

比較すると、Citrix ADM GUI に監査テンプレートと実行構成の違いが表示されます。また、実行構成を監査テンプレートに修正するコマンドも表示されます。

デフォルトでは、[テンプレートとランニングドリフト] の設定が選択されています。ドリフト設定を変更するには、ADM GUI から、[構成監査] ページで [設定] を選択します。



詳しくは、「テンプレートと実行中の差分」を参照してください。

[NSHELP-6463]

Citrix ADC セカンダリノードで構成ジョブを実行する

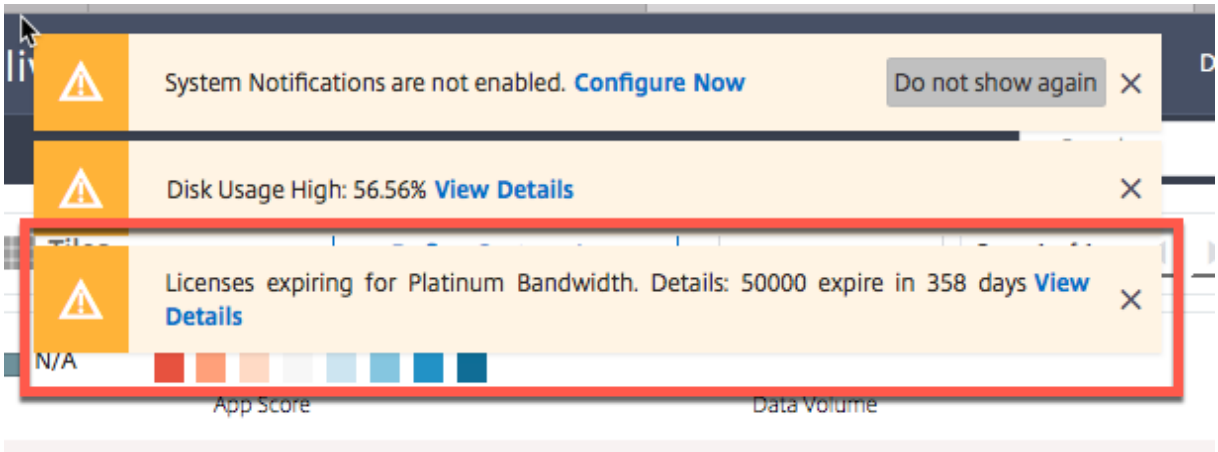
Citrix ADC の高可用性ペアで、プライマリノードまたはセカンダリノードのいずれか、または両方のノードを選択して構成ジョブを実行できるようになりました。ノードを指定しない場合、構成ジョブはプライマリノード上で自動的に実行されます。

以前は、プライマリノードでのみ構成ジョブを実行できました。詳しくは、「構成ジョブの作成方法」を参照してください。

[NSHELP-6567]

チェックイン・チェックアウトライセンスの有効期限通知

ADM サービスにログオンすると、チェックインチェックアウトライセンスの有効期限が近づくと、システム警告メッセージが表示されます。アラートを取得するには、ライセンス通知を構成する必要があります。の設定方法の詳細については、仮想サーバライセンスの有効期限チェックを参照してください。



[NSADM-42655]

プールされたキャパシティライセンス通知の帯域幅の詳細

ADM プールキャパシティライセンスの有効期限通知には、帯域幅の詳細が含まれるようになりました。プール全体から期限切れになる帯域幅を確認できます。以前は、帯域幅の詳細は GUI でのみ使用できました。有効期限の通知を取得するには、ADM サービスを構成する必要があります。詳しくは、「仮想サーバライセンスの有効期限チェック」を参照してください。

[NSADM-39332]

インフラストラクチャ分析でのインスタンスの詳細の表示

インフラストラクチャ分析で、インスタンスの IP アドレスをクリックすると、[概要] タブで次の詳細を表示できるようになりました。

- インスタンススコア、インスタンススコアに影響する問題のカテゴリ、およびその他のインスタンスの詳細。
- CPU 使用率、メモリ使用量、スループット、HTTPS リクエスト/秒、TCP 接続、SSL トランザクションなどのインスタンスの主要なメトリック。
- インスタンススコアに影響するすべての問題の詳細。

詳しくは、「インフラストラクチャ分析」を参照してください。

[NSADM-42276]

既知の問題

May 7, 2021

Citrix Application Delivery Management（Citrix ADM）には、次の既知の問題があります。

Analytics

Gateway Insight で、レポートをスケジュールすると (**[**レポートのエクスポート**] > [**エクスポートのスケジュール**])**、生成されたレポートに「ページが見つかりません」と表示されます。

[NSHELP-26283]

ネットワーク

- [ネットワーク**] > [**** インスタンスアドバイザリ**] > [**セキュリティアドバイザリ] の [セキュリティアドバイザリ **] の [セキュリティアドバイザリ] で、すべての CVE が表示されず、レポートまたはアドバイザリダッシュボードに CVE が 1 つだけ表示される場合があります。

  回避策: オンデマンドスキャンを実行するには、**[**今すぐスキャン] をクリックします。スキャンが完了すると、スコープ内のすべての CVE（約 15）が GUI またはレポートに表示されます。

[NSADM-69920]

- 実行中の設定ジョブを中止すると、**[** 実行設定**]** ページの **[** コマンド失敗時**]** オプションで **[** 成功したコマンドのロールバック**]** オプションが選択されている場合、成功したコマンドはロールバックされません。

[NSADM-34246]

- ADM は SSH 経由で ADC BLX インスタンスと通信しないため、設定監査や設定ジョブなどの ADC 機能の一部が BLX では動作しない場合があります。

  [NSADM-68985]

ライセンス

Citrix ADM ライセンスを選択して AutoScale グループを作成すると、プールされたライセンスは表示されません。

[NSADM-62727]

以前のリリース

May 7, 2021

このトピックは、Citrix Application Delivery Management（Citrix ADM）の以前のリリースのリストです。

2019 年 **12** 月 **03** 日

新機能と機能強化

サービスグラフでのしきい値の設定

管理者として、Kubernetes サービスのしきい値を設定できるようになりました。Citrix ADM では、サービスの応答時間とエラー数に基づいて、サービスの状態（重大、レビュー、および良好）が表示されます。デフォルトでは、すべてのサービスに適用されるデフォルトのしきい値（サービス応答時間 = 200 ms、エラー数 = 0）を表示できます。

詳しくは、「サービスグラフでのしきい値の設定」を参照してください。

[NSADM-41290]

サービスの **TCP** および **SSL** メトリック

Service Graph では、HTTP トランザクションの詳細とは別に、TCP および SSL サービスの依存関係とメトリックを表示できるようになりました。これで、サービスで使用されるプロトコルとともにサービスグラフが表示されます。TCP メトリックと SSL メトリックを使用すると、次のことができます。

- サービス間の TCP 接続の詳細を表示する
- TCP 関連の問題が送信元サービスまたは宛先サービスにあるかどうかを確認します。
- SSL エラーが送信元サービスまたは宛先サービスからのものであるかを表示する
- SSL サービスが使用する SSL プロトコルのバージョンの表示

詳しくは、「サービスグラフ」を参照してください。

[NSADM-41295], [NSADM-41296]

キープアライブインターバルの設定

これで、ADM サービスとエージェント間の接続を維持するために、内部キープアライブを設定できます。内部は 30～120 秒である必要があります。間隔を構成するには、ADM サービスの GUI から、[設定] > [システム設定**] > [**システム構成**] > [**エージェントとタイムゾーン] に移動します。

[NSADM-43641]

状況依存ヘルプのサポート

ユーザーエクスペリエンスを向上させるために、Citrix ADM GUI にヘルプパネルが追加されました。ADM サービスにログオンするときに、疑問符 (?) をクリックします。をクリックして、ヘルプパネルを起動します。

このヘルプパネルには、次の情報を表示するオプションがあります。

- コンテキストヘルプ: 表示している UI 画面に固有のコンテンツを起動します。現在、ヘルプリンクは新しいブラウザタブで開き、製品ドキュメントの状況依存コンテンツを表示します。
- ドキュメント:ADM サービスのドキュメントの概要ページを起動し、必要なコンテンツに移動します。
- ディスカッションフォーラム: フォーラムサイトを立ち上げ、当社の専門家コミュニティが議論している内容を表示します。
- 購入方法:ADM サービスを購入できる場所から citrix.com サイトを起動します。
- カスタマーサポート: サポートサイトを起動して、サポートチームにお問い合わせください。

[NSADM-39656]

解決された問題

ネットワーク

[ADM GUI] > [ネットワーク**] > [**インフラストラクチャ分析**]** で、右上隅の **Circle Pack** 表示または表形式表示をクリックすると、Firefox ブラウザーでページが正しくレンダリングされません。

[NSADM-40660]

Autoscale グループを追加するページ（**ADM GUI >** ネットワーク **> Autoscale** グループ **>** 追加）で、ライセンスエディションを選択するオプション（たとえば、Citrix ADC VPX Advanced Edition-10Mbps）が［ライセンス］タブの代わりに［クラウドパラメータ］タブに表示されます。

[NSADM-43759]

ADC SSL 証明書の有効期限を設定したメール、SMS、または Slack 通知が機能しません。

[NSADM-44008]

Analytics

AppFlow コレクタにカスタム名がある場合、ADM Analytics 機能が無効になることがあります。

[NSADM-43723]

2019 年 11 月 12 日

新機能と機能強化

バーストライセンスによる帯域幅の増加

バーストライセンスは、プールされた容量に追加の帯域幅またはインスタンスライセンスを提供する特別なプログラムです。仮想 CPU サブスクリプションでは、仮想 CPU ライセンスが追加されます。基本サブスクリプション制限に達すると、新しいライセンスを調達しなくても、すぐに使用できるライセンスを使用できます。これらのバーストライセンスは、1 か月あたりの実際の使用量に基づいて課金されます。バーストライセンスプログラムは、特定のお客様のみを必要に応じて利用できます。

毎月、年間のサマリーを表示して、プールされた容量の帯域幅使用状況を追跡できます。ライセンスの使用状況を表示するには、Citrix ADM GUI で［プールされた容量］**>**［ライセンス使用状況］ページに移動します。

[NSADM-36649]

サービスグラフでの入力メトリックとクライアントメトリックの表示

サービスグラフでは、Ingress を介して接続されたサービスとともにネットワークマップが表示されます。これで、次の項目を表示できます。

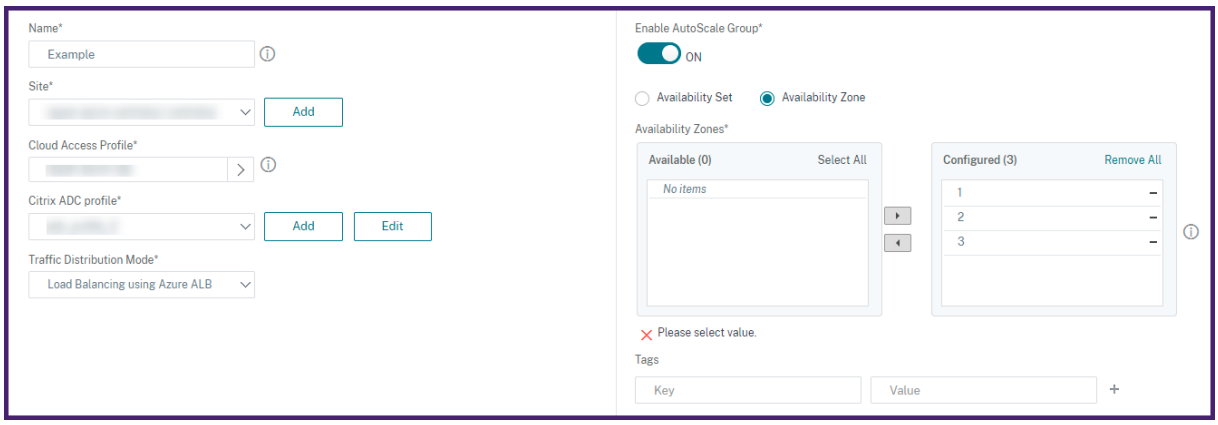
- ADC インスタンス（MPX、VPX、CPX）が要求を処理するのに要した平均時間。
- クライアントと Ingress 間の通信のためのクライアント RTT。

詳しくは、「クラウドネイティブ (Kubernetes) アプリのサービスグラフ」を参照してください。

[NSADM-41287]

Citrix ADM AutoScale グループの Azure 可用性セットのサポート

Azure クラウドにデプロイされた Citrix ADC VPX インスタンスを Autoscale するために Citrix ADM サービスで Autoscale グループを作成する場合、アベイラビリティセットまたはアベイラビリティーゾーンのいずれかを選択できるようになりました。以前は、アベイラビリティーゾーンが唯一のオプションでした。



詳しくは、「構成」を参照してください。

[NSADM-42598]

解決された問題

ネットワーク

仮想サーバーを選択すると、「**ADM GUI**」**>**「ネットワーク」**>**「ネットワーク機能」**>**「コンテンツスイッチング」の「ビジュアライザー」タブをクリックすると、
「エラー：Citrix ADC 構成を取得できませんでした。」「

[NSADM-42066]

GSLB ネットワーク機能は、Citrix ADC メトリックの処理時間が長くなります。この問題により、GSLB サイトの検出中にレイテンシーが追加され、Citrix ADM 分析で ADC デバイスの不一致が生じます。この問題は、複数のテナントに対して複数の GSLB デバイスを構成するときに発生することがあります。

[NSADM-40997]

オーケストレーション

Citrix ADM サービスで既存の Kubernetes クラスターを編集すると、「応答エラー」と応答ステータス「500」というエラーが表示されます。
今回の修正により、ADM はエージェント上の Kubernetes クラスターを編集した値で再構成します。また、Citrix ADM GUI には、クラスタの再構成の状態を示すメッセージが表示されます。クラスタ構成のステータスは、次のとおりです。

- Citrix ADM が Kubernetes クラスターに正常に追加されました。
- トークンには、編集したクラスターを構成するために必要な権限がありません。
- Citrix ADM が Kubernetes クラスターに接続できませんでした。

[NSADM-41023]

Analytics

分析を有効にすると、ADM GUI で Web Insight がデフォルトで選択されます。

[NSADM-40606]

2019 年 10 月 17 日

新機能と機能強化

新しい指標を追加した強化されたインフラストラクチャ分析

既存のインジケータとは別に、インフラストラクチャ分析で次の新しい指標を表示して、Citrix ADC インスタンススコアを充実させることができます。

- 不正な IP ヘッダー
- 不正な L4 チェックサム
- IP 移動による CPU 使用率の向上
- 過剰なパケットステアリング
- 再構成制限ヒットによる TCP パケットのドロップ
- レイヤ 2 ループ
- タグ付き VLAN の不一致

詳しくは、「新しいインジケータによるインフラストラクチャ分析の強化」を参照してください。

[NSADM-39152]

エージェントイメージのダウンロードオプション

これで、ADM サービスにエージェントが存在しない場合でも、ADM UI から最新のエージェントイメージをダウンロードできます。詳しくは、「エージェントのアップグレード設定の構成」を参照してください。

[NSADM-40097]

複数のクラスターでの **Kubernetes Ingress** 設定の管理

Kubernetes は、クライアントトラフィックがアプリケーションのマイクロサービスにアクセスするときに使用する Ingress 機能を使用します。Citrix ADC インスタンスは、Kubernetes クラスター内で実行されているアプリケーションへの入力として機能できます。Citrix ADC インスタンスはロードバランサーになり、クライアントから Kubernetes クラスター内のマイクロサービスへの（南北）トラフィックへのプロキシになります。また、インスタンスは、Kubernetes 環境でマイクロサービスのエンドポイントが変更されたときに更新されます。

入力として動作するように複数の ADC インスタンスを設定し、入力ポリシーに基づいて各 ADC を異なるアプリケーションに割り当てることができます。入力設定をデプロイするには、次のように指定します。

- クラスタ — 入力設定をデプロイする Kubernetes クラスター。Kubernetes クラスターを追加するには、「オーケストレーション」**>**「**Kubernetes**」**>**「クラスター」を参照してください。
- ポリシー — ポリシーは、入力設定をデプロイする ADC インスタンス、クラスタ、名前空間を決定します。ポリシーを定義するには、[オーケストレーション**] > [Kubernetes] > [**ポリシー**]** に移動します。
- 入力設定：この設定には、コンテンツスイッチングルール、およびマイクロサービスとそのポートの対応する URL パスが含まれます。また、Kubernetes シークレットを使用して SSL/TLS 証明書を指定して、ADC インスタンスの HTTPS トラフィックをオフロードすることもできます。

Citrix ADM は、入力構成と ADC インスタンスを自動的にマッピングします。Citrix ADM は、ADC インスタンスを選択し、指定された入力ポリシーに応じて入力構成をホストします。進入デプロイステータスを表示するには、[オーケストレーション**] > [Kubernetes] > [Ingress**] に移動します。

成功した入力構成ごとに、Citrix ADM は StyleBooks 構成パックを生成します。ConfigPack は、入力設定に対応する ADC インスタンスに適用される ADC 設定を表します。設定パックを表示するには、[アプリケーション] > [**StyleBooks**] > [構成] に移動します。

詳しくは、「Citrix ADM で Kubernetes 入力構成を管理する」を参照してください。

[NSADM-40847]

ネットワーク機能エンティティをユーザーに許可する

管理者は、特定のネットワーク機能エンティティを選択し、ユーザーにアクセス権を付与できます。このオプションを使用すると、ネットワーク機能エンティティの個々のレベルでユーザーアクセスを管理できます。この機能を使用すると、エンティティレベルで特定のアクセス許可をユーザーまたはグループに動的に割り当てることができます。

ネットワーク機能エンティティを承認するには、グループの構成時に **[**個々のエンティティタイプを選択**]** オプションを選択します。Citrix ADM GUI では、次のネットワーク機能エンティティタイプを認証できます。

- アプリケーション（仮想サーバ）
- サービス
- サービスグループ
- サーバー

個々のエンティティを追加するか、必要なエンティティタイプの下にあるすべてのエンティティを選択して、ユーザーにアクセスを許可できます。詳しくは、「Citrix ADM でのグループの構成」を参照してください。

[バインドされたエンティティにも適用] オプションは、選択したエンティティタイプにバインドされているエンティティを承認します。たとえば、アプリケーションを選択し、「バインドされたエンティティにも適用」を選択すると、アプリケーションにバインドされたエンティティも承認されます。

正規表現を使用してネットワーク関数エンティティを選択できます。エンティティは、指定された正規表現に応じて検出されます。検出されたエンティティの [バインドされたエンティティを許可する] オプションを選択すると、ユーザーは選択したエンティティにバインドされているエンティティに自動的にアクセスできます。

> 注
>
> バインドされたエンティティを承認する場合は、エンティティタイプを 1 つだけ選択してください。

[NSHELP-6078]

新しい構成監査グラフ

［構成監査］ページに［Citrix ADC 構成ファイルの状態 **］グラフが追加されます。このグラフには、nsconfig フォルダ内に存在する Citrix ADC ファイルのステータスが表示されます。Citrix ADM は、nsconfig フォルダー内のファイルの変更を記録して比較し、相違点を表示します。

このグラフを使用すると、nsconfig フォルダ内のファイルが追加、変更、または削除されたかどうかを監視できます。

たとえば、ADC インスタンスでライセンス・ファイルが更新された場合、このファイルが最後に更新された日時を確認し、適切なアクションを実行できます。

変更されたファイルステータスイベントに関する通知を受信するようにアラートを設定できます。[構成ファイルの相違通知] で、電子メールまたは slack の情報を指定できます。詳しくは、「インスタンス間の設定変更の監査」を参照してください。

[NSADM-36469]

解決された問題

ネットワーク

- Citrix ADM からダウンロードされたcertkeysが破損しています。

  [NSADM-41630]

- [ネットワーク] > [AutoScale グループ] で新しい **AutoScale** グループを作成すると、HTML タグが [ライセンス] タブに表示されます。

  [NSADM-42234]

オーケストレーション

Citrix ADM エージェントが変更または無効になった場合、クラスタを削除することはできません。

[NSADM-41021]

2019 年 **10** 月 **03** 日

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで Citrix ADM 最新ビルドに自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エ

ージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

負荷分散サービスのネットワークレポートの生成

これで、負荷分散サービスのネットワークレポートダッシュボードを作成できます。このダッシュボードには、選択したサービスの次のレポートを表示できます。

- 接続: クライアントとサーバーの接続カウンタ。
- スループット: 要求バイト数と応答バイトカウンタ。
- 最初のバイトまでの時間（TTFB）: 要求パケットをサービスに送信し、サービスから最初のパケットを受信するのに要した平均時間。この応答時間は TTFB と呼ばれます。

ネットワークレポートダッシュボードの作成方法の詳細については、「ネットワークレポート作成」を参照してください。

[NSADM-18228]

修正された問題

ネットワーク

RBAC ユーザが ADM GUI にログオンすると、そのユーザが子メニューにアクセスできるが親メニューにアクセスできない場合は、エラーメッセージが表示されます。

[NSHELP-20409]

2019 年 **9** 月 **18** 日

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで Citrix ADM 最新ビルドに自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

Citrix ADM サービスを使用して **ServiceNow** でインシデントを自動生成する

Citrix ADC イベント、SSL 証明書イベント、および Citrix ADM ライセンスイベントに対して、ServiceNow インシデントを自動生成できます。

- **Citrix ADC** イベント：Citrix ADM は、選択した管理対象の Citrix ADC インスタンスから、選択した一連の Citrix ADC イベントの ServiceNoW インシデントを生成できます。

  管理対象インスタンスから Citrix ADC イベントの ServiceNow 通知を送信するには、イベントルールを構成し、ルールのアクションを「**ServiceNow** 通知の送信」として割り当てる必要があります。

  [ネットワーク**]** > **[**イベント**]** > **[**ルール**]** に移動して、ADM サービスでイベントルールを作成します。詳しくは、「サービスノウ通知の送信」を参照してください。

- **SSL** 証明書と **ADM** ライセンスイベント：Citrix ADM は、SSL 証明書の有効期限および ADM ライセンス有効期限イベントの ServiceNoW インシデントを生成できます。

  SSL 証明書の有効期限に関する ServiceNow 通知を送信するには、「SSL 証明書の有効期限」を参照してください。

  ADM ライセンスの有効期限に関する ServiceNow 通知を送信するには、「Citrix ADM ライセンスの有効期限」を参照してください。

> 重要
>
> - この機能は ServiceNow クラウドでのみサポートされます。
> - Citrix Cloud ITSM アダプタが ServiceNow 用に構成され、Citrix ADM サービスと統合されていることを確認します。Citrix ADM サービスと ServiceNow インスタンスの統合を参照してください。

[NSADM-23783]

ボット攻撃の分析を表示する

Citrix ADC インスタンスで構成されたボット検出テクニックのインサイトを表示できるようになりました。［分析］> ［ボットインサイト］の順に選択し、Citrix ADC インスタンスに対するボット攻撃を表示します。ボットインサイトを有効にして、ボット攻撃の分析を表示します。

詳しくは、「ボットインサイト」を参照してください。

[NSADM-36648]

Express アカウントを使用して **Citrix ADM** サービスを管理する

このリリースでは、Citrix ADM サービスアカウントを作成すると、Express ライセンスアカウントが自動的に割り当てられます。別の試用ライセンスは不要です。すでに試用期間に入っている場合、試用期間が終了すると、アカウントは Express アカウントに変換されます。

Citrix ADM ライセンスのサブスクリプションと猶予期間が終了すると、アカウントは Express アカウントに変換されます。

詳しくは、「Citrix ADM Express アカウント」を参照してください。

[NSADM-31715]

ロールバックコマンドをカスタマイズして設定ジョブを作成する

設定ジョブを作成するときに、コマンドが失敗したときに実行するロールバックコマンドを指定できるようになりました。[ネットワーク] > [構成ジョブ] に移動して、[ロールバックのカスタマイズ] オプションを有効にできます。

[NSADM-31710]

高度な検索のための情報ヒント

syslog メッセージおよび監査ログメッセージの検索に使用する演算子および論理演算子について説明する情報ヒントが追加されます。情報のヒントを表示するには、ADM GUI の検索バーをクリックし、[ヘルプが必要] をクリックします。

詳しくは、「syslog メッセージの検索」を参照してください。

[NSADM-38406]

解決された問題

ライセンス

- [ライセンス使用] でタイムゾーンをローカルから GMT に変更しても、カスタム時刻は GMT に変更されません。また、ライセンス使用状況レポートは生成されません。

[NSADM-17670]

ネットワーク

- ［ネットワーク］> ［ネットワーク機能］から［今すぐポーリングする］をクリックすると、Citrix ADM GUI がしばらくハングし、データが回復できません。

[NSHELP-20143]

- すべてのファイルが削除され、エージェントが追加されていない場合でも、Citrix ADM に「ライセンスの機能には少なくとも 1 つのエージェントが必要です」というエラーメッセージが表示されます。

[NSADM-38386]

オーケストレーション

- **Citrix ADM** では、複数のクラスターを追加すると、**[**** オーケストレーション] > [クラスタ] にクラスター情報が 1 つだけ表示されます。**

[NSHELP-41020]

2019 年 9 月 03 日

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで Citrix ADM 最新ビルドに自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

クラウドネイティブ **(Kubernetes)** アプリのサービスグラフ

Citrix ADM サービスグラフ機能を使用すると、次のことができます。

- アプリケーション全体のパフォーマンスをエンドツーエンドで監視できます。
- アプリケーションのさまざまなコンポーネントの相互依存関係によって生成されるボトルネックを特定します。
- アプリケーションのさまざまなコンポーネントの依存関係に関する洞察を収集します。
- Kubernetes クラスター内のサービスを監視します。
- 問題のあるサービスを監視します。
- パフォーマンスの問題に寄与する要因を確認してください。
- サービス HTTP トランザクションの詳細な可視性を表示します。
- 次のメトリックスを分析します。
  - 総ヒット数
  - サービス応答時間
  - データボリューム
  - エラー

詳しくは、「クラウドネイティブ (Kubernetes) アプリのサービスグラフ」を参照してください。

[NSADM-23832]

Citrix ADM でインスタンス設定を変更する

Citrix ADM には、インスタンス設定を変更するオプションがあります。これらの設定は、Citrix ADM が検出したインスタンスに適用されます。インスタンス管理の設定を変更するには、**[**設定**]** > **[** システム設定**]** > **[**インスタンス設定**]** に移動します。

[NSADM-37277]

解決された問題

ネットワーク

- ［ネットワーク］>［ネットワーク機能］>［負荷分散］では、Citrix ADM GUI が仮想サーバーを表示するのに時間がかかります。

  [NSHELP-20050]

- AutoScale グループの作成中に、［AutoScale パラメータ］タブに Citrix ADC インスタンスの最小数の情報が表示されませんでした。したがって、Citrix ADM は ADC インスタンスの AutoScale に失敗します。

  [NSADM-40501]

- Citrix ADM で、エージェントを介して検出された Citrix ADC インスタンスに証明書とキーファイルをアップロードしてインストールしようとすると、エラーが表示されることがあります。

  [NSADM-34558]

システム

- Citrix ADM サービスがエージェントを含むインスタンスを検出すると、NITRO 要求は、プロファイルで構成されたプロトコルの代わりに HTTP プロトコルを使用します。この NITRO 通信は、スケジュールされたインベントリ、統計、またはエンティティの監視中に発生します。

  [NSADM-39555]

- 次のナビゲーションを使用して分析を有効にすると、Citrix ADM GUI が応答しなくなります。

  1.「アカウント」>「購読」に移動します。

  2. [負荷分散] をクリックします。

  3. [アナリティクスの有効化] をクリックします。

  [NSADM-40760]

2019 年 **8** 月 **13** 日

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで Citrix ADM 最新ビルドに自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

ADM AutoScale グループのライセンスを **ADM** からチェックアウトする

これで、Citrix ADM サービスに存在する ADC ライセンスを使用して、ADMAutoScale グループ用にプロビジョニングされた Citrix ADC インスタンスのライセンスを取得できます。

新しい [ライセンス] タブが [**AutoScale** グループの作成] ページに表示されます。このタブでは、AutoScale グループの作成時に、プールされた容量、VPX ライセンス、および仮想 CPU ライセンスを構成できます。したがって、Autocale グループ用に新しいインスタンスがプロビジョニングされると、既に設定されているライセンスタイプがプロビジョニングされたインスタンスに自動的に適用されます。

プロビジョニングされたインスタンスが破棄またはプロビジョニング解除されると、適用されたライセンスは自動的に Citrix ADM に返されます。

以前は、Autoscale グループの作成時に、各クラウドマーケットプレイスで使用できる Citrix ADC ライセンスのみを構成できました。したがって、Autocale グループ用に新しいインスタンスがプロビジョニングされると、ライセンスはクラウドマーケットプレイスから取得されます。

詳細については、次のリンクを参照してください。

- AWS ライセンス要件
- Azure ライセンス要件

[NSADM-37694、NSADM-33422]

StyleBook を使用した **Citrix ADC** アプリケーション構成の移行を簡素化

> 注:
>
> この機能はプレビューです

StyleBooks 構成ビルダーを使用すると、既存の ADC 構成から Citrix ADC アプリケーション構成 StyleBook を作成できます。この機能により、ある Citrix ADC インスタンスから別のインスタンスへのアプリケーション構成の移行も自動化されます。
移行を開始するには、次のいずれかの構成ソースを指定します。

- Citrix ADC インスタンス：このオプションは、選択した ADC インスタンス上のアクティブなアプリケーションを検出します。
- CLI コマンドのセット：このオプションは、CLI コマンドを分析し、内のアプリケーションを抽出します。

ソースが指定されると、ADM はソース内で検出されたすべてのアプリケーションを検出します。次に、移行先の ADC インスタンスに移行するアプリケーション構成を選択できます。詳しくは、「Citrix ADC アプリケーション構成の移行」を参照してください。

移行後、対応する StyleBook とともに Citrix ADM で ConfigPack が作成されます。ConfigPack を表示するには、[アプリケーション] > [**StyleBooks**] > [構成] に移動します。

[NSADM-36438]

AutoScale グループ内の **Citrix ADC** インスタンスのアップグレードを簡素化

Autocale グループの一部であるクラウドサービス内のすべてのインスタンスをシームレスにアップグレードできるようになりました。詳しくは、「Autoscale グループのアップグレードをスケジュールする」を参照してください。

> 注
>
> アップグレード中、Citrix ADC インスタンスの自動スケーリングは、選択した AutoScale グループに対して無効になります。

アップグレード後、Autosale グループが新しいインスタンスをプロビジョニングする場合、新しいインスタンスは、アップグレード時に指定されたバージョンと同じになります。

[NSADM-34401、NSADM-34285]

フィルターを使用して **Citrix ADM** 監査ログメッセージを検索する

フィルターを使用して Citrix ADM 監査ログメッセージを検索し、結果を絞り込んで探しているものを正確に検索できるようになりました。新しいフィルタカテゴリは、ソース、イベント、重大度、メッセージです。

ADM に存在するすべてのアプリケーションの監査ログメッセージを検索するには、ADM GUI から、[ネットワーク] > [ネットワーク機能] > [監査] に移動します。

ADM の特定のアプリケーションの監査ログメッセージを検索するには、ADM GUI から [アプリケーション] > [ダッシュボード] に移動し、監査ログメッセージを検索する仮想サーバーを選択します。次に、[監査ログ] タブをクリックします。

詳しくは、「syslog メッセージの表示とエクスポート」を参照してください。

[NSADM-38705]

解決された問題

アカウント

- Citrix ADM GUI では、**Syslog** サーバーオプションを使用できません。

  [NSADM-39256]

Analytics

- 分析を有効にすると、ジオデータ収集もデフォルトで有効になりますが、ジオマップは Citrix ADM に表示されませんでした。

  [NSADM-39543]

ネットワーク

- ライセンスされた仮想サーバーのいくつかは、アップグレード後にライセンスなしになります。この問題により、分析データが失われました。

  [NSADM-39379]

- ネットワーク機能ダッシュボードに仮想サーバーの合計が正しく表示されませんでした。

  [NSADM-39512]

- [**Schedule Export**] オプションを使用してレポートを構成すると、電子メール/slack で受信したレポートに空白の画面が表示されます。

  [NSADM-38974]

- イベントサブシステムのスレッド数が 15 を超えると、Citrix ADM は Syslogs を処理できません。このリリースでは、スレッド制限が 20 に増加しました。

  [NSADM-39518]

2019 年 **7** 月 **31** 日

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで、Citrix ADM 13.0 build 41.12 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

Web トランザクション分析

ウェブトランザクション分析により、複数の詳細なトランザクションを検索して、誤った 5xx レスポンスコードを表示できます。[トランザクションの概要] ページでは、応答時間を短縮するために、詳細なトランザクションを表示することもできます。この機能を使用すると、詳細なトランザクションを調べることができるだけでなく、クライアント、ADC、サーバー間で分割されたレスポンス・タイム・メトリックを視覚的に理解できます。

この機能は、アプリケーションダッシュボードと統合されており、サーバーエラー-5XX の [トランザクションの概要] ページにアクセスできます。詳しくは、「サーバーエラーの Web トランザクション分析」を参照してください。

[NSADM-34701]

マーカー用の **2** つの新しいインジケータ

**** クリティカルイベントとメジャーイベントは ** 、マーカーに追加された新しい指標です。［ネットワーク］ > ［インスタンス］では、マップ上のマーカーは Citrix ADM で作成されたサイトを表します。これで、インスタンスで発

生したクリティカルイベントとメジャーイベントの数がマーカーに表示されます。この情報は、注意が必要なイベントを迅速に評価するのに役立ちます。

詳しくは、「Citrix ADM でグローバルに分散したサイトの監視」を参照してください。

[NSADM-38638]

機械学習とルールベースのアルゴリズムを使用したインテリジェントなアプリケーション分析

Intelligent App Analytics では、機械学習とルールベースのアルゴリズムを使用して、アプリケーションのパフォーマンスの問題を特定できます。管理者は、これらのアルゴリズムを使用して、アプリケーションのパフォーマンスの根本原因分析をより迅速に特定できます。以前は、アプリケーションをダブルクリックすると、応答時間、平均 CPU 使用率、メモリ使用量などのコンポーネントの分析を表示できました。これで、次の新しい指標を表示できます。

- サーバ遅延の異常（機械学習アルゴリズムを使用）
- セッションビルドアップイベント（ルールベースのアルゴリズムを使用）
- サービスフラップイベント（ルールベースのアルゴリズムを使用）

詳しくは、「インテリジェントなアプリケーション分析」を参照してください。

[NSADM-33674]

新しいインジケータによるインフラストラクチャ分析の強化

以前は、Citrix ADM インフラストラクチャ分析を使用して、複数のデータソースを関連付けることで、Citrix ADC インスタンスのスコアを監視することができました。インフラストラクチャ分析で新しい指標を表示して、Citrix ADC インスタンススコアを充実させられるようになりました。これらの新しいインジケータは、管理者が問題の根本原因をすばやく分析するのに役立ちます。

Citrix ADM で、[ネットワーク] > [インフラストラクチャ分析] に移動して、次のインジケータを表示します。

- ポート割り当ての失敗
- デフォルトのルート設定なし
- IP の競合
- VRID の競合
- VLAN の不一致
- TCP スモールウィンドウ攻撃
- GSLB サイト名の不一致

詳しくは、「インフラストラクチャ分析」を参照してください。

[NSADM-30188]

解決された問題

システム

イベントサブシステムのスレッド数が 15 を超えると、Citrix ADM は Syslogs を処理できません。このリリースでは、スレッド制限が 20 に増加しました。

[NSADM-39518]

2019 年 **7** 月 **16** 日

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで Citrix ADM 13.0 ビルド 40.24 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

ジョブのスケジューリングを有効または無効にするオプション

インスタンスバックアップ、インスタンス設定監査、インスタンスネットワークレポート、インスタンス SSL 証明書などのスケジューリングジョブを有効または無効にできます。以前は、これらのジョブはデフォルトで有効になっていましたが、無効にするオプションはありません。

スケジュールジョブを有効または無効にするには、Citrix ADM GUI から、［設定］、［システム設定］、［構成可能な機能］の順に選択します。

[NSADM-36650]

Logstream によるパーティションの分析をトランスポートモードとして有効にする

管理対象インスタンスに管理パーティションを作成する場合、管理パーティションごとに別々に Citrix ADM の分析レポートを表示できます。以前の Citrix ADM は、インスタンスの IP アドレスに基づいて統合分析レポートを表示し、**IPFIX** をトランスポートモードとして使用していました。トランスポートモードとして **Logstream** を選択して、管理者パーティションの分析レポートを取得できるようになりました。

> 注
>
> **13.0 36.27** より前のバージョンの Citrix ADC では、**IPFIX** がトランスポートモードのデフォルトのオプションです。**13.0 36.27** より後の Citrix ADC では、トランスポートモードとして［ログストリーム］または［**IPFIX** ］を選択できます。

1. ［ネットワーク］>［インスタンス］**>**［**Citrix ADC**］の順に選択し、インスタンスのタイプを選択します。たとえば、VPX です。
2. 「パーティション」をクリックします。

3. [管理パーティション] ページで、パーティションを選択し、[アクションの選択] リストから [**Analytics** の設定] を選択します。
4. 仮想サーバーを選択し、[アナリティクスを有効にする] をクリックします。
5. **[Analytics** の有効化] ウィンドウで、次の操作を行います。
   a) インサイトタイプの選択 (Web Insight)

   > 注
   >
   > パーティションの場合、Web Insight のみがサポートされます。

   b) 転送モードとして **Logstream** を選択します
   c) 式はデフォルトで true です
   d) [**OK**] をクリックします。

[NSADM-30252]

仮想サーバーライセンスを適用し、単一のワークフローで分析を実現

仮想サーバーのライセンスを取得し、ライセンス取得済みの仮想サーバーで分析を有効にするプロセスが簡素化されました。以前は、仮想サーバーの分析を有効にするには、[ネットワーク] > [インスタンス] **>** [**Citrix ADC**] の順に選択し、仮想サーバーを選択して分析を有効にする必要があります。インスタンスに対して仮想サーバーのライセンスがない場合は、次のようにします。

- まず、[アカウント] > [サブスクリプション] の順に選択して、仮想サーバーのライセンスを取得する必要があります
- 次に、[ネットワーク] > [インスタンス] > [**Citrix ADC**] の順に選択し、仮想サーバーの分析を有効にします。

Citrix ADM では、この二重プロセスを排除し、仮想サーバーのライセンスを取得し、単一のワークフローで分析を適用できます。

詳しくは、「Analytics の有効化」を参照してください。

[NSADM-32893]

複数のデータセンターにまたがるプール容量ライセンスのサポート

ライセンスプールを複数のデータセンターで共有できるようになりました。Citrix ADM に追加されたプールライセンスを使用して、管理対象の Citrix ADC インスタンスにライセンスを割り当てることができます。

Citrix Cloud アカウントからライセンスを自動インポートするには:

1. [ネットワーク] > [ライセンス] に移動します。
2. [ライセンスファイル] タブで、[ライセンスファイルを追加] をクリックします。
3. [ライセンスアクセスコードを使用] オプションを選択します。

4. [ライセンスの取得] をクリックします。
5. リストから製品を選択します。
6. [**Download**] をクリックします。

詳しくは、「プール容量を構成する」を参照してください。

[NSADM-36695]

ユーザーへの有効化/無効化パーミッションの付与

ユーザー定義のアクセスポリシーは、ユーザー、グループ、またはロールに適用できます。これらのポリシーでは、Citrix ADM 機能に対するユーザー権限を定義できます。

このリリースでは、**Enable-Disable** オプションは、有効または無効のアクションを許可する ネットワーク機能にのみ追加されています。この権限では、[今すぐポーリング] アクションを実行することもできます。

ユーザーに **Enable-Disable** パーミッションを付与すると、表示権限も付与されます。このオプションの選択を解除することはできません。機能の「有効/無効化」アクセス許可を付与するには、「Citrix ADM でのアクセスポリシーの構成」を参照してください。

> 注
>
> アップグレード前に、機能に対する編集権限が付与されている場合は、有効化/無効化および表示権限も付与されます。自動選択オプションの選択を解除することはできません。

[NSADM-37684, NSHELP-18635]

Citrix ADM での **Citrix ADC BLX** インスタンスの追加サポート

Citrix ADC BLX アプライアンスは軽量ソフトウェアパッケージで、使用するサーバーハードウェア上で動作します。これで、Citrix ADM を使用して、Citrix ADC BLX インスタンスを管理できます。詳細については、インスタンスの追加およびプール容量を構成するを参照してください。

[NSADM-29983]

RBAC ユーザーに対するアプリケーションベースの認証の簡素化

Citrix ADM では、管理者として、必要なアプリケーションの他の管理者を、必ずしもインスタンスを選択しなくても、承認できるようになりました。以前は、インスタンスを選択してから、それらのインスタンスからアプリケーションを選択する必要がありました。また、アプリケーションがホストされている Citrix ADC インスタンスを管理者が知る必要がない場合もあります。この機能を使用すると、アプリケーションを直接選択できます。

アプリケーションをグループに追加するには

1. [アカウント] > [ユーザー管理] > [グループ] に移動します。

2. [追加] をクリックします。

   「システム・グループの作成」ページが表示されます。

3. [グループ設定] ページで必要な詳細を指定し、[次へ] をクリックします。

4. [承認設定] ページで、[アプリケーションの選択] リストから次のいずれかのオプションを選択します。

   - すべてのアプリケーション: このオプションはデフォルトで選択されています。Citrix ADM に存在するすべてのアプリケーションが追加されます。
   - [選択したインスタンスのすべてのアプリケーション]: このオプションは、[すべてのインスタンス] カテゴリからインスタンスを選択した場合にのみ表示されます。これは、インスタンス上に存在するすべてのアプリケーションを追加します。
   - 特定のアプリケーション: このオプションを使用すると、ユーザーがアクセスする必要なアプリケーションを追加できます。「アプリケーションの追加」をクリックし、リストから必要なアプリケーションを選択します。

5. [**Create Group**] をクリックします。

   詳しくは、「Citrix ADM でのグループの構成」を参照してください。

[NSADM-37213]

ホスト名をクリックして、**Citrix ADC** インスタンス **GUI** にアクセスします

以前は、IP アドレスのみを使用して GUI にアクセスできました。これで、インスタンスのホスト名または IP アドレスをクリックすると、Citrix ADM から Citrix ADC インスタンスの GUI にアクセスできます。

詳しくは、「インスタンスの追加」を参照してください。

[NSADM-37503]

フィルタを使用した **syslog** メッセージと監査ログメッセージの検索

これで、フィルタを使用して syslog メッセージと監査ログメッセージを検索し、結果を絞り込み、探しているものを正確に見つけることができます。新しいフィルタカテゴリは、インスタンス、モジュール、イベント、重大度、およびメッセージで、syslog メッセージと監査ログメッセージの両方で同じです。

Syslog メッセージを検索するには、ADM GUI から、[ネットワーク] > [イベント] > [**Syslog** メッセージ] に移動します。

監査ログメッセージを検索するには、ADM GUI から [アカウント] > [監査ログメッセージ] に移動します。

検索方法の詳細については、「syslog メッセージの表示とエクスポート」を参照してください。

[NSADM-25835]

エンティティの自動検出

Citrix ADM で構成された Citrix ADC インスタンスにエンティティを追加すると、そのエンティティは 10 分以内に ADM に自動的に表示されます。また、エンティティの変更はすぐに ADM に反映されます。

この機能を使用するには、ADM を介して ADC インスタンスで SNMP を有効にする必要があります。SNMP を有効にするには、ADM GUI から［ネットワーク］>［インスタンス］**>**［**Citrix ADC**］の順に移動します。インスタンスを選択し、[**Select Action**] メニューの [**SNMP** の設定] をクリックします。

また、Citrix ADC インスタンスで仮想サーバーを一括構成した場合、一部の仮想サーバーは 10 分以内に自動的に表示されます。他の仮想サーバーが表示されるまでに時間がかかることがあります (最大 20 分)。

[NSADM-23622]

クラウドで **Citrix ADC** インスタンスをプロビジョニングするための新しいタブ

これで、Citrix ADM GUI で [プロビジョニング] をクリックすると、Microsoft Azure クラウドと AWS クラウドで Citrix ADC VPX インスタンスをすばやくプロビジョニングできます。［ネットワーク］>［インスタンス］**>**［**Citrix ADC**］の順に選択し、［プロビジョニング］オプションを表示します。以前は、プロビジョニングオプションは **[**アクションの選択**]** リストにネストされていました。プロビジョニングを解除するには、インスタンスを選択し、[プロビジョニング解除] をクリックします。

詳しくは、次のトピックを参照してください:

AWS での Citrix ADC VPX インスタンスのプロビジョニング

Microsoft Azure での Citrix ADC VPX インスタンスのプロビジョニング

[NSADM-38057]

エージェント列とサイトの列

［ネットワーク］**>**［インスタンス］**>**［**Citrix ADC**］の順に選択し、インスタンスを表示するときに、サイトとエージェントの情報を表示できるようになりました。

[NSADM-38057]

解決された問題

ネットワーク

- Citrix ADM 遅延値は 0 ミリ秒と表示され、これは 1 ミリ秒未満に変更されました。

[NSADM-38207]

- Citrix ADM は、CPX インスタンスを MPX インスタンスとして検出しました。この問題は修正されました。

[NSADM-37725]

- エージェントで`masd`再起動コマンドが失敗しました。この問題は修正されました。

[NSADM-37447]

設定

- アクセス制御ダッシュボードには、Citrix ADM サービスのサブスクリプションの有効期限が切れた後の期間のデータは表示されません。この問題は、アクセス制御サービスのサブスクリプションも持っている場合に発生します。

[NSADM-37827]

2019 年 **7** 月 **02** 日

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで、Citrix ADM 13.0 ビルド 39.14 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

バックアップファイルを外部システムに転送する

予防措置として、バックアップファイルのコピーを別のシステムに転送できます。構成を復元する場合は、まずバックアップファイルを Citrix ADM サーバーにアップロードしてから、復元操作を実行する必要があります。

Citrix ADM バックアップファイルを転送するには:

1. ［ネットワーク］**>**［インスタンス］**>**［**Citrix ADC** ］の順に選択し、インスタンスタイプを選択します。たとえば、VPX です。
2. インスタンスを選択し、**[**アクションの選択**]** リストから [バックアップ**/**復元] を選択します。
3. バックアップファイルを選択し、[転送] をクリックします。

   [バックアップファイルの転送] ページが表示されます。次のパラメータを指定します。

   a) サーバ：バックアップファイルを転送するシステムの IP アドレス。

   b) ユーザー名とパスワード：バックアップ・ファイルのコピー先となる新しいシステムのユーザー資格情報。

   c) **Port** ： ファイルの転送先となるシステムのポート番号。

   d) 転送プロトコル：バックアップファイルの転送に使用されるプロトコル。バックアップファイルを転送するには、SCP、SFTP、または FTP プロトコルを選択できます。

   e) ディレクトリパス：バックアップファイルが新しいシステム上で転送される場所。

4. [**OK**] をクリックします。

[NSADM-31702]

ライセンスタイプの名前の変更

次のライセンスタイプの名前が変更されます。

既存のライセンス名	新しいライセンス名
標準	Standard（変更なし）
Enterprise	詳細設定
Platinum	Premium

[NSADM-36694]

インストールされた **SSL** 証明書を更新し、**CSR** を作成する

これで、インストールされた SSL 証明書を更新し、証明書署名要求 (CSR) を作成できます。

- インストールされた証明書を更新する

認証局（CA）から更新された証明書を受け取った後、Citrix ADM から既存の証明書を更新できます。各 Citrix ADC インスタンスにログオンする必要はありません。
Citrix ADM から SSL 証明書、キー、またはその両方を更新するには:

1. [ネットワーク**] > [SSL** ダッシュボード] に移動します。
2. いずれかのグラフをクリックして、SSL 証明書の一覧を表示します。
3. [SSL 証明書] ページで、証明書を選択し、[更新] をクリックします。または、**SSL** 証明書をクリックして詳細を表示し、[SSL 証明書] ページの右上隅にある [更新] をクリックします。
4. [**SSL** 証明書の更新] ページで、要件に応じて証明書、キー、またはその両方を変更し、[**OK**] をクリックします。

- **CSR** を作成する

証明書署名要求 (CSR) は、証明書が使用されているサーバーで生成される暗号化されたテキストのブロックです。これには、組織名、共通名 (ドメイン名)、地域、国など、証明書に含まれる情報が含まれています。

Citrix ADM を使用して CSR を作成するには:

1. [ネットワーク**] > [SSL** ダッシュボード] に移動します。
2. グラフのいずれかをクリックして、インストールされている SSL 証明書のリストを表示し、CSR を作成する証明書を選択し、**[Select Action]** リストから **[Create CSR]** を選択します。

3. [**Create Certificate Signing Request (CSR)**] ページで、CSR の名前を指定します。
4. 次のいずれかを行います:
   a) キーのアップロード: キーファイルをアップロードするには、[ローカル]（ローカルマシン）または [アプライアンス]（キーファイルが Citrix ADM 仮想インスタンスに存在する必要があります）を選択します。
   b) キーを作成する -次のパラメータを指定します。

暗号化アルゴリズム	キーのタイプ（RSA など）
キーファイル名	RSA キーが保存されたファイル名。
キーサイズ	キーサイズ（ビット）。
公開指数値	表示されたリストから [3] または [F4] を選択します。この値は、RSA キーを作成するのに必要な暗号アルゴリズムの一部です。
キーの形式	デフォルトでは PEM が選択されています。SSL 証明書には、PEM が推奨されるキーの形式です。
PEM エンコーディングアルゴリズム	リストから、生成された RSA キーの暗号化に使用するアルゴリズム（DES または DES3）を選択します。このアルゴリズムを選択する場合は、PEM パスフレーズを指定する必要があります。
PEM パスフレーズ	「PEM エンコーディングアルゴリズム」を選択した場合は、パスフレーズを入力します。
PEM パスフレーズの確認	PEM パスフレーズを確認します。

5. [続行] をクリックします。
6. 次のページで、詳細を入力します。デフォルト値を変更せずに CSR を作成する場合は、[**Continue**] をクリックします。

> 注
>
> 大半のフィールドには、選択した証明書のサブジェクトから抽出したデフォルト値が設定されます。サブジェクトには、共通名、組織名、州、国などの詳細が含まれています。
>
> ほとんどの CA が電子メールによる証明書の送信を受け付けています。CA から CSR を送信した電子メールアドレスに、有効な証明書が送信されます。

[NSADM-37278]

Citrix ADM 分析の新しい洞察

Citrix ADM の［分析］で次のインサイトを表示できるようになりました。

- Video Insight
- TCP Insight
- WAN Insight
- SSL フォワードプロキシ分析

[NSADM-36692]

AWS と **Azure** で高可用性モードでの **Citrix ADC** インスタンスのプロビジョニング

これで、Citrix ADM を使用して、AWS および Microsoft Azure クラウドの高可用性モードで Citrix ADC インスタンスをプロビジョニングしました。
展開するには、次の手順を実行します。

1. [ネットワーク**] > [**インスタンス**] > [Citrix ADC**] に移動します。
2. **VPX** で、「アクションの選択」をクリックし、「パブリッククラウドでのプロビジョニング」を選択します。
3. ［**Citrix ADC VPX** のプロビジョニング］ページで、Citrix ADC VPX インスタンスをプロビジョニングするクラウドサービスを選択します。
4. **[**基本パラメータ**]** で、**[** インスタンスのタイプ**]** リストから **[HA]** を選択します。
5. 次のオプションから [**Zone]** タイプを選択します。
   - 単一ゾーン：このオプションは、Citrix ADC VPX インスタンスを同じゾーンに展開します。
   - マルチゾーン：このオプションは、Citrix ADC VPX インスタンスを複数のゾーンに展開します。クラウド上に作成される各ゾーンについて、**[**クラウドパラメータ**]** でネットワークの詳細を指定します。

   詳しくは、AWS での Citrix ADC VPX のプロビジョニングまたはMicrosoft Azure で Citrix ADC VPX をプロビジョニングするを参照してください。

[NSADM-31108、NSADM-30099]

Citrix ADM から **Citrix ADC** インスタンスを表示する新しいオプションフィールド

Citrix ADM から Citrix ADC インスタンスを表示するために、次の新しいオプションフィールドが追加されました。これらのフィールドを選択するには、［**Citrix ADM GUI**］**>** ［ネットワーク］**>** ［インスタンス］**>** ［**Citrix ADC**］の順に選択し、［設定］アイコンをクリックします。

- HA マスターの状態
- HA 同期の状態
- 管理プロファイル
- 状況

- アップタイム
- モデル ID
- パケットエンジン
- SSL カード
- CPU
- ハードウェアバージョン
- LOM バージョン
- ホスト ID
- シリアル番号
- エンコードされたシリアル番号
- UUID

次に、設定アイコンと新しいフィールドが強調表示されている例を示します。

[NSHELP-6170]

解決された問題

ネットワーク

- Citrix ADM を使用して Citrix ADC SDX インスタンスをアップグレードしようとすると、アップグレードが失敗し、次のエラーメッセージが表示されます。

  ```
  "SCP: Unable to open a session on <IP address of the SDX instance>.
  Agent id not found"
  ```

  [NSHELP-19767]

- 同じリージョンに複数の AutoScale グループを作成すると、そのような AutoScale グループのアプリケーション展開が失敗することがあります。この問題は、これらの AutoScale グループのトラフィック分散モードとして ALB を選択するときに発生します。

  [NSLB-4934]

システム

- Citrix ADM スーパー管理者が Citrix Cloud から他のユーザーを招待した場合、招待されたユーザーのデフォルトの権限は管理者です（ユーザー管理を除く）。（ユーザー管理を表示するには、**Citrix ADM GUI >** ［システム］**>** ［ユーザー管理］に移動します）。以前は、既定のアクセス許可は読み取り専用でした。詳しくは、「ロールベースのアクセス制御の設定」を参照してください。

  [NSADM-37914]

2019 年 6 月 19 日

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで Citrix ADM 13.0 ビルド 38.20 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

[GSLB サービスグループ**]** タブ

Citrix ADM GUI の［ネットワーク］>［ネットワーク機能］>［**GSLB**］の下に［サービスグループ］タブが表示されるようになりました。
このタブには、ADM で検出されたインスタンスのすべてのサービスグループが表示されます。[**Service Groups]** タブを使用すると、サービスグループエンティティの有効化と無効化、そのエンティティにバインドされているメンバーと仮想サーバーの確認などのタスクを実行できます。また、エンティティをポーリングして最新のステータスを取得することもできます。

2019 年 5 月 31 日

Citrix アプリケーションデリバリーマネージャー（ADM）エージェントは、デフォルトで Citrix ADM 13.0 ビルド 37.26 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

インフラストラクチャ分析 ― 概要パネル

これで、［概要］パネルに、**SSL** 構成および構成の偏差に関する Citrix ADC インスタンス統計を表示できます。

- **SSL** 設定 — SSL 証明書がインストールされたインスタンスを表示します。
  - 発行者：非推奨 -Citrix 証明書の発行者は推奨しません。
  - アルゴリズム：非推奨 -ADC インスタンスにインストールされている SSL 証明書の署名アルゴリズムが Citrix 標準を満たしていません。
  - キー強度：非推奨 -SSL 証明書のキー強度が Citrix 標準を満たしていません。
- [**Config Deviation**] — 次の設定の偏差があるインスタンスのリストを表示します。
  - 保存済みと実行中 -インスタンスに保存された設定と、同じインスタンス上で現在実行されている設定の違い。

- 実行とテンプレート-テンプレートと実行中テンプレートには、保存されたテンプレートと実行中以外のすべてのテンプレートが含まれます。

[NSADM-24161]

Citrix ADM での署名ルールの通知

署名ベースの脅威は、割り当てられたシグニチャに基づく既知の脅威の検出を示します。Citrix ADC Web AppFirewall に署名オブジェクトを追加するたびに、Citrix ADM は電子メール、slack、PagerDuty、イベントメッセージ、およびセキュリティインサイトを通じて通知を送信します。詳しくは、「署名」を参照してください。

Citrix ADM でイベントルールを作成すると、**AppfwNewSignatuReadded** という新しいカテゴリを表示できるようになりました。Citrix ADC Web AppFirewall に追加された新しい署名オブジェクトの通知を有効にするには、イベントルールを作成します。

1. [ネットワーク] > [イベント] > [ルール] に移動し、[追加] をクリックします。
2. カテゴリパネルで、検索バーに`signature`と入力し、「**AppFWNewSignatureDed**」を選択します。
3. イベントルールを作成するには、「イベントルールの作成」を参照してください。

イベントルールの作成後、設定されたイベントルールのアクションに基づいて通知を受け取ります。通知を表示するには:

- [ネットワーク] > [イベント] > [イベントメッセージ] に移動します。
- [分析] > [**Security Insight**] に移動し、署名通知を表示するインスタンスを選択します。

  シグニチャ通知は、[イベント履歴] タブに表示されます。

[NSADM-34153]

StyleBooks へのラベルの追加をサポート

Citrix ADM で任意の StyleBook にラベルを追加できるようになりました。ラベルはキーと値のペアで、異なる基準を使用して StyleBook をグループ化できます。Citrix ADM で StyleBooks を検索またはフィルタリングするときに、これらのラベルを使用できます。詳しくは、「スタイルブックのラベルを作成する」を参照してください。

[NSADM-34877]

Microsoft Azure の **Citrix ADM** 自動スケーリングは、トラフィック分散のための **Azure** ロードバランサーをサポート

Microsoft Azure の Citrix ADC インスタンスの自動スケーリングは、次の 2 つのモードのトラフィック分散をサポートしています。

- Azure トラフィックマネージャーを通じて
- Azure ロードバランサー経由で

詳しくは、「Citrix ADM を使用した Microsoft Azure における Citrix ADC VPX の自動スケーリングアーキテクチャ」を参照してください。

[NSADM-33423]

解決された問題

ネットワーク

- 中止された設定ジョブを実行しようとすると、「無効な要求」エラーが表示されることがあります。

  [NSADM-34242]

- ［エージェントの追加］ページで［サイトの接続］オプションを選択すると、Citrix ADM はそのサイトまたはエージェントに属するインスタンスのサイトを更新しません。

  [NSADM-35049]

- インスタンスグループの作成または構成時に、Citrix ADM GUI に、高可用性 Citrix ADC インスタンスの 2 倍の IP アドレスが表示されることがあります。いずれかの IP アドレスを選択すると、両方のインスタンスがインスタンスグループに追加されます。

  この修正は、アップグレード後のインスタンスグループの作成に適用されます。以前に作成したグループについては、重複したエントリをグループから削除する必要があります

  [NSHELP-19176]

設定

Citrix ADM エージェントがアプリケーションサーバーから正しい時刻値を受け取らない場合、分析情報は Citrix ADM に表示されません。

[NSHELP-18898]

2019 年 **4** 月 **25** 日

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで Citrix ADM 13.0 ビルド 36.21 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

デフォルトのランディングページを設定する機能

Citrix Application Delivery Management（ADM）ポータルでは、優先ページをデフォルトのランディングページとして設定できます。既定のランディングページとして設定するタブで、ブックマークアイコンをクリックします。

SSL ダッシュボードをデフォルトのランディング・ページとして設定する例を次に示します。

[NSADM-21938]

Citrix ADM エージェント用のテクニカルサポートファイルを生成する

GUI から、選択した Citrix ADM エージェントのテクニカルサポートファイルを生成できます。また、このファイルをダウンロードして Citrix テクニカルサポートに送信して、調査とトラブルシューティングを行うこともできます。

[NSADM-30238]

インフラストラクチャ分析ダッシュボードの改善

インフラストラクチャ分析ダッシュボードが更新され、主題の変更が反映され、テーブル列も読みやすくなるようにサイズが変更されました。これで、ホスト名をクリックして、インスタンス化されたダッシュボード内のインスタンスにナビゲートできます。UI には、インフラストラクチャ分析ダッシュボードを使用するユーザーエクスペリエンスが向上する、いくつかのマイナーな更新もあります。

[NSADM-30191]

解決された問題

Analytics

- 「**HDX Insight** 」>「ユーザー」では、「現在のセッション」テーブルで選択したセッションに、「現在のセッション」テーブルに表示される IP アドレスとは異なるクライアント IP アドレスが表示されます。

  [NSHELP-6395, TSK0715071]

アプリケーション

- 特定のケースでは、複数の仮想サーバーに対して AppFlow を有効にすると、Citrix ADM GUI が応答しなくなります。この問題は、通常、TCP を含む複数の種類の負荷分散サーバーを選択し、TCP がリストの先頭にある場合に発生します。

  回避策:「サービスタイプ」列を昇順でソートします。したがって、TCP の種類は、リストの一番下に移動し、AppFlow を有効にします。

  [NSADM-35039]

- 現在、Citrix ADM から送信された電子メールには、違反したしきい値が含まれていません。

  [NSHELP-6093]

ネットワーク

- [種類] 検索条件を使用して構成テンプレートを検索すると、Citrix ADM では [True] または [False] と表示されます。「True = デフォルト設定テンプレート」と「False = カスタム構成テンプレート」ことに注意してください。それに応じて選択する必要があります。

  [NSADM-34802]

- [Suppress Action] を使用してイベントルールを作成すると、エージェントを介して検出されたインスタンスについては、スケジュールされた時間が経過してもイベントが抑制されます。

  [NSADM-35023]

- Slack チャンネルにレポートを送信している間、Slack プロファイルは Config Job モジュールに表示されません。

  [NSADM-35079]

- パーティションを持つ Citrix ADC VPX を Citrix SDX から削除すると、ADC VPX は Citrix ADM から削除されますが、パーティションは保持されます。

  [NSADM-34829]

2019 年 **4** 月 **04** 日

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで Citrix ADM 13.0 ビルド 35.17 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

設定ジョブを中止する場合の **UI** の強化

[エラーを無視して続行] アクションの [中止] オプションが削除されました。コマンド失敗実行モードの [エラーを無視して続行] オプションを選択すると、実行中の構成ジョブを中止できません。

[NSADM-32836]

Citrix ADM テーブルの列でソートの種類を表示する機能

Citrix ADM デフォルトビューでは、列を必要な順序で並べ替えることができますが、列ヘッダーにレコードが昇順または降順のどちらで配置されているかを示すインジケータが表示されるようになりました。この変更は、該当する Citrix ADM ページに適用されます。

[NSADM-21463]

Citrix ADM GUI でのテーマの変更

Citrix ADM GUI が更新され、いくつかのページでテーマが変更されました。確認ウィンドウとエラーウィンドウには、新しいカラーテーマと一連の新しいフォントが表示されます。

[NSADM-22535]

解決された問題

Analytics

- [ユーザー] > [トランザクション] に移動すると、0.1 万を超えるトランザクションのトランザクションレポートが表示されない場合があります。

  [NSHELP-18785]

- Citrix ADM が同じ名前の 2 つの Citrix ADC ゲートウェイを管理する場合、Citrix ADM は、これらの Citrix ADC ゲートウェイに属するセッションを区別できません。

  [NSHELP-18716]

- Citrix ADC の高可用性ペアで構成されたアプリケーションのアプリケーションの概要パネルに、アプリケーションダッシュボードに適切なメトリックが表示されない。

  [NSHELP-18733]

- アプリケーションダッシュボードでは、文字列の長さが長いと、データボリュームなどの一部の文字が正しく表示されません。

  [NSADM-31818]

- ノードからの CPU とメモリの情報がすべての仮想サーバーに追加されないため、アプリケーションダッシュボードに正しいデータが表示されません。

  [NSHELP-18736]

- AppFlow は、キャッシュリダイレクト仮想サーバーではサポートされていません。したがって、Citrix ADM で CR 仮想サーバーの「AppFlow を有効にする」オプションは削除されます。

  [NSHELP-18817]

ライセンス

- Citrix ADM は、ライセンスサーバーとして構成されている場合、ライセンスポート構成を読み取れません。

  [NSADM-33966]

システム

- 既定のビューでは、列を必要な順序で並べ替えたときに、並べ替えが昇順または降順のどちらであるかを示すインジケータが列に表示されません。レコードが昇順または降順のどちらに配置されているかを示すインジケーターが提供されるようになりました。この変更は、該当する Citrix ADM ページに適用されます。

  [NSHELP-18647]

2019 年 **4** 月 **01** 日

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで、Citrix ADM 13.0 ビルド 34.25 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

ADM で **Citrix SDX** インスタンスのネットワークレポートを生成するためのサポート

Citrix ADM では、グローバルレベルのインスタンスだけでなく、仮想サーバーやネットワークインターフェイスなどのエンティティについてもレポートを生成できます。インスタンスファミリーは、Citrix ADC、Citrix SDX、および Citrix SD-WAN インスタンスで構成されます。

[NSADM-25092]

インスタンスを選択せずに **StyleBooks** を使用して構成パックを作成するサポート

Citrix ADM では、インスタンスを選択せずに、StyleBooks を使用して構成パックを作成できます。その後、構成をデプロイするターゲットインスタンスを選択して、後で構成パックを更新できます。この機能を使用すると、インスタンスにアクセスできない場合でも、アプリケーション用の設定パックを作成できます。

[NSADM-25552]

Microsoft Azure の **Citrix ADM** 自動スケーリングは、**Azure** トラフィックマネージャを使用して **DNS** トラフィックのみをサポートします

> 注:
>
> この機能は現在プレビュー中です。

Citrix ADM 自動スケーリングは、ネットワークリソースの実際の使用状況に応じて、Azure の Citrix ADC クラスターノードを追加または削除します。Citrix ADM は、AutoScale プロビジョニングされたクラスターから統計（CPU 使用率、メモリ使用率、スループット）を収集します。これらの統計情報は、カスタマーが設定したしきい値に対して評価されます。スケールインまたはスケールアウトは、統計情報が最大しきい値を超えているか、最小しきい値を下回っているかに応じてトリガーされます。

自動スケーリング機能の利点は次のとおりです。

- トラフィック要求に関係なく、アプリケーションが常に起動し、実行されていることを確認します。
- Citrix ADC インスタンスは動的に追加および削除され、ゼロタッチ手動構成になります。
- DNS 管理は自動で行われます。
- コスト管理を向上させます。

Microsoft Azure のオートスケーリングは、Azure トラフィックマネージャを使用して、DNS トラフィックのみをサポートしています。

> 注
>
> 現在、ALB を使用したトラフィック分散はサポートされていません。

AutoScale 機能を使用するには、StyleBooks を使用して AutoScale グループを作成し、アプリケーションをデプロイする必要があります。このリリースでは、Microsoft Azure 仮想マシンスケールセットでのアプリケーションの自動スケーリングがサポートされています。詳細については、「AutoScale グループのアプリケーションを構成する」を参照してください。

[NSADM-31259]

Citrix ADM ユーザーインターフェイスエクスペリエンスの向上

このリリースでは、Citrix ADM ポータルのユーザーインターフェイスエクスペリエンスが向上します。このような UI の変更のハイライトを次に示します。

LOM バージョンは、Citrix ADC SDX アプライアンスのみに適用されます。したがって、［インスタンスダッシュボード］ページでは、Citrix ADC SDX アプライアンスの LOM バージョンのみが表示されます。

[フィルタの抑制] ボタンは、[Syslog メッセージ] ページに表示されます。以前は、このオプションは左側のナビゲーションの Syslog メッセージの下に表示されていました。

[NSADM-32322]

時間に基づいてデータを表示する **GUI** の機能強化

時間間隔リストを使用し、期間を選択して、アプリケーション分析とイベントレポートの詳細を表示できるようになりました。

[NSADM-22529]

Citrix ADM での **PagerDuty** サポート

以前の Citrix ADM GUI では、メール、SMS、Slack を使用して通知を送信できます。PagerDuty で行った設定に基づいて PagerDuty に通知を送信できるようになりました。PagerDuty では、電子メール、SMS、プッシュ通知、登録番号への電話などの通知を設定できます。

PagerDuty プロファイルをオプションの 1 つとして選択して、次の機能に関する通知を受け取ることができます。

- イベント — Citrix ADC インスタンスに対して生成されるイベントのリスト。
- [Licenses]：現在アクティブで、期限切れが近づいているなどのライセンスのリスト。
- 「SSL 証明書」— 現在アクティブな、有効期限が近い、など、SSL 証明書のリスト。

Citrix ADM で PagerDuty プロファイルを追加する前に、PagerDuty で必要な構成が完了していることを確認してください。詳しくは、「ページデューティのドキュメント」を参照してください。

[NSADM-25940]

解決された問題

Analytics

- キャッシュリダイレクト仮想サーバーの AppFlow を有効にすると、エラーメッセージが表示され、その仮想サーバーに対して AppFlow を有効にできないことがあります。

  [NSHELP-18817]

アプリケーション

- アプリケーションダッシュボード情報パネルとアプリケーション詳細ダッシュボードページで、「トランザクション」タイトルの下のデータが異なって表示されていました。これは、1 つの場所の累積データであり、他の場所での取引率でした。今回の修正により、データはトランザクション合計として正しく表示されるようになり、[Key Metric Trends] セクションに 1 秒あたりのトランザクションが表示されます。

  [NSHELP-18799]

ネットワーク

- ADM サービスエージェントが CPX 自動登録要求を許可していないため、Citrix ADM で CPX 登録に失敗することがあります。

  [NSADM-33020]

- 既存の SSL 証明書を更新する場合は、[ネットワーク] > [**SSL** ダッシュボード] に移動します。SSL ダッシュボードには、Citrix ADC SSL 証明書、SSL 仮想サーバー、SSL プロトコルの詳細が表示されます。SSL 証明書、SSL 仮想サーバー、または SSL プロトコルに関連する詳細を表示するには、[合計] 証明書リンクをクリックします。これで、証明書を選択して [更新] をクリックしたときに、更新する証明書の形式を指定する必要はありません。Citrix ADM は、以前にアップロードした証明書ファイルから形式を取得できるようになりました。

  [NSHELP-18763]

システム

- [システム] > [イベント] に移動してイベントを選択し、[履歴] をクリックすると、[イベント履歴] にはメインの [イベント] 画面が表示され、そのイベントの予想される履歴は表示されません。[Events History] ページを閉じて選択を繰り返して、そのイベントの正しい履歴を表示する必要があります。この問題は修正されました。

  [NSHELP-18651]

- 特殊文字を使用して Citrix ADM テーブルを検索できませんでした。ADM では、$、&、’ などの特殊文字を使用して検索できるようになりました。

  [NSHELP-5927]

2019 年 **2** 月 **28** 日

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで Citrix ADM 13.0 ビルド 33.23 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

Microsoft Azure にデプロイされた **Citrix ADC** インスタンスの自動スケーリングのサポート

> 注:
>
> この機能はプレビューです。

Citrix ADM 自動スケーリング機能は、Microsoft Azure の Citrix ADC インスタンスのスケーリングをサポートするようになりました。Citrix ADM 自動スケーリング機能は、ネットワークリソースの実際の使用状況に応じて、Azure にデプロイされた Citrix ADC クラスターノードを追加または削除します。Citrix ADM は、AutoScale プロビジョニングされたクラスターから統計（CPU 使用率、メモリ使用率、スループット）を収集します。これらの統計情報は、カスタマーが設定したしきい値に対して評価されます。統計が最大しきい値を超えるか、最小しきい値を下回っているかによって、スケールインまたはスケールアウトがトリガーされます。

自動スケーリング機能の利点は次のとおりです。

- トラフィック要求に関係なく、アプリケーションが常に起動し、実行されていることを確認します。
- Citrix ADC インスタンスは動的に追加および削除され、ゼロタッチ手動構成になります。
- DNS 管理は自動で行われます。
- コスト管理を向上させます。

Microsoft のオートスケーリングでは、次の 2 つのモードのトラフィック分散がサポートされています。

- Azure トラフィックマネージャーを通じて
- Azure ロードバランサー経由で

AutoScale 機能を使用するには、StyleBooks を使用して AutoScale グループを作成し、アプリケーションをデプロイする必要があります。

> 注:
>
> バックエンド AutoScale は、この Citrix ADM バージョンではサポートされていません。

[NSADM-24780]

ライセンス仮想サーバーページでの分析の有効化表示のサポート

Citrix ADM で、分析が有効になっている仮想サーバーの一覧が表示されるようになりました。[ネットワーク] > [ライセンス] に移動し、[ライセンスされた仮想サーバー] セクションで、ボタンをクリックして、ライセンスを取得する仮想サーバーを選択します。仮想サーバのタイプを選択し、［ライセンス］ タブを選択します。[**AppFlow Logging**] 列には、仮想サーバーで有効になっている分析が表示されます。

[NSADM-25857]

［ライセンス仮想サーバ］ ページにすべての仮想サーバの統合表示

Citrix ADM では、ネットワーク内のすべての仮想サーバーの統合ビューが表示されるようになりました。これで、[ネットワーク] > [ライセンス] に移動し、[ライセンスされた仮想サーバー] セクションで、ボタンをクリックしてライセンスを取得する仮想サーバーを選択できます。[ライセンス仮想サーバー] ページには、[すべての仮想サーバー] タブが表示されます。このタブには、負荷分散、コンテンツスイッチング、またはその他の仮想サーバーの種類に関係なく、すべての仮想サーバーが表示されます。必要な仮想サーバを選択し、そのサーバにライセンスを適用できます。

[NSADM-25194]

インフラストラクチャ分析ページからインスタンスの詳細を表示するサポート

Citrix ADM インフラストラクチャ分析機能は、インスタンスで問題を引き起こした、または引き起こす可能性のある要因を視覚化するのに役立ちます。これで、表形式のビューでインスタンスの IP アドレスをクリックすると、そのインスタンスの詳細をダッシュボードとして表示できます。インスタンスダッシュボードには、インスタンスの概要が表示され、インスタンスの CPU、メモリ、ディスク使用量を確認できます。SSL 証明書管理、設定監査、ネットワーク機能、およびインスタンスの詳細なネットワーク使用状況を示すネットワークレポートに関連する詳細も確認できます。

[NSADM-30194]

解決された問題

Analytics

- ADC インスタンスでの分析の設定時に、仮想サーバーの詳細を検索してから検索をキャンセルすると、ADM は他の ADC インスタンスからの仮想サーバーも一覧表示されることがあります。

[NSHELP-18623]

- 「読み取り専用」権限を持つユーザーの場合、診断関連のアイコンはどのアナリティクスページにも表示されません。

  [NSHELP-6407]

- Citrix ADM で SD-WAN WO インスタンスの AppFlow ow を構成すると、サービスエージェントの IP アドレスはコレクタ IP アドレスとして構成されません。この修正により、エージェントは SD-WAN WO インスタンスから AppFlow データを受信するように構成されています。

  [NSADM-32565]

ハイブリッドクラウドとマルチクラウド

- **AWS AutoScale**: Citrix ADC リリース 12.1 ビルド 51.16 イメージを使用して、AutoScale グループを作成できます。

ネットワーク

- [ネットワーク] > [構成監査] で、[構成変更による上位 10 インスタンス] セクションでインスタンスをクリックすると、ADM がそのインスタンスのデータが表示されない場合があります。また、「毎日」などの特定の期間を選択し、「構成変更による上位 10 インスタンス」セクションでインスタンスを選択すると、ADM は異なる期間のデータが表示されることがあります。

  [NSHELP-18452]

- [ネットワーク] > [構成の監査] に移動するときのシナリオを検討します。「構成変更による上位 10 インスタンス」セクションで、ADC の上にマウスを置いたときに、ツールチップに完全な ADC 情報が表示されないことがあります。これは、ツールチップで表示できる文字数の制限によるものです。

  [NSHELP-18470]

- Citrix ADM は、ADC インスタンスから受信した SNMPv3 パケットを断続的に処理できません。このエラーは、Citrix ADC インスタンスまたは Citrix ADM 自体をアップグレードした後、または ADC インスタンスを再起動した後に発生する可能性があります。このような障害は、他のメモリ割り当てに無効なメモリ (解放されたメモリ) が使用されているために発生します。

  [NSHELP-5880]

システム

- この問題は、Citrix ADM リリース 12.1 ビルド 50.28 にアップグレードした後に発生します。[システム] > [ユーザ管理] > [グループ] に移動し、ユーザグループを作成することを検討します。そこで、まず [**Authorization**] タブのすべてのオプションの選択を解除し、手動でいくつかのインスタンスを選択し、グ

ループの作成を完了します。後で同じグループを編集して [**Authorization**] タブを選択すると、インスタンスは表示されなくなります。

[NSHELP-18442]

- 次の 2 つのシナリオでは、ユーザーグループに GSLB 仮想サーバーを追加できないことがあります。
  1. グループの作成中:GSLB 仮想サーバーの既存のリストに、さらにいくつかの GSLB 仮想サーバーを追加しようとすると。
  2. 既存のグループの編集中：GSLB 仮想サーバーの一覧をすでに持っている既存のグループに GSLB サーバーを追加しようとすると。

[NSHELP-18152]

2019 年 **2** 月 **8** 日

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで Citrix ADM 13.0 ビルド 32.32 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

このリリースは、以前の Citrix ADM 13.0 ビルド 32.30 リリースに対する拡張機能です。このリリースでは、Citrix ADM パフォーマンスをさらに強化するために、プラットフォームと分析を含むさまざまな改善が行われました。

2019 年 **1** 月 **28** 日

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで、Citrix ADM 13.0 ビルド 32.30 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

AutoScale ダッシュボード上のすべてのアクティブノードの表示をサポート

Citrix ADM は、AWS で作成されたクラスターのすべてのアクティブノードの表示をサポートするようになりました。アベイラビリティーゾーンに含まれるアクティブなノードの数は、いつでも表示できます。詳しくは、「Autoscale ダッシュボード」を参照してください。

[NSADM-25785]

ネットワークレポートダッシュボードのエクスポートのサポート

ネットワークレポートダッシュボードページのエクスポートは、定期的にスケジュールできます。たとえば、過去 1 時間のダッシュボードレポートを毎週生成するオプションを設定できます。レポートは、現在のダッシュボードに基

づいていない、ユーザーが設定した時刻と日付スタンプについて毎週生成されました。新しい機能強化では、レポートは設定された時刻と日付スタンプを上書きし、ダッシュボードの状態を表示します。詳しくは、「ネットワークレポートのエクスポート」を参照してください。

[NSADM-20017] 秒

承認されたアプリケーションについてのみインサイトレポートの表示をサポート

Citrix ADM 分析では、仮想 IP アドレスベースの認証がサポートされるようになりました。特定のアプリケーションまたは仮想サーバーのセットに対してユーザーを認証すると、ユーザーは承認されているアプリケーション（仮想サーバー）の分析レポートのみを表示できます。

[NSADM-17971]

Citrix ADM でのレポートのエクスポートのスケジュールをサポート

Citrix ADM は、さまざまなページのレポートのエクスポートのスケジュールをサポートしています。レポートのエクスポートをスケジュールするときに、さまざまなアクションを実行できます。

- レポートの生成とエクスポートを定期的にスケジュールします。
- レポート生成の繰り返し設定を指定し、レポートのエクスポート先のメールプロファイルを作成します。
- 指定した Slack チャンネルにレポートを書き出します。

この拡張機能は、Citrix ADM ソフトウェアにある機能に似ています。

[NSADM-24829]

2019 年 **1** 月 **16** 日

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで Citrix ADM 13.0 ビルド 30.15 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

このリリースでは、パフォーマンスを向上させるために、プラットフォームの改良が行われました。

2019 年 **1** 月 **4** 日

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで Citrix ADM 13.0 ビルド 30.14 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

2018 年 12 月 07 日

このリリースには、機能強化とバグ修正が含まれています。

Citrix Application Delivery Manager（ADM）エージェントは、デフォルトで Citrix ADM 13.0 ビルド 30.14 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

インフラストラクチャ分析

> 注:
>
> この機能は現在プレビューで利用できます。

Citrix ADM インフラストラクチャ分析機能は、Citrix ADC インスタンスから収集されたすべてのデータを、Citrix ADM 上の単一ページで視覚的に表現します。Infrastructure Analytics 機能は、インスタンスで問題が発生した、または発生する可能性のある要因を視覚化するのに役立ちます。この視覚化は、
問題とその再発を防ぐために実行する必要があるアクションを決定するのにも役立ちます。

インフラストラクチャ分析を円パック表示で表示するには、次の手順を実行します。

1. [ネットワーク] > [インフラストラクチャ分析] に移動します。
2. 円パックビューアイコンを選択します。

詳しくは、「インフラストラクチャ分析」を参照してください。

[NSADM-23680]

Citrix ADM と **Citrix Virtual Citrix Director** の統合

Citrix ADM は Citrix Director と統合されました。これにより、Director は［ネットワーク］および［ユーザーの詳細］ページに Citrix ADM からの HDX Insight レポートを表示し、ユーザー、アプリケーション、デスクトップ、インスタンス、ライセンス固有の情報を表示できます。
詳細については、「Citrix ADM と Citrix Virtual Citrix Director の統合」を参照してください。

[NSADM-17085]

SSL 証明書のダウンロードのサポート

これで、［ネットワーク］>［**SSL** ダッシュボード］の順に選択して、**Citrix ADM** から **SSL** 証明書をダウンロードできます。SSL 証明書を選択し、[アクション] リストから [ダウンロード] をクリックします。詳しくは、「SSL 証明書のダウンロード」を参照してください。

[NSADM-19790]

Citrix ADC SDX インスタンスのバックアップと復元のサポート

Citrix ADM から Citrix ADC SDX インスタンスをバックアップおよび復元できるようになりました。詳しくは、「Citrix ADC インスタンスのバックアップと復元」を参照してください。

[NSADM-19882]

解決された問題

アプリケーション

- アプリケーションダッシュボード集約ロジックでは、最新のデータボリューム値は総カウンタとして保持されます。しかし、時には値が高く見られ、最新の値よりもかなり高いことがあります。

  [718359]

2018 年 **11** 月 **19** 日

このリリースには、機能強化とバグ修正が含まれています。

Citrix Application Delivery Manager（Citrix ADM）エージェントは、デフォルトで Citrix ADM 12.1 ビルド 505.130 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

複数の仮想サーバー上で **AppFlow** を構成し、進行状況情報を表示します

複数の仮想サーバーで AppFlow を同時に構成すると、ポップアップウィンドウに AppFlow 構成の進捗状況が表示されます。この情報には、インスタンスレベルで構成されている仮想サーバーの数が表示されます。進行状況情報は、多くの仮想サーバーで AppFlow を構成するときに役立ちます。

> 注:
>
> Citrix ADM は、仮想サーバー上で AppFlow を構成する際に、デフォルトのトランスポートモードとして IPFIX をサポートしています。Citrix ADC 12.0 リリース以降では、Citrix **ADM** はログストリームをサポートするため、必要に応じてログストリームを明示的に選択する必要があります。

Citrix Gateway インスタンスで AppFlow を有効にするときに、トランスポートモードとして ICA または TCP のいずれかを選択してください。両方を選択した場合、ICA は TCP よりも優先されます。ICA または TCP とともに HTTP を選択できます。ADM を使用して AppFlow を有効にする方法の詳細については、「Citrix ADM を使用して AppFlow を有効にする」を参照してください。

解決された問題

Analytics

- 仮想サーバーの名前が 60 文字を超えると、AppFlow アクション名は 128 文字を超えます。このようなアクション名を設定可能にすると、ADC インスタンスが動作しなくなる可能性があります。

  [717663]

- ADC インスタンス上の複数の仮想サーバーに対して AppFlow の設定をクリアするには、より長い時間がかかります。

  [717675]

ネットワーク

- ローカルストレージシステムから Citrix ADM に証明書または証明書キーファイルをアップロードできますが、ADM では「読み取り」権限は保持されません。このようなファイルが ADM によって各 ADC インスタンスにアップロードされると、ADC はそのファイルを無効なファイルとして表示します。

  [716691]

- 不適切な例外処理が原因で、Citrix ADM が Citrix の信頼できるサービスと通信できないことがあります。Citrix ADM サービスにログオンできない場合があります。ADM サービスでも、リソースリークが発生する可能性があります。

  [717571]

- 同じイベントに対応するイベント期間が異なる 2 つのイベントルールを構成すると、Citrix ADM では、イベント経過日数よりも短いルールのみが考慮されます。この修正により、Citrix ADM は両方のイベントルールを考慮しました。

  [716930]

- Syslog メッセージは、Citrix ADM で複数のページに表示されます。キーワードを入力して 1 つのページで Syslog メッセージを検索する場合、別のページに移動しても同じ検索結果は保持されません。同じキーワードを入力して再度検索する必要があります。この修正により、Citrix ADM は検索の結果をすべてのページに表示します。

  [715671]

2018 年 10 月 27 日

このリリースには、機能強化とバグ修正が含まれています。

Citrix Application Delivery Manager（Citrix ADM）エージェントは、デフォルトで Citrix ADM 12.1 ビルド 504.131 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

表示される **Syslog** メッセージの数を制御する機能

デフォルトでは、Citrix ADM は各ページに 50 個の Syslog メッセージを表示します。1 ページあたり 100、250、500、または 1,000 メッセージを選択することで、1 ページに複数のメッセージを表示できるようになりました。

解決された問題

Analytics

- 読み取り専用の権限がある場合、どのアナリティクスビューにも診断アイコンが表示されません。

  [715785]

アプリケーション

- Citrix ADM では、GSLB アプリケーションのトランザクション数とデータフロー量がアプリケーションダッシュボードに表示されません。

  [716878]

- Citrix ADM では、高可用性で展開された ADC インスタンスに作成されたアプリケーションに関連する仮想サーバーの情報は表示されません。

  [716906]

ネットワーク

- Citrix ADM パフォーマンスサブシステムが数時間ごとにクラッシュし、これはネットワークレポートに影響します。

  [715483]

- Citrix ADM パフォーマンスサブシステムは、ネットワークレポートに影響を与える高い CPU 使用率を報告します。

  [716235]

- ASG が複数のアベイラビリティーゾーンにデプロイされている場合、バックエンドサーバーのグレースフル/非グレースフル削除は Amazon EC2 Auto Scaling グループをサポートしない可能性があります。

  [716031]

- 検索オプションに基づいて SSL 証明書をエクスポートすると、検索条件に関係なく、すべての SSL 証明書が CSV レポートに表示されます。

  [714674]

- [ネットワーク] > [イベント] に移動すると、イベントは初めて順序で表示されません。[日付] 列見出しをクリックすると、イベントが時系列順に表示されます。

  [716615]

- Citrix ADM は断続的に、日次レポートのデータポイントの収集を見逃すことがあります。これは、週次レポートと月次レポートに影響します。

  [716778]

システム

- Citrix ADM GUI でファイルを文字列としてソートするのではなく、日付に従ってファイルをソートできるようになりました。

  [715491]

2018 年 **10** 月 **12** 日

このリリースには、機能強化とバグ修正が含まれています。

デフォルトでは、Citrix ADM エージェントは自動的に Citrix ADM 12.1 ビルド 502.127 にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

HDX Insight レポートでの **EDT** セッションのサポート

HDX Insight には、アクティブなセッションレポートの一部として EDT セッションと非 EDT セッションの数が表示されるようになりました。「ユーザー」(Users) テーブルには、システム内のすべてのユーザーの詳細なレポートが表示されます。また、新しいドーナツチャートが導入され、ユーザーが消費した帯域幅と、ユーザが使用するプロトコルのタイプに基づく総バイト数を確認できます。

Web Insight レポートでの負荷分散とコンテンツスイッチングの両方の仮想サーバーの表示のサポート

Web Insight レポートには、コンテンツスイッチング仮想サーバーにバインドされた負荷分散仮想サーバーのデータが表示されるようになりました。両方の仮想サーバーのデータを個別に表示できます。詳しくは、「コンテンツスイッチングサーバーにバインドされた負荷分散サーバー」を参照してください。

Web Insight レポートの高可用性とクラスターの両方での **Citrix ADC** インスタンスの表示をサポート

Citrix ADM Analytics レポートに、高可用性モードとクラスターモードの両方に展開された ADC インスタンスのレポートが表示されるようになりました。これら 2 つのシナリオにおける合計セッション起動数とアプリケーション数の合計は、グループ内の各インスタンスの個別のレポートではなく、結合されたレポートとして表されます。

> 注
>
> - Citrix ADM 12.1 build 503.x にアップグレードする前に収集されたすべてのデータは、データが保持されるまで、独立したレポートとして引き続き表示されます。
> - クラスタモードでデプロイされた ADC インスタンスの場合、観測ドメイン ID/観測ドメイン名は、CLIP ホスト名と CLIP に置き換えられます。以前に収集されたすべてのデータは、引き続き観測ドメイン ID/観測ドメイン名を報告します。詳しくは、「高可用性モードおよびクラスターモードで展開された Citrix ADC インスタンス」を参照してください。

Citrix ADM での **Citrix ADC CPX** インスタンスの追加

Citrix ADM は、CPX 機能で達成された機能強化をサポートするように拡張されました。Citrix ADC CPX インスタンスは、以下の 2 つの方法のいずれかで Citrix ADM に追加されるようになりました。

- CPX インスタンスが南北トラフィックの管理に使用されている場合、CPX の IP アドレスをデバイスプロファイルとともに提供する
- Citrix ADM から Citrix ADC CPX インスタンスにアクセスできない場合、Docker ホストの IP アドレスを指定します。これは、データセンター内の East-West 方向のトラフィックを管理するために CPX が必要な場合です。

デバイスが Docker IP 経由で検出された場合、データベース内の IP アドレスは NSIP_DOCKERIP として表されます。デバイスが CPX の到達可能な NSIP を介して検出された場合、IP アドレスは ADM データベース内の CPX の NSIP で表されます。

CPX インスタンスの追加プロセスは、ADM で VPX や MPX などの他の ADC タイプを追加する方法と似ています。デバイスプロファイルを指定すると、明示的に設定するのではなく、デバイスプロファイルに SSH、HTTP、HTTPS ポートを設定できます。また、ADM における CPX の登録が強化されました。CPX が起動すると、Citrix ADM は自動的に CPX インスタンスを検出して登録します。

Citrix ADM で Docker ホストを追加して Citrix ADC CPX インスタンスを検出する必要はありません。

AWS にデプロイされた **Citrix ADC** インスタンスの自動スケーリングのサポート

Citrix ADM 自動スケーリング機能は、AWS で Citrix ADC インスタンスのスケーリングをサポートするようになりました。Citrix ADM 自動スケーリング機能は、バックエンドサーバーを AutoScale するタイミングと範囲に応じて、AWS にデプロイされた Citrix ADC クラスターノードを追加または削除します。Citrix ADM は、AutoScale プロビジョニングされたクラスターから統計（CPU 使用率、メモリ使用率、スループット）を収集します。これらの統計は、カスタマーが設定した値に対して評価されます。統計が最大しきい値を超えるか、最小しきい値を下回っているかによって、スケールインまたはスケールアウトがトリガーされます。

自動スケーリング機能の利点は次のとおりです。

- トラフィック要求に関係なく、アプリケーションが常に起動し、実行されていることを確認します。
- Citrix ADC インスタンスは動的に追加および削除され、ゼロタッチ手動構成になります。
- DNS 管理は自動で行われます。
- コスト管理を向上させます。

AutoScale 機能を使用するには、StyleBooks を使用して AutoScale グループを作成し、アプリケーションをデプロイする必要があります。詳しくは、「Citrix ADM を使用した AWS での Citrix ADC の自動スケーリング」を参照してください。

解決された問題

Analytics

- [Security Insight] > [違反合計] レポートの [アプリケーションの概要] テーブルでは、すべての履歴レコードに対して攻撃時間は「NA-」として表示されます。

  [715905]

ネットワーク

- 仮想サーバーが高可用性で展開されている Citrix ADC インスタンスの一部である場合、仮想サーバーの統計は表示されません。

  [715243]

- カスタムアプリケーションの一部である Citrix ADM で GSLB 仮想サーバーを追加すると、ADM は追加した GSLB サーバーの統計情報を正しく表示しないことがあります。

  [715639]

- ADM に Citrix ADC SDX プラットフォームを追加すると、ADC SDX のバージョンが 11.0 未満の場合、Citrix ADM に表示される SDX のダッシュボードにエラーが表示されることがあります。

  [715803]

システム

- 場合によっては、Citrix ADM から Citrix ADC インスタンスを再起動できないことがあります。これは、一部のインスタンスの再起動に 10 分以上かかり、Citrix ADM がインスタンスの再起動に 10 分しか待機しないためです。この修正により、Citrix ADM の再起動時間を 30 分まで構成できるようになりました。

  [716178]

2018 年 9 月 14 日

このリリースには、機能強化とバグ修正が含まれています。

デフォルトでは、Citrix ADM エージェントは自動的に Citrix ADM 12.1 ビルド 502.127 にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

Security Insight レポートに集約された攻撃時間を含める

Security Insight の [違反合計] レポートには、選択した期間が 1 時間を超える場合、攻撃時間が「NA」と表示されます。これで、リストから「1 日」を選択すると、集約されたすべての攻撃がレポートに表示され、攻撃時間が 1 時間の範囲で表示されます。「1 週間」または「1 ヶ月」を選択すると、すべての攻撃が集計され、攻撃時間が 1 日の範囲で表示されます。詳しくは、「Security Insight」を参照してください。

[686874]

解決された問題

システム

- Citrix ADM では、ユーザー管理者プロファイルを変更しても、Citrix ADC インスタンスは再検出されず、Citrix ADC インスタンスにログオンできなくなります。インスタンスは新しいユーザー詳細で更新されず、インスタンスは最初に適用された管理者プロファイルを使用します。

  [699435]

ネットワーク

- 仮想サーバーに関連する Citrix ADM では、次の 2 つの問題が認識されます。
  - 複数の IP アドレスを持つ DNS サーバーを使用して仮想サーバーを構成すると、Citrix ADM はそれらの仮想サーバーを検出できません。
  - 仮想サーバーのコメントまたはその他のフィールドに英語以外の文字が含まれていると、Citrix ADM はエラーを返し、そのインスタンスの仮想サーバーを検出できません。

  [713472]

2018 年 8 月 23 日

このリリースには、機能強化とバグ修正が含まれています。

デフォルトでは、Citrix ADM エージェントは自動的に Citrix ADM 12.1 ビルド 501.123 にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能と機能強化

NetScaler Management and Analytics Service 名前の変更

NetScaler Management and Analytics Service、Citrix Application Delivery Management（ADM）に名前が変更されました。これは、Citrix 統合製品ポートフォリオの一部です。

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。これは、Citrix ポートフォリオとクラウド戦略の拡張の結果です。Citrix 統合ポートフォリオについて詳しくは、「シトリックス製品名ガイド」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。
- 既存の顧客スクリプトが壊れないようにするため、一部の項目（コマンドなど）は引き続き以前の名前を保持す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。

[715090]

解決された問題

ネットワーク

- 重複したエントリは、負荷分散、コンテンツスイッチング、キャッシュリダイレクトなど、ネットワーク機能でリストされているすべてのエントリをフィルタリングすると表示されます。

  [704095]

- [ネットワーク] > [インスタンス] に移動し、**[Citrix ADC** インスタンスの **Analytics** の構成] を選択して仮想サーバーでインサイトを有効にした場合、仮想サーバーに名前の入った「スペース」がある場合 **[Analytics** の構成**]** ページは仮想サーバーの詳細を反映しません。

  [713945]

- Citrix ADC インスタンス上で直接構成したコレクタを構成する場合、［分析の構成］ページの［トランスポートモード］列フィールドにデータが表示されません。

  [713946]

2018 年 8 月 03 日

このリリースには、機能強化とバグ修正が含まれています。

デフォルトでは、Citrix ADM エージェントは自動的に Citrix ADM 12.1 ビルド 500.126 にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能

StyleBooks 用の GitHub のインポートと同期

Citrix ADM の「リポジトリ」機能を使用して、GitHub リポジトリから StyleBook を直接インポートおよび同期できるようになりました。複数の GitHub リポジトリから StyleBooks を同期できます。GitHub で作成され、GitHub リポジトリからインポートされた StyleBook は、手動でインポートした StyleBook と同様に、Citrix ADM RBAC ポリシーに依存しています。GitHub のユーザー名とパスワードまたは API トークンのいずれかを使用して GitHub リポジトリを設定できます。

> 注
>
> - StyleBook をインポートおよび同期できるのは、依存する StyleBook が関連付けられていない（つまり、StyleBook がそのファイルで定義されているすべての構成を持っている必要があります）。
> - GitHub リポジトリからの同期は、Citrix ADM GUI または API から手動で開始する必要があります（つまり、StyleBooks のインポートは、GitHub コミットアクティビティに基づいて自動的に行われません）。

詳しくは、「GitHub リポジトリからの StyleBook のインポートと同期」を参照してください。

[699790]

StyleBooks を使用してアプリケーションファイアウォールで負荷分散仮想サーバーを作成する

Citrix ADM の新しいデフォルトの WAF StyleBook を使用して、Citrix WAF（Web アプリケーションファイアウォール）機能の構成を自動化できるようになりました。この StyleBook では、アプリケーションファイアウォールのポリシーと設定を関連づけて、負荷分散仮想サーバーを作成できます。

> 注:
>
> App Firewall 署名を構成する前に、適切なデフォルトの署名オブジェクトテンプレートから Citrix ADC インスタンスで署名オブジェクトを作成する必要があります。WAF StyleBook を使用してデフォルトのシグニチャオブジェクトを設定または変更することはできません。

詳しくは、「Web アプリケーションファイアウォール StyleBook」を参照してください。

[708597]

Citrix ADM エージェントのパスワードを変更する機能

これで、コマンドラインでスクリプト “change_agent_system_password.py” を実行できるようになります。これにより、エージェントを展開した後に Citrix ADM エージェントのパスワードを更新できます。詳しくは、「エージェント登録後のエージェントパスワードの変更」を参照してください。

[712517]

解決された問題

ネットワーク

- マスター設定テンプレートを使用して設定ジョブを作成するときに、ファイルを編集した後に同じ設定ファイルを複数回アップロードしなければならない場合があります。このファイルは初めて正常にアップロードできます。後でアップロードすると、ユーザー通知なしで失敗します。

  回避策：これは、ブラウザのデフォルトの動作が原因で発生しています。変更後に同じファイルを再度アップロードする場合は、[戻る] をクリックして [Select Instances] タブに移動し、[次へ] をクリックして同じファイルを再度アップロードします。

  [711593]

- Citrix ADM は、バインドされたすべてのサービスグループメンバーを解析できない

  [712022]

Analytics

- Citrix ADM に「読み取り専用」権限でアクセスすると、Web Insight で情報を表示することはできません。

  [713404]

- [分析] > [設定] の [**IP** ブロックの構成] ページで、都市、地域、および国を変更して以前に作成した IP ブロックを編集し、設定を再度編集しようとすると、[IP ブロックの設定] ページに以前の都市の名前が表示されます。このビルドでは、この問題は修正されます。

  [712110]

- Citrix ADM は 1 ページに 25 行のエントリしか表示されないため、テーブルが複数のページにオーバーオーバーする状況が発生する可能性があります。以前は、現在のページでのみ行エントリをソートできました。他のページには、ソートされたエントリが表示されませんでした。これで、任意のページでテーブルをソートすることができ、そのテーブルのすべてのページにソートされた結果が表示されます。

  > **注:** この機能は、テーブル内のレコード数が 25,000 未満の場合のみ機能します。

  [689564]

既知の問題

アプリケーション

- [ネットワーク] > [インスタンス] に移動し、**[Citrix ADC** インスタンスの **Analytics** の構成] を選択して仮想サーバーでインサイトを有効にした場合、仮想サーバーに名前の入った「スペース」がある場合 **[Analytics** の構成**]** ページは仮想サーバーの詳細を反映しません。たとえば、AppFlow ログは仮想サーバー上で有効になっていても、[分析の設定] ページで [無効] と表示される場合があります。

  [713945]

- Citrix ADC インスタンスでコレクタを直接構成する場合、［分析の構成］ページの［トランスポートモード］列フィールドにデータが表示されません。

  [713946]

Analytics

- 場合によっては、HDX Insight ノードと Citrix Gateway インサイトノードが Citrix ADM GUI に表示されないことがあります。

  回避策：ページを更新して、もう一度試してください。

  [690327]

ネットワーク

- 重複したエントリは、負荷分散、コンテンツスイッチング、キャッシュリダイレクトなど、ネットワーク機能でリストされているすべてのエントリをフィルタリングすると表示されます。

  [704095]

- ［ネットワーク］>［インスタンス］の順に選択し、Citrix ADC インスタンスの［分析の構成］を選択して仮想サーバーでインサイトを有効にした場合、仮想サーバーの名前に「スペース」が含まれている場合、［分析の構成］ページに仮想サーバーの詳細は反映されません。

  [713945]

- Citrix ADC インスタンス上で直接構成したコレクタを構成する場合、［分析の構成］ページの［トランスポートモード］列フィールドにデータが表示されません。

  [713946]

設定

- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。

  [686581]

2018 年 7 月 12 日

このリリースには、バグの修正が含まれています。

デフォルトでは、Citrix ADM エージェントはビルド 516.126 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能

Citrix ADM イベント通知の電子メール構成のテストボタン

イベント通知の電子メールを送信するときに、テスト電子メールを送信して、構成済みの設定をテストすることができます。「テスト」ボタンを使用すると、電子メールサーバー、関連する配布リスト、およびその他の設定を構成した後、テストメールを送信できるようになりました。この機能により、設定が正常に動作することが保証されます。詳しくは、「イベントルールの作成」を参照してください。

[684948]

イベント通知メールの件名のカスタマイズ

多数の仮想サーバーが構成されている大規模なネットワークでは、管理者として毎日大量のメールを受信することがあります。ただし、メールを受信したときに影響を受けるエンティティの名前がメールポップアップに表示され、電子メールを開かなくても影響を受けるエンティティを特定できます。[ネットワーク] > [イベント] > [ルール] で、ルールを作成して電子メール通知ルールを設定するときに、影響を受けるエンティティ (障害オブジェクト) の名前などの追加情報を含めるオプションが追加されました。詳細については、「イベントルールの作成」を参照してください。

[705142]

プールされた容量機能の向上

Citrix VPX インスタンス用の Citrix ADM の［プールライセンス］ページで、いくつかの変更が行われました。ライセンスプール内のライセンスを Citrix ADC インスタンスにオンデマンドで割り当てるときに、新しい状態セットが導入されました。州は次のとおりです。

- 割り当て済み
- グレイス
- 同期中
- 部分的に割り当てられた
- デバイスが管理されていません
- 割り当て済み。デバイスに適用されない
- 接続が失われました

また、ライセンス割り当ての状態に関する詳細が Citrix ADM に追加されました。詳しくは、「プールされた容量」を参照してください。

[709975]

Citrix ADM でのライセンス機能の可用性

Citrix ADM は、Citrix ADM で追加された Citrix VPX および MPX インスタンスをサーバーとする共通の帯域幅とインスタンスプールをホストするようになりました。この共通プールから、データセンター内の各 Citrix ADC インスタンスは、プラットフォームやフォームファクタに関係なく、1 つのインスタンスライセンスをチェックアウトし、必要な帯域幅だけをチェックアウトします。詳しくは、「プールされた容量」を参照してください。

[709679]

アドレス指定できない仮想サーバに対する構成可能な自動ライセンスサポート

デフォルトでは、Citrix ADM は、アドレス指定できない仮想サーバーにライセンスを自動的に適用しません。アドレス指定不可の仮想サーバをライセンスする場合は、自動ライセンスオプションを無効にし、アドレス指定不可の仮想サーバを手動で選択する必要があります。これにより、ライセンスを適用するとき、およびネットワークに追加されるたびにアドレス指定できない新しい仮想サーバを選択する必要があるときに、アドレス指定できないサーバを手動で選択する手間がかかります。

Citrix ADM の［ネットワーク］>［ライセンス］>［システムライセンス］の新しいオプションは、［アドレス指定できない仮想サーバーの自動選択］です。このオプションを有効にすると、アドレス指定できない仮想サーバもライセンスに含める必要があることを明示的に指定できるようになりました。

> 注
>
> - Citrix ADM は、デフォルトでは、アドレス指定できない仮想サーバーをライセンス用に自動選択しません。
> - アプリケーション分析（App Dashboard）は、ライセンスされたアドレス指定不可能な仮想サーバーで現在サポートされている唯一の分析です。詳しくは、「サブスクリプションの管理」を参照してください。

[707843]

Citrix ADM を使用して **AWS** で **Citrix ADC VPX** インスタンスをプロビジョニングする機能

Citrix ADM では、スタンドアロンデプロイとして、Amazon Web Services（AWS）プラットフォームで Citrix ADC VPX インスタンスをプロビジョニングできるようになりました。Citrix ADC VPX on AWS では、AWS クラウドコンピューティング機能を使用し、ビジネスニーズに合わせて Citrix ADC の負荷分散およびトラフィック管理機能を使用できます。Citrix ADC on AWS は、物理 Citrix ADC アプライアンスのすべてのトラフィック管理機能をサポートします。詳しくは、「AWS での Citrix ADC VPX インスタンスのプロビジョニング」を参照してください。

[680526]

解決された問題

高可用性

- 高可用性モードで Citrix ADC インスタンスのペアの 1 つのノードを構成し、IP アドレスが 171.31.200.x の範囲である場合、このペアの Citrix ADC インスタンスは Citrix ADM によって検出されません。

  [710589]

ネットワーク

- マスター設定テンプレートを使用して設定ジョブを作成するときに、ファイルを編集した後に同じ設定ファイルを複数回アップロードしなければならない場合があります。このファイルは初めて正常にアップロードできます。後でアップロードすると、ユーザー通知なしで失敗します。

  回避策：これは、ブラウザのデフォルトの動作が原因で発生しています。変更後に同じファイルを再度アップロードする場合は、[戻る] をクリックして [Select Instances] タブに移動し、[次へ] をクリックして同じファイルを再度アップロードします。

  [711593]

- ネットワークイベントダイジェストレポートデータは、書式設定の問題により切り捨てられます。

  [704980]

- Citrix ADM をバージョン 12.1 にアップグレードすると、SNMP v3 ベースのイベントレポートが機能しない。Citrix ADM で追加されたバージョン 12.1、48.13 の Citrix ADC インスタンスでは、次の回避策をお勧めします。

  回避策：SNMP v3 の問題が修正され、リリースされるまで SNMP v2 トラップを使用します。

  [710564]

- 高可用性モードで展開したときに Citrix ADC インスタンスがフェイルオーバーすると、mas_afdecoder プロセスはライセンス情報を更新するための通知を受信しません。mas_afdecoder プロセスは、プライマリノードから受信したデータパケットをドロップし、その結果、Web Insight レポートは Citrix ADM GUI に表示されません。

  [711503]

システム

- 都市の名前に Unicode 文字が含まれていると、エージェント登録が失敗します。

  [711737]

- 新しい Citrix ADM エージェントをアクティブ化しようとすると、「無効なインスタンス ID」というエラーメッセージが表示されることがあります。

  [706527]

StyleBook

- Sharepoint StyleBook は、すべてのバックエンドサービスで SSL プロトコルをサポートする必要があります。

  [706507]

- 作成者フィールドには、StyleBook に関する情報を取得するために使用される API レスポンスに null が表示されます。

  [711021]

既知の問題

Analytics

- 場合によっては、HDX Insight ノードと Citrix Gateway インサイトノードが Citrix ADM GUI に表示されないことがあります。

  回避策：ページを更新して、もう一度試してください。

  [690327]

ネットワーク

- 重複したエントリは、負荷分散、コンテンツスイッチング、キャッシュリダイレクトなど、ネットワーク機能でリストされているすべてのエントリをフィルタリングすると表示されます。

  [704095]

設定

- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。

  [686581]

2018 年 6 月 14 日

このリリースには、バグの修正が含まれています。

デフォルトでは、Citrix ADM エージェントはビルド 515.116 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能

GSLB ドメインでのロールベースのアクセス制御

現在、GSLB ドメインでも RBAC がサポートされているため、StyleBooks を使用して GSLB 構成の実行を許可する権限のあるユーザーのみを許可できるようになりました。

Citrix ADM では、「DNS ドメイン名」という新しいエンティティがサポートされるようになりました。Citrix ADM で、[ネットワーク] > [**DNS** ドメイン名] の順に選択し、DNS ドメイン名のエントリーを追加します。[システム] > [ユーザー管理] > [グループ] に移動します。使用可能なドメイン名の一覧から、選択したドメイン名のユーザーグループの RBAC 設定を定義します。

この RBAC 設定は、ユーザーが StyleBooks を使用して GSLB を構成しようとしているときに適用されます。ユーザーは、使用が許可されている 1 つ以上の DNS ドメイン名のみを使用できます。

[706988]

Citrix ADC インスタンスの検索機能の向上

Citrix ADM が多くの Citrix ADC インスタンスを管理しているシナリオを考えてみましょう。いくつかの検索パラメータに基づいてインスタンスのインベントリを検索できる柔軟性が必要な場合があります。Citrix ADM では、検索パラメーターを修飾する Citrix ADC インスタンスのサブセットを効率的に検索するためのタグとプロパティという 2 つの検索条件が提供されました。

例：バージョン 12.0 にあり、UP 状態にあるすべての Citrix ADC インスタンスを検索するとします。詳しくは、「タグを作成してインスタンスに割り当てる」を参照してください。

[709997]

Citrix ADC インスタンスにタグを付ける機能

タグは、Citrix ADC インスタンスに割り当てて、Citrix ADC インスタンスに関する追加の説明を関連付けることができる用語またはキーワードです。Citrix ADM では、Citrix ADC インスタンスをタグに関連付けることができるようになりました。これらのタグを使用すると、Citrix ADC インスタンスをグループ化、識別、検索できます。詳しくは、「タグを作成してインスタンスに割り当てる」を参照してください。

[708603]

Slack にイベント通知を送信する機能

以前は、Citrix ADM GUI では、イベントの電子メール通知を送信するオプションがありました。Slack チャンネルにもイベント通知を送信できるようになりました。

Citrix ADM GUI でプロファイル名と Webhook URL を指定して、必要な Slack チャネルを構成します。イベント通知はこのチャンネルに送信されます。詳しくは、「イベントルールの作成」を参照してください。

[656472]

解決された問題

ネットワーク

- Citrix ADM が 0/1 以外のインターフェイスで構成されている場合、仮想サーバー上で AppFlow を構成することはできません。[705330]
- 構成監査テンプレート名には空白を含めない。[708003]

StyleBook

- StyleBook でカスタムヘッダーを定義している場合は、StyleBooks を使用してエンティティを作成することはできません。[709094]

設定

- ユーザーのログアウトに関するシステム通知は表示できますが、電子メール通知を受信しない場合があります。[704344]
- NTP の詳細が rc.netscaler ファイルに追加された場合、Citrix ADM は Citrix ADC インスタンスの事前検証に失敗します。これで、これらの Citrix ADC インスタンスを選択し、インスタンスのアップグレード中に削除できます。[708466]
- Citrix ADC は、同じアプリケーションの「複数のアプリケーション終了」レコードをエクスポートします。これにより、Citrix `afdcoder` ADM プロセスがクラッシュします。[709462]

高可用性

- 高可用性モードの Citrix ADC インスタンスがユーザーグループに割り当てられ、インスタンスペアがフェイルオーバーすると、インスタンスはユーザーグループに割り当てられなくなります。[709202]

既知の問題

Analytics

- 場合によっては、HDX Insight ノードと Citrix Gateway インサイトノードが Citrix ADM GUI に表示されないことがあります。回避策：ページを更新して、もう一度試してください。[690327]

ネットワーク

- 重複したエントリは、負荷分散、コンテンツスイッチング、キャッシュリダイレクトなど、ネットワーク機能でリストされているすべてのエントリをフィルタリングすると表示されます。[704095]

設定

- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。[686581]

2018 年 5 月 24 日

このリリースには、バグの修正が含まれています。

デフォルトでは、Citrix ADM エージェントはビルド 514.117 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

解決された問題

ネットワーク

- ネットワーク、分析、およびシステムノードにのみ RBAC アクセス権があるシナリオを考えてみましょう。デフォルトの動作では、ナビゲーションペインの最初のノード（つまり、Citrix ADM にアクセスするときに、［ネットワーク］がランディングページである必要があります）。しかし、現在は [アナリティクス] ノードがランディングページになっています。[705347]
- Internet Explorer 11.0、Firefox バージョン 31.0、および Google Chrome バージョン 31.0 を使用して構成ジョブを作成すると、次のエラーが表示されます。

```
SCRIPT5017: Syntax error in regular expression rdx.js (61,583910)
    "
<!--NeedCopy-->
```

  [707767]
- Citrix ADC 監査テンプレート違反グラフに、同じインスタンスをポーリングする 2 つのスケジュール済み監査テンプレートに、違反のあるインスタンスが 1 つある場合、「相違なし」ステータスメッセージが表示されます。[708404]
- 監査テンプレート名は変更または編集できません。[708407]
- 監査テンプレートでは、変数値の ‘&’ 文字は、入力ファイルの ‘&’ 文字に置き換えられます。[708766]
- [ネットワークレポート] でインスタンスのしきい値を設定すると、インスタンスの一覧には、Citrix ADC インスタンスに加えて Citrix ADC SDX インスタンスが含まれます。
  [707980]
- Citrix SD WAN WO インスタンスを Citrix ADM に追加すると、SNMP 接続は成功せず、GUI が応答しなくなります。
  [709146]

Analytics

- ユーザー名に基づいて Gateway Insight レポートをフィルタリングすると、Citrix ADM はユーザー固有の詳細をフィルタリングできません。
  [701514]
- 大量の HTTP トランザクションがあると、mas_afdecoder プロセスが失敗することがあります。
  [706509]

既知の問題

Analytics

- 場合によっては、HDX Insight ノードと Citrix Gateway インサイトノードが Citrix ADM GUI に表示されないことがあります。
  回避策：ページを更新して、もう一度試してください。
  [690327]

ネットワーク

- 重複したエントリは、負荷分散、コンテンツスイッチング、キャッシュリダイレクトなど、ネットワーク機能でリストされているすべてのエントリをフィルタリングすると表示されます。
  [704095]

設定

- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。
  [686581]

2018 年 5 月 04 日

このリリースには、バグの修正が含まれています。

デフォルトでは、Citrix ADM エージェントはビルド 513.120 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

解決された問題

Analytics

- HDX Insight の組み合わされたグラフィカルビューには、誤ったタイムゾーンが表示されます。[703906]

- HTTP POST トランザクションの応答時間の計算が正しくないため、Web Insight レポートの生成が停止します。[707146]

ネットワーク

- レポートを.csv 形式でエクスポートすると、時間列にはユーザーが読める形式ではなく、「エポック」形式でデータが表示されます。
  [704828]
- 構成ジョブの実行サマリーは、Citrix ADC インスタンス上で構成ジョブのコマンドが完全に実行されていない場合でも、Citrix ADM では完了として表示されます。
  [707317]

既知の問題

Analytics

- 場合によっては、HDX Insight ノードと Citrix Gateway インサイトノードが Citrix ADM GUI に表示されないことがあります。
  回避策：ページを更新して、もう一度試してください。
  [690327]

ネットワーク

- 重複したエントリは、負荷分散、コンテンツスイッチング、キャッシュリダイレクトなど、ネットワーク機能でリストされているすべてのエントリをフィルタリングすると表示されます。
  [704095]

設定

- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。
  [686581]

2018 年 4 月 12 日

このリリースには、新機能とバグ修正が含まれています。

デフォルトでは、Citrix ADM エージェントはビルド 512.119 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能

Citrix ADM からデフォルトの **StyleBook** を非表示にする機能

Citrix ADM で使用可能な StyleBook のリストから、デフォルトの StyleBook をすべて非表示にできるようになりました。[アプリケーション] > [構成] > [設定**]** に移動します。[既定の **StyleBooks** を隠す**]** チェックボックスを有効にします。デフォルトの StyleBook はすべて非表示になり、ユーザーはアクセスできなくなります。さらに、**[**設定] ページ自体をユーザーから非表示にすることができます。RBAC 機能を使用すると、[設定] ページにアクセスできないようにする適切なアクセスポリシーを作成できます。[アカウント] > [ユーザー管理] > [アクセスポリシー] に移動します。ポリシーを作成し、[権限] セクションで [すべて] > [アプリケーション] > [構成] の [設定] の選択を解除します。詳しくは、「すべてのデフォルトスタイルブックを非表示にする」を参照してください。

[686914]

Citrix ADM でユーザー定義の **StyleBook** をすべて検索する機能

Citrix ADM では、タイプに基づいて StyleBook を検索できるようになりました。つまり、Citrix ADM の［StyleBooks］一覧ページで、すべてのカスタム StyleBook を検索できるようになりました。詳しくは、「カスタム StyleBook を使用する」を参照してください。

[681949]

解決された問題

Analytics

- AppFlow トラフィックが Citrix ADC クラスタからのものである場合、Citrix ADM は 7 日を超えてデータを格納しません。
  [706348]

ネットワーク

- テンプレートをインポートするとき、または構成テンプレートを使用してジョブを作成すると、変数の値は表示されません。プレビュー後に [完了] をクリックして、変数の値を表示します。
  [705884]
- 複数の構成ジョブが多数のコマンドおよび複数のインスタンスで同時に実行されている場合、構成ジョブは完全には実行されません。ジョブの実行が停滞し、「進行中」状態に表示されます。
  [706201]
- 構成テンプレートのインポートがキャンセルされた場合でも、構成テンプレートは Citrix ADM にアップロードされます。
  [706219]
- Citrix ADM では、［ネットワーク］>［イベント］>［**Syslog** メッセージ］に移動すると、最も古いメッセージが最初に表示されますが、［並べ替え］ウィンドウの［新しい順］オプションが表示されます。「古い順」を

選択し、「新しい順」を選択した場合のみ、メッセージが正しく表示されます。
[702305]

- 他のイベントルールに加えて、イベントに対して「抑制」イベントルールを構成すると、Citrix ADM は、構成されたすべてのイベントルールを実行します。
[702517]

システム

- シングルサインオン資格情報を使用しているにもかかわらず、同じ Citrix ADC インスタンスを閉じた後に再度アクセスすることはできません。
[699435]

既知の問題

Analytics

- 場合によっては、HDX Insight ノードと Citrix Gateway インサイトノードが Citrix ADM GUI に表示されないことがあります。
回避策：ページを更新して、もう一度試してください。
[690327]

設定

- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は、Citrix ADM の［設定］>［ユーザー管理］>［ユーザー］に表示されます。
[686581]

2018 年 3 月 22 日

このリリースには、新機能とバグ修正が含まれています。

デフォルトでは、Citrix ADM エージェントはビルド 511.118 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能

Citrix ADM ヘルプセンターのご紹介

Citrix ADM にはヘルプセンターがあり、実行中のさまざまなタスクのリンクにアクセスできます。たとえば、Citrix ADM を初めてオンボードする方法を学ぶことができます。また、最新のリリースノートを表示したり、サブスクリプションの管理方法を確認することもできます。

[706025]

StyleBook を使用して **Citrix ADC** インスタンスを **ADFS** プロキシとして構成する

StyleBooks を使用して、Active Directory フェデレーションサービス (ADFS 2.0) のリバースプロキシとして機能するように Citrix ADC インスタンスを構成できるようになりました。Citrix ADC インスタンスは、Active Directory 認証クライアントのシングルサインオン（SSO）エクスペリエンスをエンタープライズデータセンター外のリソースまで拡張できるようになりました。これで、インスタンスはアクティブとパッシブの ADFS 認証の両方をサポートできます。詳しくは、「Microsoft ADFS proxy StyleBook」を参照してください。

[696203]

インスタンスダッシュボードの改善

Citrix ADM インスタンスごとのダッシュボードには、特定のインスタンスからポーリングされたデータが表示されます。デフォルトでは、1 分ごとに、マネージインスタンスがデータ収集のためにポーリングされます。NITRO 呼び出しを使用して、状態、HTTP リクエスト/秒、CPU 使用率、メモリ使用量、スループットなどの統計情報を継続的に収集します。管理者は、この収集されたすべてのデータを 1 つのページで表示できます。また、インスタンス内の問題を特定し、即座に修正するアクションを実行することもできます。

特定のインスタンスのダッシュボードを表示するには、[ネットワーク**] > [**インスタンス**] >** (インスタンスタイプ) に移動します。表示するインスタンスを選択し、[**Dashboard**] をクリックします。

[**Overview**] タブには、特定のインスタンスの CPU、メモリ使用量、イベントが表示されます。他のインスタンス固有のダッシュボードを表示して、インスタンスの詳細情報を確認できます。その他のタブには、SSL、設定監査、ネットワーク機能、ネットワークの使用状況があります。

[687676]

ネットワークインベントリの改善

Citrix ADM によって維持されるインスタンスの完全なリストを表示できるようになりました。インベントリレポートを表示するには、[ネットワーク**] > [**ダッシュボード] に移動し、画面の右上隅にある [すべてのインスタンス] をクリックします。新しいインベントリレポートには、次の情報が表示されます。

- すべてのインスタンス
- インスタンスのバージョン
- シリアル番号

[687676]

ポーリングの進行状況インジケータ

Citrix ADM でインスタンスのポーリングアクションのステータスを表示できるようになりました。以前は、[**Poll Now**] アクション（証明書、構成監査、検出など）を選択すると、GUI はポーリングが開始されたときだけ表示されていました。これで、ポーリングの進行状況、実行中および完了のかどうか、およびポーリングアクション中にインスタンスから取得された情報が確認できます。

詳しくは、「Citrix ADC インスタンスとエンティティのポーリング」を参照してください。

[688916]

解決された問題

- **[** 設定**] > [**サブスクリプション**]** ページで、ストレージデータ消費が 5 GB という資格のあるストレージ制限よりも大きく表示されることがあります。
  [689330]
- Citrix ADM 506.119 ビルドから Citrix SD-WAN WO または Citrix ADC SDX インスタンスをアップグレードすることはできません。
  [699814]
- Internet Explorer 11 を使用してログオンすると、Citrix Cloud ナビゲーションバーは表示されません。
  [702339]

既知の問題

ネットワーク

- Citrix ADM では、［ネットワーク］>［イベント］>［Syslog メッセージ］に移動すると、最も古いメッセージが最初に表示されますが、［並べ替え］ウィンドウの［新しい順］オプションが表示されます。「古い順」を選択し、「新しい順」を選択した場合のみ、メッセージが正しく表示されます。
  [702305]

Analytics

- 場合によっては、HDX Insight ノードと Citrix Gateway インサイトノードが Citrix ADM GUI に表示されないことがあります。
  回避策：ページを更新して、もう一度試してください。
  [690327]

設定

- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。
  [686581]

2018 年 3 月 3 日

このリリースには、新機能とバグ修正が含まれています。

デフォルトでは、Citrix ADM エージェントはビルド 510.120 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能

ネットワークレポートダッシュボードの改善

異なるレポートデータを表示する複数のウィジェットを使用して、カスタマイズされたダッシュボードを作成できるようになりました。カスタマイズしたダッシュボードでは、任意の数の仮想サーバーおよび最大 10 個のインスタンスについて、複数のレポートを表示できます。また、レポートの期間をカスタマイズし、詳細な分析のためにエクスポートすることもできます。詳しくは、「ネットワークレポート」を参照してください。

[702016]

レポート期間のカスタマイズ

スライダーを使用して、Citrix ADM GUI で生成されるレポートの継続時間をカスタマイズできるようになりました。以前は、1 時間、日、週、または 1 か月のレポートを生成して表示することができました。詳しくは、「ネットワークレポート」を参照してください。

[666018]

新しいネットワークレポート

選択した Citrix ADC インスタンスの各インターフェイスについて、パフォーマンスレポートを生成およびエクスポートできるようになりました。収集されるパフォーマンスデータは、選択したカウンタと、Citrix ADC インスタンスが送受信するデータに基づいています。詳しくは、「ネットワークレポート」を参照してください。

[683417]

選択した Citrix ADC インスタンスについて、スループットと帯域幅に関するレポートを生成できるようになりました。生成されたスループットレポートを使用して、[Network Reporting] ダッシュボードで特定のインスタンスごとにネットワークレポートデータを監視できます。詳しくは、「ネットワークレポート」を参照してください。

[687555]

StyleBook を使用した **Citrix ADC** インスタンスへの **Oracle E-Business** スイートのデプロイ

StyleBooks を使用して、Citrix ADC で Oracle E-Business Suite 12.2 の負荷分散展開プロセスを定義できるようになりました。ロード・バランシングの構成は、LB 仮想サーバーにリンクされ、個々の Oracle E-Business Suite サーバーにバインドされる負荷分散仮想サーバーおよびサービスの定義で構成されます。詳しくは、「Oracle 電子ビジネススタイルブック」を参照してください。

[679553]

StyleBooks とアプリケーションダッシュボードを統合して、**Citrix ADC** インスタンス上で構成を作成する

Citrix ADM では、デフォルトまたはカスタム StyleBook を使用してカスタムアプリケーションを作成できるようになりました。StyleBook は、アプリケーションの複雑な Citrix ADC 構成の管理作業を簡素化します。したがって、アプリケーションダッシュボードページでカスタムアプリケーションを定義するときに、Citrix ADM に存在する StyleBook を選択できるようになりました。次に、Citrix ADM は、選択した StyleBook に基づいて、ターゲット Citrix ADC インスタンス上に構成を作成します。Citrix ADM は、構成パック内のすべての仮想サーバーで構成されたカスタムアプリケーションも作成します。

> 注:
>
> 十分な Citrix ADM ライセンスが利用可能で、仮想サーバーのライセンスが［手動］に設定されていない場合は、カスタムアプリケーションと構成パックが作成されます。詳しくは、「アプリケーション定義の作成」を参照してください。

[684460]

既存の構成パックを別の **StyleBook** に移行する機能

Citrix ADM では、構成パックを削除して再作成することなく、構成パックを新しい StyleBook へ移行（またはアップグレード）できるようになりました。この機能を使用すると、ターゲットインスタンス上のすべての設定を保持できます。

新しい StyleBook のパラメータは、既存の StyleBook のパラメータのスーパーセットであることを考えてみましょう。その後、Citrix ADM は、パラメータ値を再入力しなくても、構成パックを新しい StyleBook に移行できます。

> 注:
>
> これは、新しい StyleBook の一部である新しいパラメータは任意であることを前提としています。

移行中、Citrix ADM は、既存の構成と新しい StyleBook によって生成された新しい構成との間で構成差分を実行します。Citrix ADM は、ターゲット Citrix ADC インスタンスで追加、削除、または更新する必要がある構成オブジェクトを決定します。

Citrix ADM 内の 2 つの StyleBook 間で構成パックを移行する際に制限はありません。移行した設定パックを以前の StyleBook に戻すこともできます。詳しくは、「StyleBook の設定パックを別の StyleBook に移行する」を参照してください。

[699789]

Security Insight レポートでの署名のルール **ID** の表示

署名違反の Security Insight レポートに、各シグニチャのルール ID が含まれるようになりました。

詳しくは、「Security Insight」を参照してください。

[701416]

解決された問題

Analytics

- NITRO 呼び出しが増加すると、Citrix ADM が応答を停止します。
  [696032]

ネットワーク

- Citrix ADM の［システムバックアップ設定］ページにバックアップファイルの数が表示されません。
  [703421]
- [ネットワーク] > [ライセンス設定] > [システムライセンス] で、許可された仮想サーバの数を超える仮想サーバが選択されている場合、送信前にユーザーにプロンプト警告メッセージが表示されます。[687058]

既知の問題

ネットワーク

- Citrix ADM では、［ネットワーク］>［イベント］>［Syslog メッセージ］に移動すると、最も古いメッセージが最初に表示されますが、［並べ替え］ウィンドウの［新しい順］オプションが表示されます。「古い順」を選択し、「新しい順」を選択した場合のみ、メッセージが正しく表示されます。
  [702305]

Analytics

- 場合によっては、HDX Insight ノードと Citrix Gateway インサイトノードが Citrix ADM GUI に表示されないことがあります。
  回避策：ページを更新して、もう一度試してください。
  [690327]

設定

- [設定] > [サブスクリプション] ページで、ストレージデータ消費が 5 GB という資格のあるストレージ制限よりも大きく表示されることがあります。
  [689330]
- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。
  [686581]
- Citrix ADM から Citrix SD-WAN WO または Citrix ADC SDX インスタンスをアップグレードすることはできません。
  [699814]

GUI の問題

- Internet Explorer 11 を使用してログオンすると、Citrix Cloud ナビゲーションバーは表示されません。[702339]

2018 年 **2** 月 **9** 日

このリリースには、新機能とバグ修正が含まれています。

デフォルトでは、Citrix ADM エージェントはビルド 509.119 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能

アプリケーションダッシュボードの改善

Citrix ADM GUI では、アプリケーションダッシュボードの使いやすさを向上させるために、次の変更が加えられています。

1. *0* アプリスコアは、停止中または停止中のアプリケーション仮想サーバーの数を表します。この *0* アプリスコアは、アプリケーションダッシュボードビューの既存のアプリスコアの凡例の一部になりました。
2. アプリの概要パネルに、以前の「合計アプリ数 *N/N*」ではなく、「*N/N* アプリを表示」というテキストが表示されるようになりました。アプリのスコアグラフで 60 を選択する例を考えてみましょう。アプリスコアが 40～60 のアプリケーションの合計 26 個のうち、16 個のアプリケーションがあります。アプリの概要パネルに「*16/26* アプリを表示」と表示されます。条件が選択されていない場合、アプリの概要パネルに「*26/26* アプリを表示」と表示されます。
3. アプリケーションの概要パネルに、適用可能なカテゴリに基づいてアプリケーションをフィルタリングするための新しいグラフが表示されるようになりました。アプリケーションの概要パネルに新しいアプリケーションカテゴリグラフが追加されます。このグラフには、Citrix ADM で定義されているすべてのカテゴリのヒストグラムが表示されます。すべての個別アプリケーションが [その他] カテゴリに表示され、カスタムアプリケーションはそれぞれのカテゴリ名の下に表示されます。これらのカテゴリ名は、カスタムアプリケーションの定義時に割り当てられます。

詳しくは、「アプリケーションの分析と管理」を参照してください。

[695980]

アプリケーションをフィルタリングするためのパラメータとして、負荷分散仮想サーバの状態とヘルスのパーセンテージを選択する機能

仮想サーバーの正常性棒グラフでは、Citrix ADM は仮想サーバーの正常性の割合に基づいてアプリケーションを分類します。棒グラフには、ヘルス値が 0% ～100% の範囲でグループ化されているアプリケーションの数が表示されます。

仮想サーバーの正常性とは、個別のアプリケーションの下にグループ化された仮想サーバーの正常性を表します。ただし、複数の仮想サーバで構成されるカスタムアプリケーションがある場合は、グループ間で仮想サーバのヘルスの最小数が考慮されます。

これで、フィルタを適用し、選択条件に一致するアプリケーションのみをアプリケーションダッシュボードに表示できます。

詳しくは、「アプリケーションの分析と管理」を参照してください。

[694425]

Citrix ADC インスタンスへの組み込みの **Citrix ADM** エージェント

リリース 12.0 ビルド 56.20 以降を実行している Citrix ADC インスタンスには、Citrix ADM 組み込みエージェントが含まれています。このエージェントは、インスタンスと Citrix ADM 間の通信を有効にします。外部エージェントをインストールする必要はありません。

管理、監視、およびアプリケーションダッシュボード機能は、組み込みエージェントを使用する Citrix ADC インスタンスでサポートされます。Web インサイト、SSL Insight、HDX Insight、Citrix Gateway インサイト、Security Insight、インテリジェントアプリ分析の機能はサポートされていません。

この組み込みエージェントを使用するには、Citrix ADC インスタンスをリリース 12.0 ビルド 56.20 にアップグレードし、エージェントを開始する必要があります。

> 注:
>
> 組み込みエージェントは、次の Citrix ADC インスタンスタイプでのみ使用できます。
>
> - Citrix ADC MPX アプライアンス
> - Citrix ADC VPX アプライアンス
> - Citrix Gateway
> - Citrix Secure Web Gateway

組み込みエージェントの使用方法の詳細と手順については、次の記事を参照してください。

- Citrix ADM の使用開始
- 組み込みエージェントを起動する

[694701]

Web Insight サポート

Citrix ADM は、Web Insight をサポートするようになりました。Web Insight 機能は、エンタープライズ Web アプリケーションを可視化します。IT 管理者は、アプリケーションの統合されたリアルタイム監視を提供することにより、Citrix ADC が提供するすべての Web アプリケーションを監視できます。詳しくは、「Web Insight」を参照してください。

Web Insight は、近似アルゴリズムを使用して Citrix ADC からのデータを処理します。企業内の Web アプリケーションに関連するメトリックの上位 1,000 レコードを提供します。

[688206]

SSL インサイトのサポート

Citrix ADM は SSL Insight をサポートするようになりました。SSL インサイト機能は、Web 上のセキュアなトランザクション (HTTPS) を可視化します。IT 管理者は、統合されたリアルタイムの Web トランザクション監視を提供することにより、Citrix ADC によって提供されるすべての Web アプリケーションを監視できます。詳しくは、「SSL Insight」を参照してください。

SSL インサイトは、近似アルゴリズムを使用して Citrix ADC からのデータを処理します。企業内の Web トランザクションに関連するメトリックの上位 1,000 レコードを提供します。

[688206]

Citrix Gateway Insight での **SAML** 認証レコードのサポート

Citrix Gateway Insight は、SAML 認証失敗に関する洞察を提供するようになりました。SAML 認証の失敗は、［分析］**>**［**Citrix Gateway** インサイト］**>**［概要］ページの［認証］タブに表示されます。

[634094]

場所情報を提供してサイトへの **Citrix ADC** インスタンスの追加機能

Citrix ADM では、Citrix ADC インスタンスを追加してサイトに関連付けることができるようになりました。インスタンスの検出時に、サイトを作成するか、既存のサイトを選択できます。Citrix ADM エージェントの詳細を指定し、常にエージェントをサイトに関連付けます。

インスタンスを追加するには、次の手順に従います。

1. [ネットワーク] > [インスタンス] に移動します。
2. Citrix ADC インスタンスのタイプを選択し、［追加］をクリックします。
3. IP アドレスを入力し、プロファイルを選択します。
4. サイトとエージェントを選択します。
5. [Agent] フィールドの横にある編集アイコンをクリックします。
6. エージェントを選択し、[**Attach Site**] をクリックし、必要なサイトを選択します。
7. [**OK**］をクリックします。

これで、インスタンスはサイトに関連付けられます。[ネットワークダッシュボード] に移動して、関連付けられたサイトの下に新しく追加されたインスタンスを表示します。

詳しくは、「グローバルに分散されたサイトを監視する方法」を参照してください。

[702019]

同じプライベート **IP** アドレスで **Citrix ADC** インスタンスを検出する機能

Citrix ADM を使用して組み込みエージェントを使用してインスタンスを登録するときに、異なるネットワーク上の同じプライベート IP アドレスを持つ Citrix ADC インスタンスを検出できるようになりました。

[699962]

解決された問題

ネットワーク

- 異なるプロパティを含む SSL プロファイルが SSL 仮想サーバーに接続されている場合、DH (Diffie-Hellman) および一時的な RSA キーの値が正しく表示されません。値は、SSL プロファイルを持たない SSL 仮想サーバー IP に対してのみ正しく表示されます。
  [702680]
- Citrix ADC フェイルオーバー後、各パーティションのサービスまたはサービスグループについて、重複するサービスまたはサービスグループのエントリが表示されます。この問題は、既定のパーティションに属するサービスまたはサービスグループでは発生しません。
  [699224]

既知の問題

Analytics

- 場合によっては、HDX Insight ノードと Citrix Gateway インサイトノードが Citrix ADM GUI に表示されないことがあります。
  回避策：ページを更新して、もう一度試してください。
  [690327]

設定

- [設定] > [サブスクリプション] ページで、ストレージデータ消費が 5 GB という資格のあるストレージ制限よりも大きく表示されることがあります。
  [689330]
- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。
  [686581]
- Citrix ADM から Citrix SD-WAN WO または Citrix ADC SDX インスタンスをアップグレードすることはできません。
  [699814]

GUI の問題

- Internet Explorer 11 を使用してログオンすると、Citrix Cloud ナビゲーションバーは表示されません。[702339]

2018 年 **1** 月 **18** 日

このリリースには、新機能とバグ修正が含まれています。

デフォルトでは、Citrix ADM エージェントはビルド 508.116 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能

特定の **Citrix ADC** インスタンスから証明書をインポートする

特定の Citrix ADC インスタンスから証明書をインポートし、Citrix ADM GUI から他のターゲット Citrix ADC インスタンスに適用できるようになりました。この機能強化では、証明書をローカルシステムにダウンロードしてから、選択したインスタンスにダウンロードした証明書を適用する必要がありません。詳しくは、「Citrix ADC インスタンスに SSL 証明書をインストールする方法」を参照してください。

[688029]

複数の **Citrix ADC** インスタンスのネットワークレポートを表示する

Citrix ADM では、ネットワークレポートを生成しながら、複数の Citrix ADC インスタンス（および最大 5 台の仮想サーバー）を選択できます。複数のインスタンスのネットワークレポートデータを同時に監視できるようになりました。

Citrix ADM ネットワークレポート機能から生成されたレポートをエクスポートしてスケジュールすることもできます。詳しくは、「ネットワークレポート作成」を参照してください。

[665989]

高可用性モードで **Citrix ADC** インスタンスをアップグレードする

高可用性モードで Citrix ADC インスタンスを Citrix ADM からアップグレードするプロセスが改善されました。メンテナンスタスクを作成して、HA ペアを 2 段階でアップグレードできます。最初に最初のノードでアップグレードをスケジュールまたは実行し、その後で 2 番目のノードのアップグレードをスケジュールできます。管理者は、最初のノードのアップグレードが成功した場合のみ、2 番目のノードのアップグレードを続行できます。

> 注
>
> - 現在、HA ペアの 2 番目のノードが最初にアップグレードされ、最初のノードのアップグレードは後でス

> ケジュールされます。
> - ノードの同期と伝播は、両方のノードが正常にアップグレードされるまで無効になります。
> - 最初のノードのアップグレード時に、HA ペアのノードが異なるビルドまたはバージョン上にある場合、警告が表示されます。2 番目のノードが同じビルドとバージョンになるまで、2 番目のノードのアップグレードプロセスをキャンセルできます。または、ノードが同じビルドとバージョンにある後で、後でスケジュールすることもできます。

詳しくは、「Citrix ADC インスタンスをアップグレードする方法」を参照してください。

[694907]

サーバーのバインドされたエンティティの表示

これで、管理対象 Citrix ADC インスタンス上の特定のサーバーのバインドされたエンティティを表示できます。これで、次の項目が表示されます。

1. これで、選択した負荷分散サーバーのバインドされたサービスおよびバインドされたサービスグループを表示できます。

   [ネットワーク] > [ネットワーク機能] > [負荷分散] > [サーバー] に移動します。サーバーを選択し、[バインドされたサービスの表示] または [** バインドされたサービスグループの表示 **] をクリックします。[バインドされたサービス] ページで、サービスを有効または無効にし、エンティティをポーリングできます。同様に、[バインドされたサービスグループ] ページでは、サービスグループを有効または無効にしたり、バインドされたサービスグループのメンバーを表示したり、エンティティをポーリングしたりできます。

2. コンテンツスイッチング仮想サーバー上のサーバーのバインドされた LB 仮想サーバーを表示できます。

   [ネットワーク] > [ネットワーク機能] > [コンテンツスイッチング] に移動します。サーバーを選択し、[バインドされた **LB** 仮想サーバーの表示] をクリックします。[バインドされた LB サーバー] ページでは、仮想サーバーを有効または無効にしたり、ポーリングしたりできます。

   > 注: コンテンツスイッチング仮想サーバーを選択し、[バインドされた **LB** 仮想サーバーの表示] をクリックします。Citrix ADM には、デフォルトの LB サーバーとポリシーベースのターゲット LB 仮想サーバーが表示されます。

3. キャッシュリダイレクト仮想サーバー上のサーバーのバインドされたターゲット LB 仮想サーバーを表示できます。

   [ネットワーク] > [ネットワーク機能] > [キャッシュリダイレクト] に移動します [キャッシュリダイレクト仮想サーバー] ページに、新しい [ターゲット **LB** 仮想サーバー] 列が表示されます。このページには、ターゲットの LB 仮想サーバーの名前が表示されます。

[698772]

ライセンスされた仮想サーバーのスループットの詳細の表示

スループットの詳細（要求バイト数と応答バイトの合計）に基づいて、仮想サーバーに対するライセンスを管理および割り当てることができます。これは、[システムライセンス] ページの列として表示されます。[スループット] 列を並べ替えて、スループットの使用量が少ない仮想サーバを確認し、それに応じてライセンスを割り当てることができます。

スループットの詳細を表示する手順は、次のとおりです。

1. [ネットワーク] > [ライセンス] > [システムライセンス] に移動します。
2. [システムライセンス] ページの [管理対象仮想サーバー] で、[仮想サーバーの自動選択] オプションがオフになっていることを確認します。これで、管理する仮想サーバーを明示的に選択できます。
3. 仮想サーバを選択するには、[クリックして選択] を選択します。
4. [仮想サーバーの選択] ページで、各仮想サーバータブの下の列として [スループット] の詳細が表示されます。

[687056]

エージェントの設定と **Citrix ADC** インスタンスの追加に関する新しい構成フロー

Citrix ADM では、Citrix ADM エージェントを設定したり、Citrix ADC インスタンスを Citrix ADM に追加したりするための、直感的な新しい GUI が提供されるようになりました。詳しくは、「はじめに」を参照してください。

[700033]

スタイルブックの **Python SDK** サポート

Citrix ADM では、Python SDK は StyleBooks の NITRO 呼び出しをサポートするようになりました。

[672420]

Citrix ADC インスタンスに関する追加情報の表示

Citrix ADM 上の Citrix ADC インスタンスの次のパラメータに関する情報を表示できるようになりました。

- モデル **ID**：Citrix ADC インスタンスに適用されるライセンスのタイプから派生したモデル ID が表示されます。モデル ID は、[インスタンス] ページと [インスタンスダッシュボード] に表示されます。
- ホスト **ID**：ホスト ID が表示されます。ホスト ID は、Citrix ADC インスタンスの Mac ID です。ホスト ID は、インスタンスのライセンスを生成するために使用されます。ホスト ID は、[インスタンス] ページと [インスタンスダッシュボード] で確認できます。
- **NetScaler UUID**：一意のインターネットデバイスまたはデータを識別する汎用一意識別子（UUID）。アルゴリズムは、インスタンスのネットワークアドレスに基づく値を使用して UUID を生成します。インスタンスダッシュボードで NetScaler UUID を表示できます。
- **CPU: CPU** の現在の周波数を表示します。CPU は、負荷容量に応じて異なる周波数で動作します。MHz の増加/減少は、CPU、マザーボードのアーキテクチャ、および温度によって決まります。インスタンスダッシュボードで CPU 使用率の詳細を表示できます。
- 製造日：インスタンスダッシュボードに Citrix ADC インスタンスの製造日を表示します。

> 注**:** デフォルトでは、インスタンスのモデル ID とホスト ID は [インスタンス] ページに表示されません。

新しいパラメータを表示するには**:**

1. ［ネットワーク］ > ［インスタンス］ に移動し、パラメータ情報を表示する Citrix ADC インスタンスのタイプを選択します。
2. モデル ID とホスト ID を表示するには、次の手順を実行します。
   a) 右上にある [検索] の横にある [設定] アイコンをクリックします。
   b) [モデル ID] と [ホスト ID] を選択し、[完了] をクリックします。
   次の図に示すように、モデル ID とホスト ID の値が表示されます。
   c) ホスト ID、NetScaler UUID、CPU、および製造日をダッシュボードに表示するには、次の手順を実行します。
      i. インスタンスを選択し、[**Dashboard**] をクリックします。
      ii. ［情報］ セクションでは、次の図に示すように、モデル **ID**、ホスト **ID**、**NetScaler UUID**、**CPU**、および製造の上の詳細を表示できます。

[699550, 700266]

解決された問題

Analytics

- HDX Insight でセッションレポートにアクセスすると、Citrix ADM が断続的に失敗します。[701042]

ネットワーク

- デバイス API プロキシ要求が Citrix ADM に送信されると、応答ヘッダーにコンテンツ長と転送エンコードが返されます。これは RFC 2616 に反します。[700717]
- 現在、一部の依存リソース (ns_lbvserver、ns_csvserver など) に対するアクセス許可は、ネットワークレポート機能のアクセス許可の一部として与えられています。しかし、新しい機能強化の一環として、これらの権限は、[ネットワーク機能] の下の対応するノードにアクセスできる場合にのみ付与する必要があります。たとえば、負荷分散仮想サーバーでレポートを実行する場合は、[ネットワーク機能] の下の [負荷分散仮想サーバー] にのみアクセスでき、その逆も同様です。
  [700859]

既知の問題

Analytics

- 場合によっては、HDX Insight ノードと Citrix Gateway インサイトノードが Citrix ADM GUI に表示されないことがあります。
  回避策：ページを更新して、もう一度試してください。
  [690327]

設定

- [設定] > [サブスクリプション] ページで、ストレージデータ消費が 5 GB という資格のあるストレージ制限よりも大きく表示されることがあります。
  [689330]
- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。
  [686581]
- Citrix ADM から Citrix SD-WAN WO または Citrix ADC SDX インスタンスをアップグレードすることはできません。
  [699814]

2017 年 **12** 月 **28** 日

このリリースには、新機能とバグ修正が含まれています。

デフォルトでは、Citrix ADM エージェントはビルド 507.114 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能

ネットワーク機能サブノード用の **Citrix ADM** での **RBAC** のアクセスポリシーの構成

Citrix ADM ロールベースのアクセス制御（RBAC）のアクセスポリシー管理では、ネットワーク機能のサブノードの権限も構成できるようになりました。アクセスポリシー設定は、仮想サーバ、サービス、サービスグループ、サーバなど、すべてのサブノードに対して構成できます。現時点では、負荷分散ノードの下のサブノード、および GSLB ノードの下のサブノードに対してのみ、このような細かいレベルのアクセス許可を提供できます。詳細については、「Citrix Application Delivery Management アクセスポリシーの構成」を参照してください。

[692034]

選択したネットワーク機能のレポートをエクスポートおよびスケジュールする機能

Citrix ADM では、負荷分散、コンテンツスイッチング、キャッシュリダイレクト、グローバルサーバー負荷分散(GSLB)、認証、Citrix Gateway などの特定のネットワーク機能に関する包括的なレポートを生成できます。このレポートでは、ネットワークに存在する Citrix ADC インスタンス、パーティション、および対応するバインドされたエ

ンティティ（仮想サーバー、サービスグループ、サービス）間のマッピングの高レベルなビューを表示できます。これらのレポートは、.csv ファイル形式でエクスポートできます。

このレポートには、次の仮想サーバデータが表示されます。

- NetScaler の IP アドレス
- ホスト名
- パーティション・データ
- 仮想サーバのタイプ
- 仮想サーバ名
- ターゲット LB 仮想サーバー
- サービス名
- サービスグループ名。

詳細については、「ネットワーク機能レポートのエクスポートまたはエクスポートをスケジュールする方法」を参照してください。

[696259]

ファイルまたは **ZIP** バンドルを使用した **StyleBooks** のインポート

Citrix ADM では、複数の StyleBook を YAML 形式でインポートできます。複数の YAML StyleBook ファイルを Zip 形式 (.zip) 形式または tarball (.tgz, .gz) 形式で圧縮できます。詳しくは、「ユーザー定義スタイルブックの使用方法」を参照してください。

[694938]

SSL ダッシュボードでのデフォルトの **Citrix ADC** 証明書の除外

Citrix ADM では、SSL ダッシュボードのグラフに表示されるデフォルトの Citrix ADC 証明書の表示と非表示を切り替えることができます。SSL ダッシュボードでデフォルトの証明書を表示または非表示にするには:

1. Citrix ADM GUI で［ネットワーク］>［**SSL** ダッシュボード］に移動します。
2. [**SSL** ダッシュボード] ページで、[設定] をクリックします。
3. [設定] ページで、[編集] アイコンをクリックします。
4. [証明書フィルタの設定**]** セクションで、[既定の証明書を表示する] チェックボックスをオフにします。

詳細については、「SSL ダッシュボードのデフォルトの Citrix ADC 証明書を除外する」を参照してください。

[687609]

解決された問題

ネットワーク

- テンプレートリストからユーザー定義テンプレートを使用して設定ジョブを作成するには、テンプレートをエディタにドラッグし、新しい値を指定して変数を編集する必要があります。しかし、設定ジョブが実行されると、変数はユーザーが指定した新しい値に置き換えられません。[698812]
- Citrix ADM では、イベントのルールにイベント経過期間が設定されている場合、それらのイベントは GUI に表示されません。また、EntityUp、entityDown、および entityYOFS エンティティは相関関係にあるため、同じイベントに対して更新する必要があります。しかし、これらのトラップはイベントメッセージで別々に見られます。[699487]
- Citrix ADM が HDX Insight レポートをエクスポートすると、チャネル帯域幅の値が正しくありません。[700011]
- Citrix ADM は、［イベント］に、ライセンスが今後 30 日以内に期限切れになることを示すメッセージを表示します。ただし、ライセンスはそれより早く期限切れになる可能性があります。[696976]

既知の問題

Analytics

- 場合によっては、HDX Insight ノードと Citrix Gateway インサイトノードが Citrix ADM GUI に表示されないことがあります。

回避策：ページを更新して、もう一度試してください。[690327]

ネットワーク

- 現在、一部の依存リソース(`ns\\_lbvserver,ns\\_csvserver etc`)に対するアクセス許可は、ネットワークレポート機能のアクセス許可の一部として与えられています。しかし、新しい機能強化の一環として、これらの権限は、[ネットワーク機能] の下の対応するノードにアクセスできる場合にのみ付与する必要があります。たとえば、負荷分散仮想サーバーでレポートを実行する場合は、[ネットワーク機能] の下の [負荷分散仮想サーバー] にのみアクセスでき、その逆も同様です。[700859]

設定

- [設定] > [サブスクリプション] ページで、ストレージデータ消費が 5 GB という資格のあるストレージ制限よりも大きく表示されることがあります。[689330]
- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。[686581]
- Citrix ADM 506.119 ビルドから Citrix SD-WAN WO または Citrix ADC SDX インスタンスをアップグレードすることはできません。[699814]

2017 年 12 月 07 日

このリリースには、新機能とバグ修正が含まれています。

デフォルトでは、Citrix ADM エージェントはビルド 506.122 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能

親子デプロイおよび統計ベースの **GLB** アルゴリズムをサポートするためのマルチクラウド **GLB StyleBook** の機能強化

Global Load Balancing（GLB）ソリューションにより、ユーザーはクライアント要求を複数のデータセンターおよびアプリケーションサーバーに分散できます。データセンターは複数のクラウドに分散され、アプリケーションサーバーはオンプレミスでデプロイされます。このソリューションでは、次の機能をサポートしています。

- 親子トポロジ。トポロジは、統計情報ベースの GLB アルゴリズムを使用して GLB ノードと LB ノードを設定する場合に使用されます。このトポロジは、LB ノードが別の Citrix ADC インスタンスに展開されている場合にも使用されます。
- スピルオーバーの持続性。プライマリへの負荷がしきい値を下回った後も、バックアップ仮想サーバは、受信した要求を処理し続けます。
- インターネットプロトコルバージョン 6 (IPv6)。
- メトリックベース、非メトリックベース、および近接ベースの GLB メソッド。

「マルチクラウド GLB StyleBook」バージョン 1.1 を使用して、選択した GLB Citrix ADC インスタンスで GLB 構成を実行します。次のいずれかの場合に、マルチクラウド GLB StyleBook for LB ノードを使用して、一度に 1 つの LB ノードを設定して GLB 親子トポロジを作成します。

- メトリックベースの GLB アルゴリズム（最小パケット、最小接続、最小帯域幅）を使用して GLB ノードと LB ノードを構成する場合
- LB ノードが別の Citrix ADC インスタンスに展開されている場合
- サイトの永続性を構成する場合

最大 1024 の子サイトを構成できます。

詳しくは、「ハイブリッドおよびマルチクラウド環境向けの Citrix ADC グローバル負荷分散」を参照してください。

[694250]

グループ作成時の **StyleBook** の **RBAC** サポート

Citrix ADM では、ユーザーがユーザーグループの作成中にアクセスできる選択した StyleBook を追加できます。

選択した **StyleBook** をグループに追加するには**:**

1. Citrix ADM で、［システム］>［ユーザー管理］>［グループ］に移動します。
2. ［追加］をクリックします。
3. [グループ名] ボックスに、グループの名前を入力し、必要なロールを選択します。

4. [アプリケーションとテンプレート] タブで、[StyleBooks] チェックボックスをオフにし、ユーザーがアクセスできる必須の StyleBooks を選択します。
5. [ユーザーの選択] タブで、グループに追加するユーザーを選択します。
6. [完了] をクリックします。

詳しくは、「Citrix Application Delivery Management でのグループの構成」を参照してください。

[657834, 664844]

グループの説明の提供

Citrix ADM では、グループを作成するときに、[グループの説明] ボックスにグループの説明を入力できるようになりました。グループの適切な説明を入力します。良い説明は、後でより良い方法でグループの役割と機能を理解するのに役立ちます。詳しくは、「Citrix Application Delivery Management でのグループの構成」を参照してください。

[685186]

Citrix ADM インテリジェントアプリ分析の統合

Citrix ADM インテリジェントなアプリケーション分析機能は、アプリケーション用に構成された仮想サーバーとサービスを監視し、それらに関する重要な情報を表示します。この機能を使用すると、システム停止やその他のイベント時の監視、管理、および意思決定を行うことができます。インテリジェントアプリ分析のいくつかの主要な機能は次のとおりです。

- 機械学習アルゴリズムを活用
- トラフィック動作を学習します
- 許容可能なパターンと許容できないパターンを区別する
- 管理者に明確な洞察を提供
- 管理者が適切なアクションを実行できるようにする

詳しくは、「インテリジェントなアプリケーション分析」を参照してください。

[698730]

AWS の **Citrix ADM** エージェントを **Citrix ADM** に自動的に登録する

Amazon Web Services（AWS）で Citrix ADM エージェントをデプロイするときに、Citrix ADM のサービス URL とアクティベーションコードの詳細を指定することで、Citrix ADM エージェントを Citrix ADM に自動的に登録できるようになりました。詳しくは、「AWS に Citrix ADM エージェントをインストールする」を参照してください。

[688901]

Citrix ADM が **ChangeConfig SNMP** トラップを受信したときの構成監査

ネットワーク内の Citrix ADC インスタンスで構成が変更されると、インスタンスによって構成が更新されます。その後、インスタンスは、ConfigChange SNMP トラップを Citrix ADM に送信します。Citrix ADM を有効にして、そのインスタンスに対して構成監査を実行できます。ConfigChange SNMP トラップを受信するたびに、構成監査差分を生成するように Citrix ADM を構成できます。詳しくは、「ConfigChange SNMP トラップの構成監査差分を生成する方法」を参照してください。

[682007]

メンテナンスタスクのスケジューリングのサポート

Citrix ADM を使用して、次のすべてのメンテナンスタスクを特定の日時にスケジュールできるようになりました。

- Citrix ADC インスタンスのアップグレード
- Citrix SDWAN-WO インスタンスのアップグレード
- Citrix ADC SDX インスタンスのアップグレード
- Citrix ADC インスタンスの HA ペアを構成する
- HA インスタンスのペアをクラスターに変換する

メンテナンスタスクのスケジューリング中に電子メール通知を設定することもできます。設定が完了すると、ジョブが実行またはスケジュールされるたびに、電子メール通知が送信されます。

[681934]

StyleBook の定義を表示/作成するための組み込みの **YAML** ビューア/エディタ

Citrix ADM には、YAML ガイドラインに対応する StyleBook を作成できる組み込みの YAML エディタが用意されています。コンテンツは YAML 標準に照らして検証され、偏差が強調表示されます。その後、コンテンツを修正し、StyleBook を Citrix ADM にインポートできます。組み込みの YAML エディタは、独自の StyleBook を作成する際に 2 つの利点を提供します。

- 色分けされています。コンテンツの色分けは、YAML コンテンツで定義されているキーと値を簡単に区別するのに役立ちます。
- YAML 検証です。入力時にコンテンツが YAML エラーに対して検証され、偏差が即座に強調表示されます。

詳しくは、「ユーザー定義スタイルブックの使用方法」を参照してください。

[695951]

Citrix ADM GUI でのプライベートスタイルブックの表示

StyleBooks（パブリックとプライベートの両方）の数が増えるにつれて、アクセスしたい特定の StyleBook を検索する機能が必要です。また、両方のタイプの StyleBook を別々に表示する機能も必要です。Citrix ADM GUI で［アプリケーション］>［StyleBooks］に移動すると、システムに存在する StyleBook のリストを表示できます。両

方のタイプの StyleBook には、プライベートまたはパブリックとして宣言する個別のアイコンがあります。詳しくは、「StyleBook の異なるグループを表示する方法」を参照してください。

[686913]

HAProxy アプリダッシュボードの統合

Citrix ADM では、アプリケーション分析と管理機能が拡張され、HAProxy アプリケーションがサポートされます。アプリケーションダッシュボードには、Citrix ADM によって監視されるすべてのアプリケーション、つまり Citrix ADC と HAProxy の両方のアプリケーションの完全なビューが表示されます。HAProxy 個別のアプリケーションは、管理対象の HAProxy フロントエンドごとに自動的に作成されます。これらのアプリケーションをグループ化して、Citrix ADC アプリケーションと同様のカスタムアプリケーションを形成することもできます。

> 注:
>
> HAProxy アプリケーションではアプリアクティビティ調査員を利用できません。詳しくは、「アプリケーションダッシュボードの HAProxy アプリケーション」を参照してください。

[693309]

アプリダッシュボードとセキュリティダッシュボードのレポートのエクスポート

Citrix ADM では、［アプリダッシュボード］ページと［セキュリティダッシュボード］ページをレポートとしてエクスポートできます。

1. [アプリケーションダッシュボード] ページで、ページの右上にある [エクスポート] アイコンをクリックします。
2. エクスポートオプションを.pdf または.png ファイルとして選択します。
3. ［**OK**］をクリックします。

レポートがシステムにダウンロードされます。現在、一度に 1 つのアプリケーションのレポートしかダウンロードできません。詳しくは、「アプリダッシュボードとセキュリティダッシュボードのレポートをエクスポートする」を参照してください。

[693753]

Citrix ADM でのアプリスコアの構成

Citrix ADM では、アプリスコアを構成できます。アプリスコアの計算は、次の 3 つの主要コンポーネントの平均値に基づいています。

- パフォーマンススコア（アプリケーションの APDEX スコア）
- Citrix ADC インスタンスリソース
- サーバリソース

検出されたすべてのアプリケーションと、アプリケーションダッシュボードで定義したカスタムアプリケーションについて、アプリケーションスコアが表示されます。詳しくは、「アプリケーションのパフォーマンス分析」を参照してください。

[693758]

アプリアクティビティ調査官の **AppScore** コンポーネントのしきい値違反の詳細の表示

[ダッシュボード] タブの [App Activity Investigator] には、App Score コンポーネント、エラー、イベント、異常など、選択したアプリケーションの主要な情報が表示されます。各凡例は、選択した期間が 1 時間の場合は 1 分間隔で、選択した期間が 1 日の場合は 1 時間間隔で集計されます。これらの偏差は、グラフ上に長方形の凡例として表示されます。これらの凡例は集計され、発生したイベントの数に応じて色分けされます。

[693769]

HDX Insight のしきい値の作成とルールとアラートの構成

Citrix ADM HDX Insight のしきい値管理では、設定したしきい値を超えるたびにアラートをプロアクティブに構成できます。このしきい値管理は、しきい値ルールのグループを設定し、個々のルールではなくグループをモニタするように拡張されます。しきい値ルールグループは、期待値を持つユーザー、アプリ、デスクトップなどのエンティティから選択されたメトリックのユーザー定義しきい値ルールを 1 つ以上構成します。

[652441]

HDX Insight のしきい値の作成とルール、アラート、ジオロケーションの構成

Citrix ADM HDX Insight のしきい値管理では、設定したしきい値を超えるたびにアラートをプロアクティブに構成できます。このしきい値管理は、しきい値ルールのグループを設定し、個々のルールではなくグループをモニタするように拡張されます。しきい値ルールグループは、期待値を持つユーザー、アプリ、デスクトップなどのエンティティから選択されたメトリックのユーザー定義しきい値ルールを 1 つ以上構成します。しきい値グループは、ユーザーエンティティの地理固有のモニタリングのために、ジオロケーションにバインドすることもできます。

[652447]

解決された問題

ネットワーク

- Citrix ADM GUI では、Citrix ADC インスタンスのホスト名が［SSL 証明書］の詳細ページに表示されません。この修正により、ホスト名が表示されます。

    1. Citrix ADM で、［ネットワーク］>［**SSL** ダッシュボード］に移動します。
    2. [**SSL** ダッシュボード] ページで、円の 1 つをクリックします。
    3. [**SSL** 証明書**]** ページで証明書を選択し、[詳細] をクリックします。[670374]

- インスタンスバックアップ設定をスケジュールする場合、スケジュールされたバックアップ時刻と Citrix ADM GUI に表示される時刻には数時間の差があります。[695489]
- Citrix ADM GUI の［ネットワークレポート］ページから 2 つのグラフをエクスポートする場合、最初のグラフのみがレポートとしてエクスポートされます。この修正により、[ネットワークレポート] ページのすべてのグラフがエクスポートされるようになりました。

  > 注:
  >
  > レポートは、.pdf、.png、または.jpeg 形式でエクスポートされます。[699380]

- Citrix ADM で、［ネットワーク］>［構成ジョブ］>［メンテナンスタスク］の順に選択し、［**NetScaler** アップグレード］を選択すると、Citrix ADC インスタンスのアップグレードが失敗します。[692538]

高可用性

- Citrix ADC インスタンスバックアップは、インスタンスが高可用性で展開されると、プライマリおよびセカンダリ Citrix ADC インスタンスの両方に対してトリガーされます。[698903]
- 高可用性セットアップの Citrix ADC インスタンスがフェイルオーバーし、新しいプライマリに Citrix ADM からアクセスできない場合、そのインスタンスは Citrix ADM GUI に表示されなくなります。[697017]

設定

- Citrix ADM メンテナンスタスクが機能していません。[696952]

既知の問題

Analytics

- 場合によっては、Citrix ADM GUI に HDX Insight サイトノードと Gateway Insight ノードが表示されないことがあります。
  回避策：ページを更新して、もう一度試してください。[690327]

設定

- [設定] > [サブスクリプション] ページで、ストレージデータ消費が 5 GB という資格のあるストレージ制限よりも大きく表示されることがあります。[689330]
- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。[686581]
- Citrix ADM 506.119 ビルドから Citrix SD-WAN WO または Citrix ADC SDX インスタンスをアップグレードすることはできません。[699814]

2017 年 11 月 17 日

このリリースには、新機能とバグ修正が含まれています。

デフォルトでは、Citrix ADM エージェントはビルド 505.117 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能

Citrix ADM でのエージェントのプロキシサーバーのサポート

これで、プロキシサーバーを使用してエージェントを Citrix ADM に接続できます。この機能強化を使用すると、エージェントはすべてのデータをプロキシサーバーに転送し、プロキシサーバーはそのデータをインターネット経由で Citrix ADM に送信します。

プロキシ・サーバを使用してデータを転送するには、次のスクリプトを使用してエージェント上のプロキシ・サーバの詳細を入力し、スクリプトの指示に従って詳細情報を入力します。proxy_input.py エージェントは、プロキシサーバーを使用して Citrix ADM に接続している間、この情報を取得します。

ユーザー名とパスワード情報を入力して、プロキシサーバーを認証できます。エージェントがデータを送信すると、プロキシサーバーはユーザー資格情報を認証してから、Citrix ADM に転送します。

> 注**:** プロキシサーバーは、基本認証のみをサポートしています。

[697617]

StyleBook を使用して **Citrix ADC** インスタンスで **Google Apps** シングルサインオンを有効にする

Citrix ADM のデフォルトの SSO Google Apps StyleBook では、Citrix ADC インスタンスで Google アプリケーションのシングルサインオンを有効にできます。StyleBook は、ユーザーが Google Apps にアクセスできるように認証するための SAML アイデンティティプロバイダとして Citrix ADC インスタンスを構成します。詳しくは、「SSOGoogle Apps 使い方 StyleBook」を参照してください。

[697027]

アプリケーションのピーク使用率トレンドをアプリケーションのパフォーマンスで評価する機能

これで、アプリケーションのピーク使用傾向を評価できます。Citrix ADM の［アプリケーションダッシュボード］から、アプリケーションスコアに基づいてアプリケーションのパフォーマンスへの影響を比較することもできます。アプリケーション情報に対するピーク使用傾向とパフォーマンスの影響を使用して、展開で必要な変更を加えることができます。これは、アプリケーションのパフォーマンスを向上させるのに役立ちます。

アプリケーションのピーク使用傾向を表示するには、「アプリケーション」>「**App Dashboard** 」に移動します。アプリケーションを選択し、[ピーク使用量] をクリックします。

詳しくは、「アプリケーション使用率のトレンド」を参照してください。

[688208]

解決された問題

ネットワーク

- Citrix **ADM** 構成［ジョブ］>［ジョブ］ページで、背景が青色の行の場合、［ジョブの作成］ボタンは無効になります。今回の修正により、[**Create Job**] ボタンがアクティブになり、無効になりません。[695397]
- [**Citrix ADM Networks**］>［イベント］>［イベントメッセージ］で、日付に基づいてイベントメッセージをソートしようとすると、ソートが正しく行われません。メッセージは、ソート矢印の方向と逆の順序でソートされます。たとえば、メッセージを新しいものから古い順にソートすると、矢印は上向きになります。[696737]
- 構成のアドバイスのために ns.conf ファイルを Citrix ADM にアップロードすると、検証エラーが発生します。[696920]
- Citrix ADM に送信されたトラップメッセージには、エンティティの名前と、トラップの発信元の仮想サーバーの IP アドレスとポートが表示されます。次の例は、Citrix ADM が受信したトラップメッセージのエンティティ名を示しています。

```
1     Entity Name
2      server_svc_NSSVC_IPFIX_10.102.29.150:4739       (service_10
          .102.29.150_33554)_DOWN
3  <!--NeedCopy-->
```

- **Citrix ADM** では、［ネットワーク］**>** ［イベント］**>** ［イベントメッセージ］テーブルの［メッセージ］列に、エンティティの名前、**IP** アドレス、およびポート番号が個別のパラメーターとして表示されません。[696639]
- イベントルールでは、スペース (“ “) を含むメッセージを持つスクリプトを実行すると、スクリプトはアクティブになりません。[696896]
- 一部のネットワークレポートは、Citrix ADM で生成するのに長い時間がかかります。このようなレポートのエクスポートがスケジュールされている場合、不完全なレポートがエクスポートされます。この修正により、Citrix ADM はレポートが完全に生成されるまで待機してからエクスポートします。[695500]
- Citrix ADM では、一部の表形式のビューとダッシュボードのレポートをエクスポートできません。この修正により、テーブルとダッシュボードのコンテンツをエクスポートできるようになりました。[670226]
- Citrix ADM では、リストビューに表示され、さらに特定のページに移動したとします。GUI の左側にあるナビゲーションペインを使用して戻ることはできません。ページの上部にあるパンくずリストを使用して移動する必要がある場合があります。たとえば、現在 [ネットワーク] > [インスタンス] > [**NetScaler VPX**] > [バックアップ**/**復元] ページが表示されているとします。［ネットワーク］>［インスタンス］で［Citrix **ADC** インスタンスタイプ］を選択すると、ナビゲーションペインで［NetScaler VPX］をクリックした後、対応する Citrix ADC インスタンスリストページが開きません。[684922]

- Citrix ADM では、Citrix ADM を使用した Citrix ADC インスタンスのアップグレードが失敗します。［ネットワーク］>［構成ジョブ］>［メンテナンスタスク］の順に選択し、［**NetScaler** アップグレード］を選択すると、Citrix ADC インスタンスのアップグレードが失敗します。[692538]
- 特定の時刻に実行するようにスケジュールされている構成監査テンプレートは、グローバルポーリング中にも実行され、構成監査テンプレートが繰り返し実行されます。[697157]
- 特定の変数値を使用した構成監査は、高可用性モードの Citrix ADC インスタンスでは機能しません。[696990]
- 設定監査テンプレートの作成中は、変数値の入力ファイルをアップロードできません。[697137]
- Citrix ADM では、構成監査レポートの処理中にエラーが発生すると、メールの受信者に空のメールが送信されます。[697138]

設定

- 高可用性での Citrix ADM でのノードの登録と展開時に、両方のノードのパスワードはデフォルトのパスワード「ns root」である必要があります。パスワードが`nsroot`と異なる場合、ノードの登録は失敗します。[691836]
- Citrix ADM では、名前や説明などの入力フィールドに「&」などの特殊文字を入力すると、「&」が「&」に置き換えられます。[692656]
- Citrix ADM では、名前や説明などの入力フィールドに「&」などの特殊文字を入力すると、「&」が「&」に置き換えられます。[692656]
- グループにアプリケーションを追加したり、正規表現を指定して検索条件を適用してグループにアプリケーションを追加することもできます。このような場合、グループを複数回編集すると、アプリケーションの名前が無効な regex 式に変換されます。これにより、RBAC が失敗し、ユーザーはすべてのアプリケーションを表示できます。

  1. Citrix ADM で、［システム］>［ユーザー管理］>［グループ］の順に選択し、［追加］をクリックします。グループ名を入力し、[承認設定] タブで、必要なアプリケーションを選択してグループに追加し、[グループの作成] をクリックします。
  2. 正規表現を追加する場合は、[グループ] ページに移動し、グループを選択して [編集] をクリックします。
  3. [承認設定] タブで、[正規表現の追加] テキストボックスに正規表現を追加し、設定を保存します。
  4. グループを再度編集する場合は、[承認の設定] タブで、以前に追加したアプリケーションの名前が正規表現に変換されることがあります。これは無効な正規表現であるため、RBAC は失敗し、ユーザーはすべてのアプリケーションを見ることができます。[696515]

高可用性

- 高可用性セットアップの Citrix ADC インスタンスがフェイルオーバーし、新しいプライマリに Citrix ADM からアクセスできない場合、そのインスタンスは Citrix ADM GUI に表示されなくなります。[697017]

- 高可用性セットアップ内のある Citrix ADC インスタンスから、同じペアの別のインスタンスにバックアップファイルを復元すると、IP アドレスが競合するため、その Citrix ADC インスタンスにアクセスできなくなります。Citrix ADM は、バックアップファイル内の IP アドレスと復元を実行するインスタンスの IP アドレスが同じかどうかをチェックします。IP アドレスが一致しない場合は、エラーメッセージが表示され、復元が停止します。[686829]
- 高可用性にある Citrix ADC インスタンスのペアをアップグレードすると、Citrix ADC インスタンスは不安定になります。インスタンスは、Citrix ADM から送信された NITRO 呼び出しに応答する前に、しばらく待たなければならない場合があります。
- この修正により、インスタンスプロファイルで待機時間を設定して、Citrix ADM がインスタンスに NITRO 呼び出しを送信する前に、設定された時間を待つようにすることができます。デフォルトの待機時間は 60 秒です。[690860]

既知の問題

Analytics

- 場合によっては、Citrix ADM GUI に HDX Insight サイトノードと Gateway Insight ノードが表示されないことがあります。
  回避策：ページを更新して、もう一度試してください。[690327]

ネットワーク

- Citrix ADM で、［ネットワーク］>［構成ジョブ］>［メンテナンスタスク］の順に選択し、［**NetScaler** アップグレード］を選択すると、Citrix ADC インスタンスのアップグレードが失敗します。[692538]

設定

- [設定] > [サブスクリプション] ページで、ストレージデータ消費が 5 GB という資格のあるストレージ制限よりも大きく表示されることがあります。[689330]
- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。[686581]
- Citrix ADM メンテナンスタスクが機能していません。[696952]

2017 年 10 月 27 日

このリリースには、新機能とバグ修正が含まれています。

デフォルトでは、Citrix ADM エージェントはビルド 504.115 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。また、エージェントのアップグレードを実行する時刻を指定することもできます。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

新機能

構成テンプレートをインポートおよびエクスポートする機能

構成テンプレートをエクスポートして、Citrix ADM 内の同じテナントまたは別のテナントにテンプレートをインポートできます。エクスポートされたテンプレートデータ（構成コマンド、変数定義、パラメータなど）は、インポート後も失われません。

構成テンプレートをエクスポートするには、[ネットワーク**] > [**構成ジョブ**] > [**構成テンプレート] に移動します。構成テンプレートを選択し、[**Export**] をクリックします。エクスポートされた構成テンプレートは、**JSON** ファイル形式でローカルシステムに保存されます。その後、Citrix ADM 内の同じテナントまたは別のテナントにこのファイルをインポートして、構成テンプレートを作成できます。設定テンプレートをインポートするには、[**Import**] をクリックし、ローカルに保存した **JSON** ファイルを選択します。

詳しくは、「構成テンプレートのインポートとエクスポート方法」を参照してください。

[691585]

管理者パーティションのリビジョン履歴差分と監査テンプレートのサポート

Citrix ADM では、リビジョン履歴の違いと管理者パーティションの監査テンプレートがサポートされるようになりました。

管理者パーティションのリビジョン履歴の違いにより、パーティション化された Citrix ADC インスタンスの 5 つの最新の構成ファイルの違いを確認できます。構成ファイルを相互に（構成リビジョン 1 と構成リビジョン-2 の例）、または Configuration Revision を使用して現在実行または保存された構成と比較できます。構成の違いとともに、修正構成も示されています。すべての修正コマンドをローカルフォルダにエクスポートし、設定を修正できます。

パーティションの監査テンプレートを使用すると、カスタム構成テンプレートを作成し、それをパーティションインスタンスに関連付けることができます。監査テンプレートを使用したインスタンスの実行構成の変化は、[Audit Reports] ページの [Template vs Running diff] 列に表示されます。構成の違いとともに、修正構成も示されています。また、すべての修正コマンドをローカルフォルダにエクスポートして、設定を修正することもできます。

[657300]

構成ジョブに異なるタイプの複数のテンプレートを追加する機能

設定ジョブの作成中に、設定ジョブエディタで異なるタイプの複数のテンプレートを追加できるようになりました。複数のテンプレートを追加するには、[ネットワーク**] > [**構成ジョブ] に移動し、[ジョブの作成**]** をクリックします。[**Create Job**] ページで、ジョブ名を入力し、インスタンスタイプを選択します。[**Configuration Source**] ドロップダウンリストから、必要なソースを選択し、必要な複数のテンプレートを構成エディタにドラッグできます。テンプレートのソースタイプは、設定テンプレート、作成テンプレート、マスター構成、レコードと再生、インスタンス、ファイルです。

詳しくは、「Citrix ADM で構成ジョブを作成する方法」を参照してください。

[686881]

設定ジョブの入力変数値を保持する機能

Citrix ADM では、構成ジョブの作成中に、入力ファイルを含む指定された入力変数値が永続化されるようになりました。これらの値と、構成ジョブの作成時に以前にアップロードした入力ファイルも表示および編集できます。入力変数の値を表示するには、[ネットワーク**] > [**構成ジョブ] に移動し、ジョブを選択して [編集] をクリックします。[変数値の指定] タブでは、永続的な変数値を表示できます。以前にアップロードした入力ファイルも保持されます。入力ファイルをダウンロードし、ファイルを編集してから、名前を変更せずに同じ入力ファイルをアップロードできます。

[691584]

構成ジョブエディタでコマンドを並べ替える機能

これで、構成ジョブエディタでコマンドを並べ替えたり、順序を変更したりできます。これで、コマンドラインをドラッグして、コマンドを 1 行から別の行に移動できます。コマンドライン番号を変更するだけで、コマンドラインを 1 行から任意のターゲット行に移動または並べ替えることもできます。

[684164]

Citrix ADM ネットワークレポートプルーンの設定の構成

Citrix ADM でネットワークレポートデータのプルーニング間隔を構成できるようになりました。これにより、Citrix ADM サーバーのデータベースに保存されるネットワークレポートデータの量が制限されます。デフォルトでは、ネットワークが履歴データをレポートする場合、プルーニングは 24 時間ごと（01.00 時間ごと）実行されます。

[692461]

設定ジョブで変数をプレビューおよび変更する機能

Citrix ADM では、単一の統合ビューで構成ジョブを作成または編集するときに定義したすべての変数をプレビューできるようになりました。

[構成ジョブエディタ] の [変数のプレビュー] タブをクリックして、単一の統合ビューで変数をプレビューします。新しいポップアップウィンドウが表示され、名前、表示名、タイプ、デフォルト値などの変数のすべてのパラメータが表形式で表示されます。これらのパラメータを編集および修正することもできます。パラメータを編集または変更したら、[完了] をクリックします。

次のいずれかの操作を実行して、単一の統合ビューですべての変数をプレビューできます。

- 設定ジョブの作成 [ネットワーク**] > [**構成ジョブ] に移動し、[ジョブの作成] を選択します。**[** ジョブの作成] ページでは、すべての変数をプレビューできます。
- 設定ジョブの編集 [ネットワーク**] > [**構成ジョブ] に移動し、ジョブ名を選択して [編集] をクリックします。[ジョブの構成] ページでは、構成ジョブの作成時に追加されたすべての変数をプレビューできます。

[684166]

Citrix ADM でアプリケーションをグループに動的に追加するためのワイルドカードサポート

Citrix ADM でグループにアプリケーションを追加する場合、正規表現を使用して、正規表現の条件を満たすアプリケーションを検索し、グループに追加できます。これらのグループにバインドされているユーザーは、それらの特定のアプリケーションにのみアクセスできます。指定された正規表現式は、Citrix ADM に保持されます。新しいアプリケーションがシステムに追加されると、Citrix ADM は新しいアプリケーションに検索条件を適用し、条件に一致するアプリケーションが動的にグループの一部になります。新しいアプリケーションをグループに手動で追加する必要はありません。アプリケーションはシステム内で動的に更新され、各グループのユーザーは、Citrix ADM 適切なモジュールの下にあるアプリケーションを表示できます。

詳しくは、「Citrix ADM でのグループの構成」を参照してください。

[692032]

設定監査テンプレートでの特定の変数値の割り当て

Citrix ADM では、構成監査テンプレートの作成中に変数を作成し、変数に値を割り当てることができます。**[** ネットワーク**]** > **[** 構成監査**]** > **[** 監査テンプレート**]** > **[** 追加**]** > **[** テンプレートの作成**]** の **[** 変数値の指定**]** タブで、変数に値を割り当てる 2 つのオプションがあります。

1. すべてのインスタンスの共通の変数値。選択したインスタンスについて、このページにリストされている変数に共通の値を入力するには、このオプションを選択します。
2. 変数値の入力ファイルをアップロードします。ファイルをダウンロードし、変数の値を入力し、ファイルを Citrix ADM にアップロードするには、このオプションを選択します。

詳しくは、「監査テンプレートの作成」を参照してください。

[691127]

設定監査相違レポートのエクスポート

Citrix ADM では、構成監査セクションで構成監査差分レポートをダウンロードできます。[Configuration Audit] セクションでは、すべてのインスタンスおよびインスタンスごとにサマリーレポートをエクスポートできます。また、インスタンステンプレートペアごとに詳細な差分レポートをエクスポートすることもできます。

詳しくは、「監査レポートの表示」を参照してください。

[679736]

構成監査テンプレートと電子メール設定相違レポートをスケジュールする機能

Citrix ADM では、[ネットワーク] > [構成監査] > [監査テンプレート**]** のすべての監査テンプレートを、要件に応じて個別またはグローバルにスケジュールした時刻に実行できます。システムによって設定されたデフォルトの時刻にテンプレートを実行するのではなく、設定監査テンプレートを特定の時刻に実行するようにスケジュールできます。[テンプレートのスケジュールをカスタマイズ] オプションを選択すると、毎日、週の特定の日、または月の特定の日に

テンプレートを実行するようにスケジュールできます。各オプションについて、Citrix ADM でテンプレートを実行する必要があるスケジュール時刻も入力する必要があります。Citrix ADM では、構成監査差分レポートのエクスポートをスケジュールするために、次のオプションが用意されています。

- グローバルポーリング間隔を使用します。Citrix ADM でグローバルに構成されたインスタンスでテンプレートを一度に実行するには、このオプションを選択します。
- テンプレート集計表をカスタマイズします。このオプションを使用して、テンプレートを実行する必要がある時刻と頻度を設定します。
- 電子メールでレポートを送信します。このオプションを使用して、差分レポートの送信先となるメールプロファイルをメール添付ファイルとして構成します。

詳しくは、「監査テンプレートの作成」を参照してください。

[681957]

StyleBook の依存関係をグラフとして視覚化する機能

StyleBook のすべての依存関係、つまり選択した StyleBook が依存している他の StyleBook を視覚化できるようになりました。依存関係は、既存の StyleBook を使用して新しい StyleBook を構成した結果として作成されます。依存関係は、ボックスと矢印のグラフとして視覚化されます。各ボックスは StyleBook を表し、各矢印は StyleBook から依存する方向への依存を表します。「アプリケーション」>「構成」>「**StyleBooks** 」の順に選択し、右側のパネルに表示される StyleBook のリストで、表示する StyleBook の「依存関係の表示」リンクをクリックします。

[697175]

カスタム **StyleBook** と依存カスタム **StyleBook** のダウンロード

カスタム StyleBook とその依存 StyleBook を YAML 形式で ZIP または TGZ ファイルとしてシステムにダウンロードできるようになりました。Citrix ADM で、［アプリケーション］>［構成］>［**StyleBooks**］の順に選択し、右側のパネルに表示されている StyleBook のリストから、ダウンロードする **StyleBook** の［ダウンロード］リンクをクリックします。

> 注**:** 既定の StyleBooks をダウンロードすることはできません。

[696383]

カスタム **StyleBook** と依存するカスタム **StyleBook** の削除

カスタム StyleBook とその依存する StyleBook は、Citrix ADM フォルダシステムから削除できます。「アプリケーション」>「構成」>「**StyleBooks**」の順に選択し、右側のパネルに表示されている StyleBook のリストから、削除する StyleBook の右側にある「**X**」アイコンをクリックします。ファイルだけを削除するか、依存しているすべての StyleBook を削除するかを選択できます。

> 注：デフォルトの StyleBook は削除できません。

[696384]

HAProxy インスタンスの管理と監視

Citrix ADM を使用して、展開内の HAProxy インスタンスを管理および監視できるようになりました。HAProxy ホストを Citrix ADM に追加すると、ホスト上の HAProxy インスタンスが自動的に検出され、以下の情報を指定して管理および監視できるようになります。

- **HAProxy** アプリケーションダッシュボード: HAProxy インスタンスのフロントエンドのリアルタイム統計を表示します。ダッシュボードには、検出されたアプリケーションとしてフロントエンドが表示され、リアルタイムトランザクション、スループット、およびアプリケーションに関するセッション情報が表示されます。
- **HAProxy** インスタンスを再起動する機能：Citrix ADM GUI から HAProxy インスタンスを再起動できます。また、Citrix ADM GUI から HAProxy インスタンスをハード再起動またはソフト再起動することもできます。

詳しくは、「HAProxy インスタンスの管理とモニタリング」を参照してください。

[637830]

解決された問題

このリリースでは、次の問題が修正されました。

Analytics

- Citrix ADM で Citrix ADC CPX インスタンスを追加した場合、分析機能にはデータが表示されません。
  回避策：Citrix ADC CPX インスタンスを Citrix ADM に追加しないでください。[694792]

エージェント

- [ネットワーク] > [エージェント] に移動し、[エージェント] 画面からエージェントをダウンロードしようとすると、「ファイルが見つかりません」などのエラーが表示されることがあります。
  回避策：エージェントをダウンロードするには、[設定] > [エージェントの設定] に移動し、ハイパーバイザーを選択して [イメージのダウンロード] をクリックします。[695998]

既知の問題

このリリースの既知の問題は次のとおりです：

Analytics

- 場合によっては、Citrix ADM GUI に HDX Insight サイトノードと Gateway Insight ノードが表示されないことがあります。
  回避策：ページを更新して、もう一度試してください。[690327]

ネットワーク

- Citrix ADM では、Citrix ADM を使用した Citrix ADC インスタンスのアップグレードが失敗します。［ネットワーク］>［構成ジョブ］>［メンテナンスタスク］の順に選択し、［**NetScaler** アップグレード］を選択すると、Citrix ADC インスタンスのアップグレードが失敗します。[692538]
- 特定の時刻に実行するようにスケジュールされている構成監査テンプレートは、グローバルポーリング中にも実行され、構成監査テンプレートが繰り返し実行されます。[697157]
- 特定の変数値を使用した構成監査は、高可用性モードの Citrix ADC インスタンスでは機能しません。[696990]
- 設定監査テンプレートの作成中は、変数値の入力ファイルをアップロードできません。[697137]
- Citrix ADM では、構成監査レポートの処理中にエラーが発生すると、メールの受信者に空のメールが送信されます。[697138]

設定

- [設定] > [サブスクリプション] ページで、ストレージデータ消費が 5 GB という資格のあるストレージ制限よりも大きく表示されることがあります。[689330]
- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。[686581]
- Citrix ADM では、名前や説明などの入力フィールドに「&」などの特殊文字を入力すると、「&」が「&」に置き換えられます。[692656]
- Citrix ADM メンテナンスタスクが機能していません。[696952]
- グループにアプリケーションを追加したり、正規表現を指定して検索条件を適用してグループにアプリケーションを追加することもできます。このような場合、グループを複数回編集すると、アプリケーションの名前が無効な regex 式に変換されます。これにより、RBAC が失敗し、ユーザーはすべてのアプリケーションを表示できます。

  1. Citrix ADM で、［設定］>［ユーザー管理］>［グループ］の順に選択し、［追加］をクリックします。グループ名を入力し、[承認設定] タブで、必要なアプリケーションを選択してグループに追加し、[グループの作成] をクリックします。
  2. 正規表現を追加する場合は、[グループ] ページに移動し、グループを選択して [編集] をクリックします。
  3. [承認設定] タブで、[正規表現の追加**]** テキストボックスに正規表現を追加し、設定を保存します。

4. グループを再度編集する場合は、[承認の設定] タブで、以前に追加したアプリケーションの名前が正規表現に変換されることがあります。これは無効な正規表現であるため、RBAC は失敗し、ユーザーはすべてのアプリケーションを見ることができます。

[696515]

2017 年 **10** 月 **7** 日

このリリースには、新機能とバグ修正が含まれています。

Citrix ADM エージェントは、ビルド 503.115 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。

新機能

このリリースでは、次の機能強化が使用できます。

エージェントのアップグレード時間の構成

デフォルトでは、新しいバージョンが利用可能になると、エージェントは自動的にアップグレードされます。ただし、エージェントのアップグレードを実行する時刻を指定できます。特定の時刻を選択すると、エージェントはその指定された時刻にアップグレードされますが、エージェントが展開されているタイムゾーンでアップグレードされます。アップグレード中に、約 30 分のダウンタイムが発生することがあります。エージェントのアップグレード時刻を指定するには、[ネットワーク] > [エージェント] に移動し、[アップグレード設定の構成] をクリックし、エージェントをアップグレードするタイミングを指定します。詳しくは、「エージェントアップグレード設定の構成」を参照してください。

Citrix ADM から管理された **Citrix ADC** インスタンスの **GUI** へのアクセス

Citrix ADM から管理対象 Citrix ADC インスタンスの GUI にアクセスできるようになりました。Citrix ADC インスタンスを管理および監視するには、それらを Citrix ADM に追加します。その後、Citrix ADM からアクセスできます。Citrix ネットワークに接続していることを確認します。

Citrix ADM から Citrix ADC インスタンス GUI にアクセスするには、［ネットワーク］ > ［インスタンス］に移動します。［インスタンス］で、表示するインスタンスの種類（Citrix ADC VPX など）を選択し、アクセスするインスタンスの IP アドレスをクリックします。

[693970]

Citrix ADM から **Citrix SWG** インスタンスを管理する

Citrix ADM は、Citrix Secure Web Gateway（SWG）インスタンスの検出、管理、および監視をサポートするようになりました。次の図に示すように、［ネットワーク］ > ［インスタンス］で Citrix **SWG** インスタンスを表示できます。

[692493]

ライセンス有効期限後の猶予期間のサポート

ライセンスの有効期限が切れた後、Citrix ADM は 90 日間の猶予期間を提供します。猶予期間中、Citrix ADM によって収集されたデータは 30 日間保持され、構成は 90 日間保持されます。猶予期間中は、Citrix ADM にアクセスできません。

[691069]

エンティティ固有のポーリングのサポート

Citrix ADM では、インスタンスに構成されている特定のエンティティをポーリングできます。これにより、Citrix ADM がインスタンスにバインドされたエンティティの最新の状態を表示するために必要な更新時間が短縮されます。サービス、サービスグループ、負荷分散仮想サーバー、キャッシュ削減仮想サーバー、コンテンツスイッチング仮想サーバー、認証仮想サーバー、VPN 仮想サーバー、GSLB 仮想サーバー、およびアプリケーション・サーバー。詳細なドキュメントについては、Citrix ADC インスタンスとエンティティをポーリングする方法を参照してください。

[692958]

解決された問題

このリリースでは、次の問題が修正されました。

エージェント

- Microsoft Azure クラウドでプロビジョニングされたエージェントを使用している場合、このエージェントに関連付けられた管理対象インスタンスは Citrix ADM GUI でダウン状態で表示されます。[690941]
- エージェントの登録が完了すると、ハイパーバイザーコンソールからエージェントにログオンできなくなる場合があります。[691181]

ネットワーク

- Citrix ADM では、構成ジョブの作成中にファイルが自動的にアップロードされません。アップロードするファイルを選択し、**[**アップロード**]** ボタンをクリックする必要があります。[アップロード] ボタンは現在使用できません。アップロードするファイルを選択すると、ファイルが自動的にアップロードされます。[686889]
- [ネットワーク] > [構成ジョブ] > [プレビュー] で、[プレビュー] ページで構成ジョブに関連付けられたロールバックコマンドを表示できます。[687621]

設定

- Citrix ADM では、Citrix SD-WAN WO の高度なプラットフォームバックアップは、ユーザー定義のデバイスプロファイルと互換性がありません。[690508]

既知の問題

このリリースの既知の問題は次のとおりです:

エージェント

- [ネットワーク] > [エージェント] に移動し、[エージェント] 画面からエージェントをダウンロードしようとすると、「ファイルが見つかりません」などのエラーが表示されることがあります。
  回避策: エージェントをダウンロードするには、[設定] > [エージェントの設定] に移動し、ハイパーバイザーを選択して [イメージのダウンロード] をクリックします。[695998]

Analytics

- 場合によっては、Citrix ADM GUI に HDX Insight サイトノードと Gateway Insight ノードが表示されないことがあります。
  回避策: ページを更新して、もう一度試してください。[690327]
- Citrix ADM で Citrix ADC CPX インスタンスを追加した場合、分析機能にはデータが表示されません。
  回避策: Citrix ADC CPX インスタンスを Citrix ADM に追加しないでください。[694792]

ネットワーク

- Citrix ADM では、Citrix ADM を使用した Citrix ADC インスタンスのアップグレードが失敗します。［ネットワーク］**>**［構成ジョブ］**>**［メンテナンスタスク］の順に選択し、［**NetScaler** アップグレード］を選択すると、Citrix ADC インスタンスのアップグレードが失敗します。[692538]
- Citrix ADM では、フォーム入力テキストボックスに名前や説明などの入力フィールドに「&」などの特殊文字を入力すると、「&」が「&」に置き換えられます。[692656]

設定

- [設定] > [サブスクリプション] ページで、ストレージデータ消費が 5 GB という資格のあるストレージ制限よりも大きく表示されることがあります。[689330]
- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。[686581]

> 注 [XXXXXX] ラベルは、Citrix ADM チームが使用する内部トラッキング ID です。

2017 年 9 月 14 日

このリリースには、新機能とバグ修正が含まれています。

Citrix ADM エージェントは、ビルド 502.119 に自動的にアップグレードされます。[ネットワーク] > [エージェント] ページでエージェントの詳細を表示できます。

新機能

このリリースでは、次の機能強化が使用できます。

ハイブリッドおよびマルチクラウド環境向けの **Citrix ADC** グローバル負荷分散ソリューション

グローバル負荷分散 (GLB) ソリューションを使用すると、ユーザーはクライアント要求を複数のクラウド内の複数のデータセンターに分散したり、オンプレミスにデプロイされたアプリケーションサーバーに分散したりできます。このソリューションは、マルチクラウドとハイブリッドクラウドの両方の展開をサポートします。このソリューションの主な利点は次のとおりです。

- 単一の統合コンソールから、地理的な場所全体で GLB ノードを作成、管理、監視できます。
- インフラストラクチャの一部をクラウドに移動できる柔軟性を提供します。
- ディザスタリカバリ用のアクティブ/パッシブ・トポロジをサポート
- 静的近接、ラウンドロビン、送信元 IP ハッシュ、ラウンドトリップ時間など、複数のグローバル負荷分散方式をサポートします。

Citrix ADM に関連付けられた「マルチクラウド GLB StyleBook」は、複数のデータセンターにあるすべての GLB ノードを管理するための単一のユーザーインターフェイスを提供します。StyleBook を使用する利点は次のとおりです。

- 変更は 1 か所で行う必要があるため、既存の構成の変更は簡単です。
- StyleBooks を使用してすべての GLB ノードに設定をプッシュする方が速くなります。

完全なドキュメントについては、ハイブリッドおよびマルチクラウド環境向けの Citrix ADC グローバル負荷分散を参照してください。

[691937]

HAProxy インスタンスの管理と監視 **(**プレビュー**)**

Citrix ADM を使用して、展開内の HAProxy インスタンスを管理および監視できるようになりました。HAProxy ホストを Citrix ADM に追加すると、ホスト上の HAProxy インスタンスが自動的に検出され、以下の情報を指定して管理および監視できるようになります。

- **HAProxy** アプリケーションダッシュボード: HAProxy インスタンスのフロントエンドのリアルタイム統計を表示します。ダッシュボードには、検出されたアプリケーションとしてフロントエンドが表示され、リアルタイムトランザクション、スループット、およびアプリケーションに関するセッション情報が表示されます。
- **HAProxy** インスタンスを再起動する機能: Citrix ADM GUI から HAProxy インスタンスを再起動できます。また、Citrix ADM GUI から HAProxy インスタンスをハード再起動またはソフト再起動することもできます。

詳しくは、「HAProxy インスタンスの管理とモニタリング」を参照してください。

[637830]

Citrix ADM 初回ユーザーエクスペリエンス画面のスキップオプション

Citrix ADM では、エージェント登録手順をスキップして、Citrix ADM アプリのダッシュボードに直接移動できるようになりました。エージェント登録をスキップするには、[エージェントの設定] ページで [スキップ] をクリックします。

さらに、Citrix ADM 初回ユーザーエクスペリエンスページには、この Citrix Cloud サービスの概要を示すビデオが表示されるようになりました。

[693963]

[サブスクリプション**]** ページの機能強化

[サブスクリプション] ページに、サブスクリプションの概要、仮想サーバー、およびサードパーティ仮想サーバーが表示されます。[設定] > [サブスクリプション] ページで、次の変更を表示できます。

- 仮想サーバの種類ごとのライセンスの概要
- サードパーティのロードバランサーのライセンス。
- 自動ライセンス仮想サーバを選択または選択解除できます。

仮想サーバの種類をクリックして、ライセンスが適用されている仮想サーバの一覧を表示することもできます。

詳細については、サブスクリプションの管理の「ライセンスされた仮想サーバの表示」を参照してください。

[693954]

解決された問題

このリリースでは、次の問題が修正されました。

ネットワーク

- エージェントの起動プロセス中に制御プロキシが使用できない場合、エージェントは Citrix ADM から SNMP トラップ設定を取得できず、Citrix ADC インスタンスから受信されたすべてのトラップがドロップされます。[687027]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、フィルタ条件に一致するイベントの電子メールは送信されません。[688985]
- メンテナンスタスクの Citrix ADC 機能のアップグレードは、Citrix ADM ではサポートされていません。しかし、あなたはまだ GUI でオプションを見ることができます。[689068]
- Citrix ADM では、［ナビゲーション］ドロップダウンメニューをクリックして開くと、ハンバーガーアイコン（左隅のメニューアイコン）が［閉じる］アイコン（X）に変わります。この修正により、[インスタンスの追加]、[インサイトの構成] などの設定ページを開くと、ナビゲーションメニューパネルは非表示になり、[**X**] アイコンが無効になります。[687203]

- [ネットワーク] > [イベント] > [イベントメッセージ] で、イベントを選択して [詳細] タブをクリックすると、[ユーザー名]、[構成コマンド]、[承認ステータス]、[実行ステータス]、[エンティティタイプ] などのパラメータの値が [イベントの詳細] ページ。[686791]
- [ネットワーク**] > [**ネットワーク機能**] > [**負荷分散**] > [**サービスグループ] で、アプリケーションを ID でフィルタリングし、Python SDK で使用できるようになりました。[692061]
- **[** ネットワーク**] > [**ネットワーク機能**] > [**負荷分散**] > [**仮想サーバー] で、248 日以上の UP 状態にある一部の負荷分散仮想サーバーでは、[**UP]** 列には正しくない値が表示されます。[693146]

設定

- Citrix ADM でスペースを含むグループ名を作成すると、アプリの取得など、アクセス許可にグループ名を使用する特定の機能が期待どおりに機能しないことがあります。[692629]
- セカンダリノードの再起動に時間がかかり、プライマリからの強制フェールオーバーが失敗するため、Citrix ADM からの高可用性モードの Citrix ADCitrix ADC インスタンスのアップグレードは失敗します。[693119]

StyleBook

- 「*****」は、CLI コマンドの`tcp-port`パラメータの有効な入力として受け入れられます。[694155]

既知の問題

このリリースの既知の問題は次のとおりです:

エージェント

- Microsoft Azure クラウドでプロビジョニングされたエージェントを使用している場合、このエージェントに関連付けられた管理対象インスタンスは Citrix ADM GUI でダウン状態で表示されます。[690941]
- エージェントの登録が完了すると、ハイパーバイザーコンソールからエージェントにログオンできなくなる場合があります。
  回避策：SSH クライアントを使用してエージェントにログオンします。[691181]

Analytics

- 場合によっては、Citrix ADM GUI に HDX Insight サイトノードと Gateway Insight ノードが表示されないことがあります。
  回避策：ページを更新して、もう一度試してください。[690327]
- Citrix ADM で Citrix ADC CPX インスタンスを追加した場合、分析機能にはデータが表示されません。
  回避策：Citrix ADC CPX インスタンスを Citrix ADM に追加しないでください。[0694792]

設定

- [設定] > [サブスクリプション] ページで、ストレージデータ消費が 5 GB という資格のあるストレージ制限よりも大きく表示されることがあります。[689330]
- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM の［設定］>［ユーザー管理］>［ユーザー］に表示されます。[686581]

> 注 [XXXXXX] ラベルは、Citrix ADM チームが使用する内部トラッキング ID です。

2017 年 **8** 月 **25** 日

このリリースには、新機能とバグ修正が含まれています。

新機能

このリリースでは、次の機能強化が使用できます。

Citrix ADM エバーグリーンエージェントのアップグレード

Citrix ADM では、ソフトウェアバージョン 12.0 ビルド 501.117 以降で実行されているエージェントは、Citrix ADM によって新しい推奨バージョンに自動的にアップグレードされます。
Citrix ADM エージェントに対してこの機能を有効にするには、既存のエージェントを手動で Citrix ADM エージェントバージョン 12.0 ビルド 501.117 にアップグレードする必要があります。

解決された問題

このリリースでは、次の問題が修正されました。

ネットワーク

- Citrix ADM で、検出された Citrix ADC インスタンスのデフォルト証明書を削除しようとすると、エラーメッセージが表示されます。これで、デフォルトの証明書を選択すると、「削除」ボタンが無効になります。
  [687610]
- Citrix ADM では、Citrix ADC インスタンスを削除しても、対応する Citrix ADC インスタンスに関連付けられた障害オブジェクトは削除されません。
  [690059]
- 選択した期間が「1 ヶ月」の場合、イベントレポート ([ネットワーク] > [イベント] > [レポート]) は表示されません。
  [692054]
- Citrix ADM では、エンティティのポーリングの実行中に、検出される Citrix ADC インスタンスの数が非常に多い場合、Citrix ADM UI が応答しなくなることがあります。

回避策：Web ブラウザを閉じ、10〜15 分後に Citrix ADM に再ログオンします。
[692617]

オンボーディング

- Citrix ADM で新しいテナントをオンボードし、[管理] ボタンをクリックすると、初めて「ページが機能していません」というエラーが表示されることがあります。
  [691018]

既知の問題

このリリースの既知の問題は次のとおりです：

エージェント

- Microsoft Azure クラウドでプロビジョニングされたエージェントを使用している場合、このエージェントに関連付けられた管理対象インスタンスは Citrix ADM GUI でダウン状態で表示されます。[690941]
- エージェントの登録が完了すると、ハイパーバイザーコンソールからエージェントにログオンできなくなる場合があります。
  回避策：SSH クライアントを使用してエージェントにログオンします。[691181]

Analytics

- 場合によっては、Citrix ADM GUI に HDX Insight サイトノードと Gateway Insight ノードが表示されないことがあります。
  回避策：ページを更新して、もう一度試してください。[690327]

ネットワーク

- エージェントの起動プロセス中に制御プロキシが使用できない場合、エージェントは Citrix ADM から SNMP トラップ設定を取得できず、Citrix ADC インスタンスから受信されたすべてのトラップがドロップされます。
  回避策：Citrix ADM への接続が確立されたときに、`masd restart` エージェントで実行します。[687027]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、フィルタ条件に一致するイベントの電子メールは送信されません。[688985]
- メンテナンスタスクの Citrix ADC 機能のアップグレードは、Citrix ADM ではサポートされていません。しかし、あなたはまだ GUI でオプションを見ることができます。[689068]

設定

- [設定] > [サブスクリプション] ページで、ストレージデータ消費が 5 GB という資格のあるストレージ制限よりも大きく表示されることがあります。[689330]

- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。[686581]

> 注 [XXXXXX] ラベルは、Citrix ADM チームが使用する内部トラッキング ID です。

2017 年 8 月 13 日

これはバグ修正リリースです。このリリースには新機能はありません。

解決された問題

このリリースでは、次の問題が修正されました。

Analytics

- Citrix ADM で HDX インサイトを使用している間、プライベート IP ブロックを介して作成された IP ブロックではジオマップが機能しないことがあります。[691947]
- 2 つの IP ブロックサイトを作成している間、最初の IP サイトの地ジオロケーションが正しく表示されません。最初の IP サイトを削除して再作成すると、ジオマップには最初の IP サイトに関する情報が表示されません。[691965]

ネットワーク

Citrix ADM で簡単にデバッグできるように、サブシステムのログファイルには、スローされたデータベース例外のテナント名が表示されます。[692663]

既知の問題

このリリースの既知の問題は次のとおりです：

エージェント

- Microsoft Azure クラウドでプロビジョニングされたエージェントを使用している場合、このエージェントに関連付けられた管理対象インスタンスは Citrix ADM GUI でダウン状態で表示されます。[690941]
- エージェントの登録が完了すると、ハイパーバイザーコンソールからエージェントにログオンできなくなる場合があります。
  回避策：SSH クライアントを使用してエージェントにログオンします。[691181]

Analytics

- 場合によっては、Citrix ADM GUI に HDX Insight サイトノードと Gateway Insight ノードが表示されないことがあります。
  回避策：ページを更新して、もう一度試してください。[690327]

ネットワーク

- エージェントの起動プロセス中に制御プロキシが使用できない場合、エージェントは Citrix ADM から SNMP トラップ設定を取得できず、Citrix ADC インスタンスから受信されたすべてのトラップがドロップされます。
  回避策：Citrix ADM への接続が確立されたときに、`masd restart` エージェントで実行します。[687027]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、フィルタ条件に一致するイベントの電子メールは送信されません。[688985]
- メンテナンスタスクの Citrix ADC 機能のアップグレードは、Citrix ADM ではサポートされていません。しかし、あなたはまだ GUI でオプションを見ることができます。[689068]

オンボーディング

- Citrix ADM で新しいテナントをオンボードし、[管理] ボタンをクリックすると、初めて「ページが機能していません」というエラーが表示されることがあります。
  回避策：
  1 時間（60 分）待ってから、再度ログインします。この遅延は、新しいテナントのプロビジョニングに要した時間が原因です。[691018]

設定

- [設定] > [サブスクリプション] ページで、ストレージデータ消費が 5 GB という資格のあるストレージ制限よりも大きく表示されることがあります。[689330]
- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。[686581]

> 注 [XXXXXX] ラベルは、Citrix ADM チームが使用する内部トラッキング ID です。

2017 年 8 月 10 日

このリリースには、新機能とバグ修正が含まれています。

新機能

このリリースでは、次の機能強化が使用できます。

Citrix ADM で **Syslog** メッセージを抑制する

Citrix ADM は、管理対象 Citrix ADC インスタンスによって送信されたすべての構成済み Syslog を受信します。syslog メッセージの数が多いため、syslog はデータベース内の大きな領域を占有します。これらのメッセージの多くは、ユーザにとって重要ではないため、重要な syslog メッセージだけを取得したい場合があります。

フィルタを設定することで、Citrix ADM で受信した syslog の一部を抑制できるようになりました。syslog を抑制するために使用できる 2 つのフィルタは、重大度とファシリティです。1 つ以上の Citrix ADC インスタンスからのメッセージを抑制できます。

テキストパターンを使用して、メッセージを検索および抑制することもできます。Citrix ADM は、指定された条件に一致するすべてのメッセージをドロップします。ドロップされた syslog は Citrix ADM に表示されず、顧客データベースにも保存されません。したがって、ストレージサーバー上に大量の領域が保存されます。

詳しくは、次のトピックを参照してください：Citrix ADM で Syslog メッセージを抑制する方法

[6779274]

Citrix ADC インスタンスで構成された負荷分散エンティティのレポートを生成および表示する

管理対象の Citrix ADC インスタンスに構成されている仮想サーバーやサービスなど、負荷分散エンティティのレポートを生成できます。すべてのエンティティの統合レポートを表示できます。これらのレポートでは、次の概要を表示できます。

- Citrix ADC インスタンス
- 仮想サーバの負荷分散
- 管理パーティション
- サービス
- サービスグループ

統合レポートを使用すると、これらのエンティティ間のマッピングを作成できます。詳しくは、次のトピックを参照してください：負荷分散エンティティのレポートを生成する方法

[663174]

後で実行するために設定ジョブを保存するときに変数値を保存する

構成ジョブを作成するときは、変数の値を指定できますが、後でジョブを保存して実行するか、後で実行するようにジョブをスケジュールします。このようなシナリオでは、Citrix ADM は保存されたジョブに変数値を保持するようになりました。

[637830]

Citrix ADC インスタンス用のカスタマイズされた **SSH** ポートのサポート

Citrix ADM と Citrix ADC インスタンス間の通信にユーザー定義の SSH ポートを指定できるようになりました。

インスタンスプロファイルの SSH ポートを設定するには

1. サポートされている Web ブラウザを使用して Citrix ADM にログオンします。
2. ［ネットワーク］に移動し、Citrix ADM で検出する Citrix ADC インスタンスのインスタンスタイプを選択します。
3. [プロファイル] をクリックします。
4. [管理者プロファイル] ページで、[追加] をクリックします。
5. ［**SSH** ポート］に、Citrix ADC インスタンスが Citrix ADM と通信するための構成済みのカスタム SSH ポート番号を入力します。
6. ［**OK**］をクリックします。

[689369]

解決された問題

このリリースでは、次の問題が修正されました。

エージェント

デフォルトでは、エージェントをサービスに登録するために必要なアクティベーションコードを生成する権限は、スーパー管理者ユーザー（組織で最初にサインアップして Citrix ADM にログオンしたユーザー）だけです。委任された管理者 (ログオンする後続のすべてのユーザー) には、アクティベーションコードを生成するアクセス許可がありません。委任された管理者が [アクティベーションコードの生成] をクリックすると、次のエラーが表示されます。「この操作を実行する権限がありません。」
[690576]

アプリケーションの分析と管理

Citrix ADM のアプリケーションダッシュボードには、カスタム定義アプリケーションの誤ったセキュリティメトリックが表示されます。

[689041]

ネットワーク

- Citrix ADM で特定のイベントを監視するようにルールを構成すると、SNMP トラップは外部トラップ送信先に送信されません。
  [689018]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、指定したフィルタ条件に一致するイベントに対してジョブは実行されません。[688986]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、構成された期間はイベントは抑制されません。[688988]

- ［設定］>［ユーザー管理］>［グループ］の順に選択し、Citrix ADM でグループを作成すると、ウィザードのすべての手順が完了する前に、グループが作成されたことを示す成功メッセージが表示されます。[684944]

既知の問題

このリリースの既知の問題は次のとおりです:

エージェント

- Microsoft Azure クラウドでプロビジョニングされたエージェントを使用している場合、このエージェントに関連付けられた管理対象インスタンスは Citrix ADM GUI でダウン状態で表示されます。[690941]
- エージェントの登録が完了すると、ハイパーバイザーコンソールからエージェントにログオンできなくなる場合があります。
  回避策：SSH クライアントを使用してエージェントにログオンします。[691181]

Analytics

- 場合によっては、Citrix ADM GUI に HDX Insight サイトノードと Gateway Insight ノードが表示されないことがあります。
  回避策：ページを更新して、もう一度試してください。[690327]

ネットワーク

- エージェントの起動プロセス中に制御プロキシが使用できない場合、エージェントは Citrix ADM から SNMP トラップ設定を取得できず、Citrix ADC インスタンスから受信されたすべてのトラップがドロップされます。
  回避策：Citrix ADM への接続が確立されたときに、`masd restart` エージェントで実行します。[687027]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、フィルタ条件に一致するイベントの電子メールは送信されません。[688985]
- メンテナンスタスクの Citrix ADC 機能のアップグレードは、Citrix ADM ではサポートされていません。しかし、あなたはまだ GUI でオプションを見ることができます。[689068]

オンボーディング

- Citrix ADM で新しいテナントをオンボードし、[管理] ボタンをクリックすると、初めて「ページが機能していません」というエラーが表示されることがあります。
  回避策：
  1 時間（60 分）待ってから、再度ログインします。この遅延は、新しいテナントのプロビジョニングに要した時間が原因です。[691018]

設定

- [設定] > [サブスクリプション] ページで、ストレージデータ消費が 5 GB という資格のあるストレージ制限よりも大きく表示されることがあります。[689330]
- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。[686581]

> 注 [XXXXXX] ラベルは、Citrix ADM チームが使用する内部トラッキング ID です。

2017 年 **7** 月 **23** 日

これはバグ修正リリースです。このリリースには新機能はありません。

解決された問題

このリリースでは、次の問題が修正されました。

Citrix Cloud

citrix.cloud.com にログオンした後、Citrix ADM タイルの［管理］ボタンをクリックすると、次のエラーが表示されます。”page not available.”
[690267]

ネットワーク

Citrix ADC インスタンスでセキュアオンリーのアクセスを有効にした場合、これらのインスタンスは Citrix ADM で正しく検出されず、検出プロセスの完了後にステータスが「サービス外」と表示されることがあります。
[690431]

既知の問題

このリリースの既知の問題は次のとおりです:

エージェント

- Microsoft Azure クラウドでプロビジョニングされたエージェントを使用している場合、このエージェントに関連付けられた管理対象インスタンスは Citrix ADM GUI でダウン状態で表示されます。[690941]
- エージェントの登録が完了すると、ハイパーバイザーコンソールからエージェントにログオンできなくなる場合があります。
  回避策：SSH クライアントを使用してエージェントにログオンします。[691181]

- デフォルトでは、エージェントをサービスに登録するために必要なアクティベーションコードを生成する権限は、スーパー管理者ユーザー（組織で最初にサインアップして Citrix ADM にログオンしたユーザー）だけです。委任された管理者 (ログオンする後続のすべてのユーザー) には、アクティベーションコードを生成するアクセス許可がありません。委任された管理者が [アクティベーションコードの生成] をクリックすると、次のエラーが表示されます:「この操作を実行する権限がありません。」
  回避策: スーパー管理者は、委任された管理者に必要なアクセス許可を割り当てる必要があります。詳しくは、「委任された管理者ユーザーに追加のアクセス許可を割り当てる方法」を参照してください。[690576]

Analytics

- 場合によっては、Citrix ADM GUI に HDX Insight サイトノードと Gateway Insight ノードが表示されないことがあります。
  回避策：ページを更新して、もう一度試してください。[690327]

アプリケーションの分析と管理

- Microsoft Windows オペレーティングシステムで Safari ブラウザーを使用している場合、アプリダッシュボードとセキュリティ分析ダッシュボードは読み込まれません。Citrix ADM その他の機能を見ることができます。[688617]
- Citrix ADM のアプリケーションダッシュボードには、カスタム定義アプリケーションの誤ったセキュリティメトリックが表示されます。[689041]

ネットワーク

- エージェントの起動プロセス中に制御プロキシが使用できない場合、エージェントは Citrix ADM から SNMP トラップ設定を取得できず、Citrix ADC インスタンスから受信されたすべてのトラップがドロップされます。
  回避策：Citrix ADM への接続が確立されたときに、`masd restart` エージェントで実行します。[687027]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、フィルタ条件に一致するイベントの電子メールは送信されません。[688985]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、指定したフィルタ条件に一致するイベントに対してジョブは実行されません。[688986]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、構成された期間はイベントは抑制されません。[688988]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、SNMP トラップは外部トラップ送信先に送信されません。[689018]
- メンテナンスタスクの Citrix ADC 機能のアップグレードは、Citrix ADM ではサポートされていません。しかし、あなたはまだ GUI でオプションを見ることができます。[689068]

設定

- [設定] > [サブスクリプション] ページで、ストレージデータ消費が 5 GB という資格のあるストレージ制限よりも大きく表示されることがあります。[689330]
- Citrix ADM から突然ログアウトすることがあります。
  回避策：Citrix ADM に再度ログオンします。[689012]
- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。[686581]

> 注 [XXXXXX] ラベルは、Citrix ADM チームが使用する内部トラッキング ID です。

2017 年 7 月 16 日

これはバグ修正リリースです。このリリースには新機能はありません。

解決された問題

このリリースでは、次の問題が解決されています。

Analytics

- AWS（AWS）で Citrix ADM エージェントを使用している場合、ULFD 機能を含む Telemetry パッケージがエージェント AMI にないため、分析データは表示されません。[690225]
- Citrix ADM では、PDF/JPEG/PNG へのレポートのエクスポートが機能しません。[683778]
- Citrix ADM からインサイトを有効にすると、AppFlow の横のチェックマークは有効になりません。ただし、AppFlow を有効にする構成は、Citrix ADC インスタンスにプッシュされます。[688309]

ネットワーク

- 構成ジョブの作成中にコマンドファイルをアップロードすることはできません。ただし、[ネットワーク] > [設定ジョブ] > [ジョブの作成] を選択すると、ファイルをアップロードするオプションが表示されます。
  [688967]
- カスタマー名にタイトルの大文字と小文字を使用すると、エージェント登録が失敗します。たとえば、`Haroldmas`、`kimiRKN`。
  [689648]

既知の問題

このリリースの既知の問題は次のとおりです：

アプリケーションの分析と管理

- Microsoft Windows オペレーティングシステムで Safari ブラウザーを使用している場合、アプリダッシュボードとセキュリティ分析ダッシュボードは読み込まれません。Citrix ADM その他の機能を見ることができます。[688617]
- Citrix ADM のアプリケーションダッシュボードには、カスタム定義アプリケーションの誤ったセキュリティメトリックが表示されます。[689041]

ネットワーク

- エージェントの起動プロセス中に制御プロキシが使用できない場合、エージェントは Citrix ADM から SNMP トラップ設定を取得できず、Citrix ADC インスタンスから受信されたすべてのトラップがドロップされます。
  回避策：Citrix ADM への接続が確立されたときに、`masd restart` エージェントで実行します。[687027]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、フィルタ条件に一致するイベントの電子メールは送信されません。[688985]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、指定したフィルタ条件に一致するイベントに対してジョブは実行されません。[688986]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、構成された期間はイベントは抑制されません。[688988]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、SNMP トラップは外部トラップ送信先に送信されません。[689018]
- メンテナンスタスクの Citrix ADC 機能のアップグレードは、Citrix ADM ではサポートされていません。しかし、あなたはまだ GUI でオプションを見ることができます。[689068]

設定

- [設定] > [サブスクリプション] ページで、ストレージデータ消費が 5 GB という資格のあるストレージ制限よりも大きく表示されることがあります。[689330]
- Citrix ADM から突然ログアウトすることがあります。
  回避策：Citrix ADM に再度ログオンします。[689012]
- Citrix Cloud からユーザーを削除すると、削除されたユーザー名は引き続き Citrix ADM 設定］>［ユーザー管理］>［ユーザー］に表示されます。[686581]

> 注 [XXXXXX] ラベルは、Citrix ADM チームが使用する内部トラッキング ID です。

2017 年 6 月 30 日

これは、Citrix ADM の最初のリリースです。使用可能な機能の一覧については、機能とソリューションを参照してください。

このリリースの既知の問題は次のとおりです：

Analytics

- Citrix ADM では、PDF/JPEG/PNG へのレポートのエクスポートが機能しません。[683778]
- Citrix ADM からインサイトを有効にすると、AppFlow の横のチェックマークは有効になりません。ただし、AppFlow を有効にする構成は、Citrix ADC インスタンスにプッシュされます。[688309]

アプリケーションの分析と管理

- Microsoft Windows オペレーティングシステムで Safari ブラウザーを使用している場合、アプリダッシュボードとセキュリティ分析ダッシュボードは読み込まれません。Citrix ADM の他の機能を確認できます。[688617]
- Citrix ADM のアプリケーションダッシュボードには、カスタム定義アプリケーションの誤ったセキュリティメトリックが表示されます。[689041]

ネットワーク

- エージェントの起動プロセス中に制御プロキシが使用できない場合、エージェントは Citrix ADM から SNMP トラップ設定を取得できず、Citrix ADC インスタンスから受信されたすべてのトラップがドロップされます。
  回避策：Citrix ADM への接続が確立されたときに、`masd restart` エージェントで実行します。[687027]
- 構成ジョブの作成中にコマンドファイルをアップロードすることはできません。ただし、[ネットワーク] > [設定ジョブ] > [ジョブの作成] を選択すると、ファイルをアップロードするオプションが表示されます。[688967]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、フィルタ条件に一致するイベントの電子メールは送信されません。[688985]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、指定したフィルタ条件に一致するイベントに対してジョブは実行されません。[688986]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、構成された期間はイベントは抑制されません。[688988]
- Citrix ADM で特定のイベントを監視するようにルールを構成すると、SNMP トラップは外部トラップ送信先に送信されません。[689018]
- メンテナンスタスクの Citrix ADC 機能のアップグレードは、Citrix ADM ではサポートされていません。しかし、あなたはまだ GUI でオプションを見ることができます。[689068]

設定

- [設定] > [サブスクリプション] ページで、ストレージデータ消費が 5 GB という資格のあるストレージ制限よりも大きく表示されることがあります。[689330]
- Citrix ADM から突然ログアウトすることがあります。
  回避策：Citrix ADM に再度ログオンします。[689012]
- Citrix Cloud からユーザーを削除すると、削除したユーザー名は、Citrix ADM の［設定］>［ユーザー管理］>［ユーザー］に表示されます。[686581]

> 注 [XXXXXX] ラベルは、Citrix ADM チームが使用する内部トラッキング ID です。

はじめに

May 7, 2021

このドキュメントでは、Citrix ADM（Citrix Application Delivery Management ADM）のオンボーディングとセットアップを初めて開始する方法について説明します。このドキュメントは、Citrix ネットワークデバイス（Citrix ADC、SD-WAN WO、Citrix Gateway、Citrix Secure Web Gateway など）を管理するネットワーク管理者およびアプリケーション管理者を対象としています。Citrix ADM を使用して管理するデバイスの種類に関係なく、このドキュメントの手順に従います。

オンボーディングを開始する前に、ブラウザの要件、エージェントのインストール要件、および ポートの要件を確認します。

手順 **1**：**Citrix Cloud** にサインアップします

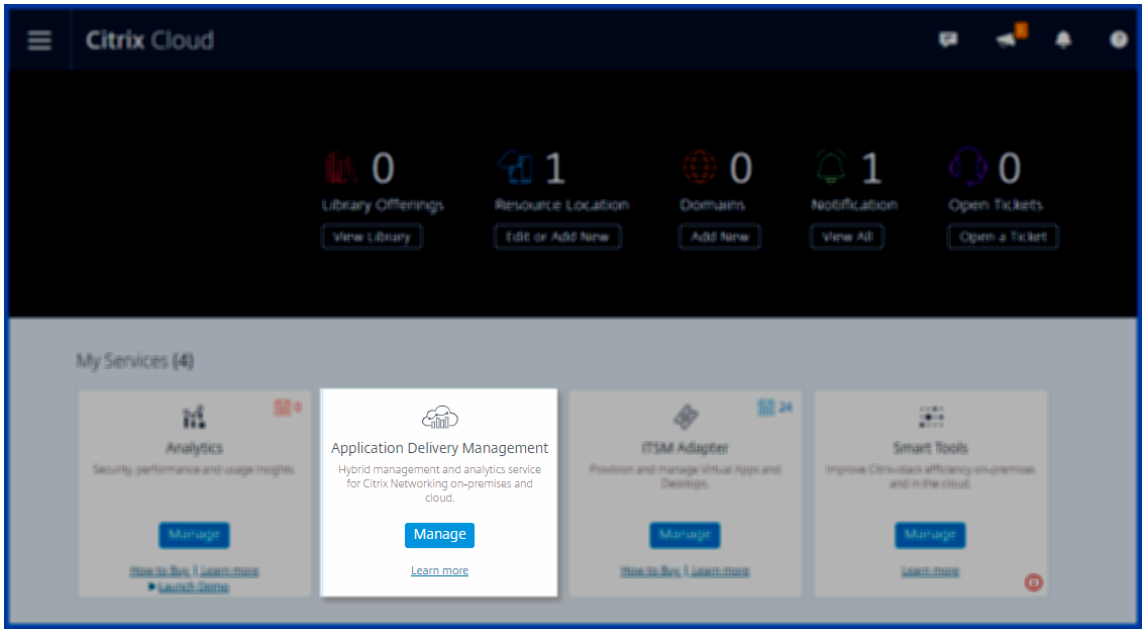
Citrix ADM の使用を開始するには、まず Citrix Cloud の会社アカウントを作成するか、社内の他のユーザーが作成した既存のアカウントに参加する必要があります。詳細なプロセスと手順については、「Citrix Cloud へのサインアップ」を参照してください。

手順 **2: Express** アカウントを使用して **Citrix ADM** を管理する

Citrix Cloud にログオンしたら、次の操作を行います。

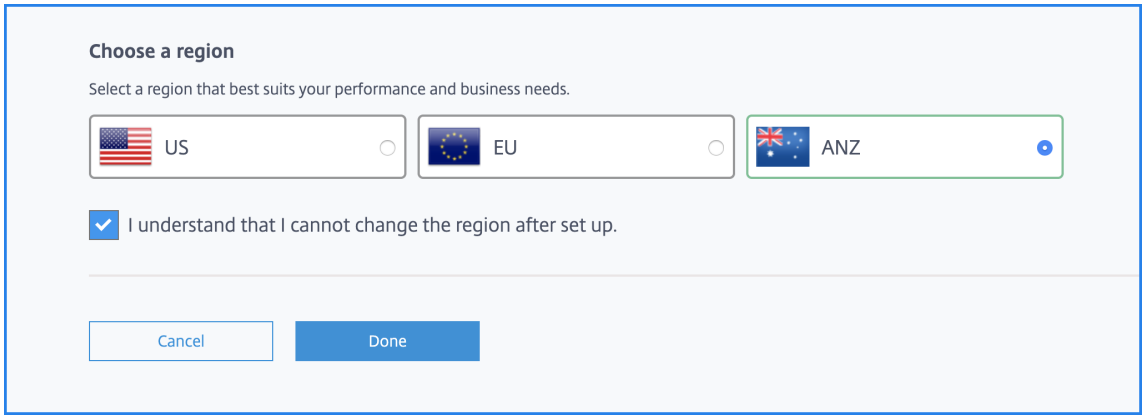
1. [利用可能なサービス] セクションに移動します。
2. [アプリケーション配信の管理] タイルで、[管理] をクリックします。

   [**Application Delivery Management**] タイルが [マイサービス] セクションに移動します。



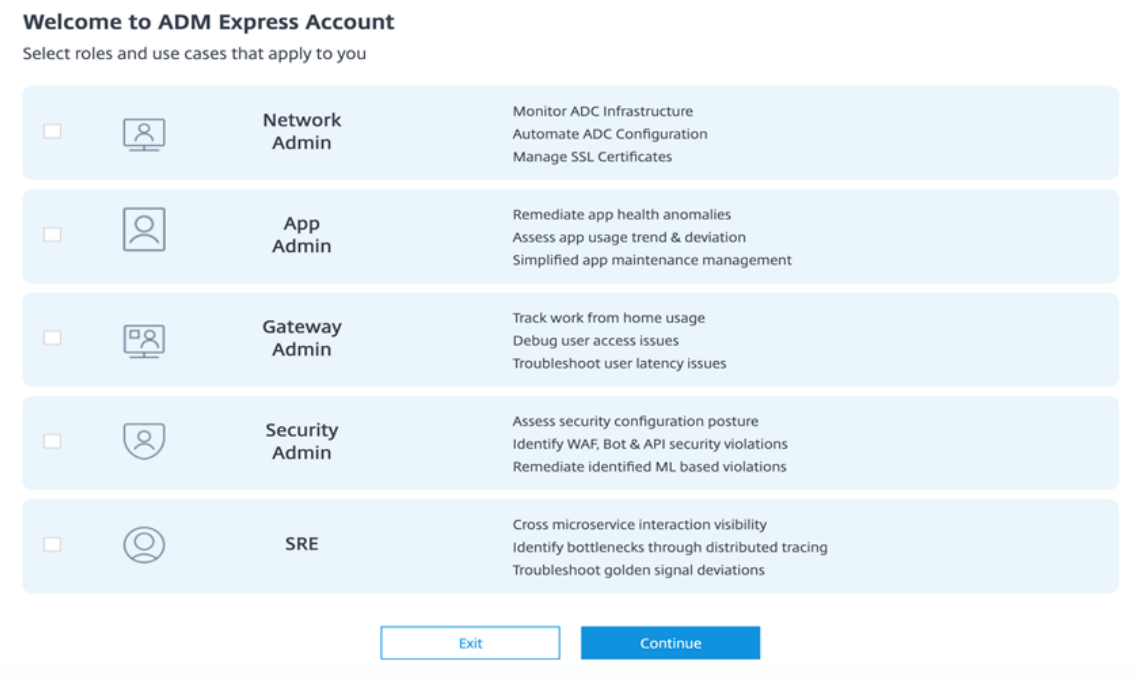
3. ビジネスニーズに合った地域を、次のいずれかに選択します。

   - 米国（米国）
   - ヨーロッパ (EU)
   - オーストラリア（ANZ）

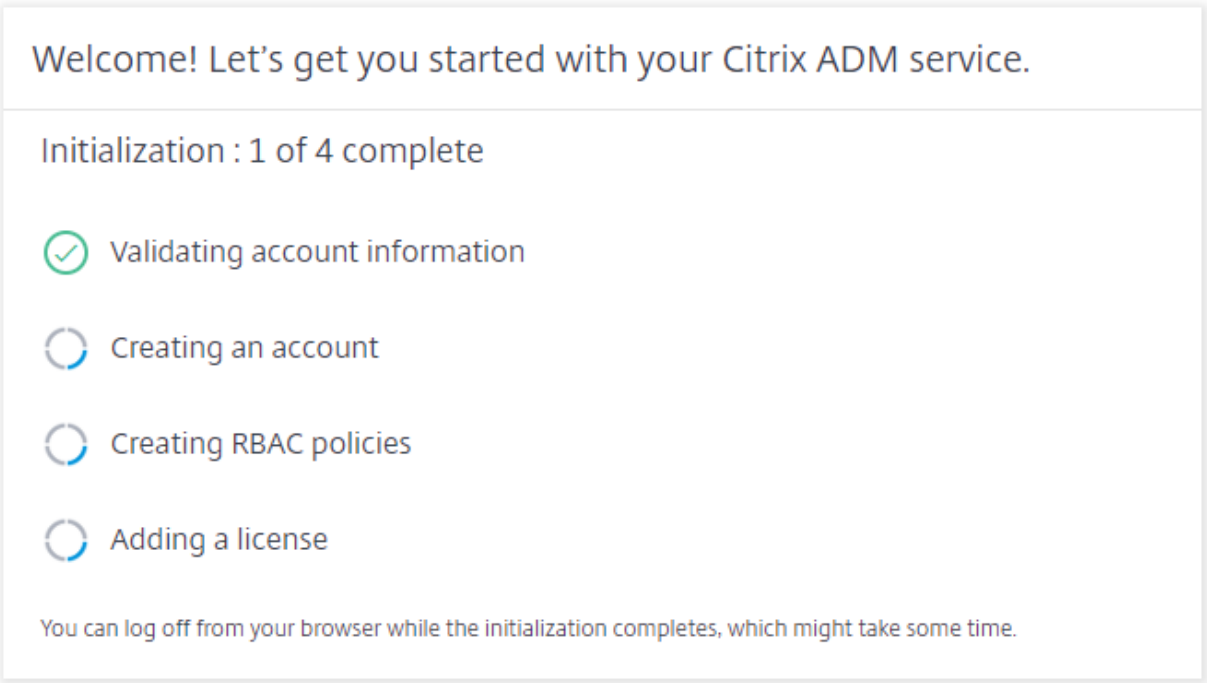


> 重要:
>
> 後でリージョンを変更することはできません。

4. 自分に適用されるロールとユースケースを選択します。

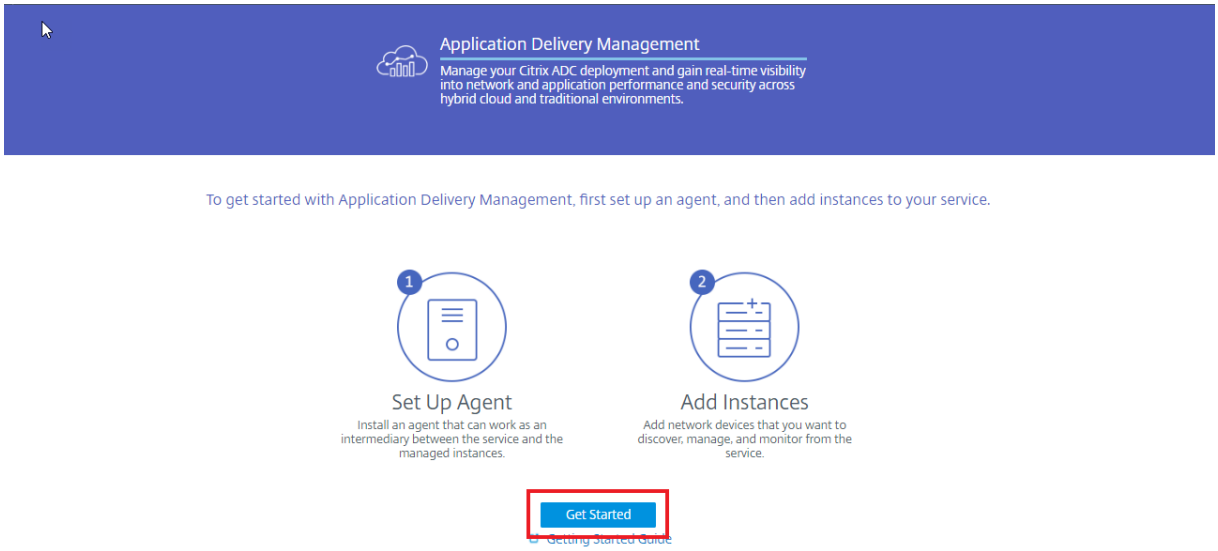


初期化がバックグラウンドで完了している間、ブラウザからログオフできます。これには時間がかかる場合があります。



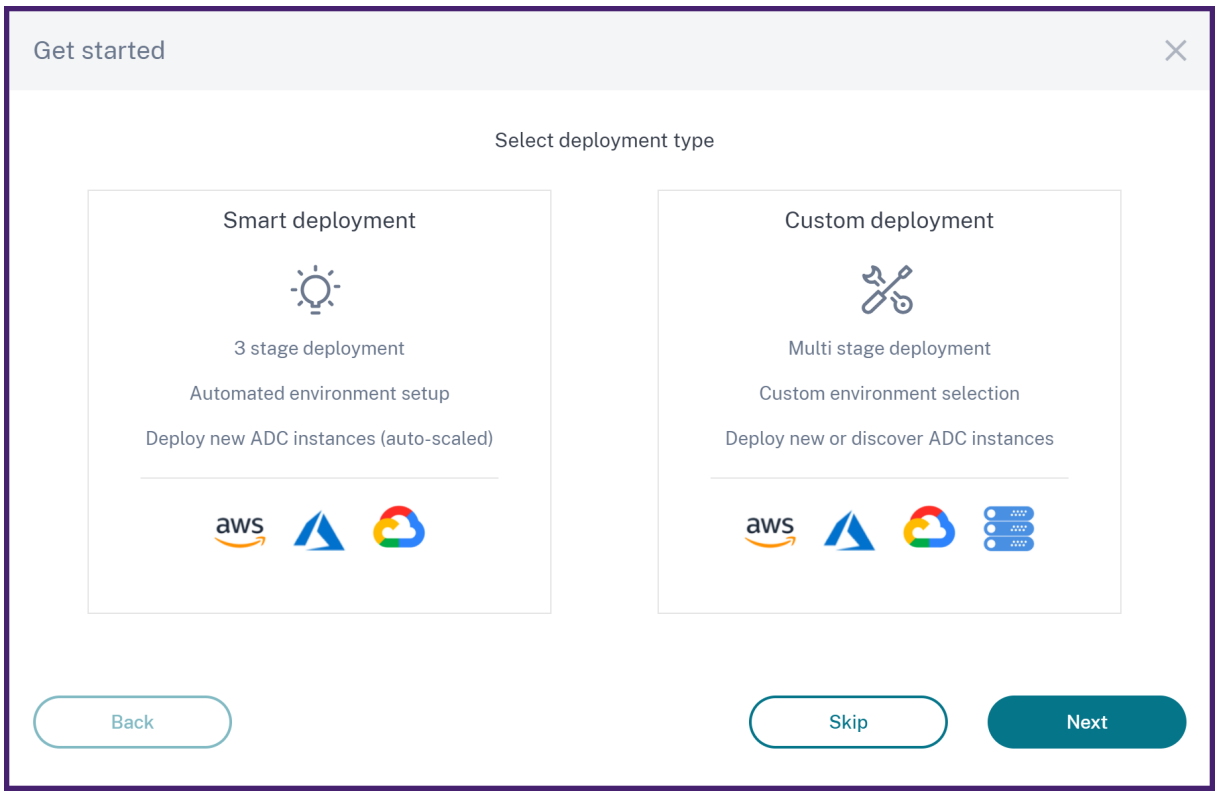
> 注
>
> Citrix は、ADM リソースを管理するために Express アカウントを割り当てます。Citrix ADM Express アカウントが 90 日間非アクティブのままの場合、アカウントは削除されます。詳しくは、「エクスプレスアカウントを使用して Citrix ADM サービスを管理する」を参照してください。

Citrix Cloud アカウントに再びログオンすると、**Citrix ADM GUI** 画面が表示されます。[開始] をクリックして、サービスの初回セットアップを開始します。



ステップ **3: ADC** 展開の種類を選択する

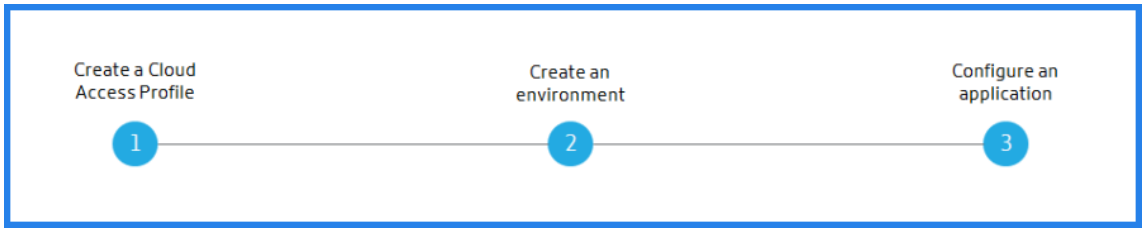
ビジネス要件に応じて、次の展開オプションのいずれかを選択します。



- スマートな導入 -このオプションは、新しい ADC インスタンスをデプロイするための自動化された環境設定です。エージェントが自動的にインストールされ、Citrix ADM と管理対象のインスタンス間の通信が有効にな

ります。

このオプションは、現在 AWS 環境のみをサポートしています。3 つのステップで、ADC インスタンスを使用して AWS に存在するアプリケーションを配信できます。



- カスタムデプロイ -このオプションは多段階展開です。各環境オプションを選択し、ADC インスタンスをデプロイまたは検出できます。

スマートな展開を選択

このデプロイオプションでは、AWS に次のインフラストラクチャが作成されます。

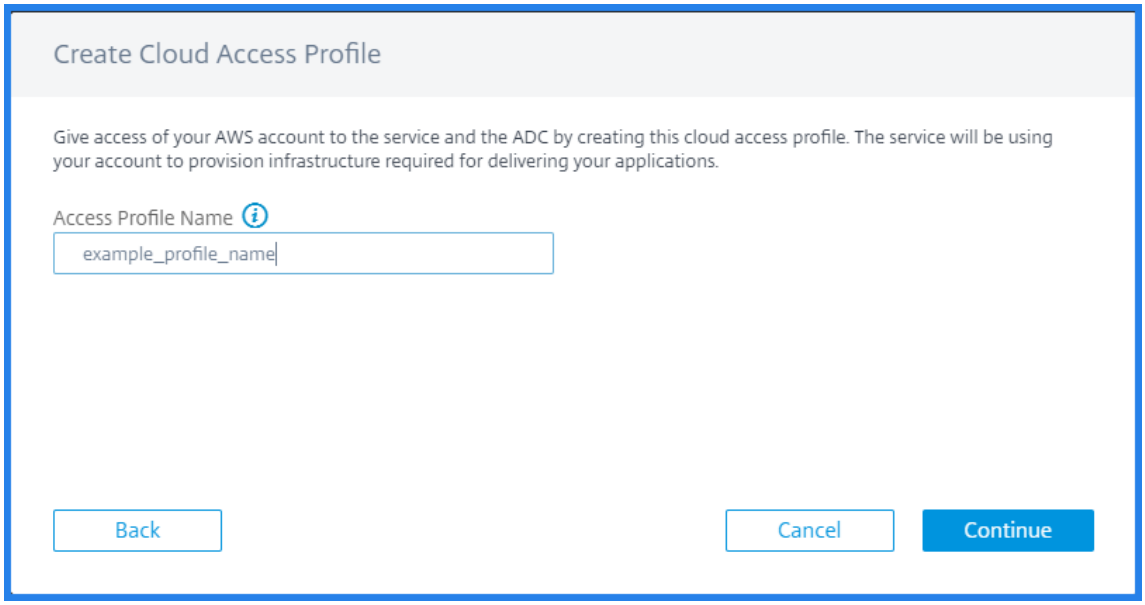
- サブネット、セキュリティグループ、NAT ゲートウェイなどを含む必要なインフラストラクチャを作成する AWS の CloudFormation スタック。
- ADC インスタンスを管理する VPC 内の ADM エージェント。
- ADC オートスケール・グループこのグループは、後で [ネットワーク**] > [AutoScale** グループ] ページでカスタマイズできます。

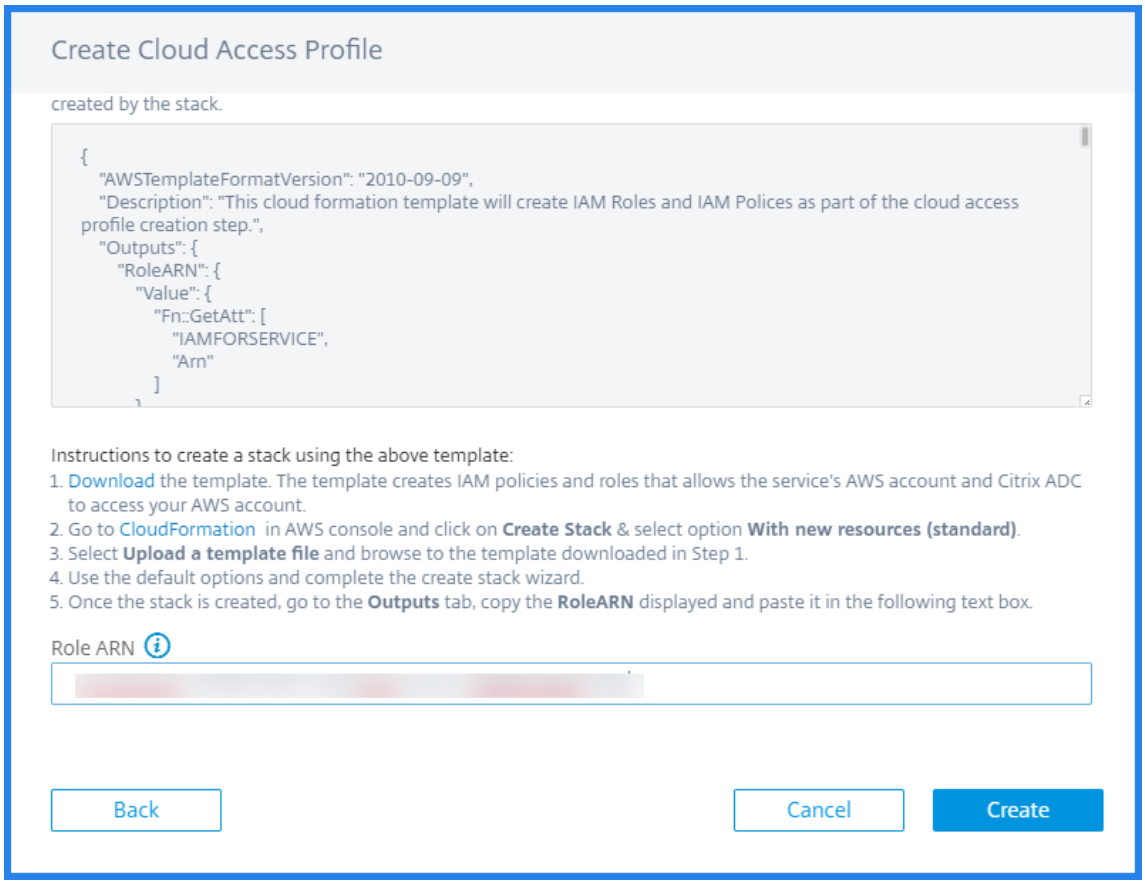
ADC インスタンスをデプロイする前に、次の点を確認してください。

1. すでに AWS アカウントを所有しています。
2. すべての管理者権限を持つ IAM ユーザーを作成しました。

ADC インスタンスをデプロイするには、次の手順を実行します。

1. クラウドアクセスプロファイルを作成するには、アクセスプロファイル名とロール **ARN** を指定します。



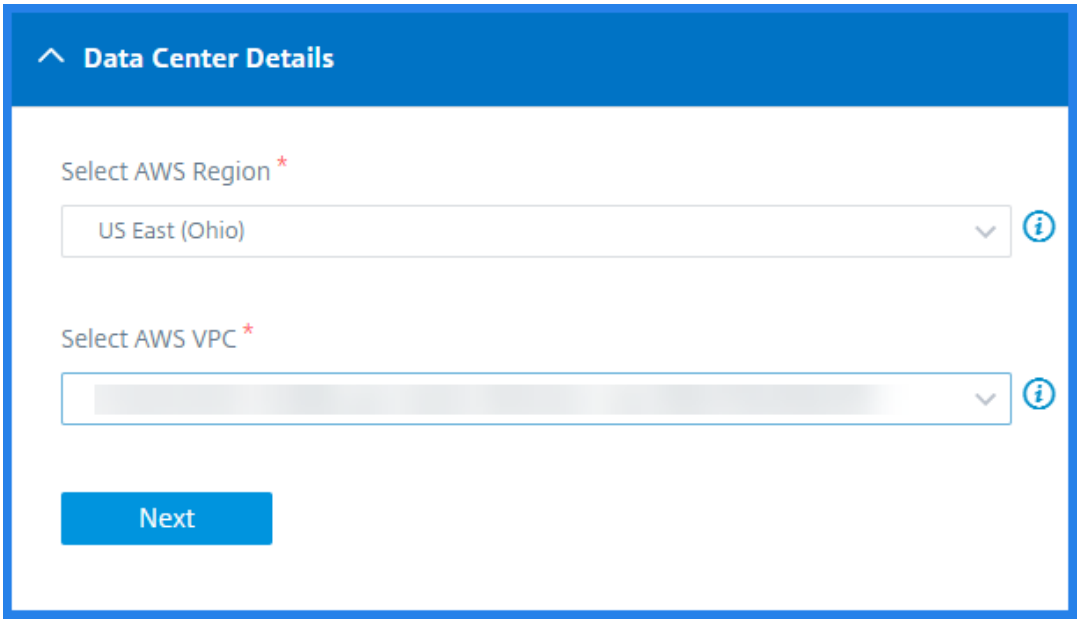


ADM サービスは、クラウドアクセスプロファイルを使用して AWS アカウントにアクセスします。

2. AWS 環境を準備するには、次の詳細を指定します。

   a) [データセンターの詳細] で、ADC インスタンスをデプロイする **AWS** リージョンと **AWS VPC** を選択します。

AWS VPC には、選択した **AWS** リージョンに存在する VPC が一覧表示されます。



b) [**ADC AutoScale** グループの詳細] で、AWS クラウドの ADC インスタンスを AutoScale するには、次のように指定します。

- **AutoScale** グループ名 -AutoScale グループを識別するための名前。
- **Availability** Zones-AutoScale グループを作成するゾーンを選択します。

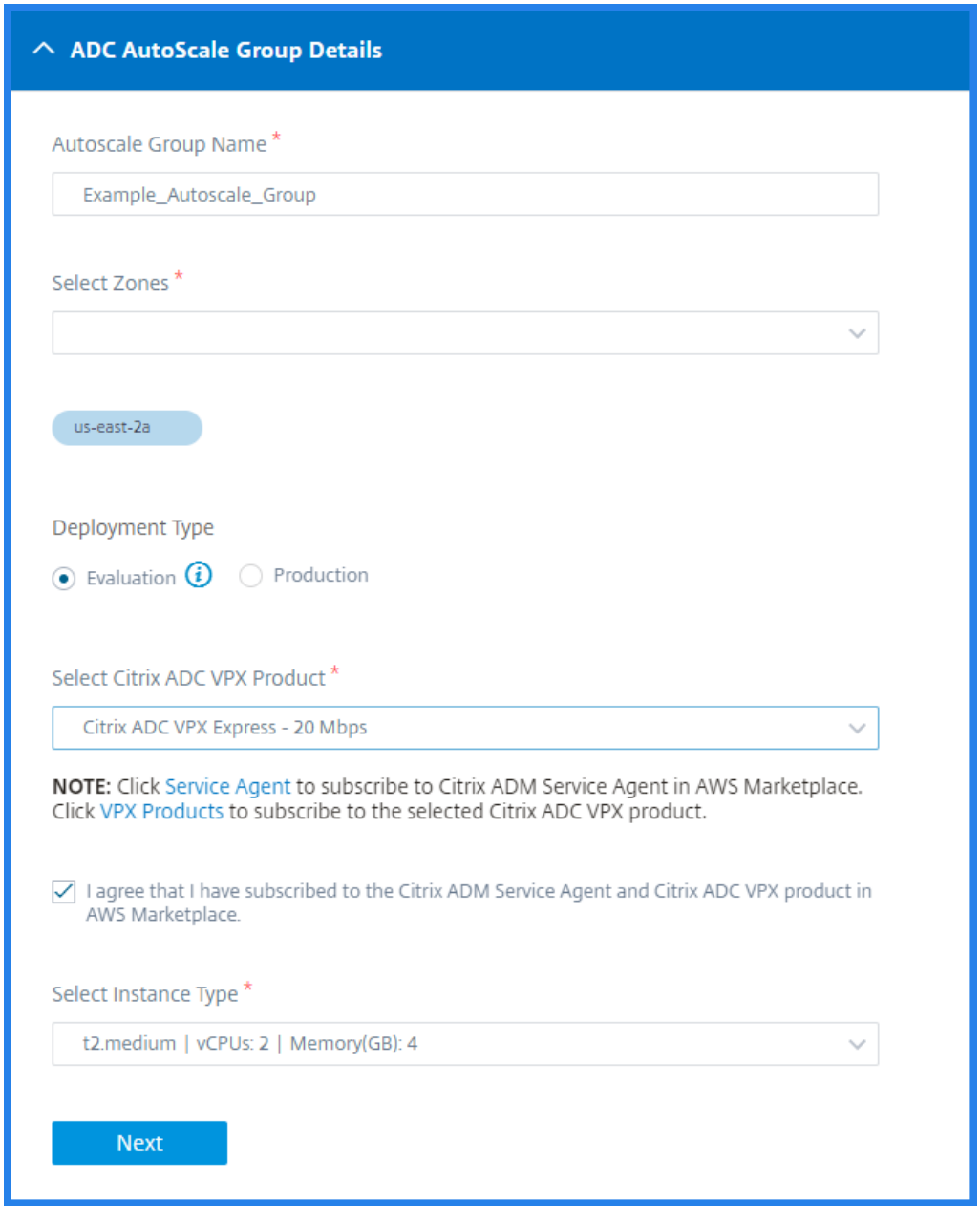
  リストから複数のゾーンを選択できます。
- 展開の種類**:** [評価] または [実稼働] オプションを選択します。

  実稼働ライセンスを購入する前に ADM Autocale ソリューションを評価する場合は、[評価] オプションを選択します。

  > 重要
  >
  > – 評価オプションは、アベイラビリティーゾーンを 1 つだけサポートします。
  > - 評価オプションでは、Citrix ADC VPX Express のみを選択できます。また、ADM Autoscale ソリューションは、最大 3 つの ADC インスタンスまで拡張できます。
- **Citrix ADC VPX** 製品 -ADC インスタンスをプロビジョニングするライセンスを選択します。

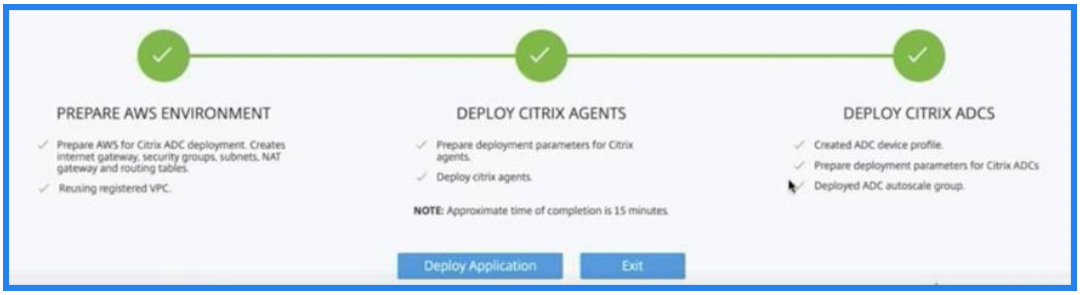
  AWS Marketplace で選択したライセンスを購読し、このページに戻ります。

  ユーザーの同意メッセージを確認して選択します。
- インスタンスタイプ -必要なインスタンスタイプを選択します。



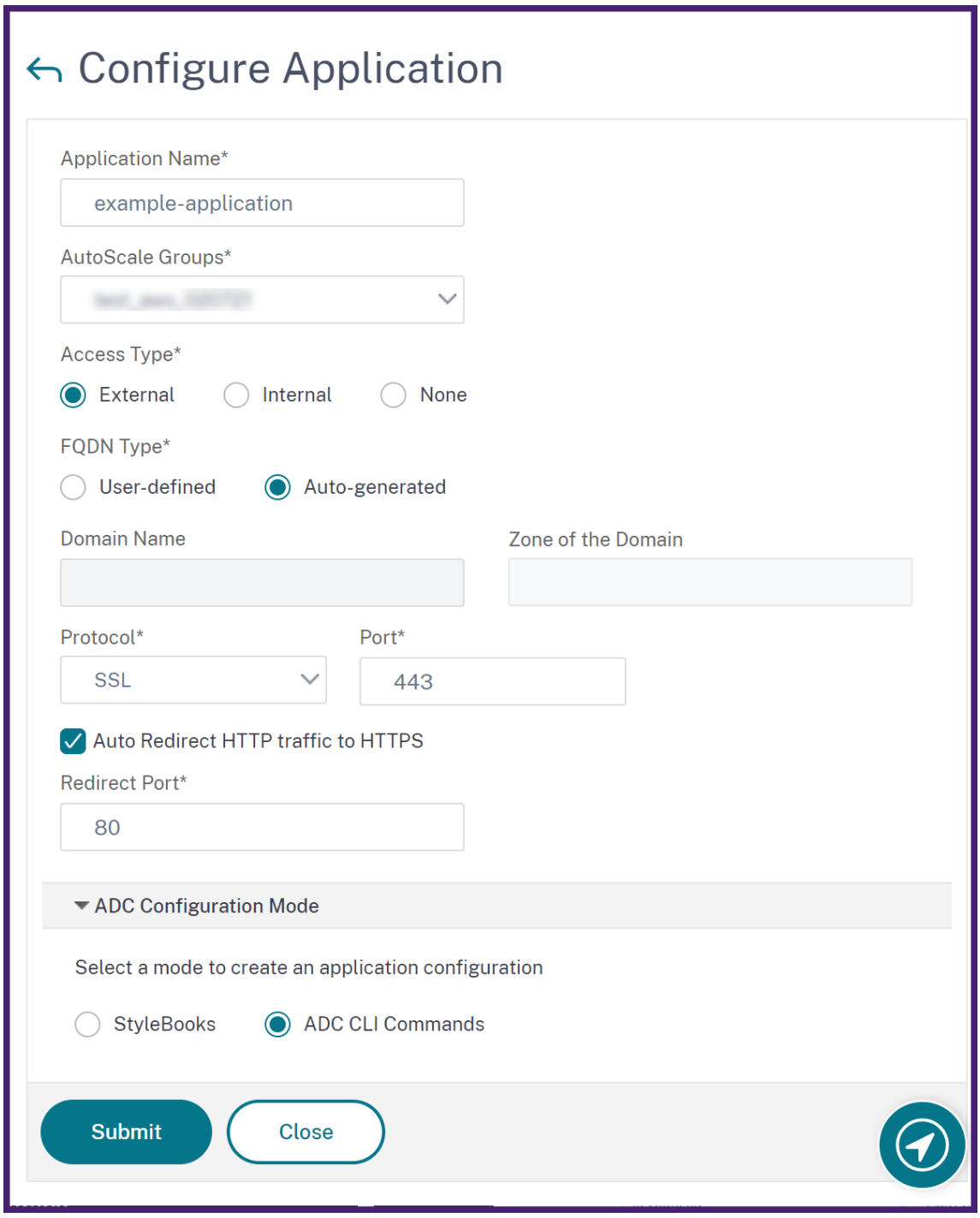
c)［次へ］をクリックします。

検証が成功したら、[**Create**] をクリックして ADC インスタンスを AWS にデプロイし、Autosale グループを作成します。

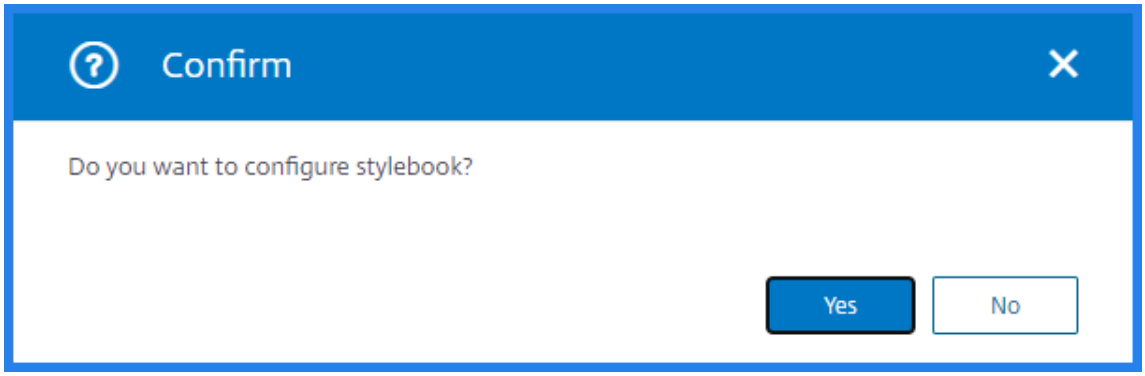


3. ADC の配備が成功したら、[アプリケーションの配置] をクリックします。

    a)「アプリケーションの構成」で、必要な詳細を指定し、「送信」をクリックします。



StyleBooks を使用してアプリケーションを構成する場合は、確認ウィンドウで [はい] を選択します。



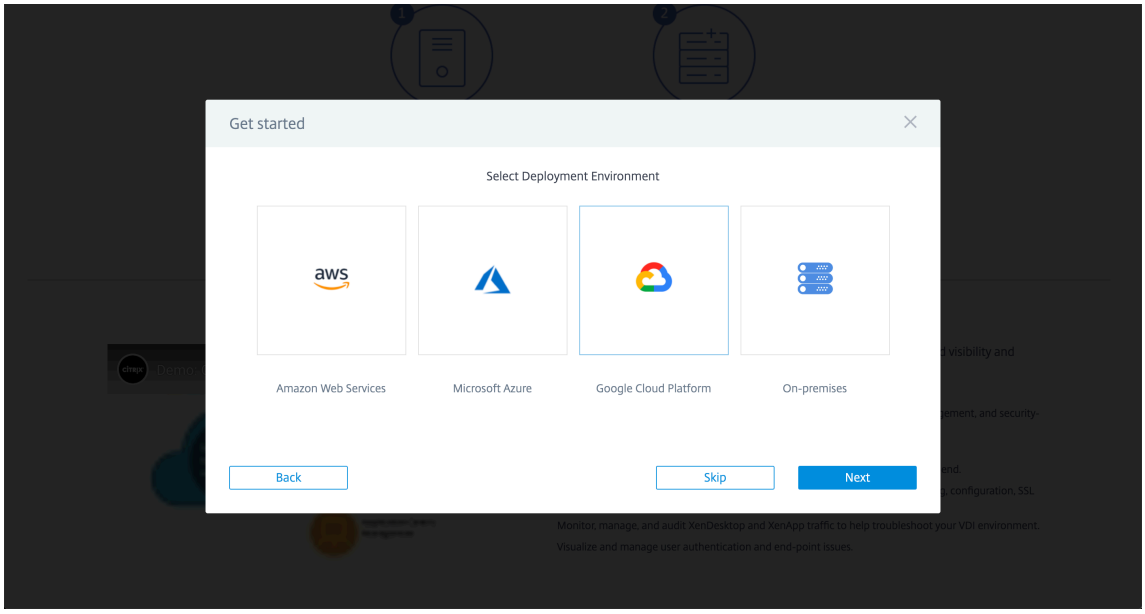
詳しくは、「AutoScale グループのアプリケーションを構成する」を参照してください。

カスタム配置を選択

このオプションは、マルチステージ展開を提供します。さまざまな環境から ADC インスタンスを検出するには、このオプションを選択します。このオプションでは、カスタム環境オプションを指定して、新しいインスタンスをデプロイすることもできます。

次の手順を実行して、ADC インスタンスをデプロイまたは検出します。

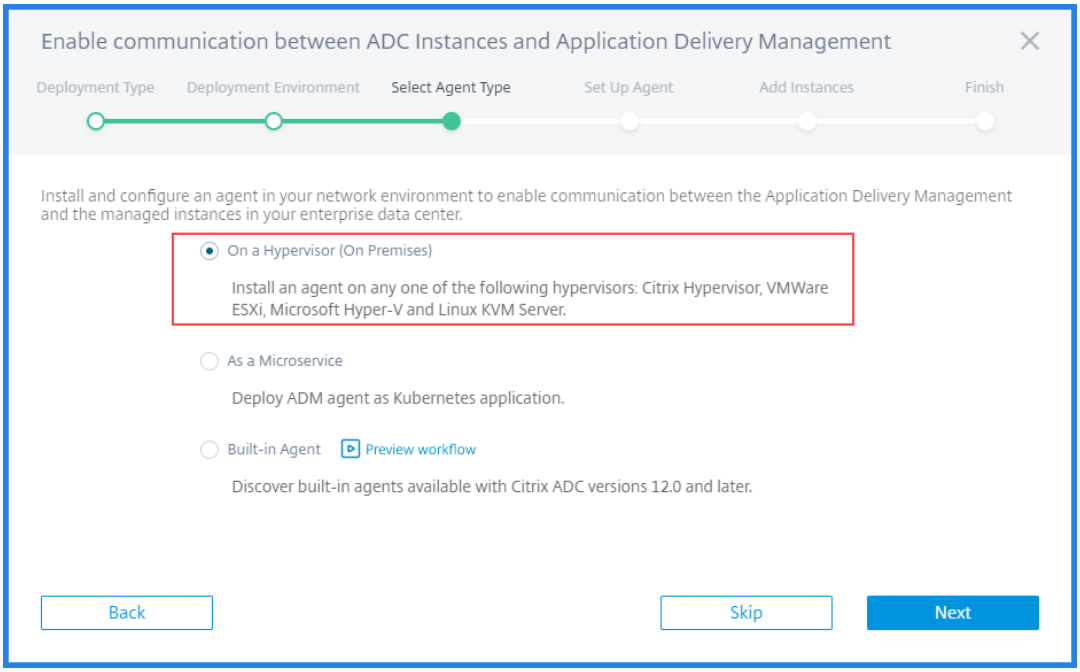
1. 次の環境のいずれかを選択します。
   - **Amazon Web Services**
   - **Microsoft Azure**
   - **Google Cloud Platform**
   - オンプレミス



2. Citrix ADM Agent をインストールして、データセンターまたはクラウド内の Citrix ADM と管理対象のインスタンス間の通信を有効にします。

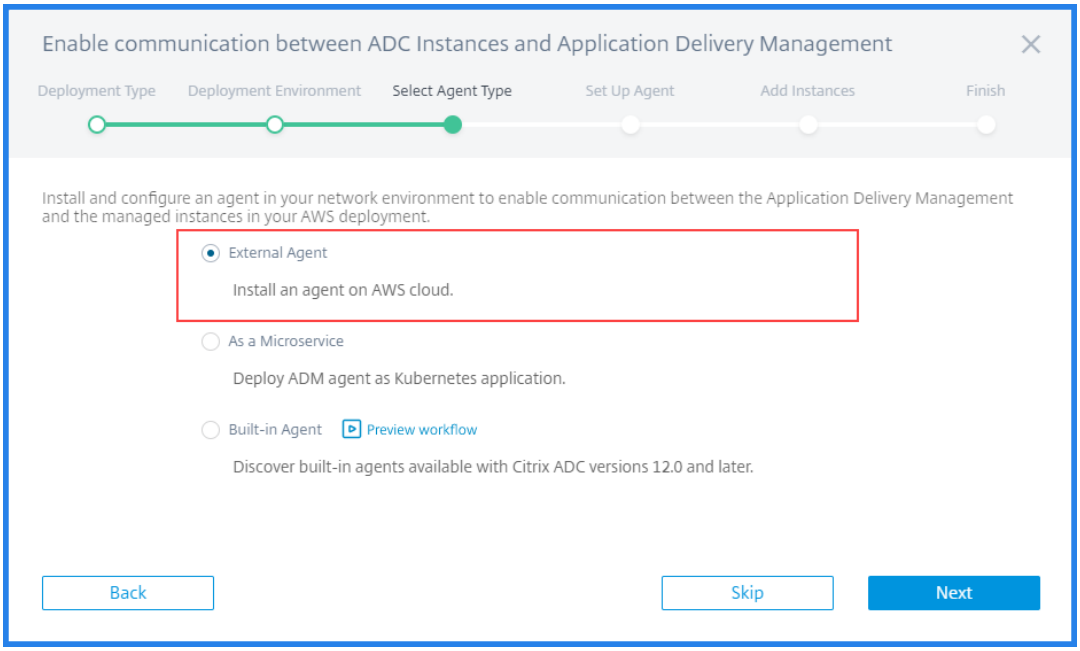
[エージェントタイプの選択] ステップでは、選択した環境に応じてエージェントのインストールオプションが異なります。

- オンプレミス -[オンプレミス] を選択すると、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

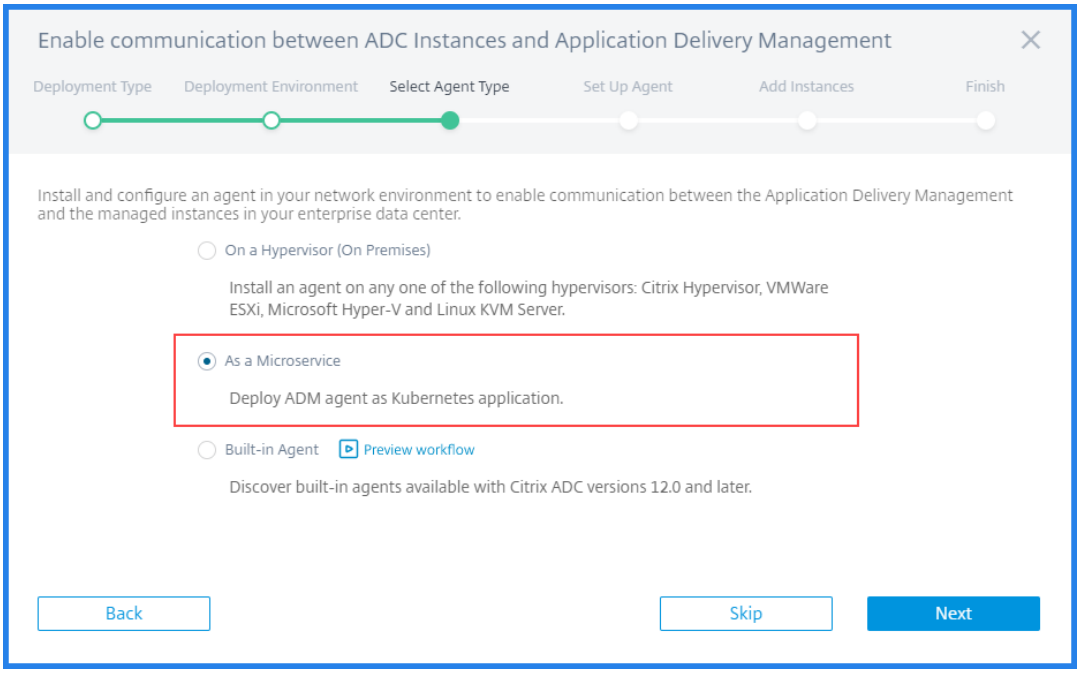


- パブリッククラウド - **Amazon Web Services**、**Microsoft Azure** 、または **Google Cloud Platform** を選択した場合、選択したクラウドにエージェントを外部インストールできます。

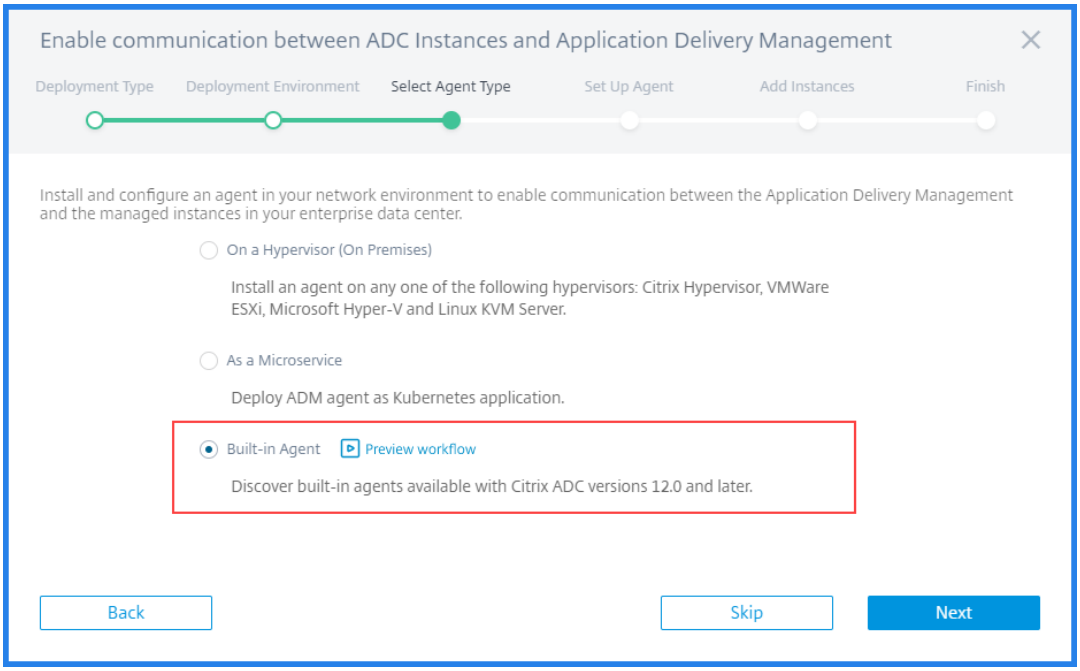
  AWS 環境のイメージの例を次に示します。



- マイクロサービスとして -エージェントを Kubernetes アプリケーションとしてデプロイします。



- 組み込みエージェント -Citrix ADC バージョン 12.0 以降で使用可能な組み込みエージェントを検出します。



3. [次へ] をクリックします

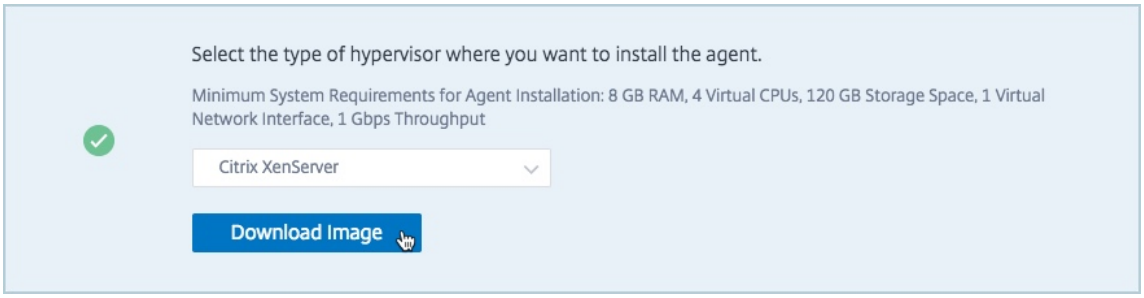
   エージェントをインストールする手順は、各オプションによって異なります。次のリンクは、エージェントをインストールするための特定の手順を示しています。

   - ハイパーバイザー
   - 外部エージェント
   - マイクロサービスとして
   - 組み込みエージェント

ハイパーバイザーにエージェントをインストールする

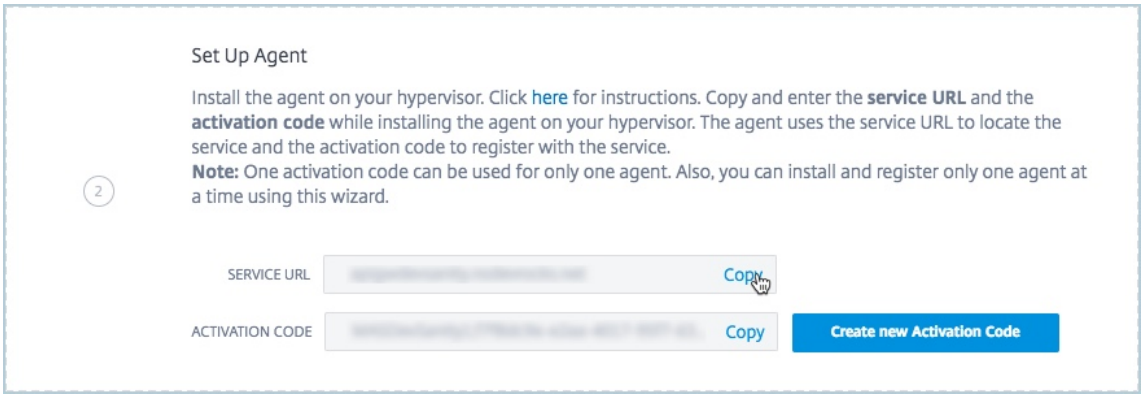
ハイパーバイザーで ADM エージェントを設定するには、次の手順に従います。

1. ハイパーバイザーを選択し、[**Download Image**] 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。

   サービス URL とアクティベーションコードが生成され、GUI に表示されます。

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。



3. 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、コピーしたサービス URL とアクティベーションコードを指定します。

   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。オンプレミスの Hypervisor にエージェントをインストールする方法の詳細については、「Citrix ADM エージェントをオンプレミスでインストールする」を参照してください。

4. エージェントのインストールが正常に完了したら、[エージェントの設定] ページに戻り、[エージェントの登録] をクリックします。

次のステップ: インスタンスを追加する。

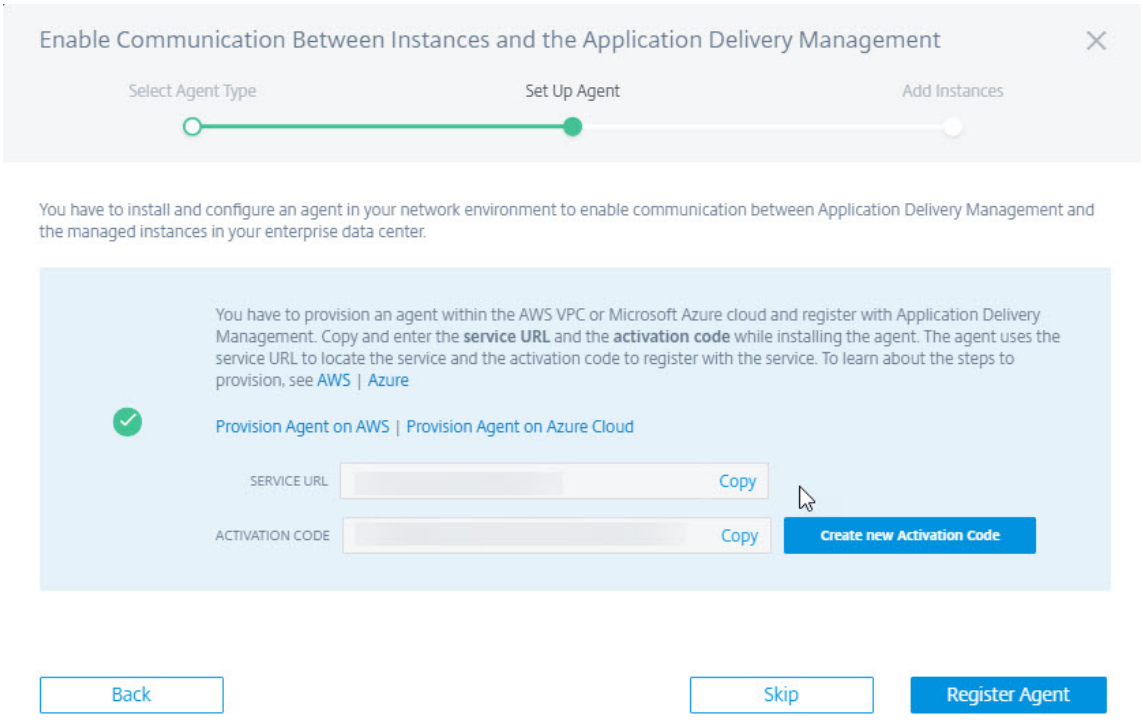
> 注
>
> 初期セットアップ時にエージェントを追加しない場合は、［スキップ］をクリックして Citrix ADM が提供する機能を確認します。エージェントとインスタンスは後で追加できます。エージェントを後で追加するには、[設定] **>** [エージェントの設定] に移動します。後でインスタンスを追加する方法については、「インスタンスの追加」を参照してください。

パブリッククラウドへのエージェントのインストール

[エージェントの設定（**Set Up Agent**）] ページからエージェントイメージをダウンロードする必要はありません。エージェントイメージは、それぞれのクラウドマーケットプレイスで入手できます。

1. エージェントのインストール時に使用するサービス URL とアクティベーションコードをコピーして保存します。

   新しいアクティベーションコードが必要な場合は、[新しいアクティベーションコードの作成] をクリックし、エージェントのインストール時に使用するコードをコピーして保存します。



- Microsoft Azure クラウドにエージェントをインストールする方法の詳細については、「Microsoft Azure クラウドへの Citrix ADM エージェントのインストール」を参照してください。
- AWS にエージェントをインストールする方法の詳細については、「AWS に Citrix ADM エージェントをインストールする」を参照してください。
- Google Cloud にエージェントをインストールする方法の詳細については、「GCP に Citrix ADM エージェントをインストールする」を参照してください。

2. エージェントのインストールが正常に完了したら、[エージェントの設定] ページに戻り、[エージェントの登録] をクリックします。

次のステップ: インスタンスを追加する。

エージェントをマイクロサービスとしてインストールする

Citrix ADM エージェントをマイクロサービスとして Kubernetes クラスターに展開し、Citrix **ADM** でサービスグラフを表示できます。

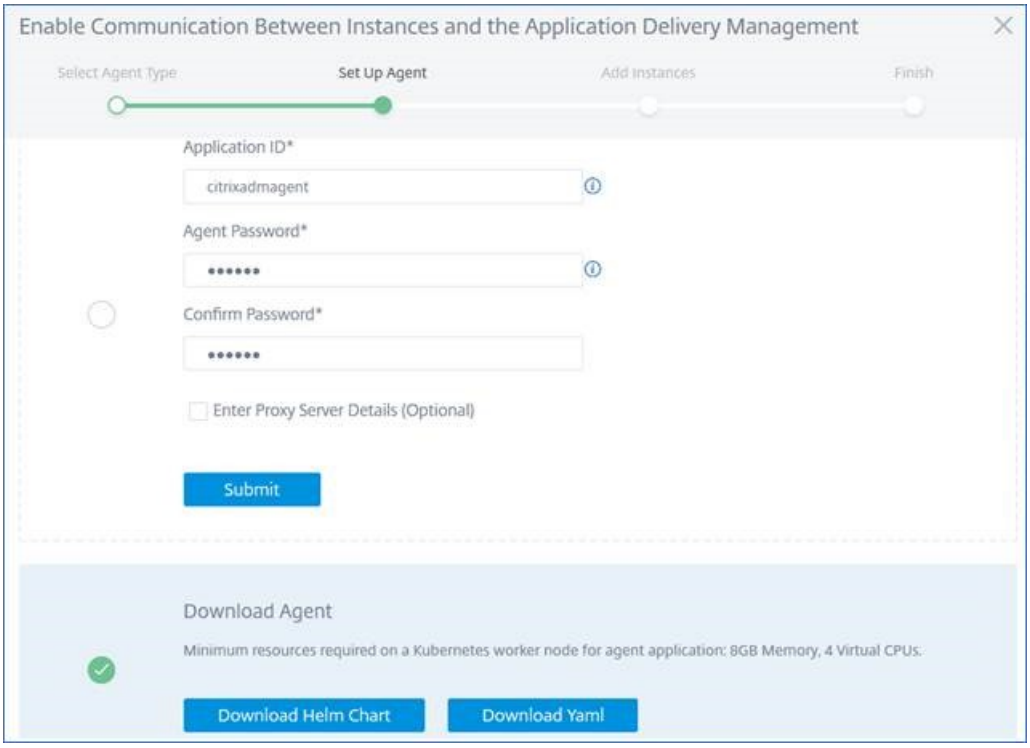
サービスグラフの使用を開始する方法については、「サービスグラフの設定」を参照してください。

1. 次のパラメータを指定します。

   a) アプリケーション **ID** — Kubernetes クラスタ内のエージェントのサービスを定義し、このエージェントを同じクラスタ内の他のエージェントと区別するための文字列 ID。

b)「エージェントパスワード」— このパスワードを使用して、エージェントを介して CPX から ADM サービスへのオンボードに使用する CPX のパスワードを指定します。

c)「パスワードの確認」— 確認のために同じパスワードを指定します。



d)「送信」をクリックします。

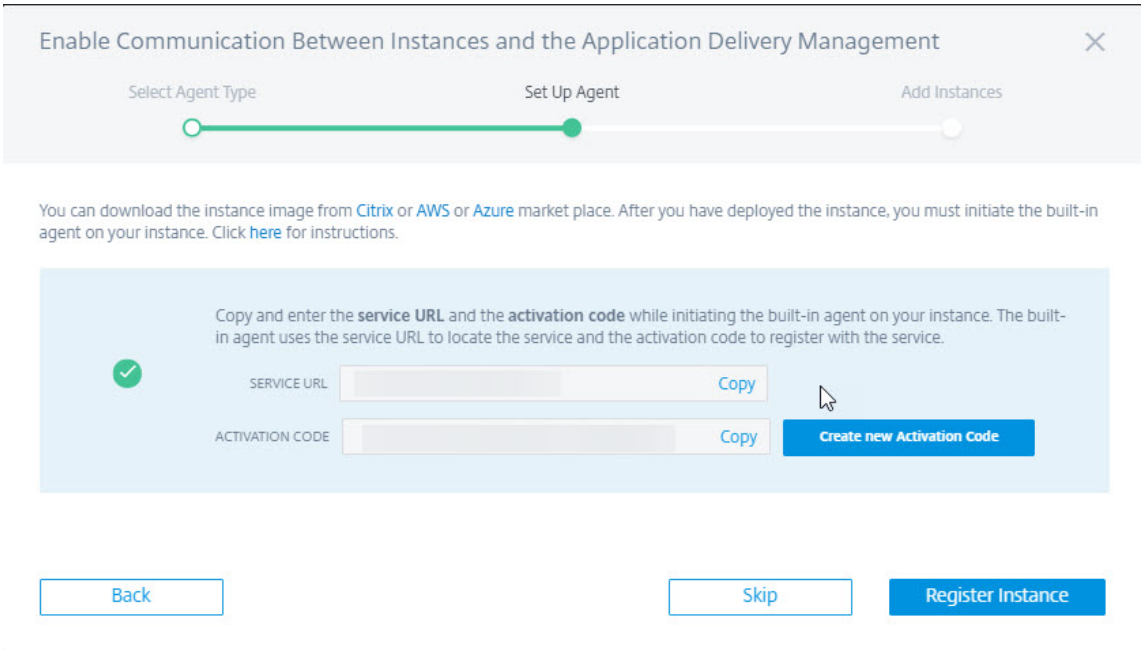
2. [**Submit**] をクリックすると、YAML または Helm チャートをダウンロードできます。
3. [閉じる] をクリックします。

詳しくは、「Kubernetes クラスタに Citrix ADM エージェントをインストールする」を参照してください。

Citrix ADC インスタンスで組み込みエージェントを使用する

環境内の Citrix ADC インスタンスには、組み込みエージェントが含まれています。組み込みエージェントを起動し、それを使用してインスタンスと Citrix ADM 間の通信を確立できます。

1. 生成されたサービス **URL** とアクティベーションコードをコピーします。Citrix ADC インスタンスで組み込みエージェントを起動するときに使用するように、これらを保存します。



Citrix ADC インスタンスで組み込みエージェントを起動する方法の詳細については、「Citrix ADC インスタンスで組み込みエージェントを起動する」を参照してください。

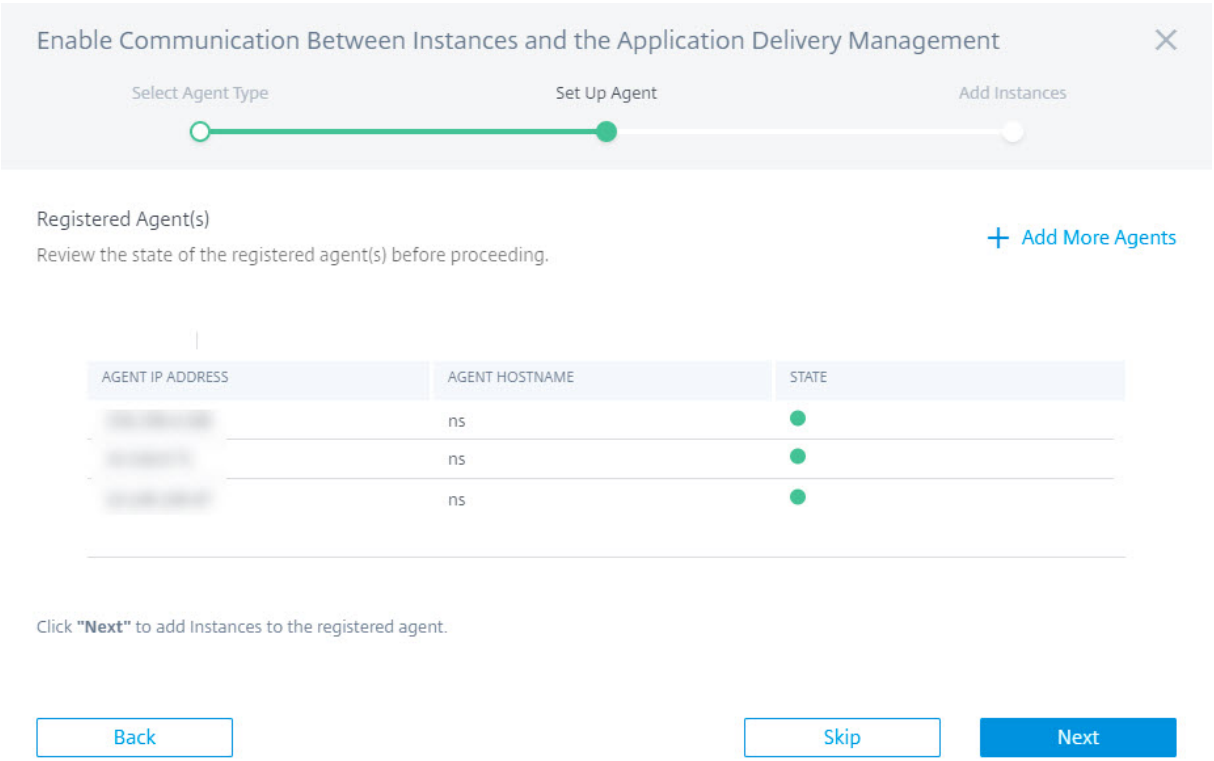
2. 組み込みエージェントが開始されたら、[エージェントの設定] ページに戻り、[**Register Instance**] をクリックします。

次のステップ: インスタンスを追加する。

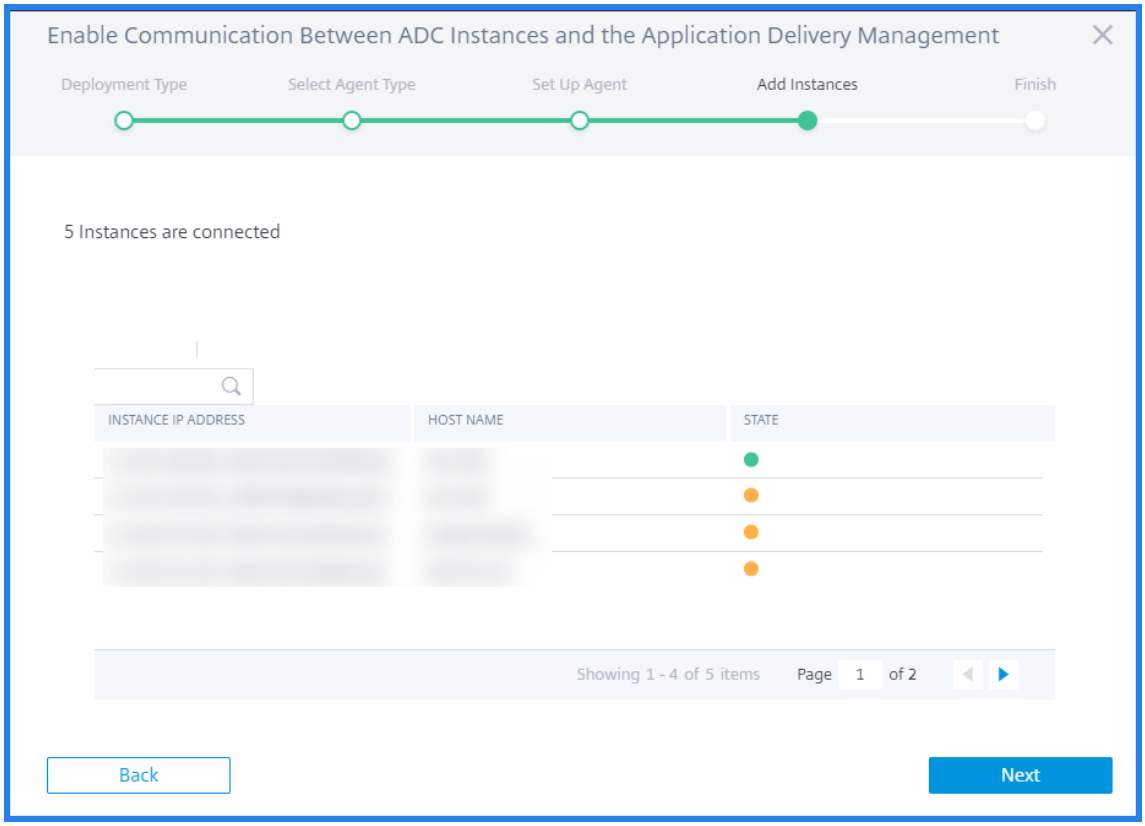
Citrix ADM へのインスタンスの追加

インスタンスとは、Citrix ADM から検出、管理、監視するネットワークアプライアンスまたは仮想アプライアンスです。これらのインスタンスを管理および監視するには、インスタンスをサービスに追加する必要があります。

エージェントのインストールと登録が正常に完了すると、エージェントが [エージェントの設定] ページに表示されます。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。



1. [**Add Instances**] ページで、登録エージェントに接続されている ADC インスタンスを表示します。インスタンスが [**Up**] ステータスになっていることを確認し、[**Next**] をクリックします。

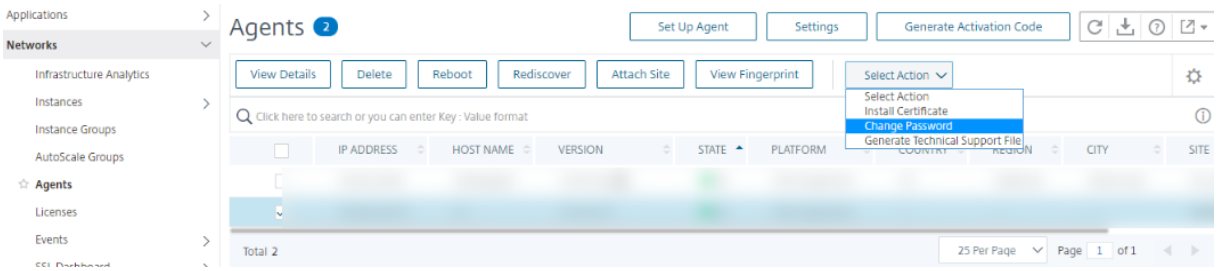


2. [完了] をクリックして初期セットアップを完了し、配置の管理を開始します。

> 注
>
> 初期セットアップ時にインスタンスを追加しない場合は、[完了] をクリックしてセットアップを完了し、後でインスタンスを追加します。後で Citrix ADM にインスタンスを追加する方法については、「インスタンスの追加」を参照してください。

エージェントアクション

ADM サービスをセットアップしたら、エージェントにさまざまなアクションを適用できます。[ネットワーク] **>** [エージェント] に移動します。



[アクションの選択] では、次の機能を使用できます。

新しい証明書をインストールする: セキュリティ要件を満たすために別のエージェント証明書が必要な場合は、証明

書を追加できます。

デフォルトのパスワードを変更する: インフラストラクチャのセキュリティを確保するために、エージェントのデフォルトのパスワードを変更します。

テクニカルサポートファイルを生成する: 選択した Citrix ADM エージェントのテクニカルサポートファイルを生成します。このファイルをダウンロードし、Citrix テクニカルサポートに送信して、調査とトラブルシューティングを行うことができます。

インスタンスを管理するように **ADC** 組み込みエージェントを構成する

May 7, 2021

組み込みエージェントは、バージョン`12.1.48.13`以降を実行している Citrix ADC MPX、VPX、Gateway インスタンス、およびバージョン 13.0 61.x 以降および 12.1 58.x 以降を実行する Citrix ADC SDX インスタンスで使用できます。データセンターやパブリッククラウドに専用エージェントをインストールする代わりに、ADC インスタンスでこのエージェントを開始できます。組み込みエージェントは、インスタンスと Citrix ADM サービス間の通信を可能にします。

> 注
>
> 組み込みエージェントは、次の Citrix ADC インスタンスタイプでのみ使用できます。
>
> - Citrix ADC MPX
> - Citrix ADC VPX
> - Citrix ADC SDX
> - Citrix Gateway

内蔵エージェントは、小規模な ADC スタンドアロンまたは HA ペアの導入に最適です。複数の ADC インスタンスがある場合は、デプロイ用に専用エージェントを使用します。このエージェントにより、組み込みエージェントよりも優れたデータ集約機能が確保されます。詳しくは、「エージェントをオンプレミスでインストールする」を参照してください。

Citrix ADM サービスは、組み込みエージェントを使用した Citrix ADC インスタンスの管理と監視をサポートします。ただし、次の機能は組み込みエージェントではサポートされていません。

- アプリケーションダッシュボード
- Web Insight
- SSL insight
- HDX Insight
- Gateway insight
- セキュリティに関する洞察
- 高度な分析
- プールライセンス

組み込みエージェントから外部エージェントに移行できます。詳しくは、「組み込みエージェントから外部エージェントへの移行」を参照してください。

前提条件

Citrix ADC インスタンスで組み込みエージェントを構成する前に、次のことを確認してください。

- Citrix ADC（MPX、VPX、またはゲートウェイ）インスタンスがバージョン`12.1.48.13`以降で実行されている。SDX インスタンスは、バージョン`13.0.61.x`以降を実行しています。
- Citrix ADC インスタンス上に DNS ネームサーバーが追加されます。

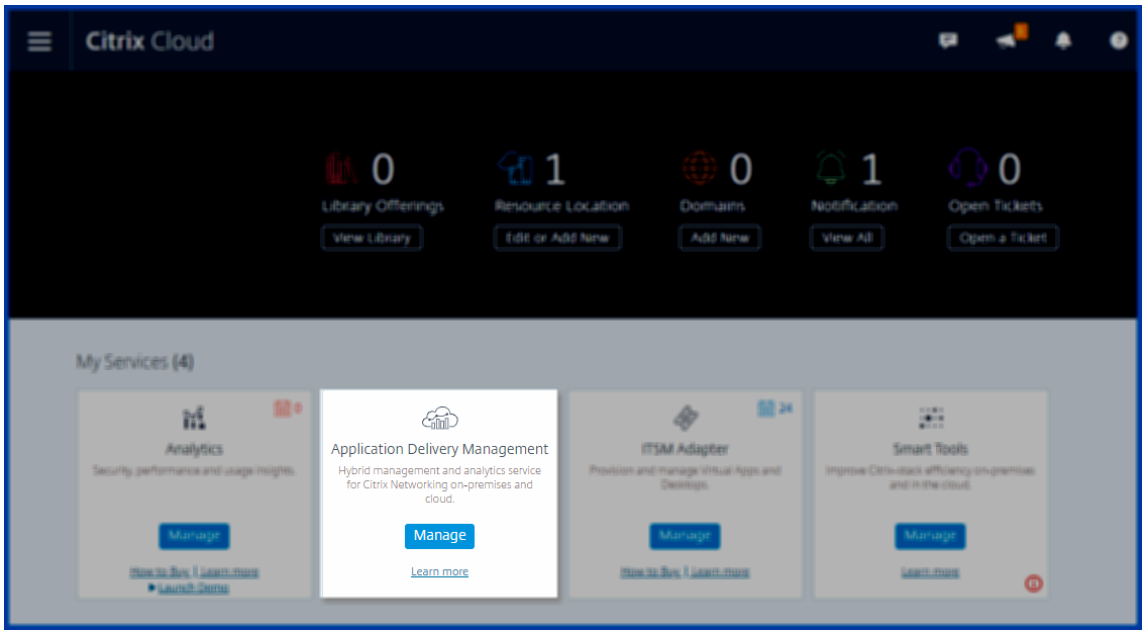
  詳しくは、「ネームサーバの追加」を参照してください。
- Citrix Cloud アカウントがある。詳しくは、「Citrix Cloud へのサインアップ」を参照してください。

> 注
>
> ポートおよびその他のシステム要件に関する情報については、「システム要件」を参照してください。

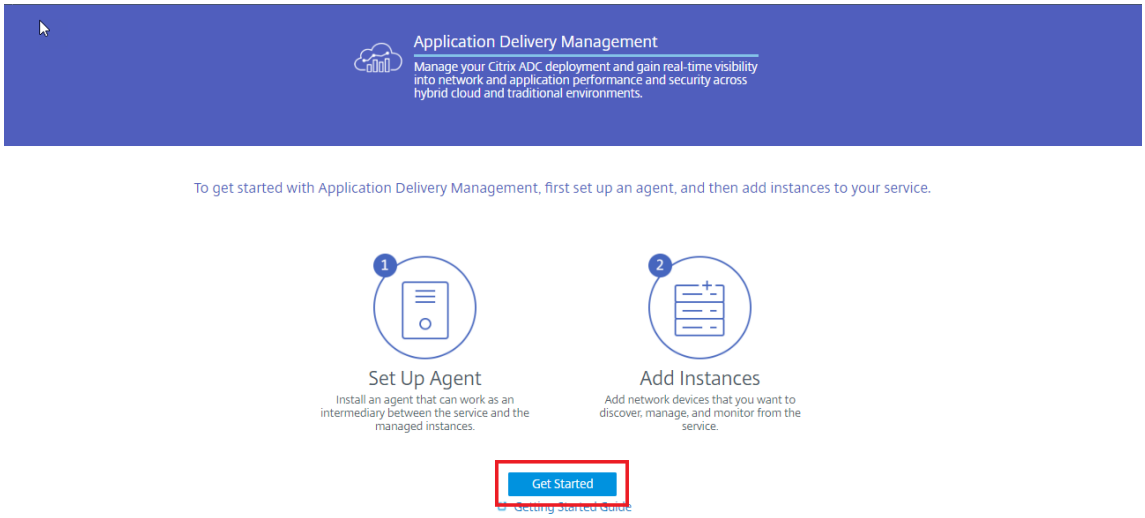
組み込みエージェントの設定

ADC 組み込みエージェントを設定するには、次の作業を実行します。

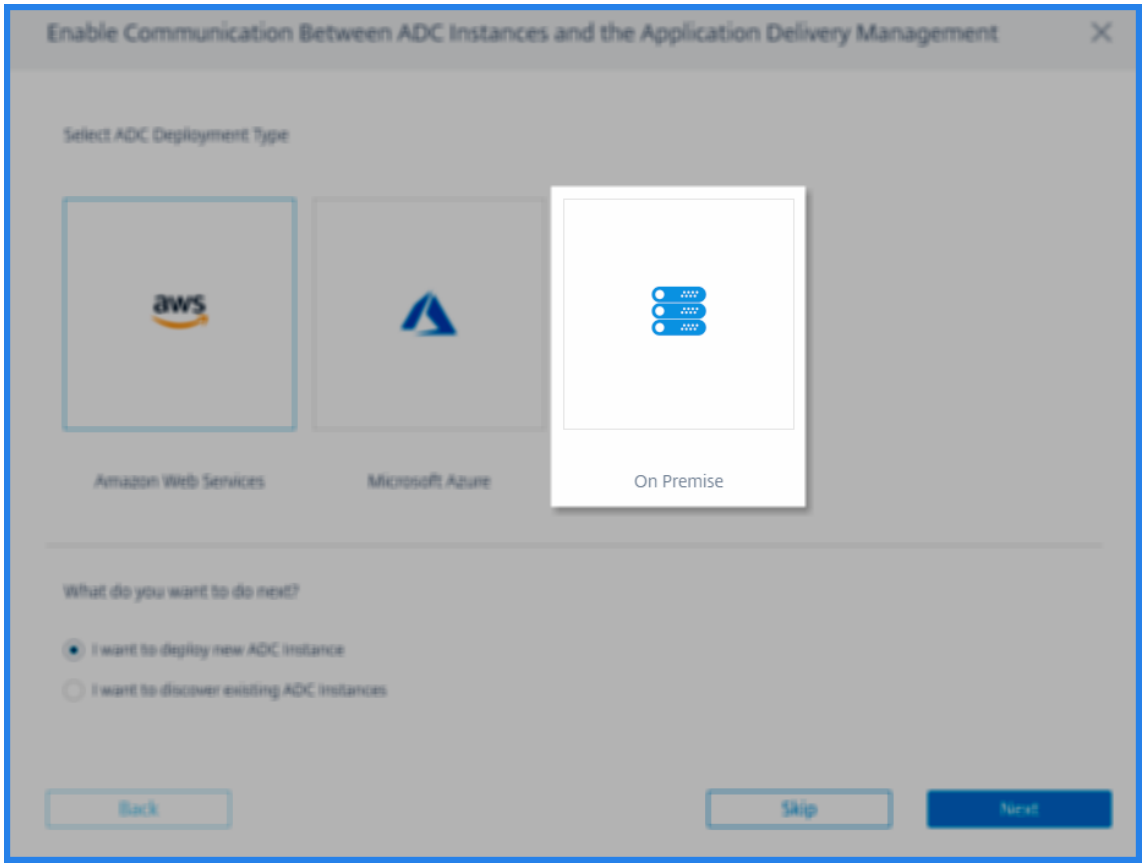
1. Citrix Cloud にサインインします。
2. [アプリケーション配信の管理] タイルで、[管理] をクリックします。次に、ビジネスニーズに合った地域を選択します。詳しくは、「エクスプレスアカウントで Citrix ADM を管理する」を参照してください。



3. [開始] をクリックします。

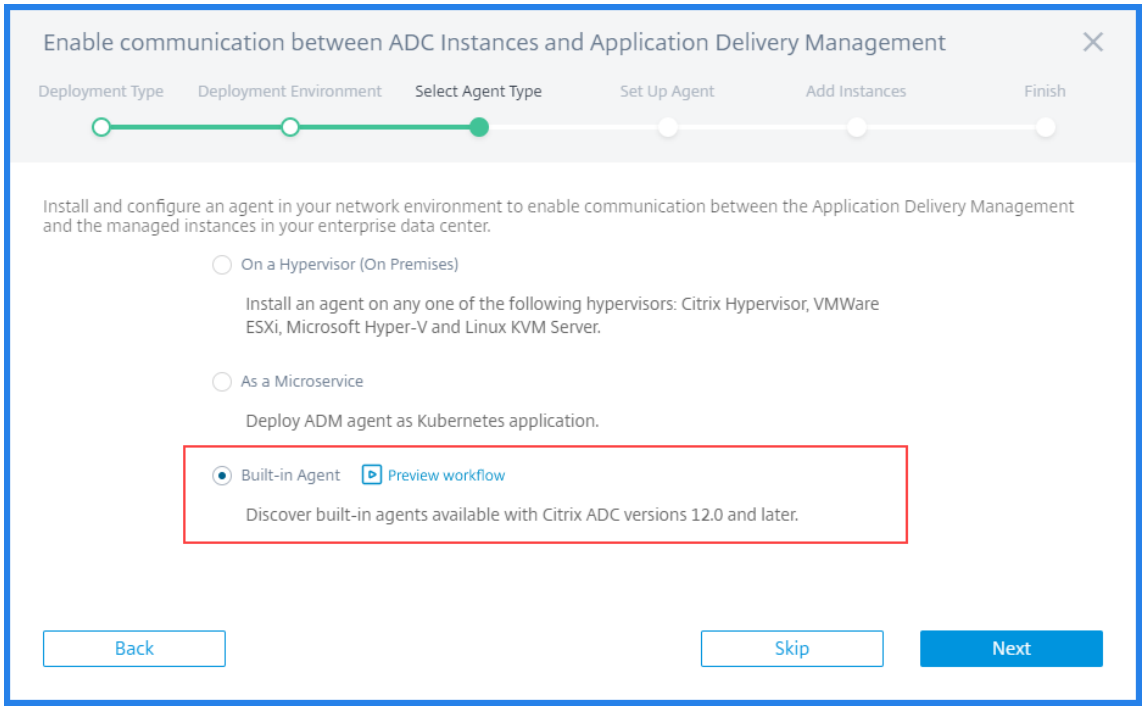


4. ADC 展開の種類として [オンプレミス] を選択します。



5.「組み込みエージェント」を選択します。

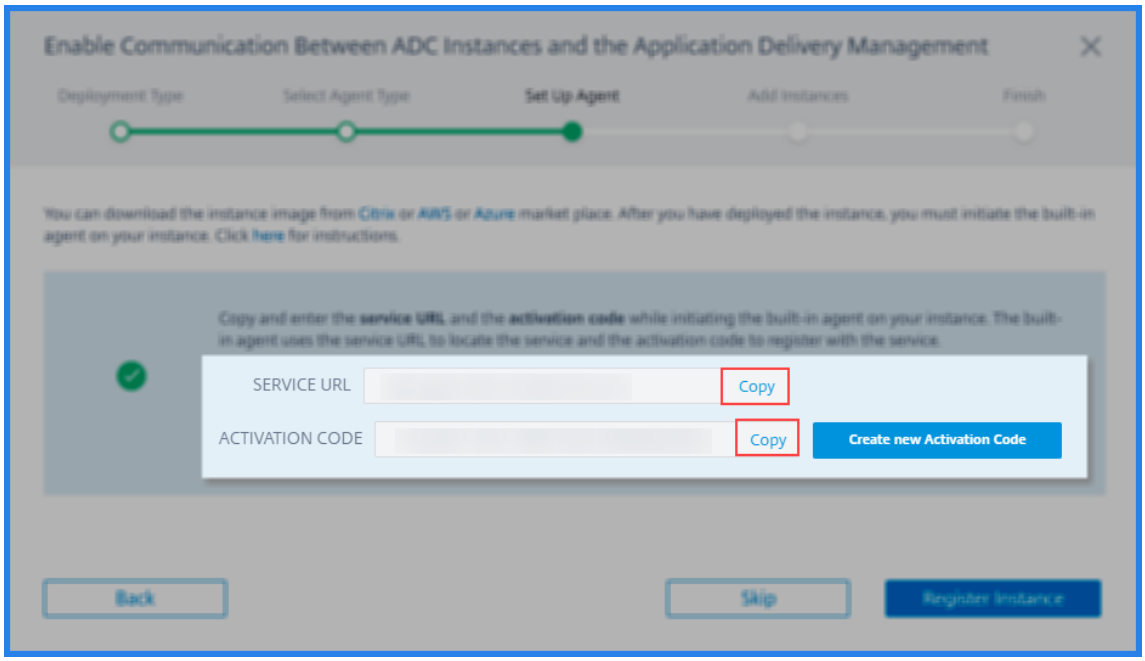
> 重要:
>
> 組み込みエージェントを使用するには、Citrix ADC インスタンスがバージョン 12.1 ビルド 48.13 以上である必要があります。



サービス URL とアクティベーションコードが生成され、GUI に表示されます。

6. 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。

   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。MPX または Gateway カスタマーの場合は、手順 7 をスキップします。



7. SSH クライアントを使用して組み込みエージェントを開始します。ゲートウェイユーザーは、この手順を省略する必要があります。

a) Citrix ADC インスタンスにログオンします。詳しくは、「Citrix ADC へのアクセス」を参照してください。

b) /var/mastools/scriptsディレクトリに移動し、次のコマンドを入力します。

SDX インスタンス

```
./mastool_int.sh <user-name> <service-url> <activation-code> -sdx
<!--NeedCopy-->
```

または

```
./mastool_init.sh <device-profile-name> <service-url> <activation-code> -sdx -profile

<!--NeedCopy-->
```

> 注:
>
> ADM は、その SDX 上で実行されているすべての VPX インスタンスを検出します。VPX インスタンスを個別に登録する必要はありません。

SDX アプライアンスおよび **MPX** インスタンスおよびゲートウェイインスタンスで実行されていない **VPX** インスタンス

ADM イメージのバージョンが 13.0 61.x または 12.1 57.x より低い場合は、コマンドcat /var/mastools/version.confを入力してmastoolsバージョンを確認する必要があります。出力が0.0-0.0の場合、これが初めてです。

ソフトウェアのバージョンに応じて、次のコマンドのいずれかを入力します。

ADC イメージ・バージョン	mastools_version0.0-0.0ですか?	プロファイルで登録するためのコマンド	プロファイルなしで登録するためのコマンド
13.0 61.xx と 12.1 57.xx より低い	はい	./mastools_init.sh <device_profile_name> <service_url> "MAS;<activation_code>"-profile	./mastools_init.sh <user_name> <pwd> <service_url> "MAS;<activation_code>"

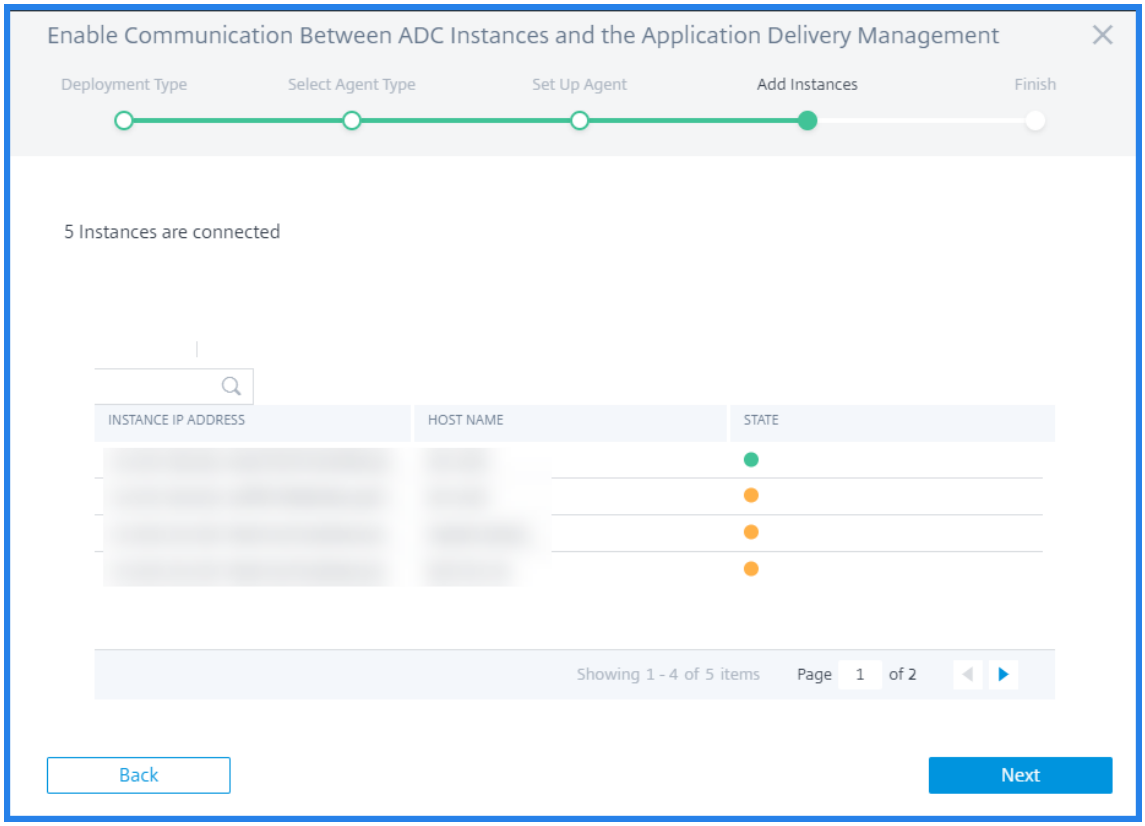
ADC イメージ・バージョン	mastools_version0.0-0.0ですか?	プロファイルで登録するためのコマンド	プロファイルなしで登録するためのコマンド
13.0 61.xx と 12.1 57.xx より低い	いいえ	./mastools_init.sh <device_profile_name> <service_url> <activation_code> -profile	./mastools_init.sh <user_name> <pwd> <service_url> <activation_code>
13.0 61.x と 12.1 57.xx より高い	該当なし	./mastools_init.sh <device_profile_nam> <service_url> <activation_code> -profile	./mastools_init.sh <user_name> <pwd> <service_url> <activation_code>

- <username>で、Citrix ADC ユーザー名を入力します。
- <password>で、ADC パスワードを入力します。
- <service_url>で、前の手順でコピーした URL を貼り付けます。
- <activation_code>で、前の手順でコピーしたアクティベーションコードを貼り付けます。

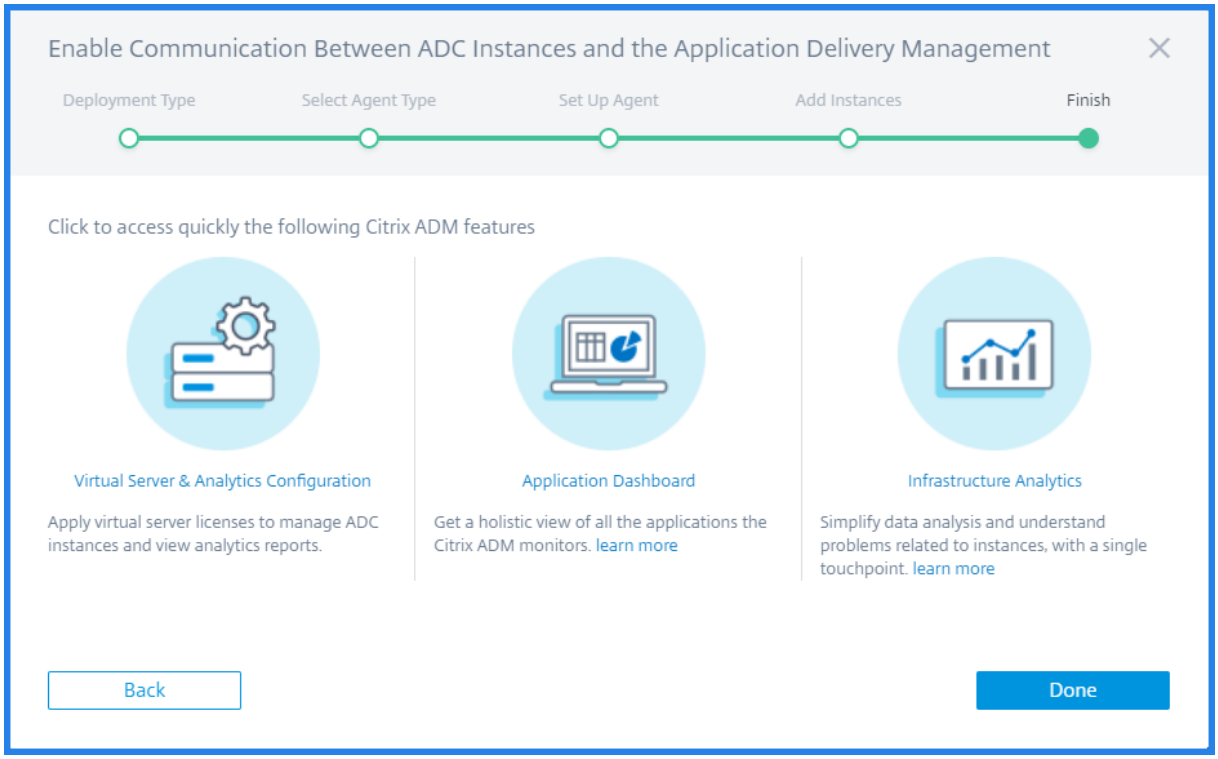
MPX、VPX、および Gateway インスタンスの場合、mastoolsコマンドを使用した初期化が完了すると、エージェントと ADM サービス間の通信が確立されます。エージェントは、最新のソフトウェアバージョンが使用可能になると、自動的にアップグレードされます。ただし、バージョン ADC 12.1 57.18 以降、および ADC 13.0 61.48 以降では、組み込みエージェントは初期化なしで ADM サービスと通信し、定期的に最新のソフトウェアバージョンに自動的にアップグレードされます。
SDX インスタンスの場合、エージェントには 13.0 61.x 以降、12.1 58.x 以降のすべてのサポートされているバージョンで自動アップグレード機能が付属しています。

> 注:
>
> HA ペアでは、プライマリノードでの登録を完了します。2 次ノードで登録を実行すると、次のメッセージが表示されます。
>
> **1** 次ノードで登録コマンドを実行してください。

8. ADM サービスページに戻り、[インスタンスの登録] をクリックします。
9. [**Add Instances**] で、組み込みエージェントを開始したインスタンスを表示します。インスタンスが [**Up**] ステータスになっていることを確認し、[**Next**] をクリックします。



10. [完了] をクリックします。



組み込みエージェントの設定に成功すると、次のような ADM 機能にアクセスできます。

- 仮想サーバーと分析 — ライセンスを仮想サーバーに適用して、ADC インスタンスを管理します。詳しくは、「サブスクリプションの管理」を参照してください。
- アプリケーションダッシュボード — すべてのアプリケーションを総合的に表示します。詳しくは、「アプリケーション管理とダッシュボード」を参照してください。
- インフラストラクチャ分析 — この機能は、インスタンスに問題を引き起こした、または結果として生じる可能性のある要因を視覚化するのに役立ちます。詳しくは、「インフラストラクチャ分析」を参照してください。

> 注:
>
> **[ネットワーク] > [エージェント] > [アクティベーションコードの生成]** ページに移動して、組み込みエージェントを構成することもできます。URL とアクティベーションコードをコピーして ADC インスタンスに貼り付け、そのインスタンスを検出します。

組み込みエージェントが起動したら、［ネットワーク］**>**［インスタンス］**>**［**Citrix ADC**］の順に移動します。このページには、組み込みエージェントを使用して検出された管理対象インスタンスの詳細が表示されます。

トラブルシューティング

登録が失敗した場合、または登録は成功しても、組み込みエージェントが ADM GUI に表示されない場合は、ログをチェックできます。

- 登録に失敗した場合は、`/var/mastools/logs/mastools_reg.py.log`のログをチェックしてください
- 登録は成功しても、組み込みエージェントが ADM GUI に表示されない場合は、次の点を確認してください。
  - `/var/mastools/logs/mastools_upgrade.log`ログの **Mastools_upgrade**
  - `/var/log/mastoolsd.log`のバイナリログ。

Citrix ADM エージェントをオンプレミスでインストールする

May 7, 2021

エージェントは、Citrix Application Delivery Management（Citrix ADM）とデータセンターで検出されたインスタンスの仲介者として動作します。

エージェントのインストールを開始する前に、ハイパーバイザーが各エージェントに提供する必要のある必要な仮想コンピューティングリソースがあることを確認してください。エージェント要件は次のとおりです。

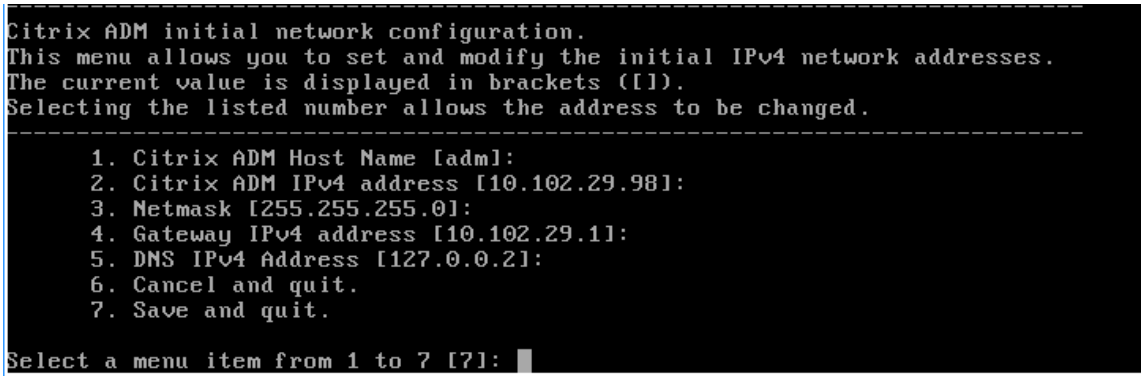
コンポーネント	条件
RAM	32GB
仮想 CPU	8

コンポーネント	条件
記憶域	30 ギガバイト
仮想ネットワークインターフェイス	1
スループット	1Gbps

> 注
>
> ポートおよびその他の要件に関連するすべての情報については、「システム要件」を参照してください。

Citrix ADM エージェントをインストールするには

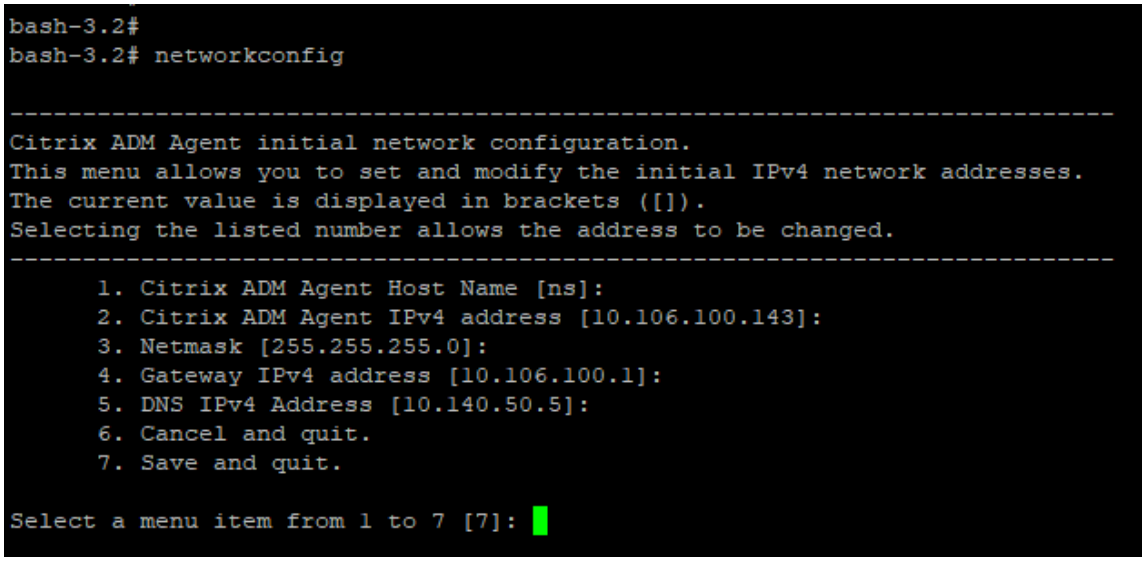
1. はじめにの説明に従って、エージェントイメージをダウンロードします。
2. エージェントイメージファイルを Hypervisor にインポートします。
3. [**Console**] タブで、次の例に示すように、初期ネットワーク構成オプションを設定します。



> 注
>
> Citrix ADM 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 を構成してください。

4. 初期ネットワーク構成が完了したら、構成設定を保存します。プロンプトが表示されたら、デフォルト（`nsrecover`/`nsroot`）資格情報を使用してログオンします。

   エージェントで設定したネットワーク設定を変更する場合は、`networkconfig` コマンドを入力し、CLI のプロンプトに従います。

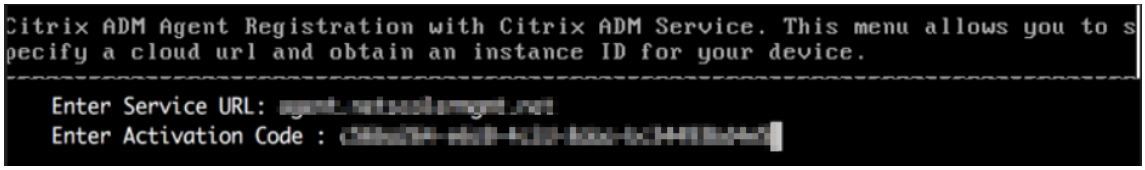


5. サービス URL の入力を求めるプロンプトが表示されない場合は、Citrix ADM エージェントで/mps に移動し、次のいずれかのスクリプトを実行します。

```
deployment_type.py
<!--NeedCopy-->
```

```
register_agent_cloud.py
<!--NeedCopy-->
```

6. エージェントイメージをダウンロードしたときに保存した サービス **URL** と アクティベーションコードを入力します。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。



7. 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。

エージェントを再起動したら、Citrix ADM GUI にアクセスし、［ネットワーク］>［エージェント］の順に選択し、エージェントの状態を確認します。

Microsoft Azure クラウドに Citrix ADM エージェントをインストールする

May 7, 2021

エージェントは、Citrix Application Delivery Management（Citrix ADM）と、エンタープライズデータセンターまたはクラウド上の管理対象インスタンスの間の仲介として機能します。

Microsoft Azure クラウドに Citrix ADM エージェントをインストールするには、仮想ネットワークにエージェントのインスタンスを作成する必要があります。Azure Marketplace から Citrix ADM エージェントイメージを取得し、Azure Resource Manager ポータルを使用してエージェントを作成します。

Citrix ADM エージェントインスタンスの作成を開始する前に、インスタンスが配置される必須サブネットで仮想ネットワークを作成していることを確認します。仮想マシンのプロビジョニング時に仮想ネットワークを作成することもできますが、柔軟性に欠けるため別のサブネットを作成することはできません。仮想ネットワークの作成については、http://azure.microsoft.com/en-us/documentation/articles/create-virtual-networkを参照してください。

仮想マシンがインターネットリソースにアクセスできるようにする DNS サーバーと VPN 接続を構成します。

前提条件

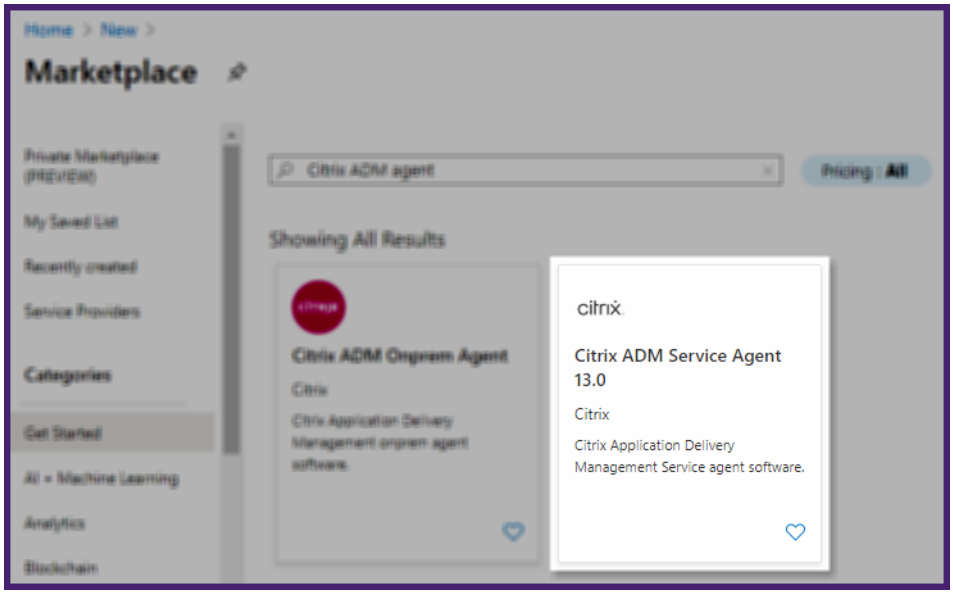
以下が割り当てられていることを確認してください。

- Microsoft Azure ユーザーアカウント
- Microsoft Azure Resource Manager へのアクセス

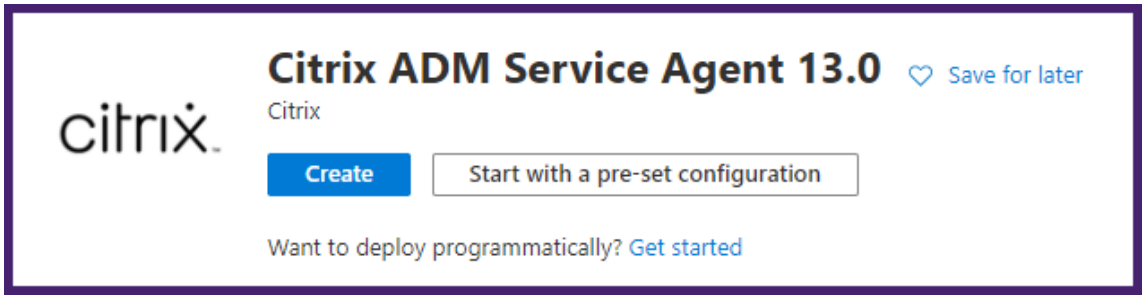
> 注
>
> - Citrix ADM エージェント仮想マシンをプロビジョニングする前に、リソースグループ、ネットワークセキュリティグループ、仮想ネットワークなどのエンティティを作成して、Provisioning 中にネットワーク情報を使用できるようにすることをお勧めします。
> - Citrix ADM エージェントが Citrix ADM および Citrix ADC インスタンスと通信するには、推奨ポートが開いていることを確認します。Citrix ADM エージェントのポート要件の詳細については、「ポート」を参照してください。

Microsoft Azure クラウドに **Citrix ADM** エージェントをインストールするには:

1. Microsoft Azure 資格情報を使用して、Azure ポータル (https://portal.azure.com) にログオンします。
2. [**+** リソースの作成] をクリックします。
3. 検索バーに`Citrix ADM Agent`を入力し、**Citrix ADM** サービスエージェントを選択します。



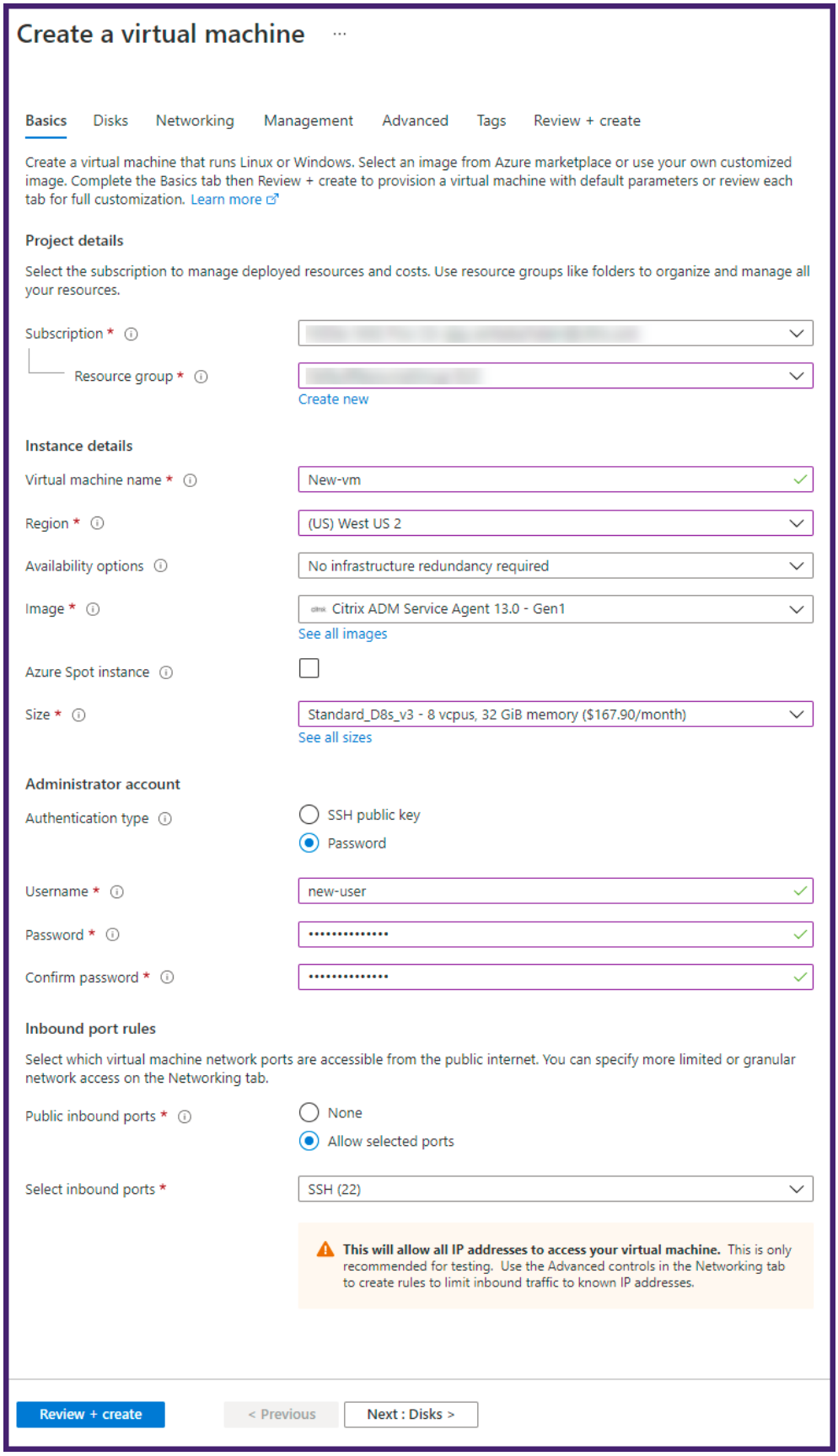
4. [作成] をクリックします。



5. [仮想マシンの作成] ウィンドウで、各セクションで必要な値を指定して、仮想マシンを作成します。

   基本:

   このタブで、プロジェクトの詳細、インスタンスの詳細、および管理者アカウントを指定します。



- 「リソースグループ」— 作成したリソースグループをドロップダウンリストから選択します。

  > 注:
  >
  > この時点でリソースグループを作成できますが、Azure Resource Manager のリソースグループからリソースグループを作成し、ドロップダウンリストからグループを選択することをお勧めします。

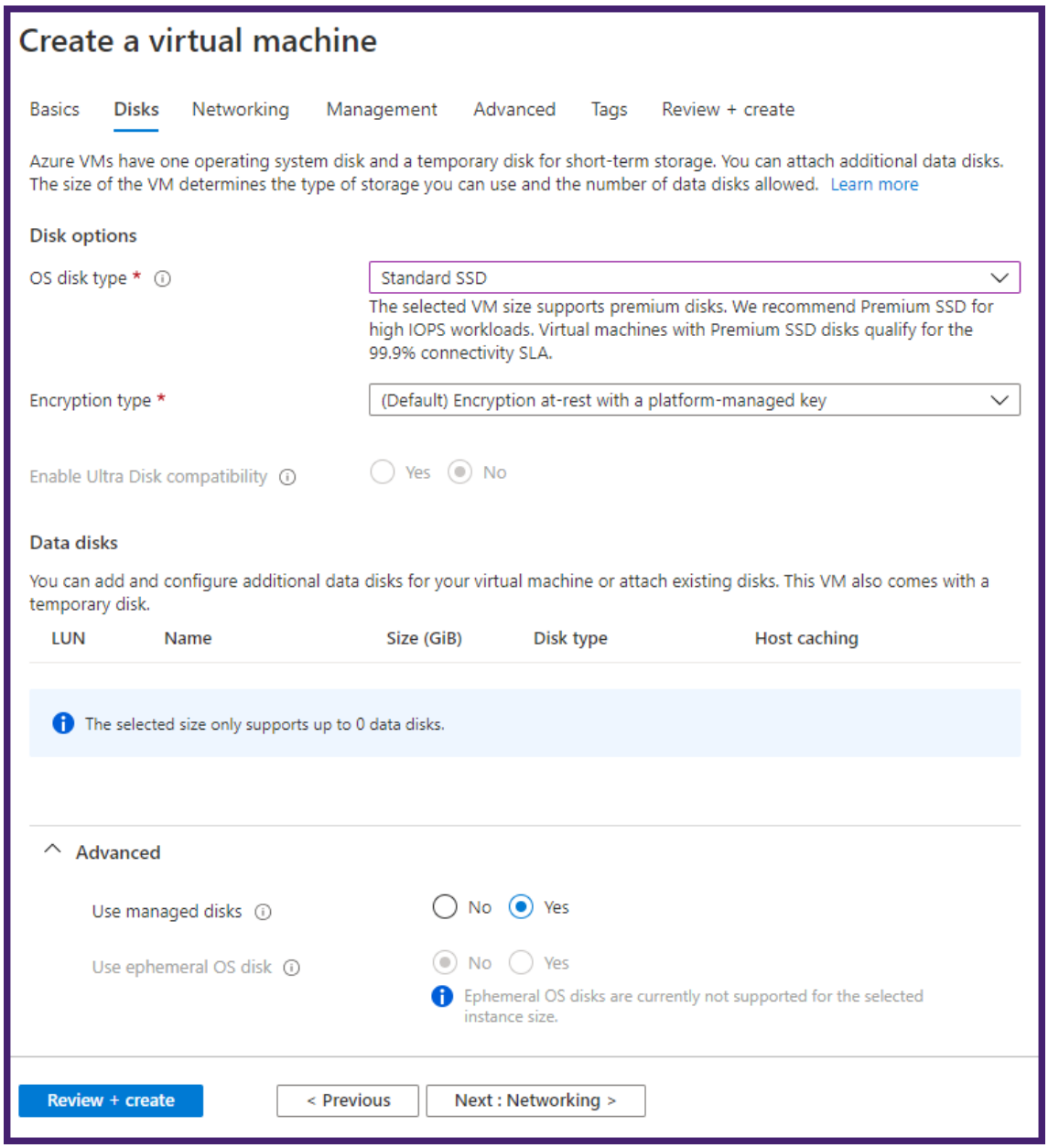
- 「仮想マシン名」 — Citrix ADM エージェントインスタンスの名前を指定します。
- [**Region**]: エージェントをデプロイするリージョンを選択します。
- 「可用性オプション」— リストから可用性セットを選択します。
- イメージ: このフィールドには、すでに選択されているエージェントイメージが表示されます。別のエージェントイメージに変更する場合は、リストから必要なイメージを選択します。
- [サイズ]: Citrix ADM エージェントを展開する仮想ディスクのタイプとサイズを指定します。

  リストから [サポートされる仮想ディスクの種類 (**HDD** または **SSD**)] を選択します。

- 「認証タイプ」—「パスワード」を選択します。
- 「ユーザー名とパスワード」— 作成したリソースグループ内のリソースにアクセスするためのユーザー名とパスワードを指定します。

ディスク**:**

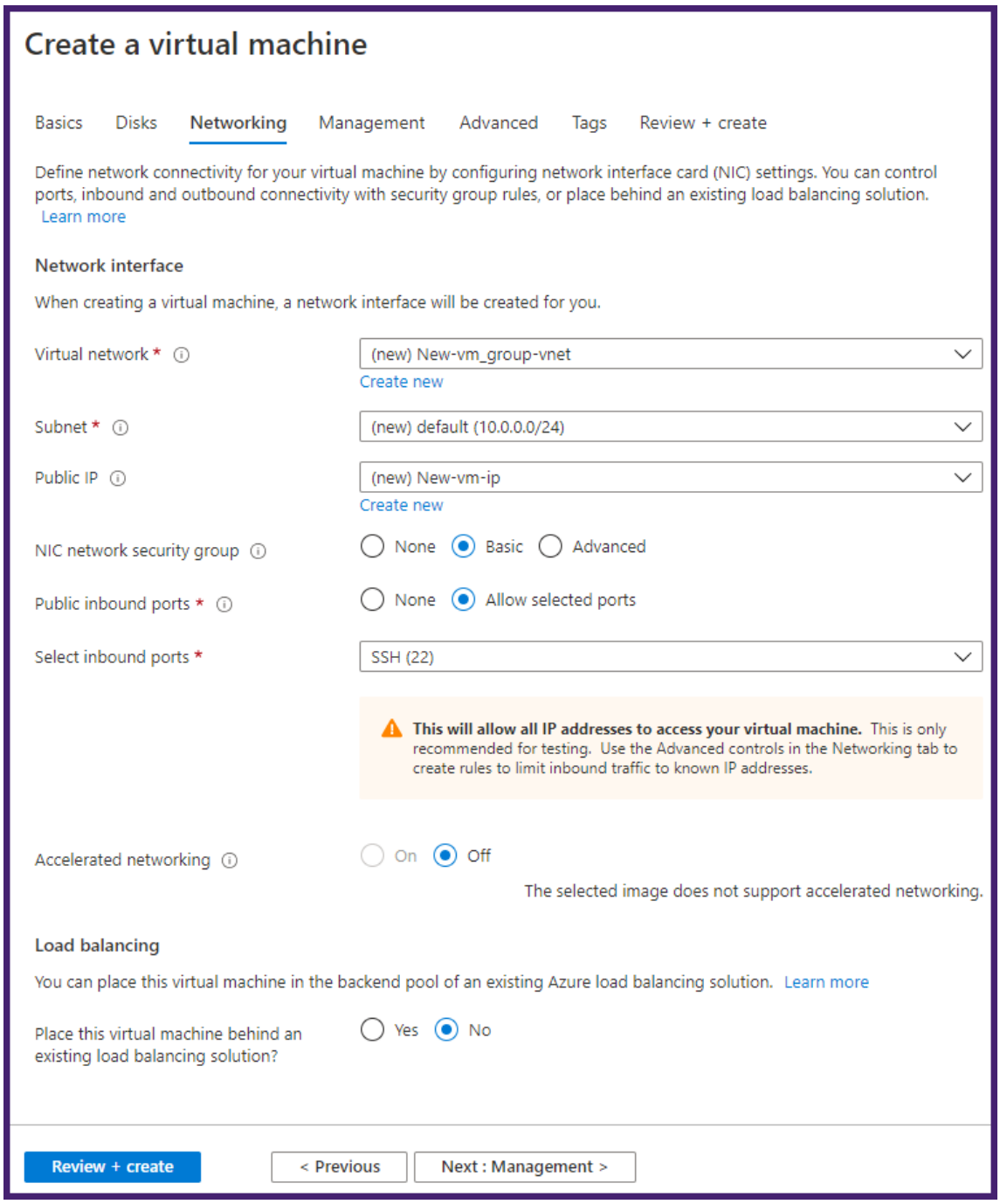
このタブで、[ディスクオプション] と [データディスク] を指定します。



- **OS** ディスクタイプ：仮想ディスクの種類（HDD または SSD）を選択します。

ネットワーク**:**

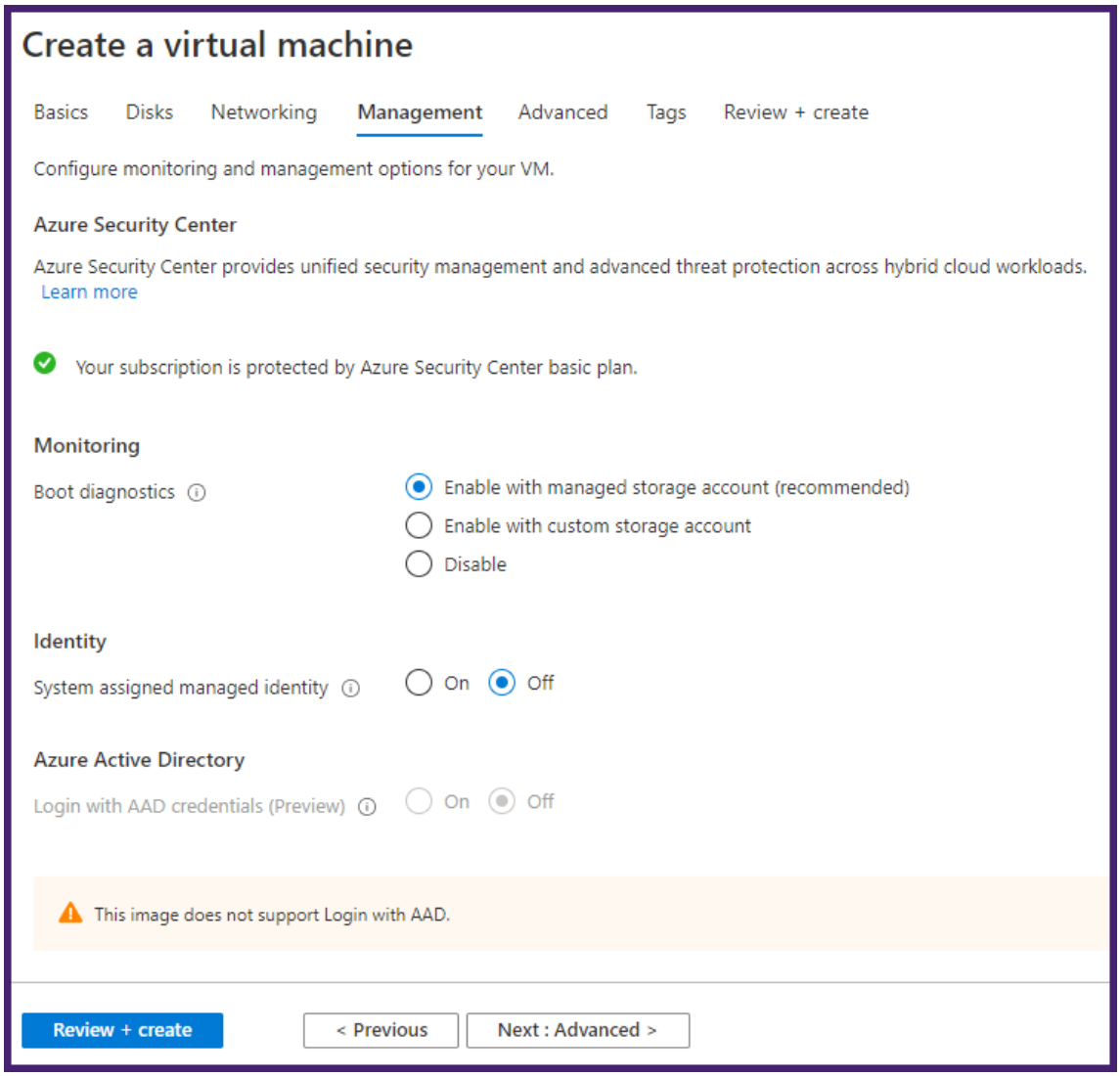
必要なネットワークの詳細を指定します。



- [仮想ネットワーク] — 仮想ネットワークを選択します。
- [Subnet] —サブネットアドレスを設定します。
- 「パブリック **IP** アドレス」— IP アドレスを選択します。
- [ネットワークセキュリティグループ] — 作成したセキュリティグループを選択します。
- インバウンドポートの選択 -パブリックインバウンドポートを許可する場合は、インバウンドルールとアウトバウンドルールがセキュリティグループで設定されていることを確認します。次に、リストから受信ポートを選択します。詳細については、「前提条件」を参照してください。

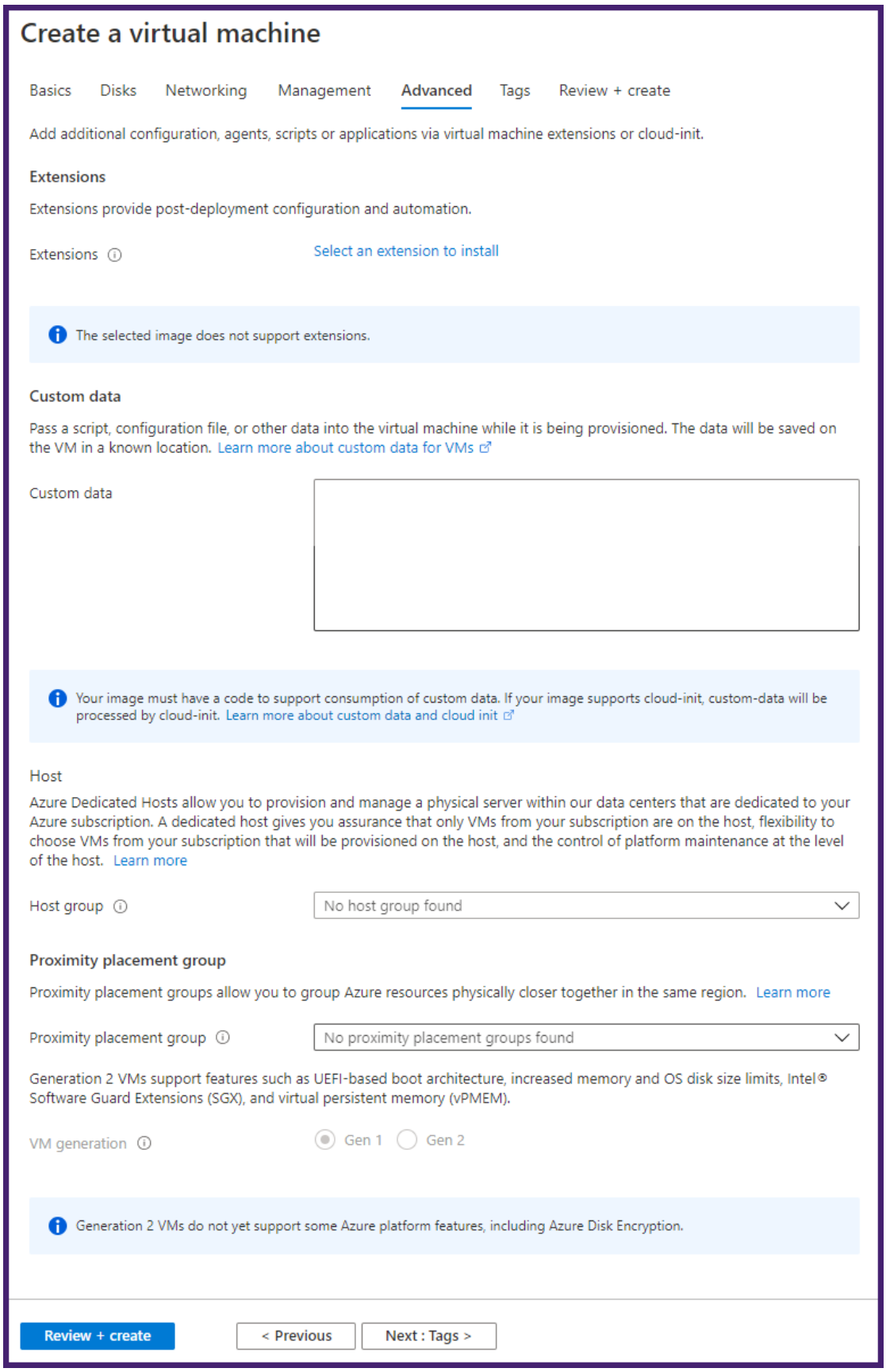
管理**:**

Azure セキュリティセンター、監視、および **ID** を指定します。



詳細設定**:**

オプション、拡張機能、カスタムデータ、および近接プレイスメントグループを指定します。



[カスタムデータ] では、エージェントの自動登録スクリプトを指定して、エージェントを ADM サービスに登録できます。スクリプトを実行し、エージェントを登録するdeployment.pyスクリプトの例を次に示します。

```
```python
#!/var/python/bin/python2.7
import os
import requests
import json
import time
import re
import logging
import logging.handlers
import boto3

'''
スクリプトの概要:
このスクリプトは、ADM エージェントを ADM に登録するのに役立ちます。これをuserdata に渡して、AWS の ADM エージェントを起動時に自動登録するようにします。ワークフローは次のとおりです
1) AWS シークレットストアから ADM サービス API 認証情報（ID とシークレット） を取得する（注:AWS シークレットストアからシークレットをフェッチする許可を与える ADM Agent に IAM ロールを割り当てる必要があります）
2) ステップ 1 で取得した認証情報を使用して ADM サービスにログインします。
3) ADMサービスを呼び出して、エージェント登録のための資格情報（ServiceURLとトークン）を取得する
4) 手順 3 で取得した認証情報を使用して登録を呼び出す
'''

'''
これらは、セットアップの設定に応じて置き換える必要があるプレースホルダです
aws_secret_id: ADM 認証情報を格納した AWS シークレットの ID
秘密の値は次のjson形式にする必要があります
{
  "adm_user_id_key": "YOUR_ID", " adm_user_secret_key": "YOUR_SECRET" }

'''

aws_secret_id = "<AWS_secret_id>」
adm_ip_or_hostname = "<YOUR_ADM_POP> .adm.cloud.com」

```


```

```
'''
Set up a specific logger with your desired output level and log
    file name
'''
log_file_name_local = os.path.basename (__file__)
LOG_FILENAME = '/var/log/' + 'bootstrap' + '.log'
LOG_MAX_BYTE = 50*1024* 1024
LOG_BACKUP_COUNT = 20

logger = logging.getLogger(__name__)
logger.setLevel (logging.debug)
logger_handler = logging.handlers.RotatingFileHandler(LOG_FILENAME
    , maxBytes=LOG_MAX_BYTE, backupCount=LOG_BACKUP_COUNT)
logger_fortmater = logging.Formatter(fmt='%(asctime)-2s:%(funcName
)30s:%(lineno)4d: [%(levelname)s] %(message)s', datefmt="%Y-%m
    -%d %H:%M:%S")
logger_handler.setFormatter (logger_fortmater)
logger.AddHandler (logger_handler

class APIHandlerException(Exception):
def __init__(self, error_code, message):
self.error_code = error_code
self.message = message

def __str__(self):
return self.message + ". Error code '" + str(self.error_code) + "'
    "

def parse_response(response, url, print_response=True):
if not response.ok:
if "reboot" in url:
logger.debug('No response for url: reboot')
resp = {
 "errorcode": "500", "message": "Error while reading response." }

return resp

if print_response:
logger.debug('Response text for %s is %s' % (url, response.text))

response = json.loads(response.text)
logger.debug("ErrorCode - " + str(response['errorcode']) + ".
    Message -" + str(response['message']))
raise APIHandlerException(response['errorcode'], str(response['
    message']))
```

```
elif response.text:
if print_response:
logger.debug('Response text for %s is %s' % (url, response.text))

result = json.loads(response.text)
if 'errorcode' in result and result['errorcode'] > 0:
raise APIHandlerException(result['errorcode'], str(result['message
    ']))
return result

def _request(method, url, data=None, headers=None, retry=3,
    print_response=True):
try:
response = requests.request(method, url, data=data, headers=
    headers)
result = parse_response(response, url, print_response=
    print_response)
return result
except [requests.exceptions.ConnectionError, requests.exceptions.
    ConnectTimeout]:
if retry > 0:
return _request(method, url, data, headers, retry-1,
    print_response=print_response)
else:
raise APIHandlerException(503, 'ConnectionError')
except requests.exceptions.RequestException as e:
logger.debug(str(e))
raise APIHandlerException(500, str(e))
except APIHandlerException as e:
logger.debug("URL: %s, Error: %s, Message: %s" % (url, e.
    error_code, e.message))
raise e
except Exception as e:
raise APIHandlerException(500, str(e))

try:
'''Get the AWS Region'''
client = boto3.client('s3')
my_region = client.meta.region_name
logger.debug("The rgion is %s" % (my_region))

'''Creating a Boto cleint session'''
session = boto3.session.Session()
client = session.client(
service_name='secretsmanager',
```



```
region_name=my_region
)

'''Getting the values stored in the secret with id: <aws_secret_id>'''
get_id_value_response = client.get_secret_value(
secretID = aws_secret_id
)
adm_user_id = json.loads(get_id_value_response["SecretString"])["adm_user_id_key"]
adm_user_secret = json.loads(get_id_value_response["SecretString"])["adm_user_secret_key"]

except Exception as e:
logger.debug("Fetching of ADM credentials from AWS secret failed with error: %s" % (str(e)))
raise e

'''
Initializing common ADM API handlers
'''
mas_common_headers = {

'Content-Type': "application/json",
'Accept-type': "application/json",
'Connection': "keep-alive",
'isCloud': "true"
 }


'''
API to login to the ADM and fetch the Session ID and Tenant ID
'''
url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/login"
payload = 'object={
 "login":{
 "ID":"' + adm_user_id + '","Secret":"' + adm_user_secret + '" }
  }
 '
try:
response = _request("POST", url, data=payload, headers=mas_common_headers)
sessionid = response["login"][0]["sessionid"]
tenant_id = response["login"][0]["tenant_name"]
```



```
except Exception as e:
logger.debug("Login call to the ADM failed with error: %s" % (str(e)))
raise e

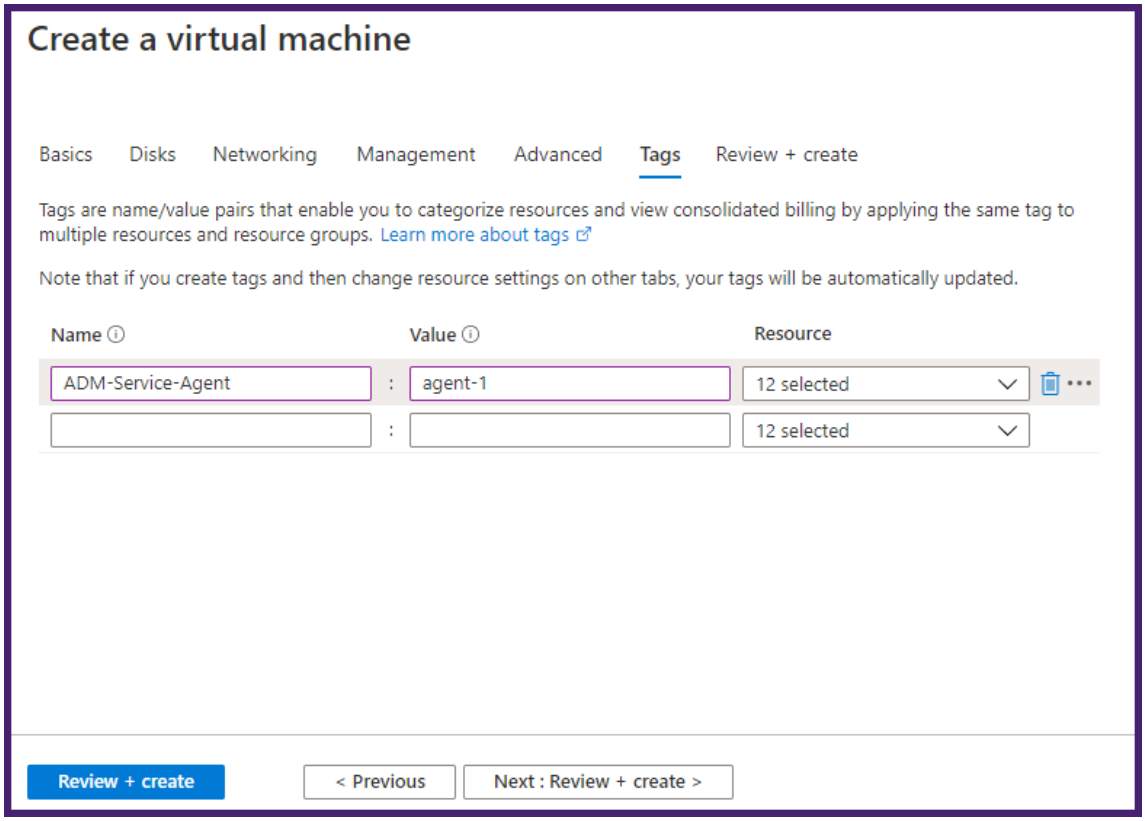
'''
API to fetch the service URL and Token to be used for registering the agent with the ADM
'''
mas_common_headers['Cookie'] = 'SESSID=' + str(sessionid)
url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/trust_preauthtoken/" + tenant_id +"?customer="+ tenant_id
logger.debug("Fetching Service URL and Token.")
try:
response = _request("GET", url, data=None, headers=mas_common_headers)
service_name  = response["trust_preauthtoken"][0]["service_name"]
token = response["trust_preauthtoken"][0]["token"]
api_gateway_url = response["trust_preauthtoken"][0]["api_gateway_url"]
except Exception as e:
logger.debug("Fetching of the Service URL Passed with error. %s" % (str(e)))
raise e

'''
Running the register agent command using the values we retrieved earlier
'''
try:
registeragent_command = "registeragent -serviceurl "+api_gateway_url+" -activationcode "+service_name+"\;"+token
file_run_command = "/var/python/bin/python2.7 /mps/register_agent_cloud.py "+registeragent_command
logger.debug("Executing registeragent command: %s" % (file_run_command))
os.system(file_run_command)
except Exception as e:
logger.debug("Agent Registeration failed with error: %s" % (str(e)))
raise e
<!--NeedCopy--> ```
```

この自動登録スクリプトを指定する場合は、手順 7 と 8 を省略します。

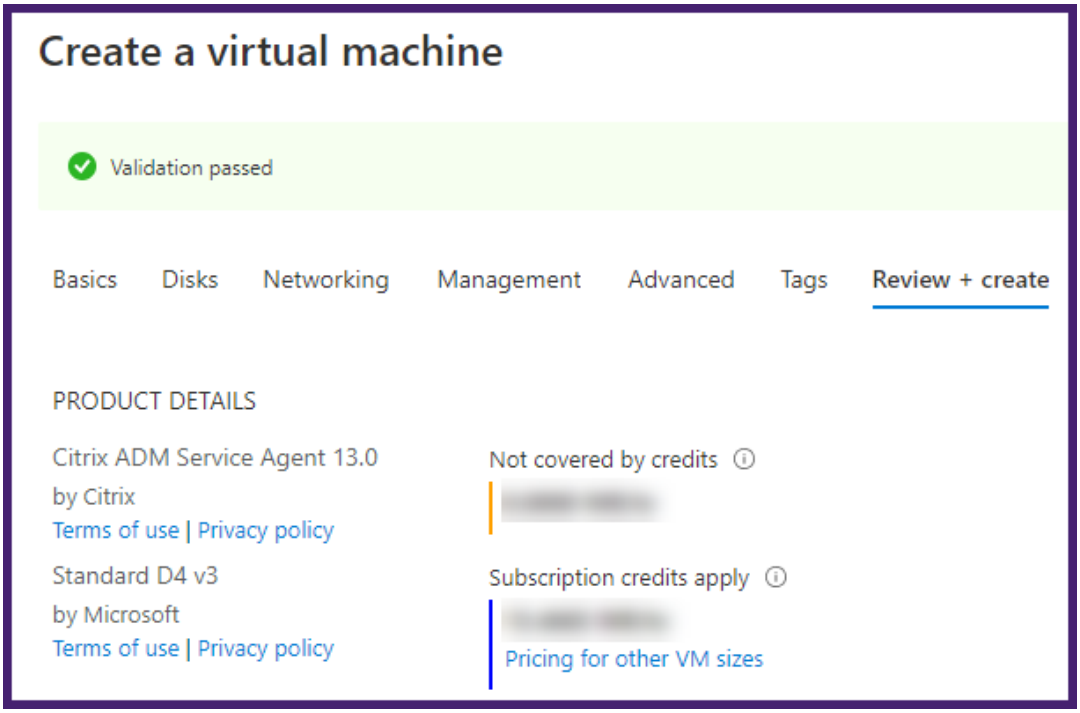
タグ**:**

ADM エージェントタグのキーと値のペアを入力します。タグは、大文字と小文字を区別するキーと値のペアで構成されます。これらのタグを使用すると、エージェントを簡単に整理して識別できます。タグは、Azure と Citrix ADM の両方に適用されます。

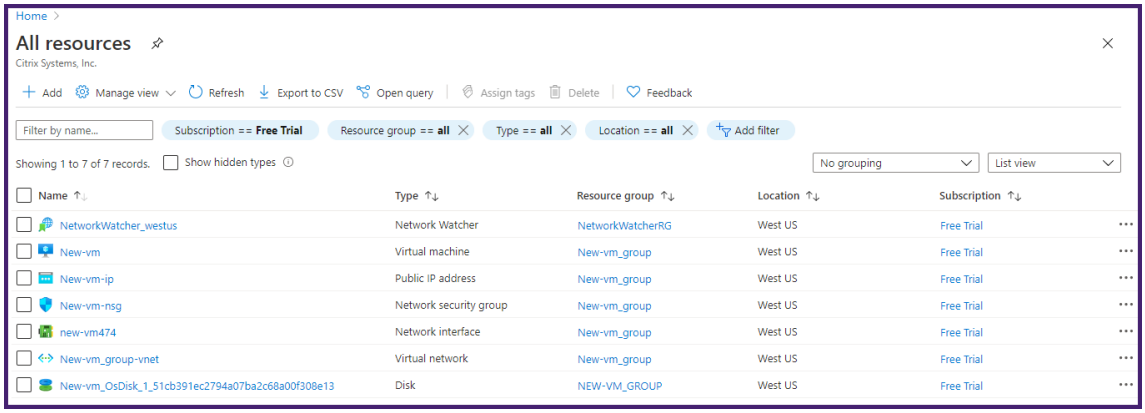


構成設定が検証され、[レビューと作成] タブに検証の結果が表示されます。

- 検証が失敗した場合、このタブに失敗した理由が表示されます。個別のセクションに戻り、必要に応じて変更します。
- 検証に合格した場合は、[作成] をクリックします。エージェントの展開プロセスが開始されます。



展開プロセスには約 10 ～15 分かかる場合があります。展開が正常に完了すると、Microsoft Azure アカウントで Citrix ADM エージェント仮想マシンを表示できます。



6. エージェントが起動して実行されたら、SSH クライアントを使用して、パブリック **IP** アドレスを使用して **Citrix**ADM エージェントにログオンします。

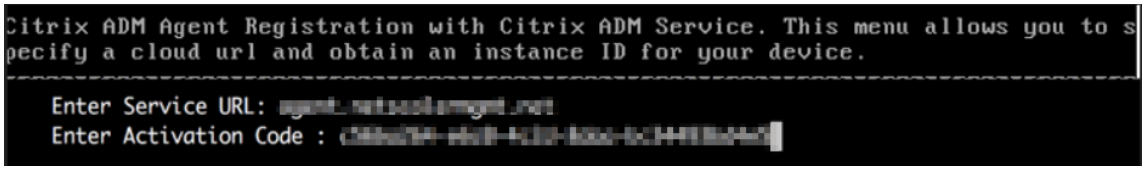
   注

   ```
   1   - ユーザー名として指定した場合は `nsrecover`、デフォルトの Citrix ADMエージェント資格情報（**nsrecover/nsroot**）を使用して仮想マシンにログオンします。
   ```

   - 最初のログオン後にデフォルトのパスワードを変更することをお勧めします。パスワードを変更するには、シェルで **passwd nsroot** と入力します。

7. 次のコマンドを入力して、展開画面を起動します。**deployment_type.py**

8. はじめにの説明に従って、Citrix ADM の［エージェントの設定］ページからコピーして保存した サービス **URL** と アクティベーションコードを入力します。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。



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 ADM にアクセスし、［エージェントの設定］ページの［検出されたエージェント］で、エージェントの状態を確認します。

Amazon Web Services（AWS）に Citrix ADM エージェントをインストールする

May 7, 2021

Citrix Application Delivery Management（Citrix ADM）エージェントは、Citrix ADM とデータセンターまたはクラウドで検出されたインスタンスの間の仲介として機能します。

前提条件

Amazon GUI を使用して、Amazon Web Services（AWS）仮想プライベートクラウド（VPC）内で Citrix ADM エージェント AMI を起動するには、次のものが必要です。

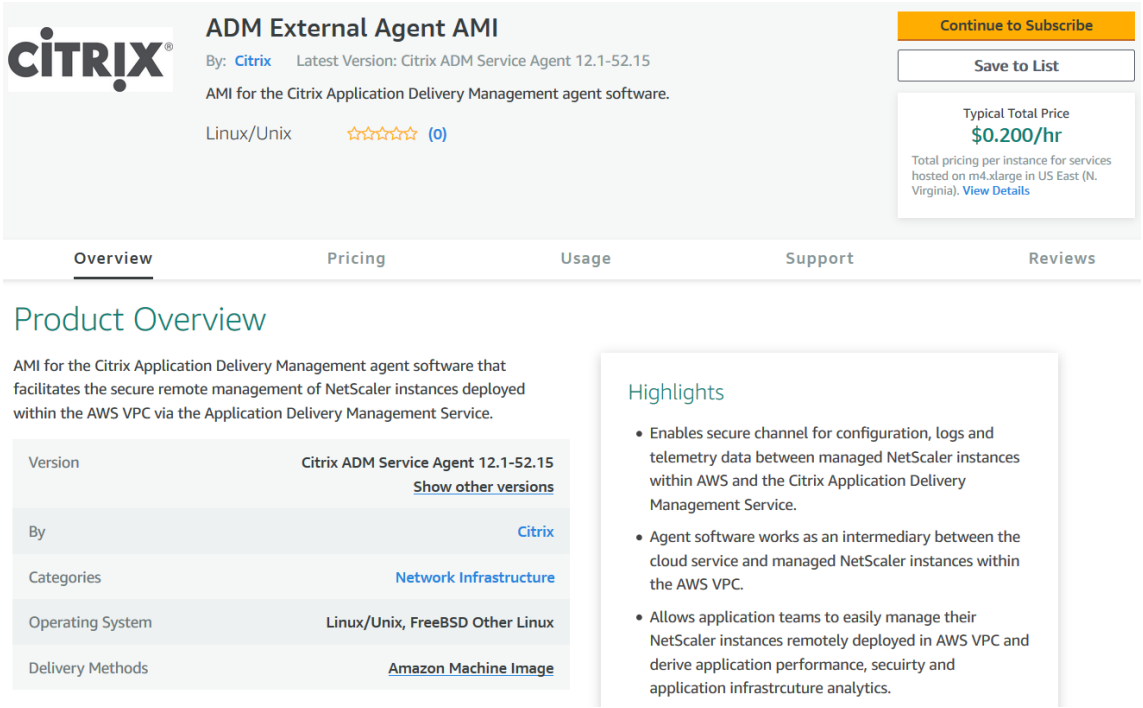
- AWS アカウント
- AWS 仮想プライベートクラウド（VPC）
- IAM アカウント

> 注
>
> - ADM Agent 仮想マシンをプロビジョニングする前に、セキュリティグループ、仮想プライベートネットワーク、キーペア、サブネット、およびその他のエンティティを作成することをお勧めします。したがって、ネットワーク情報は、プロビジョニング中に利用できます。
> - Citrix ADM エージェントが Citrix ADM および Citrix ADC インスタンスと通信するには、推奨ポートが開いていることを確認します。Citrix ADM エージェントのポート要件の詳細については、「ポート」を参照してください。

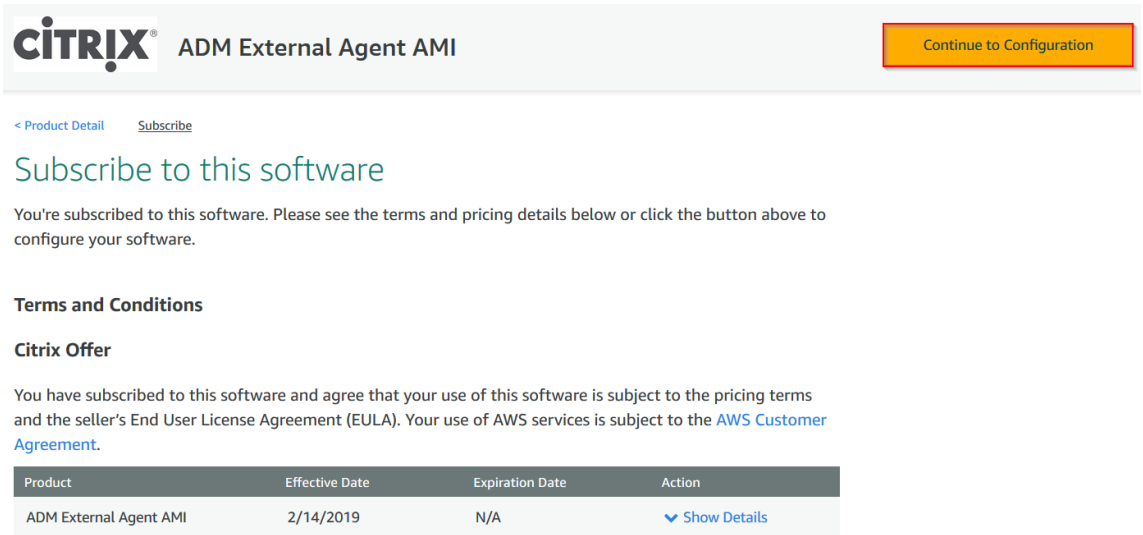
AWS に **Citrix ADM** エージェントをインストールするには**:**

1. AWS 認証情報を使用してAWS マーケットプレイスにログインします。

2. ［検索］フィールドに「**Citrix ADM** エージェント」と入力して Citrix ADM エージェント AMI を検索し、［実行］をクリックします。
3. 検索結果ページで、利用可能なリストから **ADM** 外部エージェント **AMI** をクリックします。
4. [**ADM** 外部エージェント **AMI**] ページで、[続行] **[**サブスクライブ] をクリックします。



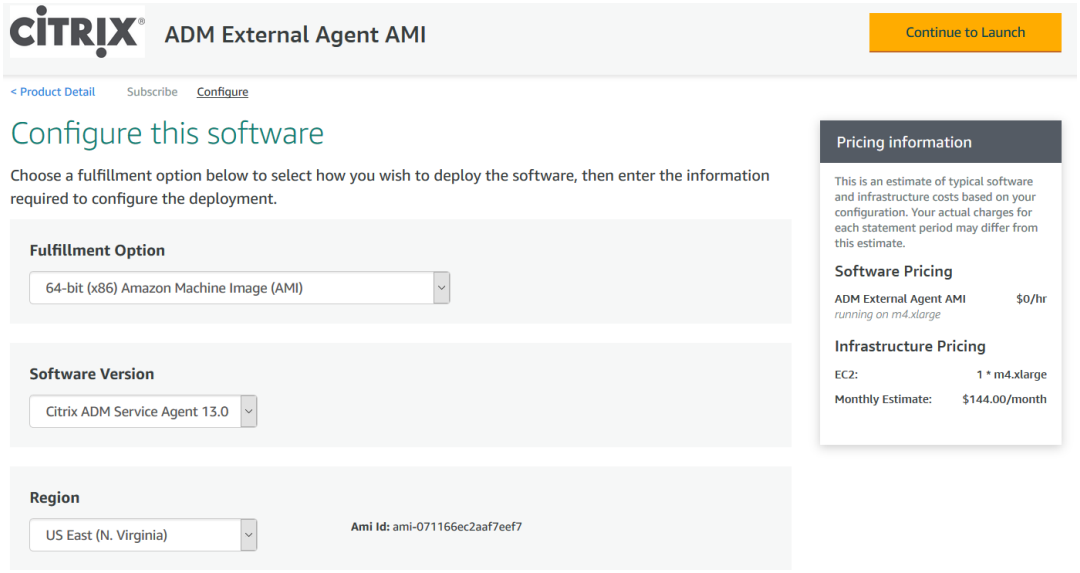
5. サブスクリプションが正常に完了したら、[構成に進む] をクリックします。



6. [このソフトウェアの構成] ページで、次の操作を行います。
   a) フルフィルメントオプションリストから **AMI** を選択します。
   b) ［ソフトウェアバージョン］の一覧から、最新の **Citrix ADM** エージェントバージョンを選択します。

c) [地域] リストから地域を選択します。

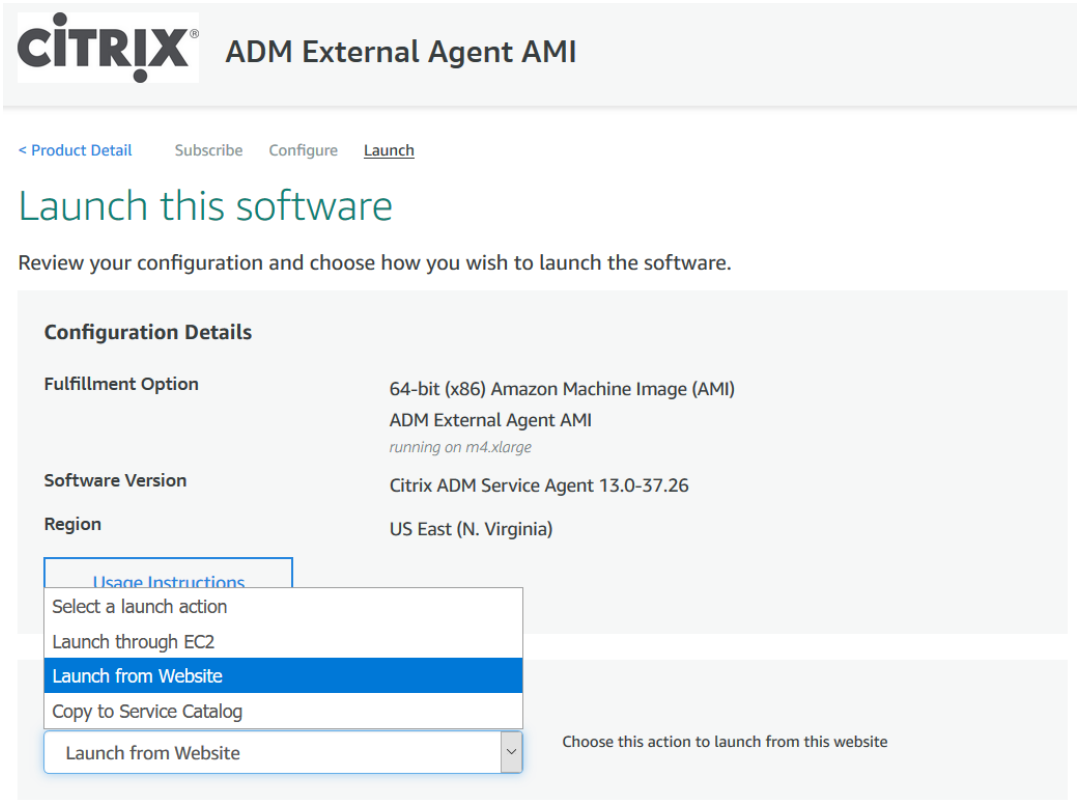
d) [続行] をクリックして起動



7. [このソフトウェアの起動] ページでは、Citrix ADM エージェントを登録する 2 つのオプションがあります。

a) ウェブサイトからの起動

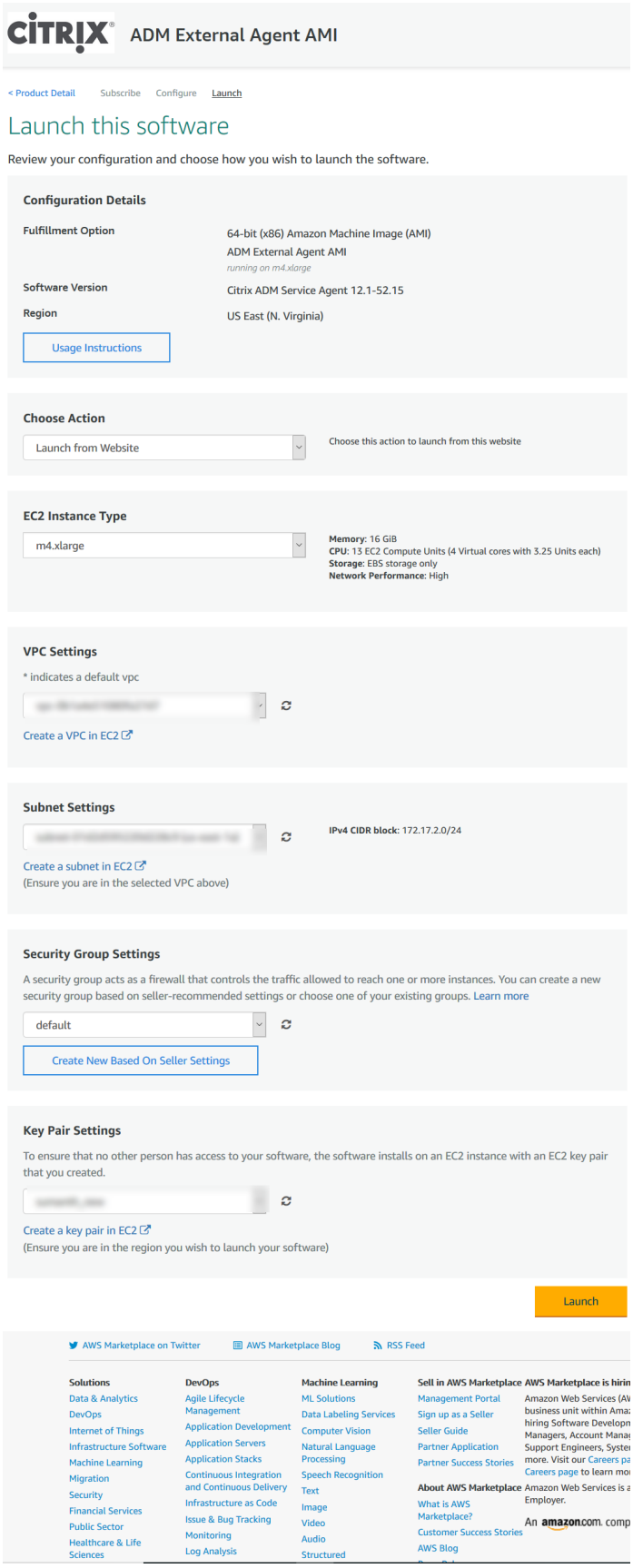
b) **EC2** で起動



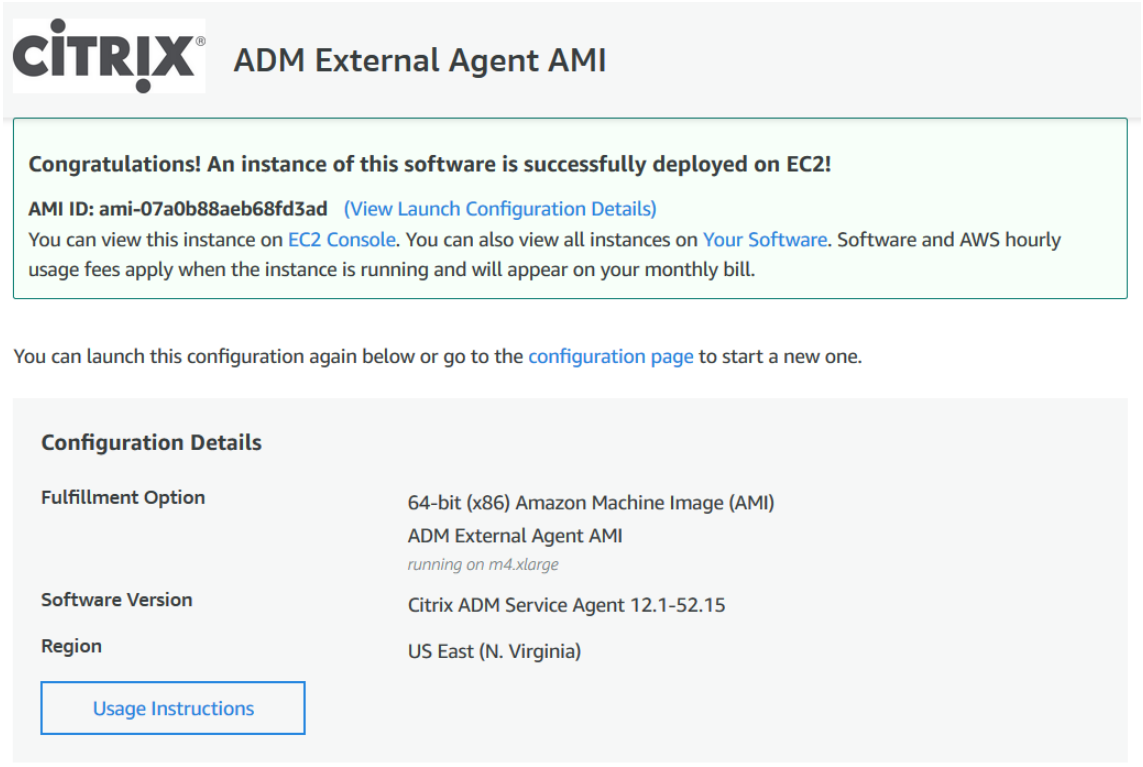
ウェブサイトからの起動

Web サイトから起動するには、次を選択します。

1. EC2 インスタンスタイプリストの **EC2** インスタンスタイプ
2. [VPC 設定**]** リストから **VPC** 。[**EC2** で **VPC** を作成] をクリックして、ソフトウェアの VPC を作成します。
3. **[** サブネット設定**]** リストのサブネット。VPC を選択した後にサブネットを作成するには、**[EC2** にサブネットを作成] をクリックします。
4. [セキュリティグループ設定**]** リストからファイアウォールのセキュリティグループ。出品者設定に基づいて新規作成をクリックし、セキュリティグループを作成します。
5. [Key Pair **Settings]** リストからアクセスセキュリティを確保するためのキーペア。[**EC2** でキーペアを作成する] をクリックして、ソフトウェアのキーペアを作成します。
6. [起動] をクリックします



7. ウェブサイトからの起動は成功しました。



> 注
>
> 展開プロセスには約 10 ～15 分かかる場合があります。デプロイが正常に完了すると、AWS アカウントの Citrix ADM エージェント仮想マシンを表示できます。

8. エージェントを展開したら、Citrix ADM エージェントの名前を割り当てます。
9. エージェントが起動して実行されたら、Citrix ADM エージェントに Elastic IP アドレスを割り当てます。

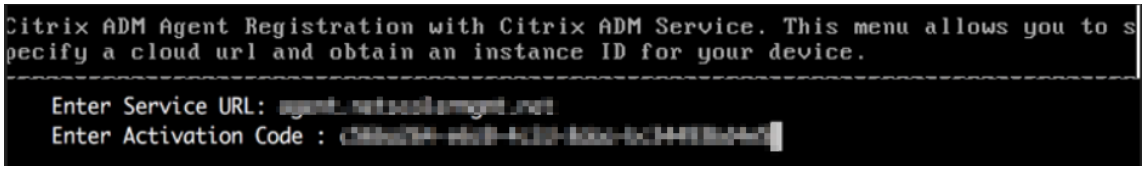
> 注
>
> Elastic IP アドレスを使用すると、Citrix ADM エージェントが Citrix ADM と通信できるようになります。ただし、トラフィックをインターネットにルーティングするように NAT ゲートウェイを設定している場合は、Elastic IP アドレスは必要ありません。

10. SSH クライアントを使用して、パブリック IP アドレスを使用して Citrix ADM エージェントにログオンします。

> 注:
>
> 次のいずれかの方法で、Citrix ADM エージェントにログオンできます。
>
> - ユーザー名として`nsrecover`を使用し、パスワードとして AWS インスタンス ID を使用します。
> - `nsroot`をユーザー名として、有効なキーペアをパスワードとして使用します。

11. 次のコマンドを入力して、展開画面を起動します。**deployment_type.py**

12. はじめにの説明に従って、Citrix ADM の［エージェントの設定］ページからコピーして保存した サービス **URL** と アクティベーションコードを入力します。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。



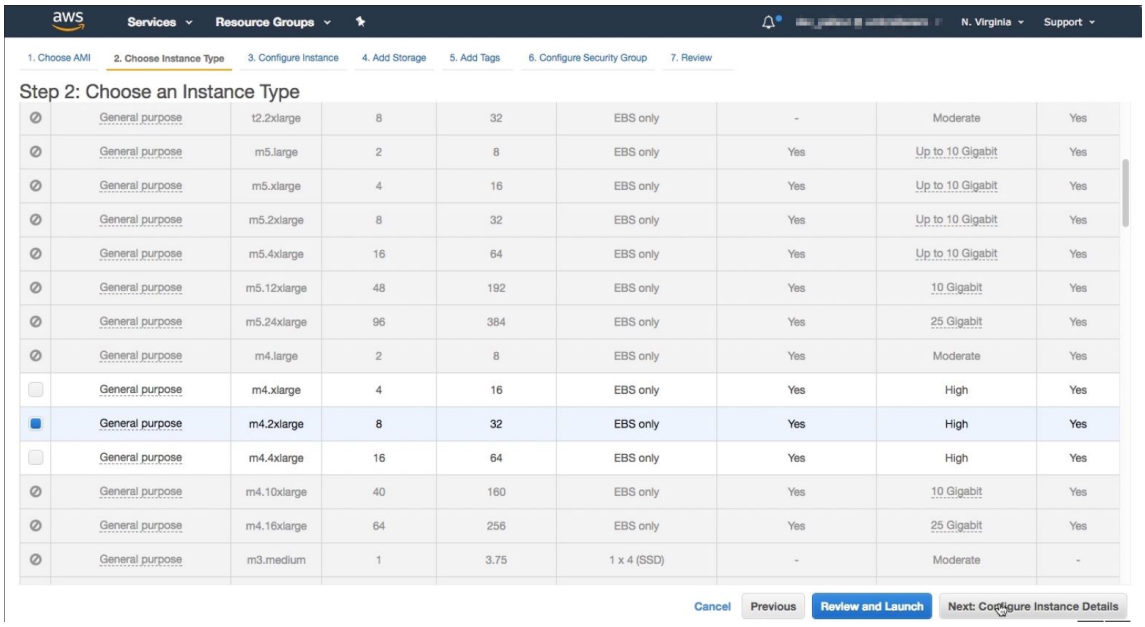
エージェントの登録に成功すると、エージェントは再起動してインストールプロセスを完了します。

エージェントが再起動したら、Citrix ADM にアクセスし、［エージェントの設定］ページの［検出されたエージェント］で、エージェントの状態を確認します。

EC2 で起動

EC2 で起動するには、**[** アクションの選択**]** リストから **[EC2** 経由で起動**]** を選択し、**[Launch]** をクリックします。

1. **[** インスタンスタイプの選択] ページで、インスタンスを選択し、[次へ**:** インスタンスの詳細の設定] をクリックします。



2. [インスタンスの詳細の設定] ページで、必要なパラメータを指定します。

   [詳細情報] セクションで、[**User data**] フィールドに認証の詳細またはスクリプトを指定して、ゼロタッチエージェントを有効にできます。

   - 認証の詳細 -の説明に従って、はじめにで Citrix ADM の［エージェントの設定］ページからコピーしたサービス **URL** とアクティベーションコードを指定します。次の形式で詳細を入力します。


```
registeragent -serviceurl <apigatewayurl> -activationcode <
    activationcodevalue>
<!--NeedCopy-->
```

エージェントはこの情報を使用して、起動時に ADM サービスに自動登録します。

- スクリプト: ユーザーデータとしてエージェント自動登録スクリプトを指定します。スクリプトの例を次に示します。

```
#!/var/python/bin/python2.7
import os
import requests
import json
import time
import re
import logging
import logging.handlers
import boto3

'''
Overview of the Script:
The script helps to register an ADM agent with ADM. Pass it
    in userdata to make ADM agent in AWS to autoregister on
    bootup. The workflow is as follows
1)  Fetch the ADM service API credentials (ID and secret)
    from AWS secret store (NOTE: you have to assign IAM role
    to the ADM Agent that will give permission to fetch
    secrets from AWS secret store)
2)  Login to ADM service with credentials fetched in step 1
3)  Call ADM service to fetch credentials (serviceURL and
    token) for agent registration
4)  Calls registration by using the credentials fetched in
    step 3
'''

'''
These are the placeholders which you need to replace
    according to your setup configurations
aws_secret_id: Id of the AWS secret where you have stored ADM
     Credentials
The secrets value should be in the following json format
{
 "adm_user_id_key": "YOUR_ID", " adm_user_secret_key": "
     YOUR_SECRET" }

```



```
'''

aws_secret_id = "<AWS_secret_id>"
adm_ip_or_hostname = "<YOUR_ADM_POP>.adm.cloud.com"

'''
Set up a specific logger with your desired output level and
   log file name
'''
log_file_name_local = os.path.basename(\_\_file\_\_)
LOG_FILENAME = '/var/log/' + 'bootstrap' + '.log'
LOG_MAX_BYTE = 50\*1024\*1024
LOG_BACKUP_COUNT = 20

logger = logging.getLogger(\_\_name\_\_)
logger.setLevel(logging.DEBUG)
logger_handler = logging.handlers.RotatingFileHandler(
   LOG_FILENAME, maxBytes=LOG_MAX_BYTE, backupCount=
   LOG_BACKUP_COUNT)
logger_fortmater = logging.Formatter(fmt='%(asctime)-2s:%(
   funcName)30s:%(lineno)4d: [%(levelname)s] %(message)s',
   datefmt="%Y-%m-%d %H:%M:%S")
logger_handler.setFormatter(logger_fortmater)
logger.addHandler(logger_handler)

class APIHandlerException(Exception):
    def \_\_init\_\_(self, error_code, message):
        self.error_code = error_code
        self.message = message

    def \_\_str\_\_(self):
        return self.message + ". Error code '" + str(self.
           error_code) + "'"

def parse_response(response, url, print_response=True):
    if not response.ok:
        if "reboot" in url:
            logger.debug('No response for url: reboot')
            resp = {
"errorcode": "500", "message": "Error while reading response.
   " }

            return resp

        if print_response:
```



```
65              logger.debug('Response text for %s is %s' % (url,
                    response.text))
66
67          response = json.loads(response.text)
68          logger.debug("ErrorCode - " + str(response['errorcode
                '']) + ". Message -" + str(response['message']))
69          raise APIHandlerException(response['errorcode'], str(
                response['message']))
70      elif response.text:
71          if print_response:
72              logger.debug('Response text for %s is %s' % (url,
                    response.text))
73
74          result = json.loads(response.text)
75          if 'errorcode' in result and result['errorcode'] > 0:
76              raise APIHandlerException(result['errorcode'],
                    str(result['message']))
77          return result
78
79  def _request(method, url, data=None, headers=None, retry=3,
        print_response=True):
80      try:
81          response = requests.request(method, url, data=data,
                headers=headers)
82          result = parse_response(response, url, print_response
                =print_response)
83          return result
84      except [requests.exceptions.ConnectionError, requests.
            exceptions.ConnectTimeout]:
85          if retry > 0:
86              return _request(method, url, data, headers, retry
                    -1, print_response=print_response)
87          else:
88              raise APIHandlerException(503, 'ConnectionError')
89      except requests.exceptions.RequestException as e:
90          logger.debug(str(e))
91          raise APIHandlerException(500, str(e))
92      except APIHandlerException as e:
93          logger.debug("URL: %s, Error: %s, Message: %s" % (url
                , e.error_code, e.message))
94          raise e
95      except Exception as e:
96          raise APIHandlerException(500, str(e))
97
98  try:
```



```
99        '''Get the AWS Region'''
100       client = boto3.client('s3')
101       my_region = client.meta.region_name
102       logger.debug("The rgion is %s" % (my_region))
103
104       '''Creating a Boto cleint session'''
105       session = boto3.session.Session()
106       client = session.client(
107           service_name='secretsmanager',
108           region_name=my_region
109       )
110
111       '''Getting the values stored in the secret with id: <
              aws_secret_id>'''
112       get_id_value_response = client.get_secret_value(
113           SecretId = aws_secret_id
114       )
115       adm_user_id = json.loads(get_id_value_response["
              SecretString"])["adm_user_id_key"]
116       adm_user_secret = json.loads(get_id_value_response["
              SecretString"])["adm_user_secret_key"]
117
118   except Exception as e:
119       logger.debug("Fetching of ADM credentials from AWS secret
              failed with error: %s" % (str(e)))
120       raise e
121
122   '''
123   Initializing common ADM API handlers
124   '''
125   mas_common_headers = {
126
127       'Content-Type': "application/json",
128       'Accept-type': "application/json",
129       'Connection': "keep-alive",
130       'isCloud': "true"
131    }
132
133
134   '''
135   API to login to the ADM and fetch the Session ID and Tenant
          ID
136   '''
137   url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/
          config/login"
```



```
payload = 'object={
"login":{
"ID":"' + adm_user_id + '","Secret":"' + adm_user_secret + '"
    }
 }
'
try:
    response = _request("POST", url, data=payload, headers=
       mas_common_headers)
    sessionid = response["login"][0]["sessionid"]
    tenant_id = response["login"][0]["tenant_name"]
except Exception as e:
    logger.debug("Login call to the ADM failed with error: %s
       " % (str(e)))
    raise e

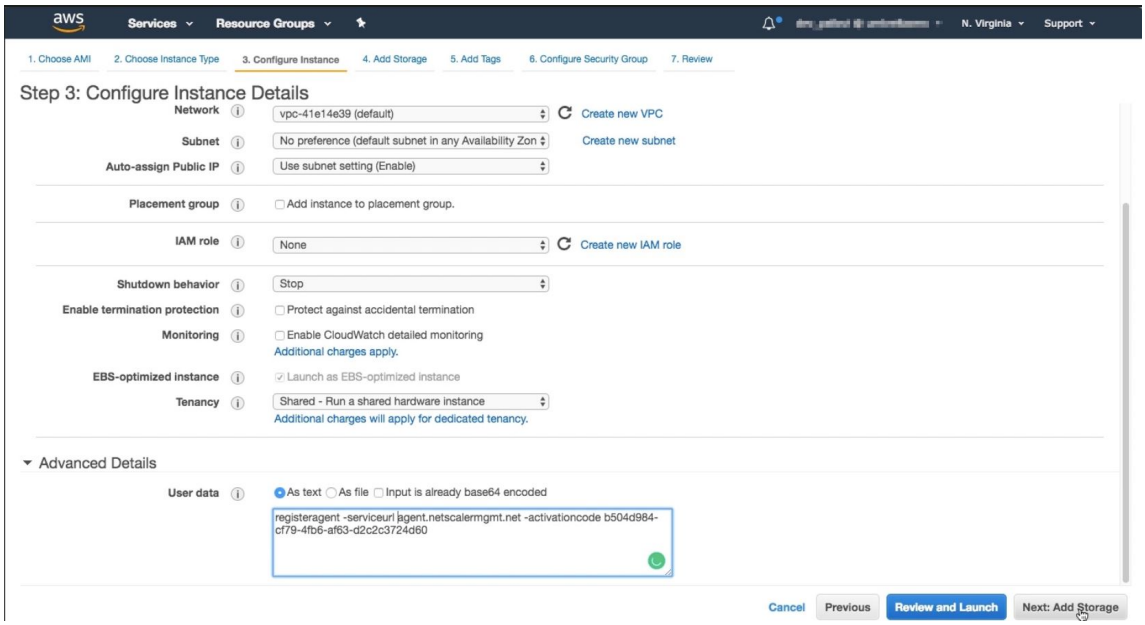
'''
API to fetch the service URL and Token to be used for
   registering the agent with the ADM
'''
mas_common_headers['Cookie'] = 'SESSID=' + str(sessionid)
url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/
   config/trust_preauthtoken/" + tenant_id +"?customer="+
   tenant_id
logger.debug("Fetching Service URL and Token.")
try:
    response = _request("GET", url, data=None, headers=
       mas_common_headers)
    service_name  = response["trust_preauthtoken"][0]["
       service_name"]
    token = response["trust_preauthtoken"][0]["token"]
    api_gateway_url = response["trust_preauthtoken"][0]["
       api_gateway_url"]
except Exception as e:
    logger.debug("Fetching of the Service URL Passed with
       error. %s" % (str(e)))
    raise e

'''
Running the register agent command using the values we
   retrieved earlier
'''
try:
    registeragent_command = "registeragent -serviceurl "+
       api_gateway_url+" -activationcode "+service_name+";"+
```



```
            token
171         file_run_command = "/var/python/bin/python2.7 /mps/
                register_agent_cloud.py "+registeragent_command
172         logger.debug("Executing registeragent command: %s" % (
                file_run_command))
173         os.system(file_run_command)
174     except Exception as e:
175         logger.debug("Agent Registeration failed with error: %s"
                % (str(e)))
176             raise e
177     <!--NeedCopy-->
```

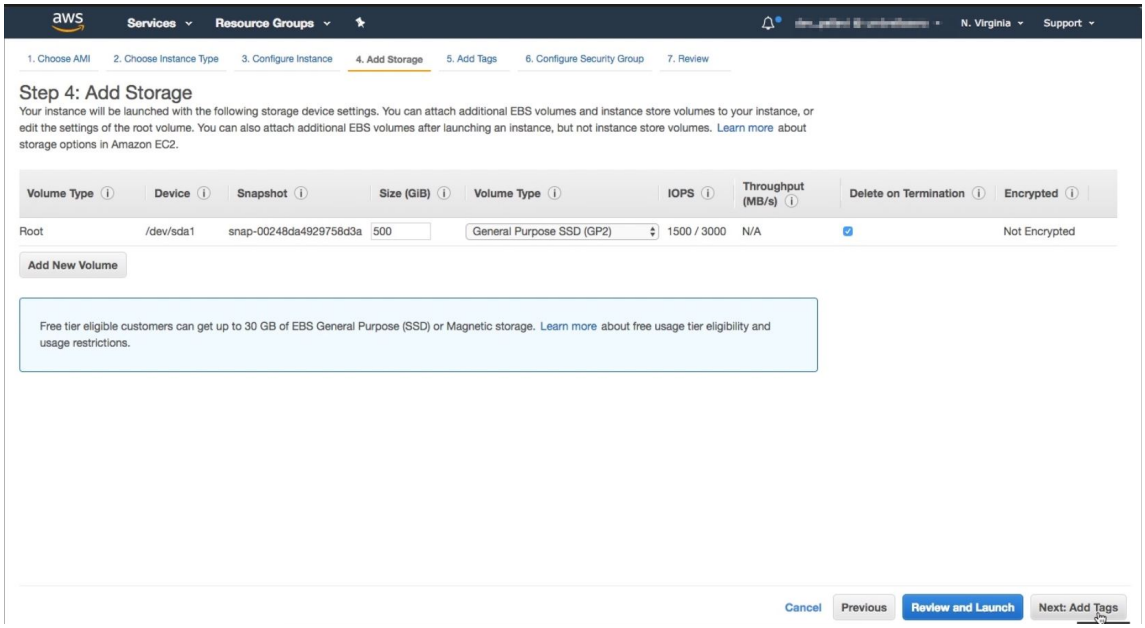
このスクリプトは、AWS シークレットマネージャーから認証の詳細を取得し、deployment.pyスクリプトを実行して、エージェントを ADM サービスに登録します。



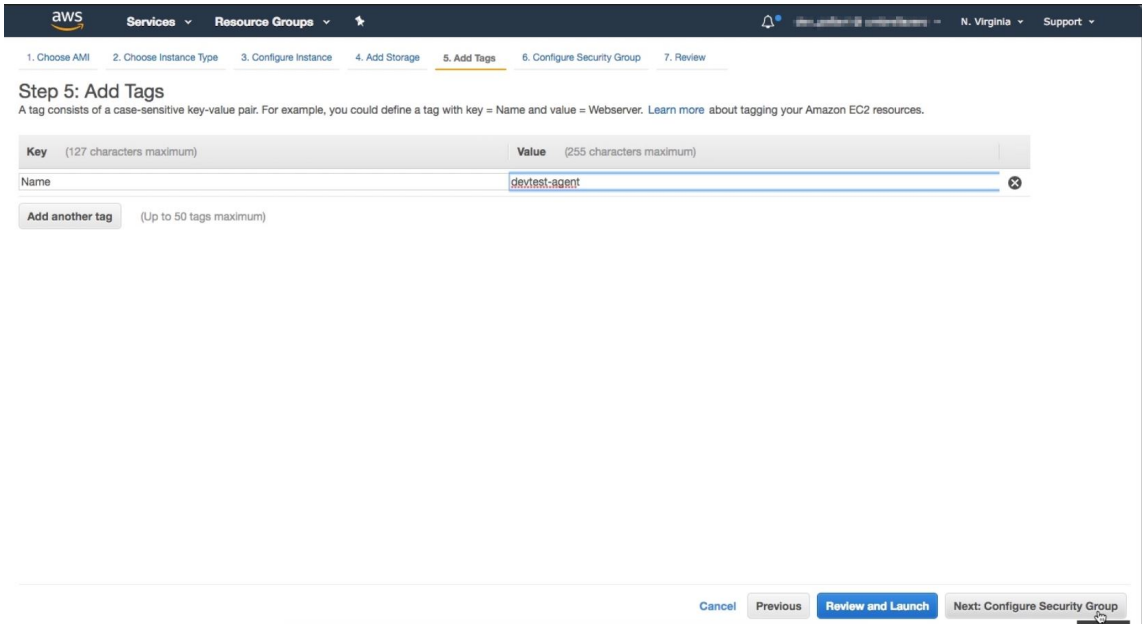
> 注
>
> パブリック IP アドレスを自動割り当てできますが、Elastic IP アドレスを割り当てることもできます。NAT Gateway が設定されていない場合は、Elastic IP アドレスを割り当てる必要があります。
>
> このステップで Elastic IP アドレスが設定されていない場合でも、EC2 コンソールで行うことができます。新しい Elastic IP アドレスを作成し、インスタンス ID または ENI-ID を使用してそれを ADM Agent に関連付けることができます。

[ストレージの追加] をクリックします。

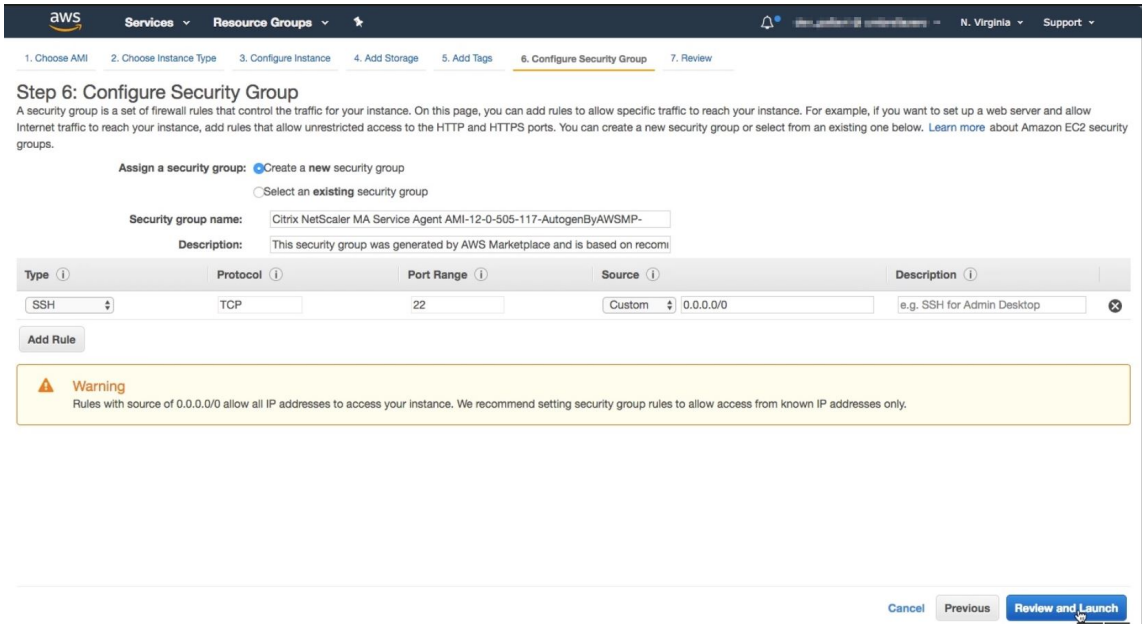
3. [**Add Storage**] ページで、インスタンスのストレージデバイス設定を構成し、[次へ**:Add Tags**] をクリックします。



4. [**Add Tags**] ページで、インスタンスのタグを定義し、[次へ**:** セキュリティグループの設定] をクリックします。

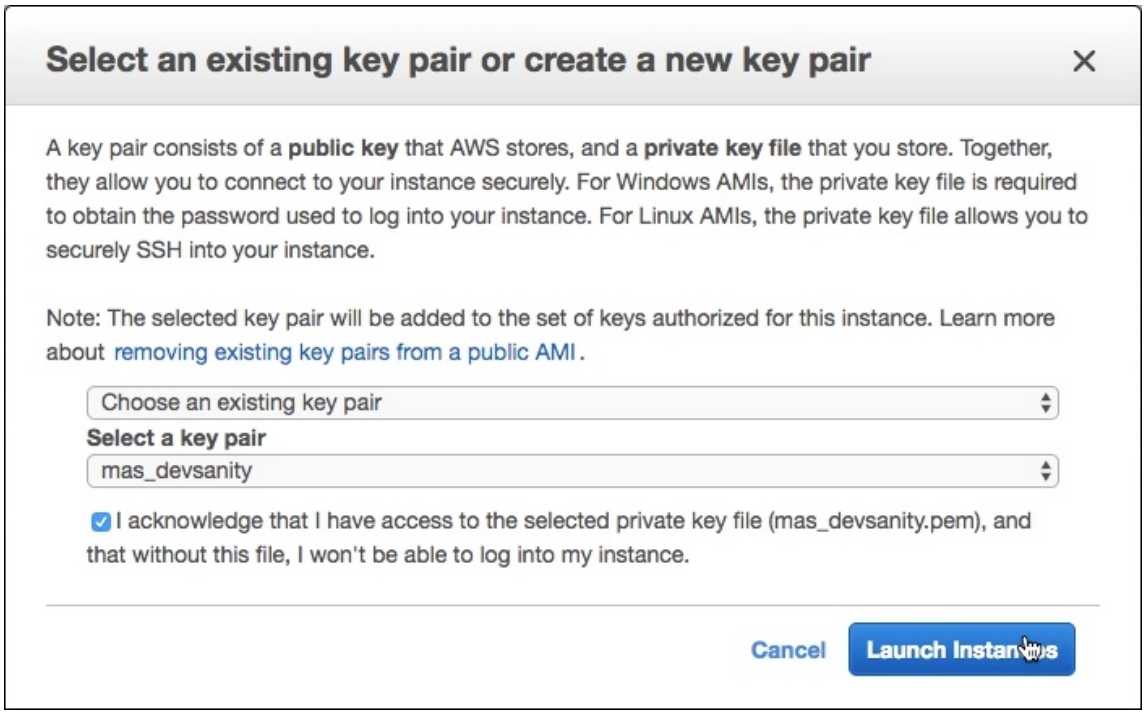


5. [**Configure Security Group**] ページで、インスタンスへの特定のトラフィックを許可するルールを追加し、[**Review and Launch**] をクリックします。



6. [**Review Instance Launch**] ページで、インスタンスの設定を確認し、[**Launch**] をクリックします。
7. **[** 既存のキーペアの選択または新しいキーペアの作成] ダイアログボックスで、キーペアを作成します。既存のキーペアから選択することもできます。

   確認を受け入れ、[**Launch Instances**] をクリックします。



展開プロセスには約 10 ～15 分かかる場合があります。デプロイが正常に完了すると、AWS アカウントの Citrix ADM エージェント仮想マシンを表示できます。

GCP に Citrix ADM エージェントをインストールする

May 7, 2021

Citrix Application Delivery Management（Citrix ADM）エージェントは、Citrix ADM とデータセンターまたはクラウドで検出されたインスタンスの間の仲介として機能します。エージェントを Google Cloud Platform（GCP）にデプロイすると、Citrix ADM を介して Google クラウド仮想ネットワーク内にデプロイされた Citrix ADC インスタンスの安全なリモート管理が容易になります。GCP の ADM エージェントが IT 管理者に提供する方法の詳細については、ブログCitrix ADM エージェントが Google Cloud Platform マーケットプレイスで利用できるようになりましたを参照してください。

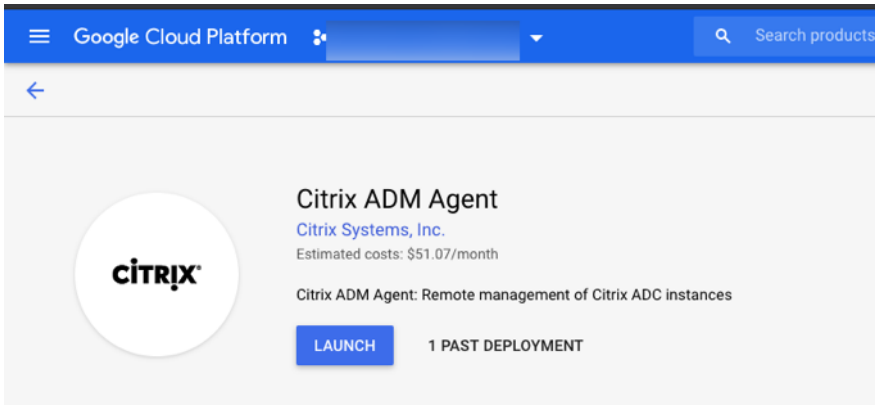
前提条件

GCP に ADM エージェントをインストールするには、GCP アカウントが必要です。

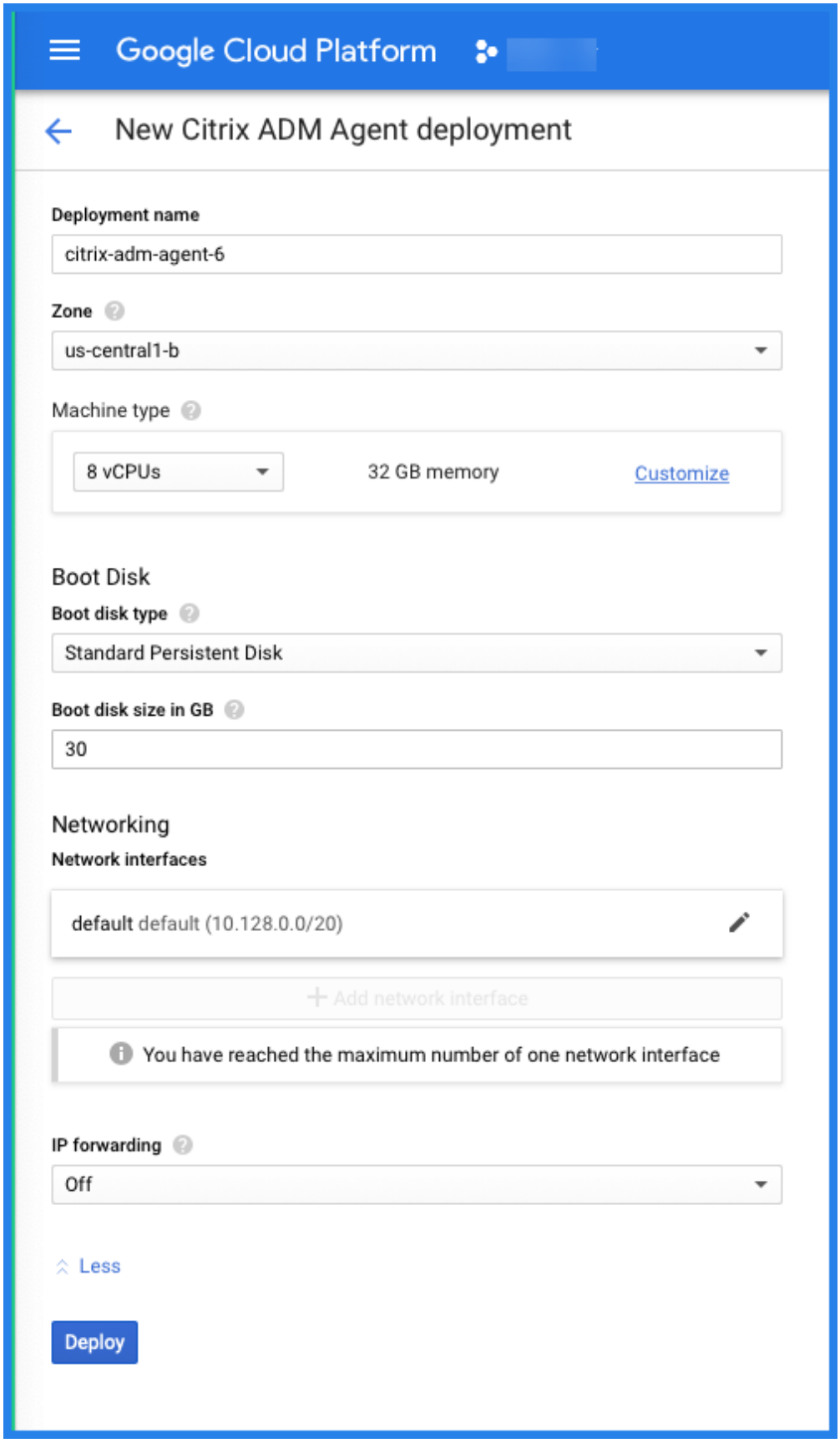
GCP に Citrix ADM エージェントをインストールする

GCP に ADM エージェントをインストールする手順は、次のとおりです。

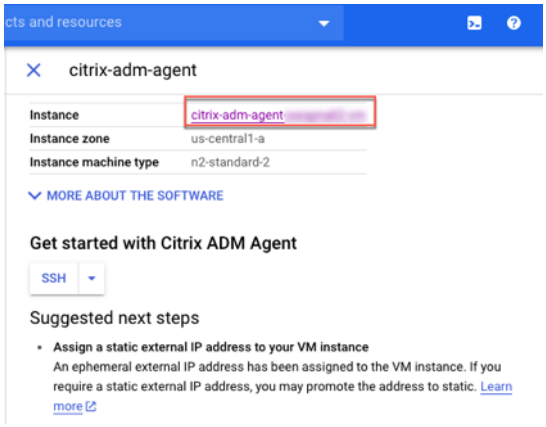
1. 認証情報を使用して GCP コンソール (console.cloud.google.com) にログオンし、マーケットプレイスに移動します。
2. 検索フィールドに「**Citrix ADM** エージェント」と入力します。
3. 結果フィールドから ［**Citrix ADM Agen**］をクリックし、［起動］をクリックします。



4. ［新しい **Citrix ADM** エージェント展開］ページでは、ほとんどのオプションがデフォルトで設定されます。必要に応じてデフォルト設定を変更し、[**Deploy**] をクリックします。



5. エージェントがデプロイされたら、インスタンスリンクをクリックし、仮想マシンインスタンスの詳細ページで詳細を確認します。

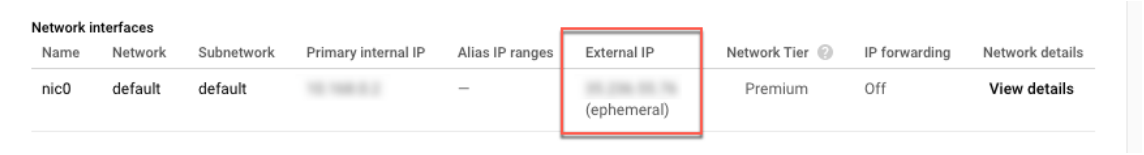


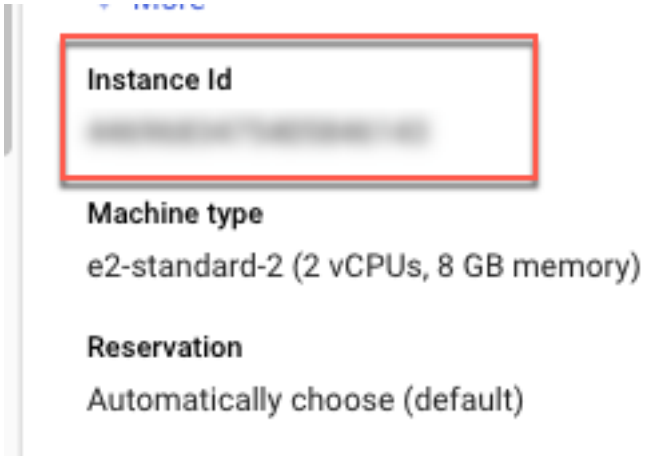
6. エージェントの外部 IP アドレスを使用して SSH クライアント経由でエージェントにログインします。次のコマンドを使用します。

```
ssh nsrecover@<external IP address of the agent>
```

パスワード: インスタンス ID

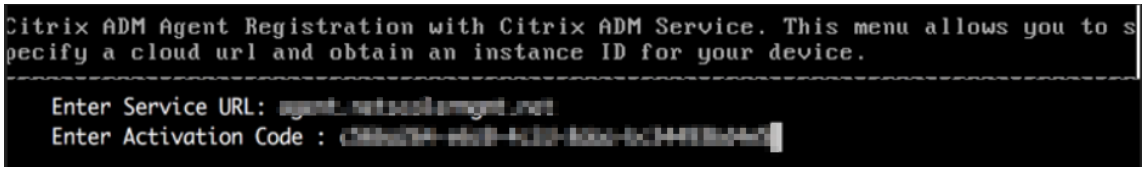
VM インスタンスの詳細ページで、外部 IP アドレスとインスタンス ID を確認できるか。





7. 次のコマンドを入力して、展開画面を起動します。**deployment_type.py**

8. はじめにの説明に従って、Citrix ADM の［エージェントの設定］ページからコピーして保存した サービス **URL** と アクティベーションコードを入力します。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。



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 ADM にアクセスし、［エージェントの設定］ページの［検出されたエージェント］で、エージェントの状態を確認します。

Kubernetes クラスタに Citrix ADM エージェントをインストールする

May 7, 2021

> 注
>
> エージェントをマイクロサービスとしてインストールする手順については、はじめにを参照してください。

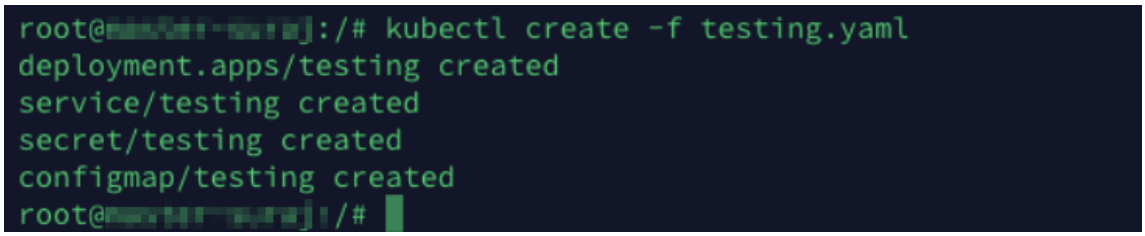
Kubernetes マスターノードで以下を実行します。

1. ダウンロードした YAML ファイルを保存します
2. 次のコマンドを実行します。

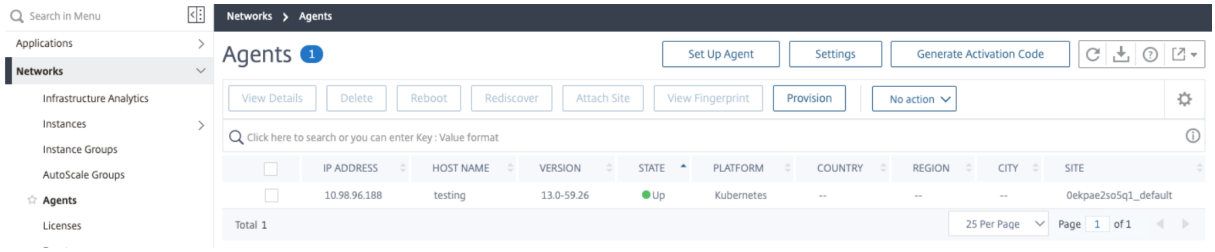
   ```
   kubectl create -f <yaml file>
   ```

   例: `kubectl create -f testing.yaml`

   エージェントが正常に作成されました。



Citrix ADM で、［ネットワーク］>［エージェント］の順に選択し、エージェントの状態を確認します。



ヘルプとサポートの利用

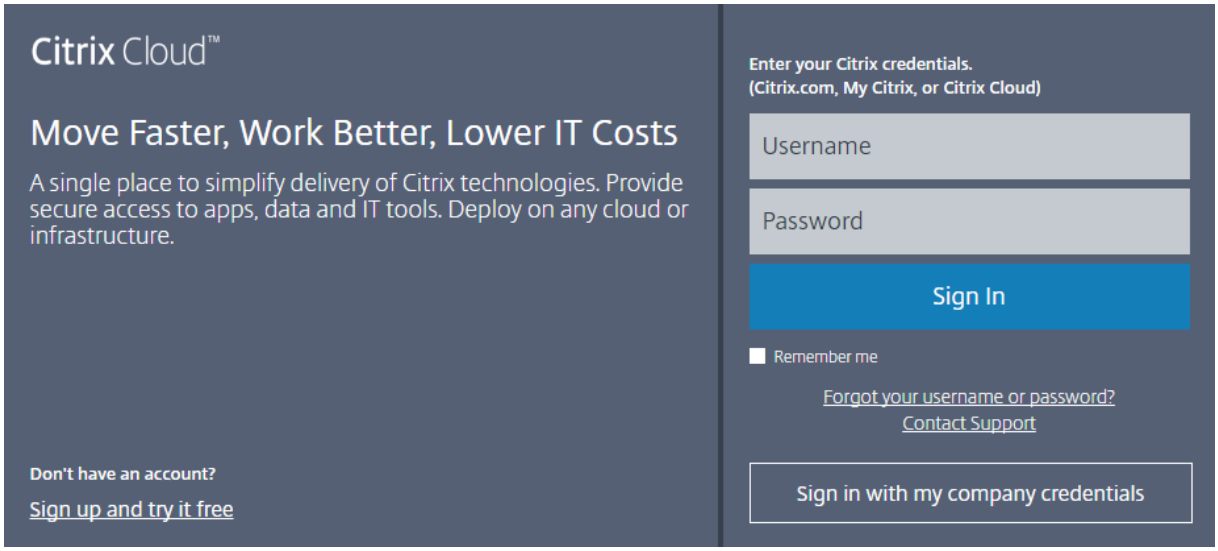
May 7, 2021

Citrix Cloud ユーザーとして, 時には、あなたは私たちのインフラストラクチャの円滑な機能を確認するための助けが必要な場合があります. このトピックでは、さまざまなヘルプとサポートオプションの詳細と、それらへのアクセス方法について説明します。

Citrix Cloud アカウントを作成する

Citrix Cloud アカウントへの登録でエラーが発生した場合、シトリックスカスタマーサービスにお問い合わせください。

アカウントにログイン



Citrix Cloud アカウントへのログインに問題がある場合は、次の手順を実行します:

- アカウントに登録した時に指定したメールアドレスおよびパスワードでログインしているかを確認してください。
- 次の場合、Citrix Cloud では、サインイン前にパスワードのリセットを求めるプロンプトが自動的に表示されます。
  - Citrix Cloud にしばらくサインインしていない
  - パスワードが Citrix Cloud の要件を満たしていません
- 詳しくは、この記事の「パスワードを変更する」を参照してください。
- 会社から Citrix アカウントではなく会社の資格情報を使用した Citrix Cloud へのサインインが許可されている場合は、［会社の資格情報でサインイン］をクリックし、会社のサインイン URL を入力します。次に、会社

の資格情報を入力すると、会社の Citrix Cloud アカウントにアクセスできます。会社のログイン URL がわからない場合、会社の管理者に問い合わせてください。

パスワードを変更する

Citrix Cloud アカウントのパスワードを忘れた場合は、[ユーザー名またはパスワードをお忘れですか?] をクリックします。にアクセスして、アカウントのメールアドレスを入力できます。パスワードをリセットするためのメールが届きます。パスワードリセットメールが届かない場合や、さらにサポートが必要な場合は、シトリックスカスタマーサービスにお問い合わせください。

アカウントのパスワードを常に保護するために、サインイン時に Citrix Cloud からパスワードのリセットを求められる場合があります。このプロンプトは次の場合に表示されます:

- パスワードが Citrix Cloud の複雑さの要件を満たしていません。パスワードは 8 文字以上で、次の要素が含まれている必要があります:
  - 1 つ以上の数字
  - 1 つ以上の大文字
  - 少なくとも 1 つのシンボル: ! @ ## $ % ^ * ? + = -
- パスワードに辞書の単語が含まれています。
- 既知の侵害されたパスワードのデータベースに含まれるパスワードです。
- 過去 6 か月間 Citrix Cloud にサインインしていません。

プロンプトが表示されたら、[パスワードのリセット] を選択してアカウント用の強力なパスワードを作成します。

Citrix Cloud サポートフォーラム

Citrix Cloud サポートフォーラムでは、ヘルプを要求したり、フィードバックや改善案を送信したり、他のユーザーの会話を表示したり、トピックを作成したりできます。

Citrix のサポートスタッフメンバーはこれらのフォーラムを追跡し、質問に回答します。他の Citrix Cloud コミュニティメンバーも、ヘルプを提供したり、ディスカッションに参加したりする場合があります。

フォーラムのトピックを閲覧する場合、ログインする必要はありません。ただし、投稿したり、トピックに返信するためには、ログインが必要です。ログインするには、既存の MyCitrix 資格情報を使用するか、Citrix Cloud アカウントの作成時に指定したメールアドレスおよびパスワードを使用してください。Citrix アカウントを作成するには、アカウントの作成またはリクエストに進みます。

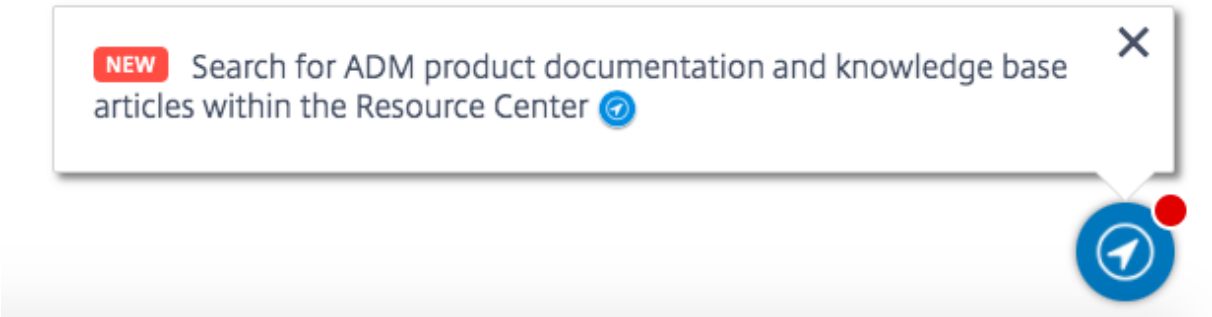
サポート記事とドキュメント

Citrix Cloud を活用し、シトリックス製品で発生する可能性のある問題を解決するための豊富な製品およびサポートコンテンツが用意されています。

Citrix Cloud リソースセンター

Citrix Cloud リソースセンターには、Citrix Cloud サービスの開始、機能の詳細、問題の解決に役立つリソースがいくつかあります。表示されるリソースは、現在操作している Citrix Cloud の機能またはサービスに適用されます。たとえば、Virtual Apps and Desktops サービスの管理コンソールを使用している場合、リソースセンターには次のリソースが表示されます。

Citrix Cloud コンソールの右下にある青いコンパスアイコンをクリックして、いつでもリソースセンターにアクセスできます。



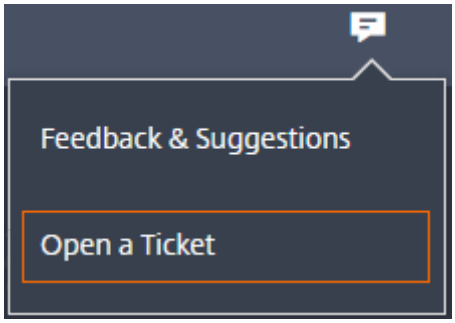
- 開始：現在使用しているサービスに固有の主なタスクについて、簡単なガイド付きのチュートリアルを提供します。また、トレーニングやオンボーディングのリソースへのリンクもあり、サービス機能の詳細を知り、エンドユーザーを成功に導くためのセットアップに役立ちます。
- お知らせ：新しくリリースされた機能の通知と、重要な Citrix コミュニケーションへのリンクを提供します。機能の通知をクリックすると、その機能の簡単なガイド付きウォークスルーが表示されます。
- 記事を検索：一般的なタスクに関する製品ドキュメントと Knowledge Center 記事の一覧を提供し、Citrix Cloud 内から多くの記事を見つけるのに役立ちます。［**How do I...**］ボックスに検索ワードを入れて、使用中のサービスごとに絞り込んだ記事の一覧を表示します。通常、サポート記事が一覧の最初に表示され、その後に製品ドキュメント記事が続きます。

Citrix Tech Zone

Citrix Tech Zoneには、Citrix Cloud およびそのほかのシトリックス製品の詳細を知るために役立つさまざまな情報が含まれています。ここでは、Citrix テクノロジの設計、構築、展開に関する洞察を提供するリファレンスアーキテクチャ、図、ビデオ、テクニカルペーパーを紹介します。

テクニカルサポート

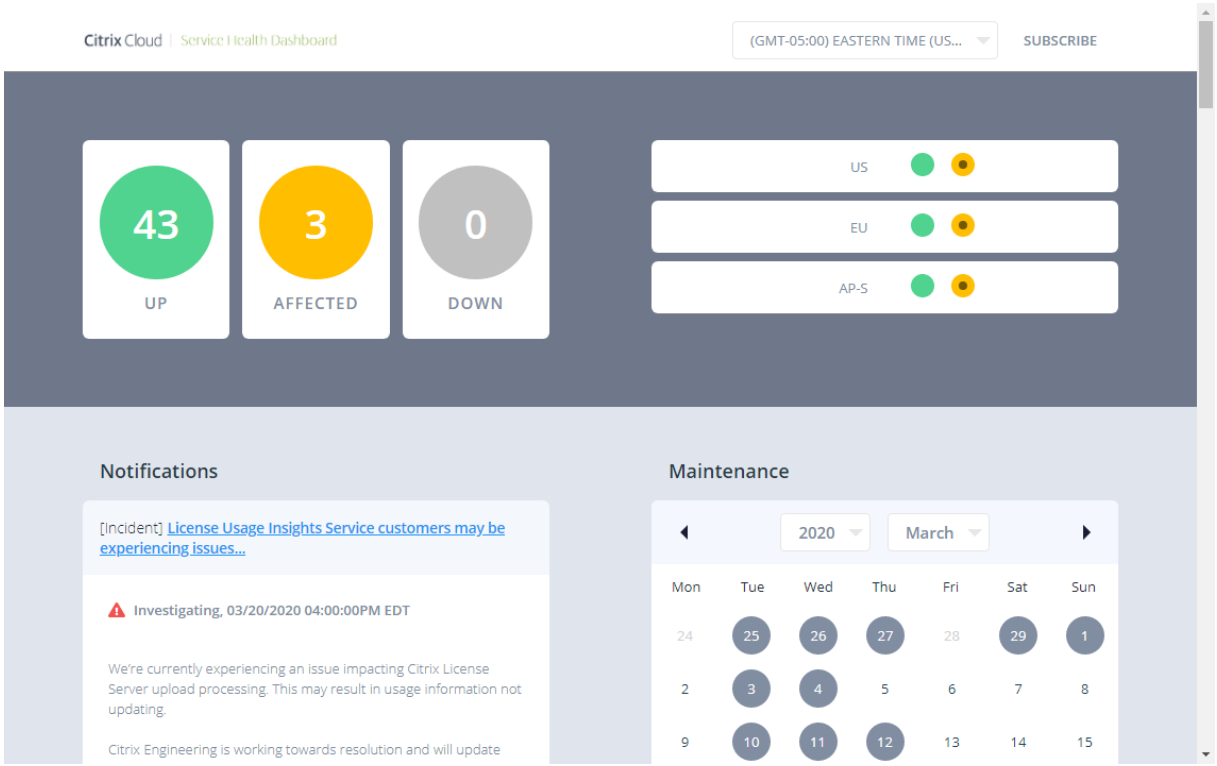
技術的なヘルプが必要な問題が発生した場合、コントロールセンターで ［フィードバックとサポート］アイコンをクリックして ［チケットを開く］を選択してください。



[**My Support** に移動] をクリックして [**My Support**] を選択し、My Support ポータルでチケットを開きます。My Support ポータルでは、既存のチケットを追跡したり、現在の製品使用権を表示することもできます。

Service Health Dashboard

Citrix Cloud サービスの正常性ダッシュボードでは、各地域における Citrix Cloud プラットフォームとサービスのリアルタイム可用性の概要について説明します。Citrix Cloud で問題が発生した場合は、サービス正常性ダッシュボードをチェックして、Citrix Cloud または特定のサービスが正常に動作していることを確認します。

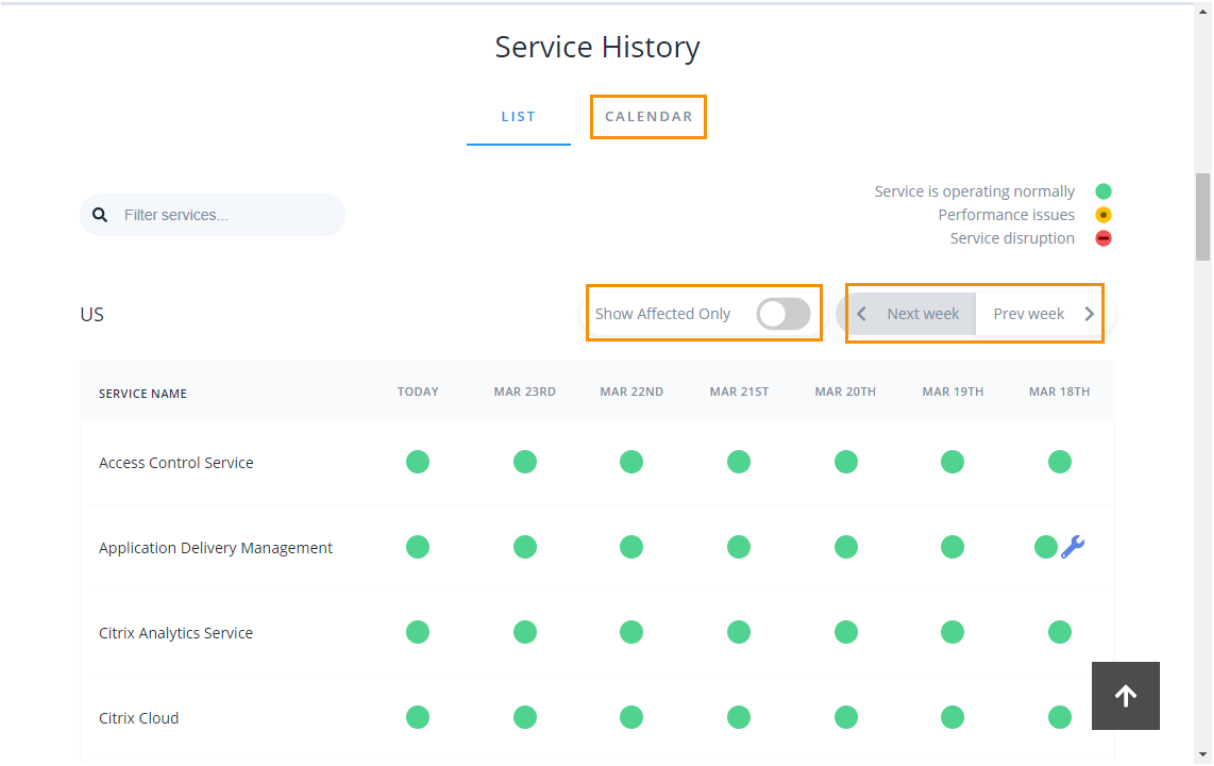


ダッシュボードを使用して、次の条件の詳細を確認します。

- 地域別にグループ化されたすべての Citrix Cloud サービスの現在の可用性ステータス
- 過去 7 日間 (デフォルト) または過去 7 日間の増分における各サービスのサービスヘルス履歴
- 特定のサービスのメンテナンスウィンドウ

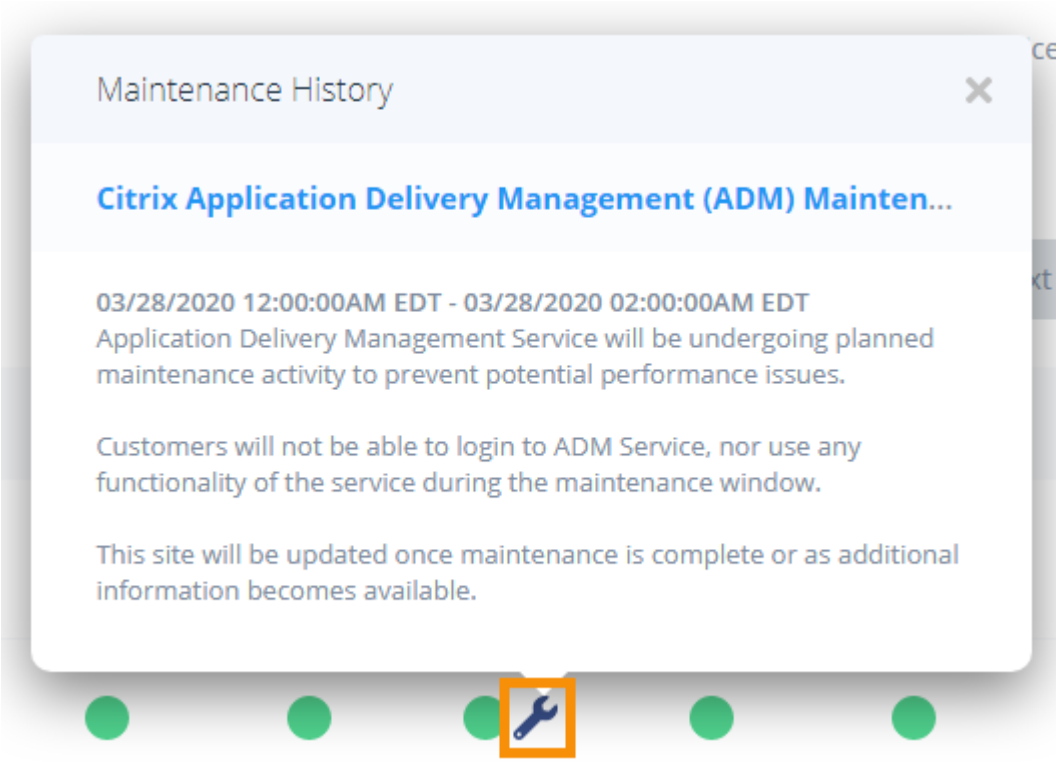
デフォルトでは、サービスの健全性ステータスはリストとして表示されますが、カレンダービューでもステータスを

表示できます。[**Next**] または [**Previous**] を選択して、7 日単位でサービスのヘルス履歴をスクロールします。一覧をフィルタして、影響を受けるサービスのみを表示することもできます。

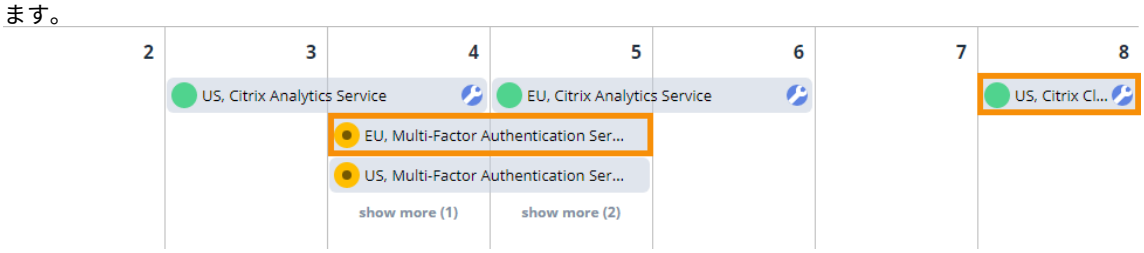


影響を受けるサービスのサービス正常性インシデントに関する詳細情報を表示するには、次の手順に従います。

- リストビューで、サービスインジケータの横にあるアイコンをクリックして、サービス正常性インシデントに関する詳細情報を表示します。

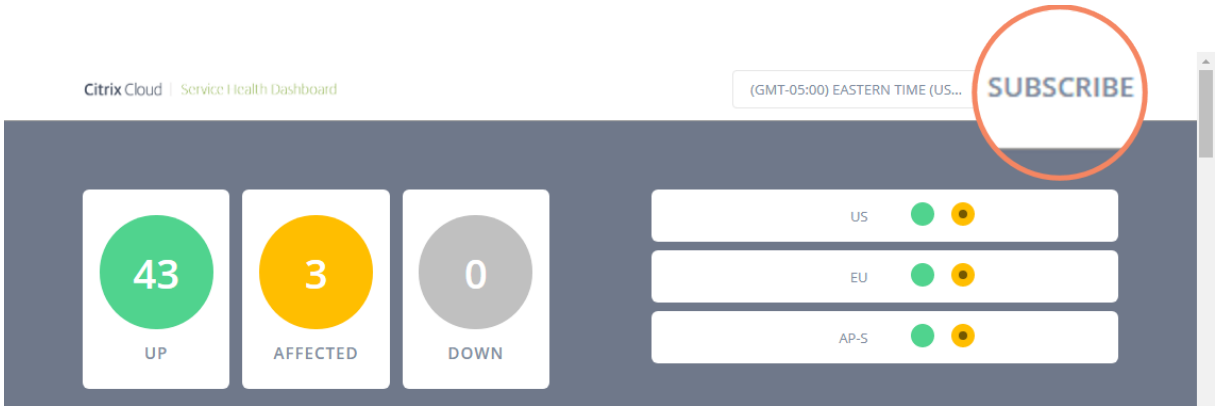


- カレンダービューで、サービスエントリをクリックして、サービス正常性インシデントのステータスを表示します。

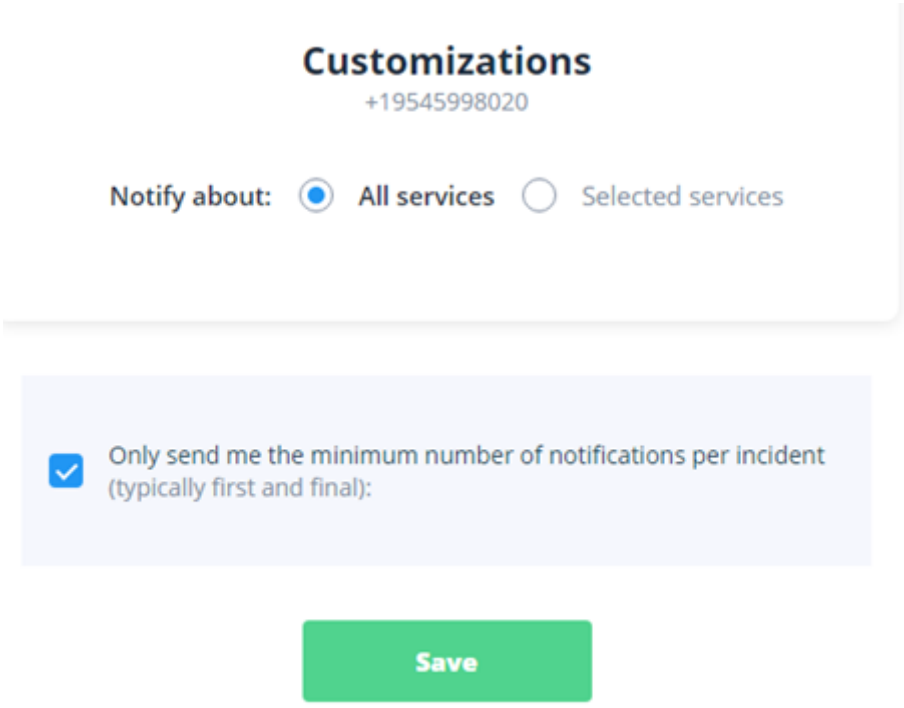


サービス正常性サブスクリプション

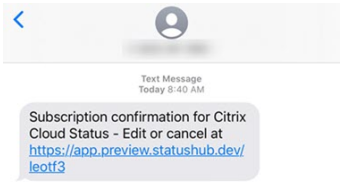
サービスの正常性通知を受信するには、ダッシュボードの右上にある [**Subscribe**] をクリックし、使用する通知方法を選択します。

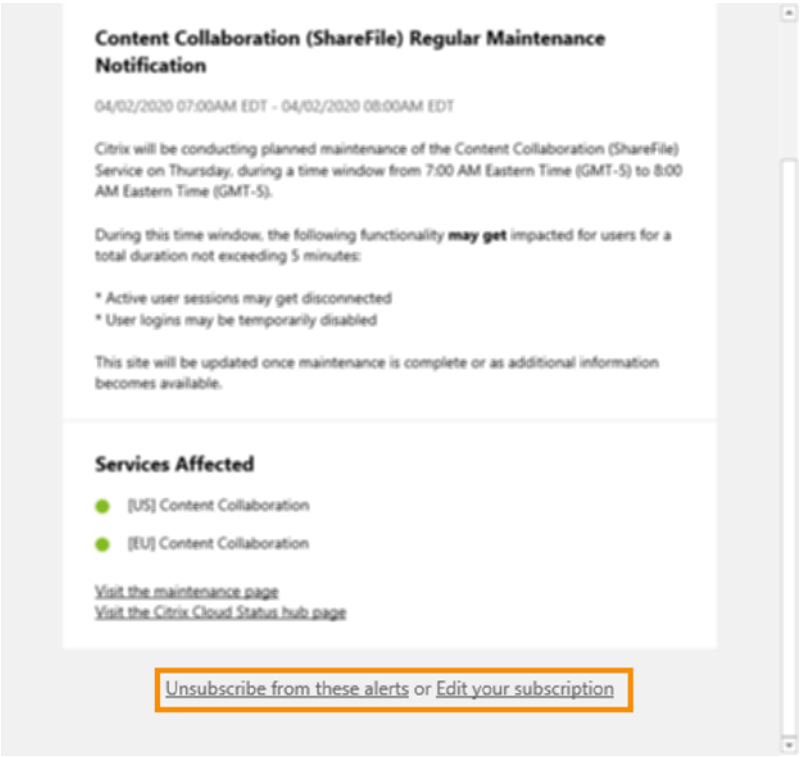


すべてのサービス、または選択したサービスのみの通知をサブスクライブできます。既定では、サービス正常性インシデントに関するすべての通知を受信します。インシデント中の通知の頻度を制限するには、最初と最後の通知のみを受信するように選択できます。



購読方法に応じて、受信するサブスクリプション確認メッセージ（電話通知のサブスクライブなど）または各通知メッセージ（電子メール通知の購読など）には、登録解除および設定の変更へのリンクが含まれます。





購読を停止または変更するには、以下の手順に従ってください。

1. 既存の通知を検索し、通知の設定を解除または変更するためのリンクを選択します。
2. 購読を解除する場合は、[登録解除] を選択し、キャンセルする通知方法を選択します。すべての通知方法からサブスクライブするには、[すべてのサブスクリプションを削除] を選択します。
3. プリファレンスを変更する場合は、通知方法を選択し、サービスと最小インシデント通知に適切な変更を加え、[保存] を選択します。

Citrix ADM サービス接続を使用した **Citrix ADC** インスタンスのロータッチオンボーディング

May 7, 2021

ハイブリッドマルチクラウド（HMC）インフラストラクチャが拡大すると、ADC インスタンスの管理、監視、分析、トラブルシューティングに関する課題は複数になります。インフラストラクチャ全体とその上で実行されているすべてのアプリケーションを可視化できる一元化されたコントローラが、時間の必要性になります。

今日の世界では、インスタンスをセントラルコントローラにオンボーディングすることは、迅速、簡単、かつ低タッチな方法で行う必要があります。このニーズを念頭に置いて、Citrix ADM サービスは新しいオンボーディングワークフローを開始します。これにより、HMC の展開を完全に可視化するための迅速な方法が提供されます。

概要:ADM サービスのオンボーディングワークフローのコンポーネント

このワークフローの構成要素は、ADC 側の 2 つのコンポーネント（ADC サービス接続と Call Home）です。

- **ADM** サービス接続：これは、Citrix ADC インスタンスの Citrix ADM サービスへのシームレスなオンボーディングを可能にする ADC の新機能です。この機能により、Citrix ADC インスタンスは自動的に Citrix ADM サービスと接続し、システム、使用状況、およびテレメトリデータを ADM サービスに送信できます。Citrix ADM サービスは、このデータに基づいて、Citrix ADC インフラストラクチャに関する洞察と推奨事項を提供します。パフォーマンスの問題、高いリソース使用率、重大なエラーの迅速な特定など。

  ADM サービス接続は、次の ADC バージョンで使用できます。

  - Citrix ADC MPX および VPX イメージのバージョン 12.1 57.18 以降および 13.0 61.48 以降。詳しくは、「Citrix ADC アプライアンス用の Citrix ADM サービス接続の概要」を参照してください。
  - Citrix ADC SDX バージョンイメージ 12.1 58.14 以降および 13.0 61.48 以降。詳しくは、「Citrix ADC SDX アプライアンス用の Citrix ADM サービス接続の概要」を参照してください。

- **Call Home**：これは ADC の既存の機能であり、定期的にインスタンスを監視し、Citrix テクニカルサポートサーバーにデータを自動的にアップロードします。詳しくは、「Call Home」を参照してください。Call Home によって収集されたデータは、この新しいワークフローを有効にするために ADM サービスにもルーティングされます。

インターネット接続または Call Home を備えたすべての ADC インスタンス、または ADM サービス接続で有効なインスタンスが ADM サービスに接続されます。ADM サービスは、Call Home ルート、ADM サービス接続ルート、またはその両方を通じて、これらの ADC インスタンスから関連するメトリックの収集を開始します。詳しくは、「MPX および VPX インスタンスのデータガバナンス」および「SDX インスタンスのデータガバナンス」を参照してください。

ADM サービスは、このデータを使用して、すべての顧客（一意の組織 ID）の ADC インスタンスのインベントリを作成し、ADC インスタンスの統合リストを表示します。また、ADM サービスはこのデータを使用して ADC インスタンスと Gateway インスタンスに関するインサイトを作成します。これにより、HMC 展開に関する有意義な洞察が得られ、問題を特定し、問題を軽減するためのアクションが推奨されます。問題を軽減する前に、ADC インスタンスを ADM サービスにオンボードする必要があります。
[オンボードする **ADC** および **Gateway** インスタンスを選択] をオンにして、ADM サービスにオンボードする ADC インスタンスを選択できます。を開始すると、オンボーディングプロセスが表示されます。

自動オンボーディングプロセスでは、ADM サービスコネクトが使用されます。これにより、エクスペリエンスが自動化され、シームレスかつ迅速になります。ADM サービス接続および自動オンボーディングをサポートしないバージョンの ADC インスタンスでは、ADM サービスではスクリプトベースのオンボーディングを使用できます。これは半自動化されたプロセスです。

> 注：
>
> 自動およびスクリプトベースのオンボーディングでは、組み込みエージェントを使用します。ただし、このワークフローでは、外部エージェントをオンボーディングに柔軟に使用できます。プールライセンスを使用するか、

> ADM サービスで完全な分析スイートを使用する場合は、外部エージェントベースのオンボーディングを使用できます。または、プールライセンスと完全な分析スイートの両方を使用する場合です。組み込みエージェントは、管理と監視のみをサポートします。

オンボーディングのクイックツアー

オンボーディングの最初のタッチポイントは、製品開始メールです。オンボーディングの旅のクイックツアーは次のとおりです。

1. **Citrix** 製品が開始するメール：ADM サービスから電子メールを受信し、ADC インフラストラクチャに関する主要な洞察を示し、ADM サービスの使用を開始するよう促します。メールに記載されているリンクをクリックします。
2. **Citrix Cloud** のログインページ：自分の **Citrix** 資格情報を使用して **Citrix** Cloud にサインインする必要があります。
3. **Citrix ADM** サービスのウェルカムページ：ADM サービスとそのメリットの概要が表示されます。
4. **ADC** および **Gateway** インスタンスに関する洞察: セキュリティアドバイザリ (現在の Citrix CVE に関するアドバイス)、アップグレードアドバイザリ (EO/EOL タイムラインに基づくアドバイス)、主要なメトリック、傾向、および ADC パフォーマンスに影響する問題のハイライトなど、ADC インフラストラクチャ全体に関する詳細な洞察を得ることができます。健康状態であり、問題を軽減する方法を推奨しています。
5. オンボードする **ADC** およびゲートウェイインスタンスを選択: ADC インベントリの統合ビューが表示されます。ADM サービスにオンボードする ADC インスタンスを選択できます。
6. オンボード **ADC** インスタンスから **ADM** へ：オンボーディング用に選択した ADC インスタンスに基づいて、ADM はオンボーディングプロセスをガイドします。デフォルトでは、組み込みエージェントが自動オンボーディング用に選択されます。
7. **ADM GUI** ダッシュボード: 初期登録が完了すると、ADM インスタンスダッシュボードが表示されます。

> 注:
>
> このワークフローは、カナリアリリースによって段階的に展開されます (GA)。ADM サービス環境でこの機能が利用可能になると、電子メールが送信されます。

これらの各オンボーディング方法の詳細については、「Citrix ADM サービス接続を使用して Citrix ADC インスタンスをオンボードする」を参照してください。

Citrix ADM サービス接続を使用して Citrix ADC インスタンスをオンボードする

May 7, 2021

次に、ADM サービスの使用を開始するためのステップバイステップガイドを示します。開始する前に、Citrix ADM サービスが新しいオンボーディングワークフローを起動する方法をお読みください。これにより、ハイブリッドマル

チクラウド（HMC）展開をより迅速に可視化できます。「Citrix ADM サービス接続を使用した Citrix ADC インスタンスのロータッチオンボーディング」を参照してください。

ステップ **1:** 開始する

ADM サービスから、ADC インフラストラクチャに関する主要な洞察を示し、ADM サービスの使用を開始するよう招待するメールが届きます。

citrix

Security and Upgrade Advisory with Citrix ADM service

Hello [redacted],

Org ID - [redacted]

As a valued Citrix customer, your application delivery infrastructure security is our top concern. To help keep your infrastructure secure, we just launched **security advisory and upgrade advisory** for your Citrix ADCs as part of Citrix ADM service.

These new features will identify outdated software deployed in your ADC fleet, notify you of known vulnerabilities in these releases, and suggest steps you can take to remediate these issues.

Below, you'll see a preview of these advisories and other key insights customized to your infrastructure. More information and recommended actions are available when you get started with Citrix ADM service for free.

Top insights on your ADC & Gateway infrastructure

These insights are based on data provided via Call Home and/or Citrix ADM service connect.

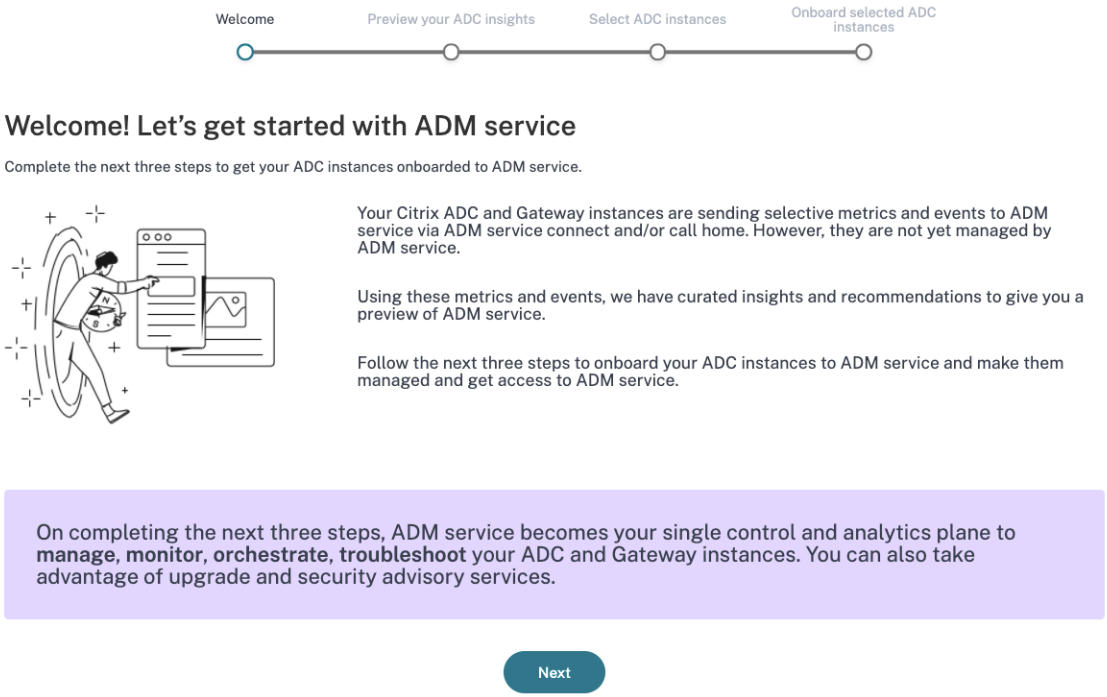
ADC instances by platforms

101	101	0	0
Total	VPX	SDX	MPX

Security Advisory	**101 ADC** instances are on versions with known common vulnerability exposures (CVEs). *This advisory is based on ADC build version scan only & more conclusive & exhaustive security advisory insights can be seen after onboarding all your ADCs to ADM Svc*
Upgrade Advisory	**101 ADC** instances are on older builds and releases.
ADC deployment	**1 ADC** instance is not deployed as High Availability (HA) pair. Citrix ADM recommends HA pair for production ADC instances.
Recent events	No critical events reported on any ADC.
Resource utilization	All ADC instances have CPU usage < 50% All ADC instances have memory usage < 50%

To get more details and recommendations on these insights, **onboard your ADC instances to Citrix ADM service today.**

1. メールで、[開始] をクリックしてオンボーディングプロセスを開始します。
2. My Citrix/Citrix Cloud の資格情報を使用して Citrix Cloud にサインインします。
3. Citrix ADM サービスのランディングページで、現在使用している理由と、ADM を使用するメリットについてお読みください。



4. [次へ] をクリックします。**ADC** インスタンスおよび **Gateway** インスタンスの **[Insights**] ページが開きます。

次のいくつかのステップは、ガイド付きのワークフローとして機能し、ADM が提供できる内容をプレビューし、ADC インスタンスを ADM サービスにシームレスにオンボード化するのに役立ちます。

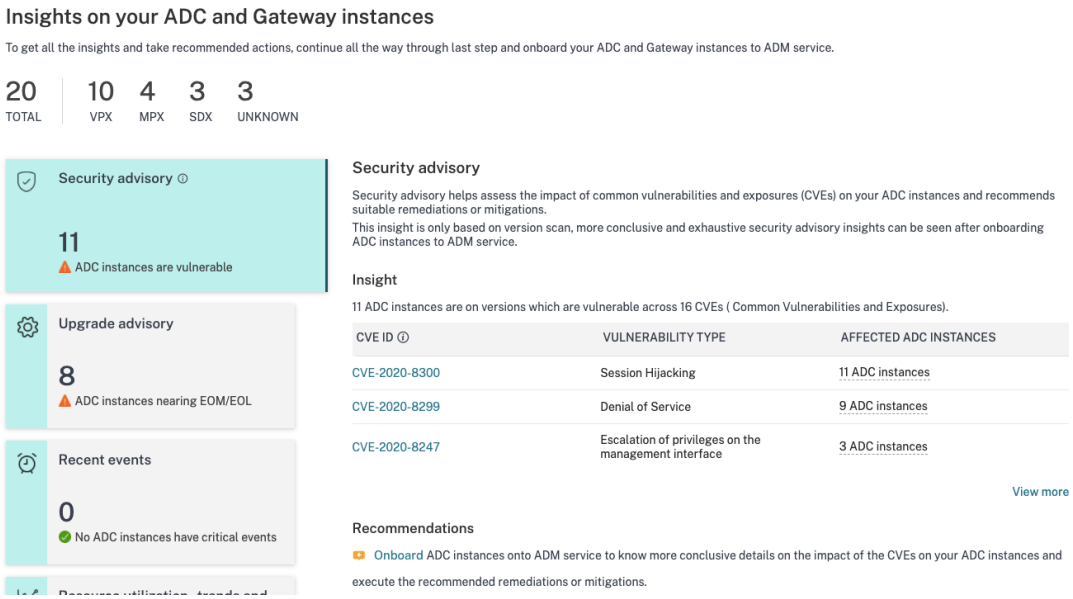
ステップ **2: ADC** インスタンスおよびゲートウェイインスタンスに関する洞察

このインサイトページでは、Call Home または ADM サービス接続、または Call Home と ADM サービス接続の両方を通じて収集されたデータを使用して、ADC インスタンスに関するインサイトを提供します。このページでは、セキュリティアドバイザリ（現在の Citrix CVE に関するアドバイス）、アップグレードアドバイザリ（EO/EOL タイムラインに基づくアドバイス）、主要なメトリック、傾向、ADC のパフォーマンスと正常性に影響する問題を強調し、問題を軽減するための推奨方法を含む、ADC インフラストラクチャ全体についての洞察を提供します。これらのインサイトと推奨事項は、ADM サービスが提供する多くのメリットと付加価値のほんの一例に過ぎません。さらに多くのメリット、詳細な洞察を得て、推奨されるアクションを実行するには、ADC インスタンスを ADM にオンボードする必要があります。

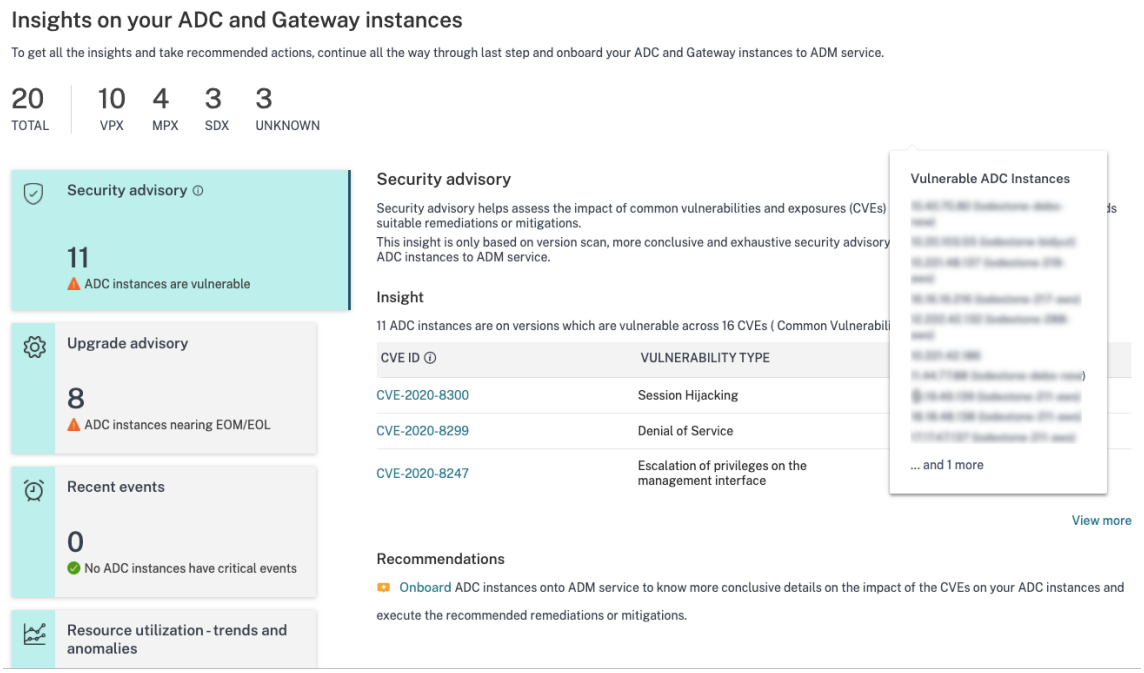
インサイトと推奨事項は、次のタイプに分類されます。

- セキュリティアドバイザリ: オンボード ADC インスタンスを使用して、ADC インスタンスの CVE 影響の詳細を取得し、推奨される修正または緩和策を実行します。
- アップグレードアドバイザリ: ADC インスタンスを ADM にオンボードして、EO/EOL に達している、または到達している ADC インスタンス、または古いリリース/ビルドにある ADC インスタンスをアップグレードします。
- 最近のイベント: ADC インスタンスを ADM にオンボードして 200 以上のイベントを定期的に監視し、電子メール、PagerDuty、Slack、ServiceNow で通知を受け取るルールを作成し、適切なアクションを実行します。
- リソース使用率-傾向と異常: ADC インスタンスを ADM にオンボードして、ADC インスタンスの健全性、パフォーマンスの問題、およびこれらの問題を軽減するための推奨事項を包括的に把握できます。また、ADC インスタンスの予測された CPU およびメモリ使用量を評価することもできます。
- **ADC** デプロイガイダンス: ADC インスタンスを ADM にオンボードし、ADM の設定ジョブを使用して HA ペアとして設定します。

1. セキュリティアドバイザリ： Citrix ADM セキュリティアドバイザリは、ADC インスタンスを危険にさらす脆弱性について警告し、緩和策と修復を推奨します。CVE ID、脆弱性の種類、および影響を受ける ADC インスタンスを確認できます。CVE ID リンクは、セキュリティ情報の記事を参照してください。



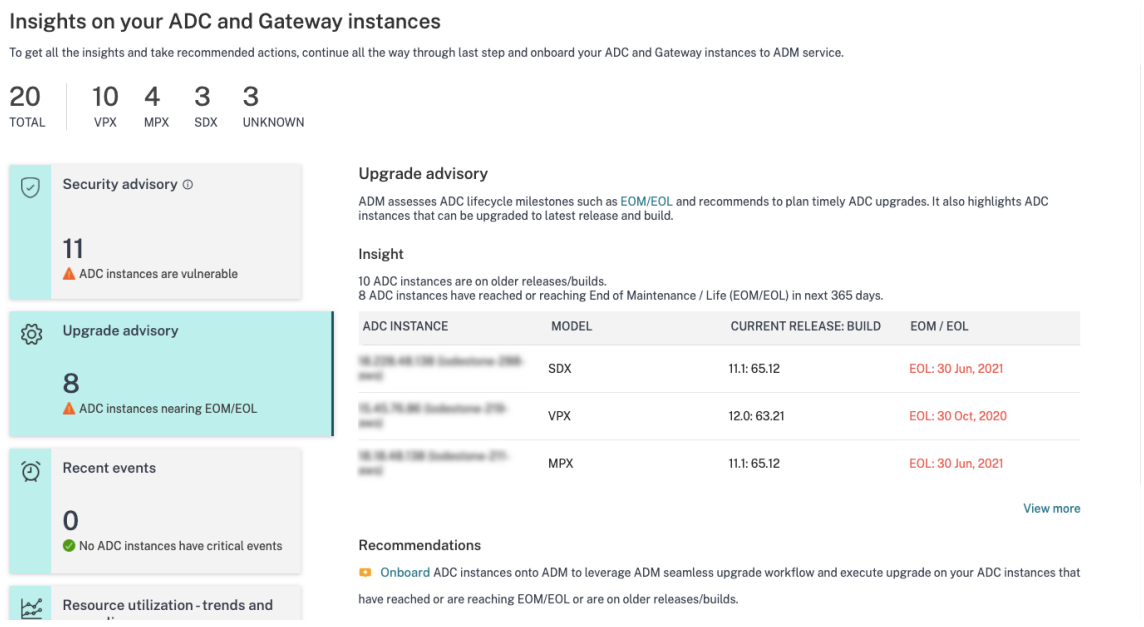
この推奨事項では、ADC インスタンスを ADM Service にオンボードして、ADC インスタンスの CVE の影響の詳細を取得し、推奨される緩和策または修正を実行します。影響を受ける ADC インスタンスをクリックして、影響を受けるインスタンスの IP アドレスを確認します。



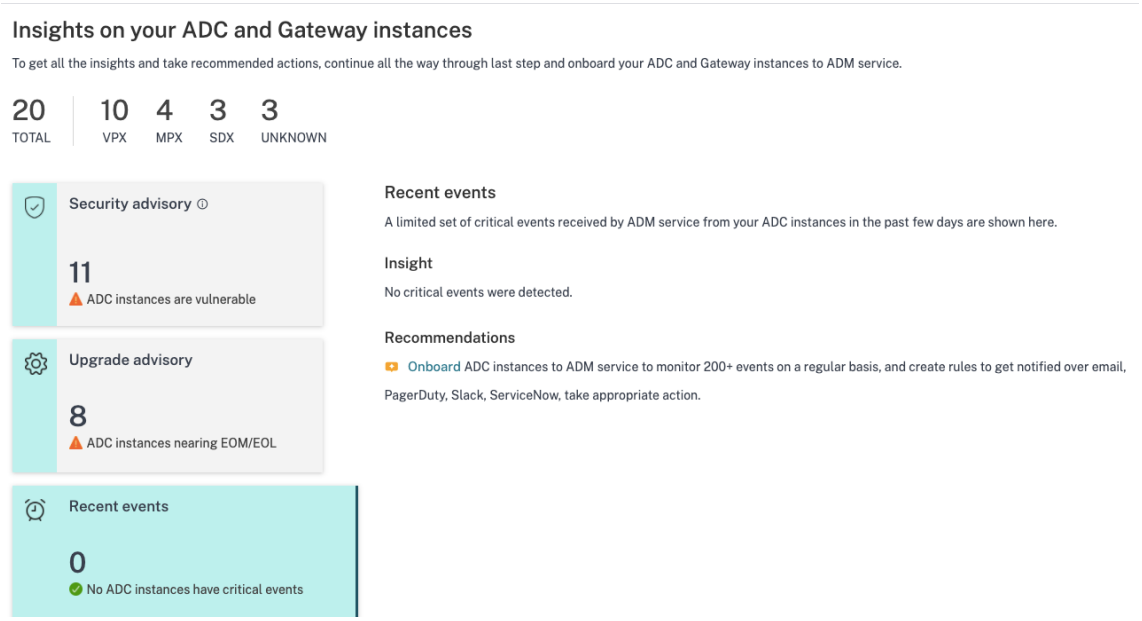
2. アップグレードアドバイザリ: このアドバイザリを使用して、EO/EOL に近づいているか、古いビルド上にある ADC インスタンスをチェックします。

   これらの洞察に基づいて、ADM では EO/EOL の前にタイムリーなアップグレードを計画するか、最新の機能と修正の恩恵を受けることをお勧めします。

   アップグレードを実行するには、ADC インスタンスを ADM サービスにオンボードする必要があります。

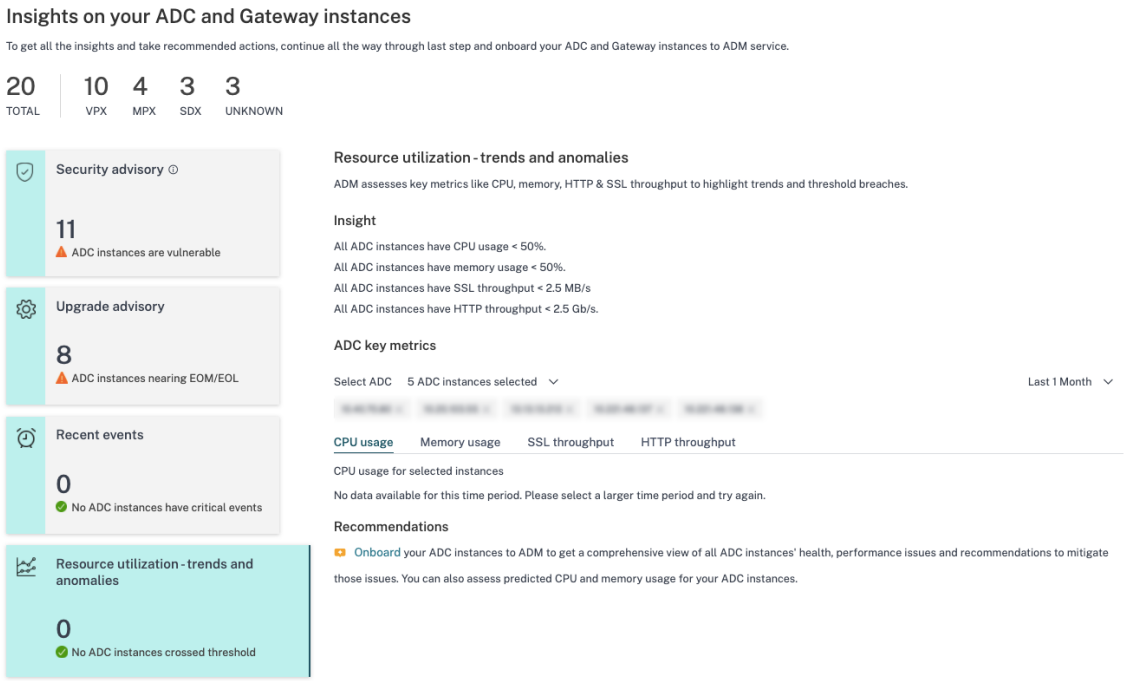


3. 最近のイベント: ADC インスタンスで発生した重大なエラーの詳細と、エラーが発生した ADC インスタンスのリストを取得します。

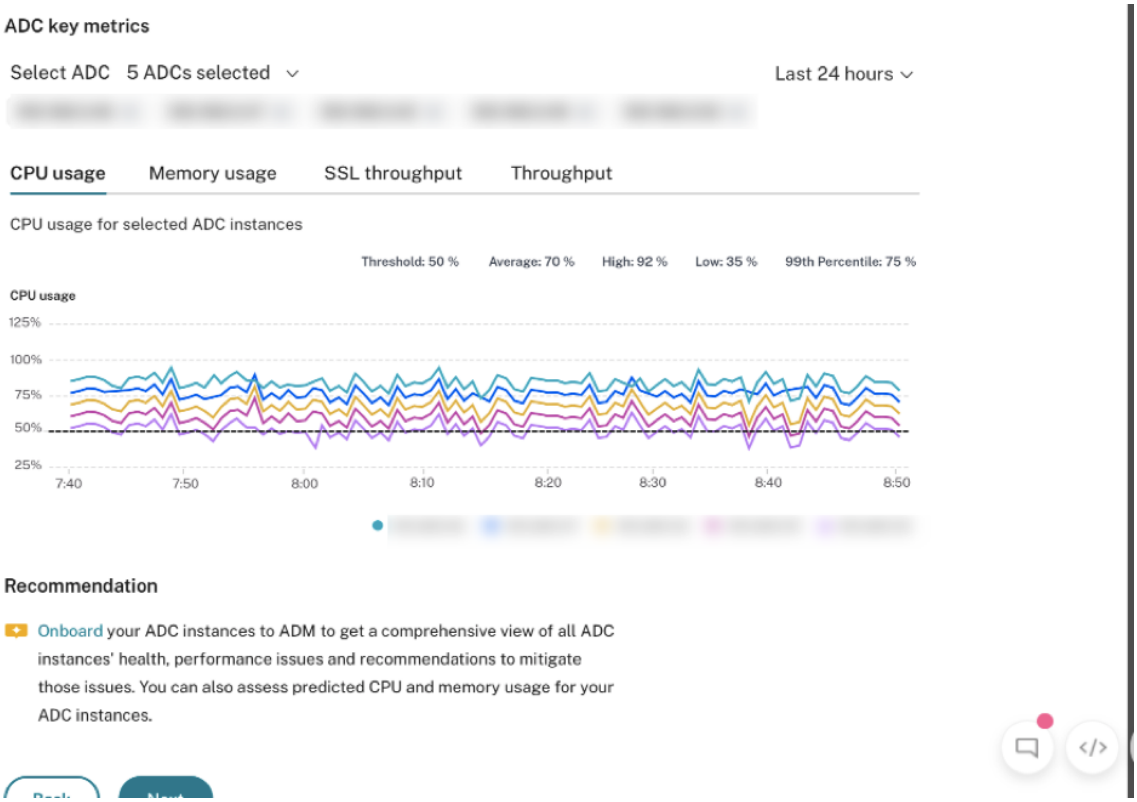


4. リソース使用率-傾向と異常: CPU、メモリ、HTTP スループット、SSL スループットの高いリソース使用率に関する洞察を見つけます。各インサイトについて、ADM は推奨されるアクションを提案します。これらの洞察と推奨事項をより詳細に把握するには、ADC インスタンスを ADM にオンボードする必要があります。オンボーディング後のいくつかの利点は次のとおりです。

    - CPU: ADM で今後 24 時間の CPU 使用率を予測します。
    - メモリ:ADM で今後 24 時間のメモリ使用率を予測します。
    - SSL スループット:ADM でのインテリジェントなアプリケーション分析により、SSL リアルタイムの最適化を表示します。
    - HTTP スループット: インフラストラクチャ分析を使用して、ADC スループット容量の問題をトラブルシューティングします。

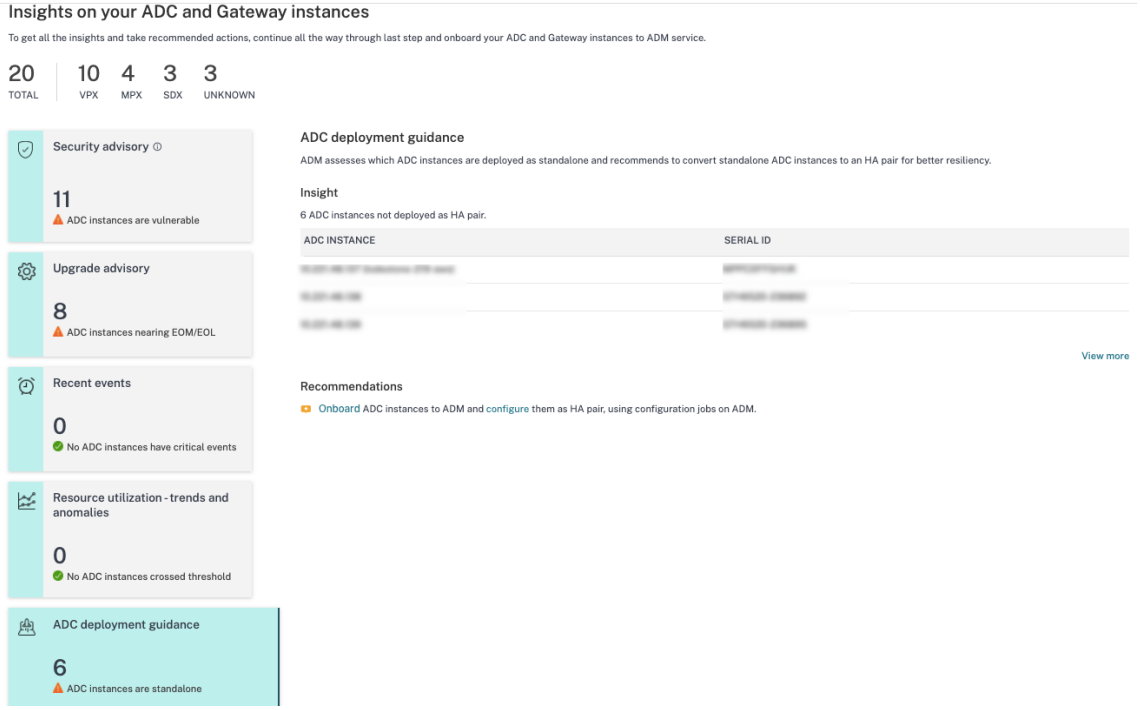


- 主要メトリック: CPU、メモリ、HTTP スループット、SSL スループットに関連する主要なメトリックの詳細を取得し、メトリックの異常な傾向を明らかにします。



5. デプロイガイダンス: スタンドアロン ADC としてデプロイされる ADC インスタンスを可視化します。ADM では、復元性の向上のために、これらの ADC インスタンスを HA ペアとして設定することを推奨します。こ

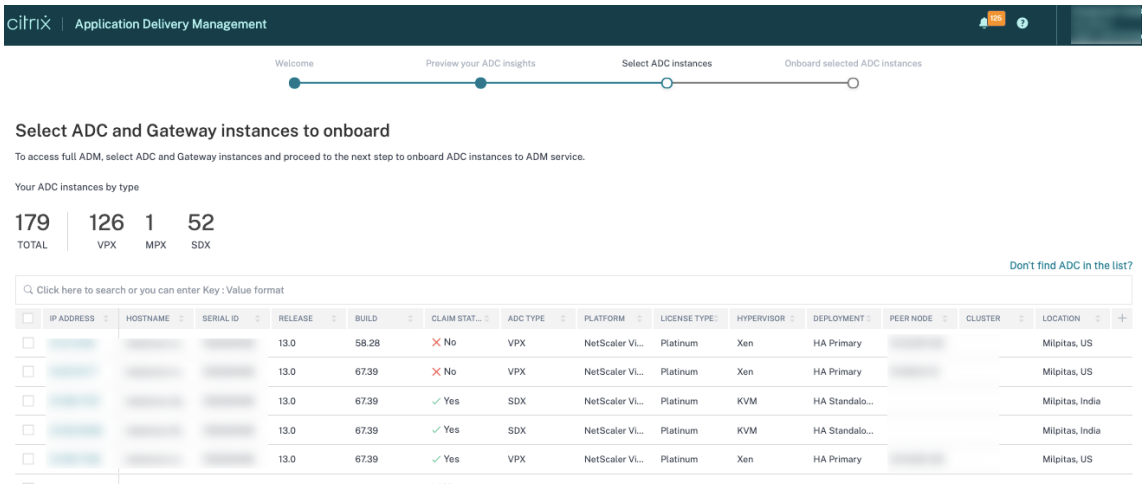
れには、ADC インスタンスを ADM にオンボードしてから、メンテナンス・ジョブを使用してインスタンスを HA ペアとして設定する必要があります。



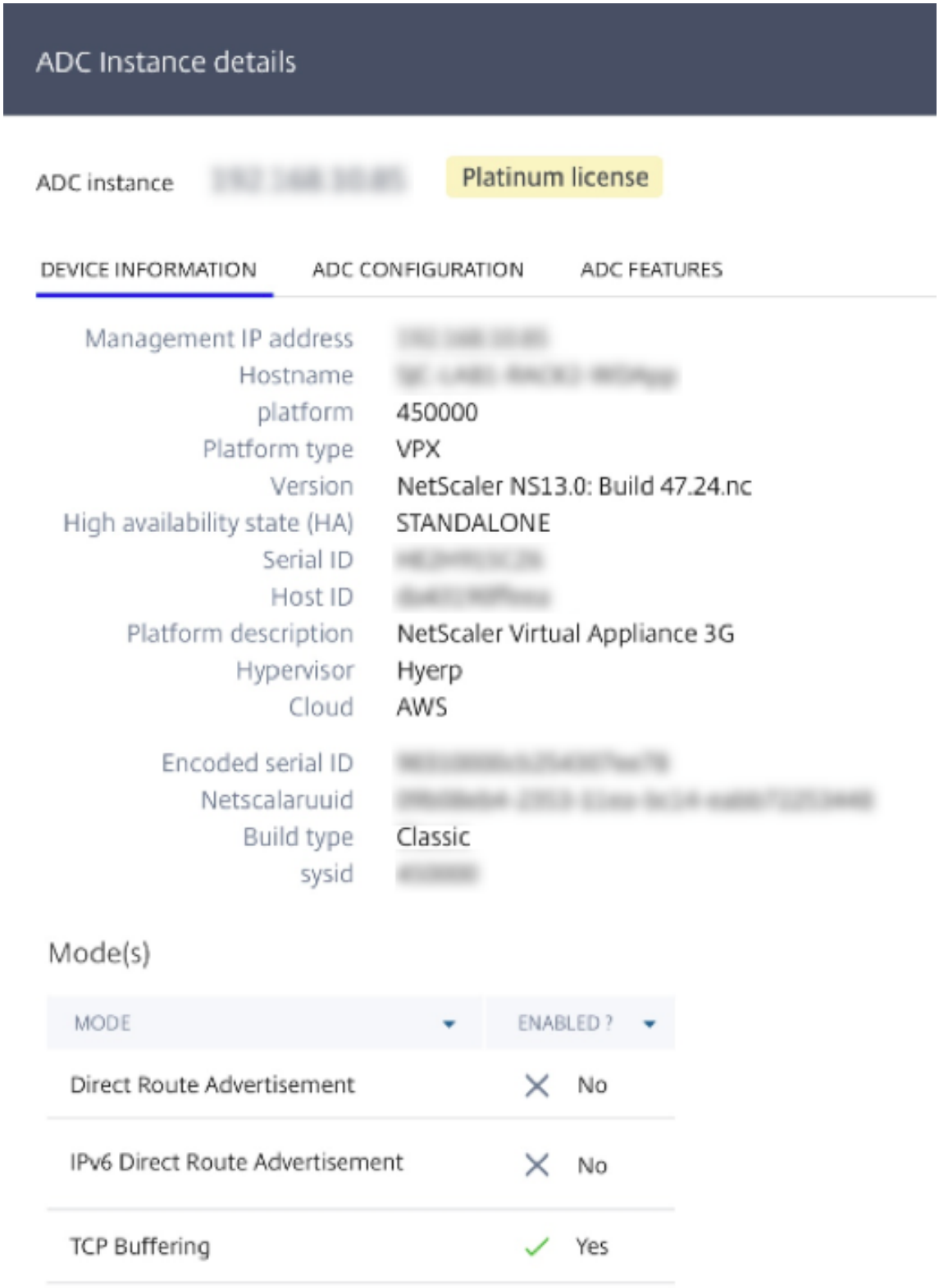
ステップ **3:** オンボードする **ADC** インスタンスと **Gateway** インスタンスを選択

このページには、環境内のすべての ADC インスタンスと Gateway インスタンスが表示されます。ADM サービスにオンボードする ADC および Gateway インスタンスを表示して選択し、[**Next**] をクリックします。

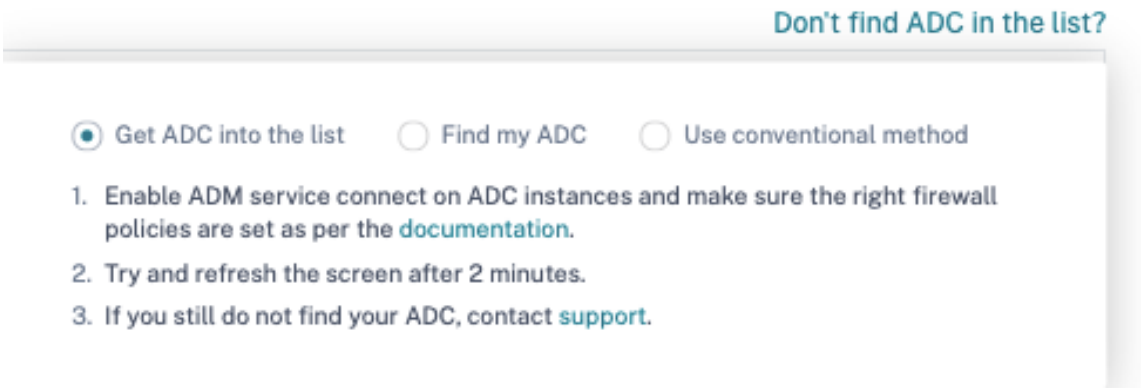
1. ADM サービスにオンボードする ADC インスタンスを表示して選択します。



デバイス情報、ADC 設定、利用可能な ADC 機能、ライセンス情報など、インスタンスの詳細が必要な場合は、ADC インスタンスの下にあるインスタンスの IP アドレスをクリックします。



インスタンスがリストに表示されない場合は、右上隅のリストにある **[Don’t find ADC**] を使用します。

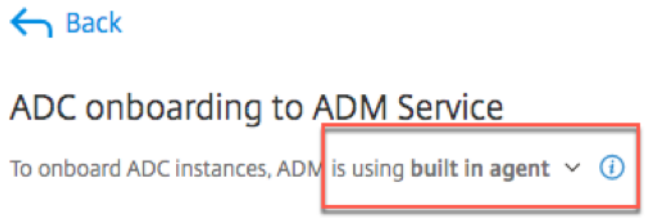


次の 3 つの方法で操作できます。[**ADC** をリストに入れる] の下にある手順に従うか、[**ADC** を検索**]** オプションを使用します。これら 2 つの手順で解決しない場合は、[**Use continional Method**] オプションをクリックします。このオプションをクリックすると、ワークフローがスキップされ、ADC インスタンスの従来の初期登録方法が表示されます。

[**Find my ADC]** オプションの場合、必須のフィールド（シリアル ID、ADC インスタンスの IP アドレス、ライセンスシリアル番号、フルフィルメント ID）に詳細を入力し、検索します。

ステップ **4: ADC** インスタンスを **ADM** にオンボードする

組み込みエージェント（デフォルトオプション）または外部エージェントを使用して、インスタンスをオンボードできます。



組み込みエージェントを使用したオンボード **ADC** インスタンス

自動およびスクリプトベースのオンボーディングでは、デフォルトで設定されている組み込みエージェントを使用します。

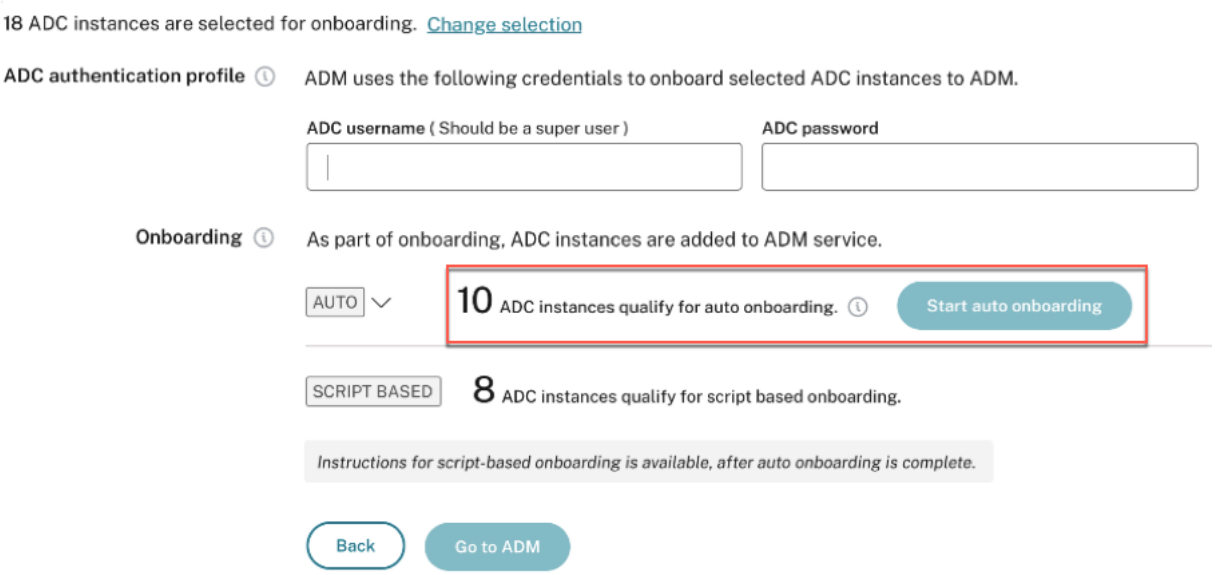
自動オンボーディング: 次のバージョンの ADC でのみサポートされます。

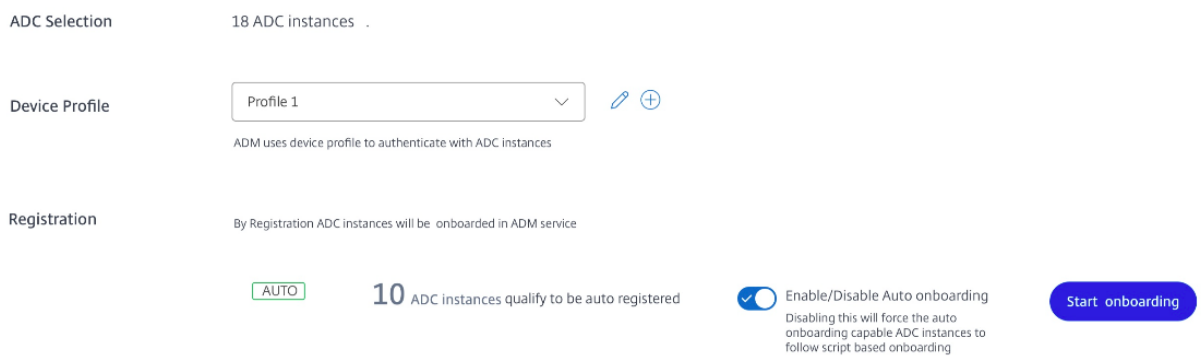
- Citrix ADC MPX および VPX イメージのバージョン 12.1 57.18 以降および 13.0 61.48 以降
- SDX バージョンイメージ 13.0 61.48 以降および 12.1 58.14 以降

別の ADC インスタンスを選択するには、**[Change**selection] をクリックします。

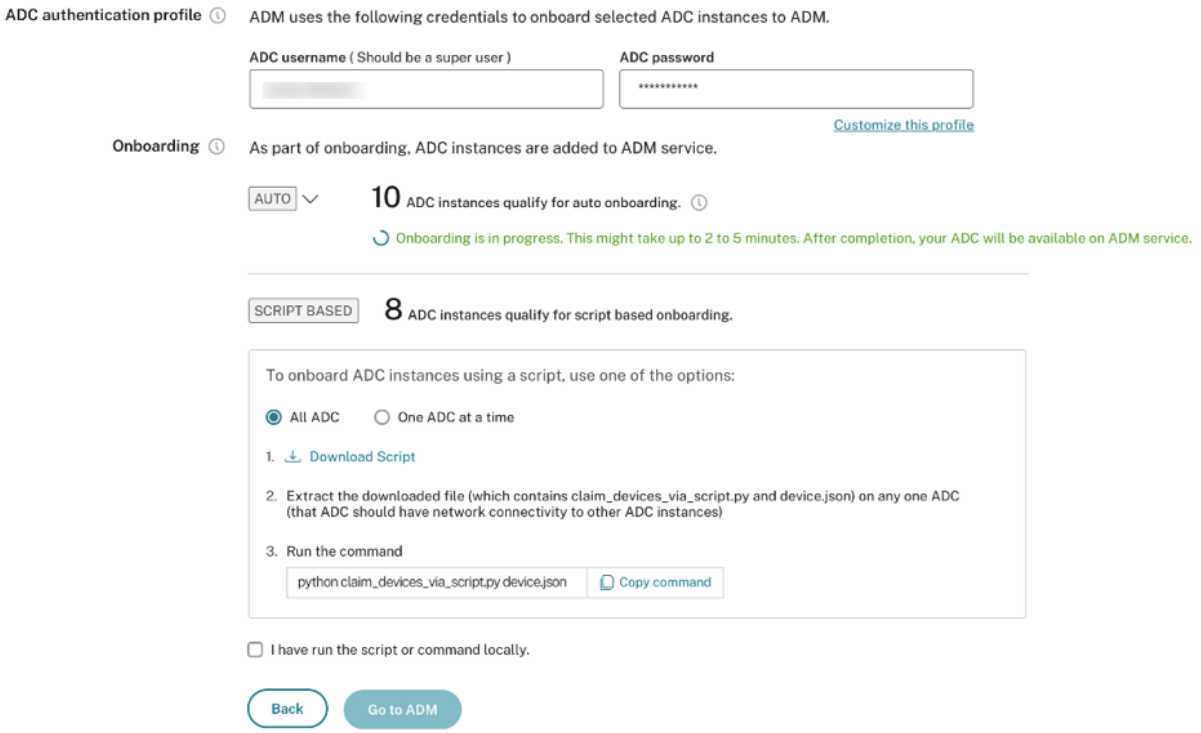
選択された ADC インスタンスの合計のうち、一部のインスタンスは（最小バージョン基準に基づいて）自動オンボーディングの対象となる場合があります。自動オンボーディングの対象となるインスタンスを確認できます。

ADC ユーザ名とパスワードを入力します。これらのクレデンシャルは ADC ユーザ管理者クレデンシャルである必要があります。また、ADM はこれらの資格情報を使用して ADC をオンボードします。[オンボーディングを開始] をクリックして、ADM の ADC インスタンスをオンボーディングします。





自動オンボーディングが完了するまでに 2 ～5 分ほどかかる場合があります。

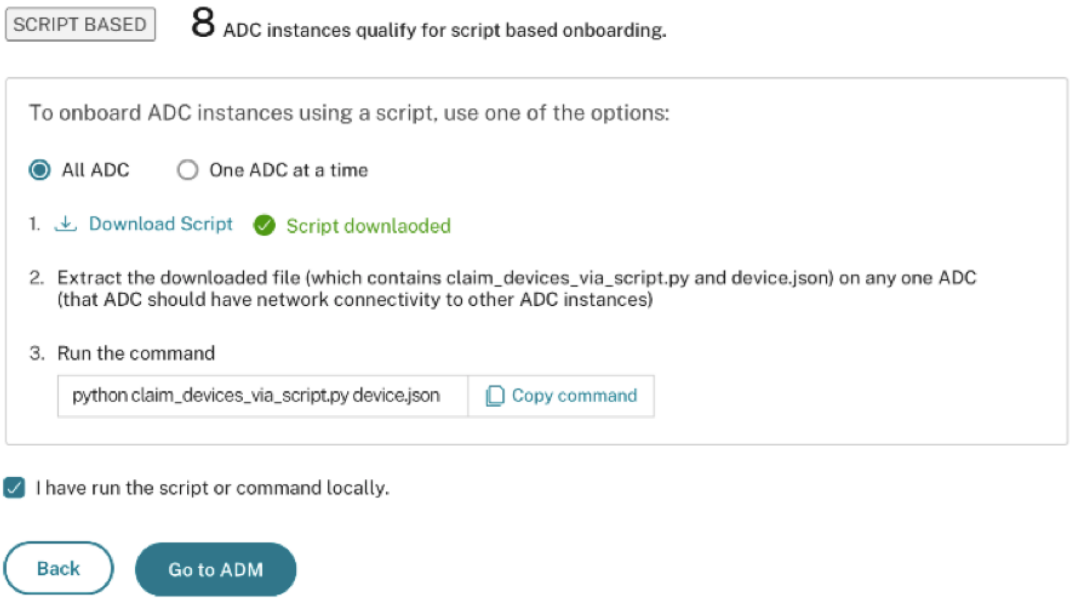


> 注:
>
> ADC インスタンスを ADM に自動オンボードしたくない場合は、自動オンボーディングを無効にして、オンボーディングのスクリプトベースのオプションを使用できます。

スクリプトベースのオンボーディング: 自動オンボーディングが完了すると、スクリプトベースのオンボーディングを使用して残りのインスタンスをオンボーディングできます。次のいずれかのオプションを使用します:

- オプション **1**: UI で与えられたコマンドを使用して、スクリプトをダウンロードし、tar ファイルを抽出し、ADC インスタンスの 1 つで実行します。このスクリプトを実行する ADC インスタンスに、選択した他のすべての ADC インスタンスへのネットワーク接続があることを確認してください。
- オプション **2**: 各 ADC インスタンスの CLI コンソールにログインし、UI で与えられたコマンドを実行します。詳細については、ドキュメントインスタンスを管理するように ADC 組み込みエージェントを構成するの手順

7 を参照してください。ADC インスタンスごとに、新しい一意のアクティベーションコードを生成してください。

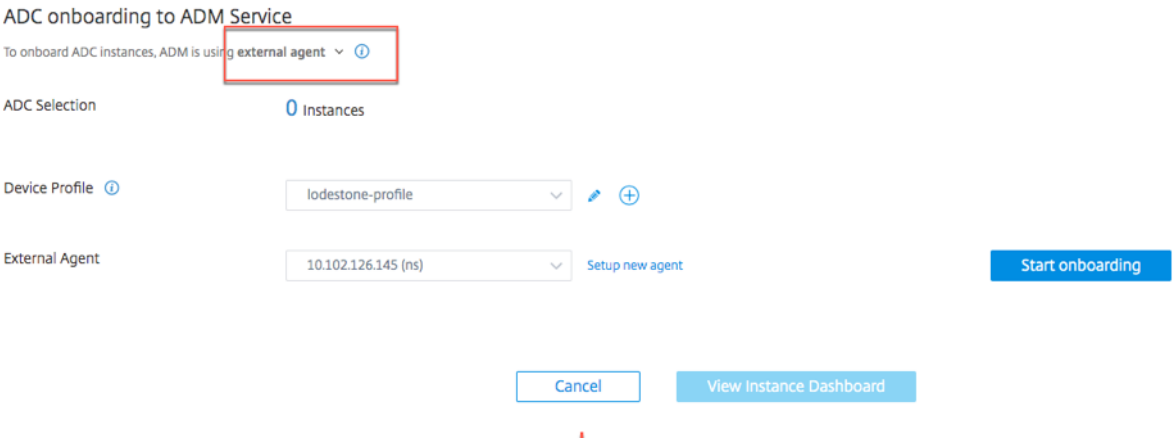


すべてのインスタンスをオンボードしたら、[**Go to ADM**] をクリックして ADM インスタンス管理 UI ダッシュボードに移動し、さまざまな機能を確認します。

> 注:
>
> ADM ライセンスのない ADM サービスの新規顧客の場合、Citrix サービスアカウントはデフォルトで Express アカウントです。ADM アカウントのエンタイトルメントの詳細については、「Express アカウントを使用して Citrix ADM リソースを管理する」を参照してください。

外部エージェントを使用したオンボード **ADC** インスタンス

ADM サービスでプールライセンスまたは完全な分析スイートを使用する場合、またはプールライセンスと完全な分析スイートを使用する場合は、外部エージェントベースのオンボーディングを使用できます。



次の手順を実行します:

1. デバイスプロファイルを選択します。

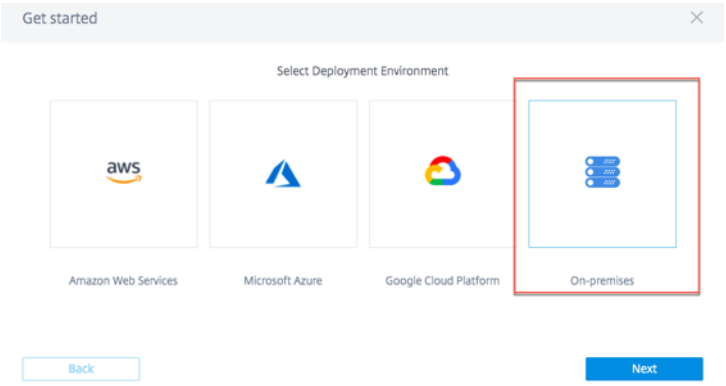
   > 注:
   >
   > セキュリティ上の理由から、デフォルトの ADC 認証情報（nsroot/nsroot）を初期登録に使用することはできません。

2. 外部エージェントを選択し、[**Setup new Agent**] をクリックします。
3. 次の環境のいずれかを選択します。

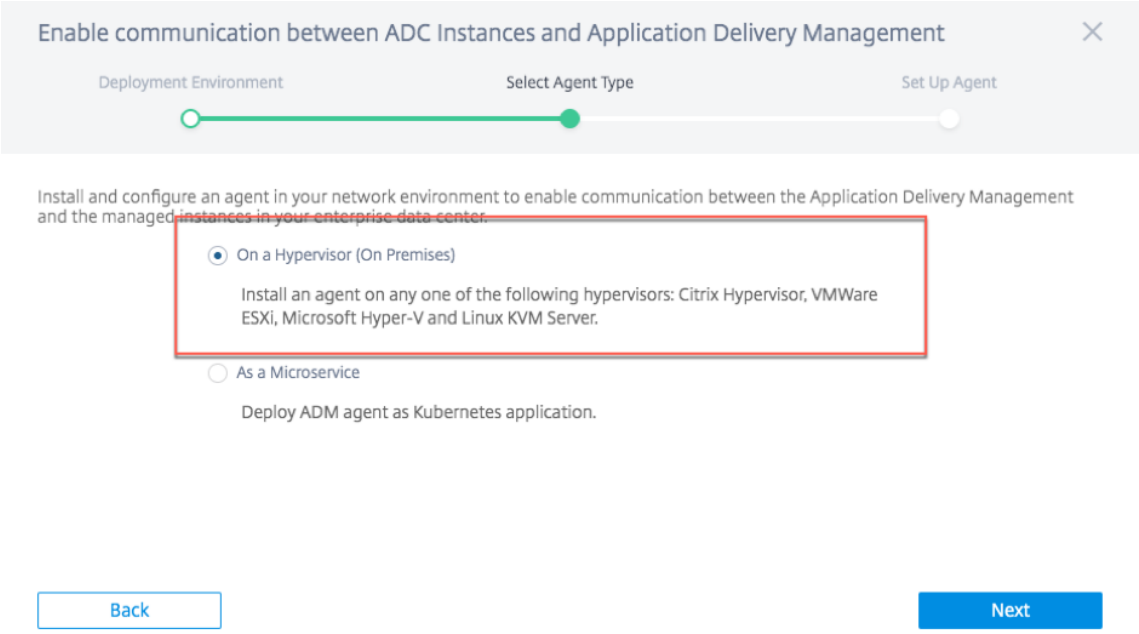
   - Amazon Web Services
   - Microsoft Azure
   - Google Cloud Platform
   - オンプレミス

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

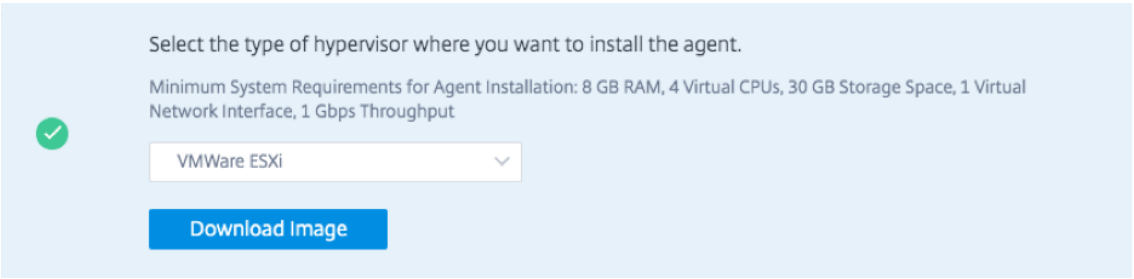
オンプレミスを選択した場合は、Citrix Hypervisor、VMware ESXi、Microsoft Hyper-V、Linux KVM サーバーのハイパーバイザーにエージェントをインストールできます。



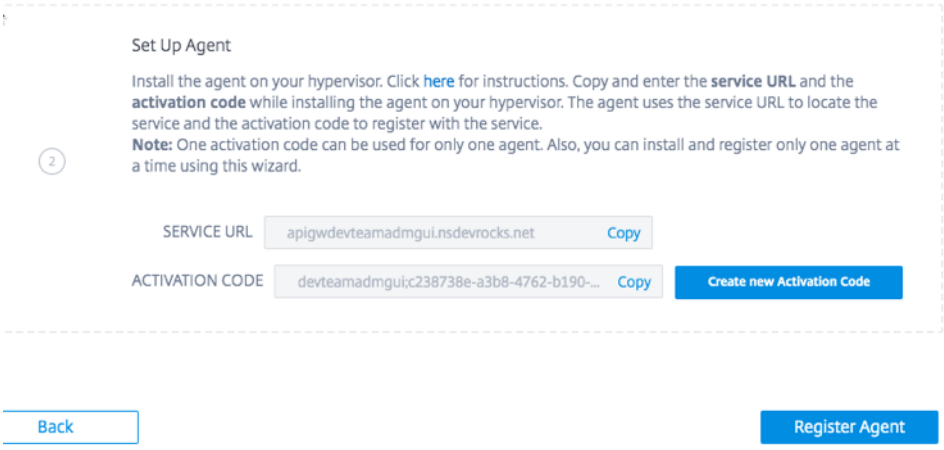
1. **[Hypervisor (**オンプレミス**)]** を選択し、[次へ] をクリックします。



2. ハイパーバイザーのタイプを選択し、イメージ（VMware ESXi など）をダウンロードします。

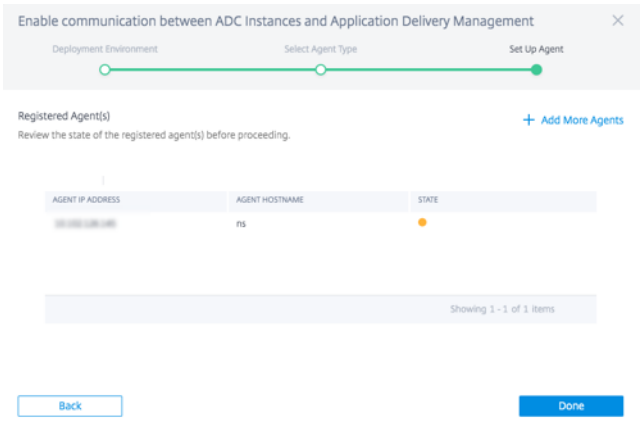


3. サービス URL とアクティベーションコードを使用して、エージェントを構成します。

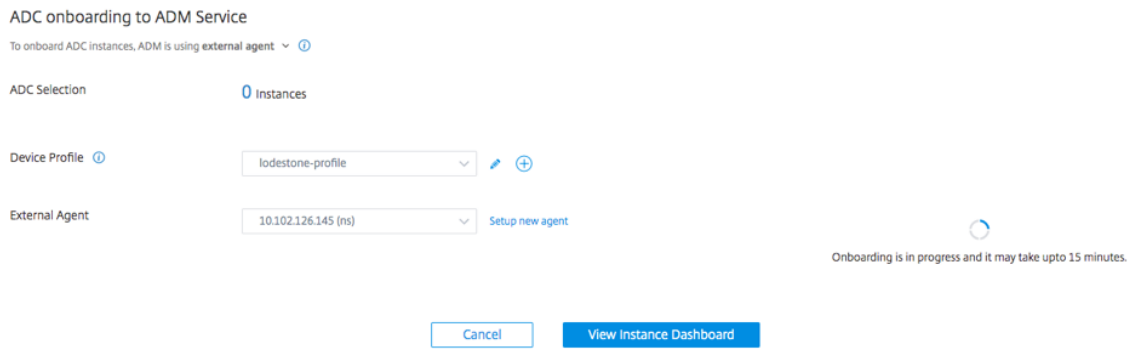


エージェントは、サービス URL を使用してサービスを検索し、アクティベーションコードを使用してサービスに登録します。オンプレミスのハイパーバイザーにエージェントをインストールする方法の詳細については、Citrix ADM エージェントをオンプレミスでインストールするを参照してください。

4. [エージェントの登録] をクリックします。完了したら、**[** 完了**]** をクリックして、ADC オンボーディング ADM サービスページに戻ります。



5. [初期登録を開始] をクリックします。すべてのインスタンスをオンボードしたら、[**View Instance Dashboard**] をクリックして ADM インスタンス管理 UI ダッシュボードに移動し、さまざまな機能を確認します。



パブリッククラウドへのエージェントのインストール

エージェントは、次のクラウド環境のいずれかにインストールできます。

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

詳しくは、次のドキュメントを参照してください。

- Microsoft Azure クラウドに Citrix ADM エージェントをインストールする
- AWS に Citrix ADM エージェントをインストールする
- GCP に Citrix ADM エージェントをインストールする

組み込みエージェントから外部エージェントへの移行

May 7, 2021

ADM サービスを使用して管理および監視のみを行うことがあり、後でプールされたライセンスや分析などの他の機能を使用することもできます。そのためには、組み込みの ADM サービスエージェントから外部エージェントに移行する必要があります。

組み込みエージェントは、ADM の管理および監視機能のみをサポートします。プールされたライセンスや分析など、その他の ADM 機能については、外部エージェントが必要です。このドキュメントでは、既存の ADM 組み込みエージェントから外部のハイパーバイザーベースのエージェントに移行する手順について説明します。

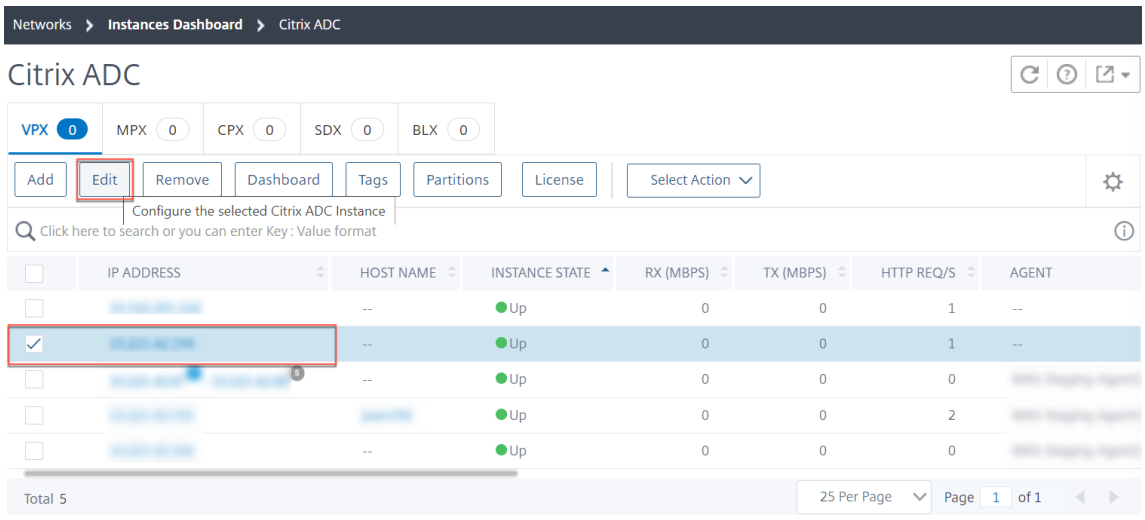
はじめに

移行を開始する前に、外部エージェントをインストールします。トピックCitrix ADM エージェントをオンプレミスでインストールするに記載されている手順に従ってください。

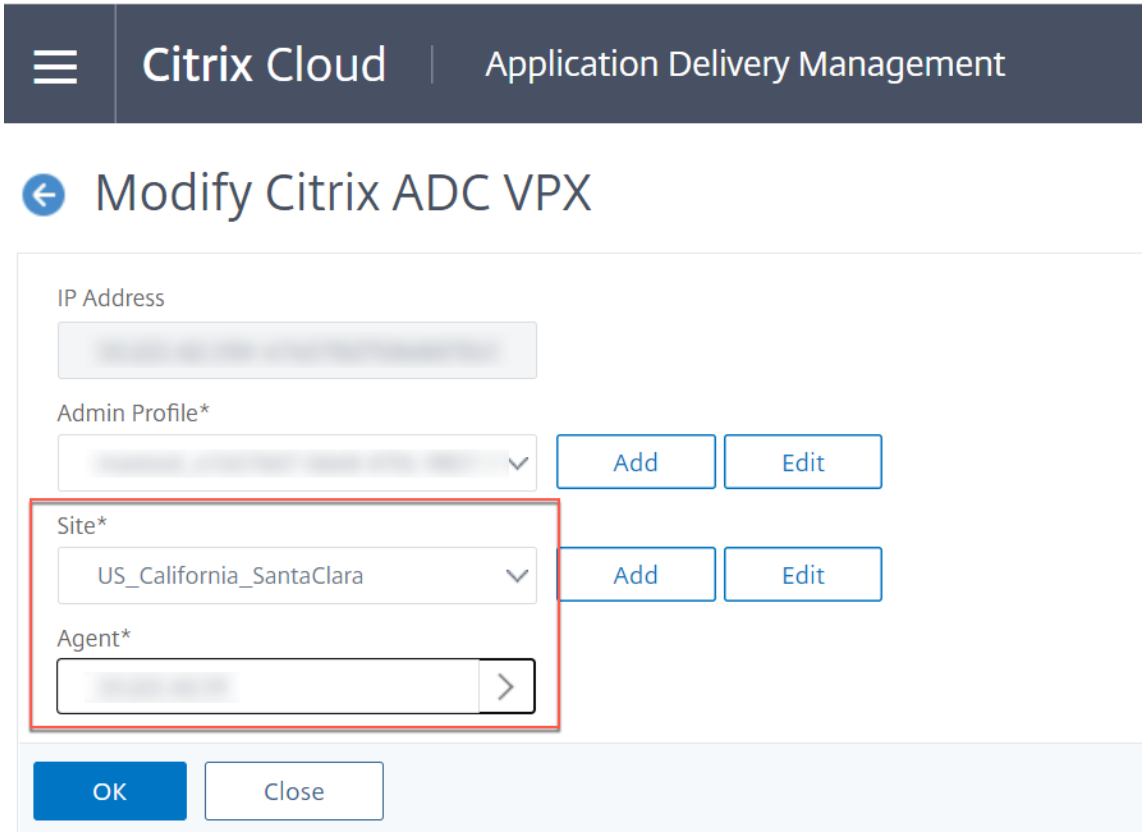
組み込みエージェントから外部エージェントへの移行

組み込みエージェントから外部エージェントに移行する手順は、次のとおりです。

1. ADM GUI で、［ネットワーク］**>**［インスタンスダッシュボード］**>**［**Citrix ADC**］で、Citrix ADC インスタンスを選択し、［編集］をクリックします。



2. サイトとエージェントを選択し、［**OK**］をクリックします。



3. インスタンスを再度選択し、[アクションの選択] **>** [再検出] をクリックします。

機能とソリューション

May 7, 2021

Citrix Application Delivery Management（Citrix ADM）は、オンプレミスバージョンの Citrix ADM で使用できるほとんどの機能と互換性があります。このマニュアルでは、サービスでサポートされる機能について説明します。

アプリケーション分析と管理

Citrix ADM のアプリケーション分析と管理機能は、アプリケーション中心のアプローチを強化し、さまざまなアプリケーション配信の課題に対処するのに役立ちます。このアプローチでは、アプリケーションの正常性スコアを可視化し、セキュリティリスクを特定し、アプリケーショントラフィックフローの異常を検出し、是正措置を講じるのに役立ちます。

- アプリケーション・パフォーマンス分析: App Score は、アプリケーションのパフォーマンスを定義するスコアリングシステムの製品です。応答性の観点からアプリケーションが適切に機能しているか、脅威に対して脆弱でないか、すべてのシステムが稼働しているかどうかが表示されます。
- アプリケーション・セキュリティ分析: アプリセキュリティダッシュボードには、アプリケーションのセキュリティ状態に関する総合的なビューが表示されます。たとえば、セキュリティ違反、シグネチャ違反、脅威指

数などの、セキュリティの主要な測定基準が表示されます。アプリセキュリティダッシュボードには、検出された Citrix ADC インスタンスに対する SYN 攻撃、スモールウィンドウ攻撃、DNS フラッド攻撃などの攻撃関連情報も表示されます。

- インテリジェントなアプリ分析: インテリジェントアプリケーション分析機能は、Citrix ADC アプライアンスを介して提供されるアプリケーションの監視とトラブルシューティングのための簡単でスケーラブルなソリューションを提供します。インテリジェントアプリ分析は、アプリケーショントランザクションのすべてのレベルを監視するだけでなく、機械学習技術を使用してネットワーク内の通常のトラフィックパターンを定義し、異常を検出します。この機能により、全体的なターンアラウンド時間が短縮され、アプリケーション全体の稼働時間が短縮されます。

StyleBook

StyleBook は、アプリケーションの複雑な Citrix ADC 構成の管理作業を簡素化します。StyleBook は、Citrix ADC 構成の作成と管理に使用できるテンプレートです。Citrix ADC の特定の機能を構成するための StyleBook を作成することも、StyleBook を設計して、Microsoft Exchange や Skype for Business などのエンタープライズアプリケーション展開用の構成を作成することもできます。

インスタンス管理

Citrix ADC、Citrix Gateway、Citrix Secure Web Gateway、および Citrix SD-WAN インスタンスを管理できます。

> 注
>
> 現在、Citrix ADM は、Citrix SD-WAN インスタンスの WAN 最適化機能のみをサポートしています。

イベントの管理

イベントは、管理対象 Citrix ADC インスタンスでのイベントまたはエラーの発生を表します。たとえば、システム障害や構成が変更された場合、イベントが生成され、Citrix ADM に記録されます。Citrix ADM を使用して構成または表示できる関連機能を次に示します。

- イベントルールの作成
- Citrix ADM を使用して Syslog メッセージをエクスポートする

証明書管理機能

Citrix ADM は、証明書管理のあらゆる側面を合理化します。1 つのコンソールから、使われていない、または期限切れが近い証明書のタブは閉じたまま、正しい発行者、キーの強度、および正しいアルゴリズムを確保する自動化されたポリシーを作成することができます。

構成管理

Citrix ADM では、エンティティの作成、機能の構成、構成変更のレプリケーション、システムのアップグレード、その他のメンテナンス作業など、構成タスクの実行に役立つ構成ジョブを作成できます。構成ジョブとテンプレートは、Citrix ADM 上で最も反復的な管理タスクを単一のタスクに簡素化します。

構成監査

インスタンスの構成を監視して、異常を特定できます。

- 構成に関するアドバイス: 設定異常を識別できます。
- 監査テンプレート: 特定の構成の変更を監視できます。

ライセンス管理

Citrix ADM をライセンスマネージャーとして構成することにより、Citrix ADC ライセンスを管理できます。

- Citrix ADC プール容量: Citrix ADC インスタンスが 1 つのインスタンスライセンスをチェックアウトできる共通のライセンスプール。必要な帯域幅のみをチェックアウトできます。インスタンスでこれらのリソースが不要になった場合、インスタンスはリソースを共通プールにチェックインし、このリソースを必要とする他のインスタンスが利用できるようになります。
- Citrix ADC VPX チェックインとチェックアウトのライセンス: Citrix ADM は、Citrix ADC VPX インスタンスをオンデマンドでライセンスを割り当てます。Citrix ADC VPX インスタンスは、Citrix ADC VPX インスタンスがプロビジョニングされたときに Citrix ADM からライセンスをチェックアウトしたり、インスタンスが削除または破棄されたときに Citrix ADM にライセンスをチェックインし直すことができます。

ネットワークレポート

Citrix ADM でネットワークレポートを監視することで、リソース使用率を最適化できます。

Analytics

Citrix ADC インスタンスのデータのさまざまな洞察を調べて、アプリケーションのパフォーマンスを説明、予測、改善するための簡単でスケーラブルな方法を提供します。1 つまたは複数の分析機能を同時に使用できます。

- HDX Insight: Citrix ADC を通過する ICA トラフィックのエンドツーエンドの可視性を提供します。HDX Insight を使用すると、管理者はリアルタイムのクライアントとネットワークの遅延指標、履歴レポート、エンドツーエンドのパフォーマンスデータを表示し、パフォーマンス問題のトラブルシューティングを行うことができます。
- Web Insight: エンタープライズ Web アプリケーションを可視化します。IT 管理者は、アプリケーションの統合されたリアルタイム監視を提供することにより、Citrix ADC が提供するすべての Web アプリケーションを監視できます。Web Insight は、近似アルゴリズムを使用して Citrix ADC からのデータを処理します。企業内の Web アプリケーションに関連するメトリックの上位 1,000 レコードを提供します。
- Gateway Insight: アクセスモードに関係なく、ログオン時にユーザーが遭遇する障害を可視化します。あらゆる期間を対象にして、ログオンしたユーザーの一覧を、アクティブユーザーの数、アクティブセッションの数、ユーザー全体によって使用されたバイト数とライセンス数の情報と共に確認できます。
- Security Insight: アプリケーションのセキュリティステータスを評価し、アプリケーションをセキュリティで保護するための修正措置を講じるための単一ペインソリューションを提供します。
- SSL Insight: Web 上のセキュアなトランザクション (HTTPS) を可視化します。IT 管理者は、統合されたリアルタイムの Web トランザクション監視を提供することにより、Citrix ADC によって提供されるすべての Web アプリケーションを監視できます。SSL インサイトは、近似アルゴリズムを使用して Citrix ADC からの

データを処理します。企業内の Web トランザクションに関連するメトリックの上位 1,000 レコードを提供します。

役割ベースのアクセス制御

ロールベースのアクセス制御 (RBAC) を使用すると、企業内の個々のユーザーのロールに基づいて、アクセス許可を付与できます。Citrix Cloud 資格情報を使用してログオンする組織の最初のユーザーは、デフォルトですべてのアクセス許可を持つスーパー管理者の役割を持ちます。その組織の他のユーザーは、後で管理者によって作成され、管理者以外のロールが付与されます。

サブスクリプション

購入したサブスクリプションのダッシュボードビューを提供します。

デフォルトでは、エクスプレスアカウントに割り当てられます。このアカウントを使用すると、制限された ADM リソースを管理できます。詳しくは、「Express アカウントを使用して Citrix ADM リソースを管理する」を参照してください。

現在、以下の Citrix ADM 機能は使用できません。

- 展開
  - シトリックス Insight Center から Citrix ADM への移行
  - Citrix ADM と Citrix Virtual Desktop Director との統合
- ネットワーク:Citrix SD-WAN EE のサポート
- 分析:TCP Insight、Video Insight、WAN Insight
- 制限されたシステム設定
- オーケストレーション
  - OpenStack と VMware NSX マネージャーとの統合
  - Citrix ACI のハイブリッドモードでの Citrix ADC オートメーション
  - コンテナーオーケストレーション:Mesos/Marathon と Kubernetes との統合

システム要件

May 7, 2021

Citrix ADM（Citrix Application Delivery Management rix ADM）の使用を開始する前に、ソフトウェア要件、ブラウザー要件、ポート情報、ライセンス情報、制限事項を確認する必要があります。

サポートされているブラウザー

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

次のブラウザーがサポートされています。

Web ブラウザー	バージョン
Internet Explorer	11.0 以降
Google Chrome	Chrome 19 以降
Safari	Safari 5.1.1 以降
Mozilla Firefox	Firefox 3.6.25 以降

エージェントのインストール要件

ネットワーク環境にエージェントをインストールして構成し、データセンター内の Citrix ADM と管理対象のインスタンス間の通信を有効にします。オンプレミスのデータセンターでは、Citrix XenServer、VMware ESXi、Microsoft Hyper-V、Linux KVM サーバーにエージェントをインストールできます。

エージェント要件は、ハイパーバイザーが各 ADM 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です。次の表に、すべての ADM 機能を利用するためのエージェント要件を示します。

コンポーネント	条件
RAM	32GB
仮想 CPU	8
記憶域	30 ギガバイト
仮想ネットワークインターフェイス	1
スループット	1Gbps

プールされたライセンス機能だけを利用するためのエージェント要件については、プールライセンス用の軽量エージェントを参照してください。

Microsoft Azure、AWS、または Google クラウドにエージェントをインストールすることもできます。すべての ADM 機能を利用するには、各クラウドマーケットプレイスの次の仮想マシンタイプの使用をお勧めします。

クラウド	エージェント要件	優先する仮想マシンの種類
AWS	8 仮想 CPU、32 GB RAM、30 GB のストレージ容量	`m4.2xlarge`
Microsoft Azure	8 仮想 CPU、32 GB RAM、30 GB のストレージ容量	`Standard_D8s_v3`
グーグルクラウド	8 仮想 CPU、32 GB RAM、30 GB のストレージ容量	`e2-standard-8`

エージェントのインストール手順については、次のリンクを参照してください。

- Microsoft Azure クラウドへの Citrix の ADM エージェントのインストール。
- AWS に Citrix ADM エージェントをインストールする。
- Google クラウドへの Citrix ADM エージェントのインストール。

プールライセンス用の軽量エージェント

プールされたライセンスだけに ADM サービスを使用する予定の場合は、次の表に示されているように、より低い仕様のエージェントを使用できます。

コンポーネント	条件
RAM	8GB
仮想 CPU	4
記憶域	30 ギガバイト

より低い仕様（軽量）のこのようなエージェントは、ADM サービスでのみサポートされます。

プールされたライセンス機能のみを利用するには、各クラウドマーケットプレイスの次の仮想マシンタイプを使用することをお勧めします。

クラウド	エージェント要件	優先する仮想マシンの種類
AWS	4 仮想 CPU、8 GB RAM、30 GB のストレージ容量	`m4.xlarge`。このインスタンスタイプは、4 つの仮想 CPU、16 GB RAM、30 GB のストレージ容量を提供します。このインスタンスタイプは、既存のインスタンスタイプのエージェント要件の大部分と一致するため、このインスタンスタイプをお勧めします。
Microsoft Azure	4 仮想 CPU、8 GB RAM、30 GB のストレージ容量	`Standard_F4s_v2`
グーグルクラウド	4 仮想 CPU、8 GB RAM、30 GB のストレージ容量	`e2-standard-4`

> 注
>
> **[** 設定**] > [**システム設定**] > [**構成可能な機能**]** に移動して、既定のスケジューリングジョブを無効にする必要があります。

ポート

Citrix ADC インスタンスと Citrix ADM エージェント、または Citrix SD-WAN インスタンスと Citrix ADM エージェント間の通信では、Citrix ADM エージェントで次のポートを開く必要があります。

種類	ポート	詳細	コミュニケーションの方向
TCP	80/443	Citrix ADM から Citrix ADC または Citrix SD-WAN インスタンスへの NITRO 通信用です。443。高可用性モードの Citrix ADM サーバー間の NITRO 通信用。	Citrix ADM から Citrix ADC へ、Citrix ADC から Citrix ADM へ

種類	ポート	詳細	コミュニケーションの方向
TCP	22	Citrix ADM から Citrix ADC または Citrix SD-WAN インスタンスへの SSH 通信用です。高可用性モードで展開された Citrix ADM サーバー間の同期用。また、このポートは、ADM エージェントと Citrix ADC 間の SSH 通信に必要です。	Citrix ADM から Citrix ADC に、Citrix ADM エージェントは Citrix ADC に
UDP	4739	Citrix ADC または Citrix SD-WAN インスタンスから Citrix ADM への AppFlow ow 通信の場合。	Citrix ADC または Citrix SD-WAN から Citrix ADM へ
ICMP	予約されているポートなし	高可用性モードで展開された Citrix ADM と Citrix ADC インスタンス、SD WAN インスタンス、またはセカンダリ Citrix ADM サーバー間のネットワーク到達可能性を検出するため。	
UDP	161、162	Citrix ADC インスタンスから Citrix ADM に SNMP イベントを受信する。	ポート **161** -Citrix ADM から Citrix ADC へ
			ポート **162** -Citrix ADC から Citrix ADM へ
UDP	514	Citrix ADC または Citrix SD-WAN インスタンスから Citrix ADM への syslog メッセージを受信する。	Citrix ADC または Citrix SD-WAN から Citrix ADM へ

種類	ポート	詳細	コミュニケーションの方向
TCP	25	Citrix ADM からユーザーに SMTP 通知を送信する場合。	
TCP	5563	Citrix ADC インスタンスから Citrix ADC ADCitrix ADM への ADC メトリック（カウンタ）、システムイベント、監査ログメッセージを受信する。	Citrix ADC から Citrix ADM へ
TCP	5557/5558	Citrix ADC から Citrix **ADM** へのログストリーム通信（Security Insight、Web Insight インサイト、HDX Insight 用）の場合。	Citrix ADC から Citrix ADM へ
TCP	5454	高可用性モードの Citrix ADM ノード間の通信およびデータベース同期用のデフォルトポート。	Citrix ADM プライマリノードから Citrix ADM セカンダリノードへ
TCP	27000 と 7279	Citrix ADM ライセンスサーバーと ADC インスタンス間の通信用のライセンスポート。これらのポートは、ADC プールされたライセンスにも使用されます。	Citrix ADC から Citrix ADM へ
TCP	443/8443/7443	Citrix ADM エージェントと Citrix ADM 間の通信用のポート。ADM エージェントは、Citrix ADM との通信を開始します。	Citrix ADM エージェントから Citrix ADM への接続

Citrix ADM エージェントと Citrix ADM 間の通信では、Citrix ADM エージェントで次のポートが開いていることを確認します。

種類	ポート	詳細
HTTPS	443	Citrix ADM エージェントから Citrix ADM への通信用。

> 注:
>
> Citrix ADM エンドポイントは、エージェントを登録するときに生成された「サービス URL」と同じです。エージェントはサービス URL を使用して Citrix ADM を検索します。

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。

- ダウンロードサービス:

```
https://download.citrixnetworkapi.net
<!--NeedCopy-->
```

- 信頼サービス:

```
*.citrixnetworkapi.net
<!--NeedCopy-->
```

- サービス URL:

```
*.agent.adm.cloud.com
*.adm.cloud.com
adm.cloud.com
<!--NeedCopy-->
```

- ADC バックアップサービス:

```
adm-prod-backup-\*.s3.amazonaws.com
adm-prod-backup-\*.s3.*amazonaws.com
<!--NeedCopy-->
```

Citrix ADM エージェントと Citrix Analytics Services 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	US 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

非推奨の **FQDN**

一部の FQDN は、次の ADM サービスの使用のために廃止される予定です。中断せずに新しい FQDN に切り替えるために、非推奨の FQDN はしばらくの間動作し続け、徐々に段階的に廃止されます。

ADM サービスエンドポイント	古い完全修飾ドメイン名	新しい FQDN
ADM サービスの UI アクセス	netscalermas.cloud.com	adm.cloud.com
サービス URL	agent.netscalermgmt.net	*.agent.adm.cloud.com 注: * の値は、データが使用できる PoP (プレゼンスポイント) によって異なります。
API インタラクション	netscalermas.cloud.com	api.adm.cloud.com

最低限必要な **Citrix ADC** バージョン

> 注
>
> Citrix ADC バージョン 10.5、11.0、および 12.0 はすでに終了日（EOL）に達しています。詳しくは「製品マトリクス」を参照してください。推奨される ADC バージョンは 12.1 です。

Citrix ADM 機能	Citrix ADC ソフトウェアのバージョン
StyleBook	10.5 以降
ジョブを使用した監視/レポート作成と構成	10.5 以降
Analytics	
HDX Insight	10.1 以降
Gateway Insight	11.0.65.31 以降
Security Insight	11.0.65.31 以降

Citrix SD-WAN インスタンス管理の要件

最低限必要な **Citrix SD-WAN WANOP** バージョン

Citrix ADM 機能	Citrix CloudBridge/Citrix SD-WAN WO
ジョブを使用した監視/レポート作成および構成	Citrix CloudBridge 7.4.0 以降
Analytics	

Citrix ADM 機能	Citrix CloudBridge/Citrix SD-WAN WO
HDX Insight	Citrix CloudBridge 7.4.0 以降
WAN Insight	Citrix CloudBridge 7.4.0 以降

Citrix SD-WAN プラットフォームエディションと **Citrix ADM** 機能の操作性マトリックス

Platform Editions	検出中	構成	監視	レポート	イベント管理（SNMP トラップ）	HDX Insight と WAN Insight 分析	マルチホップインサイト
Citrix SD-WAN WANOP	はい	はい	はい	はい	はい	はい	はい

Citrix SD-WAN インスタンスでサポートされるシンクライアント

Citrix ADM は、Citrix SD-WAN 展開を監視するために、次のシンクライアントをサポートしています。

- Dell Wyse WTOS モデル R10L Rx0L シンクライアント
- NComputing N400
- Dell Wyse WTOS Model CX0 C00X Xenith
- Dell Wyse WTOS Model TXO T00X Xenith2
- Dell Wyse WTOS Model CX0 C10LE
- Dell Wyse WTOS Model R00LX Rx0L HDX Thin Client
- Dell Wyse Enhanced SUSE Linux Enterprise, Model Dx0D, D50D
- Dell Wyse ZX0 Z90D7 (WES7) Thin Client

Citrix ADM 分析ソリューションの要件

最低限必要な **Citrix Virtual Apps and Desktops** のバージョン

Citrix ADM 機能	Citrix Virtual Apps and Desktops バージョン
HDX Insight	Citrix Virtual Apps and Desktops 7.0 以降

> 注
>
> Citrix ADC インスタンスでは、Citrix Gateway 機能（バージョン 9.3 および 10.x ではアクセスゲートウェイエンタープライズとしてブランドされている）が使用可能である必要があります。Citrix ADM では、スタンドアロンのアクセスゲートウェイ標準アプライアンスはサポートされません。

Citrix ADM では、Citrix Virtual App またはデスクトップに公開され、Citrix Receiver 経由でアクセスされるアプリケーションのレポートを生成できます。ただし、この機能は Receiver がインストールされているオペレーティングシステムによって異なります。現在、Citrix ADC は、iOS または Android オペレーティングシステム上で動作する Citrix Receiver を介してアクセスされるアプリケーションやデスクトップの ICA トラフィックを解析しません。

HDX Insight でサポートされるシンクライアント

Citrix ADM は、ソフトウェアバージョン 11.0 ビルド 65.31 以降で実行されている Citrix ADC インスタンスを監視するために、次のシンクライアントをサポートしています。

- Dell Wyse Windows ベースのシンクライアント
- Dell Wyse Linux ベースのシンクライアント
- Dell Wyse ThinOS ベースのシンクライアント
- 10ZiG Ubuntu ベースのシンクライアント

HDX Insight には **Citrix ADC** インスタンスライセンスが必要です

Citrix ADM for HDX Insight によって収集されるデータは、監視対象の Citrix ADC インスタンスのバージョンとインストールされているライセンスによって異なります。HDX Insight レポートは、ソフトウェアバージョン 10.5 以降で実行されている Citrix ADC プレミアムおよびエンタープライズアプライアンスに対してのみ表示されます。

Citrix ADC ライセンス/期間	5 分	1 時間	1 日	1 週間	1 か月超
標準	いいえ	いいえ	いいえ	いいえ	いいえ
詳細設定	はい	はい	いいえ	いいえ	いいえ
Premium	はい	はい	はい	はい	はい

サポートされているオペレーティングシステムと **Citrix Receiver** バージョン

次の表に、Citrix ADM でサポートされているオペレーティングシステムと、各システムで現在サポートされている Citrix Receiver のバージョンを示します。

オペレーティングシステム	Receiver バージョン
Windows	4.0 Standard Edition
Linux	13.0.265571 以降
Mac	11.8、Build 238301 以降
HTML5	1.5*
Chrome アプリ	1.5*

* Citrix CloudBridge リリース 7.4 以降に適用されます。

ライセンス

May 7, 2021

Citrix ADC インスタンスを管理および監視するには、Citrix ADM 認証済みの Citrix ADM ライセンスが必要です。

Citrix ADM for Services でサポートされているライセンスの種類は次のとおりです。

ライセンスの種類	権利がある
仮想サーバ	ライセンスごとに 10 台の仮想サーバと 5 GB のストレージ
ストレージ	ライセンスあたり 5 GB
エクスプレスライセンス	Citrix ADM Express アカウントは、ADM リソースを管理するデフォルトのアカウントです。

Express アカウントを使用すると、制限された ADM リソースを管理できます。詳しくは、「Express アカウントを使用して Citrix ADM リソースを管理する」を参照してください。

購入したライセンスの有効期限が切れると、60 日間の猶予期間が与えられます。猶予期間中は、Express アカウントを使用して管理できる ADM リソースを選択できます。

Express アカウントの使用を開始する方法の詳細については、「はじめに」および「サブスクリプションの管理」を参照してください。「サブスクリプションの管理」を参照してください。

ライセンスを追加する

> 注:
>
> Citrix ADC インスタンスには、プールされたライセンスのみを追加できます。

Citrix ADM では、Citrix ADC インスタンスのプールライセンスを追加できます。ライセンスを追加したら、[アカウント] > [サブスクリプション] でライセンス情報を確認できます。

プールされたライセンスを追加するには:

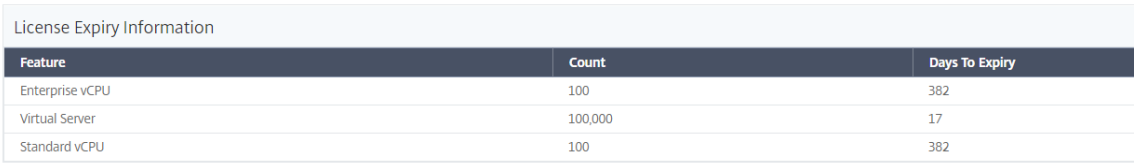
1. [ネットワーク] > [ライセンス] に移動します。
2. [**Get Licenses**] をクリックして、ローカルコンピュータからライセンスファイルを選択します。
3. ライセンスファイル（.lic）を選択し、[**OK**] をクリックします。

仮想サーバライセンスの有効期限チェック

Citrix ADM でライセンスの有効期限のステータスを表示し、アラートを設定できるようになりました。

ライセンスのステータスを表示するには、次の手順に従います。

1. [ネットワーク] > [ライセンス] に移動します。
2. [ライセンスの有効期限情報] セクションでは、有効期限が切れる予定のライセンスの詳細を確認できます。


License Expiry Information

Feature	Count	Days To Expiry
Enterprise vCPU	100	382
Virtual Server	100,000	17
Standard vCPU	100	382

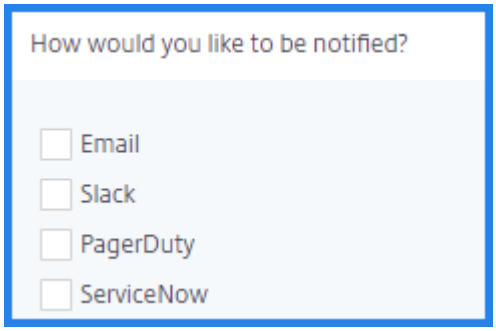
   - 機能: 有効期限が切れるライセンスの種類。
   - カウント: 影響を受けるインスタンスの数。
   - 有効期限までの日数**:** 有効期限が切れるまでの残り日数。

ライセンスの通知設定を構成するには:

1. [ネットワーク] > [ライセンス] に移動します。
2. [通知設定] セクションで、鉛筆アイコンをクリックし、パラメータを編集します。
   a) どのような通知を受け取りたいですか**?** -容量の割合を指定します。
   b) どのように通知を受け取りたいですか**?** -次の通知オプションを選択します。
      - **Email** - メールサーバーとプロファイルの詳細を指定します。ライセンスの有効期限が近づくと、メールがトリガーされます。
      - **slack** slack プロファイルを指定します。ライセンスの有効期限が近づくと、通知が送信されます。
      - **PagerDuty** -PagerDuty プロファイルを指定します。PagerDuty ポータルで構成された通知設定に基づいて、ライセンスの有効期限が近づくと通知が送信されます。

- **ServiceNow** -ライセンスの有効期限が近づくと、デフォルトの ServiceNow プロファイルに通知が送信されます。

  > 重要:
  >
  > Citrix Cloud ITSM アダプタが ServiceNow 用に構成され、Citrix ADM サービスと統合されていることを確認します。詳しくは、「Citrix ADM サービスと ServiceNow インスタンスの統合」を参照してください。



c) ライセンスの有効期限-ライセンスの有効期限が切れる前の日を指定します。

Express アカウントを使用して Citrix ADM リソースを管理する

May 7, 2021

Citrix ADM Express アカウントは、ADM リソースを管理するデフォルトのアカウントです。このアカウントは、Citrix Cloud で簡単に利用できます。

このアカウントには、選択した次の ADM リソースを管理するためのオプションが用意されています。

- 最大 2 台の仮想サーバ
- 最大 2 つの設定ジョブ
- StyleBook の設定パックを最大 2 つ

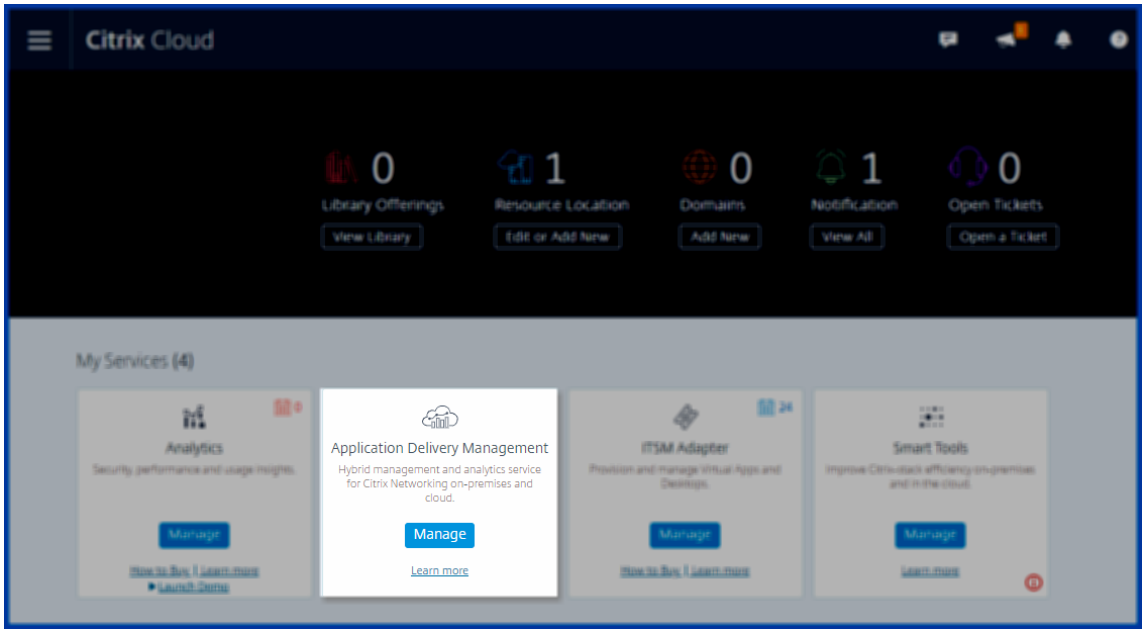
Express アカウントで特定のリソースを管理するには、猶予期間中に必要なリソースを選択する必要があります。リソースを選択しない場合、ADM サービスは Express アカウントで管理できるリソースを自動的に選択します。

> 重要
>
> - アカウントを Express アカウントに変換すると、ADM サービスは最大 500 MB または 1 日のデータのいずれか小さい方のストレージデータを保持します。
> - Citrix ADM Express アカウントが 90 日間非アクティブのままの場合、アカウントは削除されます。Citrix ADM チームは、非アクティブ状態が 60 日後にリマインダーを送信します。

ADM リソースを管理するには、次の手順に従います。

1. 資格情報を使用して Citrix Cloud にログオンします。

2. [**Citrix Application Delivery Management**] タイルで [管理] をクリックします。



Citrix ADM サブスクリプションライセンスと猶予期間が終了すると、ライセンスを更新しない限り、アカウントは Express アカウントに変換されます。Express アカウントを使用すると、Citrix ADM サービスを使用してビジネスを継続できます。Citrix ADM ライセンスを更新するには、Citrix Cloudにアクセスするか、テクニカルサポートにお問い合わせください。

サブスクリプションの管理

May 7, 2021

Citrix Application Delivery Management ADM（Citrix ADM）では、Citrix ADC インスタンス、Citrix Gateway インスタンス、およびサードパーティのロードバランサーを管理および監視するために、検証済みのライセンスが必要です。

Express アカウントを使用しているとき、または有効なライセンスを登録している場合は、任意の数のインスタンスを管理および監視できます。ただし、アプリダッシュボードで検出されたアプリケーションの管理、分析データの表示、ネットワーク機能およびネットワークレポートの監視は、ライセンスを購入した仮想サーバーの数に対してのみ行うことができます。Express アカウントで管理できる ADM リソースの詳細については、「Citrix ADM Express アカウント」を参照してください。

インストールされたライセンスごとに、特定の仮想サーバを管理するためのデータと容量が制限されます。ただし、データのみのライセンスを購入して適用し、データストレージを最大化することもできます。

Citrix ADM ライセンスの購入とアップグレードの詳細については、「Citrix Application Delivery Management」を参照してください。

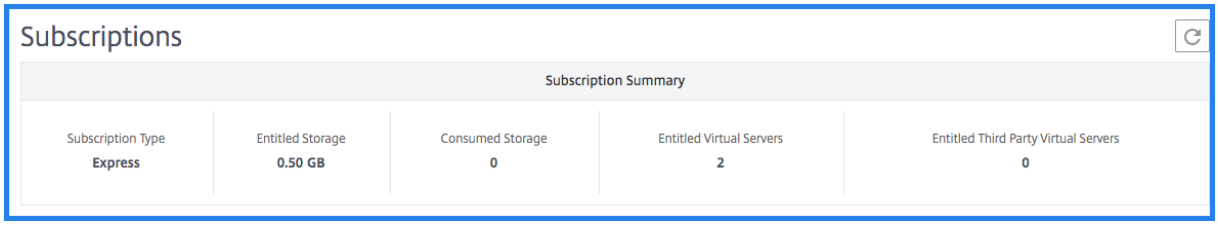
次の表に、Citrix ADM の一部の機能を使用するために必要な Citrix ライセンスを示します。

Citrix ADM 機能グループ	Citrix ADM 機能	Citrix ADC および Gateway のライセンス要件
Analytics	HDX Insight	詳細（レポート作成時間 1 時間以内）プレミアム（レポート作成時間 = 無制限）
Analytics	Security Insight	プレミアム（または）アドバンスド（App Firewall）ライセンス
Analytics	Gateway Insight	詳細（レポート作成時間 1 時間以内）プレミアム（レポート作成時間 = 無制限）
アプリケーション	アプリケーション統計情報（アプリダッシュボード、アプリセキュリティダッシュボード）	アプリダッシュボードおよびアプリセキュリティダッシュボードの Citrix Web App Firewall 関連情報には、Premium（または）App ファイアウォールライセンスで詳細設定が必要です
アプリケーション	API Gateway	プレミアム (または) アドバンスライセンス
アプリケーション	StyleBook	-
アプリケーション	インベントリ管理 — インフラストラクチャダッシュボード、インスタンスグループ、インスタンスダッシュボード、サイト	-
アプリケーション	イベント管理および syslog	-
アプリケーション	構成ジョブ、構成監査、および構成アドバイス	-
アプリケーション	ネットワークレポート（インスタンスレベル）	-
アプリケーション	ネットワークレポート (仮想サーバーレベル)	-
アプリケーション	ネットワーク機能（仮想サーバ、サービス、サービスグループ、サーバのシンプルな可視性と管理）	-
アプリケーション	SSL 証明書管理（インスタンスレベル）	-

Citrix ADM 機能グループ	Citrix ADM 機能	Citrix ADC および Gateway のライセンス要件
アプリケーション	SSL 証明書管理 (仮想サーバーレベル)	N/A
システム	RBAC および外部認証（インスタンスレベル）	N/A
システム	RBAC と外部認証 (仮想サーバーレベル)	N/A

サブスクリプションの詳細を表示する

Citrix ADM にインストールされているライセンスを表示するには、［アカウント］>［サブスクリプション］に移動します。サブスクリプションの概要セクションには、サブスクライブしているライセンスの種類、資格のあるデータサブスクリプションと消費されたデータサブスクリプション、許可および管理されている仮想サーバーとサードパーティ仮想サーバーなどのライセンスの概要も表示できます。



サードパーティ仮想サーバーのサブスクリプションの管理

試用期間中または有効なライセンスを購読しているときに、任意の数の HAProxy ホストを管理および監視できます。ただし、HAProxy App Dashboard で検出されたアプリケーションの管理、分析データの表示、ネットワーク機能の監視は、ライセンスを購入したサードパーティの仮想サーバーの数に対してのみ実行できます。試用期間中は、サードパーティの仮想サーバーまたはアプリケーションを 10 台だけ監視できます。

> 注
>
> このドキュメントでは、サードパーティの仮想サーバーは HAProxy フロントエンドを参照します。

仮想サーバの管理

Citrix ADM を使用して管理および監視する仮想サーバーまたはサードパーティ仮想サーバーを選択できます。

注意事項**:**

- デフォルトでは、Citrix ADM は、仮想サーバーのポーリングサイクルごとに仮想サーバーのライセンスをランダムに自動的に付与します。

- Citrix ADM で検出された仮想サーバーの合計数が、インストールされている仮想サーバーライセンスの数よりも少ない場合、Citrix ADM はデフォルトですべての仮想サーバーをライセンスします。

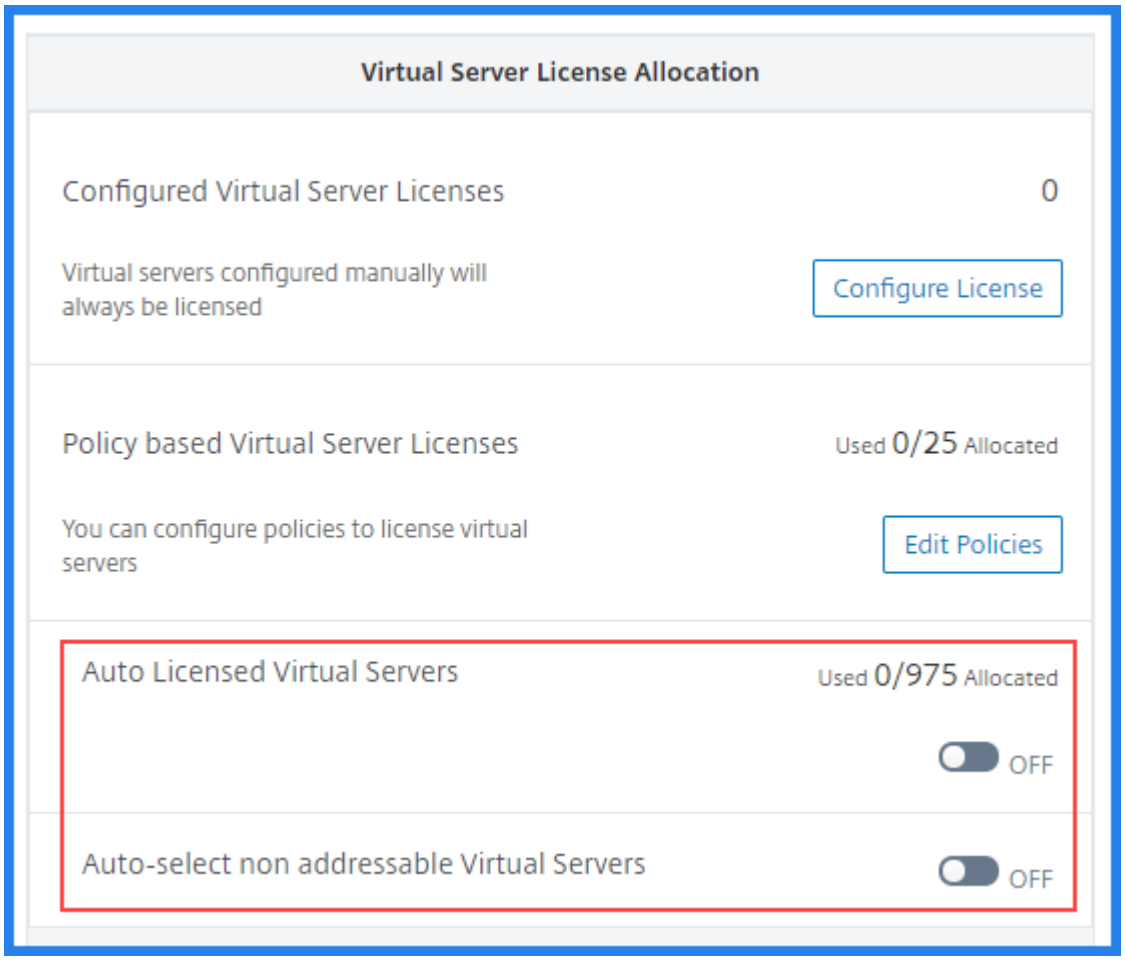
仮想サーバーを手動で選択するかライセンスの割り当て対象を一部の仮想サーバーのみに制限するには、まず仮想サーバーへの自動ライセンス割り当てを無効化してから、管理する仮想サーバーを選択する必要があります。

自動ライセンス仮想サーバーを無効にするには、次の手順に従います。

1. 「アカウント」**>**「購読」に移動します。

   ダッシュボードには、使用可能な仮想サーバライセンス、管理対象仮想サーバ、および仮想サーバタイプ、およびライセンスの有効期限情報が表示されます。

2. [仮想サーバーライセンス割り当て] で、自動ライセンス仮想サーバーを無効にし、アドレス指定できない仮想サーバーを自動的に選択します。

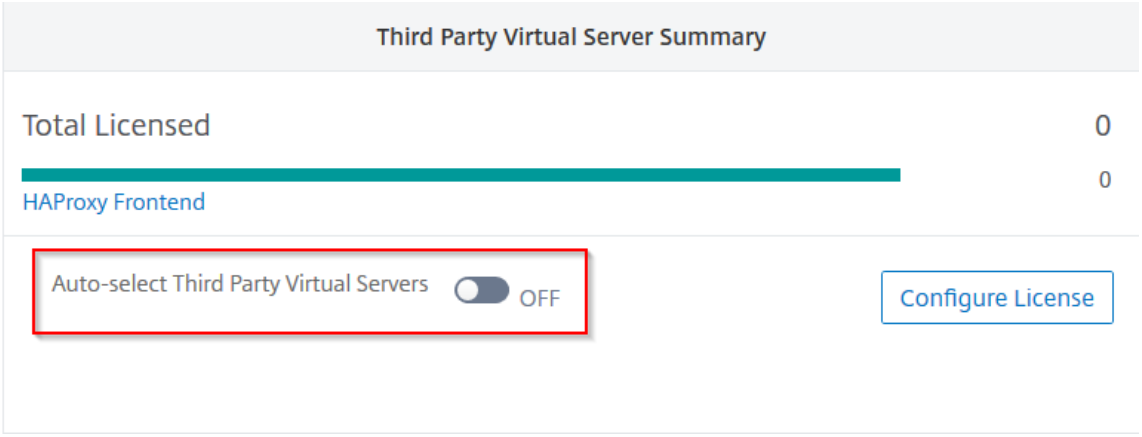


ライセンスを取得するサードパーティ仮想サーバーを選択するには、次の手順に従います。

1. 「アカウント」>「購読」に移動します。

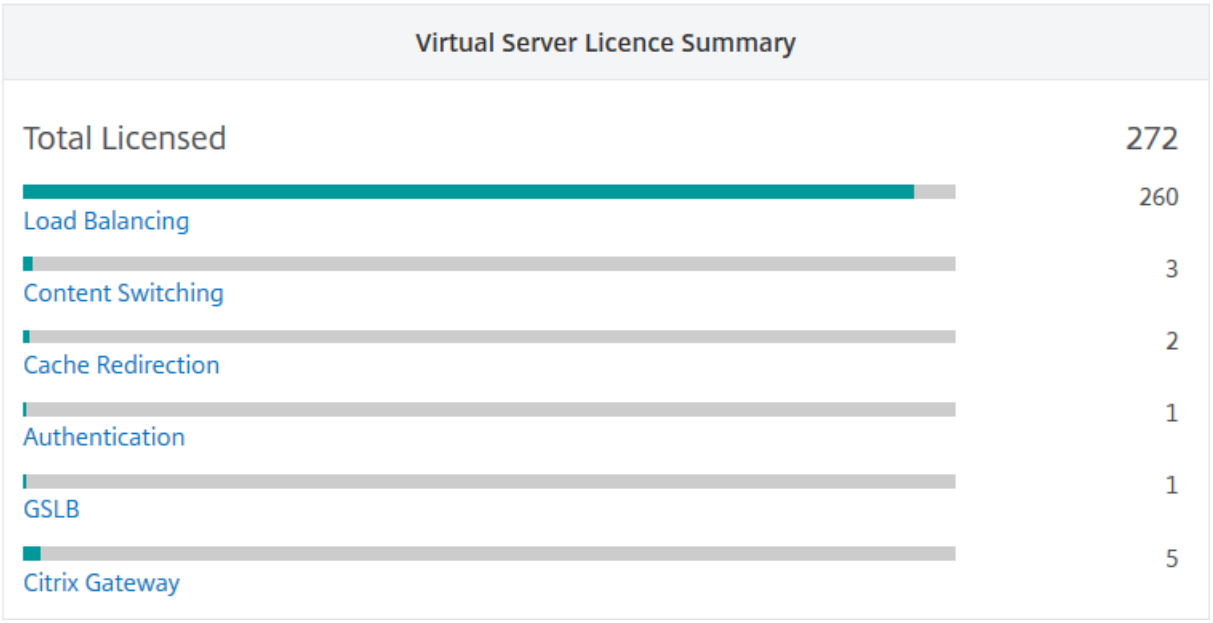
   ダッシュボードには、使用可能な仮想サーバライセンス、管理対象仮想サーバ、および仮想サーバタイプ、およびライセンスの有効期限情報が表示されます。

2. [サードパーティ仮想サーバーの概要] で、**[**サードパーティ仮想サーバーの自動選択**]** を無効にします。



ライセンスされた仮想サーバの表示

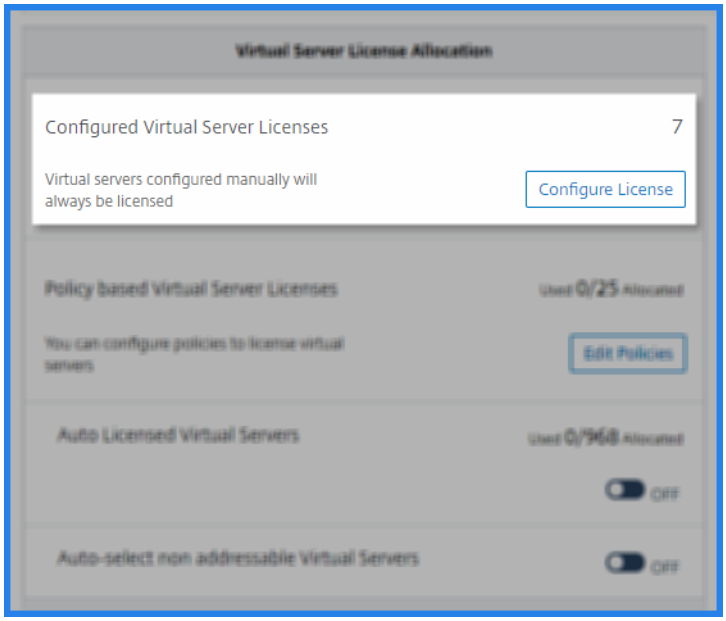
ライセンスが仮想サーバーに適用されると、ライセンスされた仮想サーバーまたはサードパーティ仮想サーバーを [サブスクリプション] ページから表示できます。ライセンスされた仮想サーバーを表示するには、**[** アカウント**] > [**サブスクリプション**]** に移動し、**[**仮想サーバーライセンスの概要**]** の **[** ライセンス合計**]** セクションで仮想サーバータイプをクリックします。



仮想サーバライセンスを手動で適用する

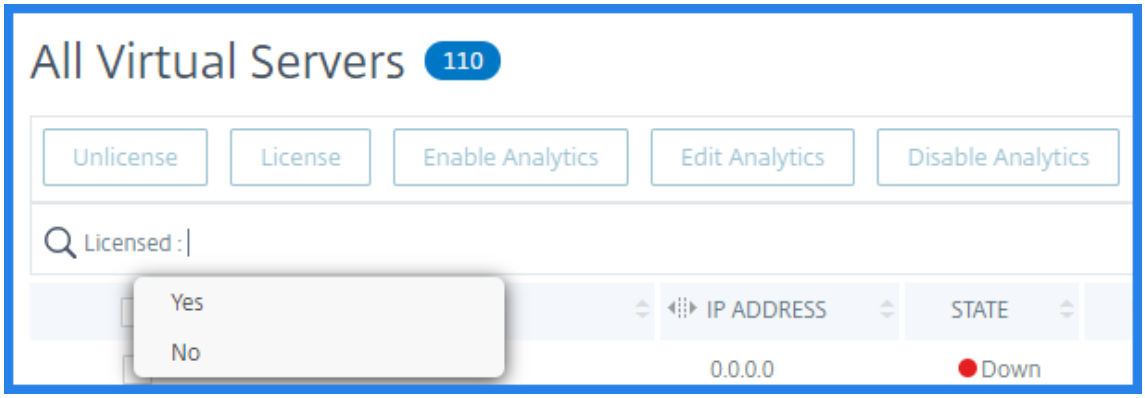
個々の仮想サーバにライセンスを手動で適用できます。

1. [仮想サーバーライセンスの割り当て] で、[ライセンスの構成] を選択します。



[すべての仮想サーバー] ページが表示されます。

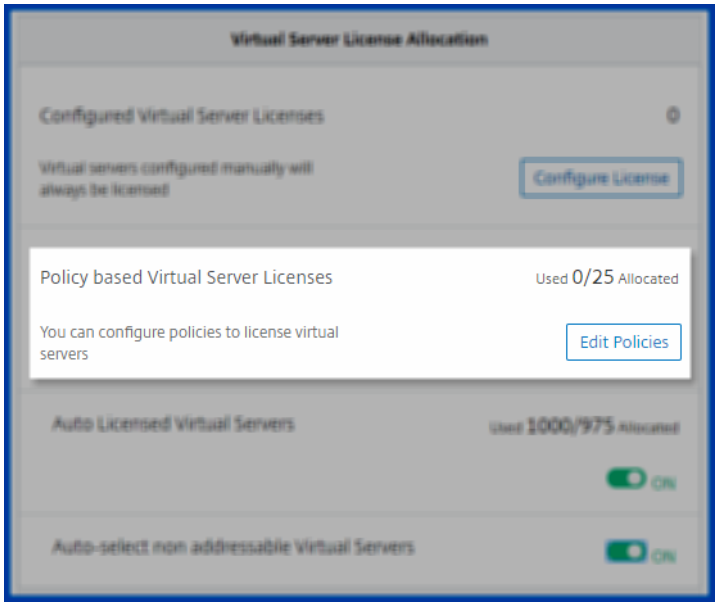
2. プロパティを使用して、ライセンスされていない仮想サーバをフィルタリングします。`Licensed: No`。



3. ライセンスを取得する仮想サーバーを選択します。
4. [ライセンス] をクリックします。

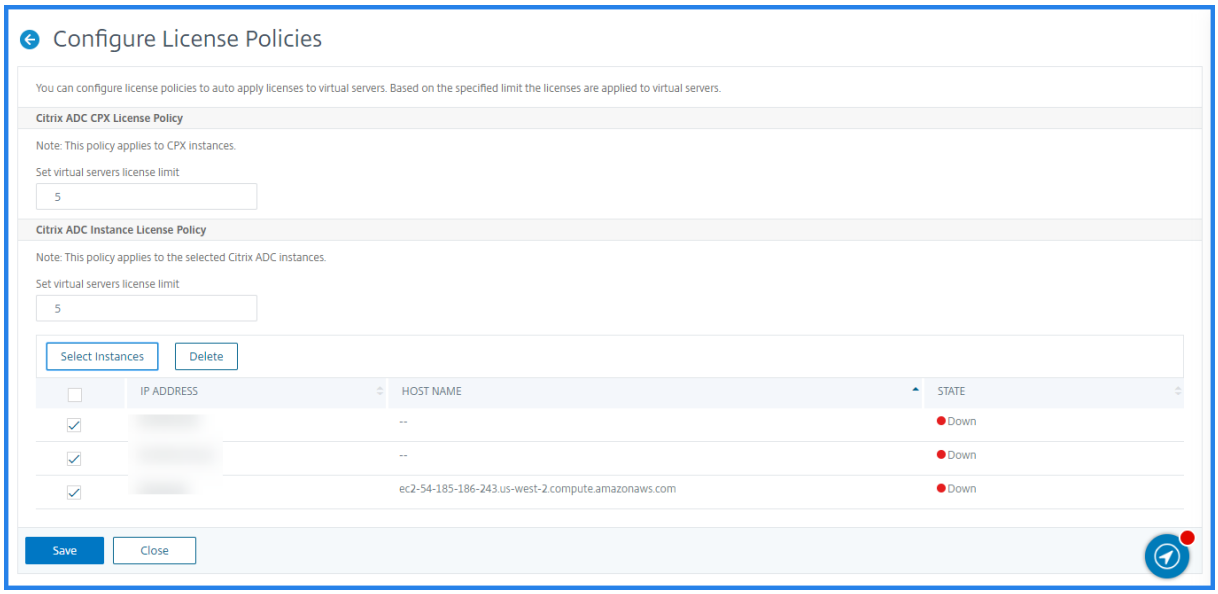
ポリシー・ベースの仮想サーバ・ライセンスの構成

仮想サーバーにライセンスを適用するポリシーを設定できます。このポリシーは、自動ライセンスを取得する仮想サーバの数を制御します。また、選択したインスタンスの仮想サーバーにのみライセンスが適用されます。



[ポリシーの編集] をクリックすると、次の項目を指定できます。

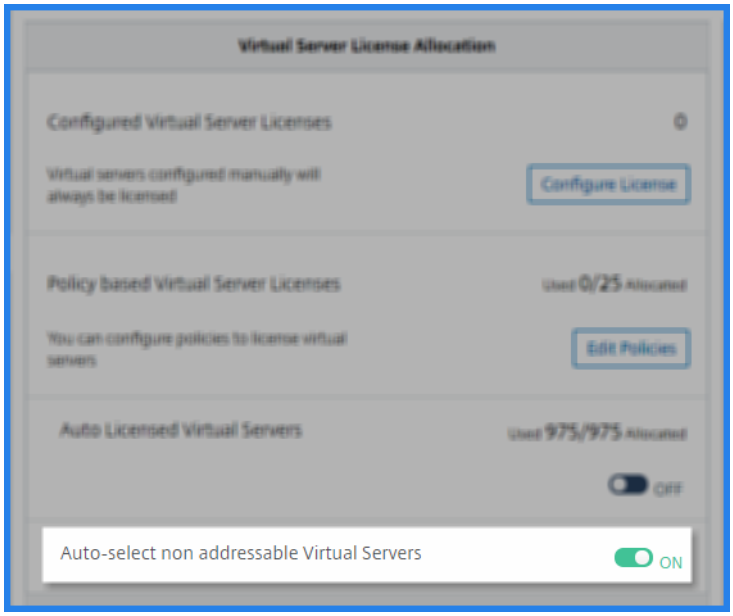
- CPX インスタンスに仮想サーバーの制限を個別に設定して、ライセンスを適用します。ADM は、指定された制限まで CPX インスタンス上の仮想サーバーにライセンスを適用します。
- ライセンスを適用するために、選択した ADC インスタンス（MPX/VPX/BLX）に仮想サーバーの制限を設定します。ADM は、指定された制限まで ADC インスタンス上の仮想サーバーにライセンスを適用します。
- 仮想サーバライセンスを適用する優先順位 ADC インスタンスを選択します。したがって、ADM は、選択したインスタンスの仮想サーバーにのみライセンスを適用できます。



アドレス指定できない仮想サーバーの自動ライセンスサポートを構成する

デフォルトでは、Citrix ADM は、アドレス指定できない仮想サーバーにライセンスを自動的に適用しません。アドレス指定不可の仮想サーバをライセンスする場合は、自動ライセンスオプションを無効にし、アドレス指定不可の仮想サーバを手動で選択する必要があります。これにより、ライセンスを適用するときに、最初にアドレス指定できないサーバを手動で選択する必要がなくなります。また、ネットワークに追加されるたびに、アドレス指定不可能な新しい仮想サーバを手動で選択する必要があります。

Citrix ADM は、Citrix ADM 仮想サーバーライセンス割り当てのオプションを提供します。アドレス指定不可仮想サーバーの自動選択オプションを有効にすると、アドレス指定不可仮想サーバーのライセンスを自動的に適用します。



> 注
>
> - Citrix ADM は、デフォルトでは、アドレス指定できない仮想サーバーをライセンス用に自動的に選択しません。
> - アプリケーション分析（App Dashboard）は、ライセンスされたアドレス指定不可能な仮想サーバーで現在サポートされている唯一の分析です。

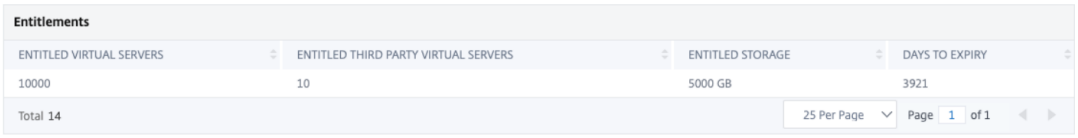
仮想サーバーサブスクリプションの有効期限チェックの表示

Citrix ADM では、インストールされているライセンスの状態を、有効期限と許可されたストレージ制限とともに表示できます。

ライセンスのステータスを表示するには、次の手順に従います。

1. 「アカウント」>「購読」に移動します。
2. [**Entitlements**] セクションでは、ライセンスされた仮想サーバーの詳細と有効期限の日付を表示できます。
    - 資格のある仮想サーバー**:** ライセンス取得可能な仮想サーバーの数。

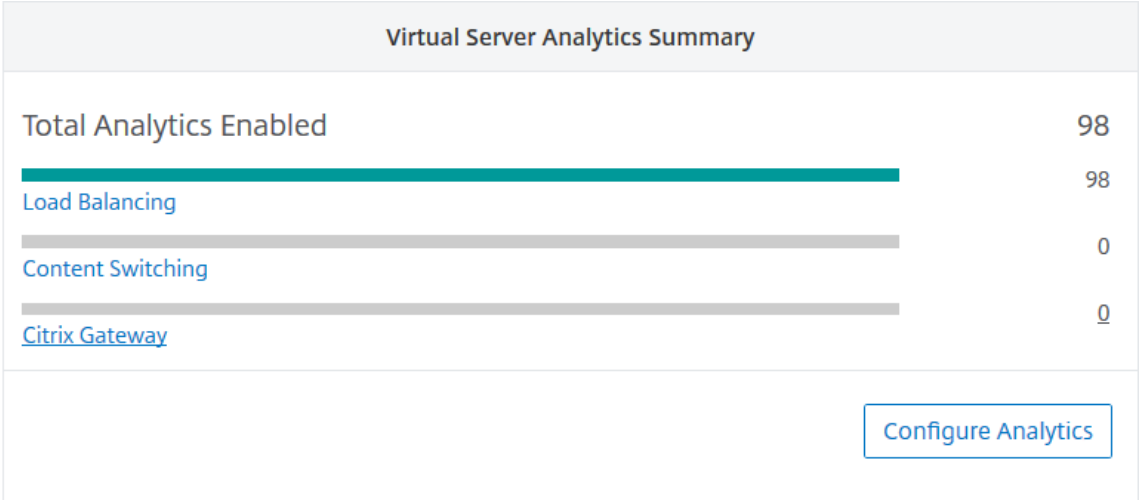
- 資格のあるサードパーティ仮想サーバー**:** ライセンスで管理できるサードパーティ仮想サーバーの数。
- 資格のあるストレージ**:** ライセンスのストレージ制限。
- 有効期限までの日数**:** ライセンスの有効期限までの残り日数。



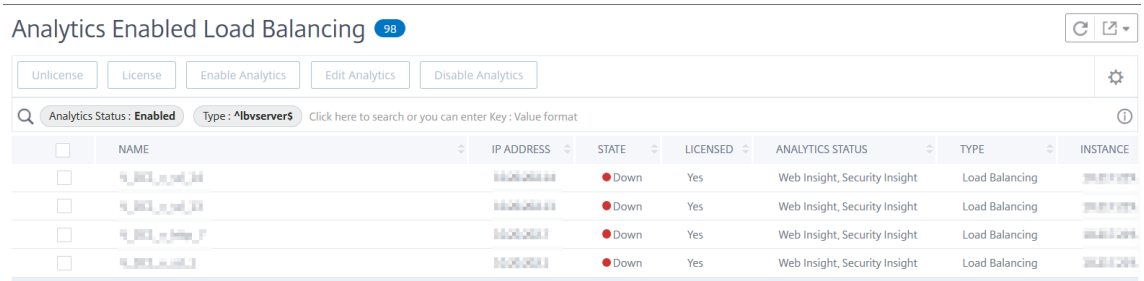
仮想サーバーで有効になっている分析の種類を表示する

選択した仮想サーバーで AppFlow を有効にした後、ライセンスされた仮想サーバーまたはサードパーティ仮想サーバー上で有効になっている分析の種類を [サブスクリプション] ページから表示できます。

1. 「アカウント」>「購読」に移動します。
2. [仮想サーバー分析の概要] セクションで、ライセンスされた仮想サーバーのタイプを選択します。



3. [ライセンスされた仮想サーバ] ページには、ライセンスされた仮想サーバのリストが表示されます。このページの [**Analytics Status**] 列には、仮想サーバーで有効になっている分析の種類が表示されます。



セットアップする

May 7, 2021

初期セットアップが完了したら、配置を完全に管理するには、特定の設定を構成する必要があります。

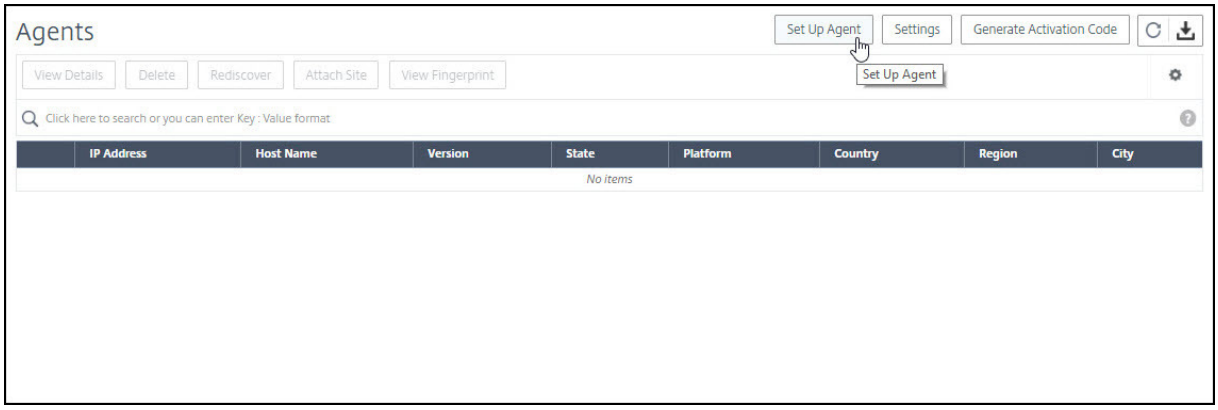
- 複数のエージェントの追加。インストールするエージェントの数は、データセンターまたはクラウド内の管理対象インスタンスの数および総スループットによって異なります。各データセンターに少なくとも 1 つのエージェントをインストールすることをお勧めします。
- インスタンスの追加。の Citrix ADM を設定している間、はじめてはまたは後でインスタンスを追加できます。インスタンスの管理と監視を開始するには、サービスにインスタンスを追加する必要があります。複数のエージェントをインストールしたら、インスタンスを追加してエージェントに関連付ける必要があります。
- アナリティクスの有効化。アプリケーショントラフィックフローの分析データを表示するには、特定のアプリケーションのトラフィックを受け取る仮想サーバーの分析機能を有効化する必要があります。
- インスタンスでの syslog の設定。すべての syslog メッセージを Citrix ADM にリダイレクトするようにデバイスを構成している場合は、Citrix ADC インスタンスで生成された syslog イベントを監視できます。syslog イベントを監視するには、まず Citrix ADM を Citrix ADC インスタンスの syslog サーバーとして構成する必要があります。
- ロールベースのアクセス制御の設定。Citrix ADM は、きめ細かな役割ベースのアクセス制御（RBAC）を提供し、企業内の個々のユーザーの役割に基づいてアクセス許可を付与できます。
- アナリティクス設定の構成。アナリティクス機能で最適なエクスペリエンスを確保するために、特定の設定を構成できます。たとえば、履歴分析データを保存する期間を指定できます。また、しきい値とアラートを設定して、必要な分析メトリックスを監視することもできます。

複数のエージェントの追加

May 7, 2021

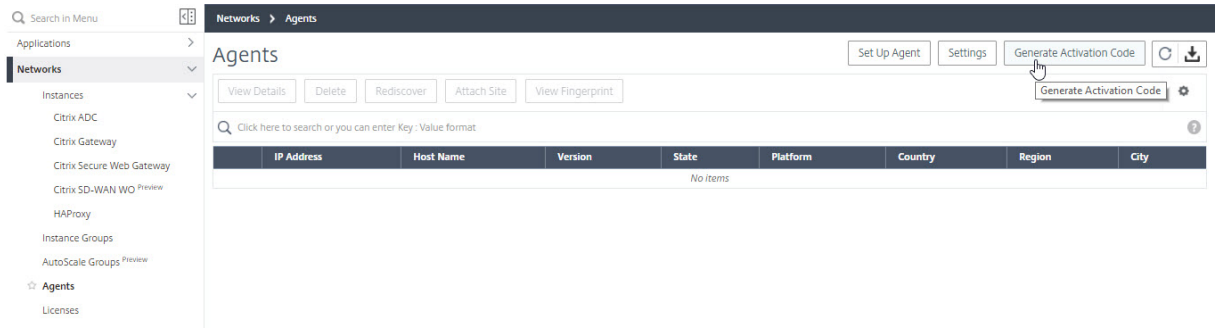
インストールするエージェントの数は、データセンター内の管理対象インスタンスの数と総スループットによって異なります。各データセンターに少なくとも 1 つのエージェントをインストールすることをお勧めします。

サービスに初めてログオンするときは、エージェントを 1 つだけインストールできます。複数のエージェントを追加するには、最初に初期セットアップを完了してから、[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] をクリックします。



必要な Hypervisor のイメージをダウンロードし、[はじめに。] の手順どおりにエージェントをインストールします。(/en-us/citrix-application-delivery-management-service/getting-started.html) 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する必要があるため、サービス URL と画面に表示されるアクティベーションコードを必ずコピーしてください。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。

同じイメージを使用して、ハイパーバイザーに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。エージェントをインストールしたら、次のエージェントのアクティベーションコードを再度生成します。新しいアクティベーションコードを生成するには、[ネットワーク**] > [**エージェント] に移動し、[アクティベーションコードの生成] をクリックします。



エージェントのインストールと登録に成功したら、サービス GUI でエージェントステータスを確認し、そのエージェントにインスタンスを追加します。

> 注
>
> Microsoft Azure クラウドまたは AWS クラウドに Citrix ADM エージェントをインストールすることもできます。エージェントイメージは、それぞれのクラウドマーケットプレイスで入手できます。
>
> - Microsoft Azure クラウドにエージェントをインストールする方法については、「Microsoft Azure クラウドへの Citrix ADM エージェントのインストール」を参照してください。
> - AWS にエージェントをインストールする手順については、「AWS に Citrix ADM エージェントをインストールする」を参照してください。

マルチサイト展開用に **Citrix ADM** エージェントを構成する

May 7, 2021

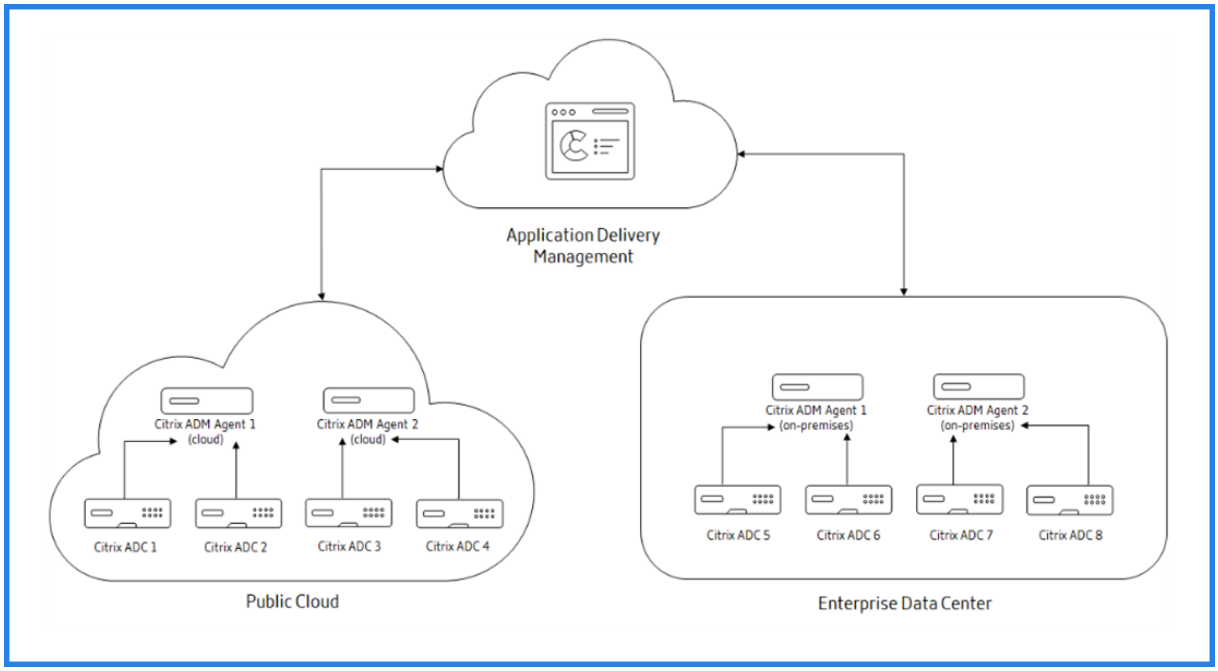
エージェントは、異なるデータセンターやパブリッククラウドにまたがる Citrix ADM サービスと検出されたインスタンスの間の仲介者として動作します。Citrix ADM は、データセンターまたはパブリッククラウド内でのエージェントのフェイルオーバーをサポートします。

エージェントをインストールすると、次のようなメリットがあります。

- エージェントに対して構成されたインスタンスは、処理されていないデータを Citrix ADM サービスの代わりにエージェントに直接送信します。エージェントは第 1 レベルのデータ処理を行い、処理されたデータを圧縮形式で Citrix ADM に送信して保管します。
- エージェントとインスタンスは同じデータセンターまたはクラウドに共存しているため、データ処理が高速化されます。
- エージェントをクラスタリングすると、エージェントのフェイルオーバー時に Citrix ADC インスタンスが再配布されます。サイト内の 1 つのエージェントに障害が発生すると、Citrix ADC インスタンスからのトラフィックは、同じサイト内の別の利用可能なエージェントに切り替わります。

アーキテクチャ

次の図は、エージェントのフェイルオーバーを実現するために、データセンターおよびパブリッククラウド内の複数のエージェントで構成された Citrix ADC インスタンスを示しています。



パブリッククラウドには、4 つの ADC インスタンスと 2 つの ADM エージェントがあります。エンタープライズデ

ータセンターには、4 つの ADC インスタンスと 2 つの ADM エージェントがあります。各エージェントは、2 つの ADC インスタンスで構成されます。

エージェントは、構成されたインスタンスから直接データを受信します。エージェントがデータを受信すると、エージェントはデータを処理し、圧縮形式で Citrix ADM サービスに送信します。エージェントは、安全なチャネルを介して Citrix ADM サーバーと通信します。

パブリッククラウドでは、**Citrix ADM Agent 1** が非アクティブ（DOWN 状態）になると、エージェントのフェイルオーバーが発生します。Citrix ADM サービスは、**Citrix AD M** エージェント **1** の ADC インスタンスを **Citrix ADM** エージェント **2** で再配布します。インスタンスの再配布は、データセンターでエージェントの 1 つに障害が発生した場合に、エンタープライズデータセンターで実行されます。

Citrix ADM エージェントをインストールするには、Citrix ADM エージェントをインストールするを参照してください。

Citrix ADM エージェントのフェイルオーバー

エージェントのフェールオーバーは、2 つ以上の登録済みエージェントがあるサイトで発生する可能性があります。サイト内でエージェントが非アクティブ（DOWN 状態）になると、Citrix ADM サービスは、非アクティブなエージェントの ADC インスタンスを他のアクティブなエージェントに再配布します。

> 重要
>
> - Citrix ADM エージェントのフェイルオーバーでは、CPX インスタンスは考慮されません。
> - アカウントで、エージェントのフェイルオーバー機能が有効になっていることを確認します。この機能を有効にするには、ADM 機能の有効化または無効化を参照してください。
> - エージェントがスクリプトを実行している場合は、サイト内のすべてのエージェントにスクリプトが存在することを確認します。したがって、変更されたエージェントは、エージェントのフェイルオーバー後にスクリプトを実行できます。

Citrix ADM GUI でサイトをエージェントに接続するには:

1. [ネットワーク**] > [**エージェント**]** に移動します。
2. サイトに接続するエージェントを選択します。
3. リストからサイトを指定します。新しいサイトを追加する場合は、[追加] をクリックします。
4. [保存] をクリックします。

エージェントのフェイルオーバーを実現するには、Citrix ADM エージェントを 1 つずつ選択し、同じサイトに接続します。

たとえば、2 つのエージェント 10.106.1xx.2x と 10.106.1xx.7x がバンガロールサイトで接続され、動作しています。1 つのエージェントが非アクティブになると、Citrix ADM はエージェントを検出し、その状態を down と表示します。

サイトで Citrix ADM エージェントが非アクティブ（ダウン状態）になると、Citrix ADM エージェントがアクティブ（アップ状態）になるまで数分間待機します。エージェントが非アクティブのままである場合、Citrix ADM は、同じサイト内の利用可能なエージェント間でインスタンスを自動的に再配布します。この再配布には、約 10 ～15 分かかります。

Citrix ADM では、30 分ごとにインスタンスの再配布がトリガーされ、サイト内のアクティブなエージェント間で負荷が分散されます。

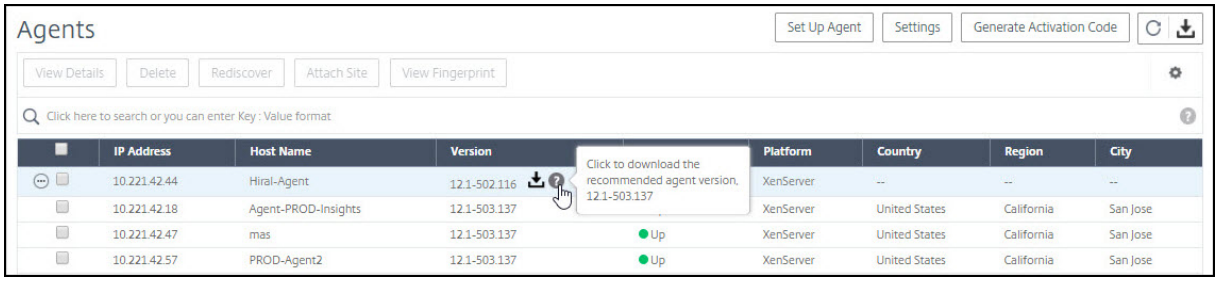
インスタンスは、トラップ宛先、syslog サーバー、および分析用に同じサイトのエージェントにアタッチされ、自動的に再構成されます。

エージェントのアップグレード設定の構成

May 7, 2021

Citrix ADM では、ソフトウェアバージョン 12.0 ビルド 507.110 以降で実行されているエージェントは、Citrix ADM によって新しい推奨バージョンに自動的にアップグレードされます。エージェントは、新しいバージョンが利用可能になったとき、またはユーザーが指定した時刻にアップグレードされます。

[ネットワーク **] >** [エージェント]** に移動すると、エージェントの現在のバージョンと推奨バージョンを表示できます。



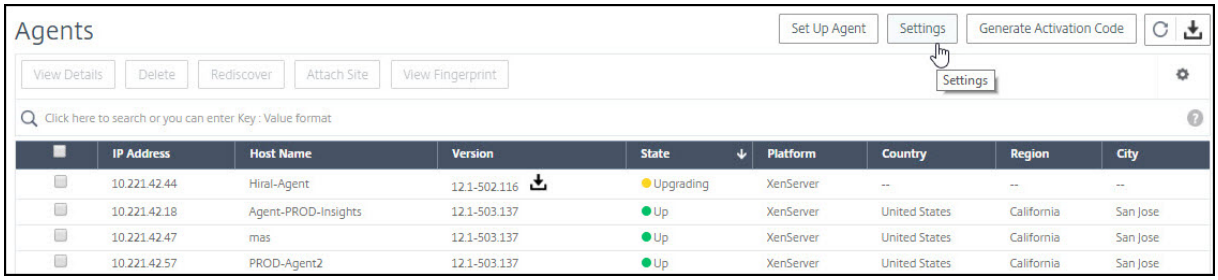
デフォルトでは、新しいバージョンが利用可能になると、エージェントは自動的にアップグレードされます。ただし、エージェントのアップグレードを実行する時刻を指定できます。

特定の時刻を選択すると、エージェントはその指定された時刻にアップグレードされますが、エージェントが展開されているタイムゾーンでアップグレードされます。

アップグレード中に、約 30 分のダウンタイムが発生することがあります。

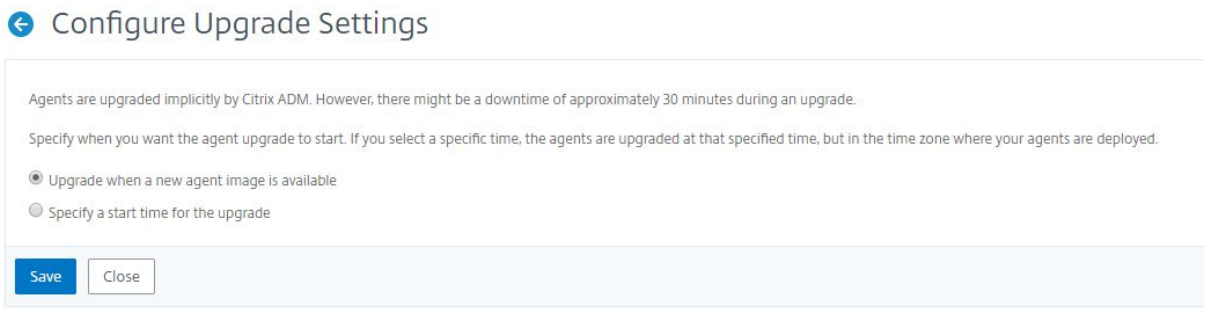
エージェントのアップグレード設定を構成するには：

[ネットワーク] > [エージェント] に移動し、[設定] をクリックします。



エージェントのアップグレードを開始するタイミングを指定します。新しいエージェントが使用可能になったときにアップグレードするか、または Citrix ADM でエージェントを暗黙的にアップグレードする特定の時刻を設定できます。設定した時間は、エージェントのタイムゾーンに固有です。

[保存] をクリックして、設定を保存します。これらの設定は、設定を変更するまで、今後のエージェントのアップグレード時に保持されます。



インスタンスの追加

May 7, 2021

インスタンスの追加は、の Citrix Application Delivery Management（Citrix ADM）のはじめてはまたはその後の設定時に行うことができます。

インスタンスは、Citrix ADM から検出、管理、監視する Citrix アプライアンスまたは仮想アプライアンスです。以下の Citrix アプライアンスと仮想アプライアンスを Citrix ADM に追加できます。

- Citrix ADC MPX
- Citrix ADC VPX
- Citrix ADC SDX
- Citrix ADC CPX
- Citrix ADC BLX
- Citrix Gateway
- Citrix Secure Web Gateway
- Citrix SD-WAN WANOP

インスタンスを追加するには、各 Citrix ADC インスタンスのホスト名または IP アドレス、または IP アドレスの範囲を指定する必要があります。SD-WAN インスタンスの場合、各インスタンスの IP アドレス、または IP アドレスの範囲を指定する必要があります。

> 注:
>
> Citrix ADM は、Citrix SD-WAN WANOP のみをサポートしています。

Citrix ADM がインスタンスにアクセスするために使用できるインスタンスプロファイルを指定します。このインスタンスプロファイルには、サービスに追加するインスタンスのユーザー名とパスワードが含まれます。インスタンスの種類ごとにデフォルトのプロファイルが用意されています。たとえば、ns-root プロファイルは、Citrix ADC インスタンスのデフォルトプロファイルです。このプロファイルは、デフォルトの Citrix ADC 管理者の資格情報によって定義されます。インスタンスのデフォルトの管理者資格情報を変更した場合は、それらのインスタンスのカスタムのインスタンスプロファイルを定義できます。インスタンスの検出後にインスタンスの認証情報を変更する場合は、インスタンスプロファイルを編集するか、プロファイルを作成してから、インスタンスを再検出する必要があります。

Citrix ADM にインスタンスを追加した後、Citrix ADM から Citrix ADC インスタンスの GUI にアクセスできます。Citrix ADM から Citrix ADC インスタンスにアクセスするには、Citrix ネットワークに接続する必要があります。

> 注
>
> - クラスターで構成された Citrix ADC インスタンスを追加するには、クラスターの IP アドレスまたはクラスター設定の個々のノードのいずれかを指定する必要があります。ただし、Citrix ADM では、クラスタ IP アドレスはクラスタを表します。
> - 高可用性ペアとしてセットアップされた Citrix ADC インスタンスの場合、1 つのインスタンスを追加すると、そのペアのもう一方のインスタンスが自動的に追加されます。

Citrix ADC インスタンスを **Citrix ADM** に追加するには

> 注
>
> ADC CPX インスタンスを除く他のすべての ADC インスタンスを追加するには、次の作業を実行します。

1. [ネットワーク] > [ダッシュボード] に移動し、[すべてのインスタンス] をクリックします。[インスタンス] ページで、ページの右上隅にある [新規] をクリックします。[インスタンスの追加] ページの [インスタンスタイプ] で、追加するインスタンスのタイプを選択します。

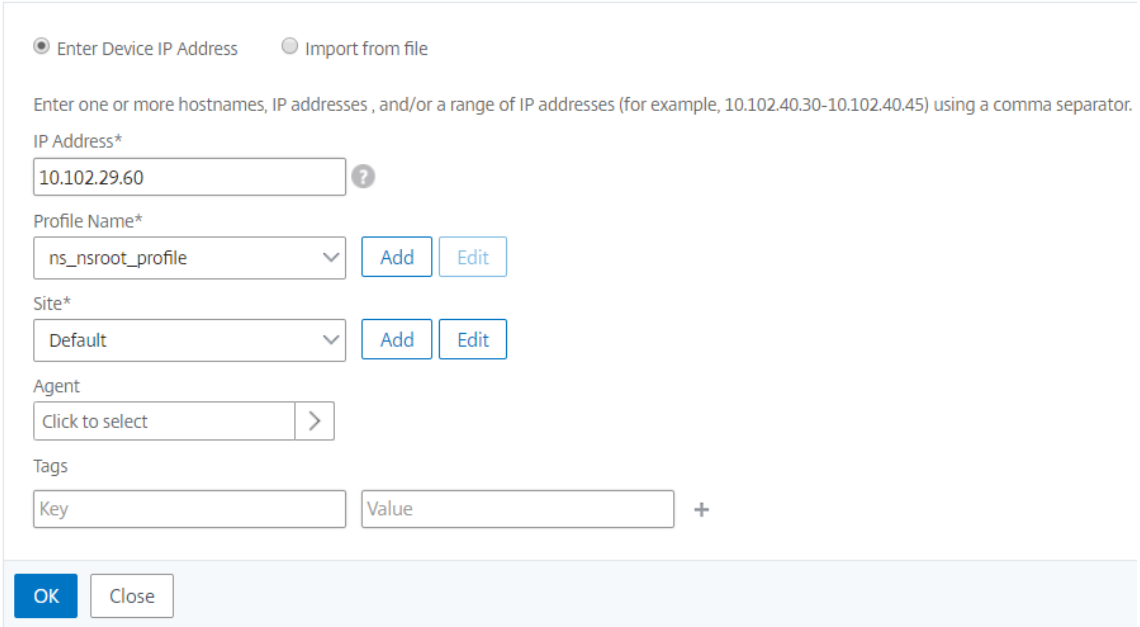
   または、[ネットワーク] > [インスタンス] に移動します。［インスタンス］で、追加するインスタンスの種類（Citrix ADC VPX など）を選択し、［追加］をクリックします。

2. 次のいずれかのオプションを選択します:

   - デバイスの **IP** アドレスを入力 -Citrix ADC インスタンスの場合は、各インスタンスのホスト名または IP アドレス、または IP アドレスの範囲を指定します。SD-WAN インスタンスの場合、各インスタンスの IP アドレス、または IP アドレスの範囲を指定する必要があります。
   - **Import from file** - ローカルシステムから、追加するすべてのインスタンスの IP アドレスを含むテキストファイルをアップロードします。

3. （オプション）初回ログイン失敗時にデバイスの追加を有効にするを選択します。このオプションを使用すると、有効な認証情報がない場合でもインスタンスを追加できます。
4. 「プロファイル名」で、適切なインスタンスプロファイルを選択するか、「**+**」アイコンをクリックしてプロファイルを作成します。
5. 「サイト」で、インスタンスを追加するサイトを選択します。
6. 「エージェント」で、インスタンスを関連付けるエージェントを選択し、「**OK**」をクリックします。

   Citrix ADM にエージェントが 1 つしか構成されていない場合、そのエージェントはデフォルトで選択されます。



ADM に Citrix ADC CPX インスタンスを追加するには

1. [ネットワーク] > [インスタンス] に移動します。［インスタンス］で ［**Citrix ADC** ］を選択し、［CPX］タブを選択します。
2. ［追加］をクリックします。
3. 次のいずれかのオプションを選択します：
   - デバイスの **IP** アドレスを入力します。各インスタンスのホスト名または IP アドレス、または IP アドレスの範囲を指定します。
   - ファイルからインポートします。ローカルシステムから、追加するすべてのインスタンスの IP アドレスを含むテキストファイルをアップロードします。
4. （オプション）初回ログイン失敗時にデバイスの追加を有効にするを選択します。このオプションを使用すると、有効な認証情報がない場合でもインスタンスを追加できます。

5. [ルーティング可能な **IP/**ドッカー **IP**] フィールドに、IP アドレスを入力します。IP アドレスは、Citrix ADC CPX インスタンス（到達可能な場合）または Docker ホストのいずれかになります。
6. [**Profile Name**] フィールドで、適切なインスタンスプロファイルを選択するか、[+] アイコンをクリックしてプロファイルを作成します。

   > 注:
   >
   > プロファイルを作成するときは、ホストの HTTP、HTTPS、SSH、および SNMP ポートの詳細を指定する必要があります。[開始ポート] および [ポート数] フィールドで、ホストによって公開されるポートの範囲を指定することもできます。

7. オプションとして、CPX インスタンスをデプロイするサイトを選択します。[追加] をクリックして、サイトを作成することもできます。
8. 可能な場合は、エージェントのリストから Citrix ADM サービスエージェントを選択します。
9. [**OK**] をクリックして、Citrix ADM にインスタンスを追加するプロセスを開始します。

   > 注 インスタンスを再検出する場合は、次の手順を実行します。
   >
   > a) [ネットワーク] > [インスタンス] > [**Citrix ADC**] > [**CPX**] に移動します。
   > b) 再検出するインスタンスを選択します。
   > c) **[** アクションの選択**]** リストから、[再検出] をクリックします。

Citrix ADM でスタンドアロンの **Citrix ADC BLX** インスタンスを追加するには

スタンドアロンの Citrix ADC BLX インスタンスは、専用ホスト Linux サーバー上で実行される単一のインスタンスです。

1. [ネットワーク] > [インスタンス] > [**Citrix ADC**] に移動します。
2. [**BLX**] タブで、[追加] をクリックします。
3. （オプション）初回ログイン失敗時にデバイスの追加を有効にするを選択します。このオプションを使用すると、有効な認証情報がない場合でもインスタンスを追加できます。
4. [インスタンスタイプ] リストから [スタンドアロン] オプションを選択します。
5. [**IP** アドレス] フィールドで、BLX インスタンスの IP アドレスを指定します。
6. [**Host IP address**] フィールドで、BLX インスタンスがホストされている Linux サーバの IP アドレスを指定します。
7. [プロファイル名] リストで、BLX インスタンスに適切なプロファイルを選択するか、プロファイルを作成します。

   プロファイルを作成するには、[追加] をクリックします。

> 重要:
>
> プロファイルで、Linux サーバの正しいホスト・ユーザー名とパスワードを指定していることを確認してください。

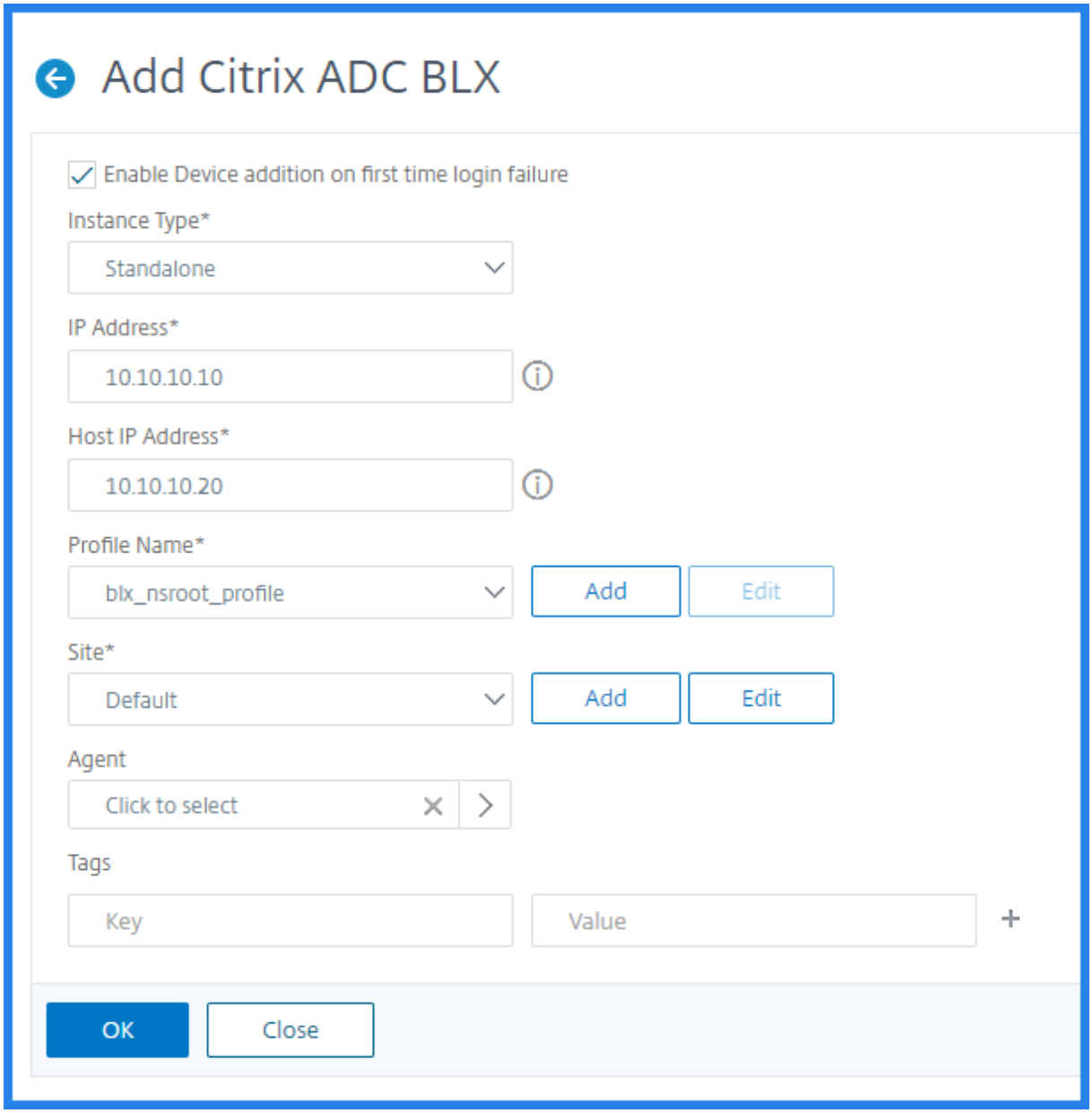
8. [サイト] リストで、インスタンスを追加するサイトを選択します。

   サイトを追加する場合は、[追加] をクリックします。

9. ［エージェント］リストで、インスタンスを関連付ける Citrix ADM エージェントを選択します。

   Citrix ADM にエージェントが 1 つしか構成されていない場合、そのエージェントはデフォルトで選択されます。

10. ［**OK**］をクリックします。



Citrix ADM で高可用性 **Citrix ADC BLX** インスタンスを追加するには

異なるホスト Linux サーバーで実行される高可用性 Citrix ADC BLX インスタンス。Linux サーバでは、複数の BLX インスタンスをホストできません。

1. [**BLX**] タブで、[追加] をクリックします。
2. （オプション）初回ログイン失敗時にデバイスの追加を有効にするを選択します。このオプションを使用すると、有効な認証情報がない場合でもインスタンスを追加できます。
3. [インスタンスタイプ] リストから [高可用性] オプションを選択します。
4. [**IP** アドレス] フィールドで、BLX インスタンスの IP アドレスを指定します。
5. [**Host IP address**] フィールドで、BLX インスタンスがホストされている Linux サーバの IP アドレスを指定します。
6. [**Peer IP address**] フィールドに、ピア BLX インスタンスの IP アドレスを指定します。
7. [ピアホスト **IP** アドレス] フィールドで、ピア BLX インスタンスがホストされている Linux サーバの IP アドレスを指定します。
8. [プロファイル名] リストで、BLX インスタンスに適切なプロファイルを選択するか、プロファイルを作成します。

   プロファイルを作成するには、[追加] をクリックします。

   > 重要:
   >
   > プロファイルで、Linux サーバの正しいホスト・ユーザー名とパスワードを指定していることを確認してください。

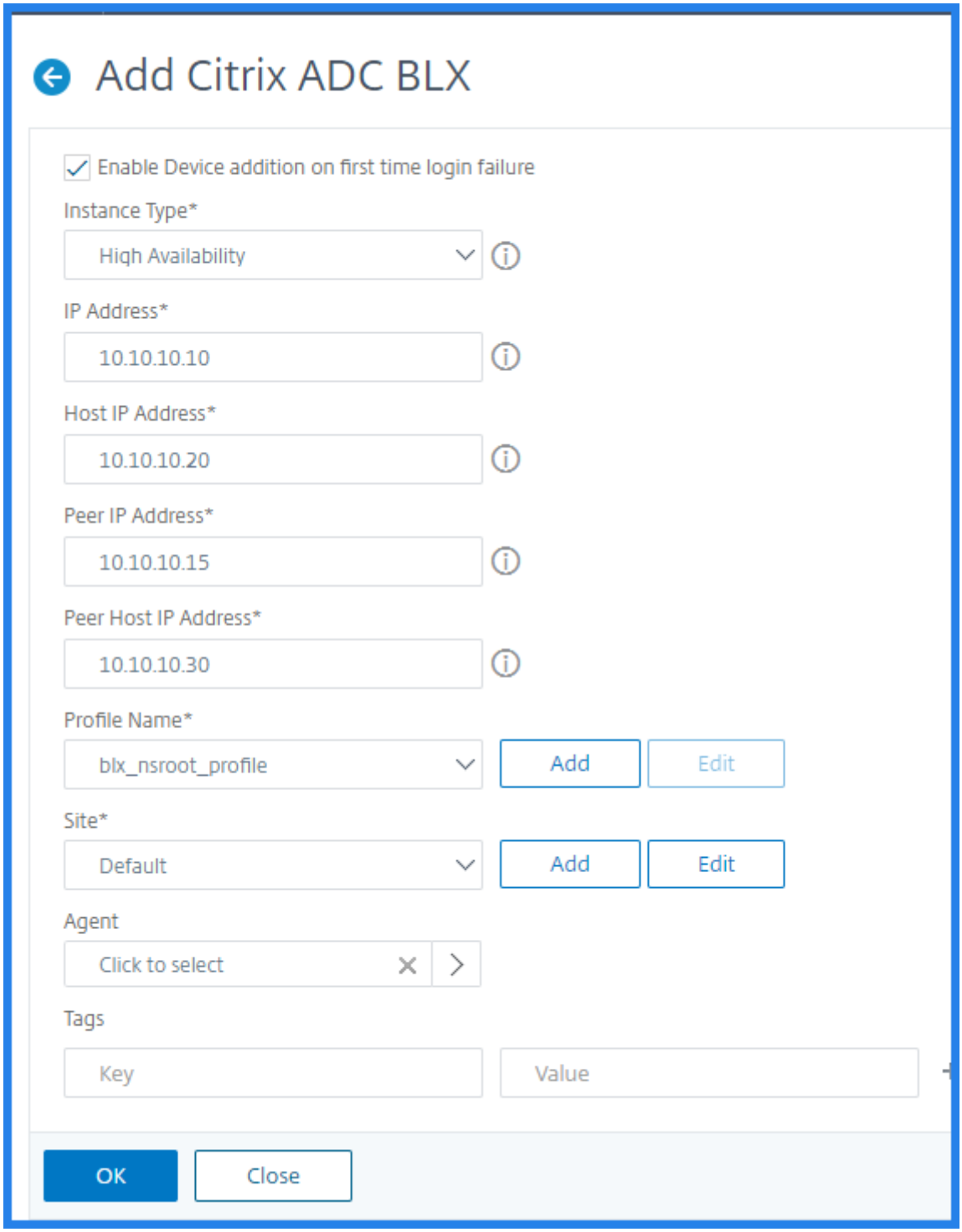
9. [サイト] リストで、インスタンスを追加するサイトを選択します。

   サイトを追加する場合は、[追加] をクリックします。

10. ［エージェント］リストで、インスタンスを関連付ける Citrix ADM エージェントを選択します。

    Citrix ADM にエージェントが 1 つしか構成されていない場合、そのエージェントはデフォルトで選択されます。

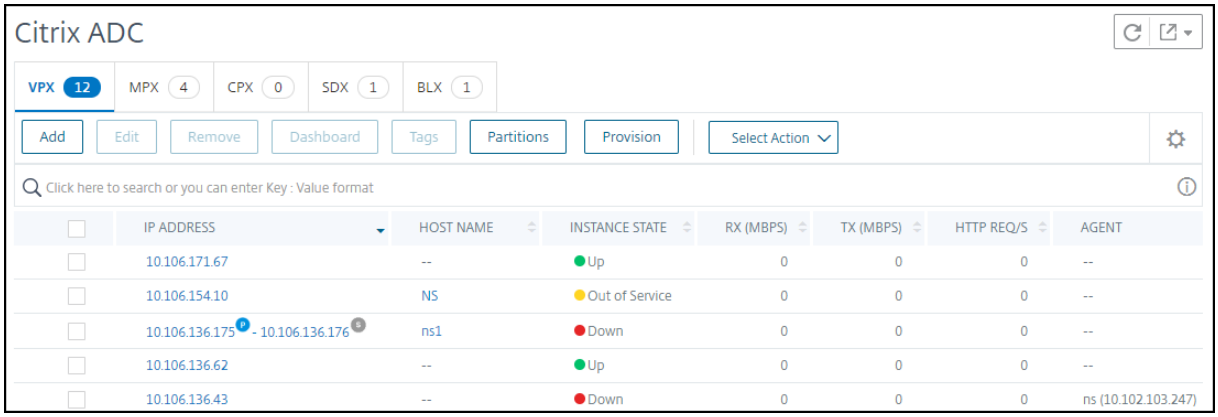
11. ［**OK**］をクリックします。



Citrix ADM からインスタンス **GUI** にアクセスするには

1. [ネットワーク**] > [**インスタンス**] > [Citrix ADC**] に移動します。
2. アクセスするインスタンスのタイプ（VPX、MPX、CPX、SDX、BLX など）を選択します。

3. 必要な Citrix ADC IP アドレスまたはホスト名をクリックします。



選択したインスタンスの GUI がポップアップウィンドウに表示されます。

インスタンスの警告を解決する

次の理由により、インスタンスに警告記号が表示されます。

- ログイン失敗 -有効な認証情報なしでインスタンスを追加すると、そのインスタンスは DOWN 状態になり、ログインに失敗した警告が表示されます。ADM でインスタンスを管理するための正しい認証情報を指定します。

  インスタンスがライセンスされていない場合、インスタンスを選択すると [**License**] オプションが表示されます。[**License**] をクリックして、ライセンスプールからインスタンスにライセンスを適用します。

- **HTTPS** プロファイルのライセンスされていないインスタンス -ライセンスされていないインスタンスが HTTPS 接続のみを使用する場合は、ADC GUI からインスタンスにライセンスを適用します。

HAProxy インスタンスの追加

May 7, 2021

ホストでプロビジョニングされた HAProxy インスタンスを追加するには、はじめては以降のの Citrix Application Delivery Management（Citrix ADM）をセットアップするときにホストの詳細を指定します。

Citrix ADM は HAProxy バージョン 1.6.3 以降をサポートしており、以下のホストでプロビジョニングされた HAProxy インスタンスを Citrix ADM に追加できます。

- Ubuntu 14.0 以降
- レッドハットエンタープライズ Linux (RHEL) 6.0 以降
- SUSE 11.0 以降
- CentOS 6.0 以降
- Amazon Linux AMI

> 注
>
> ホストが、シェル用にカスタマイズされたプロンプト文字列を使用して構成されていないことを確認します。シェルには、プロンプト文字列として $ または # を指定する必要があります。

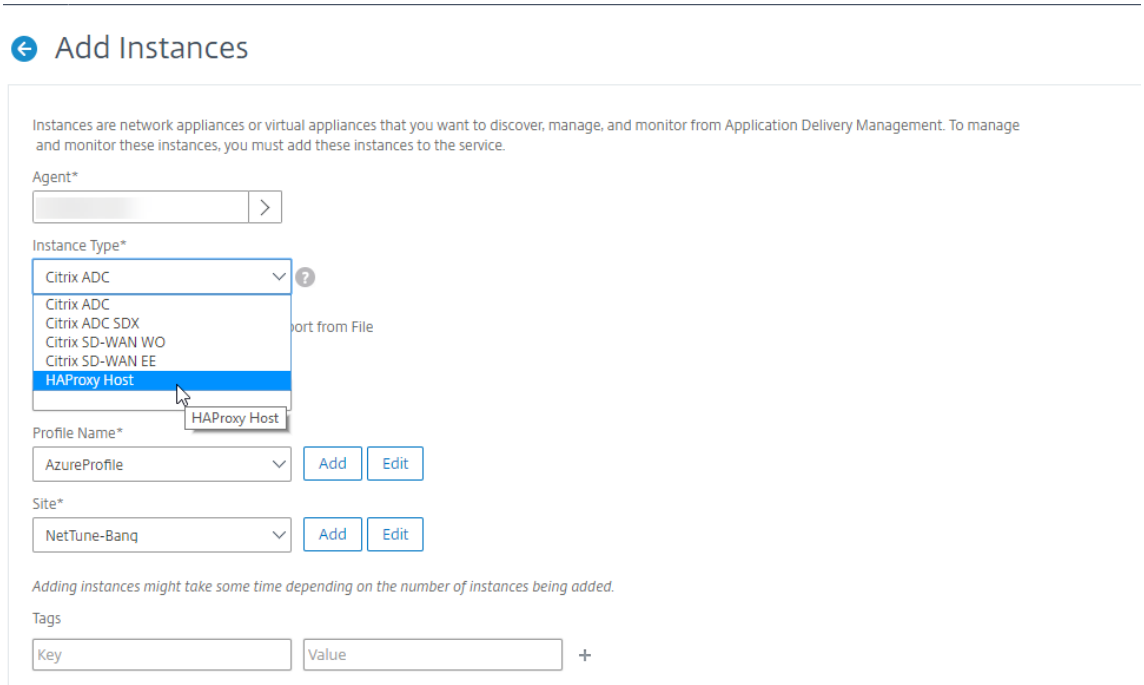
HAProxy インスタンスを追加するには、HAProxy インスタンスをプロビジョニングしたホストの IP アドレスを指定する必要があります。次に、Citrix ADM がホストにアクセスするために使用できる HAProxy プロファイルを指定する必要があります。この HAProxy プロファイルには、サービスに追加するホストのユーザー名とパスワードが含まれます。

> 注:
> ユーザー名に関連付けられたユーザー・アカウントには、次のものがあることを確認してください。
>
> - ps コマンドを実行して、ホスト上のすべての HAProxy インスタンスを一覧表示する権限。
> - ホストで HAProxy インスタンスを再起動するアクセス許可。

HAProxy インスタンスをプロビジョニングしたホストを Citrix ADM に追加すると、Citrix ADM は SSH プロトコルを使用してホストにアクセスします。ホスト上でプロビジョニングされた HAProxy インスタンスが自動的に検出され、Citrix ADM インベントリに追加されます。また、HAProxy インスタンス上に構成されているすべてのフロントエンド、バックエンド、およびサーバーを検出し、フロントエンドを検出されたアプリケーションとして扱います。

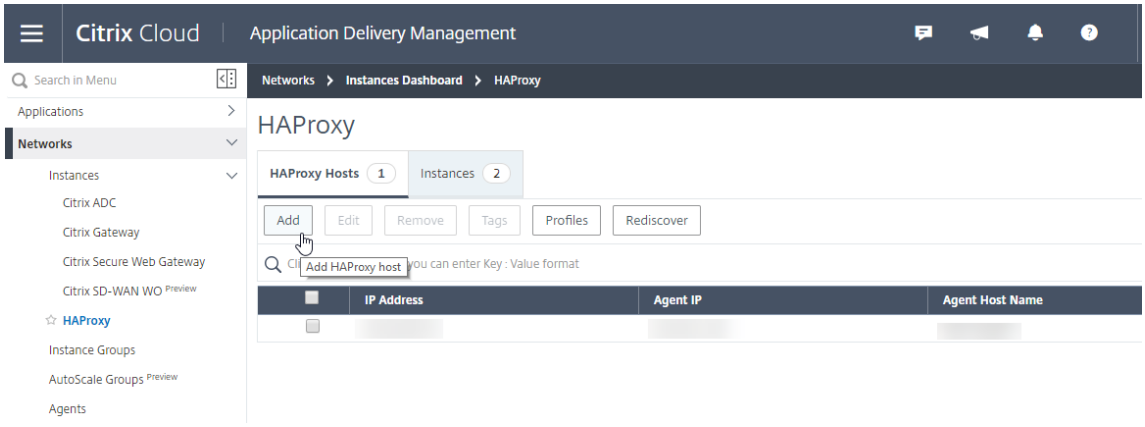
HAProxy インスタンスを **Citrix ADM** に追加するには:

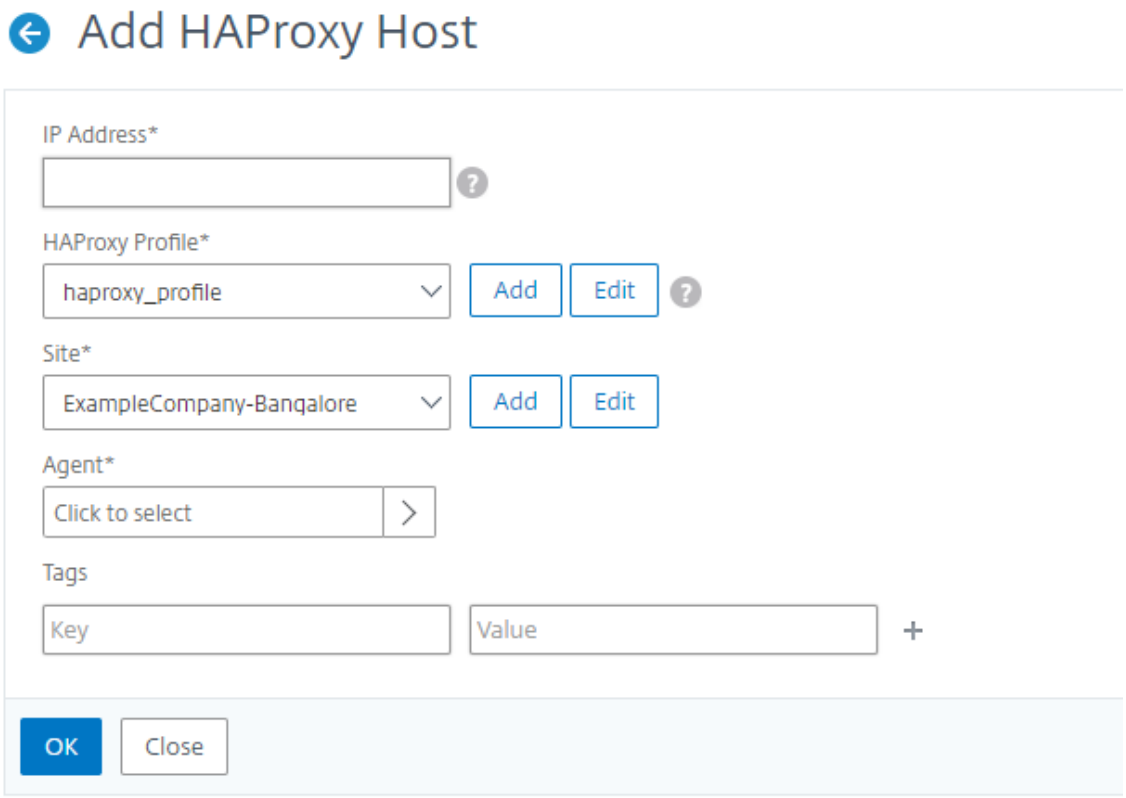
1. [ネットワーク**] > [**インスタンス] に移動し、[インスタンスの合計] をクリックします。[インスタンス] セクションで、ページの右上隅にある [追加] をクリックします。[インスタンスの追加] ページの [インスタンスタイプ] ドロップダウンリストから [**HAProxy** ホスト] を選択します。



   または、[ネットワーク**] > [**インスタンス**]** に移動します。[インスタンス] で **HAProxy** を選択し、[追加] を

クリックします。





2. [**IP Address**] フィールドに、HAProxy インスタンスをプロビジョニングしたホストの IP アドレスを入力します。
3. [**HAProxy** プロファイル] ドロップダウンリストで、既存の HAProxy プロファイルを選択するか、新しい HAProxy プロファイルを作成して選択します。HAProxy プロファイルを作成するには、[**+**] アイコンをクリックします。
4. [**HAProxy** プロファイルの追加] ダイアログボックスで、次の操作を行います。

a) [プロファイル名] フィールドに、HAProxy プロファイルの一意の名前を入力します。

b) [**User Name**] フィールドに、SSH プロトコルを使用してホストにアクセスするために使用するユーザー名を入力します。

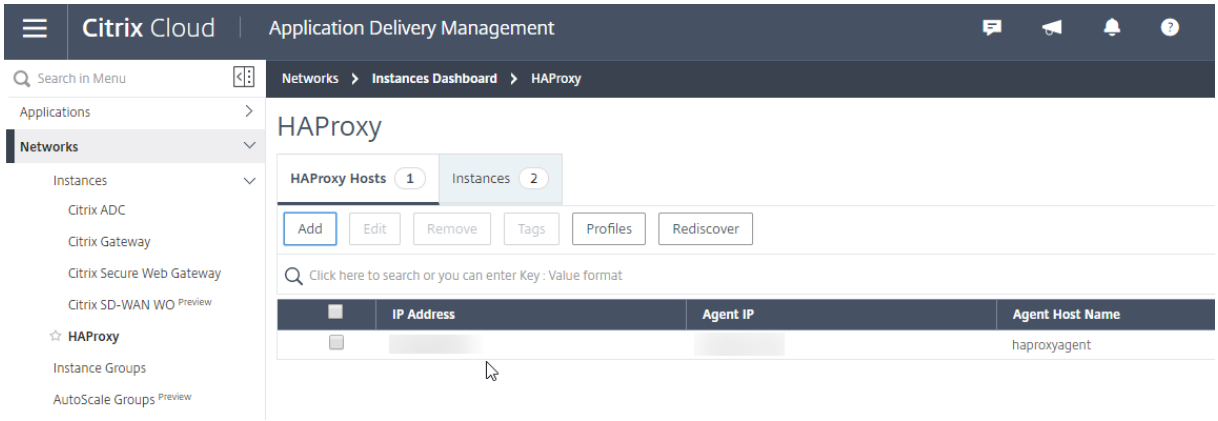
> 注
>
> ユーザー名に関連付けられているユーザーアカウントに次のものがあることを確認します。
>
> ```
> 1      - psコマンドを実行して、ホスト上のすべてのHAProxyインスタンスを一覧表示する権限。
> ```
>
> - ホストで HAProxy インスタンスを再起動するアクセス許可。

c) [**Password**] フィールドに、ホストのパスワードを入力します。

d) ［作成］をクリックします。

5. インスタンスの [サイト] を指定します。
6. [**Agent**] ドロップダウンリストで、インスタンスを関連付けるエージェントを選択します。
7. [Tags] フィールドで、HAProxy インスタンスのキーと関連する値を指定します。タグは、インスタンスの分類と識別に役立ちます。たとえば、キーとして [場所] を指定し、値として [バンガロール] を指定します。また、1 つのキーに複数の値を追加することもできます。複数の値はコンマで区切ります。
8. ［**OK**］を選択します。

Citrix ADM は、ホスト上でプロビジョニングされた HAProxy インスタンスを検出し、［ネットワーク］ **>** ［インスタンス］ **>** ［**HAProxy**］ページの［インスタンス］タブですべての **HAProxy** インスタンスを表示できます。



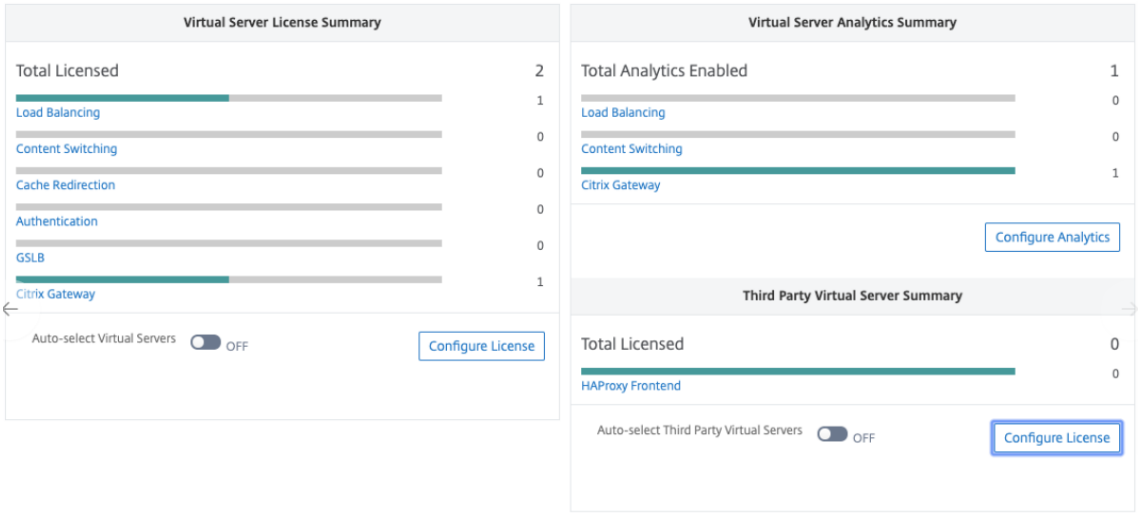
仮想サーバーでのライセンスの管理および分析の有効化

May 7, 2021

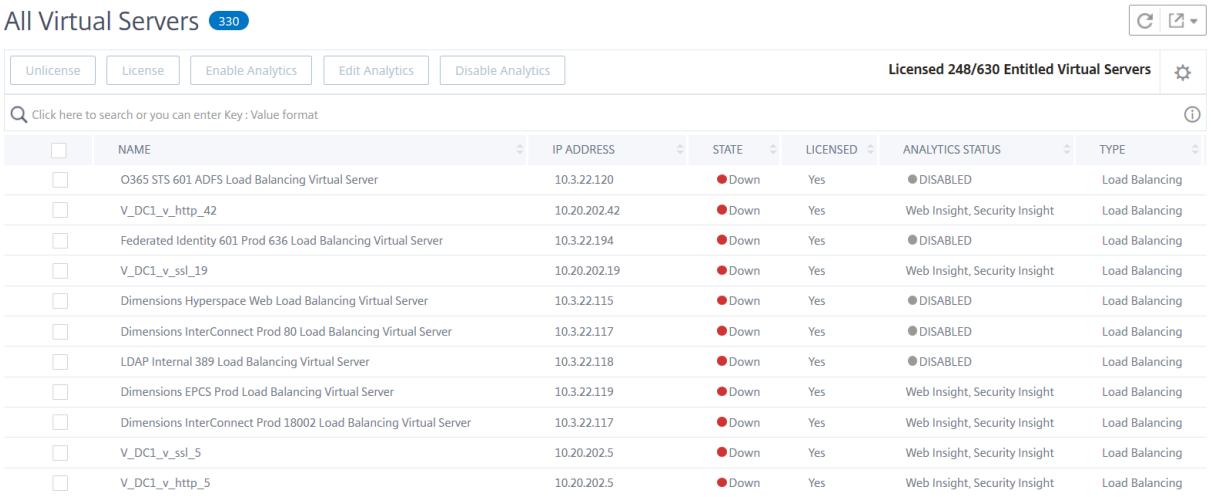
分析を有効にするプロセスが簡素化されます。これで、仮想サーバーのライセンスを取得し、単一のワークフローで分析を有効にできます。

「アカウント」>「購読」に移動します。

- 仮想サーバライセンスの概要を表示する
- 仮想サーバー分析の概要の表示



[ライセンスの構成] または [分析の構成] をクリックすると、[すべての仮想サーバー] ページが表示されます。



[すべての仮想サーバー] ページでは、次の操作を実行できます。

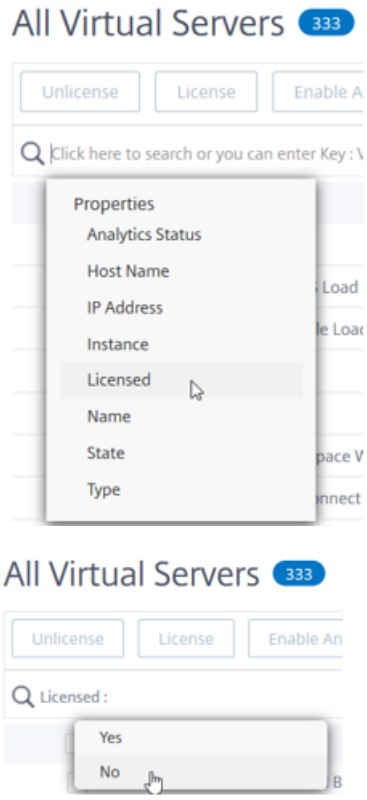
- ライセンスされていない仮想サーバのライセンスを適用する
- ライセンスされた仮想サーバのライセンスを削除
- ライセンス供与された仮想サーバーでの分析の有効化
- 分析の編集
- 分析を無効にする

> 注
>
> 分析を有効にするためにサポートされている仮想サーバーは、負荷分散、コンテンツスイッチング、Citrix Gateway です。

仮想サーバでのライセンスの管理

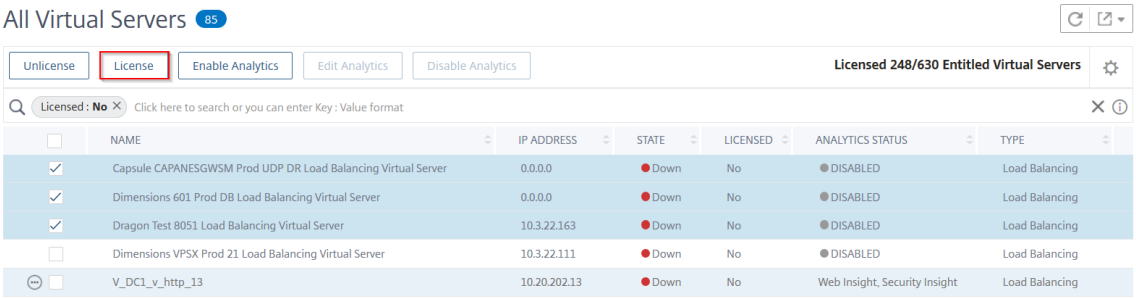
仮想サーバのライセンスを取得するには、［すべての仮想サーバ］ページを使用します。

1. 検索バーをクリックし、[ライセンス済み] を選択し、[いいえ] を選択します。



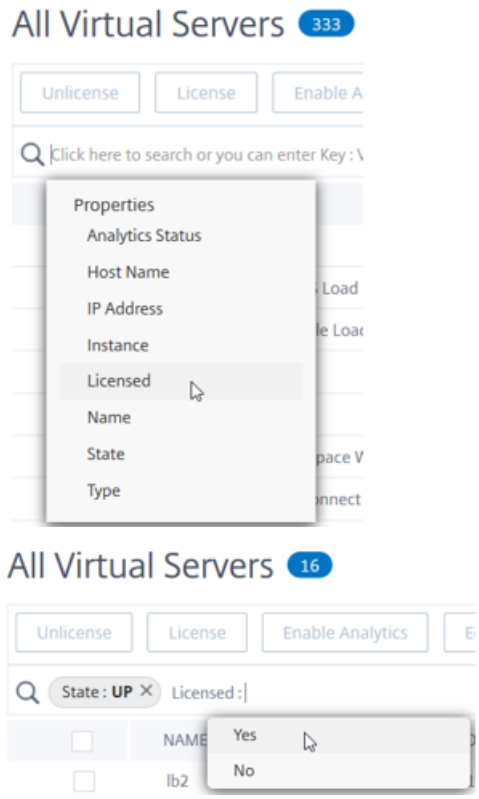
   フィルタが適用され、ライセンスされていない仮想サーバのみが表示されます。

2. 仮想サーバを選択し、［ライセンス］をクリックします。

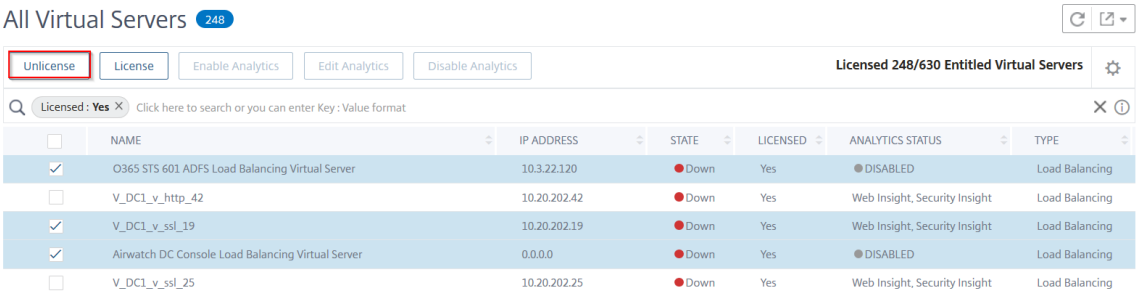


仮想サーバのライセンスを解除するには、［すべての仮想サーバ］ページを使用します。

1. 検索バーをクリックし、[ライセンス] を選択し、[はい] を選択します。



2. 仮想サーバーを選択し、[ライセンスの解除] をクリックします。



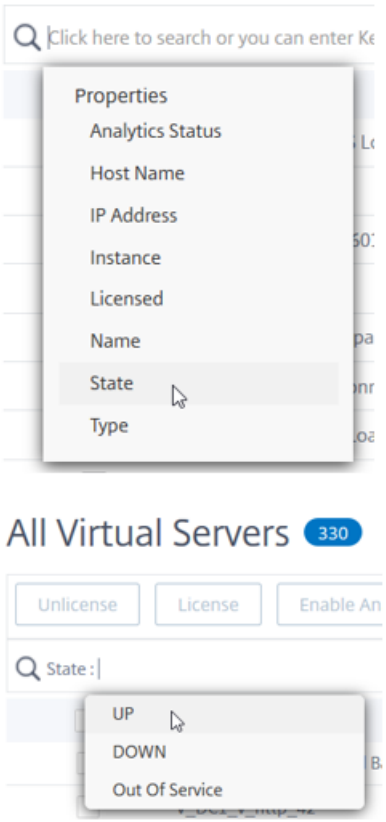
分析を有効にする

仮想サーバーの分析を有効にするための前提条件は次のとおりです。

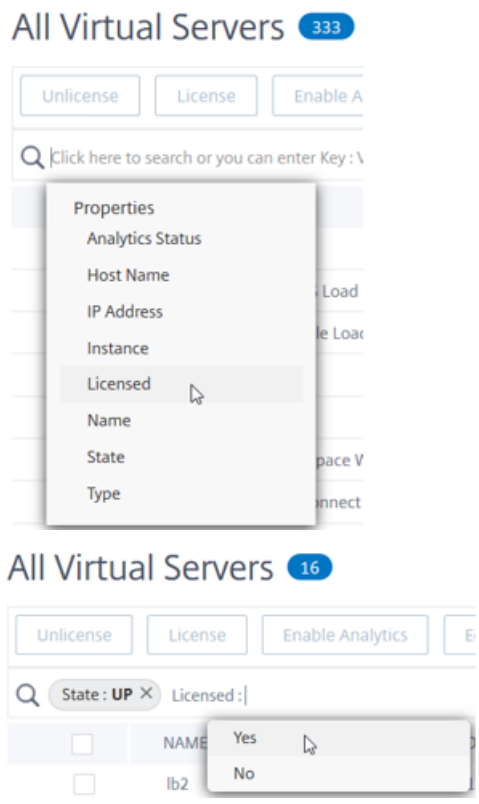
- 仮想サーバの ライセンスが付与されていることを確認する
- 分析ステータスが [無効] であることを確認します。
- 仮想サーバのステータスが **UP** であることを確認します。

結果をフィルタリングして、前提条件に記載されている仮想サーバーを特定できます。

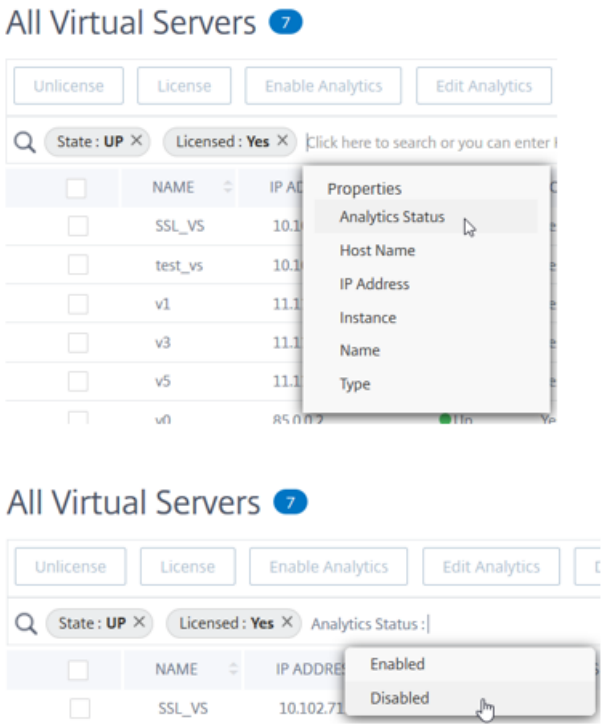
1. 検索バーをクリックし、[状態] を選択し、[**UP**] を選択します。



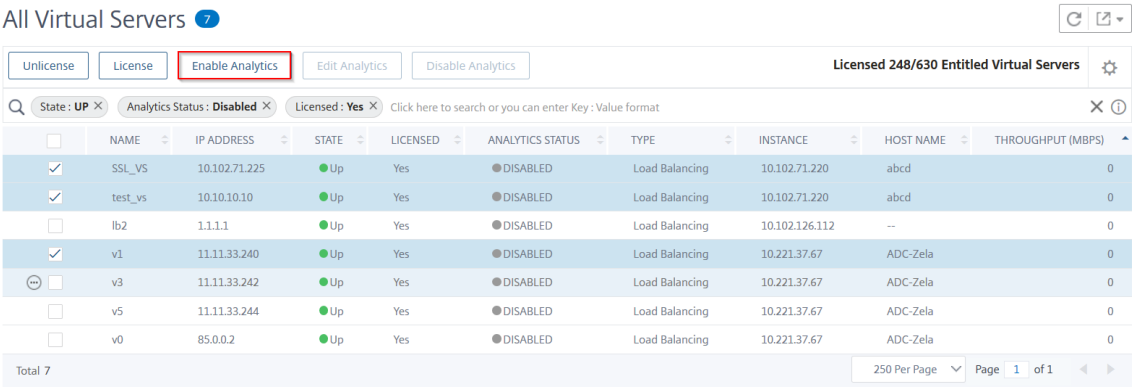
2. 検索バーをクリックして [ライセンス] を選択し、[はい] を選択します。



3. 検索バーをクリックし、[**Analytics** ステータス]、[無効] の順に選択します。



4. フィルタを適用した後、仮想サーバーを選択し、[**Analytics** を有効にする] をクリックします。



5. **[Analytics** の有効化] ウィンドウで、次の操作を行います。

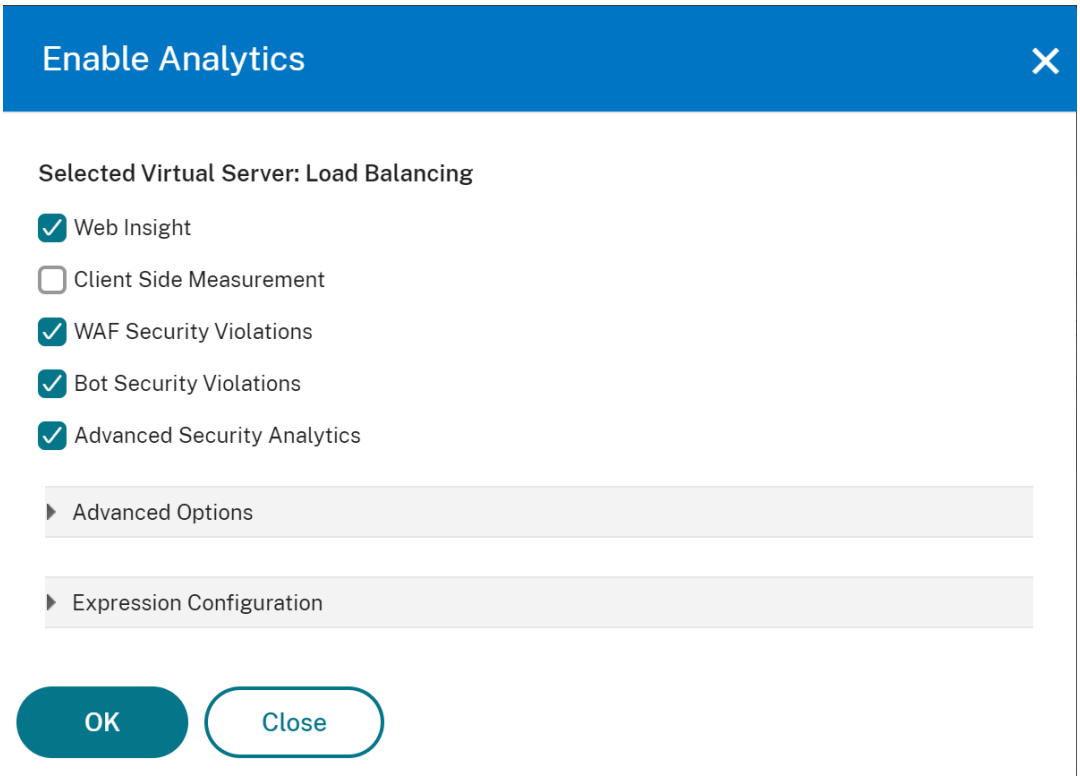
   a) インサイトの種類 (Web Insight または Security Insight) を選択します。

   b) 転送モードとして **Logstream** または **IPFIX** を選択します。

   > 注
   >
   > Citrix ADC 12.0 以前の場合、**IPFIX** はトランスポートモードのデフォルトのオプションです。Citrix ADC 12.0 以降では、トランスポートモードとして［ログストリーム］または［**IPFIX** ］を選択できます。
   >
   > **IPFIX** および **Logstream** の詳細については、「ログストリームの概要」を参照してください。

c) 式はデフォルトで true です

d) [**OK**] をクリックします。

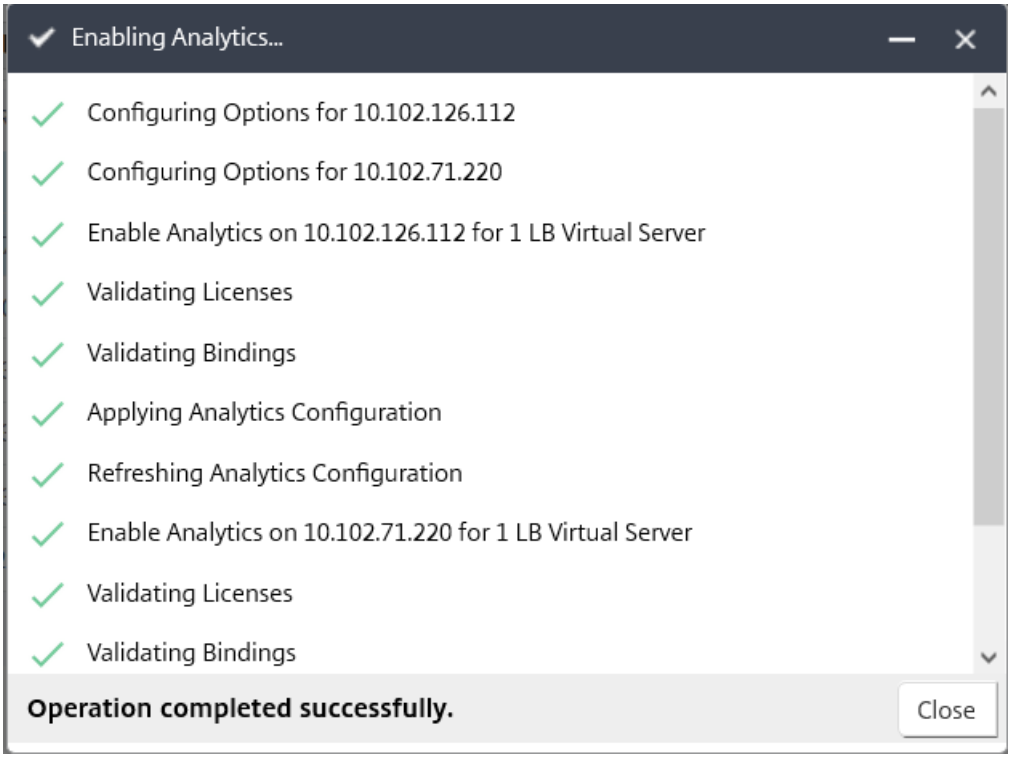


注

```
1       - ライセンスされていない仮想サーバーを選択した場合、
          Citrix ADMは最初にそれらの仮想サーバーのライセンス
          を取得してから、分析を有効にします。
2
3       - 管理パーティションの場合、 **Web Insight** のみがサ
          ポートされます。
```

- キャッシュリダイレクト、認証、**GSLB** などの仮想サーバーでは、分析を有効にできません。エラーメッセージが表示されます。

[**OK**] をクリックすると、Citrix ADM は選択した仮想サーバー上で分析を有効にするために処理します。

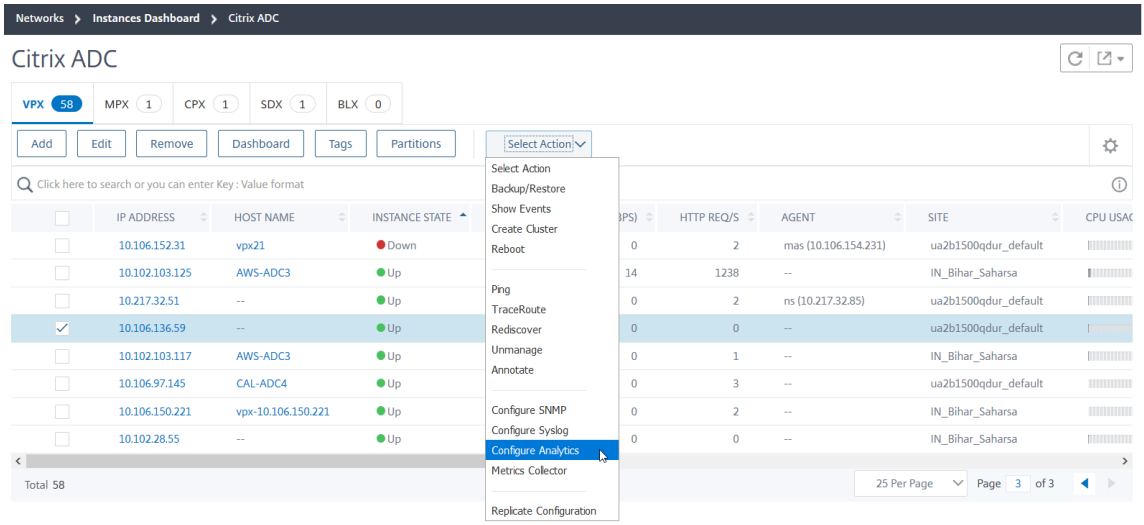


> 注
>
> Citrix ADM は、ログストリームには **Citrix** ADC SNIP を使用し、**IPFIX** には **NSIP** を使用します。Citrix ADM エージェントと Citrix ADC インスタンスの間でファイアウォールが有効になっている場合は、次のポートを開いて、Citrix ADM エージェントが AppFlow トラフィックを収集できるようにします。
>
> | トランスポートモード | ソース IP | 種類 | ポート |
> —| —| —| —| **IPFIX**
> ** | **NSIP** | **NSIP** | **UDP** | **4739**|
> | ** ログストリーム | 切り取り | TCP | 5557|

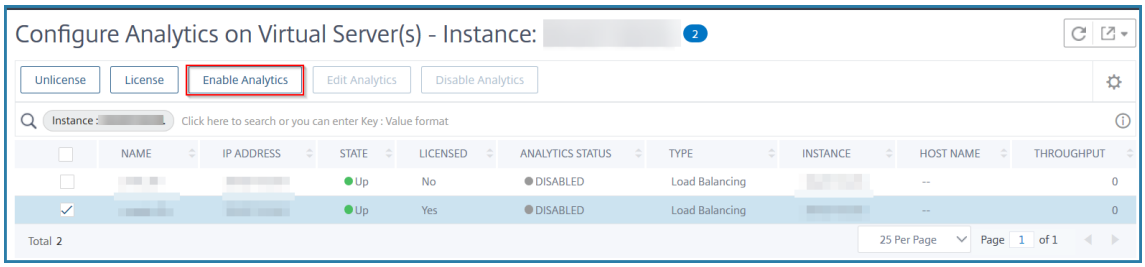
インスタンスの分析を有効にする

または、特定のインスタンスの分析を有効にすることもできます。

1. [ネットワーク] > [インスタンス] > [**Citrix ADC**] に移動し、インスタンスタイプを選択します。たとえば、VPX です。
2. インスタンスを選択し、[アクションの選択] リストから [**Analytics** を設定] を選択します。



3. [仮想サーバーでの **Analytics** の構成] ページで、仮想サーバーを選択し、[**Analytics** の有効化] をクリックします。



4. **[Analytics** の有効化] ウィンドウで、次の操作を行います。

   a) インサイトタイプ (Web Insight、Security Insight、ボットインサイト) を選択します

   b) 転送モードとして **Logstream** または **IPFIX** を選択します。

   > 注
   >
   > Citrix ADC 12.0 以前の場合、**IPFIX** はトランスポートモードのデフォルトのオプションです。Citrix ADC 12.0 以降では、トランスポートモードとして［ログストリーム］または［**IPFIX** ］を選択できます。
   >
   > **IPFIX** および **Logstream** の詳細については、「ログストリームの概要」を参照してください。

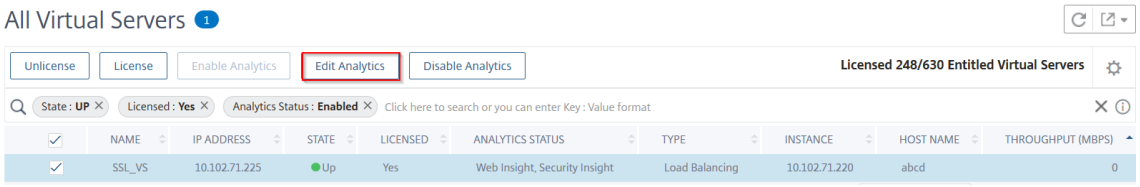
   c) 式はデフォルトで true です

   d) [**OK**]
   をクリックします。

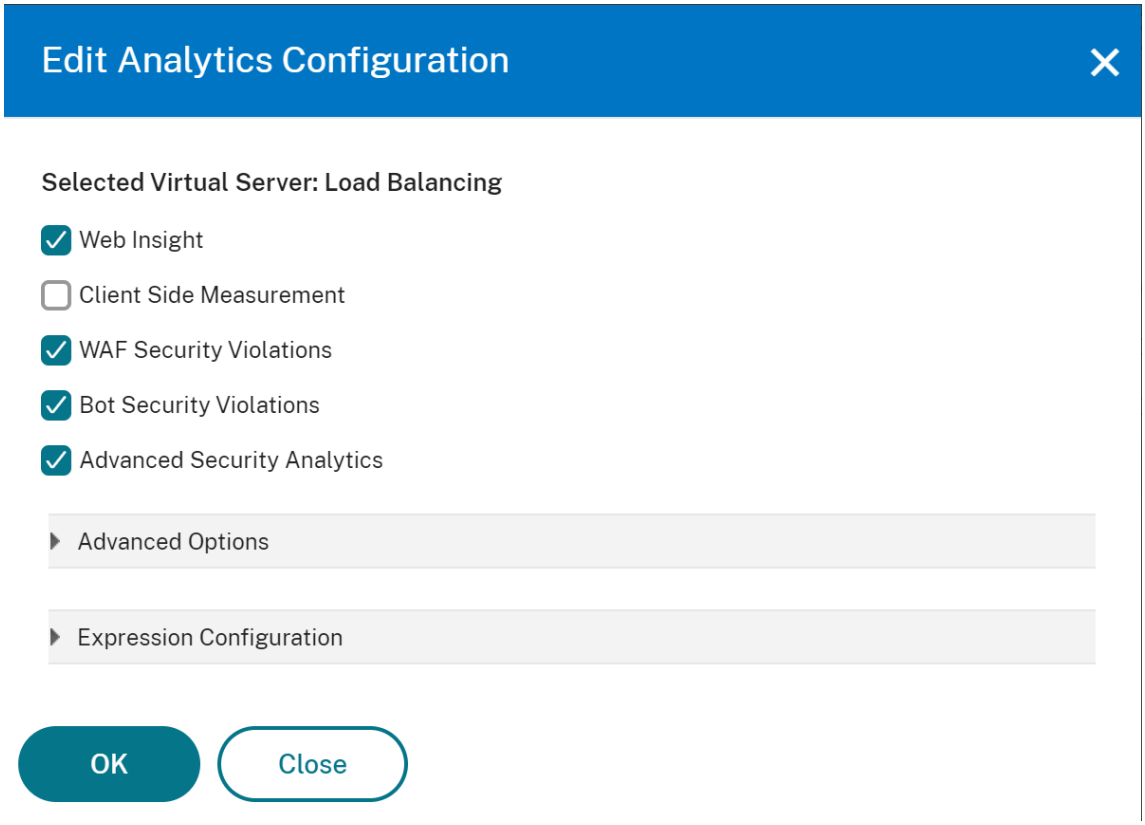
分析の編集

仮想サーバーの分析を編集するには、次の手順に従います。

1. 仮想サーバの選択
2. [**Analytics** の編集] をクリックします。



3. [**Analytics** 設定の編集] ウィンドウで適用するパラメータを編集します。
4. [**OK**] をクリックします。



インスタンスの分析を編集する

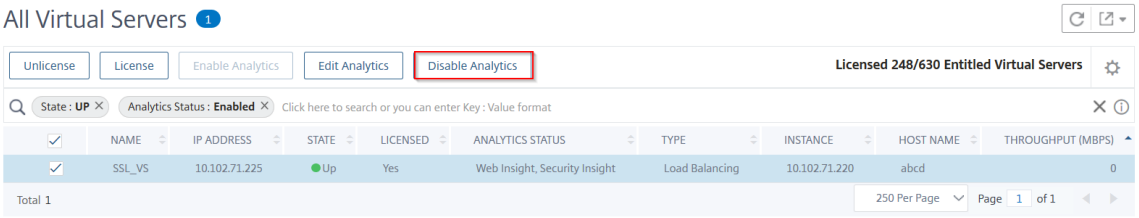
または、特定のインスタンスの分析を無効にすることもできます。

1. [ネットワーク] **>** [インスタンス] **>** [**Citrix ADC**] に移動し、インスタンスタイプを選択します。たとえば、VPX です。
2. インスタンスを選択し、[**Edit Analytics**] をクリックします。

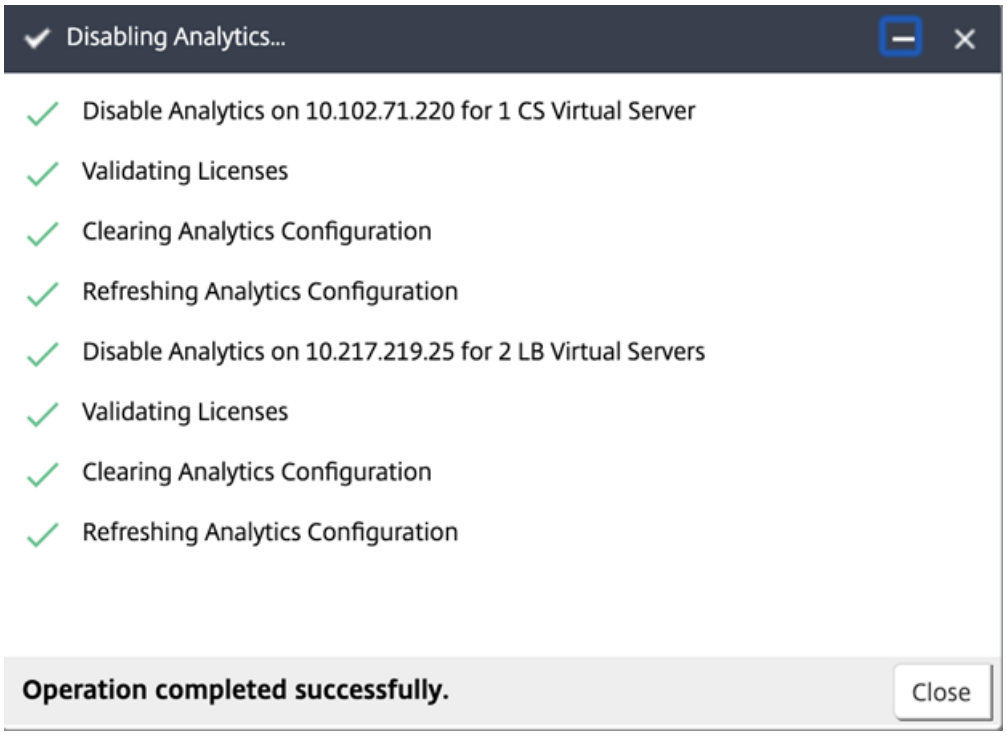
分析を無効にする

選択した仮想サーバー上で分析を無効にするには:

1. 仮想サーバの選択
2. [分析を無効にする] をクリックします。



Citrix ADM は、選択した仮想サーバーの分析を無効にします。



インスタンスでの **syslog** の設定

May 7, 2021

syslog プロトコルは、Citrix ADC インスタンスが Citrix ADM（Citrix Application Delivery Management）にイベント通知メッセージを送信できるようにするトランスポートを提供します。このプロトコルは、これらのメッセージのコレクタまたは syslog サーバーとして構成されています。

すべての syslog メッセージを Citrix ADM にリダイレクトするようにデバイスを構成している場合は、Citrix ADC

インスタンスで生成された syslog イベントを監視できます。syslog イベントを監視するには、まず Citrix ADM を Citrix ADC インスタンスの syslog サーバーとして構成する必要があります。インスタンスの構成後、すべての syslog メッセージが Citrix ADM にリダイレクトされるため、これらのログを構造化された方法でユーザーに表示できます。

Syslog は通信に User Datagram Protocol（UDP; ユーザデータグラムプロトコル）ポート 514 を使用し、UDP はコネクションレス型プロトコルであるため、インスタンスに確認応答を返しません。syslog パケットサイズは 1024 バイトに制限され、次の情報が伝送されます。

- ファシリティ
- 重大度
- ホスト名
- 日時
- メッセージ

Citrix ADM では、インスタンスのファシリティとログの重大度レベルを構成する必要があります。

- 機能 -Syslog メッセージは、それらを生成するソースに基づいて大きく分類されます。これらのソースは、オペレーティングシステム、プロセス、またはアプリケーションです。これらのカテゴリは施設と呼ばれ、整数で表されます。たとえば、0 はカーネルメッセージで使用され、1 はユーザーレベルのメッセージで使用され、2 はメールシステムで使用されます。ローカルユース施設（local0 から local7 まで）は予約されておらず、一般利用が可能です。したがって、ファシリティ値が事前に割り当てられていないプロセスおよびアプリケーションは、8 つのローカル使用施設のいずれかに転送できます。
- **Severity**： syslog メッセージを生成する送信元またはファシリティでは、次に示すように、1 桁の整数を使用してメッセージの重大度も指定します。

```
1-緊急：システムが使用できません。

2-アラート:アクションは直ちに実行する必要があります。

3-クリティカル:クリティカルな状態。

4-エラー:エラー状態。

5-警告:警告条件。

6-注意:正常だが重大な状態。

7-情報：情報メッセージ。

8-デバッグ:デバッグレベルのメッセージ。
```

Citrix ADC インスタンスで **syslog** を構成するには:

1. Citrix ADM で、[ネットワーク] > [インスタンス] に移動します。

2. Syslog メッセージを収集して Citrix ADM に表示する Citrix ADC インスタンスを選択します。
3. [アクション] ドロップダウンリストで、[**Syslog** の設定] を選択します。
4. [有効] をクリックします。
5. [**Facility**] ドロップダウンリストで、ローカルまたはユーザレベルのファシリティを選択します。
6. syslog メッセージに必要なログレベルを選択します。
7. [**OK**] をクリックします。

これにより、Citrix ADC インスタンス内のすべての syslog コマンドが構成され、Citrix ADM が syslog メッセージの受信を開始します。メッセージを表示するには、[ネットワーク] > [イベント] > [**Syslog** メッセージ] に移動します。

ロールベースのアクセス制御を構成する

May 7, 2021

Citrix Application Delivery Management（Citrix ADM）は、きめ細かな役割ベースのアクセス制御（RBAC）を提供します。RBAC（RBAC）を使用して、企業内の個々のユーザーの役割に基づいてアクセス許可を付与できます。

Citrix ADM では、すべてのユーザーが Citrix Cloud に追加されます。組織の最初のユーザーとして、まず Citrix Cloud でアカウントを作成し、Citrix Cloud の資格情報を使用して Citrix ADM GUI にログオンする必要があります。スーパー管理者の役割が付与され、デフォルトでは、Citrix ADM のすべてのアクセス権が付与されます。後で Citrix Cloud で組織内に他のユーザーを作成できます。

後で作成され、通常のユーザーとして Citrix ADM にログオンするユーザーは、委任された管理者と呼ばれます。これらのユーザーは、デフォルトで、ユーザー管理権限以外のすべての権限を持ちます。ただし、これらの委任された管理者ユーザーには、特定のユーザー管理アクセス許可を付与できます。適切なポリシーを作成し、これらの委任されたユーザーに割り当てることで、そのポリシーを実行できます。ユーザー管理権限は、[アカウント] > [ユーザー管理] にあります。特定のアクセス許可を割り当てる方法の詳細については、「委任された管理者ユーザーに追加のアクセス許可を割り当てる方法」を参照してください。

ポリシー、ロール、グループの作成方法、およびユーザーをグループにバインドする方法の詳細については、次のセクションを参照してください。

例:

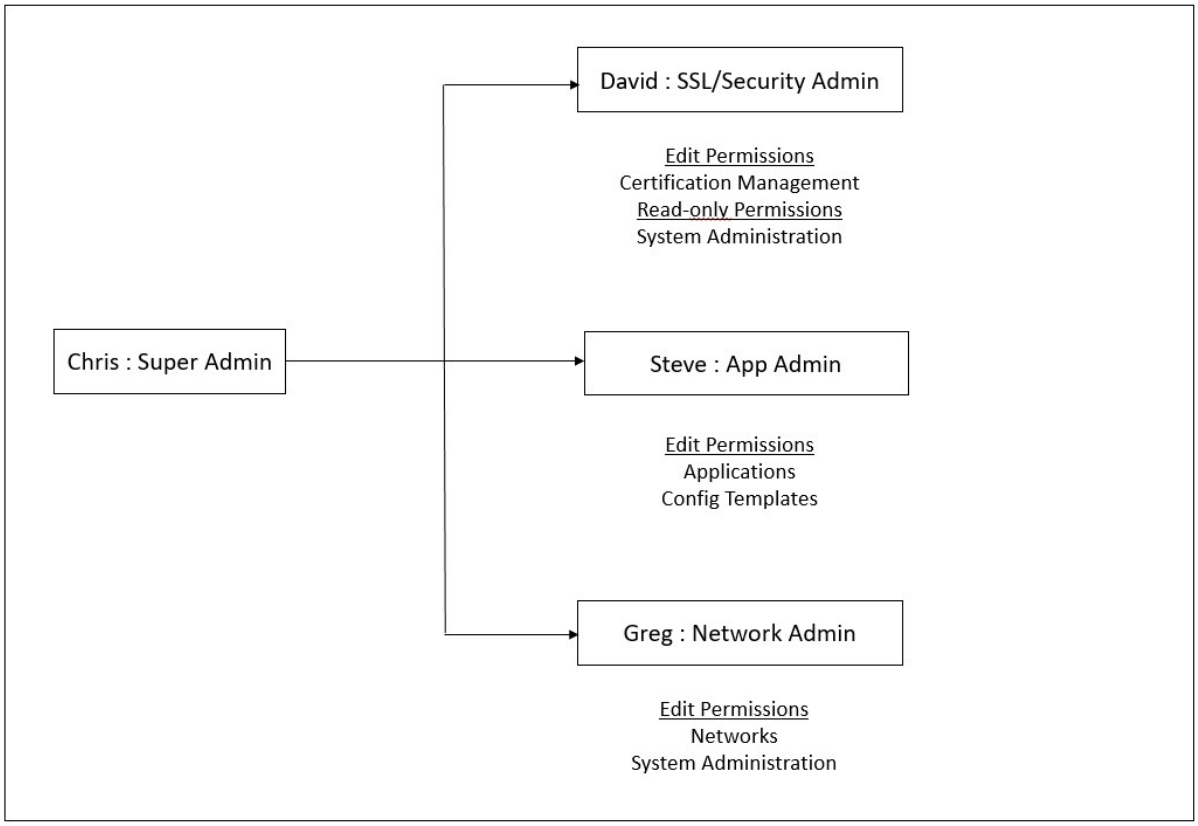
次の例は、Citrix ADM で RBAC を実現する方法を示しています。

ADC グループ長であるクリスは、組織内の Citrix ADM スーパー管理者です。クリスはセキュリティ管理者、アプリケーション管理者、ネットワーク管理者という 3 つの管理者の役割を作成します。

- セキュリティ管理者の David は、SSL 証明書の管理と監視のための完全なアクセス権を持っている必要がありますが、システム管理操作には読み取り専用アクセス権が必要です。
- アプリケーション管理者のスティーブは、特定のアプリケーションと特定の構成テンプレートのみのアクセスが必要です。

- ネットワーク管理者のグレッグは、システムとネットワーク管理へのアクセスが必要です。
- また、Chris は、ローカルまたは外部であるかどうかにかかわらず、すべてのユーザーに対して RBAC を提供する必要があります。

下図に、各種の管理者とほかのユーザーが持つ権限と社内での役割を示します。



役割ベースのアクセス制御をユーザーに提供するには、まず Citrix Cloud にユーザーを追加する必要があります。その後、Citrix ADM でユーザーを表示できます。Chris は、ロールに応じて、各ユーザーのアクセスポリシーを作成する必要があります。アクセスポリシーは、ロールに緊密にバインドされています。したがって、Chris はロールも作成する必要があります。その後、ロールはグループにのみ割り当てられ、個々のユーザーには割り当てられないため、グループを作成する必要があります。

Access は、ファイルの表示、作成、変更、削除など、特定のタスクを実行する機能です。ロールは、企業内のユーザーの権限と責任に応じて定義されます。たとえば、1 人のユーザーがすべてのネットワーク操作の実行を許可し、別のユーザーはアプリケーションのトラフィックフローを監視し、構成テンプレートの作成に役立ちます。

ロールはポリシーによって決定されます。ポリシーを作成したら、ロールを作成し、各ロールを 1 つ以上のポリシーにバインドし、ユーザーにロールを割り当てることができます。役割は、ユーザーのグループに割り当てることもできます。グループとは、共通の権限を持つユーザーの集まりです。たとえば、特定のデータセンターを管理している複数のユーザーを 1 つのグループに割り当てることができます。ロールは、特定の条件に基づいてユーザーを特定のグループに追加することによってユーザーに付与される ID です。Citrix ADM では、役割とポリシーの作成は Citrix ADC RBAC 機能に固有です。役割とポリシーは、企業のニーズが進展するにつれて簡単に作成、変更、または終了で

きます。各ユーザーの権限を個別に更新する必要はありません。

役割は機能ベースまたはリソースベースにすることができます。たとえば、SSL/セキュリティ管理者とアプリケーション管理者を考えてみましょう。SSL/セキュリティ管理者は、SSL 証明書の管理および監視機能への完全なアクセス権を持っている必要がありますが、システム管理操作には読み取り専用アクセス権が必要です。アプリケーション管理者は、スコープ内のリソースにのみアクセスできます。

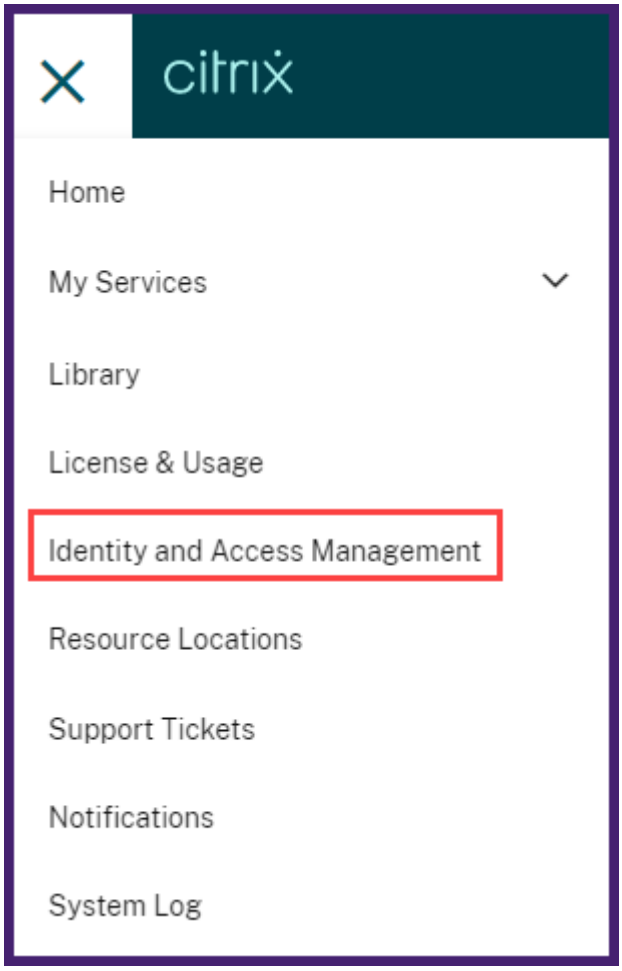
したがって、スーパー管理者である Chris（スーパー管理者）のロールで、Citrix ADM で以下の例タスクを実行して、組織のセキュリティ管理者である David のアクセスポリシー、役割、およびユーザーグループを構成します。

Citrix ADM でのユーザーの構成

スーパー管理者は、Citrix ADM ではなく Citrix Cloud でアカウントを構成することで、より多くのユーザーを作成できます。新しいユーザーが Citrix ADM に追加されると、そのユーザーに適切なグループを割り当てることによってのみ、ユーザーの権限を定義できます。

Citrix Cloud で新しいユーザーを追加するには:

1. Citrix ADM GUI で、左上のハンバーガーアイコンをクリックし、[アイデンティティとアクセスの管理] を選択します。

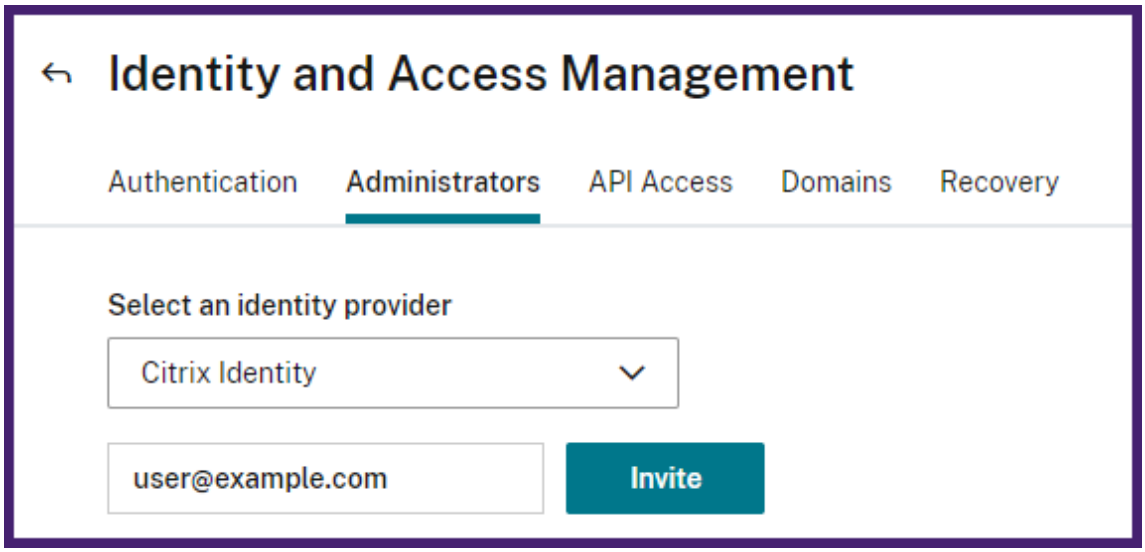


2. [ID とアクセス管理] ページで、[管理者] タブを選択します。

   このタブには、Citrix Cloud で作成されたユーザーが一覧表示されます。

3. アイデンティティプロバイダーとして **Citrix Identity** を選択します。

4. Citrix ADM に追加するユーザーの電子メールアドレスを入力し、［招待］をクリックします。

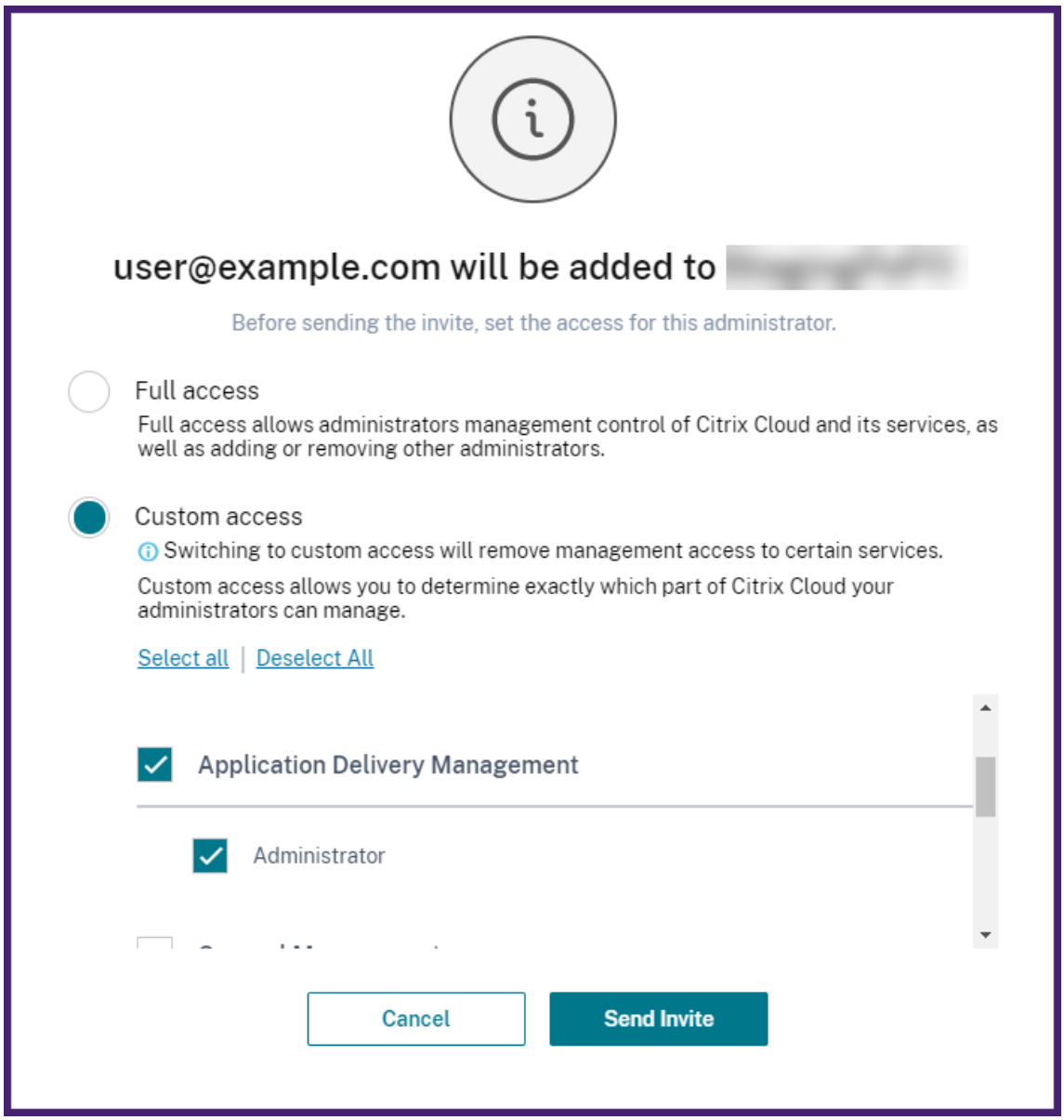


> 注
>
> ユーザーは、Citrix Cloud から招待メールを受信します。ユーザーは、電子メールに記載されているリンクをクリックして、フルネームとパスワードを入力して登録プロセスを完了し、後で資格情報を使用して Citrix ADM にログオンする必要があります。

5. 指定したユーザーの [カスタムアクセス] を選択します。

6. 「**Application Delivery Management**」を選択します。

   このオプションでは、デフォルトで管理者ロールが選択されます。

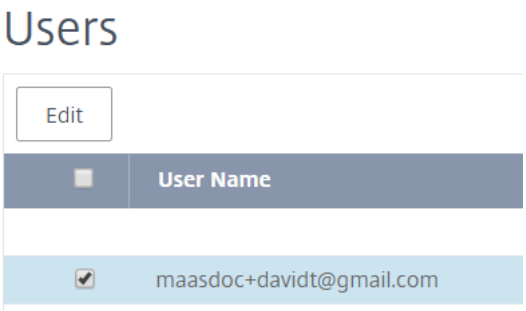


7. ［招待を送信する］をクリックします。

管理者は、ユーザーが Citrix ADM にログオンした後にのみ、［Citrix ADM ユーザー］の一覧に新しいユーザーが表示されます。

Citrix ADM でユーザーを構成するには:

1. Citrix ADM GUI で、［アカウント］>［ユーザー管理］>［ユーザー］に移動します。
2. ユーザーは **[ユーザー]** ページに表示されます。



3. ユーザーを選択して編集をクリックすると、ユーザーに付与された権限を編集できます。[設定] ノードの下の [グループ] ページで、グループのアクセス許可を編集することもできます。

> 注
>
> ```
> - ユーザーは、Citrix Cloudからのみ Citrix ADMに追加されます。したがって、管理者権限を持っていても、Citrix ADM GUIでユーザーを追加または削除することはできません。グループ権限のみを編集できます。Citrix Cloudからユーザーを追加または削除できます。
>
> - ユーザーの詳細情報は、ユーザーが Citrix ADMに少なくとも1回ログオンした後にのみ、サービスGUIに表示されます。
> ```

Citrix ADM でのアクセスポリシーの構成

アクセスポリシーでは、権限が定義されます。ロールを作成すると、ポリシーを 1 つのユーザーグループまたは複数のグループに適用できます。ロールはポリシーによって決定されます。ポリシーを作成したら、ロールを作成し、各ロールを 1 つ以上のポリシーにバインドし、ロールをユーザグループに割り当てる必要があります。Citrix ADM には、5 つの事前定義されたアクセスポリシーが用意されています。

- **admin_policy** すべての Citrix ADM ノードへのアクセスを許可します。ユーザーには表示権限と編集権限があり、すべての Citrix ADM コンテンツを表示でき、すべての編集操作を実行できます。つまり、ユーザーは、リソースに対する操作を追加、変更、および削除できます。
- **adminExceptSystem_policy**. Citrix ADM GUI のすべてのノード（[設定] ノードへのアクセスを除く）のユーザーにアクセス権を付与します。
- **readonly_policy**。読み取り専用権限を付与します。ユーザーは Citrix ADM 上のすべてのコンテンツを表示できますが、操作を実行する権限はありません。
- **appadmin_policy**。Citrix ADM アプリケーション機能にアクセスするための管理権限を付与します。このポリシーにバインドされているユーザーは、カスタムアプリケーションを追加、変更、削除できるほか、サービス、サービスグループ、および各種仮想サーバー（コンテンツスイッチ、キャッシュリダイレクト、および HAProxy 仮想サーバーなど）を有効または無効にできます。
- **appreadonly_policy**。アプリケーション機能に対する読み取り専用権限を付与します。このポリシーにバインドされているユーザーはアプリケーションを表示できますが、追加、変更、削除、有効化、および無効化

の操作は実行できません。

これらの定義済みポリシーは編集できませんが、独自の（ユーザ定義の）ポリシーを作成することはできます。

以前は、ポリシーを役割に割り当てて、その役割をユーザーグループにバインドすると、Citrix ADM GUI でノードレベルでユーザーグループのアクセス許可を提供できます。たとえば、負荷分散ノード全体へのアクセス許可のみを提供できます。ユーザーは、負荷分散ノードの下にあるすべてのエンティティ固有のサブノード（仮想サーバー、サービスなど）にアクセスする権限を持っているか、負荷分散の下にあるノードにアクセスする権限を持っていませんでした。

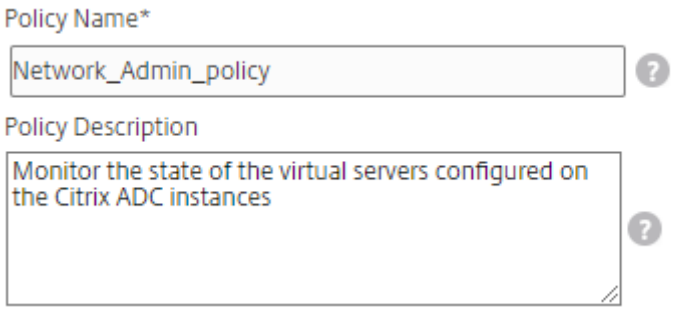
Citrix ADM 507.x 以降のビルドバージョンでは、アクセスポリシー管理が拡張され、サブノードの権限も提供されます。アクセスポリシー設定は、仮想サーバ、サービス、サービスグループ、サーバなど、すべてのサブノードに対して構成できます。

現時点では、負荷分散ノードの下のサブノードと GSLB ノードの下のサブノードに対してのみ、このような詳細なレベルのアクセス許可を提供できます。

たとえば、管理者は、[Load Balancing] ノードのバックエンドサービス、サービスグループ、およびアプリケーションサーバーではなく、仮想サーバーを表示するためのアクセス権のみをユーザーに付与できます。このようなポリシーが割り当てられているユーザーは、仮想サーバーにのみアクセスできます。

ユーザー定義のアクセスポリシーを作成するには、次の手順を実行します。

1. Citrix ADM GUI で、［アカウント］>［ユーザー管理］>［アクセスポリシー］に移動します。
2. ［追加］をクリックします。
3. [アクセスポリシーの作成] ページの [ポリシー名] フィールドにポリシーの名前を入力し、[ポリシーの説明] フィールドに説明を入力します。



［アクセス許可］セクションには、Citrix ADM のすべての機能が一覧表示され、読み取り専用、有効/無効化、または編集アクセス権を指定するためのオプションが表示されます。

a) ［+］アイコンをクリックして、各機能グループを複数の機能に展開します。

b) 機能名の横にある [権限] チェックボックスをオンにして、ユーザーに権限を付与します。

- 表示：このオプションを使用すると、ユーザーは Citrix ADM でこの機能を表示できます。

- 有効/無効化：このオプションは、Citrix ADM で有効/無効のアクションを許可する ネットワーク機能でのみ使用できます。ユーザーは、この機能を有効または無効にすることができます。また、ユーザーは [今すぐポーリング] アクションを実行することもできます。

  ユーザーに「有効/無効化」権限を付与すると、「表示」権限も付与されます。このオプションの選択を解除することはできません。

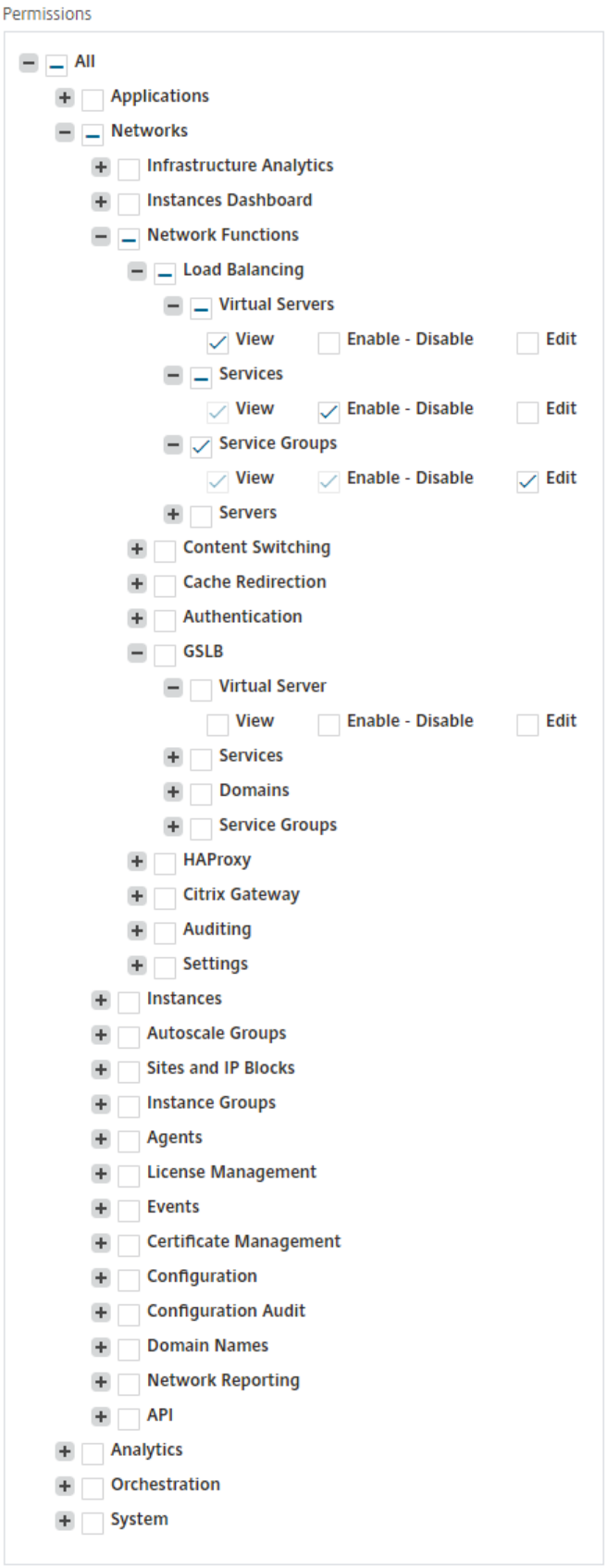
- 編集：このオプションは、ユーザーにフルアクセスを許可します。ユーザーはフィーチャーとその機能を変更できます。

  編集権限を付与すると、表示権限と 有効化/無効化権限の両方が付与されます。自動選択オプションの選択を解除することはできません。

[機能] チェックボックスをオンにすると、その機能に対するすべての権限が選択されます。

> 注:
>
> 負荷分散と GSLB を展開して、より多くの構成オプションを表示します。

次の図では、負荷分散機能の構成オプションに異なる権限があります。



仮想サーバ機能に対する 表示権限は、ユーザーに付与されます。ユーザーは、Citrix ADM で負荷分散仮想サーバーを表示できます。仮想サーバーを表示するには、[ネットワーク**] > [**** ネットワーク機能 **] > [負荷分散] に移動し、[仮想サーバー] タブを選択します。

サービス機能の 有効化/無効化権限は、ユーザーに付与されます。この権限は、表示権限も付与します。ユーザーは、負荷分散仮想サーバーにバインドされたサービスを有効または無効にすることができます。また、ユーザーはサービスに対して [今すぐポーリング] アクションを実行できます。サービスを有効または無効にするには、[ネットワーク**] > [**** ネットワーク機能 **] > [負荷分散] に移動し、[サービス] タブを選択します。

> 注:
>
> ユーザーが **Enable-Disable** アクセス許可を持っている場合、次のページで、サービスの有効化/無効化アクションが制限されます。
>
> a) [ネットワーク] > [ネットワーク機能] に移動します。
>
> b) 仮想サーバを選択し、［構成］ をクリックします。
>
> c) [負荷分散仮想サーバーサービスのバインド] ページを選択します。
> [有効] または [無効] を選択すると、このページにエラーメッセージが表示されます。

編集権限は、サービスグループ機能に対してユーザーに付与されます。このパーミッションは、「表示」および「有効化」および「無効化」のパーミッションが付与される完全なアクセスを付与します。ユーザーは、負荷分散仮想サーバーにバインドされているサービスグループを変更できます。サービスグループを編集するには、[ネットワーク**] > [**** ネットワーク機能 **] > [負荷分散] に移動し、[サービスグループ] タブを選択します。

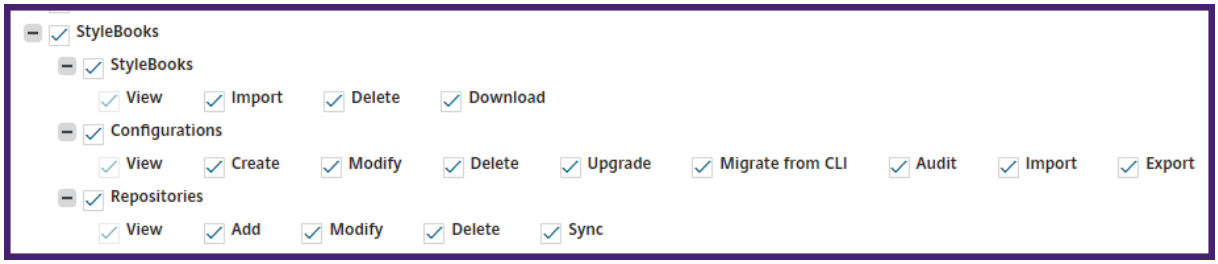
4. ［作成］ をクリックします。

> 注
>
> [編集**]** を選択すると、[権限] セクションに有効として表示されない依存アクセス許可が内部的に割り当てられることがあります。たとえば、障害管理の編集権限を有効にすると、Citrix ADM は、メールプロファイルの構成または SMTP サーバー設定の作成のためのアクセス許可を内部的に提供します。これにより、ユーザーはレポートをメールとして送信できます。

ユーザーに **StyleBook** パーミッションを付与する

アクセスポリシーを作成して、StyleBook のインポート、削除、ダウンロードなどの権限を付与できます。

> 注:
>
> 他の StyleBook 権限を付与すると、表示権限は自動的に有効になります。



Citrix ADM での役割の構成

Citrix ADM では、各役割は 1 つ以上のアクセスポリシーにバインドされます。ポリシーと役割には、1 対 1、1 対多、多対多の関係を定義できます。1 つの役割を複数のポリシーにバインドすることも、複数の役割を 1 つのポリシーにバインドすることもできます。

たとえば、ある機能のアクセス権を定義するポリシーと別の機能のアクセス権を定義する別のポリシーの 2 つのポリシーに、1 つの役割をバインドできます。一方のポリシーは、Citrix ADM で Citrix ADC インスタンスを追加するアクセス許可を付与し、もう 1 つのポリシーでは、StyleBook を作成して展開し、Citrix ADC インスタンスを構成するためのアクセス許可を付与します。

1 つの機能に対して複数のポリシーで編集権限と読み取り専用権限が定義されている場合、編集権限は読み取り専用権限よりも優先されます。

Citrix ADM には、次の 5 つの事前定義された役割が用意されています。

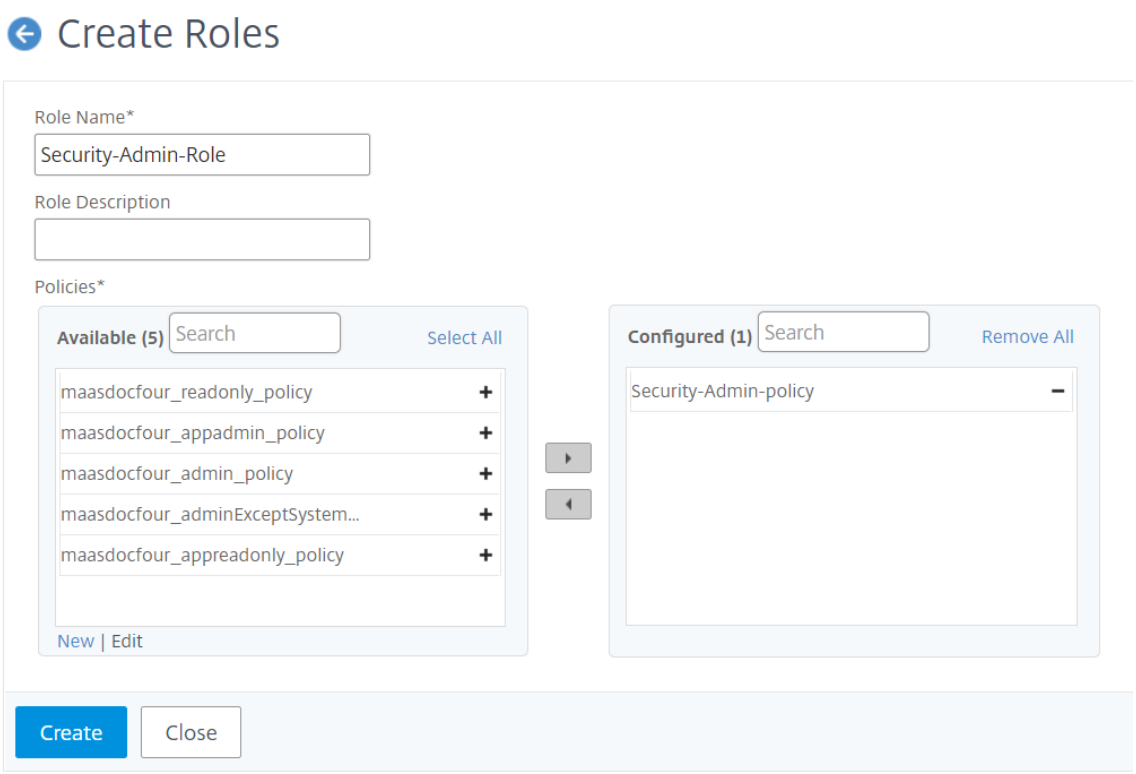
- **admin_role**。すべての Citrix ADM 機能にアクセスできます。(このロールは`adminpolicy`にバインドされています)。
- **adminExceptSystem_Role**。設定権限以外の Citrix ADM GUI にアクセスできる。(このロールは adminExceptSystem_Policy にバインドされています)
- **readonly_role**。読み取り専用アクセスが設定されています (このロールは`readonlypolicy`にバインドされています)。
- **appadmin_role**。Citrix ADM アプリケーション機能にのみ管理者権限が付与されます。(この役割は appAdminPolicy にバインドされています)。
- **appreadonly_role**。アプリケーション機能への読み取り専用アクセス権を持ちます。(この役割は appReadOnlyPolicy にバインドされています)。

定義済みのロールを編集することはできませんが、独自の (ユーザー定義) ロールを作成することはできます。

ロールを作成してポリシーを割り当てるには、次の手順に従います。

1. Citrix ADM GUI で、[アカウント] > [ユーザー管理] > [ロール] に移動します。
2. [追加] をクリックします。
3. [ロールの作成] ページの [ロール名] フィールドにロールの名前を入力し、[ロールの説明] フィールドに説明を入力します (オプション)。
4. [ポリシー] セクションで、1 つまたは複数のポリシーを [構成済み] リストに追加します。

> 注
>
> ポリシーには、すべてのテナントに固有のテナント ID（maasdocfourなど）が事前に固定されています。



> 注:
>
> [新規] をクリックしてアクセスポリシーを作成するか、[アカウント] > [ユーザー管理] > [アクセスポリシー] に移動してポリシーを作成できます。

5. [作成] をクリックします。

Citrix ADM でのグループの構成

Citrix ADM では、グループには機能レベルとリソースレベルのアクセス権の両方があります。たとえば、あるユーザーのグループが、選択した Citrix ADC インスタンスのみにアクセスしたり、少数のアプリケーションしかアクセスできない別のグループにアクセスしたりできます。

グループを作成するときに、グループにロールを割り当てたり、グループへのアプリケーションレベルのアクセスを提供したり、ユーザーをグループに割り当てることができます。Citrix ADM では、そのグループのすべてのユーザーに、同じアクセス権が割り当てられます。

Citrix ADM では、ネットワーク機能エンティティの個々のレベルでユーザーアクセスを管理できます。エンティティレベルでユーザーまたはグループに特定のアクセス許可を動的に割り当てることができます。

Citrix ADM は、仮想サーバー、サービス、サービスグループ、およびサーバーをネットワーク機能エンティティとして扱います。

- 仮想サーバー（アプリケーション）：負荷分散（lb）、GSLB、コンテキストスイッチング（CS）、キャッシュリダイレクト（CR）、認証（Auth）、および Citrix Gateway（vpn）
- サービス -負荷分散と GSLB サービス
- サービスグループ -負荷分散と GSLB サービスグループ
- サーバ -負荷分散サーバ

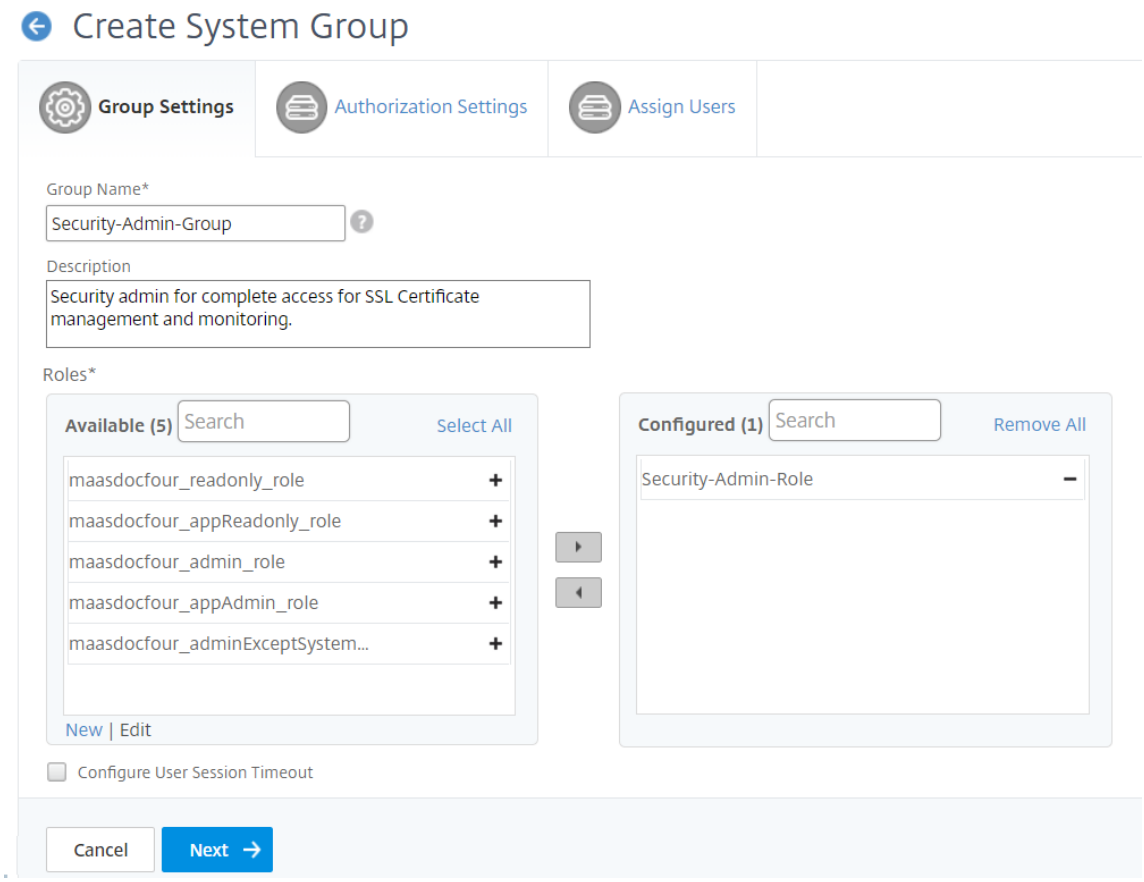
グループを作成するには、次の手順に従います。

1. Citrix ADM で、［アカウント］>［ユーザー管理］>［グループ］に移動します。
2. ［追加］をクリックします。

   「システム・グループの作成」ページが表示されます。
3. [グループ名] フィールドに、グループの名前を入力します。
4. [グループの説明] フィールドに、グループの説明を入力します。適切な説明を提供することで、グループの役割と機能を理解するのに役立ちます。
5. [ロール] セクションで、1 つまたは複数のロールを [構成済み] リストに移動します。

   > 注
   >
   > ロールには、すべてのテナントに固有のテナント ID（maasdocfourなど）が事前に固定されています。
6. [使用可能] ボックスの一覧で、[新規] または [編集] をクリックし、ロールを作成または変更できます。

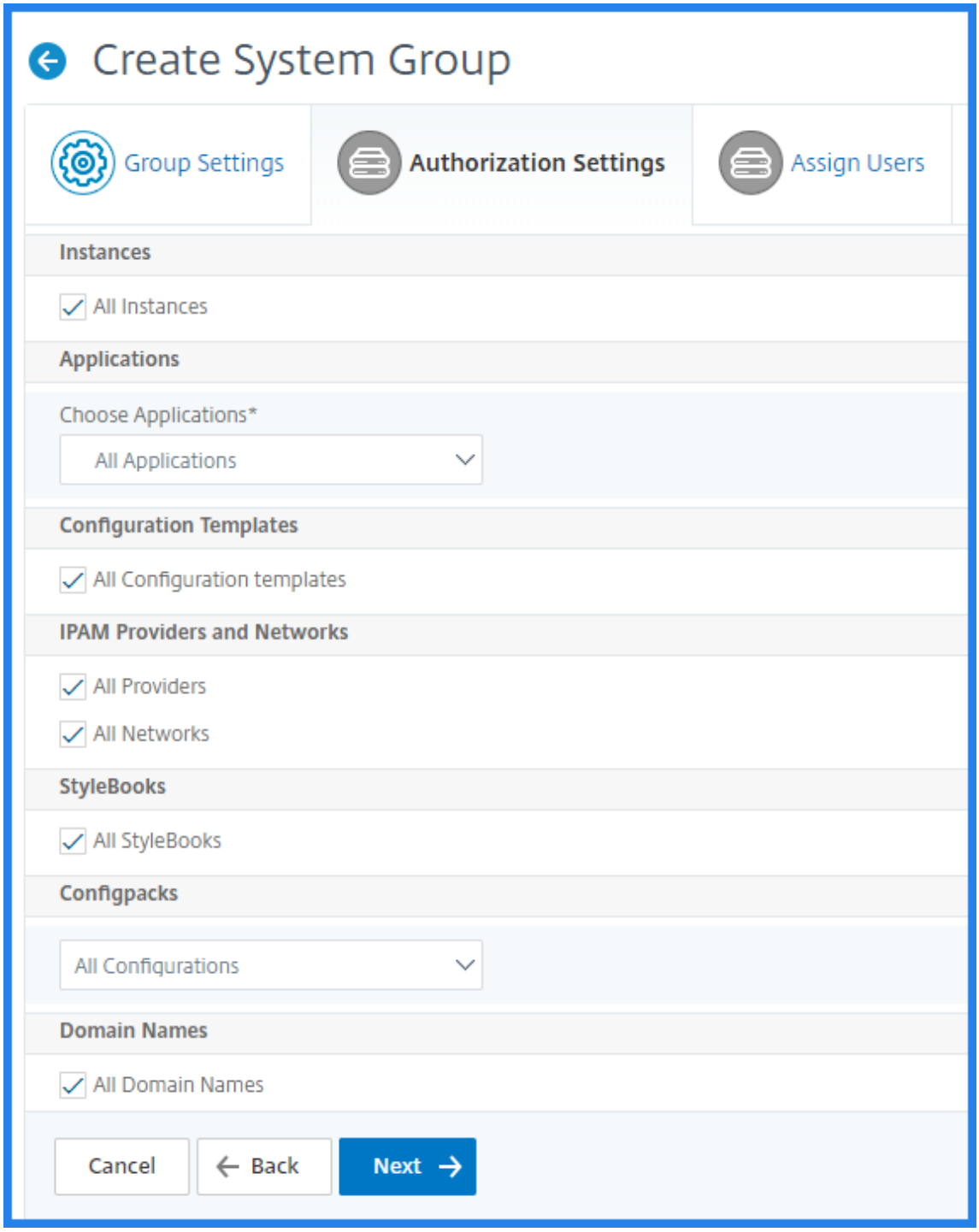
   または、[アカウント] > [ユーザー管理] > [ユーザー] に移動して、ユーザーを作成または変更することもできます。



7. [次へ] をクリックします。

8. [認証設定] タブでは、次のカテゴリからリソースを選択できます。

   - **AutoScale** グループ
   - インスタンス
   - アプリケーション
   - 構成テンプレート
   - **IPAM** プロバイダーとネットワーク
   - **StyleBook**
   - **Configpacks**
   - ドメイン名



ユーザーがアクセスできるカテゴリから特定のリソースを選択することもできます。

AutoScale グループ**:**

ユーザーが表示または管理できる特定の AutoScale グループを選択する場合は、次の手順に従います。

a) [すべての **AutoScale** グループ] チェックボックスをオフにし、[**AutoScale** グループの追加] をクリックします。

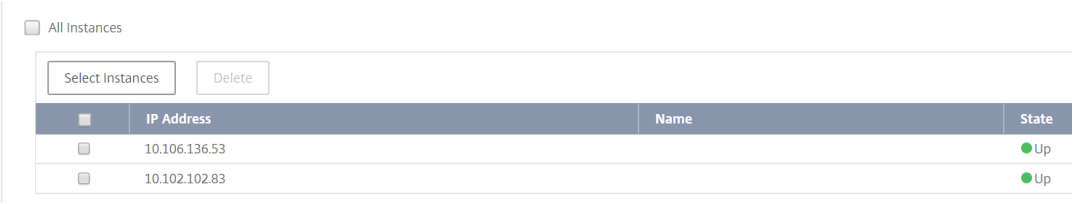
b) リストから必要な AutoScale グループを選択し、「**OK**」をクリックします。

インスタンス**:**

ユーザーが表示または管理できる特定のインスタンスを選択する場合は、次の手順を実行します。

a) [すべてのインスタンス] チェックボックスをオフにして、[インスタンスを選択] をクリックします。

b) リストから必要なインスタンスを選択し、「**OK**」をクリックします。



アプリケーション**:**

「アプリケーションの選択」リストでは、必要なアプリケーションへのアクセス権をユーザーに付与できます。

インスタンスを選択せずに、アプリケーションへのアクセスを許可できます。アプリケーションは、ユーザーアクセスを許可するためにインスタンスから独立しているためです。

アプリケーションへのアクセス権をユーザーに付与すると、インスタンスの選択に関係なく、そのアプリケーションのみにアクセスする権限が付与されます。

このリストには、次のオプションがあります。

- すべてのアプリケーション**:** このオプションはデフォルトで選択されています。これは、Citrix ADM に存在するすべてのアプリケーションを追加します。
- [選択したインスタンスのすべてのアプリケーション**]:** このオプションは、[すべてのインスタンス**]** カテゴリからインスタンスを選択した場合にのみ表示されます。これは、選択したインスタンスに存在するすべてのアプリケーションを追加します。
- 特定のアプリケーション**:** このオプションでは、ユーザーがアクセスできるように必要なアプリケーションを追加できます。「アプリケーションの追加」をクリックし、リストから必要なアプリケーションを選択します。
- **[** 個々のエンティティタイプを選択**]:** このオプションでは、ネットワーク機能エンティティと対応するエンティティの特定のタイプを選択できます。

  個々のエンティティを追加するか、必要なエンティティタイプの下にあるすべてのエンティティを選択して、ユーザーにアクセスを許可できます。

  [バインドされたエンティティにも適用] オプションは、選択したエンティティタイプにバインドされているエンティティを承認します。たとえば、アプリケーションを選択し、**[**バインドされたエンティティにも適用] を選択すると、選択したアプリケーションにバインドされているすべてのエンティティが Citrix ADM によって承認されます。

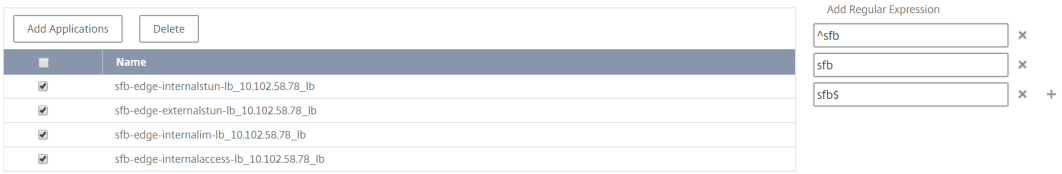
> 注記
>
> バインドされたエンティティを承認する場合は、エンティティタイプを 1 つだけ選択してください。

正規表現を使用して、グループの正規表現条件を満たすネットワーク関数エンティティを検索して追加できます。指定した正規表現式は、Citrix ADM で保持されます。正規表現を追加するには、次の手順を実行します。

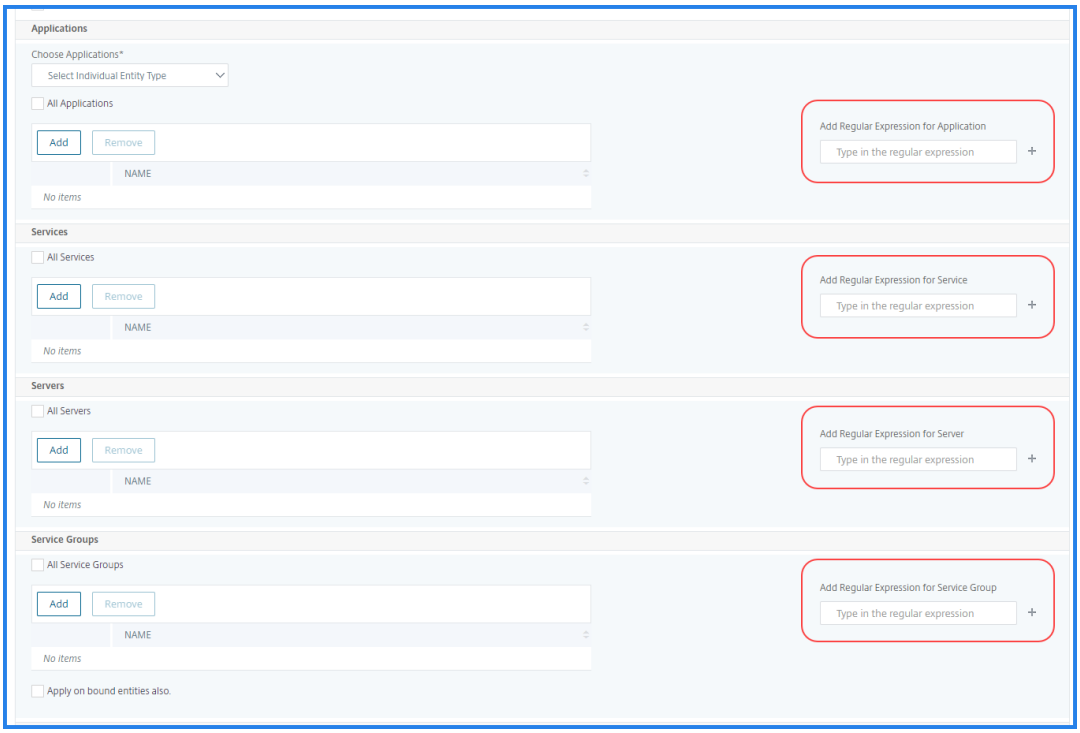
a) [正規表現の追加] をクリックします。

b) テキストボックスに正規表現を指定します。

次の図は、「特定のアプリケーション」オプションを選択した場合に、正規表現を使用してアプリケーションを追加する方法を示しています。



次の図は、[個々のエンティティタイプを選択] オプションを選択した場合に、正規表現を使用してネットワーク関数エンティティを追加する方法を示しています。



正規表現を追加する場合は、[+] アイコンをクリックします。

> 注:**
>
> 正規表現は、サーバーエンティティタイプのサーバー名にのみ一致し、サーバー IP アドレスには一致し

> ません。**

検出されたエンティティの **[**バインドされたエンティティにも適用] オプションを選択すると、ユーザーは検出されたエンティティにバインドされたエンティティに自動的にアクセスできます。

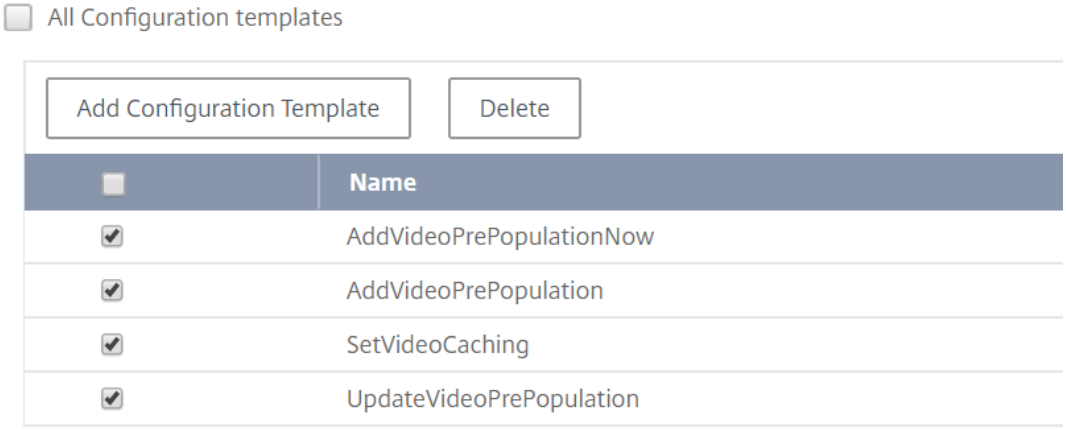
正規表現は、認可スコープを更新するためにシステムに格納されています。新しいエンティティがエンティティタイプの正規表現と一致すると、Citrix ADM は新しいエンティティに認証スコープを更新します。

構成テンプレート**:**

ユーザが表示または管理できる特定の設定テンプレートを選択する場合は、次の手順を実行します。

a) [すべての構成テンプレート] チェックボックスをオフにし、[構成テンプレートの追加] をクリックします。

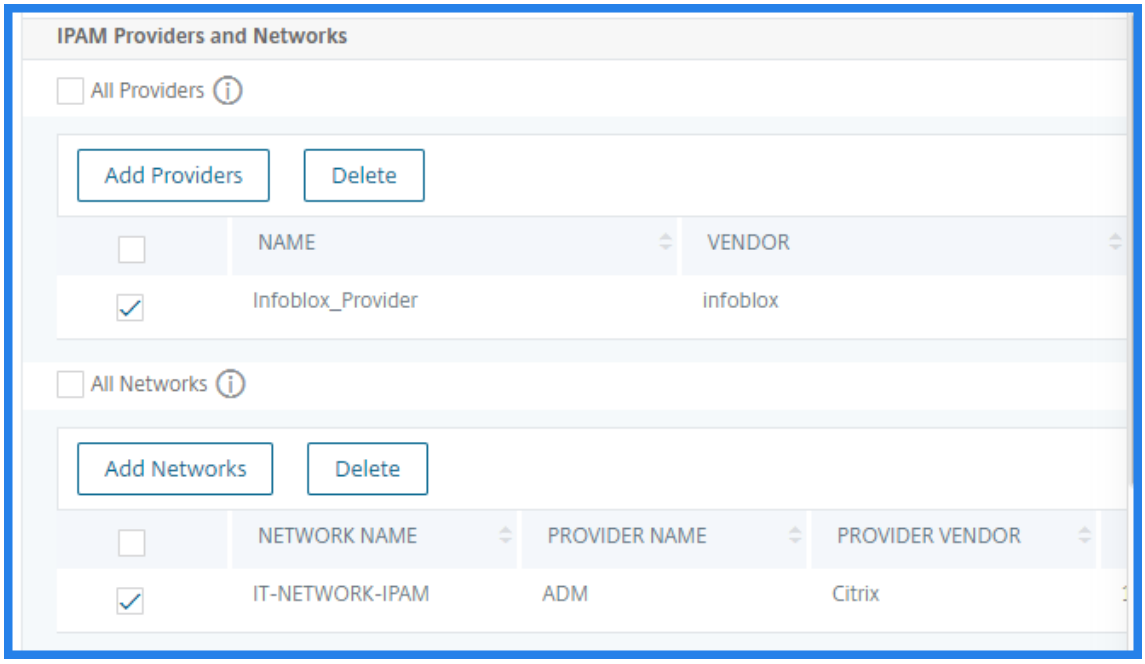
b) リストから目的のテンプレートを選択し、[**OK**] をクリックします。



IPAM プロバイダーとネットワーク**:**

ユーザーが表示または管理できる特定の IPAM プロバイダーとネットワークを追加する場合は、次の手順を実行します。

- プロバイダの追加 -[すべてのプロバイダ] チェックボックスをオフにし、[プロバイダの追加] をクリックします。必要なプロバイダを選択し、「**OK**」をクリックします。
- ネットワークの追加 -[すべてのネットワーク] チェックボックスをオフにし、[ネットワークの追加] をクリックします。必要なネットワークを選択し、[**OK**] をクリックします。



スタイルブック**:**

ユーザーが表示または管理できる特定の StyleBook を選択する場合は、次の手順を実行します。

a)「すべてのスタイルブック」チェックボックスをオフにして、「グループにスタイルブックを追加」をクリックします。StyleBooks を個別に選択することも、フィルタクエリを指定して StyleBooks を承認することもできます。

個々の StyleBooks を選択する場合は、「個別 StyleBooks」ペインから **StyleBooks** を選択し、「選択内容の保存」をクリックします。

クエリを使用して StyleBooks を検索する場合は、[カスタムフィルタ] ペインを選択します。クエリは、キーと値のペアの文字列です。キーは `name`、`namespace`、`version`です。

正規表現を値として使用して、グループの正規表現条件を満たす StyleBook を検索して追加することもできます。StyleBooks を検索するカスタムフィルタクエリは、`And`と`Or`の両方をサポートしています。

例:

```
name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
    version=1.0
<!--NeedCopy-->
```

このクエリは、次の条件を満たす StyleBook をリストします。

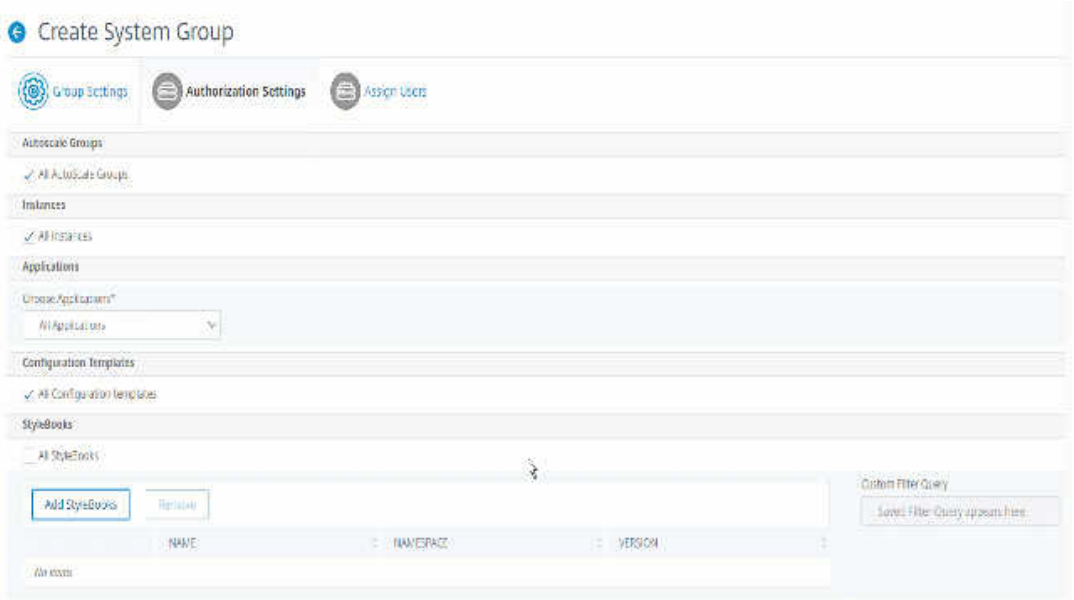
- StyleBook 名は`lb-mon`または`lb`のいずれかです。
- StyleBook の名前空間は`com.citrix.adc.stylebooks`です。
- StyleBook 版は `1.0`です。

キー式に定義された値式の間でOr演算を使用します。

例:

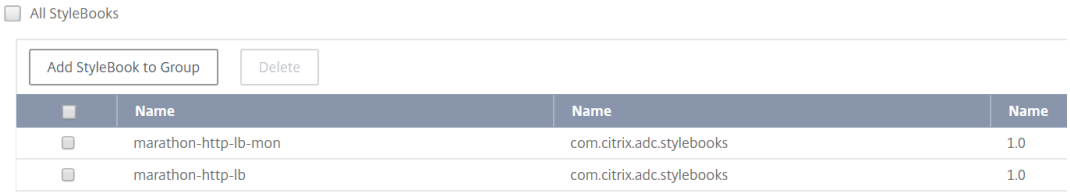
- name=lb-mon|lbクエリは有効です。これは、名前lb-monまたはlbのいずれかを持つ StyleBooks を返します。
- name=lb-mon | version=1.0 クエリは無効です。

Enterを押して検索結果を表示し、[クエリーの保存] をクリックします。



保存されたクエリが [カスタムフィルタクエリー] に表示されます。保存されたクエリに基づいて、ADM はそれらの StyleBook へのユーザーアクセスを提供します。

b) リストから必要な StyleBook を選択し、「**OK**」をクリックします。



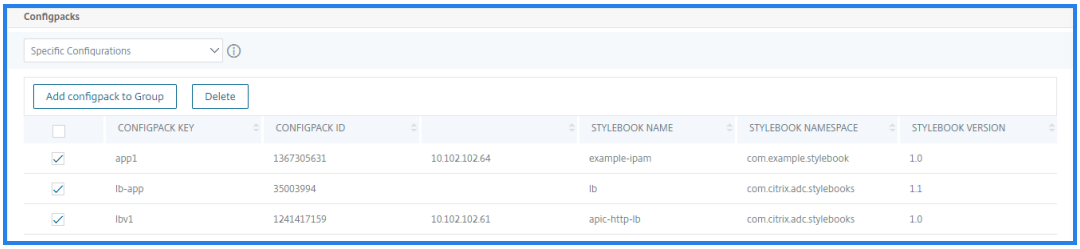
グループを作成し、そのグループにユーザーを追加するときに、必要な StyleBook を選択できます。ユーザーが許可された StyleBook を選択すると、依存するすべての StyleBook も選択されます。

コンフィグパック**:**

Configpacks で、次のいずれかのオプションを選択します。

- [すべての設定]: このオプションはデフォルトで選択されています。ADM にあるすべての構成パックが追加されます。
- 選択した **StyleBook** のすべての構成: このオプションでは、選択した StyleBook のすべての構成パックが追加されます。

- 特定の構成: このオプションでは、必要な構成パックを追加できます。



グループを作成し、そのグループにユーザーを追加するときに、必要な構成パックを選択できます。

ドメイン名**:**

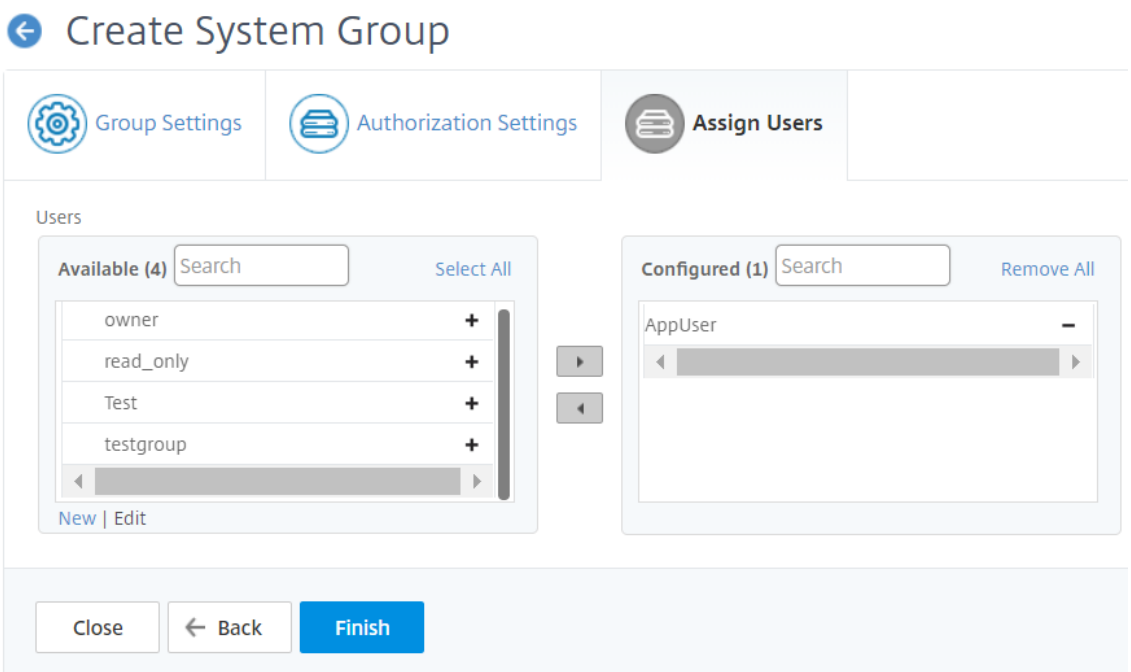
ユーザーが表示または管理できる特定のドメイン名を選択する場合は、次の手順を実行します。

a) [すべてのドメイン名] チェックボックスをオフにし、[ドメイン名の追加] をクリックします。

b) リストから必要なドメイン名を選択し、[**OK**] をクリックします。

9. [**Create Group**] をクリックします。
10. [ユーザーの割り当て] セクションで、[使用可能] ボックスの一覧でユーザーを選択し、[構成済み] リストにユーザーを追加します。

> 注
>
> [新規] をクリックして、新しいユーザーを追加することもできます。



11. [完了] をクリックします。

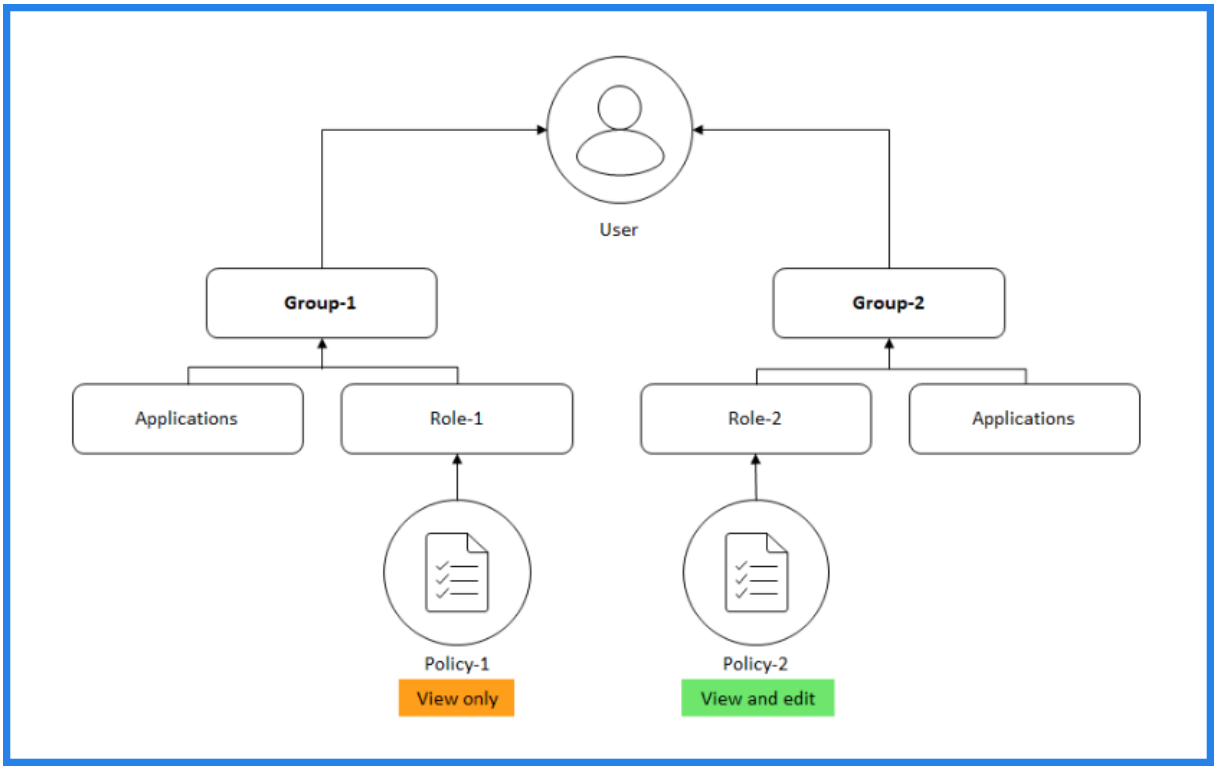
承認スコープに基づくユーザーアクセスの変更方法

管理者が異なるアクセスポリシー設定を持つグループにユーザーを追加すると、そのユーザーは複数の承認スコープとアクセスポリシーにマップされます。

この場合、ADM は、特定の認可スコープに応じて、アプリケーションへのユーザアクセスを許可します。

ポリシー 1 とポリシー 2 の 2 つのポリシーを持つグループに割り当てられているユーザを考えてみましょう。

- **Policy-1**： アプリケーションに対する権限のみを表示します。
- ポリシー **2**： アプリケーションに対する表示および編集権限。



ユーザーは、Policy-1 で指定されたアプリケーションを表示できます。また、このユーザーは、Policy-2 で指定されたアプリケーションを表示および編集できます。Group-1 アプリケーションに対する編集アクセスは、Group-1 認可スコープにはないため、制限されます。

制限事項

RBAC は、次の Citrix ADM 機能では完全にはサポートされていません。

- 分析- RBAC は、分析モジュールによって完全にはサポートされていません。RBAC のサポートはインスタンスレベルに制限され、Gateway Insight、HDX Insight、Security Insight 分析モジュールのアプリケーションレベルでは適用されません。
  - 例 1: インスタンスベースの RBAC (サポート)。いくつかのインスタンスを割り当てられている管理者は、**[HDX Insight] > [**** デバイス] でそれらのインスタンスと [**HDX Insight**] > [**Applications**]

の下にある対応する仮想サーバーのみを表示できます。これは、RBAC がインスタンスレベルでサポートされているためです。**

  - 例 2: アプリケーションベースの RBAC (サポートされていません)。いくつかのアプリケーションが割り当てられている管理者は、**[**HDX Insight**] > [アプリケーション] の下にすべての仮想サーバーを表示できますが、それらにアクセスすることはできません。これは、RBAC はアプリケーションレベルではサポートされていません。**
- StyleBooks — RBAC は、StyleBook では完全にサポートされていません。
  - 複数のユーザーが単一の StyleBook にアクセスできますが、異なる Citrix ADC インスタンスに対するアクセス権を持っている場合を考えます。ユーザーは、自分のインスタンス上で設定パックを作成および更新できますが、自分のインスタンス以外のインスタンスにはアクセスできないので、他のインスタンスでは設定パックを作成および更新できません。ただし、Citrix ADC インスタンス上で作成された構成パックとオブジェクトは、独自のもの以外のものでも表示できます。

アナリティクス設定の構成

May 7, 2021

Citrix Application Delivery Management（Citrix ADM）の分析機能を使用して、インスタンスとアプリケーションデータを可視化する前に、この機能で最適なエクスペリエンスを確保するために、いくつかの分析設定を構成することをお勧めします。

分析用のデータベース要約の設定

Citrix ADM データベース要約の構成機能を使用すると、Citrix ADC インスタンスの履歴分析データを保存する期間をカスタマイズできます。次のデータベース要約タイプを選択できます。

- 毎分データを保持する時間数
- 毎時間データを保持する日数
- 毎日データを保持する日数

データベース要約を構成するには、次の手順に従います。

1. サポートされている Web ブラウザで、Citrix ADM にログオンします。
2. [設定] > [アナリティクス設定**]** > [データベースの概要] に移動します。
3. データベース要約を設定するインサイトタイプの名前をクリックします。たとえば、Gateway Insight のデータベース要約を構成する場合は、「**GatewayInsight**」をクリックします。
4. Citrix ADM で Insight データを保持する期間を指定し、［**OK**］をクリックします。たとえば、Gateway Insight では、分析の詳細な履歴データを 2 時間、または 1 時間分のデータを 1 日保存できます。

分析用のしきい値とアラートの作成

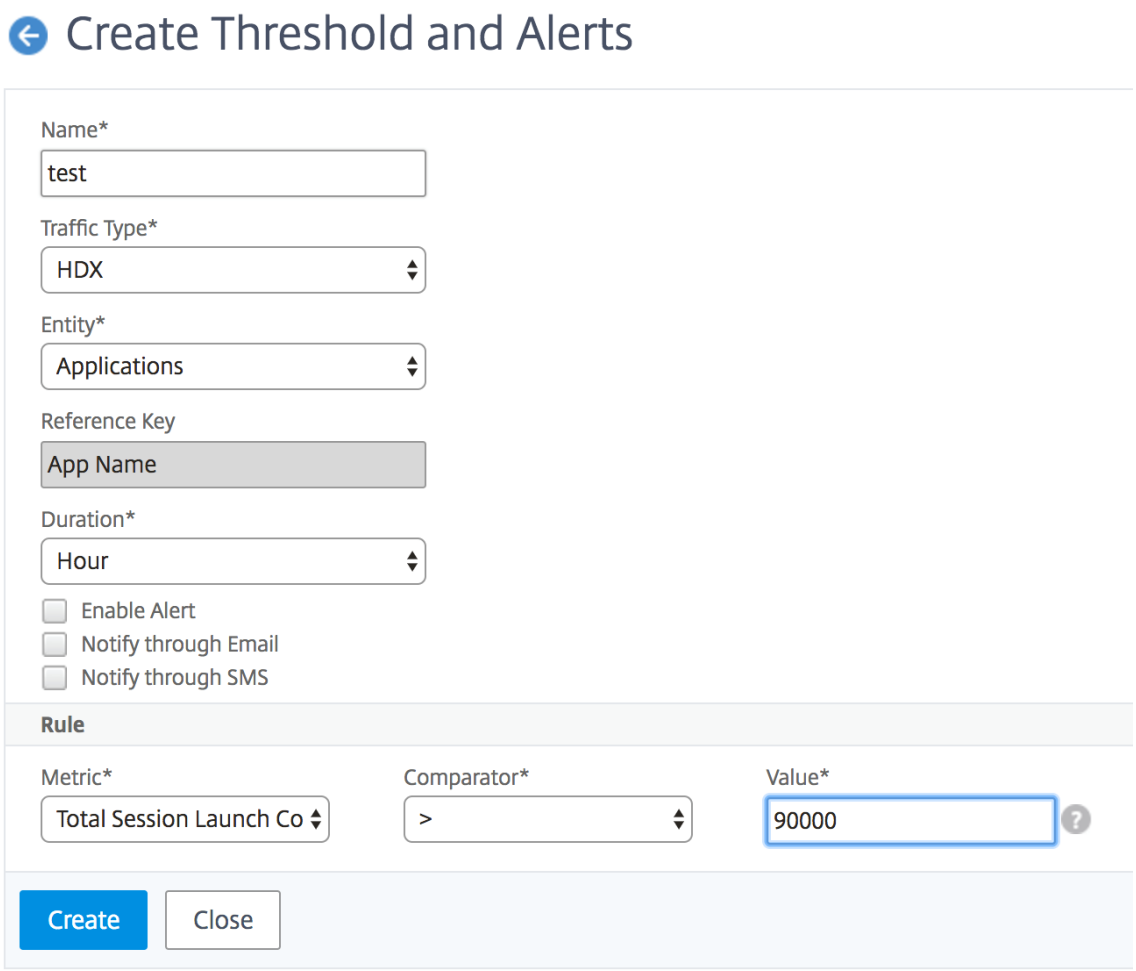
しきい値とアラートを設定して、検出されたインスタンスで構成された管理対象仮想サーバーの分析のメトリックスを監視できます。メトリックの値がしきい値を超えると、Citrix ADM はしきい値違反を示すイベントを生成します。

また、設定されたしきい値にアクションを関連付けることもできます。アクションには、GUI でのアラートの表示、設定済みのメールの送信が含まれます。

たとえば、いずれかのユーザーの ICA RTT 値が 1 秒を超えた場合に HDX Insight のイベントを生成するようにしきい値を設定できます。また、生成されたイベントのアラートを有効にし、しきい値違反情報を構成された電子メールリストに送信することもできます。

分析のしきい値とアラートを作成するには、次の手順に従います。

1. サポートされている Web ブラウザで、Citrix ADM にログオンします。
2. 設定 > アナリティクス設定 > しきい値の順にナビゲートします。
3. [**Thresholds**] 画面で、[**Add**] をクリックして新しいしきい値を追加し、設定したしきい値のアラートを構成します。
4. [**Create Thresholds and Alerts**] ページで次の詳細を指定します。
   - **Name** - しきい値の構成の名前
   - **[Traffic** Type] — しきい値を設定する分析トラフィックのタイプ。例:HDX Insight、Security Insight。
   - **Entity** - しきい値構成時のカテゴリまたはリソースの種類
   - **Reference Key** - トラフィックの種類とエンティティの選択に基づいて自動的に生成される値
   - **Duration** - しきい値構成時の間隔
5. 電子メール通知を構成するには、設定したしきい値のチェックボックスをオンにします。
6. [ルール] セクションで、次の項目を指定します。
   - [**Metric**]: しきい値を設定するための、選択したトラフィックタイプのメトリック。
   - **Comparator**： 選択したメトリック（<、>= など）へのコンパレータ。
   - **Value**： しきい値を設定し、アラートを起動するメトリックの値。
7. [作成] をクリックします。



委任された管理者ユーザーにさらに多くのアクセス許可を割り当てる方法

May 7, 2021

組織の最初のユーザーがサインアップして Citrix ADM（Citrix Application Delivery Management ADM）にログオンすると、このユーザーにはスーパー管理者権限が割り当てられます。既定では、後続のログオンするすべてのユーザーには、委任された管理者ロールが割り当てられます。委任された管理者には、ユーザー管理または RBAC 設定に関連するタスクを表示および実行する権限がありません。

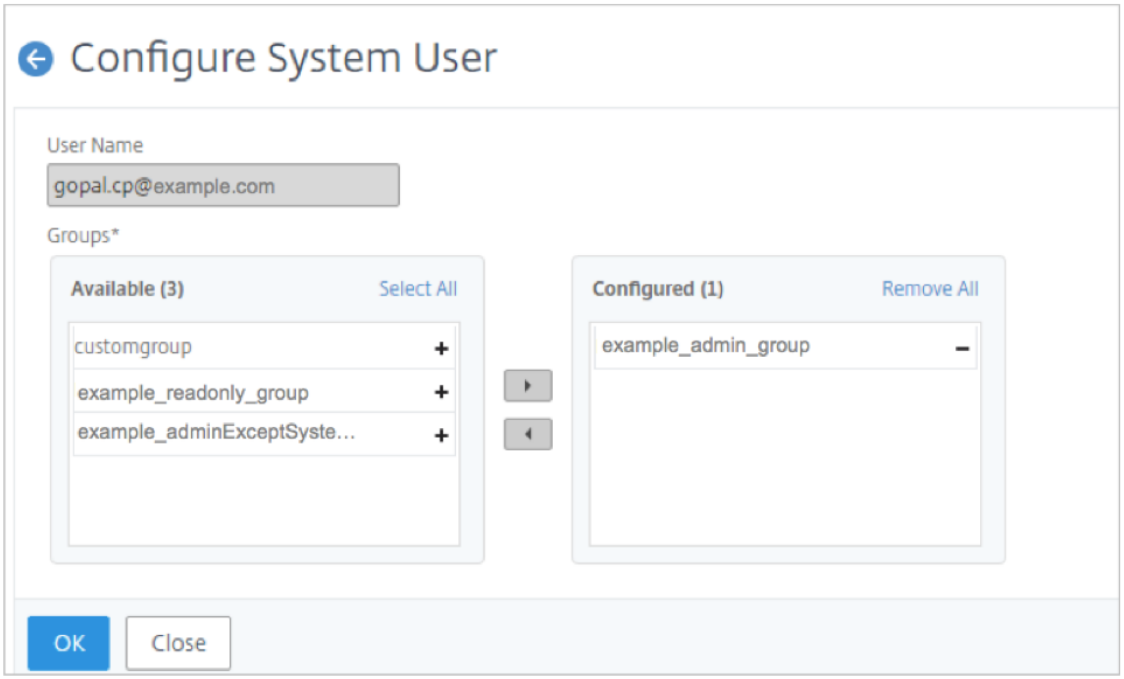
ただし、管理者がユーザー管理に関連するタスクを実行できるように、委任された管理者にスーパー管理者権限または特定の非スーパー管理者ロールを割り当てることができます。

ロールベースのアクセス制御の詳細については、ロールベースのアクセス制御の設定を参照してください。

委任された管理者へのスーパー管理者権限の割り当て

スーパー管理者権限を委任された管理者に割り当てるには、スーパー管理者はデフォルトの管理者グループを委任された管理者ユーザーに割り当てる必要があります。次のタスクを実行します。

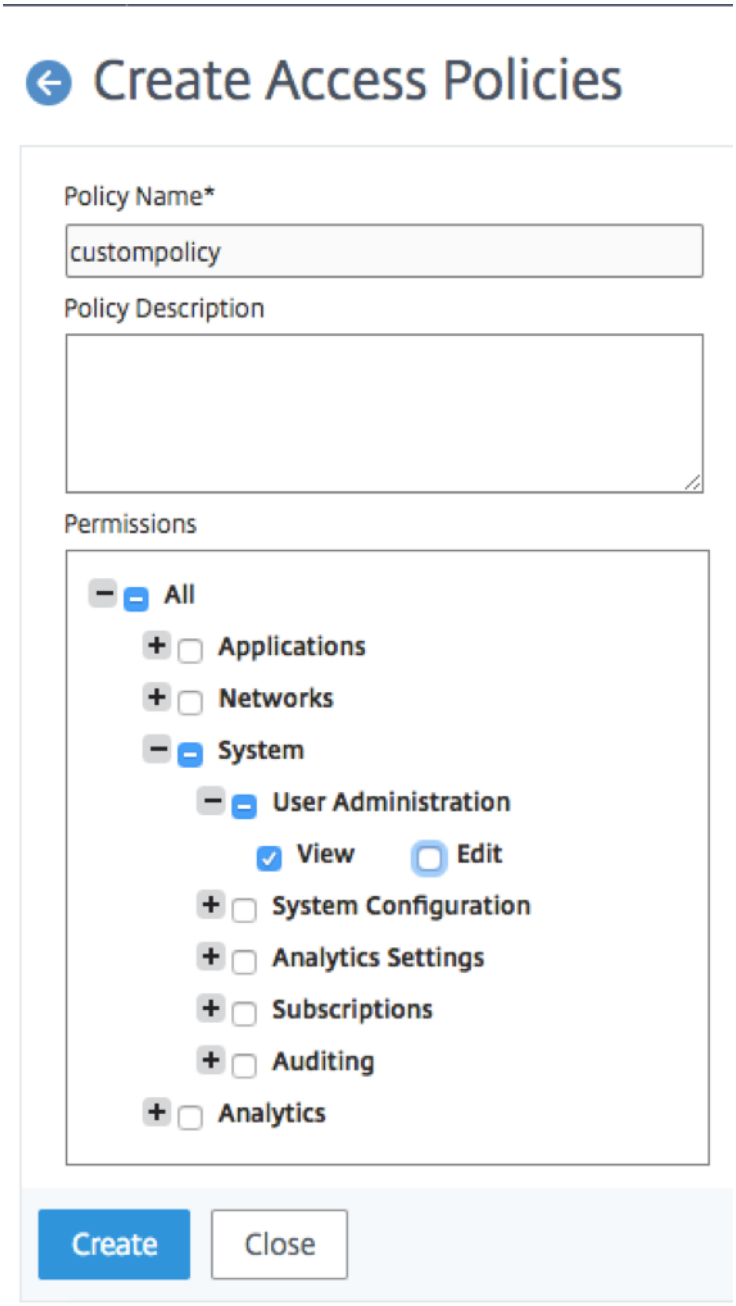
1. Citrix ADM にスーパー管理者としてログオンします。
2. [アカウント] > [ユーザー管理] > [ユーザー] に移動します。
3. 委任された管理者のユーザー名を選択し、[編集] をクリックします。
4. 委任された管理者にグループ **< tenant_name >_*admin_group*** を割り当てて、「**OK** 」をクリックします。** たとえば、次の図では、委任された管理者ユーザーに「example_admin_group」が割り当てられています。



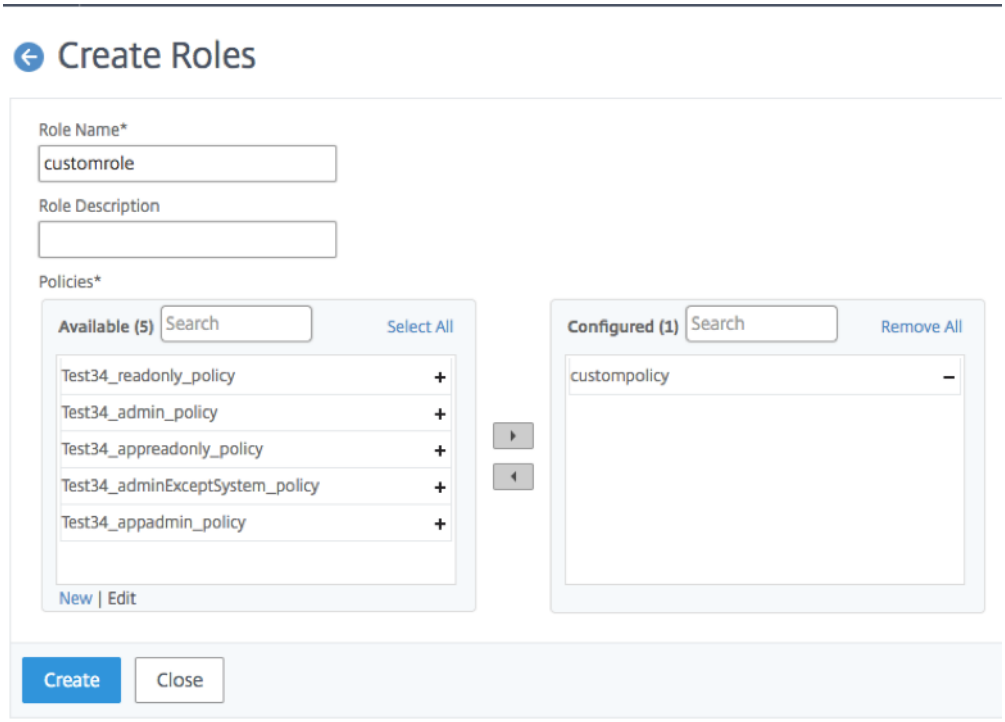
委任された管理者へのカスタムロールの割り当て

委任された管理者にカスタムロールを割り当てるには、スーパー管理者はグループ、ロール、ポリシーを作成し、委任された管理者ユーザーに割り当てる必要があります。これにより、委任された管理者は、必要なアクセス許可のみを持つようになります。次のタスクを実行します。

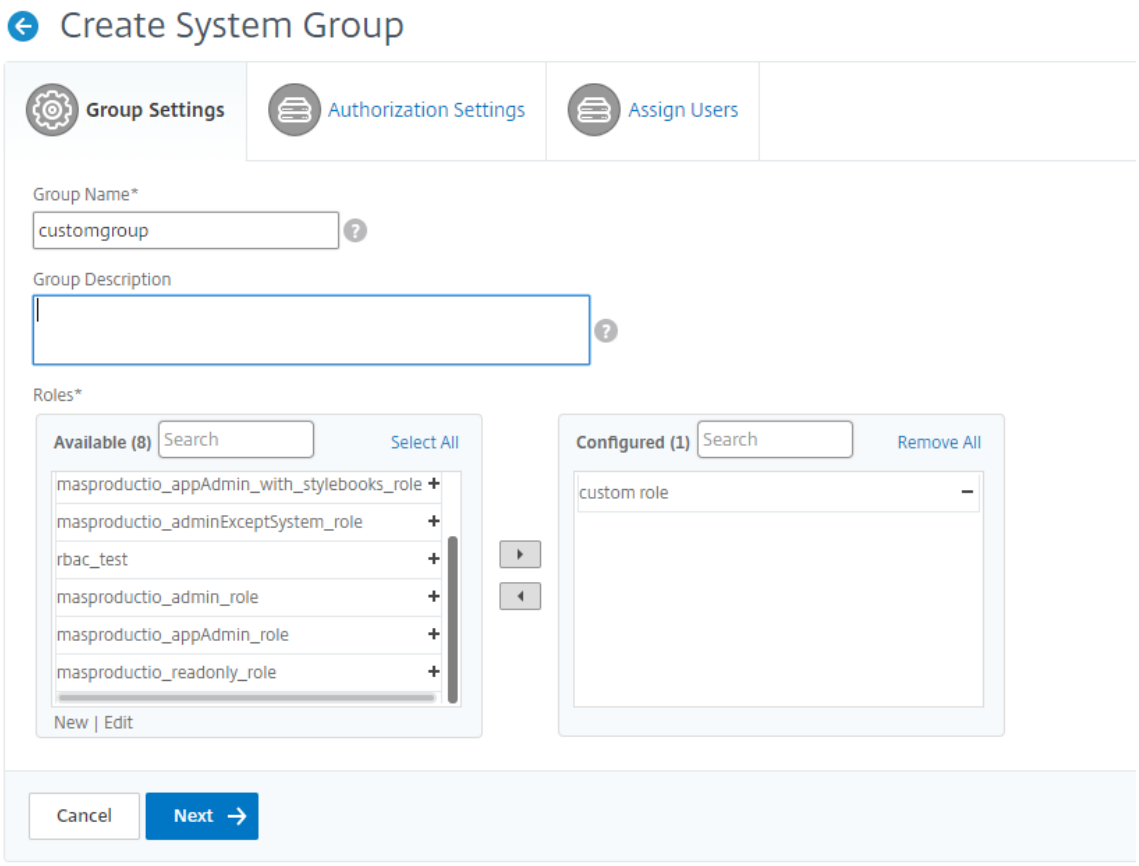
1. Citrix ADM にスーパー管理者としてログオンします。
2. [アカウント] > [ユーザー管理] > [アクセスポリシー] に移動します。[追加] を選択して、委任された管理者に必要なアクセス許可を使用してアクセスポリシーを作成します。この例では、ユーザー管理設定への表示アクセスを許可するアクセスポリシー`custompolicy`が作成されます。



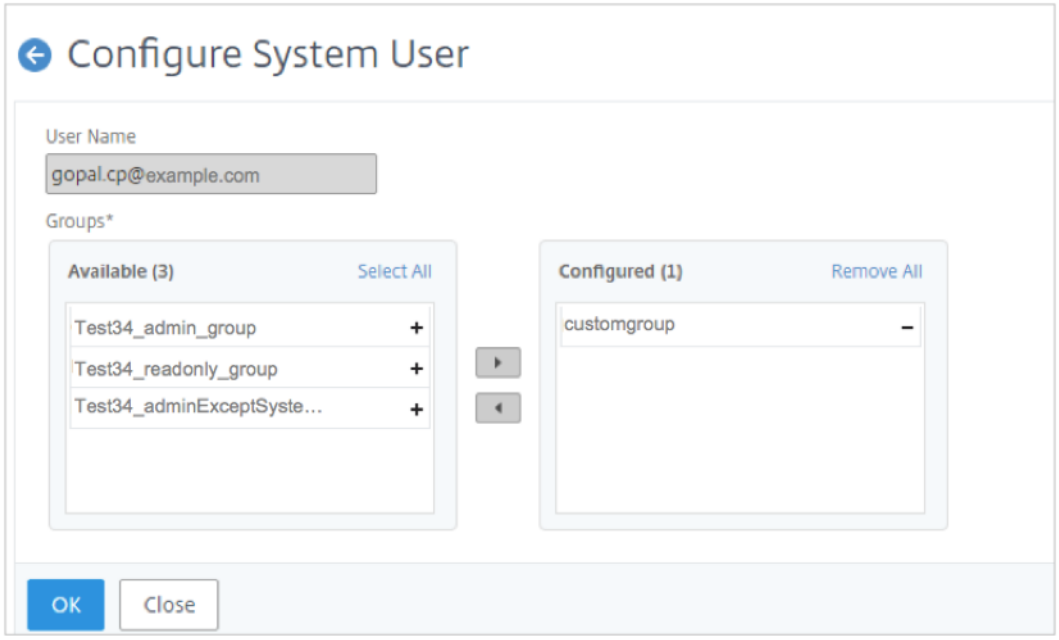
3. [アカウント] > [ユーザー管理] > [ロール] に移動します。[**Add**] を選択してロールを作成し、このロールを前の手順で作成したアクセスポリシーにバインドします。この例では、`customrole` ロールが作成され、`custompolicy` アクセスポリシーにバインドされます。



4. [アカウント] > [ユーザー管理] > [グループ] に移動します。[**Add**] を選択してグループを作成し、このグループを前の手順で作成したロールにバインドします。この例では、グループ「カスタムグループ」が作成され、ロール「カスタムロール」にバインドされます。



5. [アカウント] > [ユーザー管理] > [ユーザー] に移動します
6. 委任された管理者のユーザー名を選択し、[編集] をクリックします。
7. 前の手順で作成したグループを、委任された管理者ユーザーに割り当てます。この例では、委任された管理者ユーザーにグループ`customgroup`が割り当てられます。



Citrix ADM を ServiceNow インスタンスと統合する

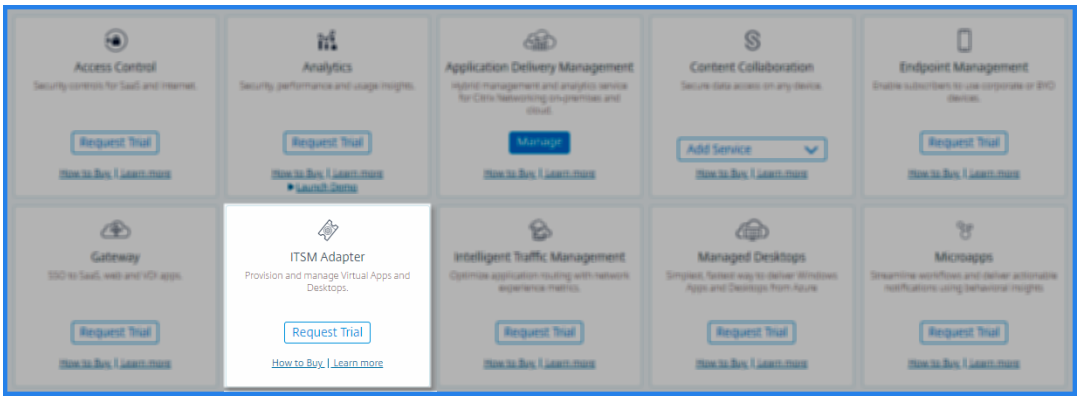
May 7, 2021

Citrix ADC イベントおよび ADM イベントの ServiceNow 通知を有効にする場合は、Citrix ADM を ServiceNow インスタンスに統合する必要があります。ADM を ServiceNow インスタンスと統合するには、Citrix ITSM コネクタを使用します。ITSM コネクタは、Citrix ADM と ServiceNow インスタンス間の通信を確立します。詳しくは、「ITSM アダプタの動作」を参照してください。

ITSM コネクタを使用して Citrix ADM と ServiceNow を統合するには、次の手順に従います。

1. Citrix Cloud で **ITSM** アダプタサービスを購読する

   a) [**ITSM** アダプタ] タイルで、[試用版の要求] をクリックします。



b) [**ID** アクセスと管理] > [**API** アクセス] に移動し、クライアント **ID** とクライアントシークレットの情報をメモします。

2. 管理者資格情報を使用して ServiceNow インスタンスにログインし、次の手順を実行します。

a) サービス Now ストアに移動します。**Citrix ITSM** コネクタをダウンロードしてインストールします。

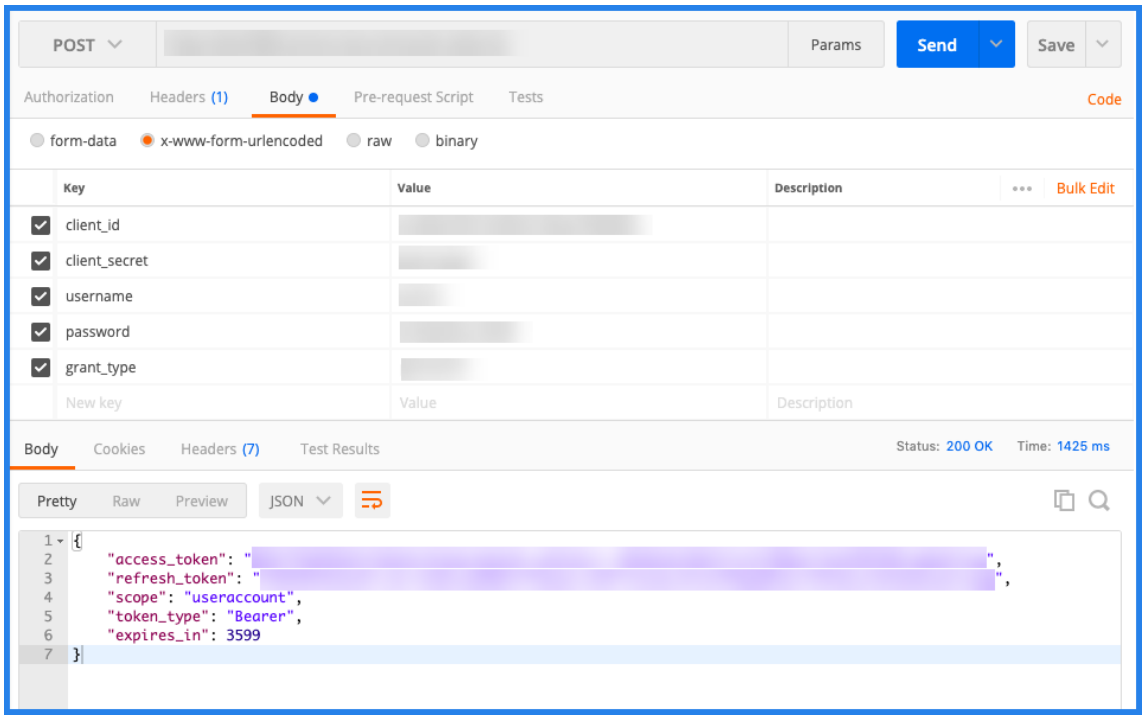
b) **Citrix ITSM** コネクタペインで、［ホーム］を選択し、［認証］をクリックします。Citrix Cloud からメモしたクライアント ID とシークレットを入力します。

c) 接続をテストします。

d) 構成を保存します。ServiceNow からの確認応答が表示され、接続がアクティブであることを示します。

3. ServiceNow インスタンスにアクセスするためのエンドポイントを作成します。「クライアントがインスタンスにアクセスするためのエンドポイントを作成する」を参照してください。

4. クライアント ID とクライアントシークレットを使用して、アクセストークンとリフレッシュトークンを取得します。「OAuth トークン」を参照してください。

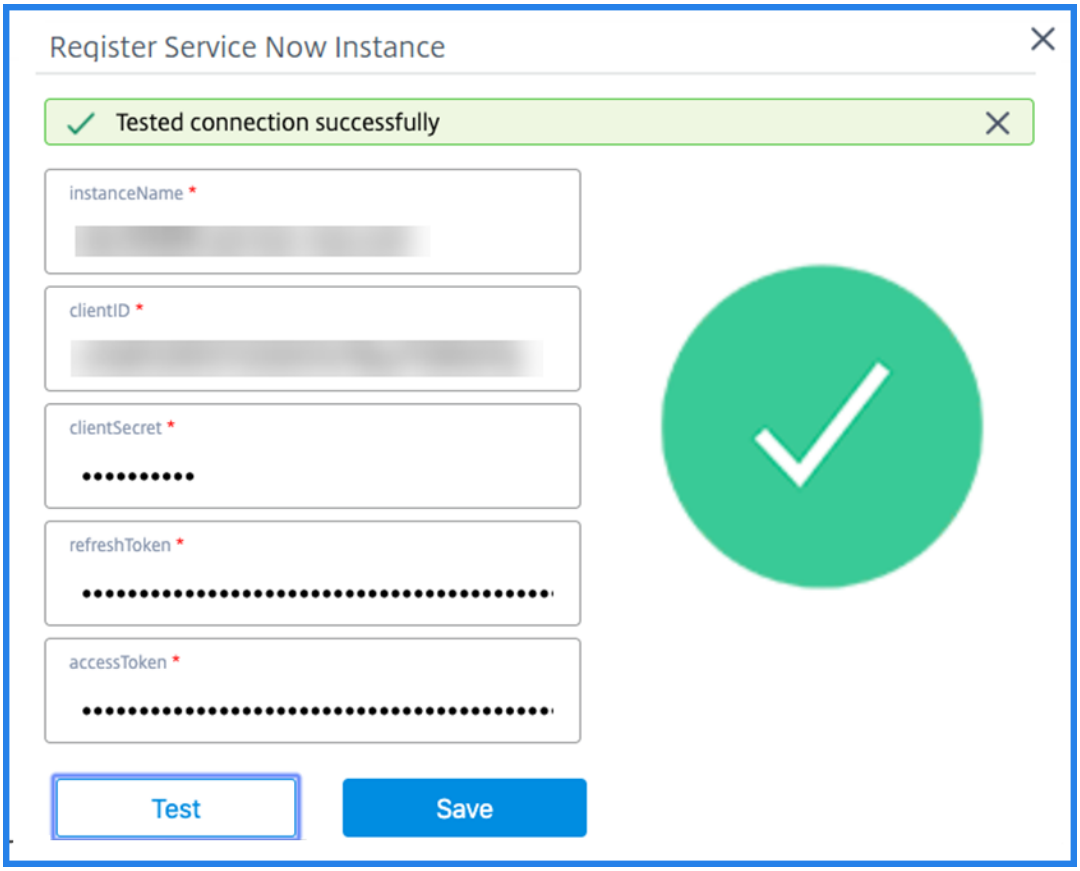


5. ITSM アダプタで、ServiceNow インスタンスを追加します。

a) [管理] タブで、[ServiceNow インスタンスの追加] を選択します。

b) インスタンス名、クライアント **ID**、クライアントシークレット、リフレッシュトークン、アクセストークンを指定します。

c) [テスト] をクリックします。



これで、ServiceNow インスタンスが ITSM アダプタサービスに接続されました。

d) 接続が正常にテストされたら、[保存] をクリックして ServiceNow インスタンスを追加します。

6. Citrix ADM で ServiceNow チケットの自動生成をテストします。

a) Citrix ADM にログインします。

b) [アカウント**] > [**通知] に移動し、[**ServiceNow**] を選択します。

c) リストから ServiceNow プロファイルを選択します。

d) [テスト] をクリックして、ServiceNow チケットを自動生成し、構成を確認します。

Citrix ADM GUI でサービスノウチケットを表示する場合は、［サービスノウチケット］を選択します。

ServiceNow インスタンスが ITSM アダプタに登録されると、Citrix ADM GUI で次のイベントに対する ServiceNow 通知を設定できます。

> 重要:
>
> この機能は、ServiceNow クラウドでサポートされています。

- **Citrix ADC** イベント: Citrix ADM は、選択した管理対象の Citrix ADC インスタンスから、選択した一連の Citrix ADC イベントの ServiceNoW インシデントを生成できます。

管理対象インスタンスから Citrix ADC イベントの ServiceNow 通知を送信するには、イベントルールを構成し、ルールのアクションを「**ServiceNow** 通知の送信」として割り当てる必要があります。

[ネットワーク**]** > **[**イベント**]** > **[**ルール**]** に移動して、ADM サービスでイベントルールを作成します。詳しくは、「サービスノウ通知の送信」を参照してください。

- **SSL** 証明書と **ADM** ライセンスイベント: Citrix ADM は、SSL 証明書の有効期限および ADM ライセンス有効期限イベントの ServiceNoW インシデントを生成できます。

  SSL 証明書の有効期限に関する ServiceNow 通知を送信するには、SSL 証明書の有効期限を参照してください。

  ADM ライセンスの有効期限に関する ServiceNow 通知を送信するには、Citrix ADM ライセンスの有効期限を参照してください。

エクスポートレポートのエクスポートまたはスケジュール設定

May 7, 2021

Citrix ADM では、選択した Citrix ADM 機能の包括的なレポートをエクスポートできます。このレポートには、インスタンス、パーティション、および対応する詳細間のマッピングの概要が表示されます。

Citrix ADM は、個別の ADM 機能の下に機能固有のスケジュールエクスポートレポートを表示します。これらのレポートは表示、編集、削除できます。たとえば、Citrix ADC インスタンスのエクスポートレポートを表示するには、［ネットワーク］**>**［インスタンス］**>**［**Citrix ADC** ］の順に選択し、［エクスポート］アイコンをクリックします。これらのレポートは、PDF、JPEG、PNG、および CSV ファイル形式でエクスポートできます。

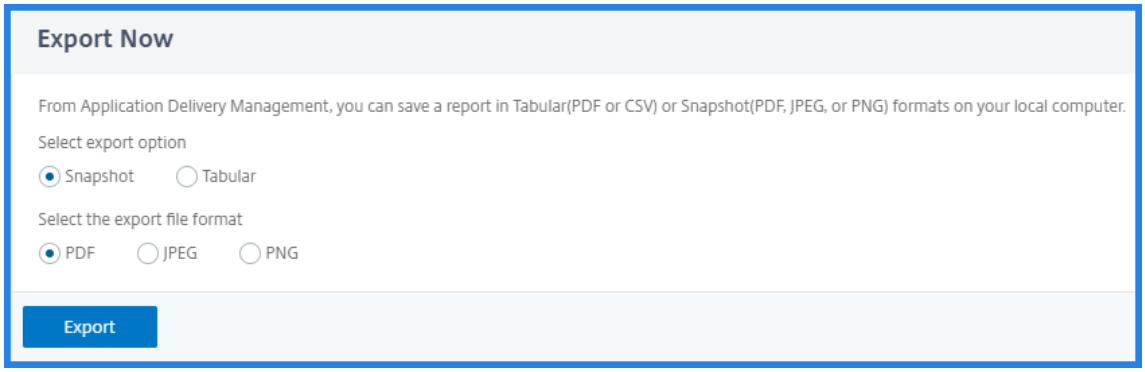
「レポートのエクスポート」では、次のアクションを実行できます。

- レポートをローカルコンピュータにエクスポートする
- エクスポートレポートのスケジュール設定
- スケジュール・エクスポート・レポートの表示、編集、削除

レポートのエクスポート

レポートを ADM からローカルコンピュータにエクスポートするには、次の手順に従います。

1. ページの右上隅にあるエクスポートアイコンをクリックします。
2. [今すぐエクスポート] を選択します。
3. 次のエクスポートオプションのいずれかを選択します。
   - [スナップショット]: このオプションは、ADM レポートをスナップショットとしてエクスポートします。
   - [表形式]: このオプションは、ADM レポートを表形式でエクスポートします。また、表形式でエクスポートするデータレコードの数を選択することもできます

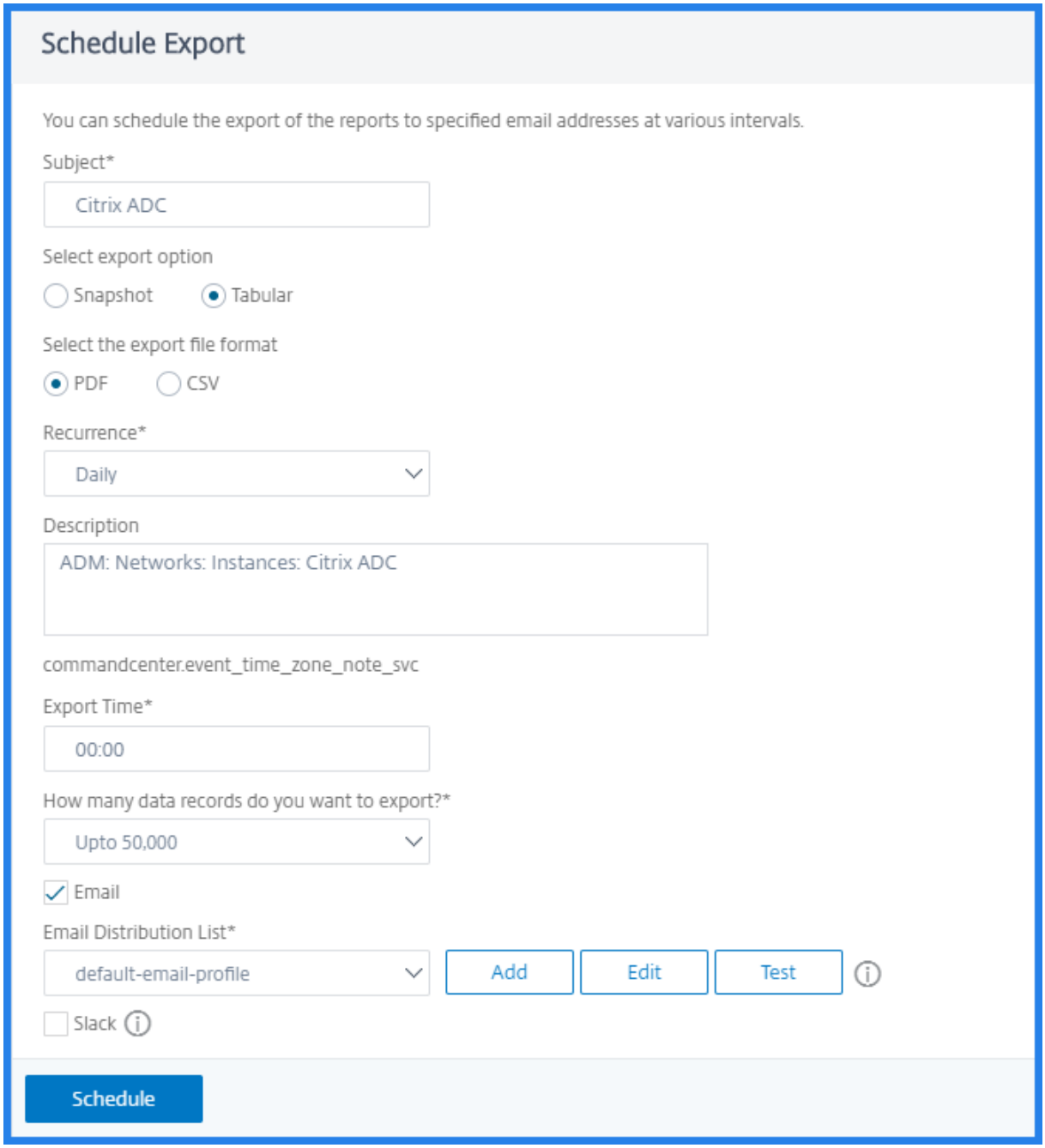


4. ローカルコンピュータにレポートを保存するファイル形式を選択します。
5. [エクスポート] をクリックします。

エクスポートレポートのスケジュール

エクスポートレポートを定期的にスケジュールするには、繰り返し間隔を指定します。エクスポートされたレポートは、構成された電子メールまたはスラックプロファイルに送信されます。

1. ページの右上隅にあるエクスポートアイコンをクリックします。
2. [エクスポートのスケジュール] を選択し、次の項目を指定します。
   - [件名]-デフォルトでは、このフィールドは選択した機能名を自動的に入力します。ただし、意味のあるタイトルで書き換えることができます。
   - エクスポートオプション -スナップショットまたは表形式で ADM レポートをエクスポートします。また、表形式でエクスポートするデータレコードの数を選択することもできます
   - [形式]-構成済みの電子メールまたは Slack のプロファイルに関するレポートを受信するファイル形式を選択します。
   - [繰り返し]-リストから [毎日]、[毎 週]、または [毎月] を選択します。
   - 説明 -レポートに意味のある説明を指定します。
   - エクスポート時刻: レポートをエクスポートする時刻を指定します。
   - 電子メール - チェックボックスをオンにし、リストボックスからプロファイルを選択します。プロファイルを追加する場合は、[追加] をクリックします。
   - [**Slack**]: チェックボックスをオンにし、リストボックスからプロファイルを選択します。プロファイルを追加する場合は、[追加] をクリックします。
3. [**Schedule**] をクリックします。



スケジュールされたエクスポートレポートの表示と編集

エクスポート・レポートを表示するには、次の手順に従います。

1. ページの右上隅にあるエクスポートアイコンをクリックします。

   [レポートのエクスポート] ページには、機能固有のエクスポートレポートがすべて表示されます。

2. 編集するレポートを選択し、**[編集]** をクリックします。

アップグレードアドバイザリ

May 7, 2021

ネットワーク管理者は、Citrix ADM 異なる ADC リリースで実行されている多数の ADC インスタンスを管理できます。各 ADC インスタンスのライフサイクルの監視は、面倒な作業になります。シトリックスの製品マトリクスにアクセスして、サポート終了（EOL）または保守終了（EOM）に達している ADC インスタンスを特定する必要があります。その後、アップグレードを計画します。

このプロセスを容易にするために、Citrix ADM アップグレードアドバイザリは、次の方法で ADC インスタンスのライフサイクルを監視するのに役立ちます。

- EOL または EOM に達または到達したインスタンスを識別します。そのため、EOL または EOM の日付より先に ADC のアップグレードを計画できます。
- 最新のリリースまたはビルドにないインスタンスを強調表示します。これらのインスタンスは、最新のリリースまたはビルドにアップグレードできます。このアップグレードでは、新機能や修正された問題に関する更新プログラムを受け取ります。
- 優先 ADC ビルド上にないインスタンスを強調表示します。組織によっては、インスタンス用に優先 ADC ビルドを使用している場合があります。ADM では、ビルドの安定性、機能、およびその他の考慮事項に応じて、組織で優先ビルドを設定することを実行できます。次に、優先ビルドにないインスタンスを確認し、アップグレードします。優先ビルドを実行しているインスタンスは、星形のアイコンで示されます。
- 最も人気のあるリリースまたはビルドで実行されているインスタンスを強調表示します。一般的なビルドを実行しているインスタンスは、リボンアイコンで示されます。

アップグレードアドバイザリには、対応するリリースノートへのリンクが記載されています。この情報を使用して、アップグレード用の ADC ビルドを確認および決定できます。[Upgrade Advisory] ページから、ADC インスタンスをアップグレードするためのメンテナンスジョブの作成に進むことができます。

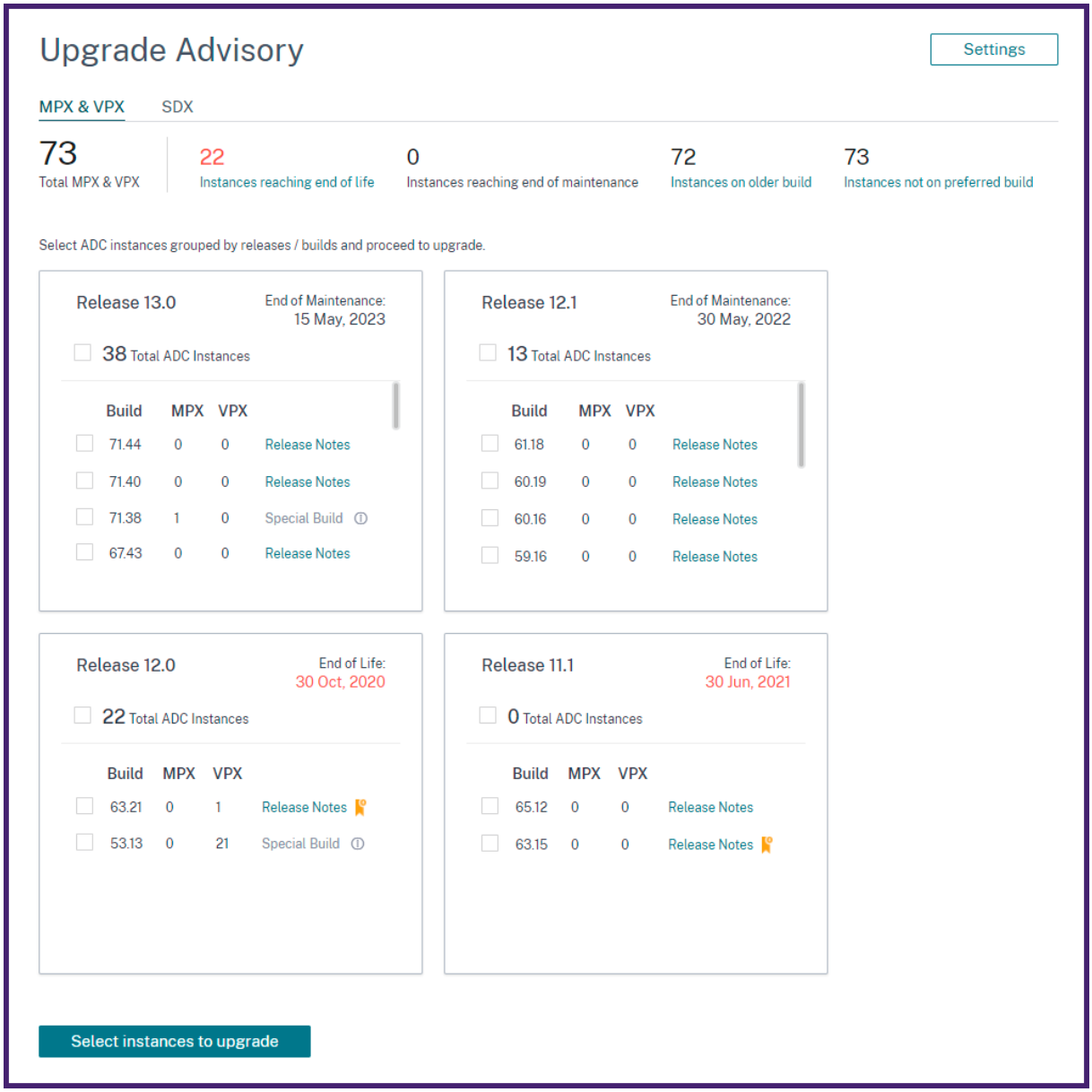
> 重要:
>
> アップグレード・アドバイザリは、ADC ソフトウェア・リリースの EOL のみを監視します。ADC アプライアンスの EOL をチェックしません。

アップグレードアドバイザリを表示

「ネットワーク」**>**「インスタンス・アドバイザ」**>**「アップグレード・アドバイザ」の順にナビゲートし、次の情報を表示します。

- ADC インスタンスの総数。
- インスタンスは、寿命の終わりに達しました。
- インスタンスがメンテナンスの終了に達しました。
- 古いビルドのインスタンス。

- インスタンスは、優先ビルドにありません。
- 各種 ADC リリースの製品寿命と保守終了日

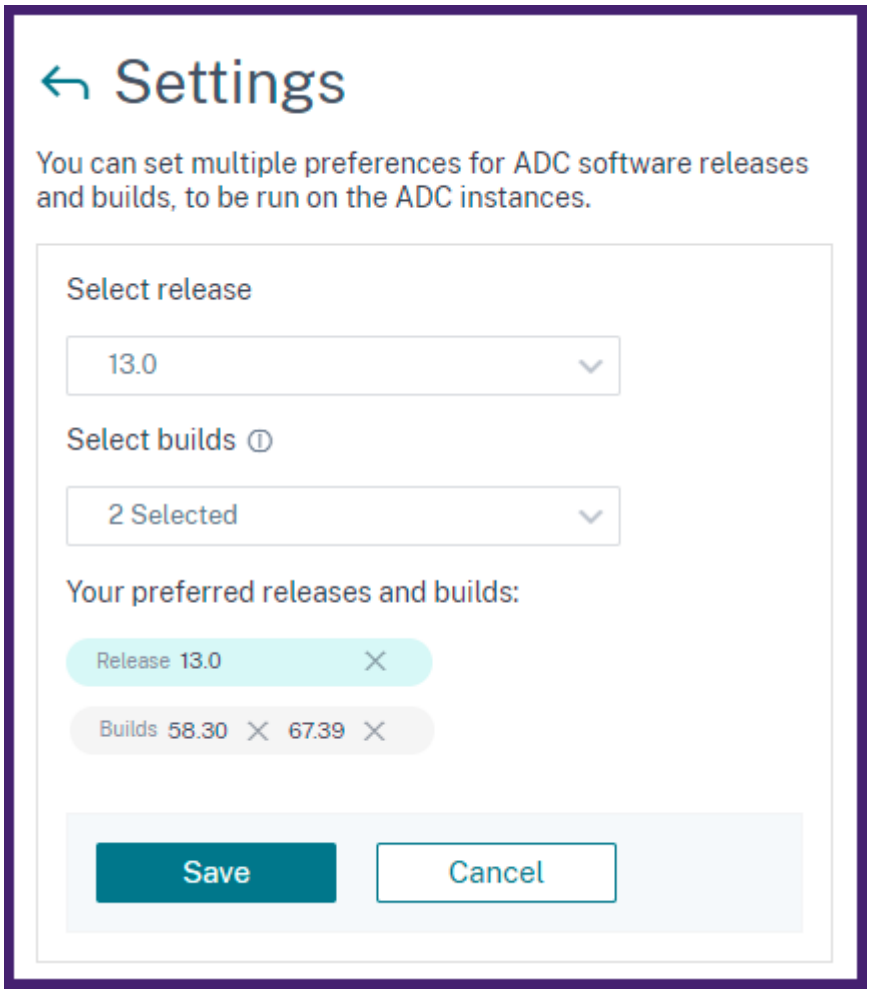


「アップグレードアドバイザ」ページには、リリースごとに ADC インスタンスがグループ化されます。**Release Notes** リンクをクリックすると、特定の ADC リリース・ノートにアクセスできます。アップグレードを決定する前に、新機能、修正された問題、既知の問題を確認します。異なるリリース間で複数の ADC インスタンスを選択して、一度にアップグレードできます。アップグレードを続行すると、アップグレードジョブが作成されます。ADC インスタンスのアップグレードを参照してください。

優先ビルドを設定する

管理者は、組織用に優先する ADC ビルドを定義できます。次の手順を実行して、優先ビルドを設定します。

1. [ネットワーク] **>** [インスタンスアドバイザリ] **>** [アップグレードアドバイザ] で、[設定] をクリックします
2. 優先リリースとビルドを選択します。



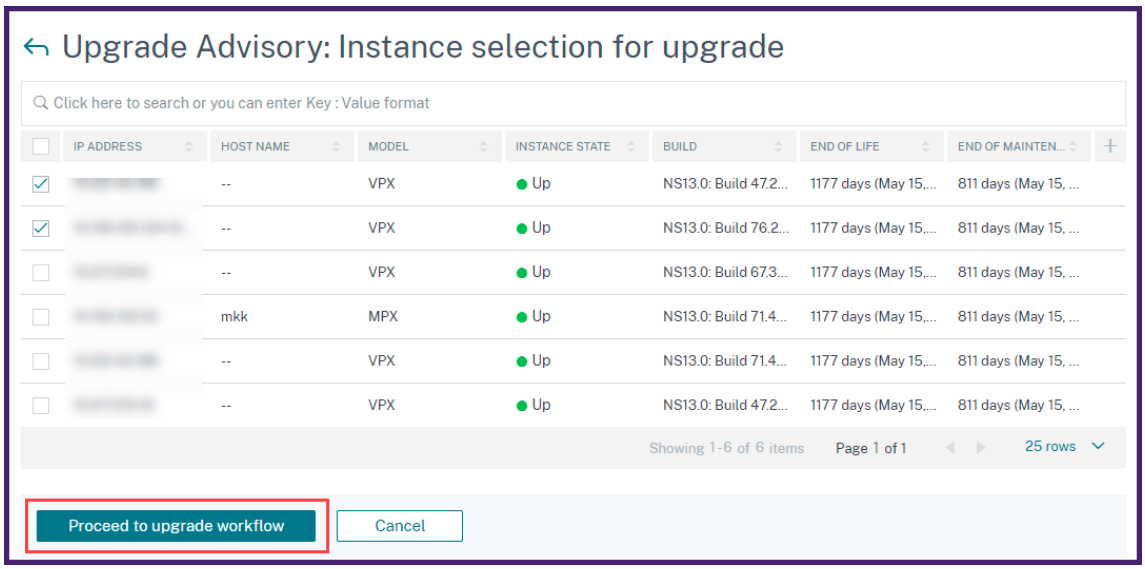
この例では、優先ビルドは`13.0-58.30`と`13.0-67.39`です。

3. [保存] をクリックします。

ADC インスタンスのアップグレード

[**Upgrade Advisory**] ページで、確認後、次の手順を実行して、必要な ADC インスタンスをアップグレードします。

1. アップグレードするインスタンスビルドを選択し、[アップグレードするインスタンスを選択] をクリックします。
2. アップグレードする ADC インスタンスを選択し、[**Proceed to upgrade workflows**] をクリックします。

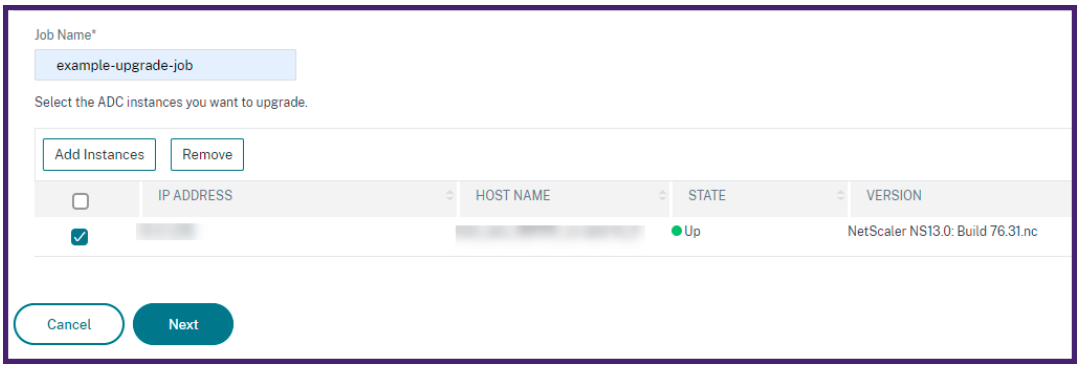


このワークフローでは、アップグレードジョブが作成されます。

3. **[** インスタンスの選択] タブで、

   a) アップグレードジョブの名前を指定します。

   b) (オプション) 他のインスタンスを追加する場合は、[**Add Instances**] をクリックします。



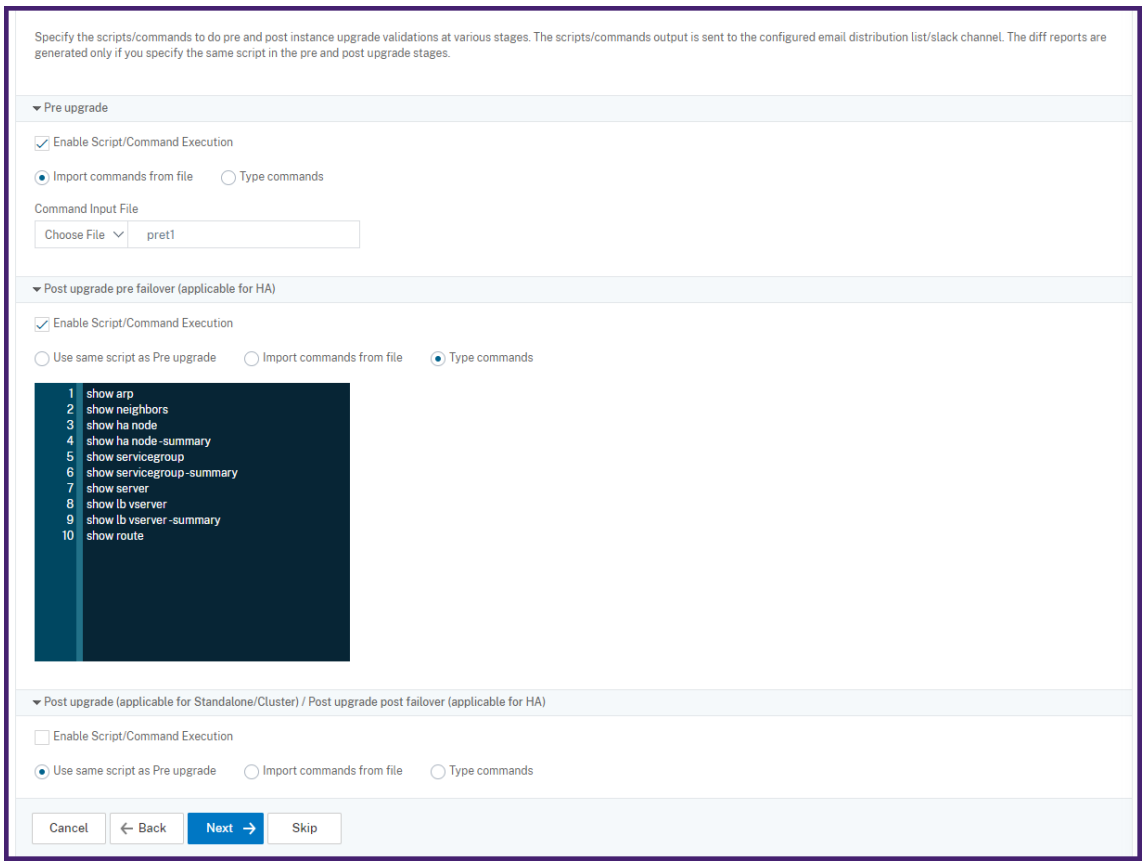
   c) [次へ] をクリックします。

   アップグレード前の検証が開始されます。

4. [アップグレード前の検証] タブで、失敗したインスタンスを削除して続行します。

   インスタンスで十分なディスク領域が発生した場合は、ディスク領域を確認してクリーンアップできます。ADC ディスク領域のクリーンアップを参照してください。

5. 必要に応じて、[**Custom scripts**] タブで、インスタンスのアップグレードの前後に実行するスクリプトを指定します。

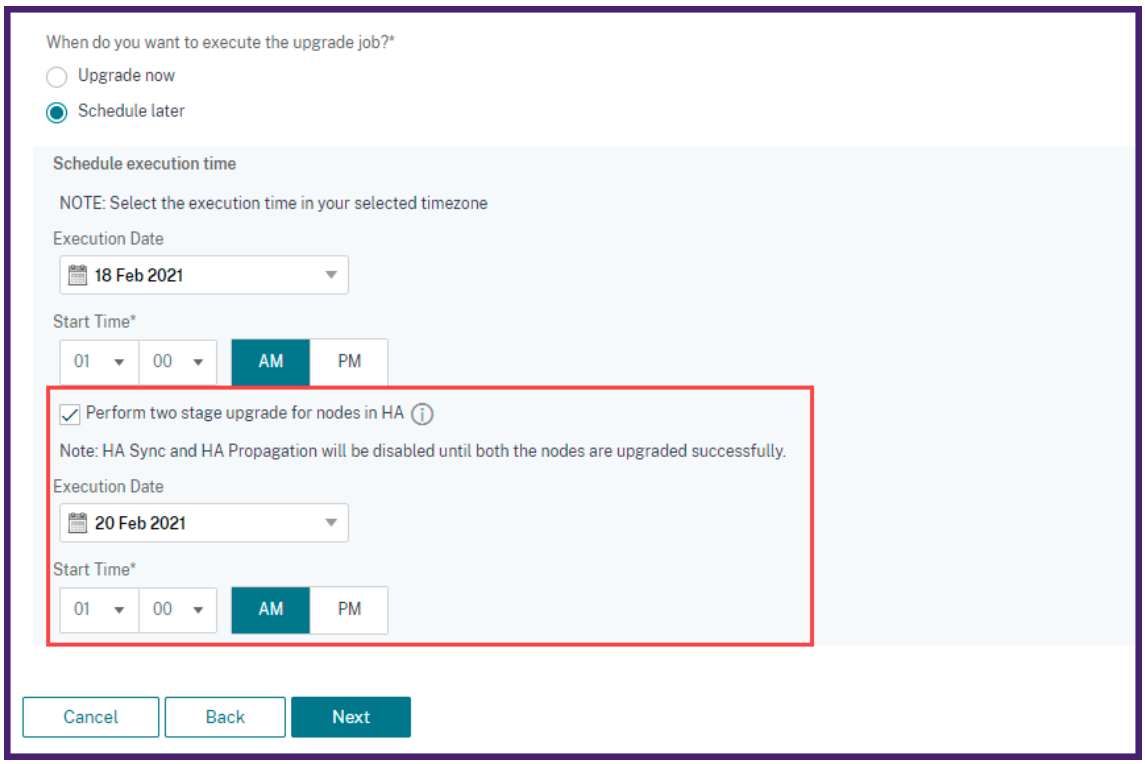


詳しくは、「カスタムスクリプトを使用する」を参照してください。

6. 「スケジュールタスク」で、次のいずれかのオプションを選択します。

   - 今すぐアップグレード -アップグレードジョブはすぐに実行されます。
   - [後でスケジュール]: このアップグレードジョブを後で実行する場合は、このオプションを選択します。インスタンスをアップグレードする場合は、[実行日] と [開始時刻] を指定します。

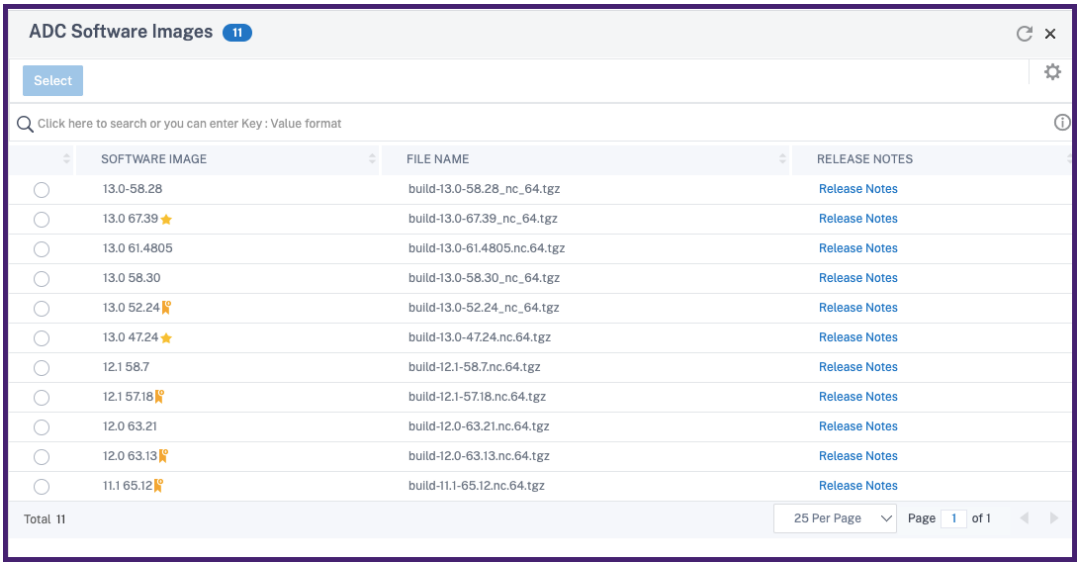
   ADC 高可用性ペアを 2 段階でアップグレードする場合は、[HA のノードに対して 2 段階アップグレードを実行する] を選択します。



詳しくは、「ADC 高可用性ペアのアップグレード」を参照してください。

7. [ジョブの作成] タブで、次のいずれかのオプションを指定します。

   - **ADC** ソフトウェアイメージを選択：リストから ADC イメージを選択します。このオプションでは、Citrix ダウンロード Web サイトで使用可能なすべての ADC イメージが一覧表示されます。



   - **ADC** ソフトウェアイメージのアップロード：ローカルコンピュータまたは ADC アプライアンスからイメージをアップロードできます。ADC アプライアンスを選択すると、`/var/mps/mps_images`に存在するインスタンスファイルが ADM GUI に表示されます。ADM GUI からイメージを選択します。

アップグレードジョブをスケジュールする場合、インスタンスにイメージをアップロードするタイミングを指定できます。

- 今すぐアップロード: 画像をすぐにアップロードするには、このオプションを選択します。ただし、アップグレードジョブは、スケジュールされた時刻に実行されます。
- **[** 実行時にアップロード**]:** アップグレードジョブの実行時にイメージをアップロードするには、このオプションを選択します。

その他のオプションの詳細については、ADC アップグレード・オプションを参照してください。

セキュリティアドバイザリ

May 7, 2021

安全で耐障害性に優れたインフラストラクチャは、あらゆる組織のライフラインです。したがって、組織は、新しい共通脆弱性とエクスポージャス（CVE）を追跡し、CVE がインフラストラクチャに与える影響を評価し、緩和と修復を理解し、脆弱性を解決するための緩和と修復を計画する必要があります。

Citrix ADM セキュリティアドバイザリでは、ADC インスタンスが危険にさらされている Citrix CVE を強調し、緩和策と修復を推奨します。ADM サービスを使用して緩和策と是正を適用することにより、推奨事項を確認し、適切なアクションを実行できます。

セキュリティアドバイザリの機能

次のセキュリティアドバイザリ機能は、インフラストラクチャを保護するのに役立ちます。

- スキャン: デフォルトのシステムスキャンとオンデマンドスキャンが含まれます。
  - システムスキャン: デフォルトで週に 1 回、すべての管理対象インスタンスをスキャンします。システムスキャンの日付と時刻は ADM によって決定され、変更することはできません。
  - オンデマンドスキャン: 必要に応じてインスタンスを手動でスキャンできます。最後のシステムスキャンの後に経過した時間が重要な場合は、オンデマンドスキャンを実行して、現在のセキュリティポスチャを評価できます。または、修正または緩和が適用された後にスキャンして、改訂された姿勢を評価します。
- CVE 影響分析: インフラストラクチャに影響を与えているすべての CVE と、すべての ADC インスタンスが影響を受ける結果を表示し、修復と緩和を提案します。この情報を使用して、緩和と修復を適用してセキュリティリスクを修正します。
- CVE レポート: 最後の 5 つのスキャンのコピーを保存します。これらのレポートは CSV 形式でダウンロードして分析できます。

- CVE リポジトリ： 2019 年 12 月以降に Citrix が発表したすべての ADC 関連 CVE の詳細ビューが表示されます。これは ADC インフラストラクチャに影響を与える可能性があります。このビューを使用して、セキュリティアドバイザリースコープの CVE を理解し、CVE について詳しく知ることができます。

注意事項

セキュリティアドバイザリを使用するときは、次の点に注意してください。

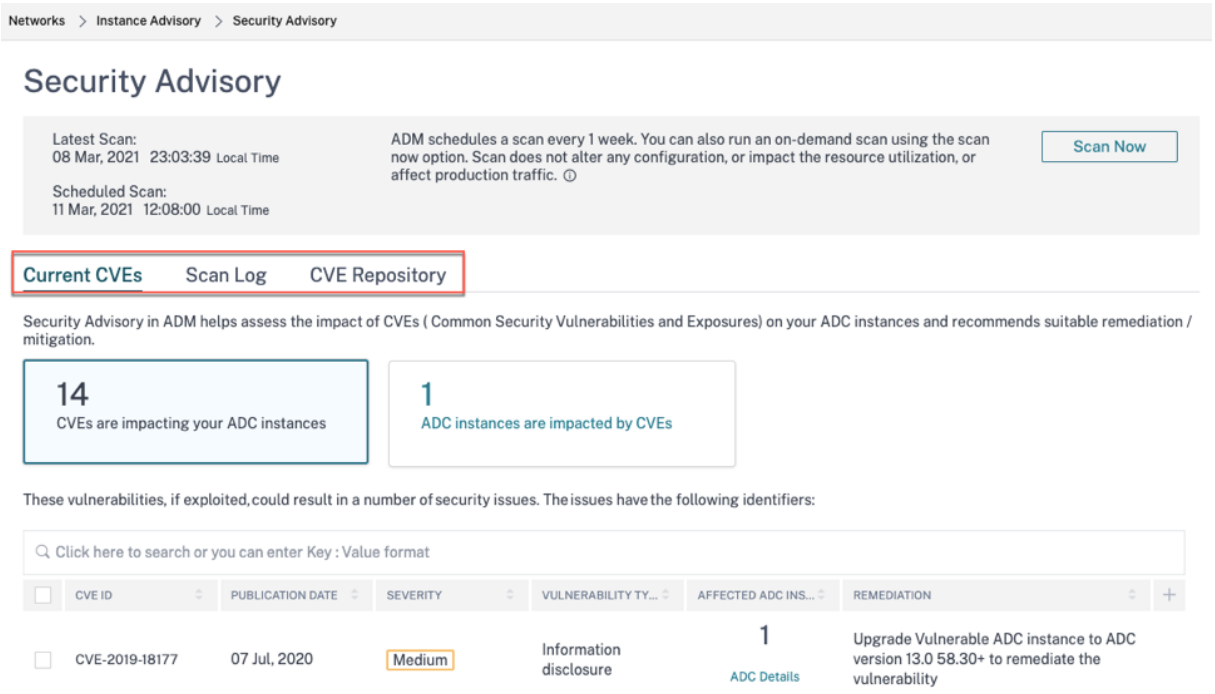
- CVE 検出でサポートされるインスタンス: すべての ADC (SDX、MPX、VPX、CPX、BLX) およびゲートウェイ
- CVE がサポートされている： 2019 年 12 月以降のすべての CVE です。
- ADC、Gateway リリースの範囲: 機能はメインビルドに限定されます。セキュリティアドバイザリには、その範囲に特別なビルドは含まれません。
  - セキュリティアドバイザリは、10.5 以降のバージョンを実行する ADC インスタンスでサポートされ、10.5 以降のバージョンを実行しているインスタンスではサポートされません。
  - セキュリティアドバイザリは、管理パーティション、SD-WAN デバイス、HAProxy、HAProxy ホストデバイスではサポートされていません。
- スキャンの種類: セキュリティアドバイザリでバージョンスキャンと構成スキャンを実行します
  - バージョンスキャン:ADC バージョンが脆弱なバージョンかどうかをチェックします。使用するロジックは、CVE が ADC リリース xx.xx で修正されている場合、xx.xx ビルドよりも低いすべてのリリースとビルドは脆弱であると見なされます。
  - Config scan — ADC 設定をスキャンして、脆弱な特定の設定パターンが存在するかどうかを確認します。
- スキャンは、ADC の本番トラフィックに影響を与えず、ADC の ADC の設定を変更しません。

セキュリティアドバイザリダッシュボードの使用方法

セキュリティアドバイザリダッシュボードにアクセスするには、ADM GUI から、**[**ネットワーク**] > [**インスタンスアドバイザリ**] > [**セキュリティアドバイザリ] に移動します。ダッシュボードには、ADM を通じて管理するすべての ADC インスタンスの脆弱性ステータスが表示されます。インスタンスは週に 1 回スキャンされますが、[Scan **Now]** をクリックすればいつでもスキャンできます。

ダッシュボードには、次の 3 つのタブがあります。

- 現在の CVE
- ログをスキャン
- CVE リポジトリ



> 重要
>
> セキュリティアドバイザリ GUI またはレポートでは、すべての CVE が表示されず、CVE が 1 つだけ表示される場合があります。回避策として、[今すぐスキャン] をクリックしてオンデマンドスキャンを実行します。スキャンが完了すると、スコープ内のすべての CVE（約 15）が UI またはレポートに表示されます。

現在の **CVE**

このタブには、インスタンスに影響を与える CVE の数（この画面キャプチャでは 14 CVE）と、CVE の影響を受けるインスタンス（この画面キャプチャでは）が表示されます。タブはシーケンシャルではなく、管理者として、ユースケースに応じてこれらのタブを切り替えることができます。

ADC インスタンスに影響する CVE の数を示す表には、次の詳細が示されています。

CVE ID: インスタンスに影響を与える CVE の ID。

公開日: その CVE のセキュリティ情報が公開された日付。

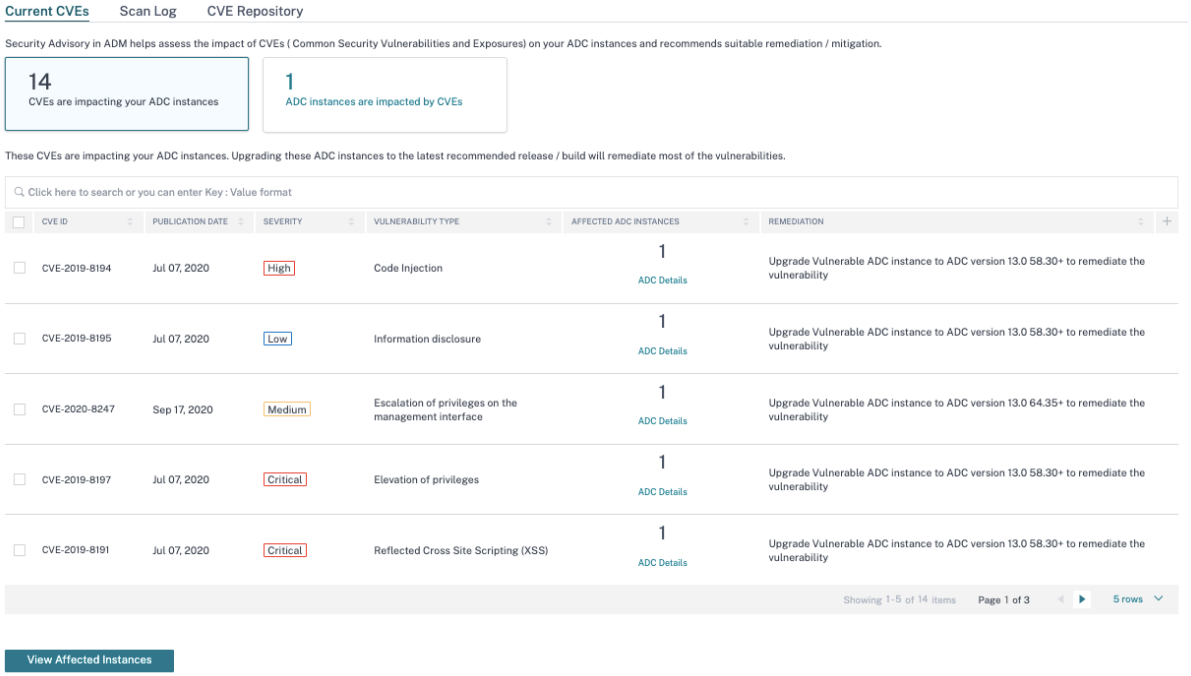
重大度スコア: 重大度タイプ（高/中/重大）およびスコア。スコアを表示するには、重要度のタイプにカーソルを合わせます。

脆弱性の種類: この CVE の脆弱性の種類。

影響を受ける **ADC** インスタンス: CVE ID が影響しているインスタンスカウント。マウスオーバーすると、ADC インスタンスのリストが表示されます。

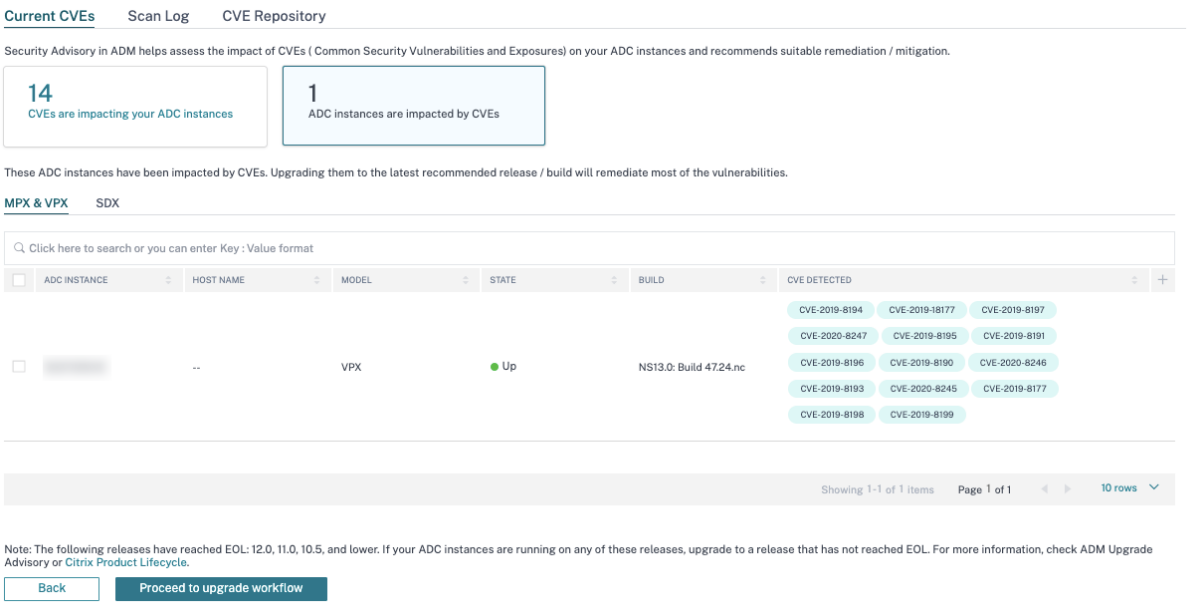
修復: インスタンスのアップグレード（通常）または構成パックの適用である、利用可能な修復。

同じインスタンスは、複数の CVE によって影響を受ける可能性があります。この表では、1 つの特定の CVE または複数の選択した CVE が影響しているインスタンスの数を確認できます。影響を受けるインスタンスの IP アドレスを確認するには、[該当する ADC インスタンス] の下の [ADC 詳細] にカーソルを合わせます。影響を受けるインスタンスの詳細を確認するには、テーブルの下部にある [影響を受けるインスタンスの表示] をクリックします。
プラス記号をクリックして、テーブルの列を追加または削除することもできます。



<number of> ADC インスタンスには、**[CVes** の影響を受ける] タブに、影響を受ける ADM 管理の ADC インスタンスがすべて表示されます。この表は、ADC の IP アドレス、ホスト名、ADC のモデル・ナンバー、ADC の状態、ソフトウェアのバージョンとビルド、および ADC に影響を与える CVE のリストを示しています。

次の画面キャプチャでは、1 つの ADC インスタンスが影響を受けます。必要に応じて、+ 記号をクリックして、これらの列を追加または削除します。



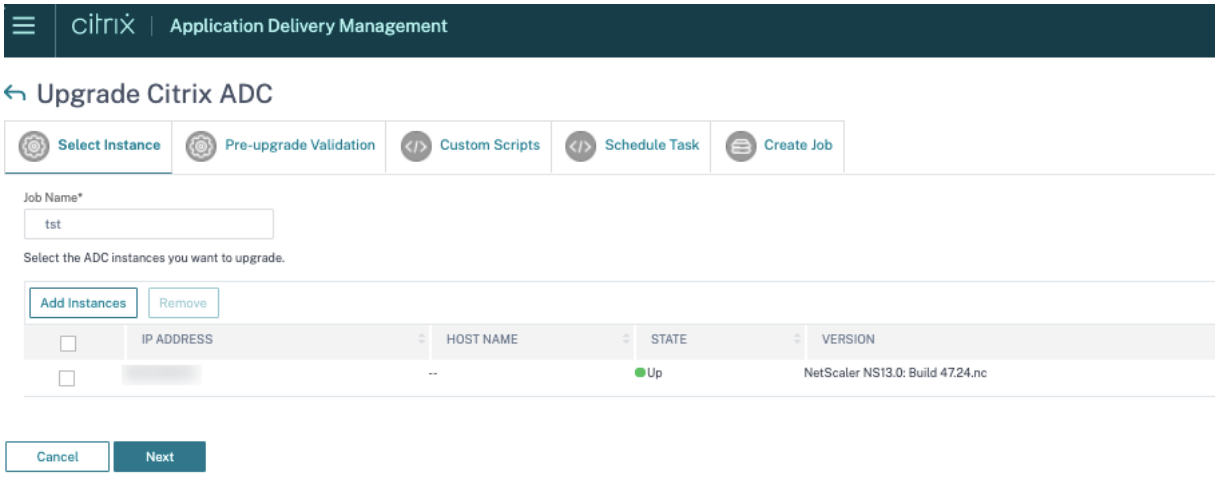
脆弱性の問題を修正するには、ADC インスタンスを選択し、インスタンスのアップグレードである推奨事項の修正を適用します。

- アップグレード: 脆弱な ADC インスタンスを、修正されたリリースおよびビルドにアップグレードできます。この詳細は、「是正」列に表示されます。アップグレードするには、インスタンスを選択し、[**Proceed to Upgrade]** ワークフローをクリックします。アップグレードワークフローでは、脆弱な ADC がターゲット ADC として自動的に入力されます。

> 注
>
> 12.0、11,0、10.5 以降のリリースは、すでにサポート終了 (EOL) です。ADC インスタンスがこれらのリリースのいずれかで実行されている場合は、サポートされているリリースにアップグレードしてください。

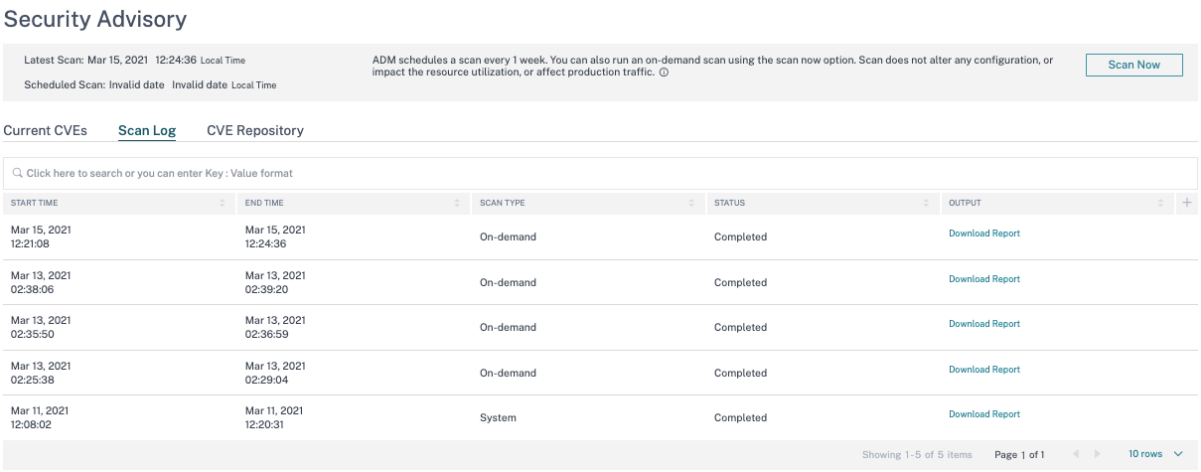
アップグレードワークフローが開始されます。ADM を使用して ADC インスタンスをアップグレードする方法の詳細については、「ADC アップグレード・ジョブの作成」を参照してください。

> 注
>
> アップグレード先のリリースとビルドは、ユーザーの判断によります。[修復] 列の下のアドバイスを参照して、セキュリティ修正を適用しているリリースとビルドを確認し、それに応じて、サポート対象リリースとビルドを選択します (サポート対象リリースとビルドはまだ終了していません)。



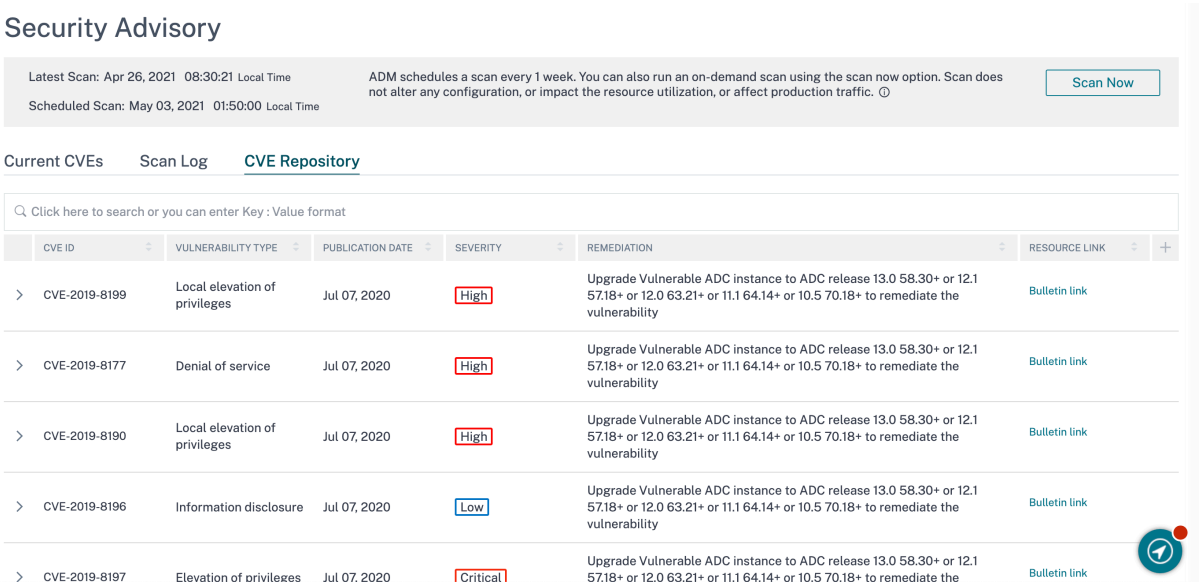
ログをスキャン

タブには、デフォルトのシステムスキャンとオンデマンドユーザー開始スキャンの両方を含む、最後の 5 つのスキャンのレポートが表示されます。各スキャンのレポートは CSV 形式でダウンロードできます。オンデマンドスキャンが進行中の場合は、ここで完了ステータスを確認できます。スキャンが失敗した場合、ステータスはそれを示します。



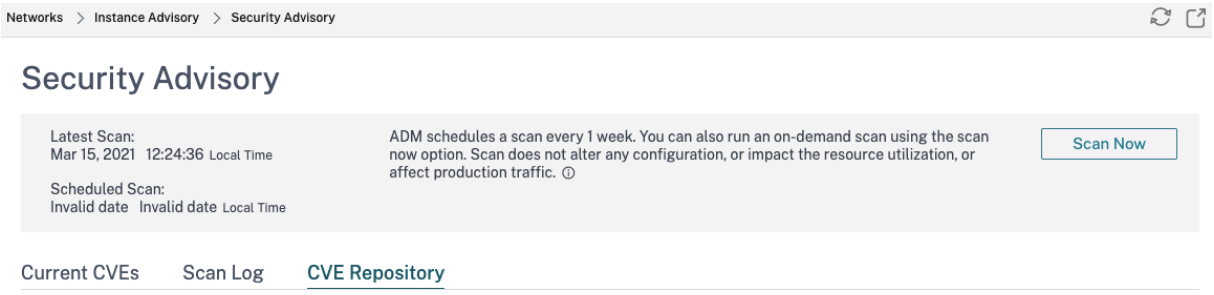
CVE リポジトリ

このタブには、2019 年 12 月以降のすべての CVE の最新情報、CVE ID、脆弱性の種類、公開日、重大度、修復、セキュリティ情報へのリンクが含まれます。

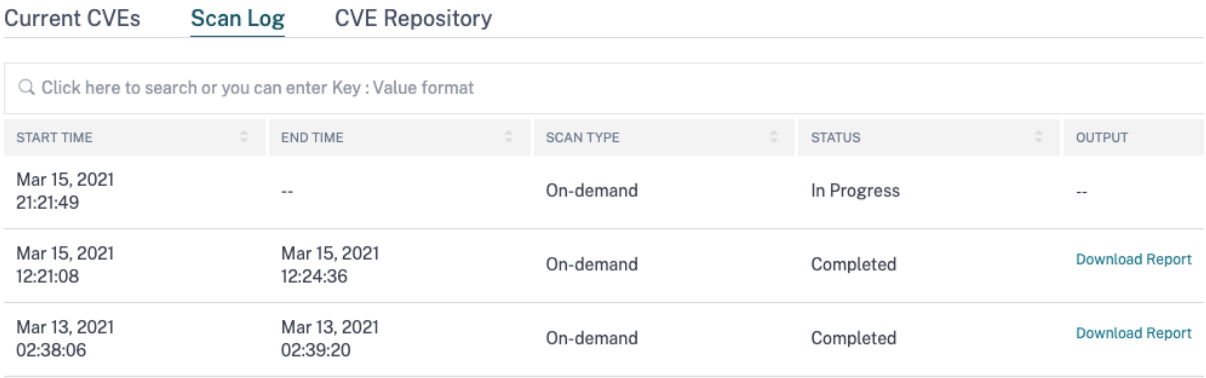


今すぐスキャン

セキュリティアドバイザリには、インスタンスが最後にスキャンされた日時と次のスケジュールの期限が表示されます。また、必要に応じていつでもインスタンスをスキャンできます。[Scan Now] をクリックして、インスタンスの最新のセキュリティレポートを取得します。ADM はスキャンを完了するのに数分かかります。



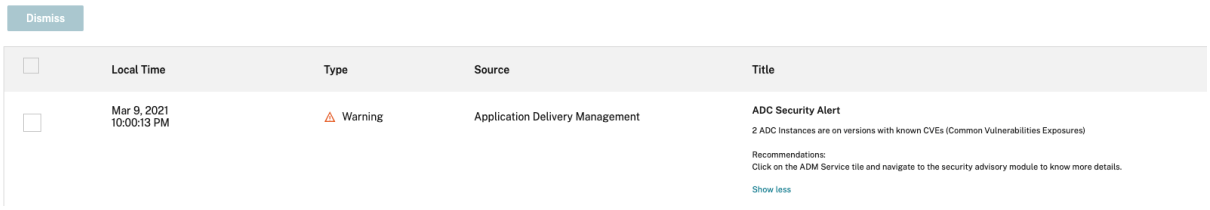
スキャンが完了すると、改訂されたセキュリティの詳細がセキュリティアドバイザリ GUI に表示されます。また、スキャンログの下にレポートがあり、ダウンロードすることもできます。



> 注
>
> スキャンログには、スケジュール済みまたはオンデマンドの両方で、最後の 5 つのスキャンのログのみが表示されます。

通知

管理者は、脆弱性のある ADC インスタンスの数を示す Citrix Cloud 通知を受け取ります。通知を表示するには、ADM GUI の右上隅にあるベルアイコンをクリックします。



アプリケーション

May 7, 2021

Citrix ADM アプリケーション分析および管理機能を使用すると、アプリケーション中心のアプローチでアプリケーションを監視できます。このアプローチは、次のことを支援します。

- スコアを確認し、アプリケーションの全体的なパフォーマンスを分析する
- サーバーまたはクライアントで発生する問題がないか確認します。
- アプリケーショントラフィックフローの異常を検出し、是正措置を講じます。

> 注
>
> アプリケーションは、インスタンス（Citrix ADC）で構成された 1 つ以上の仮想サーバーを指します。

1 時間、1 日、1 週間、1 か月などの期間、アプリケーションを監視できます。

前提条件

- Citrix ADM で Citrix ADC インスタンスを追加していることを確認します。
- Citrix ADC インスタンスの有効なライセンスがあることを確認してください。詳しくは、「ライセンス」を参照してください。
- 仮想サーバのライセンスを適用していることを確認します。詳しくは、「仮想サーバでのライセンスの管理」を参照してください。

アプリケーションの概要

アプリケーションには、次のものがあります。

- ディスクリートアプリケーション
- カスタムアプリケーション
- マイクロサービスアプリケーション (k8s_Discrete)

ディスクリートアプリケーション

ライセンスが付与されているすべての仮想サーバは、個別のアプリケーションと呼ばれます。

カスタムアプリケーション

1 つのカテゴリの仮想サーバは、カスタムアプリケーションと呼ばれます。管理者は、カテゴリに基づいてカスタムアプリケーションを追加する必要があります。その後、ダッシュボードからアプリケーションを管理および監視できます。1 つのカテゴリにグループ化されている特定のアプリケーションを簡単に監視できます。

たとえば、データセンター 1 のカテゴリを作成し、その ADC インスタンスを追加することができます。カテゴリを定義し、データセンター 1 のインスタンスを追加すると、データセンター 1 に関連するすべてのアプリケーションで構成される別のカテゴリがアプリケーションダッシュボードに表示されます。

注意事項

- カスタムアプリケーションに追加された個別アプリケーションは、個別のアプリケーションから削除されます。
- どのカテゴリにも追加されていないアプリケーションは、すべて 「その他」として利用できます。
- デフォルトでは、Citrix ADM では最大 2 つのアプリケーションのライセンスを追加できます。ライセンスに応じて、監視するアプリケーションのライセンスを選択して適用できます。

マイクロサービスアプリケーション

Kubernetes クラスタでは、Citrix ADC MPX（ハードウェア）、Citrix ADC VPX（仮想化）、および Citrix ADC CPX（コンテナ化）用の Ingress Controller を提供します。詳しくは、「Citrix Ingress Controller」を参照してください。

Citrix ADC CPX インスタンスを使用して構成される個別のアプリケーションは、マイクロサービスアプリケーションと呼ばれます。

アプリケーション管理とアプリケーションダッシュボード

May 7, 2021

Citrix ADM では、［アプリケーション］ページから アプリケーションを管理し、［ダッシュボード］ページからアプリケーションの詳細を表示できます。

アプリケーション管理

 アプリケーション｜ **Application** s ｜ emdw ・ページでは、すべてのカスタム・アプリケーションおよび個別のアプリケーションを表示できます。

管理者として、「アプリケーション」ページから、次の操作を実行できます。

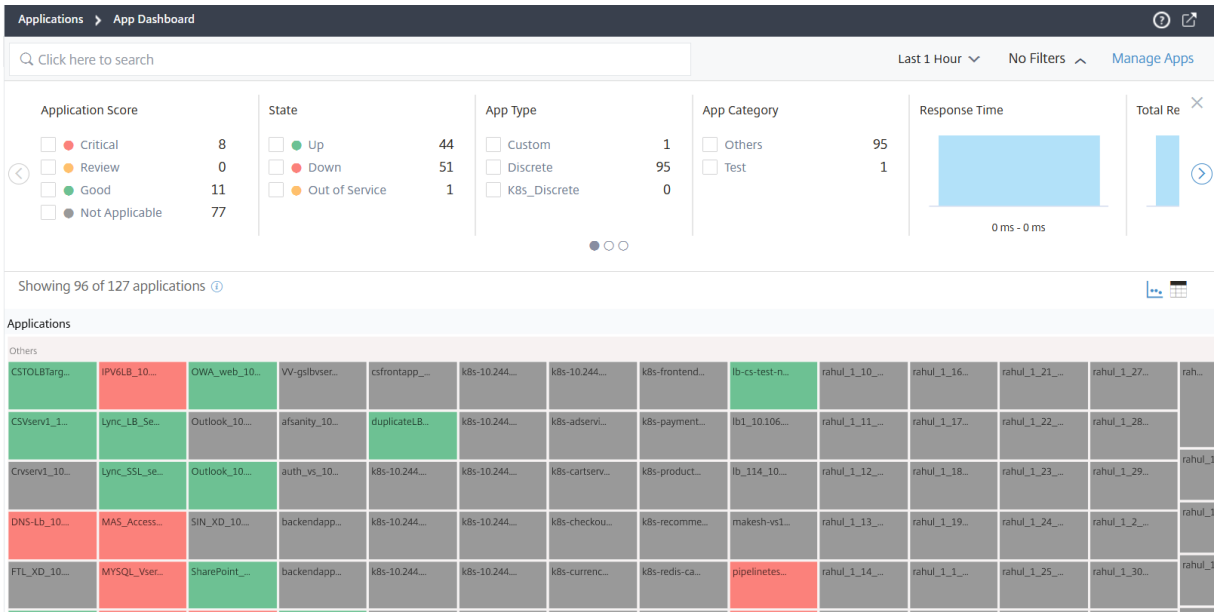
- アプリケーションの追加
- アプリケーション名、アプリケーションの種類、アプリケーションのカテゴリ、関連付けられた仮想サーバー、関連付けられたサービスなど、アプリケーションの詳細を表示します。
- カスタムアプリケーションの編集または削除

アプリケーションを追加、編集、または削除すると、その詳細が [アプリケーション] ページにすぐに反映されます。

詳しくは、「アプリケーション管理」を参照してください。

アプリケーションダッシュボード

「アプリケーション」>「ダッシュボード」に移動して、アプリケーションのリストを表形式ビューまたはグラフ・ビューで表示します。



すべてのアプリケーションは、アプリケーションがデータの入力を開始した後にのみ、ダッシュボードに表示されます。ダッシュボードからアプリケーションをクリックして、アプリケーションのパフォーマンスの詳細情報を表示します。詳しくは、「アプリケーションの詳細」を参照してください。

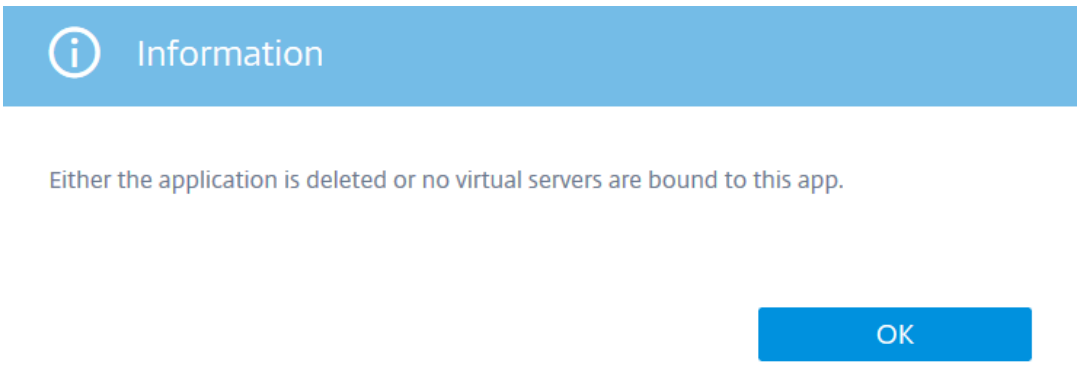
約 10 ～15 分経過してもアプリケーション分析が表示されない場合は、アプリダッシュボードのトラブルシューティングのトラブルシューティング手順を実行します。

以前のダッシュボードと比較した新しいダッシュボードの動作の更新

- カスタムアプリケーションを追加または編集した後、アプリケーションがダッシュボードに反映されるまで数分かかる場合があります。
- カスタムアプリケーションを削除しても、ADM の分析データ（最長 1 か月）が保持されるまで、ダッシュボードには削除されたアプリケーションが表示されます。

  2020 年 1 月 2 日にアプリケーションを作成し、2020 年 1 月 4 日にアプリケーションを削除したシナリオを考えてみましょう。このシナリオの内容は以下のとおりです。

  - ダッシュボードには、過去 1 日、1 週間、1 か月の期間を選択すると、2020 年 1 月 4 日削除したアプリケーションを、引き続き表示できます。
  - 過去 1 週間と 1 か月の期間を選択すると、2020 年 1 月 5 日に削除されたアプリケーションがダッシュボードに表示されます。
  - 期間がアプリの削除日を超えると、アプリケーションはダッシュボードに表示されません。つまり、ダッシュボードは、2020 年 1 月 6 日（最後の 1 日）、2020 年 1 月 12 日（過去 1 週間）、2020 年 2 月 5 日以降（過去 1 ヶ月間）に削除されたアプリケーションでは表示されません。
  - ダッシュボードから削除したアプリケーションをクリックすると、次のメッセージが表示されます。

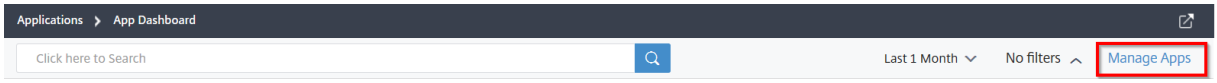


> 注
>
> アプリケーションを追加した後、関連付けられた Citrix ADC インスタンスが「ダウン」、「アウト」の場合、または一時的なネットワーク障害のために到達できない場合：
>
> -ADC インスタンスに関連付けられたアプリケーションは、［アプリケーション］ページにのみ表示されますが、ダッシュボードには表示されません。
>
> -アプリケーションは、ADC インスタンスが起動して実行されると、ダッシュボードに表示されます。

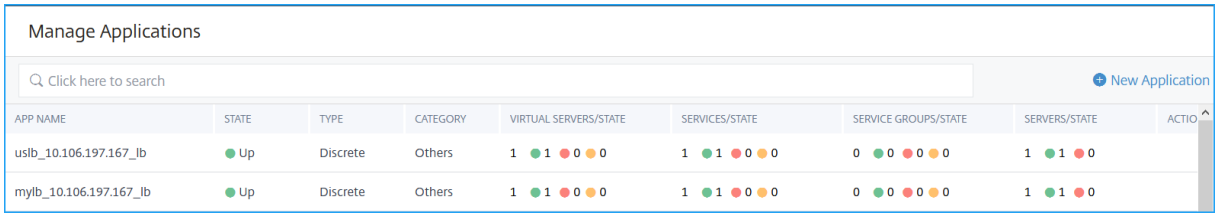
アプリケーション管理

May 7, 2021

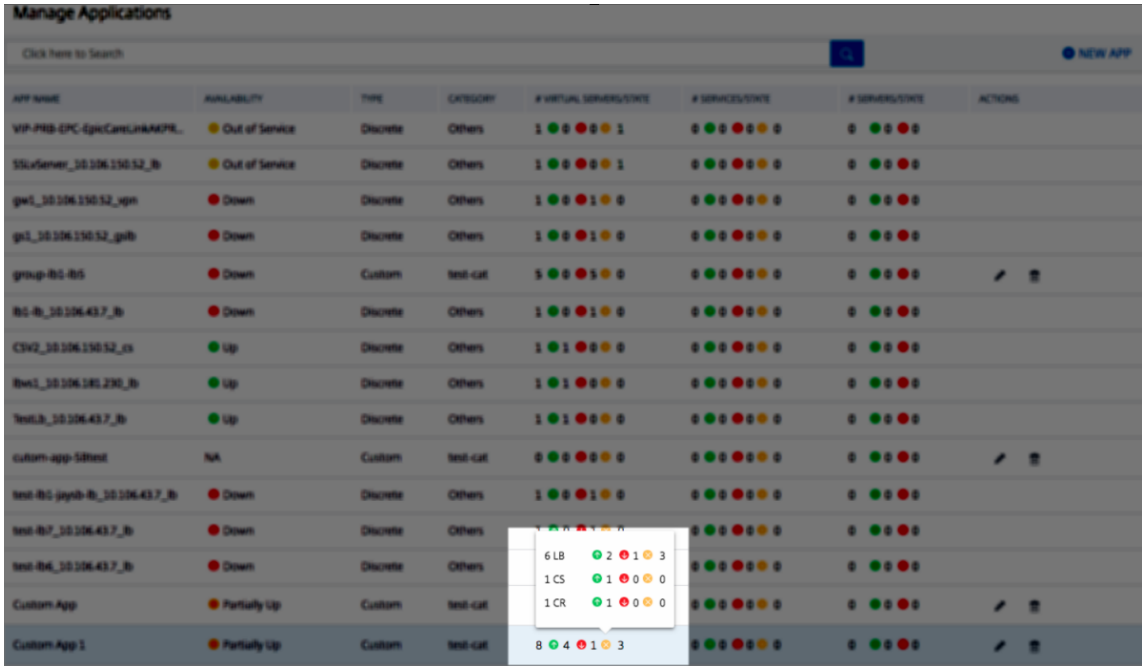
ダッシュボードで [アプリの管理] をクリックして、アプリケーションの詳細を表示し、カスタムアプリケーションの追加、編集、または削除を行います。



アプリケーション詳細の表示



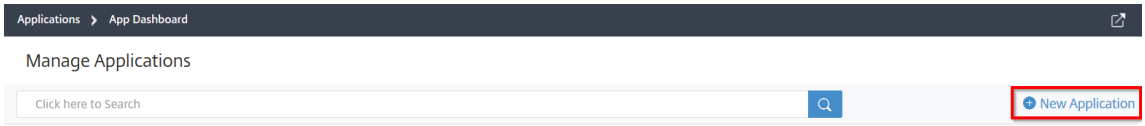
- アプリケーション名 — アプリケーション名を示します。
- [**State**]: 現在のアプリケーションのステータス（[**Up**]、[**Down**]、[部分的にアップ]、[**Out of Service**]、および **NA** など）を示します。
  - **Up**： アプリケーションに関連づけられているすべての仮想サーバが Up です。
  - **Down**： アプリケーションに関連づけられているすべての仮想サーバがダウンしている
  - 部分的にアップ: アプリケーションに関連づけられている 1 つの仮想がダウンしているか、またはアウト・オブ・サービスです。
  - **Out of Service**： アプリケーションに関連づけられているすべての仮想サーバが Out of Service
  - **NA**： アプリケーション用に仮想サーバが設定されていない
- 「タイプ」(Type) — アプリケーションがカスタムまたはディスクリートに属しているかどうかを示します。
- 「カテゴリ」 (Category) — グループ化されたアプリケーションカテゴリを示します。
- 仮想サーバ/状態: 構成済みの仮想サーバの合計とすべての仮想サーバのステータスを示します。マウスポインターを合わせると、仮想サーバーの合計、仮想サーバーの種類、仮想サーバーのステータスなどの詳細が表示されます。



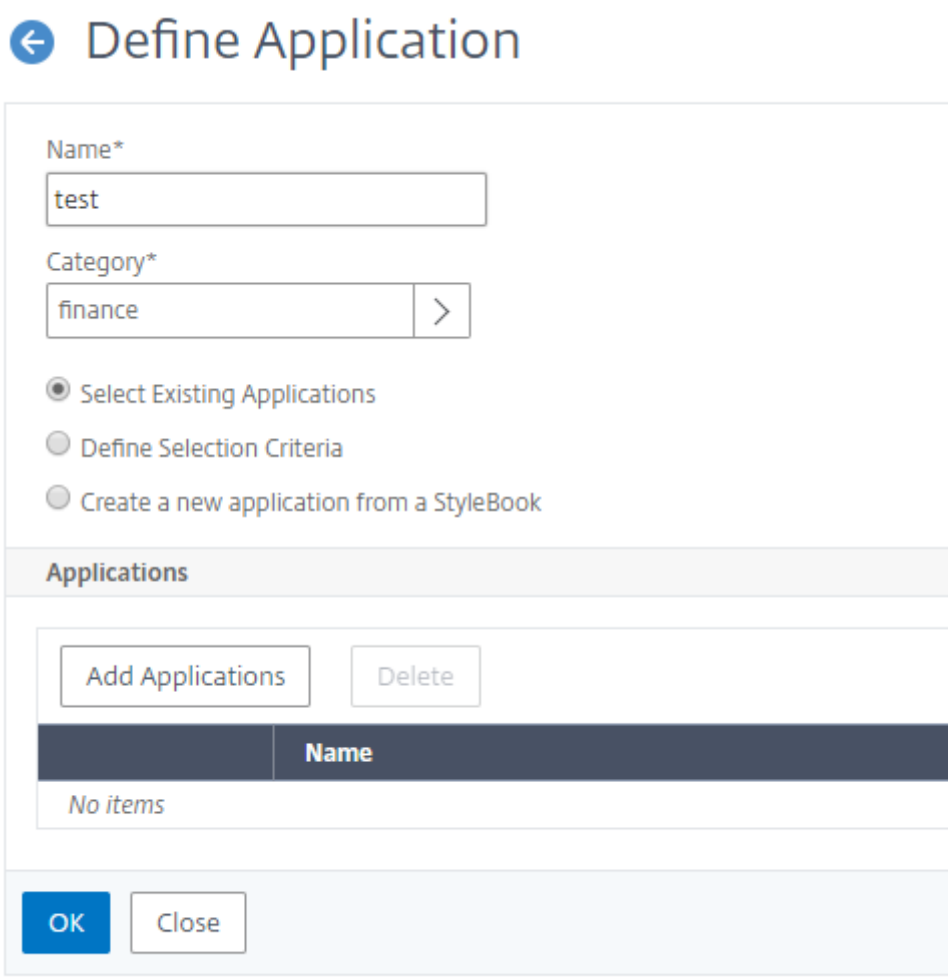
- サービス/状態：構成されたサービスの合計とすべてのサービスのステータスを示します。
- **Service Goups/state**：設定されているサービスグループの合計とすべてのサービスグループのステータスを示します。
- サーバ/状態：アプリケーション用に構成されたサーバの合計およびすべてのサーバのステータスを示します。
- 「アクション」 — カスタムアプリケーションを編集または削除できます。

アプリケーションの追加

1. [新しいアプリケーション] をクリックして、アプリケーションを作成します。



「アプリケーションの定義」ページが表示されます。



> 注
>
> [アプリケーション] をクリックし、[新しいアプリケーション] を選択してアプリケーションを作成することもできます

2. 次のパラメーターを設定します。

フィールド	説明
名前	カスタムアプリケーションの名前。たとえば、LB_TEST などです。
カテゴリ	アプリケーションをグループ化できるカテゴリ。クリックすると、[アプリケーションカテゴリ] ページが表示されます。カテゴリを選択し、[選択] をクリックします。カテゴリを追加するには、次の手順に従います。
	1. [追加] をクリックします。

フィールド	説明
	2. 選択した名前を入力します。
	3. [作成] をクリックします。
既存のアプリケーションの選択	Citrix ADC インスタンスに追加された既存のアプリケーションを選択できます。
アプリケーションの追加	インスタンスに設定されているすべての仮想サーバーを表示します。リストからアプリケーションを選択し、[**OK**] をクリックします。
選択条件の定義	仮想サーバーの範囲、または元のサーバー/サービスの IP アドレスの範囲でアプリケーションを定義するオプション。
	- サーバー。サーバーまたはサービスの IP アドレス、サーバー名、またはアプリケーションが実行されているバックエンドサーバーのポートを指定します。1 つの IP アドレスか IP アドレスの範囲、またはコンマ区切りでそれらを組み合わせて入力できます。たとえば、「10.102.29.20, 10.102.43.10-60, 10.216.43.45」と入力します。
	- 仮想サーバー。仮想サーバーの IP アドレス、仮想サーバー名、またはアプリケーションが実行されているバックエンドサーバーのポートのいずれかを指定できます。1 つの IP アドレスか IP アドレスの範囲、またはコンマ区切りによるそれらの組み合わせで入力できます。たとえば、「10.102.29.20, 10.102.43.10-60, 10.216.43.45」と入力します。
StyleBook からアプリケーションを作成する	StyleBook を使用してアプリケーションを作成できます。詳しくは、「StyleBook を使用してアプリケーションを作成する」を参照してください。

a) [**OK**] をクリックします。

> 注
>
> 現在、Application Dashboard では、負荷分散とコンテンツスイッチング仮想サーバーのみがサポートされています。

これで、アプリケーションダッシュボードがカテゴリとともに表示され、すべてのアプリケーションが下にグループ化されます。

StyleBooks を使用してアプリケーションを作成するときは、アプリケーションの展開中に必要なライセンス消費を確認します。

確認メッセージが表示されたら、**[**はい] をクリックします。ADM は、必要なライセンスをアプリケーションに割り当てます。

StyleBook を使用してアプリケーションを作成する

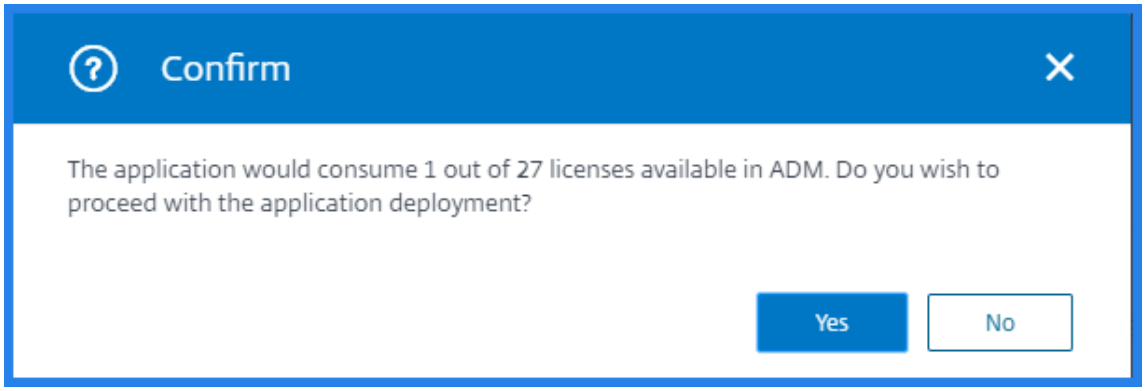
StyleBook を使用してアプリケーションを作成するには、次の手順に従います。

1. Citrix ADM で、［アプリケーション］>［ダッシュボード］に移動し、［カスタムアプリケーションの定義］をクリックしてカスタムアプリケーションを作成します。
2. [アプリケーションの定義] ページで、[名前] フィールドにアプリケーションの 名前を入力します。
3. [カテゴリ] セクションからアプリケーションカテゴリを選択します。Citrix ADM では、ユーザー定義のアプリケーションをグループ化するカテゴリを定義できます。必要に応じて、さらにカテゴリを追加することもできます。
4. [**StyleBook** から新しいアプリケーションを作成する**]** をクリックして選択し、 [**OK**] をクリックします。

   「スタイルブックの選択」ページが表示されます。このページには、Citrix ADM で使用可能なデフォルトのスタイルブックがすべて表示されます。
5. スタイルブックを選択します。
   「構成の詳細」ページが表示されます。
6. StyleBook のすべてのパラメータの値を入力します。また、[View Definition] をクリックして、使用する前に StyleBook の構成を表示することもできます。

   詳しくは、「デフォルトのスタイルブックを使用」を参照してください。
7. ［作成］をクリックします。

   必要なライセンスを消費し、アプリケーションをデプロイするための確認メッセージが表示されます。次に、メッセージの例を示します。

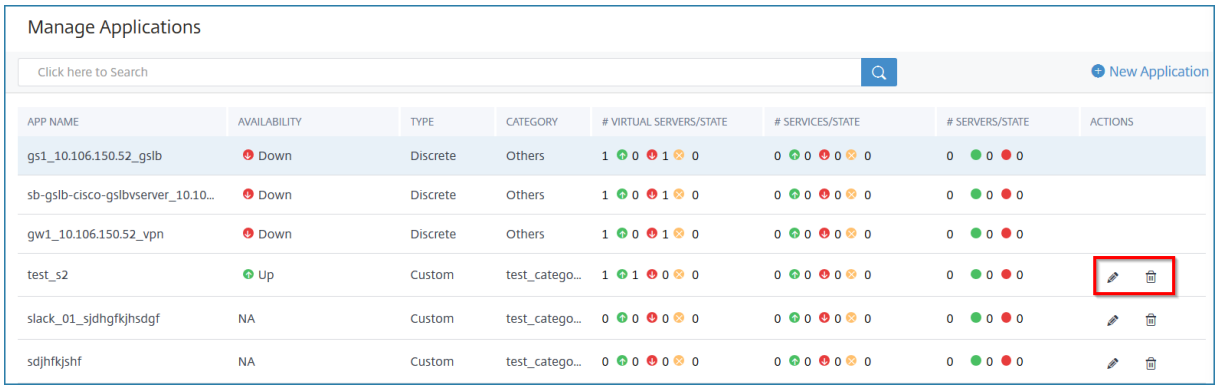


8. [**Yes**］をクリックします。

[**Dry Run**] をクリックして、選択した Citrix ADC インスタンスで Citrix ADM が作成しようとする構成を確認することもできます。このオプションは、設定の最終チェックを確認するためのテスト目的のためだけです。ドライランオプションが成功した場合でも、選択した Citrix ADC 実際の構成は、さまざまな理由（IP の競合、インスタンスにアクセスできないなど）が原因で失敗することがあります。

アプリケーションの編集または削除

「アプリケーション」ページでは、カスタムアプリケーションを編集または削除できます。アプリケーションを編集するには [編集] ボタンをクリックし、アプリケーションを削除するには [削除] ボタンをクリックします。



アプリダッシュボードとセキュリティダッシュボードのレポートのエクスポート

Citrix ADM では、現在のアプリダッシュボードのスナップショットを作成し、レポートとしてエクスポートできます。頻繁な間隔で、アプリ管理者はこれらのレポートを使用して、アプリの使用状況やパフォーマンス上のペナルティについて更新する必要があります。

この機能を使用すると、管理者はこのデータを.png、.jpeg、または.pdf レポートとして抽出できます。

> 注
>
> Citrix ADM の他のレポートエクスポートオプションとは異なり、アプリダッシュボードとセキュリティダッシュボードのレポートは、.pdf または.png ファイルとしてのみエクスポートできます。.csv 形式は現在サポートされていません。

レポートがシステムにダウンロードされます。[App Dashboard] ページと [App Security Dashboard] ページから、第 2 レベルのページに移動してレポートとしてエクスポートすることもできます。現在、一度に 1 つのアプリケーションのレポートしかダウンロードできません。

SSL 証明書管理の自動化

May 7, 2021

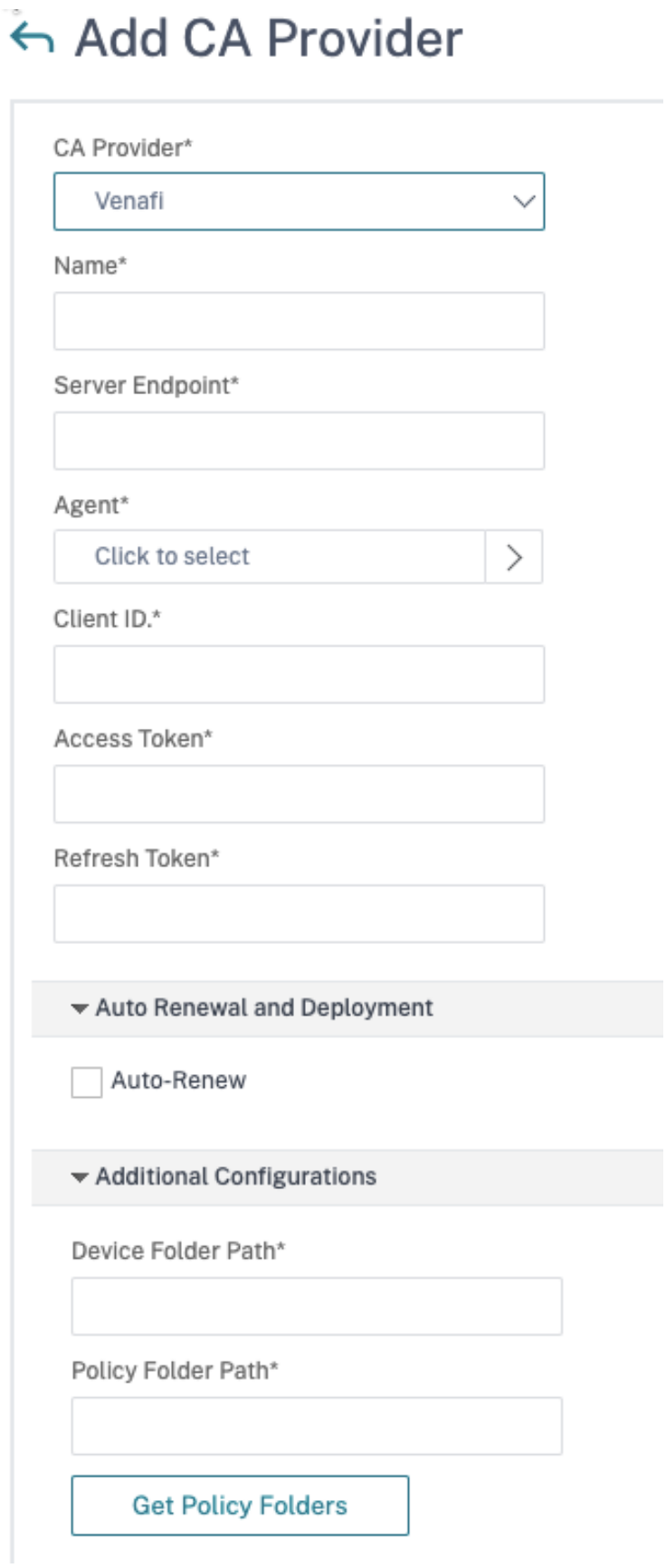
デジタルセキュリティを維持するには、環境内の SSL 証明書の管理を自動化する必要があります。すべての証明書をプロアクティブに管理および監視し、証明書の有効期限を通知し、有効期限が切れる前に証明書を自動的に更新する方法が必要です。有効期限が切れた SSL 証明書は、セキュリティリスクにつながります。Venafi Trust Protection Platform サーバーを ADM で構成して、ADC インスタンスにインストールされた SSL 証明書の管理を自動化できます。

Venafi と ADM を使用すると、ライフサイクル全体を通じて SSL 証明書を管理できます。ADM アプリケーションダッシュボードでは、次のタスクを実行できます。

- SSL の問題とアプリケーションのスコアを確認します。
- SSL の問題のトラブルシューティングを行い、推奨される修正を適用します。
- アプリケーションにバインドされた証明書をチェックします。
- 証明書の作成、インストール、および更新をすばやく行えます。
- 証明書の更新を自動化します。
- 生成された証明書を ADC 仮想サーバーにバインドすることにより、アプリケーションをセキュリティで保護します。
- 特定のアプリケーションの SSL タスク関連ログをすべて確認します。

ADM での **Venafi** サーバーの設定

Venafi サーバの設定は、2 段階のプロセスです。まず、Venafi サーバーを ADM に追加します。次に、Venafi サーバでポリシーを設定します。Venafi サーバーを ADM に追加するには、ADM GUI から、**[**ネットワーク**] > [SSL** ダッシュボード**] > [**サードパーティ **CA]** に移動します。［追加］をクリックします。

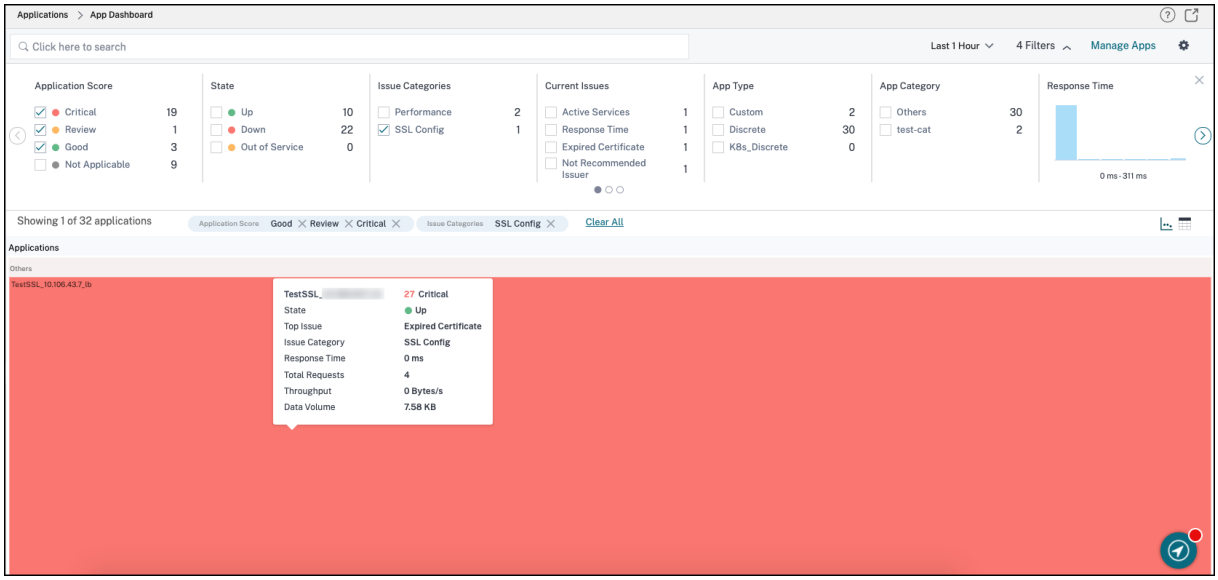


表示されたフィールドに詳細を入力します。証明書を自動的に更新する場合は、**[**自動更新] オプションをオンにします。各フィールドの詳細については、フィールドにカーソルを合わせてiアイコンをクリックします。

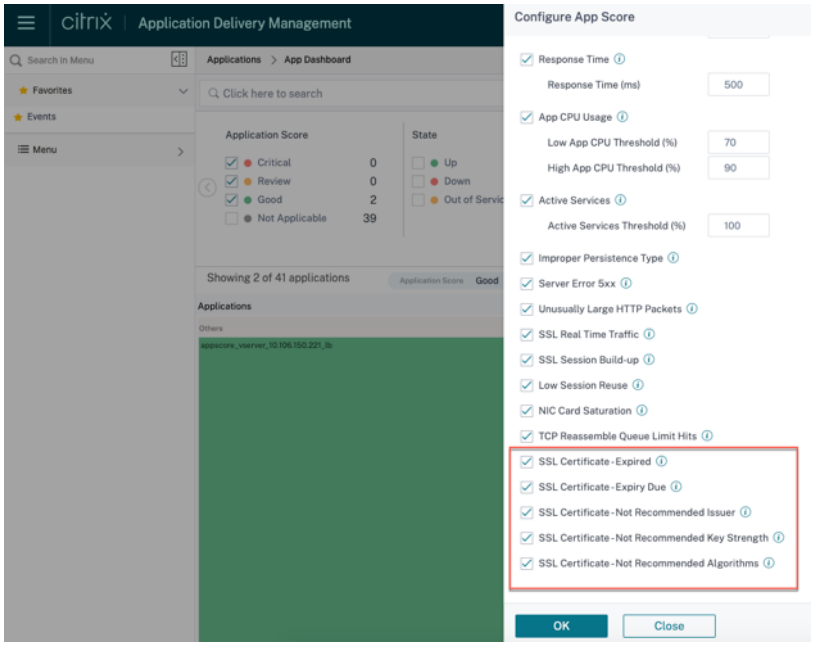
Venafi サーバーを構成したら、ADM ダッシュボードを使用して SSL 証明書を管理できます。

SSL 証明書のライフサイクルの管理

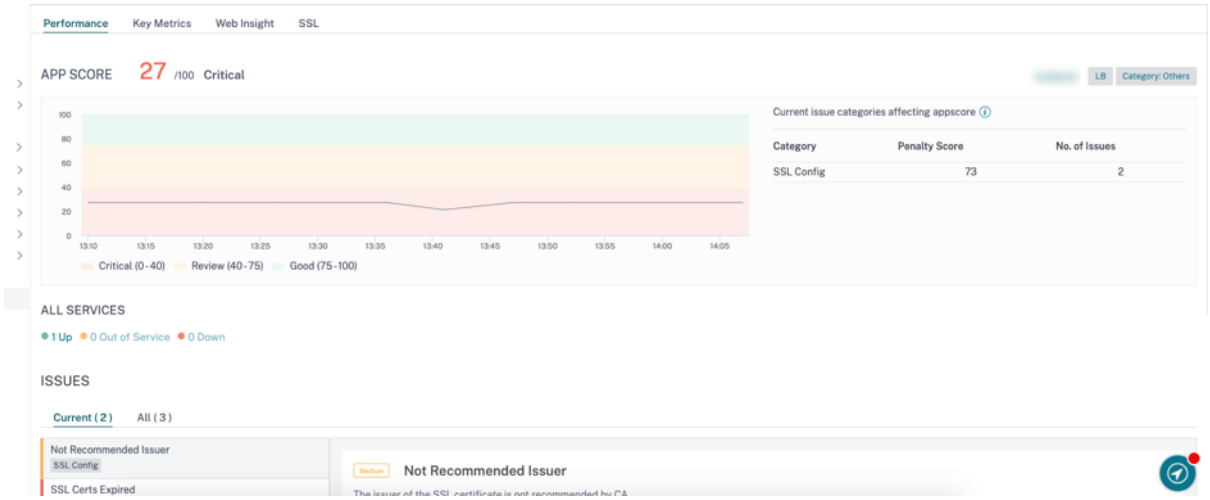
アプリケーションダッシュボードは、SSL 証明書をエンドツーエンドで管理するためのワンストップの場所です。ADM GUI から、[アプリケーション**] > [**アプリケーションダッシュボード] に移動します。[問題カテゴリ] で [**SSL** 設定] を選択します。[現在の問題] で、アプリケーションの SSL 関連の問題を確認できます。SSL レポートを表示するには、[アプリケーション] の下の [アプリ] にカーソルを合わせます。レポートの詳細を表示するには、アプリをクリックします。この例では、27 のスコアを持つアプリケーションがあります。



さらに、クリティカルやレビューなどのアプリケーションスコアを使用して、問題をフィルタリングできます。SSL アプリケーションのスコアは SSL パラメーターに基づきます。SSL パラメーターは、ダッシュボードの右上隅にある [**Manage Apps**] 設定でデフォルトで有効になっています。

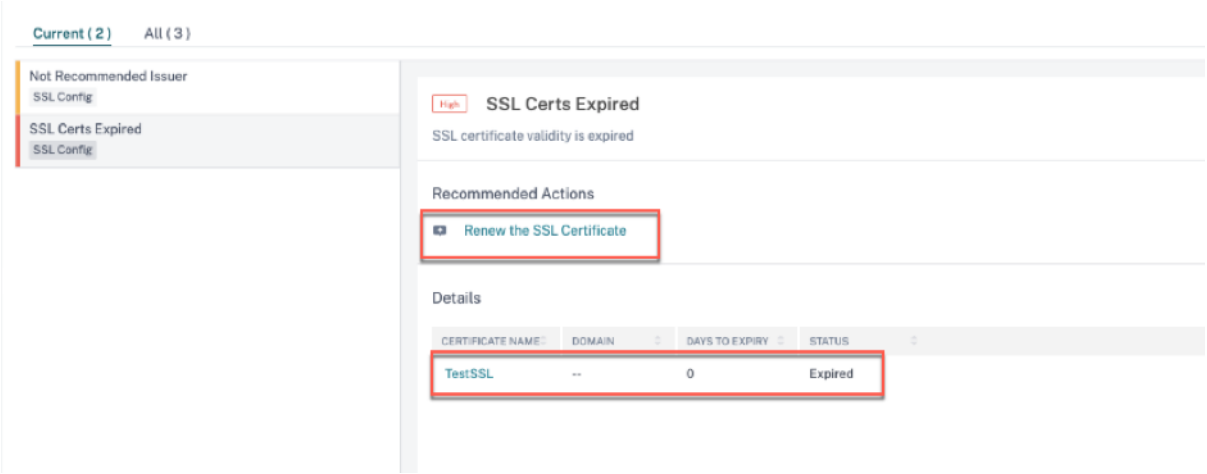


SSL パラメータを無効にするには、ボックスの選択を解除し、「**OK**」をクリックします。SSL レポートの詳細を表示するには、[アプリケーション] で、レポートを表示するアプリケーションをクリックします。



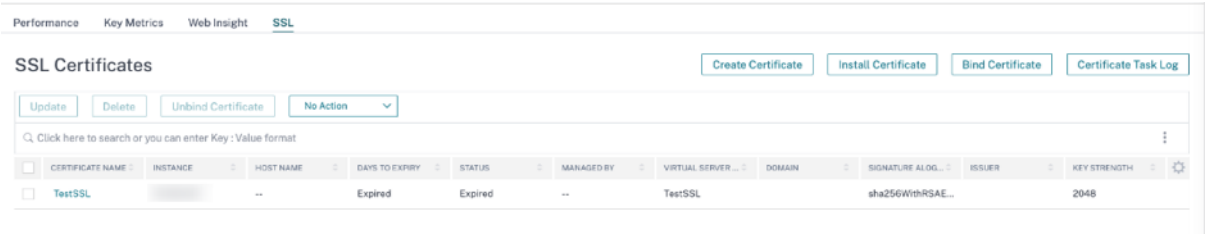
パフォーマンススコアを確認してページを下にスクロールすると、アプリが持つ仮想サーバー、仮想サーバーにバインドされた証明書、証明書の問題などの詳細を確認できます。証明書の詳細を表示するには、[証明書名] の下にあるリンクをクリックします。有効期限が切れた証明書の場合、それを更新することは可能か。

証明書を更新するには、証明書を作成し、インストールし、仮想サーバーにバインドする必要があります。

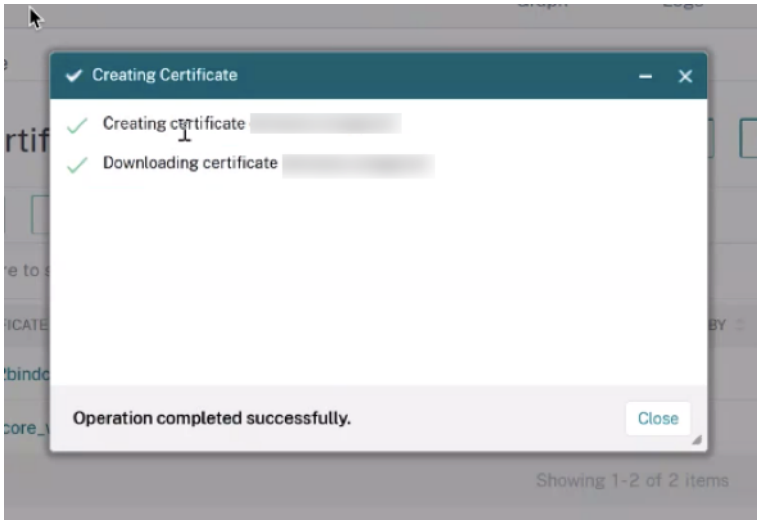


> 注:
>
> Venafi サーバーを ADM に追加すると、自動更新オプションを有効にすると、証明書の有効期限が切れる前に自動的に更新されます。

[SSL 証明書を更新する] をクリックすると、[SSL] タブが表示され、アプリケーションの仮想サーバーにバインドされているすべての証明書が一覧表示されます。このタブを使用して、証明書を作成してインストールし、仮想サーバーにバインドできます。また、特定のアプリケーションの SSL タスク関連ログで、特定のアプリケーションの SSL タスク関連ログをすべて確認することもできます。

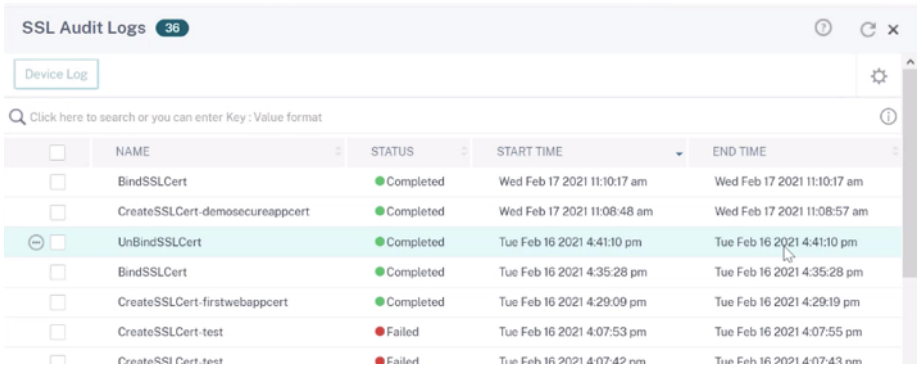


証明書を作成するには、[証明書の作成] をクリックして詳細を入力します。ダウンロードした証明書が暗号化されるため、パスワードを入力し、[**Create**] をクリックします。ADM は Venafi サーバーに接続して証明書を作成します。証明書がダウンロードされたら、[**Close**] をクリックします。



次に、[SSL] タブで [証明書のインストール] をクリックします。ダウンロードした証明書を選択し、[インストール] をクリックします。ADM を使用して ADC に SSL 証明書をインストールする方法の詳細については、Citrix ADC インスタンスへの SSL 証明書のインストールトピックの Citrix ADM からの SSL 証明書のインストールに関するセクションを参照してください。

次に、[証明書のバインド] をクリックします。必要に応じて、証明書のバインドを解除することもできます。次の SSL ポーリングの後、アプリケーションダッシュボードは新しいデータでリフレッシュされます。特定のアプリケーションのすべての SSL タスクログを確認する場合は、[証明書タスクログ] をクリックします。

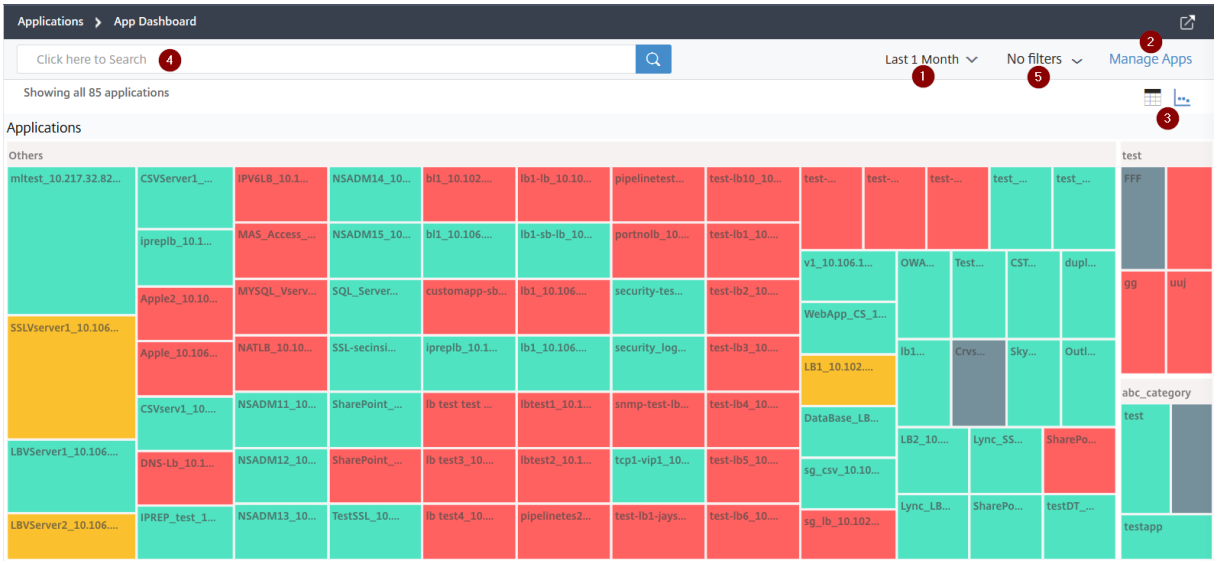


アプリケーションダッシュボードの概要

May 7, 2021

アプリケーション・ダッシュボードには、「その他」の下に個別のアプリケーションが表示され、それぞれのカテゴリにグループ化されたカスタム・アプリケーションが表示されます。

アプリケーション > ダッシュボードに移動して、アプリのダッシュボードを表示します。



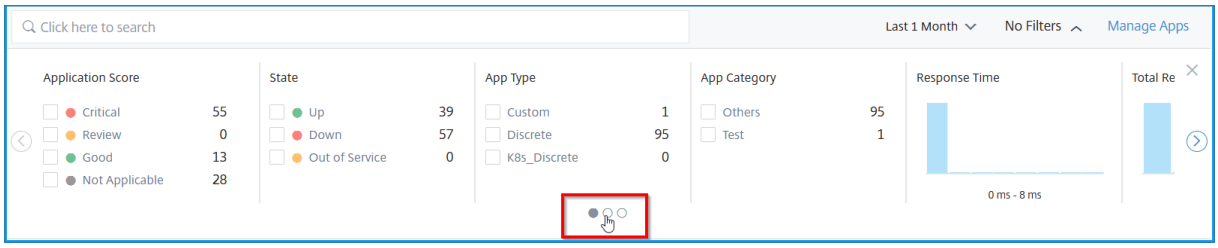
1 — 選択した期間（1 時間、1 日、1 週間、1 か月など）のアプリケーション詳細を表示します。

2： アプリケーションの管理と新しいアプリケーションの追加が可能

3： アプリケーションをテーブル・ビューまたはグラフ・ビューで表示できます。

4 — 検索バーを使用してアプリケーションを検索できます。

5： アプリケーションを表示するためにフィルタを適用できます。クリックすると、詳細が表示されます。

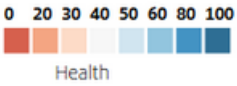


カルーセルスライダーを選択すると、すべてのオプションに簡単にアクセスできます。

次の操作を実行できます：

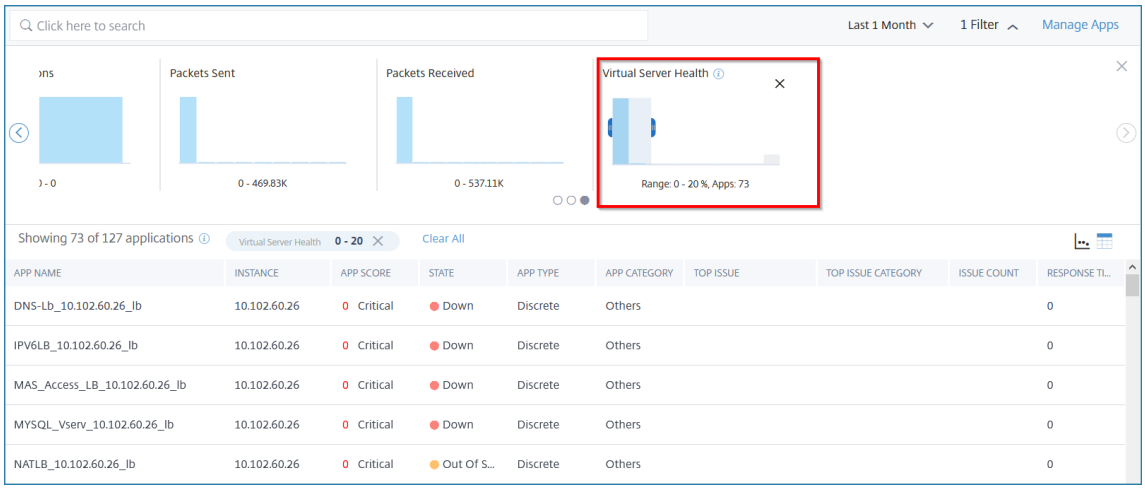
- スコアに基づいてアプリケーションを表示するために選択します。
  - 重要：アプリケーションのスコアは 0～40 未満です。
  - フェア — 申請スコアは 40～75 以下
  - 良好 — アプリケーションのスコアが 75 を超えています
  - 該当なし：アプリケーションに対して仮想サーバが設定されていません。

    次の表に、以前のアプリスコアと現在のアプリスコアの違いを示します。

アプリケーションスコア（重大、レビュー、良好、該当なし）	アプリのスコア（カラー凡例付きの以前のビュー）
スコアは、すべてのアプリケーションの現在の問題のペナルティスコアから **100** を引いたものとして計算されます。	スコアは **100** として計算されます**-**（アプリサーバーリソース **+Citrix ADC** システムリソース）
アプリケーションは、赤（重大）、オレンジ（レビュー）、緑（良好）、グレー（適用不可）などの色で表示されます。	アプリケーションは色の凡例で表示されます。 

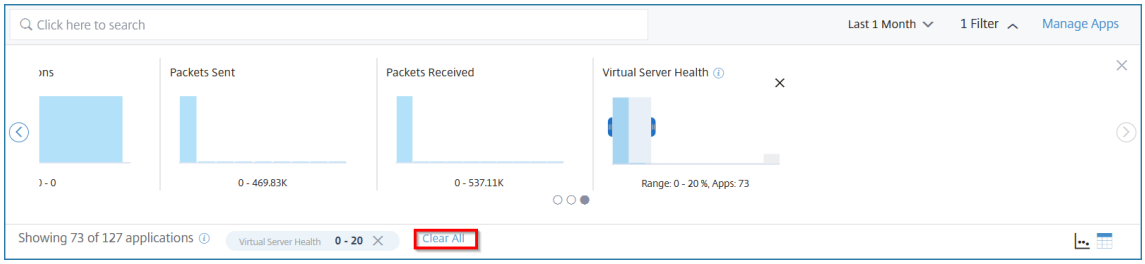
- 「Up」、「Down」、「Out of Service」などのアプリケーションのステータスに基づいてアプリケーションを表示するために選択します。
- 選択すると、「ショップ型」や「カスタム」などのアプリケーション・タイプに基づいてアプリケーションが表示されます。
- 選択すると、その下にグループ化されたカテゴリに基づいてアプリケーションが表示されます。
- ヒストグラムをドラッグして、フィルタを適用し、アプリケーションを表示します。

  たとえば、仮想サーバーの正常性が 0 ～20 のアプリケーションを表示する場合は、仮想サーバーの正常性ヒストグラムをドラッグして結果をフィルタリングします。



> 注
>
> ヒストグラムをクリックして、関連するアプリケーションを表示することもできます。

[すべてクリア] をクリックして、適用されたフィルタをクリアします。



フィルタを適用できるアプリケーションの概要を次に示します。

- アプリケーション・スコア:「クリティカル」、「レビュー」、「良好」、「該当なし」に基づいてアプリケーションを表示できます。

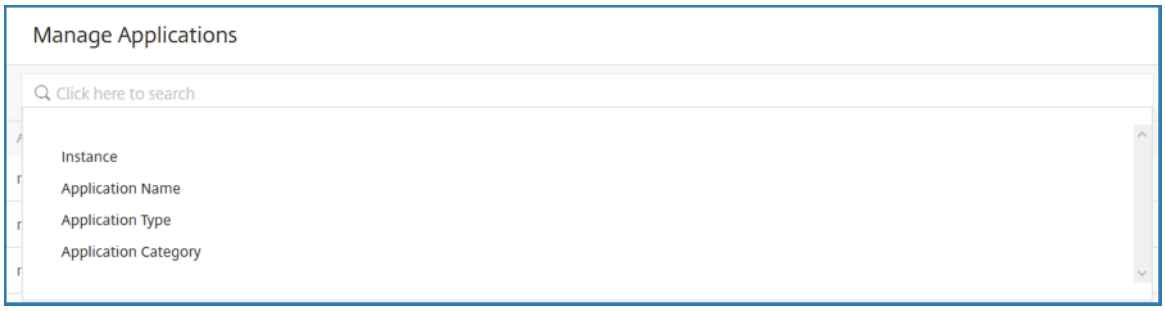
  > 注
  >
  > 既定では、[クリティカル]、[レビュー]、および [良好] ステータスのアプリケーションを表示できます。ステータスが「該当なし」のアプリケーションを表示するには、「適用不可」オプションを選択する必要があります。

- 状態:アプリケーションのステータス（Up、**Down**、**Out of Service**）に基づいてアプリケーションを表示できます。
- [現在の問題] — [パフォーマンス]、[インスタンスの状態]、[設定]、[システムリソース] などの問題の種類を選択して、特定の問題に影響を受けたアプリケーションのリストを取得できます。
- アプリケーションの種類 — カスタム、離散、**Kubernetes** サービスなどのアプリケーションの種類に基づいてアプリケーションを表示できます。
- アプリケーションカテゴリ — 割り当てられたカテゴリに基づいてアプリケーションを表示できます。
- 応答時間 — アプリケーションが受信した平均応答時間を表示するヒストグラム。
- **Total Requests** — アプリケーションによって受信された要求の総数を表示するヒストグラム。
- スループット — アプリケーションによって処理された総ネットワークスループットを表示するヒストグラム。
- **Data Volume** — アプリケーションによって処理された合計データを表示するヒストグラム。データ量は、アプリケーションの合計要求バイト数と応答バイト数で計算されます。
- クライアント接続 — アプリケーションによって確立された平均クライアント接続を表示するヒストグラム。
- サーバー接続 — アプリケーションによって確立された平均サーバー接続を表示するヒストグラム。
- **Packets Sent** — アプリケーションによって送信された合計パケットを表示するヒストグラム。
- 受信パケット数:アプリケーションによって受信された合計パケットを表示するヒストグラム。
- 仮想サーバーの健全性 — スコア範囲 0% ～100% のアプリケーションの合計を表示するヒストグラム。仮想サーバの正常性とは、アプリケーションに関連付けられたアクティブなサービスの割合（%）です。

たとえば、仮想サーバに 2 つのサービスが設定されていて、そのうちの 1 つがダウンしている場合、スコアは 50% です。

検索バーを使用して結果を検索およびフィルタする

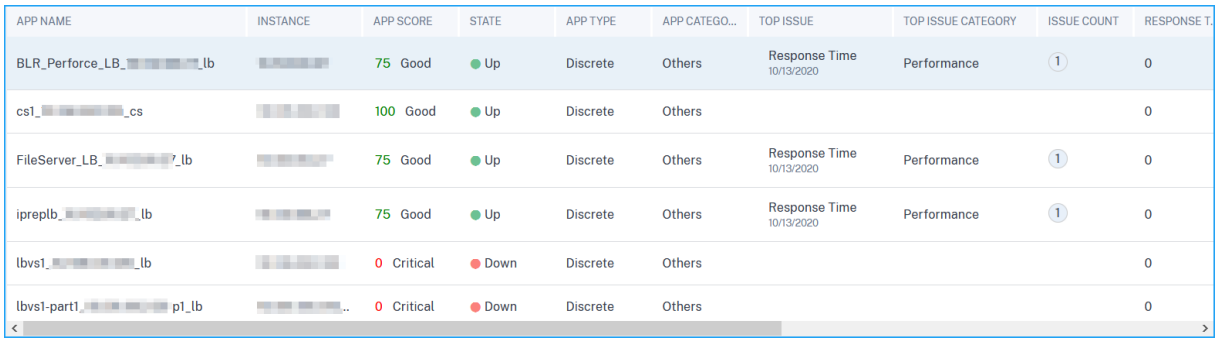
検索バーにマウスポインタを置き、カテゴリを選択して検索を絞り込むことができます。



アプリケーションの表示

May 7, 2021

デフォルトでは、アプリケーションダッシュボードにすべてのアプリケーションが表示されます。要件に応じて、フィルタオプションを使用してアプリケーションを表示できます。



ダッシュボードには、次のアプリケーション詳細が表示されます。

- 「アプリケーション名」— アプリケーション名を示します。
- インスタンス：Citrix ADC インスタンスを表します。
- アプリケーションスコア — アプリケーションのスコアと、「クリティカル」、「良い」、「フェア」、「適用不可」などのステータスを示します。
- 状態：アプリケーションの現在の可用性を示します。たとえば、「アップ」、「ダウン」、「部分的にアップ」、「サービス外」、「**NA**」などです。
  - **Up**：アプリケーションに関連づけられているすべての仮想サーバが Up です。

  - ダウン：アプリケーションに関連づけられているすべての仮想サーバがダウンしています。
  - 部分的にアップ — アプリケーションに関連づけられた仮想の 1 つが、ダウンまたはアウトアウトアウトアウトアウトアウトアウトアウトです。
  - **Out of Service**： アプリケーションに関連づけられているすべての仮想サーバが Out of Service です。
  - **NA** — アプリケーションに対して仮想サーバーが設定されていません。
- アプリケーションタイプ — カスタム、離散サービス、**Kubernetes** サービスなどのアプリケーションの種類を示します。
- 「アプリケーションカテゴリ」— アプリケーションに割り当てられているカテゴリを示します。
- 「**Top** issue」— アプリケーションのエラー数が最大である問題を示します。
- 「上位の課題カテゴリ」— 問題のカテゴリを示します。
- 「発行件数」— アプリケーションの発行件数の合計を示します。
- 応答時間：アプリケーションからの応答の平均応答時間を示します。
- 「リクエストの合計」— アプリケーションによって受信されたリクエストの合計を示します。
- 「スループット」— アプリケーションのネットワークスループットの合計を示します。スループットは、仮想サーバの Req バイト/秒 + 解像度バイト/秒で計算されます。
- **Data volume** — アプリケーションによって処理されたデータの合計を示します。
- クライアント接続 — アプリケーションによって確立された平均クライアント接続を示します。
- 「サーバー接続」— アプリケーションによって確立された平均サーバー接続を示します。

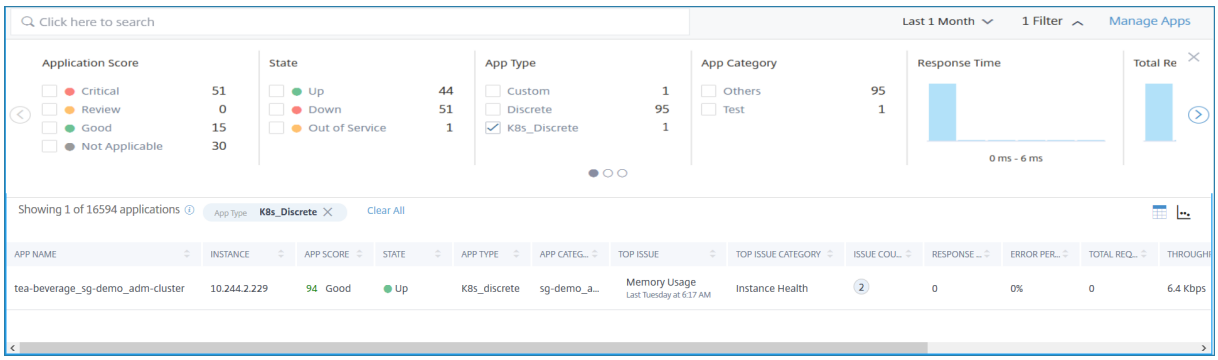
マイクロサービスアプリケーションの表示

マイクロサービスアプリケーションを表示するには、[アプリケーションの種類] フィルタの [**K8S_Discrete**] オプションを選択します。

マイクロサービスアプリケーションは、次の名前の形式で **App Dashboard** に表示できます。

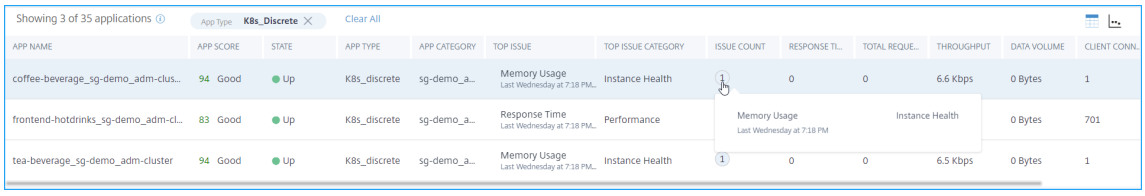
`<k8s service>_<k8s namespace>_<k8s cluster_name>`

たとえば、`tea-beverage_sg-demo_adm-cluster`は、クラスタ`adm-cluster`内の`sg-demo`の名前空間を持つ「tea-bevelage」という名前のサービスを指します。



選択した期間のダッシュボードには、次のメトリックが表示されます。

- 「アプリケーション名」— アプリケーション名を示します。
- インスタンス：Citrix ADC CPX インスタンスの IP アドレスを示します。
- 「アプリケーションスコア」— アプリケーションのスコアを示します。
  - クリティカル — アプリのスコアは 0 から 40 以下です
  - レビュー — アプリのスコアは 40 から 75 未満です
  - 良好 — アプリのスコアが 75 を超えています
- [**State**]：現在のアプリケーションのステータスを示します。
- アプリケーションカテゴリ — アプリケーションがホストされているクラスター名を示します。
- 「上位問題」— 現在のアプリケーションスコアに影響する上位課題を示します。
- 「上位課題カテゴリ」 — アプリケーションに影響する問題カテゴリを示します。
- 「問題数」— アプリケーションに影響する問題の合計を示します。問題の件数の上にマウスポインタを合わせると、問題の概要が表示されます。



- [**Response** Time]：アプリケーションが受信した平均応答時間を示します。
- 「エラーパーセンテージ」— アプリケーションの 5xx エラーの平均エラー率を示します。
- 「リクエストの合計」— アプリケーションによって受信された要求の総数を示します。
- スループット — アプリケーションによって処理される総ネットワークスループットを示します。
- **Data volume** — アプリケーションによって処理されたデータの合計を示します。データ量は、アプリケーションの要求バイト数と応答バイトの合計として計算されます。
- クライアント接続 — アプリケーションによって確立された平均クライアント接続を示します。これは、選択したサービスに接続されている関連付けられた発信サービスを参照することもできます。

- 「サーバー接続」— アプリケーションによって確立された平均サーバー接続を示します。これは、選択したサービスに接続されている関連付けられた着信サービスを参照することもできます。

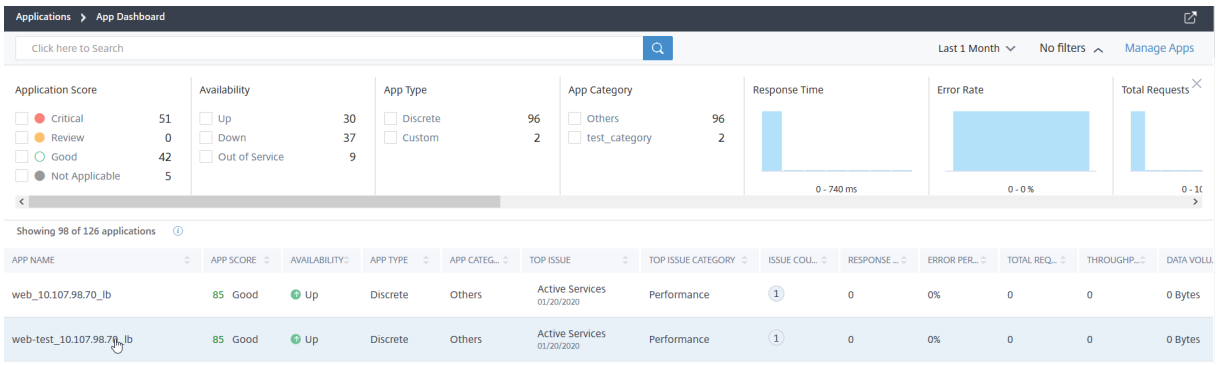
[**+**] オプションをクリックして、ダッシュボードに表示するオプションを追加または削除します。

アプリケーションをクリックして、アプリケーションの詳細を表示します。詳細については、マイクロサービスアプリケーションの詳細を参照してください。

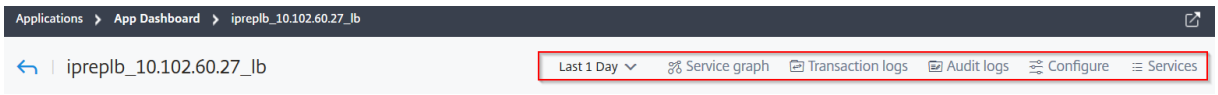
アプリケーションの詳細

May 7, 2021

ダッシュボードからアプリケーションをクリックして、詳細情報をドリルダウンします。



選択したアプリケーションページが表示されます。

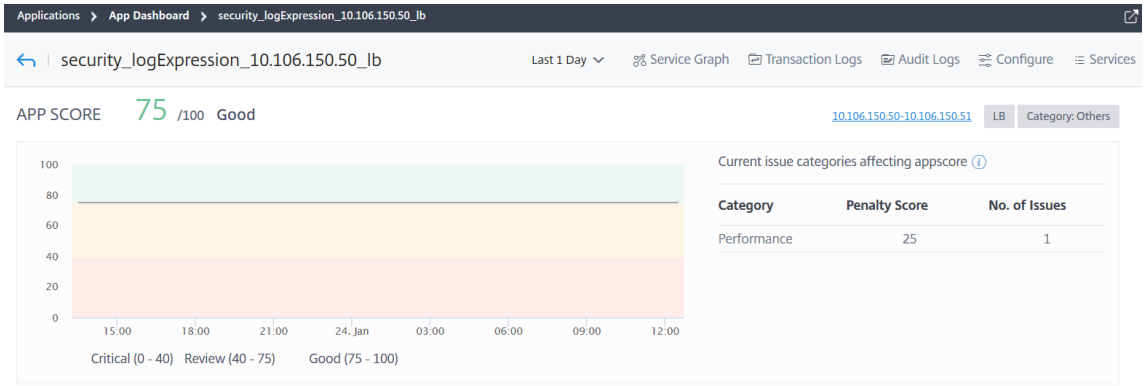


アプリケーション詳細ページから：

- リストから期間を選択して、特定の期間の詳細を表示します。
- 「サービス・グラフ」をクリックして、選択したアプリケーションのサービス・グラフを表示します。詳しくは、「アプリケーションのサービスグラフ」を参照してください。
- トランザクションログをクリックすると、選択したアプリケーションの詳細なトランザクションが表示されます。
- [監査ログ] をクリックして、監査ログの詳細情報を表示します。
- [**Configure**] をクリックして、選択したアプリケーションのサービスおよびサービスグループの構成を表示または編集します。
- [サービス] をクリックして、アプリケーションにバインドされたサービスを表示します。

期間を選択すると、次のアプリケーション詳細が表示されます。

- アプリケーションスコア — 選択した期間のアプリケーションスコア。最終的なスコアは、ペナルティ合計を差し引いた **100** として計算されます。

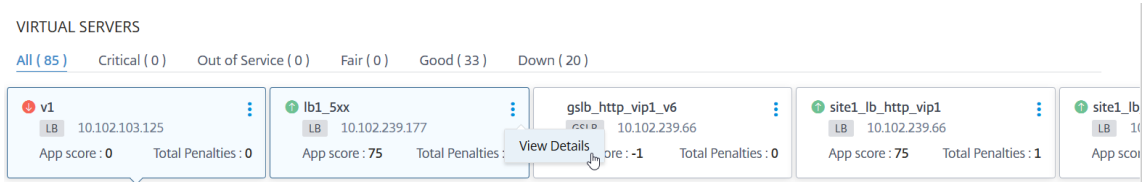


このダッシュボードでは、アプリのスコアに影響している現在の問題を表示することもできます。[懸案事項] で懸案の詳細を表示できます。

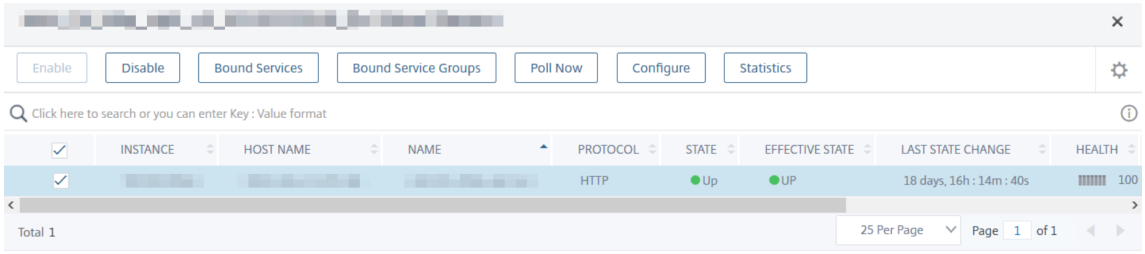
- 仮想サーバ —

> 注
>
> [仮想サーバー] セクションは、カスタムアプリケーションに対してのみ表示されます。個別のアプリケーションの場合は、**IP** アドレスをクリックして仮想サーバーの詳細を表示します。

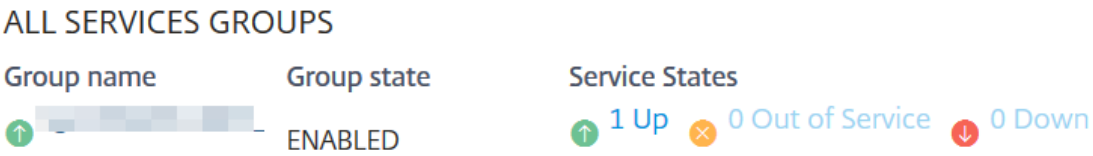
カスタムアプリケーションに関連付けられているすべての仮想サーバーを表示します。



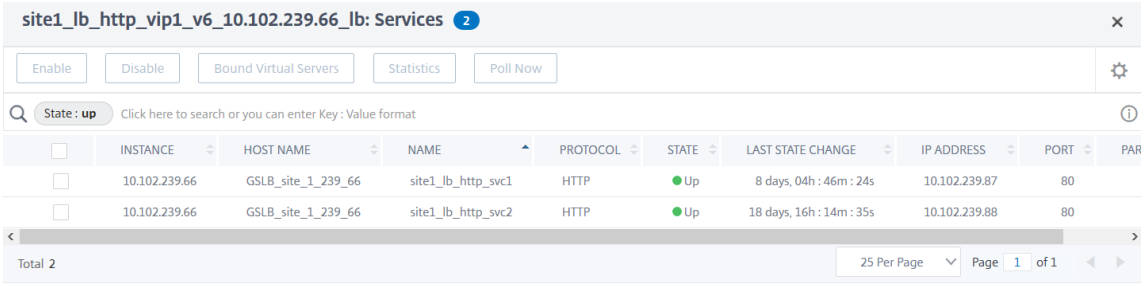
[詳細の表示] をクリックして、仮想サーバの設定を表示および管理します。



- すべてのサービス — アプリケーションにバインドされているサービス



クリックすると、サービスの詳細を表示し、サービス設定を管理できます。



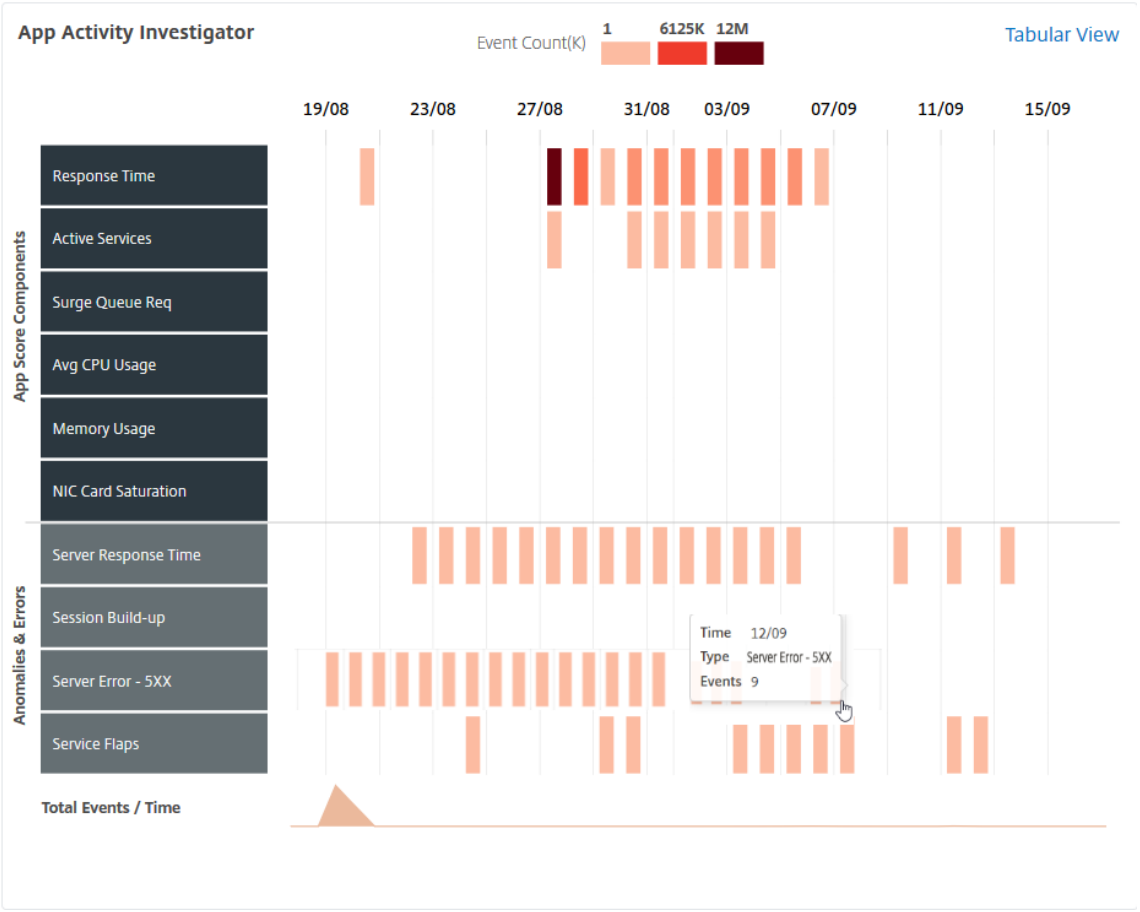
- [問題] — 選択したアプリケーションに適用可能な問題。次の問題とそのカテゴリを表示できます。

パフォーマンス	インスタンスの健全性	構成	システムリソース
応答時間	平均 CPU 使用率	不安定なサーバ	不適切な永続性タイプ
アクティブなサービス	メモリ使用率	異常に大きい HTTP パケット	NIC カードの飽和
セッションの再利用が低い		TCP 再構成キュー制限ヒット	
アプリの CPU 使用率			
サージキューのビルダップ			
SSL リアルタイムトラフィック			
セッションのビルダップ			
サーバの応答時間			
サービスフラップ			

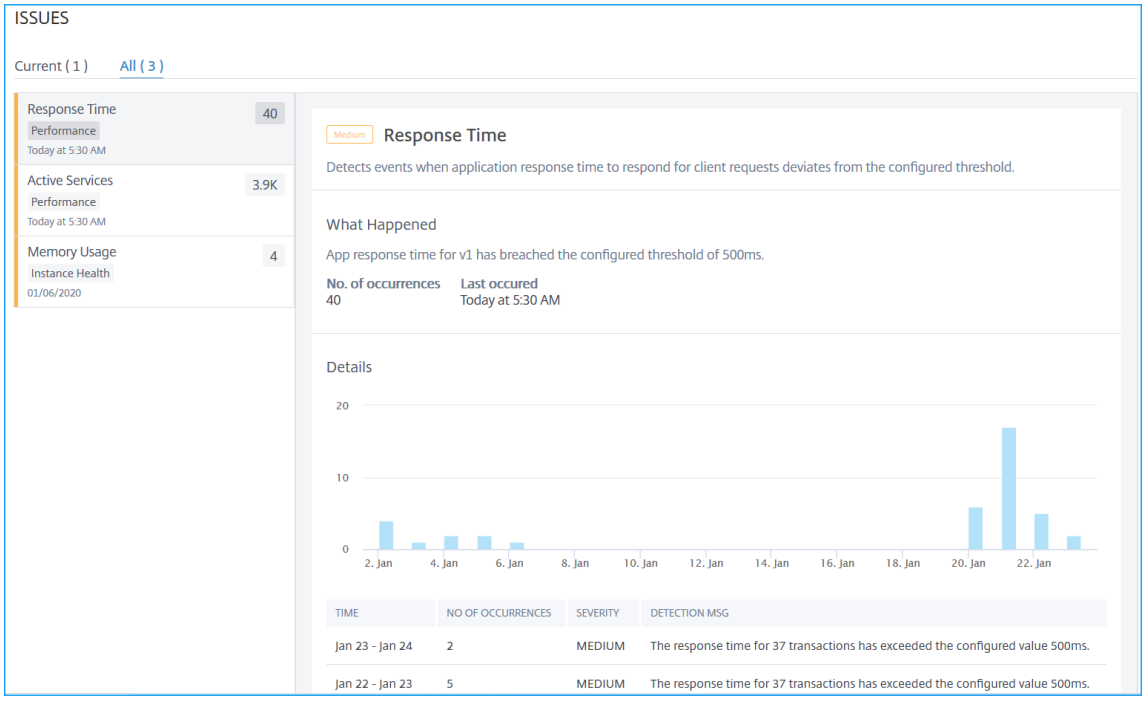
各問題をクリックして、検出メッセージ、問題が発生した日時、推奨アクション、詳細などの詳細を確認します。

詳しくは、「アプリケーション分析用のパフォーマンス・インディケータ」を参照してください。

次の画像は、アプリアクティビティ調査官のページの前のビューです。

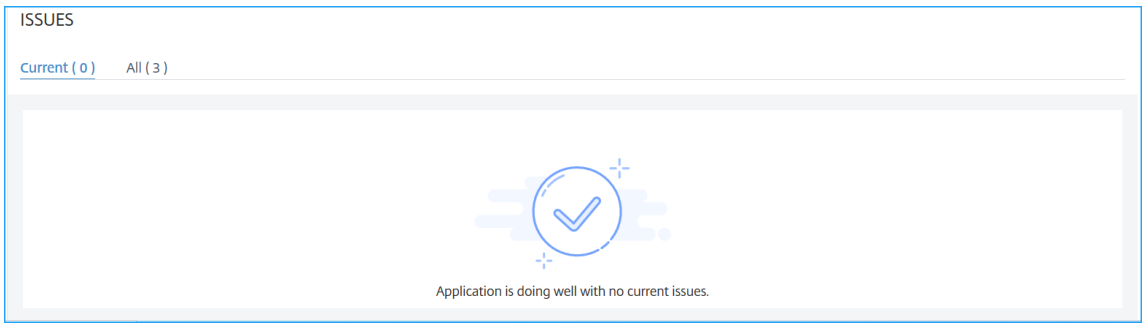


これで、[懸案事項] セクションのすべての懸案事項と、[アプリアクティビティ調査] ページで表示できたカテゴリを表示できます。

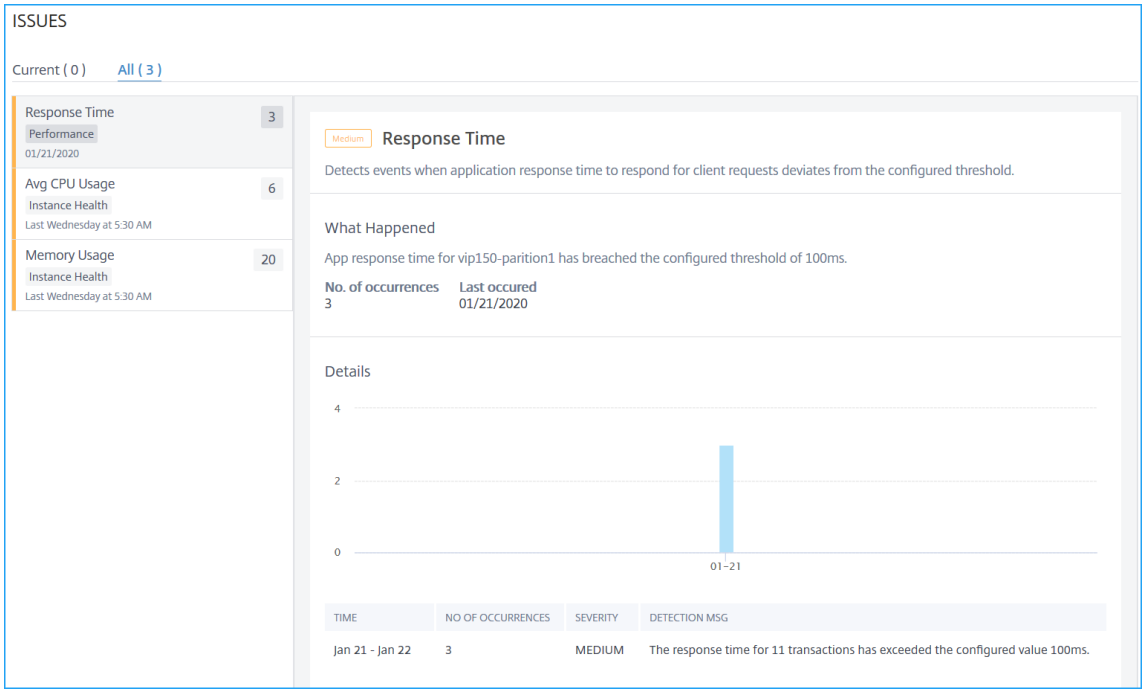


- [**Current**] タブに表示される問題は、選択した期間のアプリケーションの問題を参照します。
- [**All**] タブに表示される問題は、アプリケーションの問題の合計を示します。

次の例は、1 日間のアプリケーションの問題です。[**Current**] タブには、アプリのスコアに影響する現在の問題がないことが示されます。



[すべて] タブには、1 日の期間中に検出された問題の合計が表示されます。



ピークとリーンの使用状況の分析

May 7, 2021

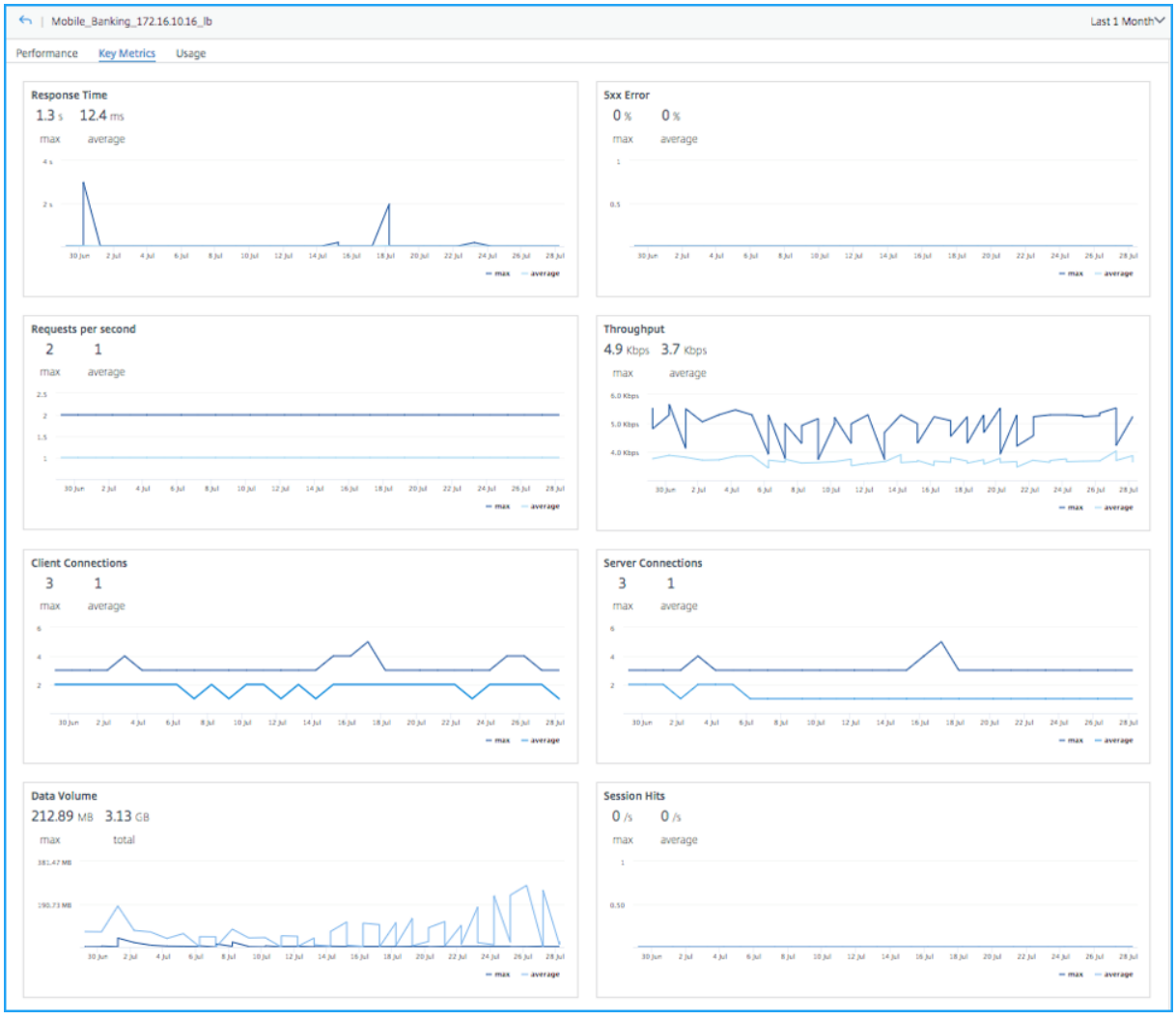
Web アプリケーションは、トラフィックが多いか、低いトラフィックを受信でき、1 日または 1 時間のトラフィック範囲は予測できません。同様に、Web アプリケーションでも、スケジュールされたメンテナンスまたはアップグレード中に、特定の期間のダウンタイムが必要になります。管理者は、トラフィックを分析し、次の適切な時間を見つける必要があります。

- ウェブアプリケーションのスケールアップ
- ウェブアプリケーションのダウンタイムを計画する

Citrix ADM ピーク使用量とリーン期間分析機能を使用すると、選択した期間の主要なメトリックを分析できます。これらのメトリックから、トラフィックを分析し、ウェブアプリケーションをスケールアップするか、スケジュールされたダウンタイムを計画するタイミングを決定できます。

アプリのスケール制限の評価

[**App Dashboard**] からアプリケーションをクリックし、[**Key Metrics**] タブを選択して、すべてのメトリックの統合ビューを表示します。メトリックを分析する期間をリストから選択します。



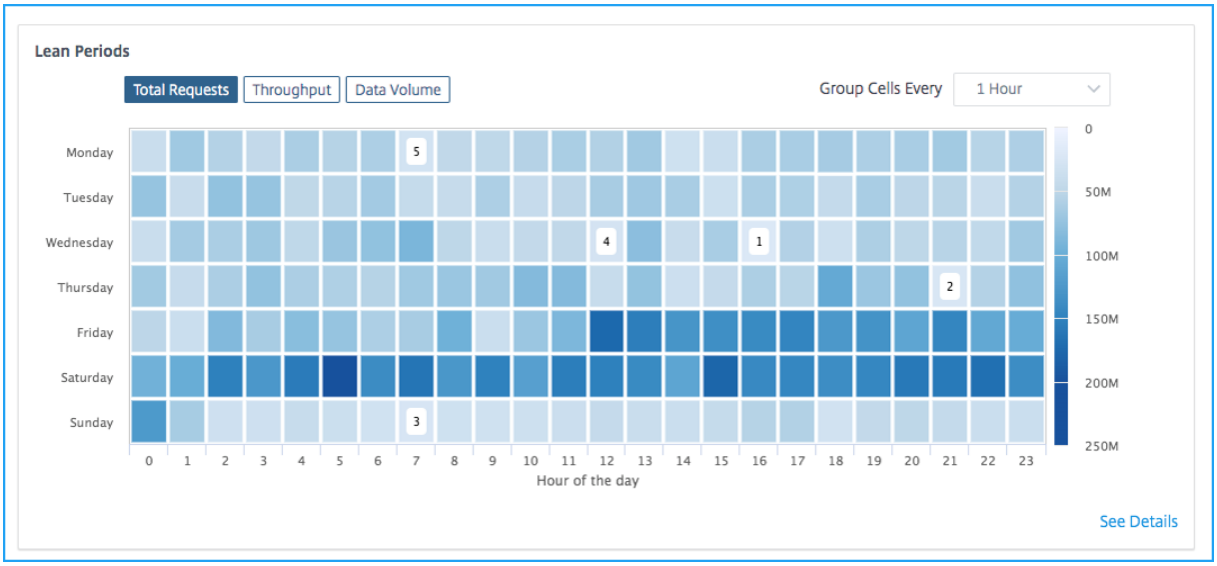
各メトリックについて、次の項目を表示できます。

- 「最大」— 選択した期間の最大値を示します
- **Average** — 選択した期間の平均値を示します。

画像の例では、応答時間の最大値は 1.3 秒を示しています。グラフチャートから、選択した期間で応答時間が長くなる回数を分析できます。同様に、他のメトリックスの詳細を表示し、アプリケーションがピーク使用量を受けているかどうかを分析し、本番環境のスケールアップを決定することもできます。

上位 **5** つのアプリのメンテナンスウィンドウを特定する

アプリケーションダッシュボードからアプリケーションをクリックし、[**Key Metrics**] タブを選択して、アプリケーションのリーン期間を表示します。アプリケーションの一般的なダウンタイムは、要件に応じて、1 時間、2 時間、または 4 時間になります。ダウンタイムを計画する時間（1 時間、2 時間、または 4 時間）をリストから選択できます。リストから時間を選択すると、総リクエスト数、スループット、データボリュームなどのメトリックスのトラフィックを分析できます。アプリケーションの使用量が少ない場合に、ダウンタイムをスケジュールする適切な時刻を選択できます。
次の例では、1 時間のダウンタイムを分析します。



ヒートマップビューには、選択した期間におけるアプリケーションの使用状況が表示されます。色が濃い (青) は、アプリケーションの使用率が高いことを示します。

ヒートマップビューでは、アプリケーションのダウンタイムを計画するために、上位 5 つの最小期間 (1、2、3、4、5) も表示されます。

1 — 水曜日の午後 4 時から午後 5 時までの最初の提案を示します

2 — 木曜日の午後 9 時から午後 10 時までの 2 番目の提案を示します

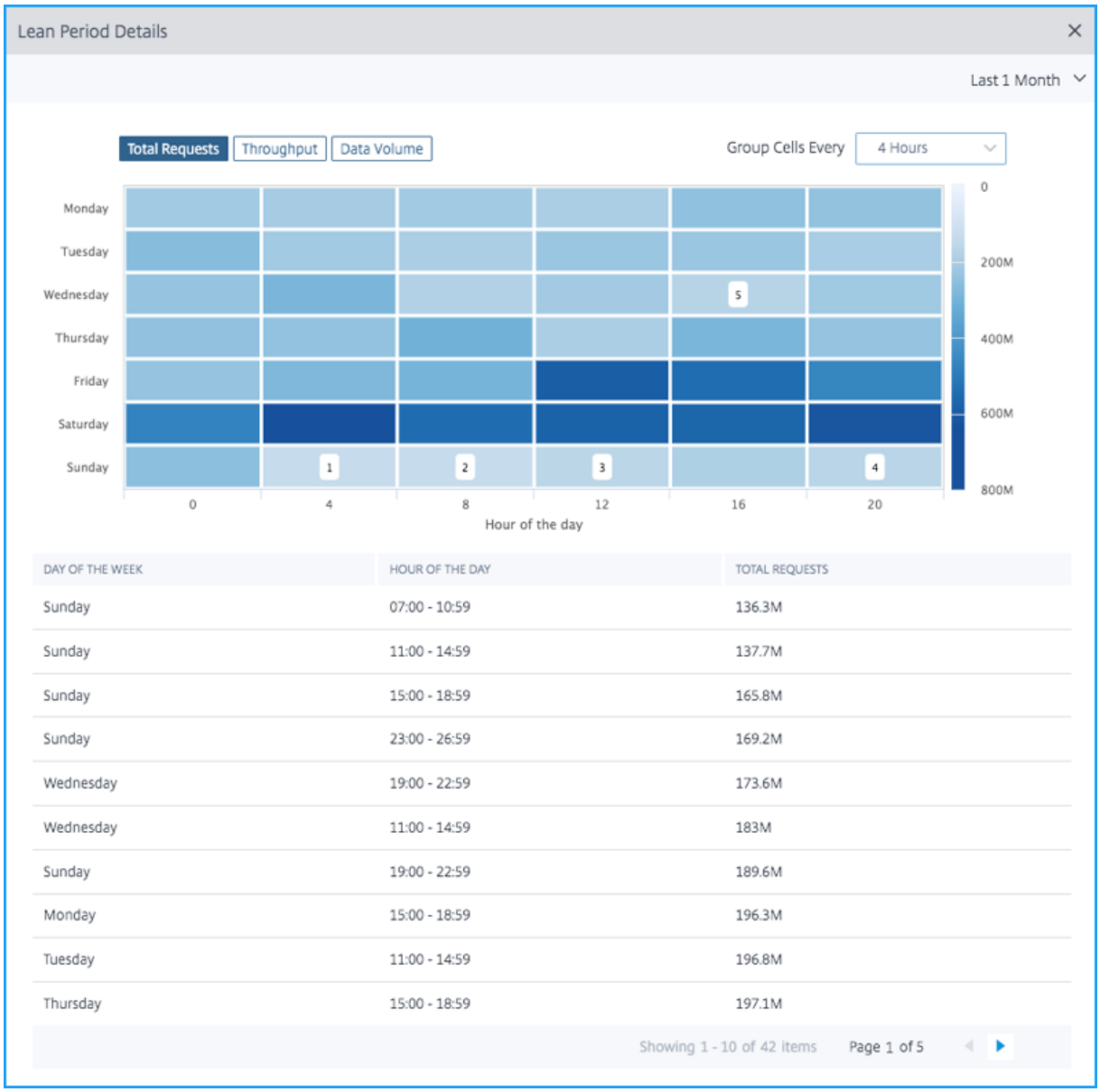
3 — 日曜日の午前 7 時から午後 8 時までの 3 番目の提案を示します

4 — 水曜日の午後 12 時から午後 1 時までの 4 番目の提案を示します

5 — 月曜日の午前 7 時から午後 8 時までの 5 番目の提案を示します

他のすべての日のトラフィックを分析した後、ダウンタイムをスケジュールする他の日および時刻を選択することもできます。

[詳細を表示] をクリックして、詳細情報を表示します。[**Total Requests**]、[スループット]、または [**Data Volume**] タブをクリックして、上位 5 つの最小期間と他の日の詳細を表示します。



アプリケーションの使用状況と異常

May 7, 2021

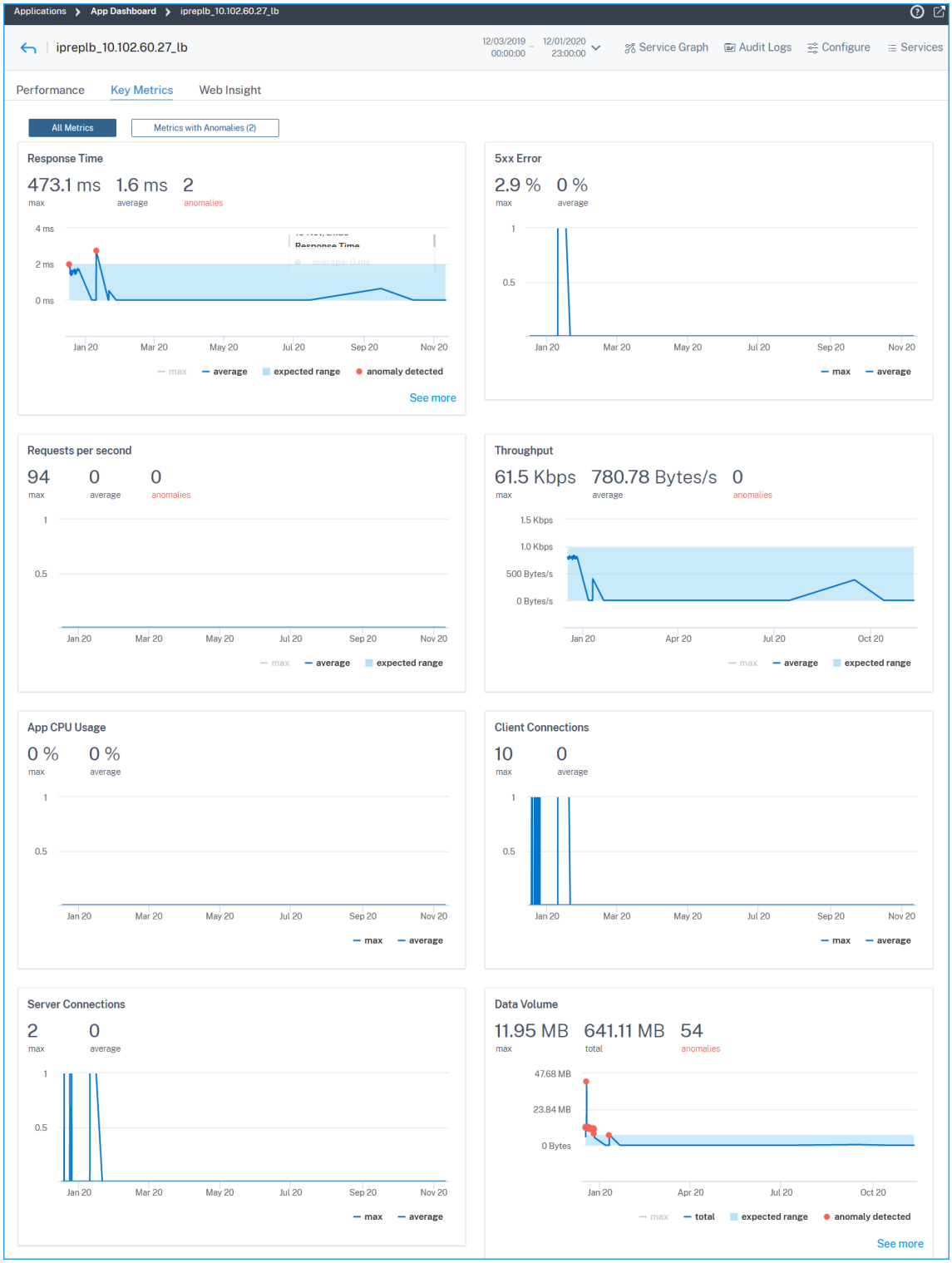
管理者は、アプリケーションがどのように利用されているかを確認する必要があります。アプリケーションキーメトリックは、アプリケーションの使用状況を特定するのに役立ちます。アプリケーションへのトラフィック範囲は予測できないため、特定の期間において、アプリケーションパフォーマンスの異常な偏差が発生することがあります。こ

のようなシナリオでは、管理者として、このような突然の異常を表示および分析し、迅速なトラブルシューティングが必要かどうかを確認することができます。

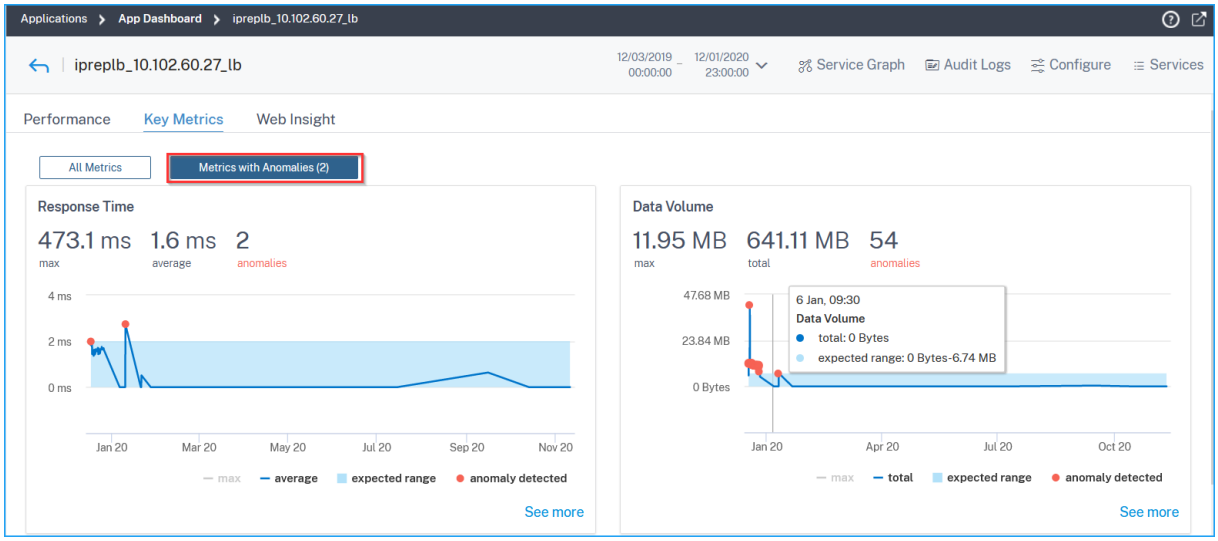
Citrix ADM は、このような異常を検出し、必要な詳細を提供します。「アプリケーション」**>**「ダッシュボード」に移動し、アプリケーションをクリックし、「キー・メトリック」タブを選択します。Citrix ADM はトラフィックパターンを監視し、主要なメトリックが予想される範囲内にあるかどうかを分析します。期待される範囲よりも偏差がある場合、Citrix ADM はこれらの偏差を異常として報告します。

次の主要メトリックの異常を表示できます。

- 応答時間
- スループット
- データ量
- 1 秒あたりのリクエスト数



[異常のあるメトリック] タブをクリックして詳細を表示します。



各メトリックで、[詳細を表示] オプションをクリックして詳細を表示することもできます。次の例は、アプリケーションデータボリューム用です。

次の項目を表示できます。

- 最大値、合計値、期待範囲、および異常を示すグラフ
- 問題のトラブルシューティングに推奨される処置
- [詳細] の下にある時刻と異常の詳細

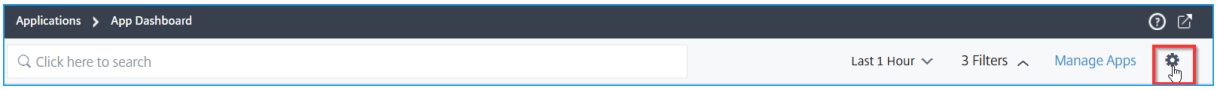
アプリスコアコンポーネントを選択し、しきい値を設定します

May 7, 2021

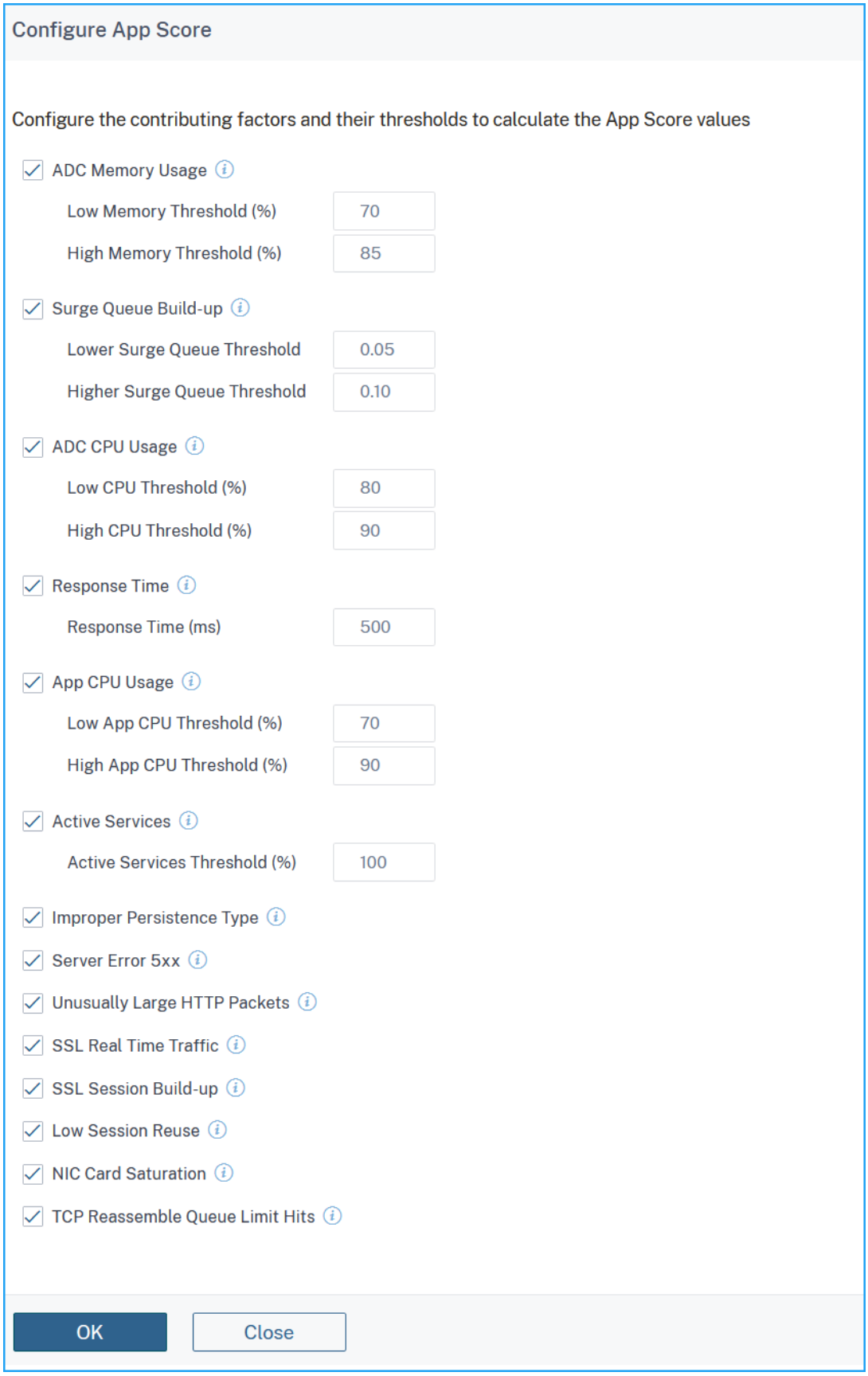
アプリダッシュボードでは、管理者は、コンポーネントを選択し、アプリスコア計算のしきい値を構成することができます。アプリスコアは、次の定義を定義するスコアリングシステムです。

- アプリケーションがどれくらいうまく実行されているか
- アプリケーションが応答性の点でうまく動作しているかどうか

[アプリケーション**] > [**ダッシュボード] に移動し、[設定] アイコンを選択します。



[アプリスコアの構成] ページで、コンポーネントを選択し、しきい値を構成して、最終的なアプリスコアを決定できます。



アプリスコアの計算は、次のコンポーネントに基づいています。

アプリスコアコンポーネント	ユーザが設定したしきい値	説明
ADC メモリ使用量	はい	Citrix ADC インスタンスの合計メモリ使用量の低しきい値と上限しきい値
サージキューの構築	はい	キューに入っており、応答を必要とするサージ要求の合計の下限および上限しきい値。
ADC の CPU 使用率	はい	Citrix ADC インスタンスの CPU 使用率の合計の下限および上限しきい値。
Response time	はい	要求パケットの送信から、仮想サーバ上で構成されたサービスからの最初の応答パケットを受信するまでの時間間隔。
アプリの CPU 使用率	はい	アプリケーションによる CPU 使用率の合計（低）および上限しきい値。
アクティブなサービス	はい	仮想サーバーにバインドされているアクティブでなければならないサービスのパーセンテージのしきい値。
不適切な永続性タイプ	いいえ	仮想サーバーでの永続性の使用率が低いかどうかを示します。
サーバーエラー (5xx)	いいえ	Web サーバが 5xx エラーで応答するかどうかを示します。
異常に大きい HTTP パケット	いいえ	HTTP ヘッダーサイズを持つ HTTP メッセージが、Citrix ADC インスタンスで構成された値を超えた場合の発生を示します。
SSL リアルタイムトラフィック	いいえ	SSL トラフィックを分析してリアルタイムトラフィックを特定し、遅延を改善するための最適な構成設定を提案します。

アプリスコアコンポーネント	ユーザが設定したしきい値	説明
SSL セッションのビルド	いいえ	一定期間にわたるセッションのビルドアップを示します。これにより、Citrix ADC インスタンスでこれらのセッションに大量のメモリが保持される可能性があります。
セッションの再利用率が低い	いいえ	Citrix ADC インスタンスによって再使用されるセッションの数が実際の数が少ないかどうかを示します。
NIC カードの彩度	いいえ	インターフェイスによって廃棄されたパケットの合計を示します。
TCP 再構成キュー制限ヒット	いいえ	TCP 接続上の順序外パケットが、設定された順序外パケットキューサイズを超えているかどうかを示します。

デフォルトでは、すべてのコンポーネントが有効です。いずれかのコンポーネントを無効にすると、Citrix ADM は選択したコンポーネントに基づいてのみ、最終的なアプリスコア計算を実行します。

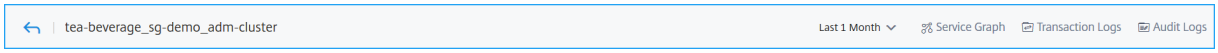
> 注
>
> [アナリティクス] > [設定] に移動して [アプリスコアの構成] をクリックして、引き続きしきい値を構成することもできます。詳しくは、「アプリケーション分析のしきい値およびアラートの作成」を参照してください。

マイクロサービスアプリケーションのアプリケーションの詳細

May 7, 2021

ダッシュボードからマイクロサービスアプリケーションをクリックして、詳細情報をドリルダウンします。

選択したアプリケーションページが表示されます。



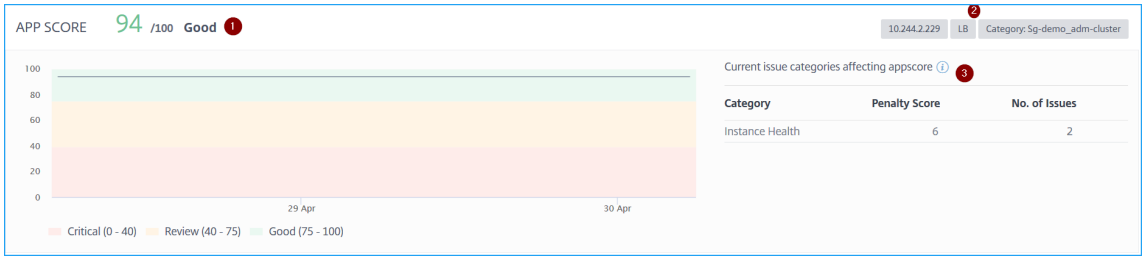
アプリケーション詳細ページから：

- リストから期間を選択して、特定の期間の詳細を表示します。
- 「サービス・グラフ」をクリックして、選択したアプリケーションのサービス・グラフを表示します。詳しくは、「アプリケーションのサービスグラフ」を参照してください。

- トランザクションログをクリックすると、選択したアプリケーションの詳細なトランザクションが表示されます。
- [監査ログ] をクリックして、監査ログの詳細情報を表示します。

期間を選択すると、次のアプリケーション詳細が表示されます。

- アプリケーションスコア — 選択した期間のアプリケーションスコア。また、現在のアプリケーションの問題も表示できます。これは、問題のカテゴリに基づいて適用可能なペナルティスコアと呼ばれます。最終的なスコアは、ペナルティ合計を差し引いた **100** として計算されます。



1 — 現在のアプリのスコアを示します。

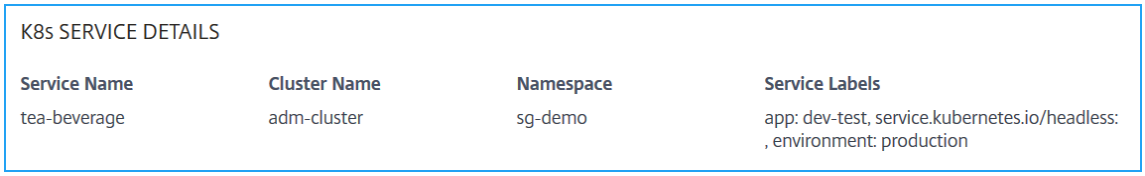
2 — CPX IP アドレス、負荷分散やコンテンツスイッチングなどのアプリケーションタイプ、サービスがホストされているサービス名前空間とクラスタ名を示します。

3 — 現在のアプリケーションスコアに影響する問題を示します

このダッシュボードでは、アプリのスコアに影響している現在の問題を表示することもできます。[懸案事項] で懸案の詳細を表示できます。

- **K8S** サービスの詳細

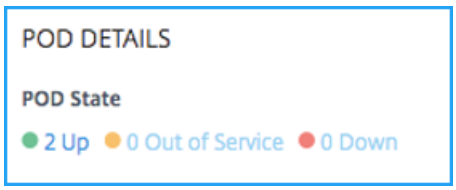
  次の詳細を表示できます。



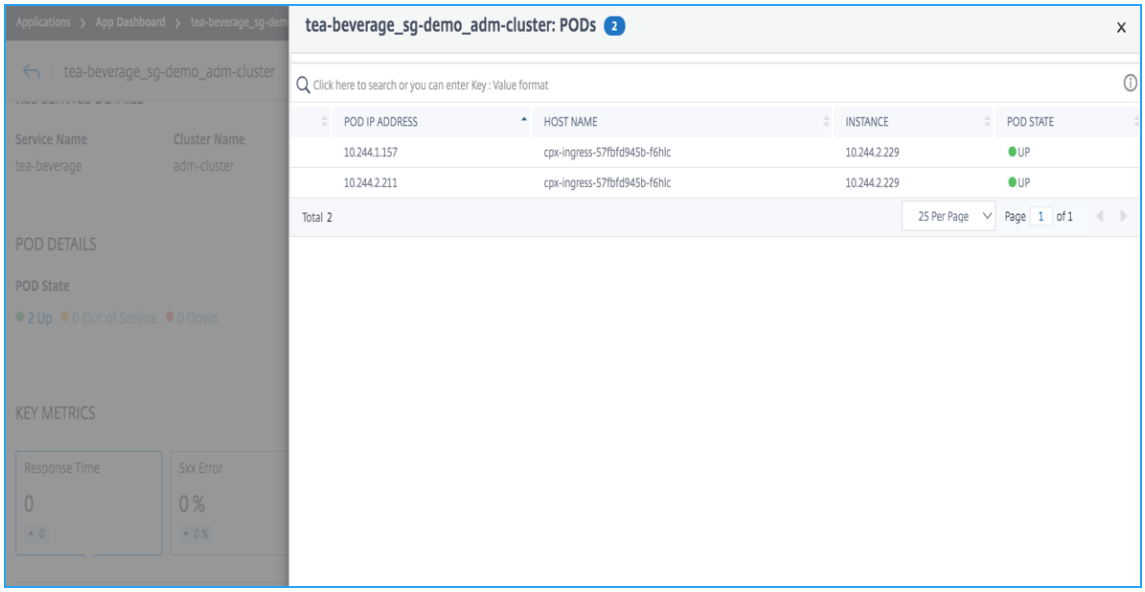
  - サービス名 — サービス名
  - クラスター名 — サービスがホストされているクラスター名
  - 名前空間 — サービスに割り当てられた名前空間
  - サービスラベル — サービスに割り当てられたサービスラベル

- ポッドの詳細

  ポッドは、Kubernetes クラスターでホストされるコンテナのグループです。Pod 内では、複数のコンテナー化されたアプリケーションをデプロイできます。各 Pod は IP アドレスに関連付けられています。



ポッドの状態をクリックして詳細を表示します

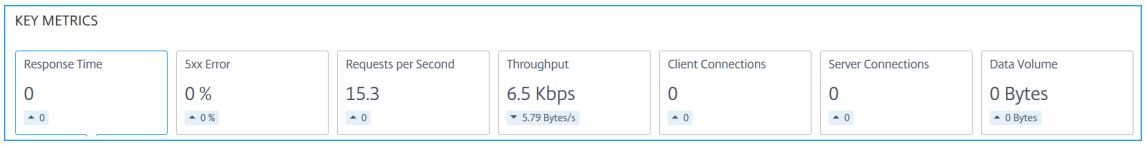


  - ポッド **IP** アドレス — ポッドの IP アドレスを表します。
  - ホスト名 — ポッドに割り当てられたホスト名を示します
  - インスタンス — Citrix ADC CPX の IP アドレスを表します
  - **POD** の状態 — Pod の現在の状態を示します

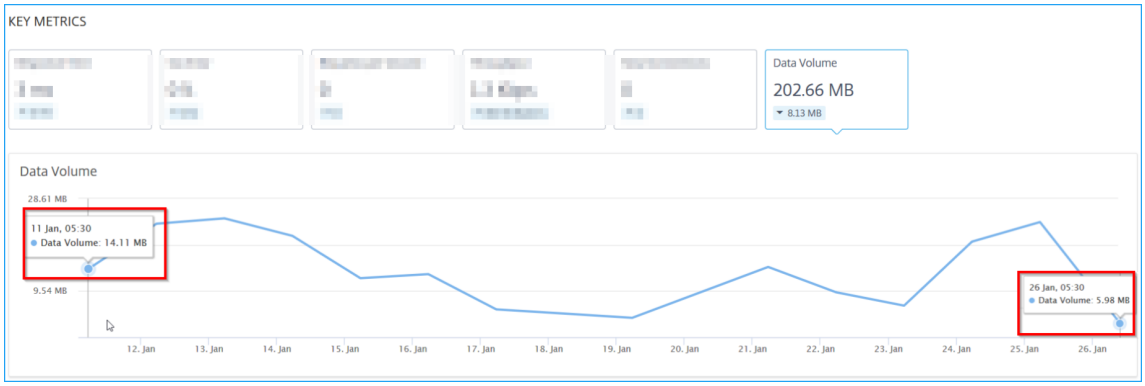
- キー・メトリック — レスポンス時間、**5xx** エラー、**1** 秒あたりのリクエスト数、スループット、クライアント接続、サーバー接続、データボリュームなどの主要なメトリックの詳細が表示されます。

  各指標で、選択した期間の平均値と差値を表示できます。差の値は、選択した期間の 最初の値から最後の値を引いた値として計算されます。

  選択した期間について、次のインスタンスメトリックスをグラフ形式で表示できます。



  次の図は、データボリュームの例で、選択した期間は 1 か月です。値 202.66 MB は、1 か月間のデータ量の合計で、値 8.13 MB は差の値です。グラフでは、最初の値は 14.11 で、最後の値は 5.98 です。差の値は 14.11 — 5.98 = 8.13 MB です。

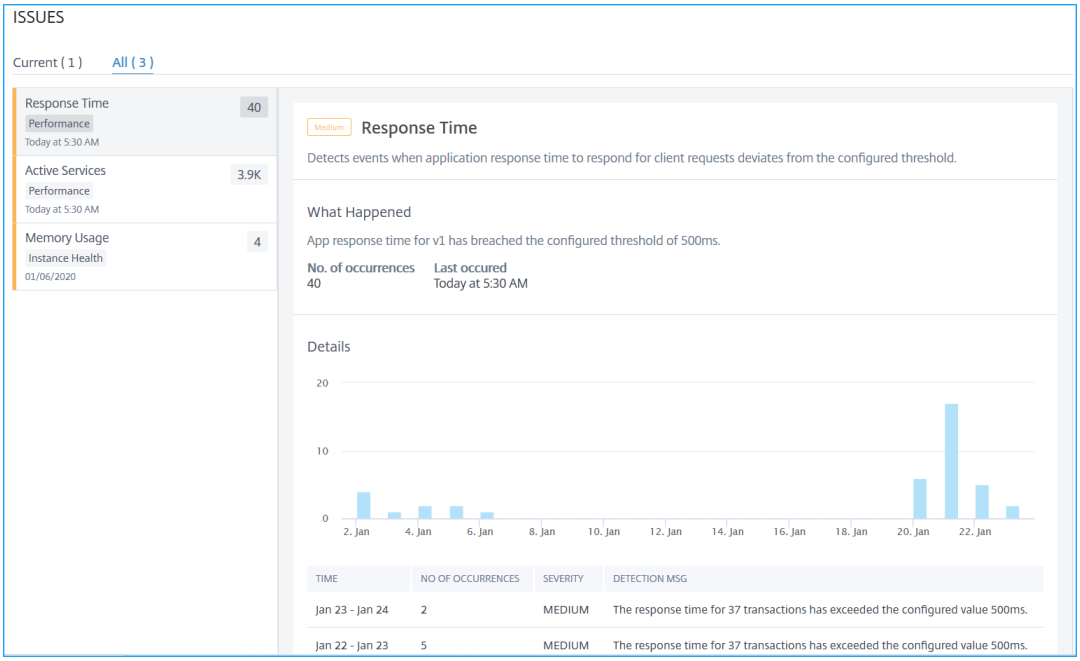


- 問題 — 選択したアプリケーションに適用可能な問題。次の問題とそのカテゴリを表示できます。

パフォーマンス	インスタンスの健全性	構成	システムリソース
応答時間	平均 CPU 使用率	高い 5xx レスポンス	不適切な永続性タイプ
セッションの再利用が低い	メモリ使用率	異常に大きい HTTP パケット	NIC カードの飽和
サージキューのビルダップ		TCP 再構成キュー制限ヒット	
SSL リアルタイムトラフィック			

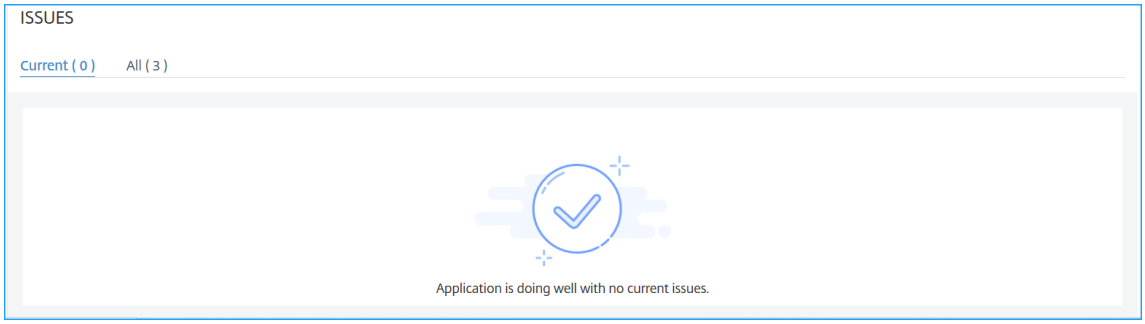
各問題をクリックすると、次の情報が表示されます。

- 総発生数
- 問題のトラブルシューティングに推奨される処置
- 時間、サービス名、発生回数の合計、重大度、検出メッセージなどの問題の詳細

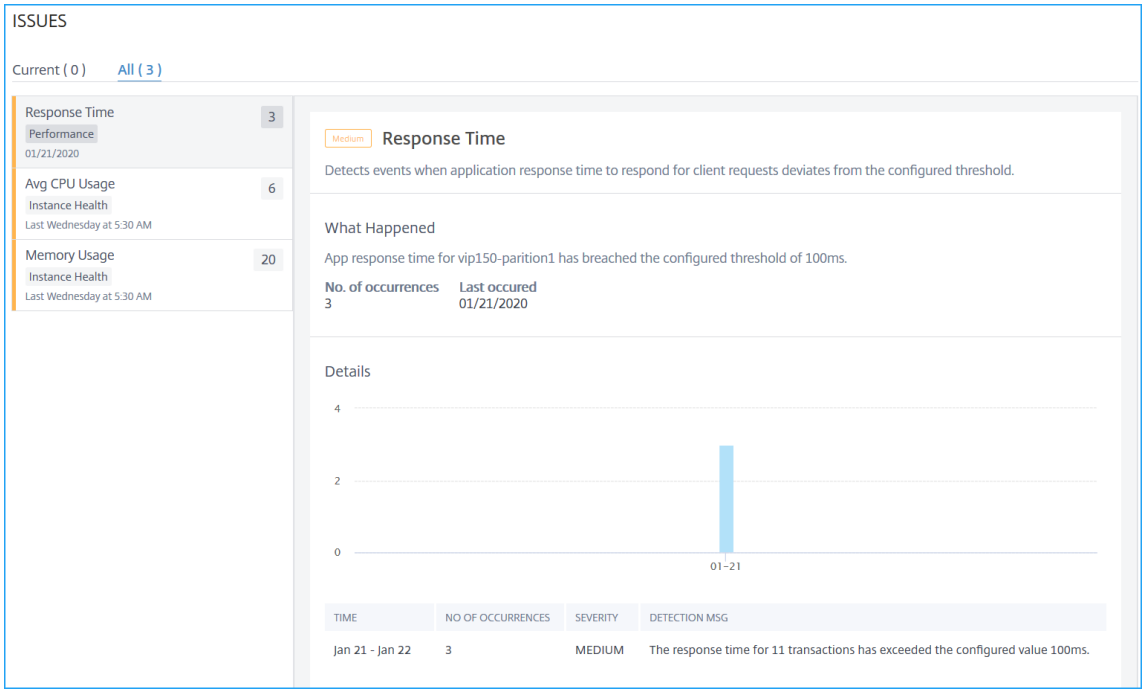


* [**Current**] タブに表示される問題は、選択した期間のアプリケーションの問題を参照します。
* [**All**] タブに表示される問題は、アプリケーションの問題の合計を示します。

次の例は、1 日間のアプリケーションの問題です。[**Current**] タブには、アプリのスコアに影響する現在の問題がないことが示されます。



[すべて] タブには、1 日の期間中に検出された問題の合計が表示されます。



Web Insight ダッシュボード

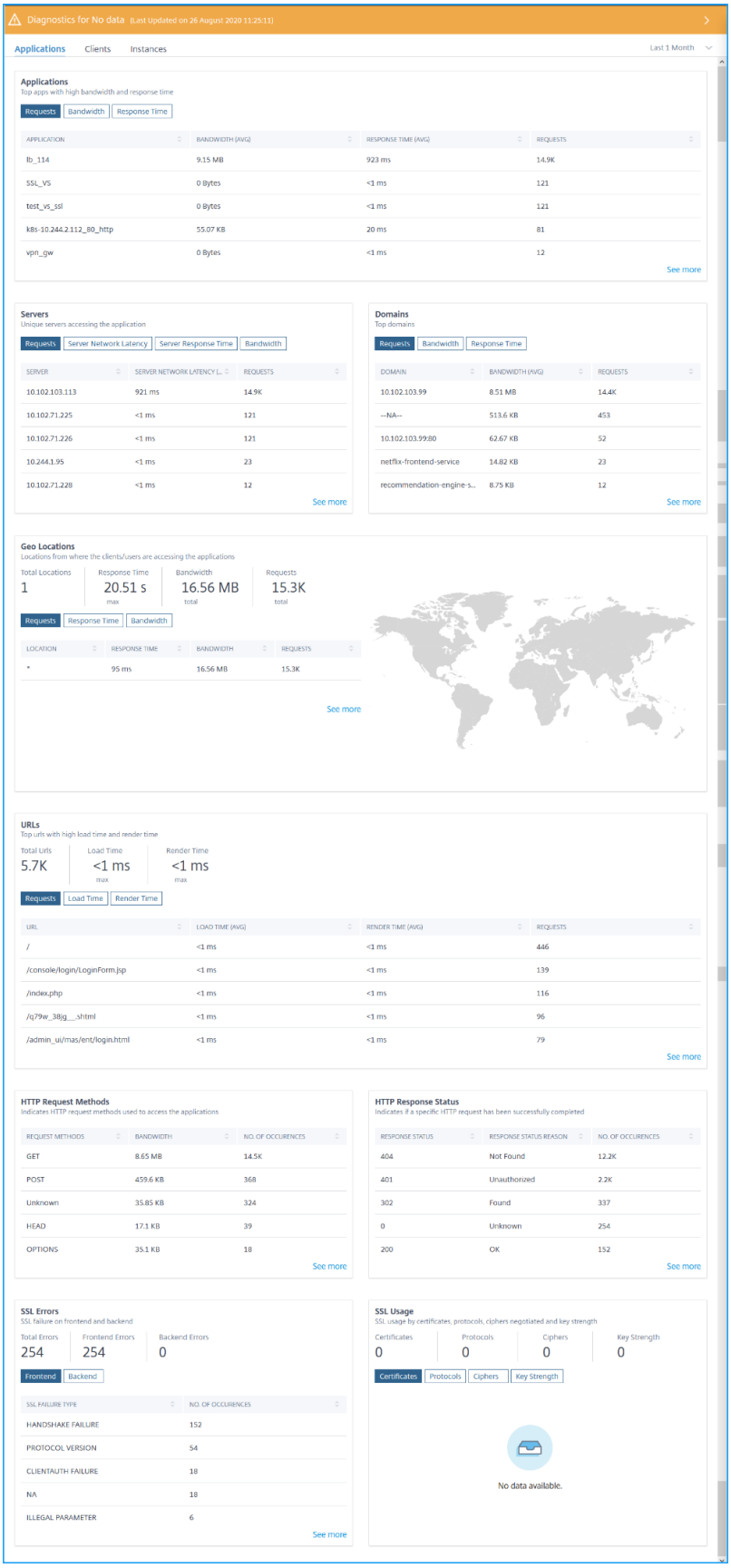
May 7, 2021

改良された Web Insight 機能が拡張され、Web アプリケーション、クライアント、Citrix ADC インスタンスの詳細なメトリックを可視化できます。この改善された Web Insight により、パフォーマンスと使用率の視点からアプリケーション全体を評価し、視覚化することができます。管理者は、次の対象 Web Insight を表示できます。

- アプリケーション。[アプリケーション**] > [**ダッシュボード] に移動し、アプリケーションをクリックし、[**Web Insight**] タブを選択して詳細なメトリックスを表示します。詳しくは、「アプリケーション使用状況の分析」を参照してください。
- すべてのアプリケーション。[アプリケーション**] > [Web Insight**] に移動し、各タブ ([アプリケーション]、[クライアント]、[インスタンス]) をクリックして、次のメトリックを表示します。

アプリケーション	クライアント	インスタンス
応答時間異常のあるアプリケーション	クライアント	インスタンス・メトリック
アプリケーション	地理的場所	アプリケーション
サーバー	HTTP 要求メソッド	ドメイン
ドメイン	HTTP 応答の状態	URL

アプリケーション	クライアント	インスタンス
地理的場所	URL	HTTP 要求メソッド
URL	オペレーティングシステム	HTTP 応答の状態
HTTP 要求メソッド	Web ブラウザー	クライアント
HTTP 応答の状態	SSL エラー	サーバー
SSL エラー	SSL 使用法	オペレーティングシステム
SSL 使用法		Web ブラウザー

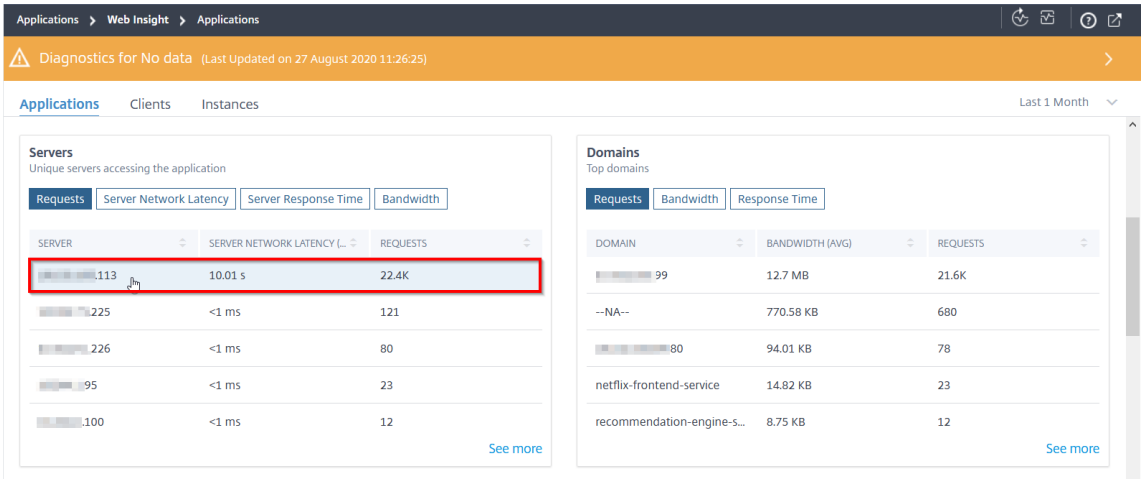


各指標で、上位 5 つの結果を表示できます。をクリックしてさらにドリルダウンして、問題を分析し、トラブルシューティングアクションを迅速に行うことができます。

> 注
>
> シナリオによっては、Citrix ADC が一部のトランザクションの RTT 値を計算できない場合があります。このようなトランザクションの場合、Citrix ADC はゼロとして値を Citrix ADM に送信し、Citrix ADM は RTT を 1 ミリ秒未満と表示します。

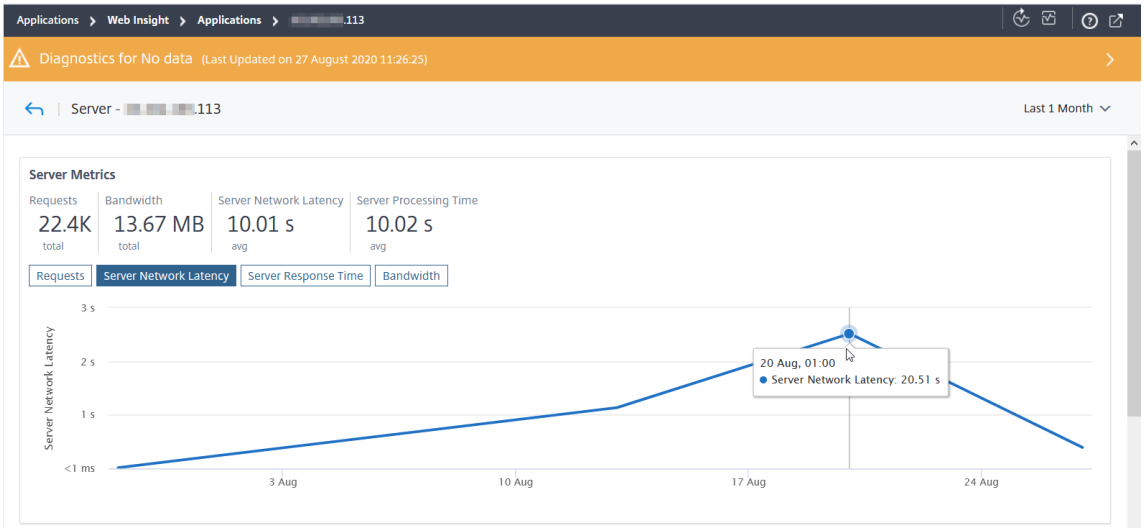
たとえば、1 か月間のサーバーネットワーク遅延を分析し、運用環境をスケールアップするかスケールダウンするかを決定するとします。これを分析するには:

1. リストから [過去 1 ヶ月] を選択し、[アプリケーション] タブから [サーバー] まで下にスクロールし、サーバーをクリックします。



選択したサーバーのメトリックの詳細が表示されます。

2. [サーバーネットワーク遅延] タブを選択して、遅延を分析します。



平均レイテンシーは 10.01 を示し、グラフから、過去 1 か月のサーバーネットワークレイテンシーが高いと思

われることを分析できます。管理者は、本番環境のスケールアップを決定できます。

Web Insight のユースケースの詳細については、「Web Insight」を参照してください。

アプリケーションの遅さの根本原因の分析

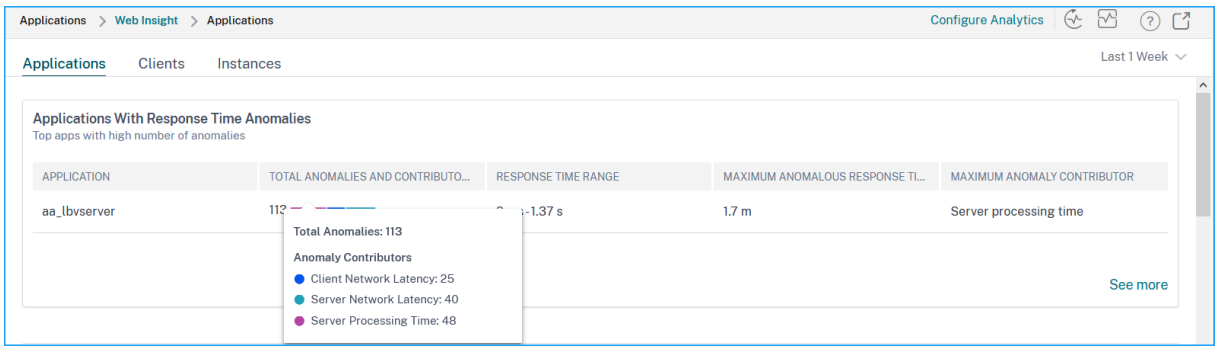
May 7, 2021

アプリケーションの遅さは、ビジネスへの影響や生産性につながるため、あらゆる組織にとって大きな懸念事項です。管理者は、ビジネスへの影響を避けるために、すべてのアプリケーションが最適に動作するようにする必要があります。ユーザーがアプリケーションへのアクセスが遅くなる場合は、次の問題があるかどうかを確認する必要があります。

- クライアントネットワークの遅延
- サーバーネットワークの待ち時間
- サーバー処理時間

Citrix ADM は、特定の前提条件に基づいて、1 時間ごとに異常チェックを実行し、過去 1 時間のトラフィックの異常を報告します。たとえば、偽陽性の結果を避けるために、応答時間が 1 ミリ秒未満の場合、これらの結果の異常チェックはスキップされます。

[アプリケーション**] > [Web Insight**] ページでは、選択した期間における応答時間の異常があるアプリケーションを表示できます。「応答時間異常のあるアプリケーション」メトリックには、異常合計に基づいて上位 5 つのアプリケーションが表示されます。[詳細を表示] をクリックして、すべてのアプリケーションを表示します。

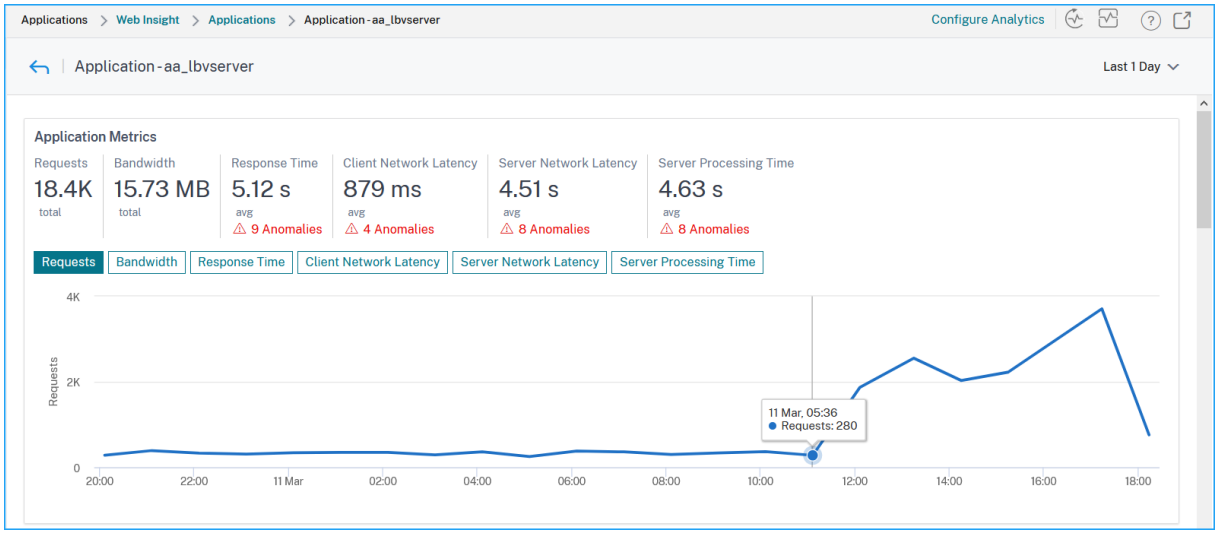


- 「アプリケーション」-アプリケーション名を示します。
- [異常値の合計**]** と **[**コントリビュータ数] — アプリケーションからの異常の総数を示します。マウスポインターを合わせると、クライアントネットワーク遅延、サーバーネットワーク遅延、およびサーバー処理時間の合計異常を表示できます。
- [**Response Time Range**]: アプリケーションからの予測応答時間の範囲を示します。
- **[** 最大異常応答時間]: アプリケーションからの応答時間が最大であることを示します。

- **[Maximum Anomaly Contributor]** — アプリケーションの異常の最大数が、クライアントネットワーク遅延、サーバーネットワーク遅延、またはサーバー処理時間からのものかどうかを示します。

アプリケーションのドリルダウン

アプリケーションをクリックして、選択した期間の「アプリケーション・メトリック」の詳細を表示します。



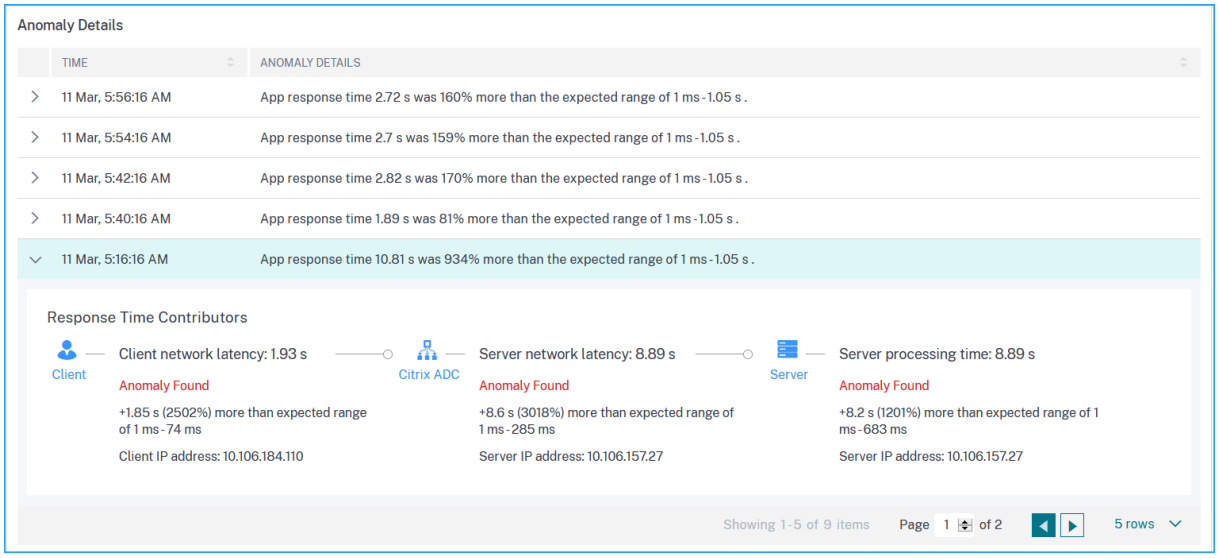
アプリケーション・メトリックを使用すると、次の項目を表示できます。

- **Requests** — アプリケーションによって受信されたリクエストの合計数
- 帯域幅：アプリケーションによって処理される合計帯域幅
- 応答時間：アプリケーションからの平均応答時間
- クライアントネットワーク遅延 — クライアントネットワーク待ち時間の平均（クライアントから ADC まで）
- サーバーネットワーク遅延 — 平均サーバーネットワーク遅延 (ADC からサーバーへ)
- サーバ処理時間：サーバの平均処理時間（サーバから ADC まで）

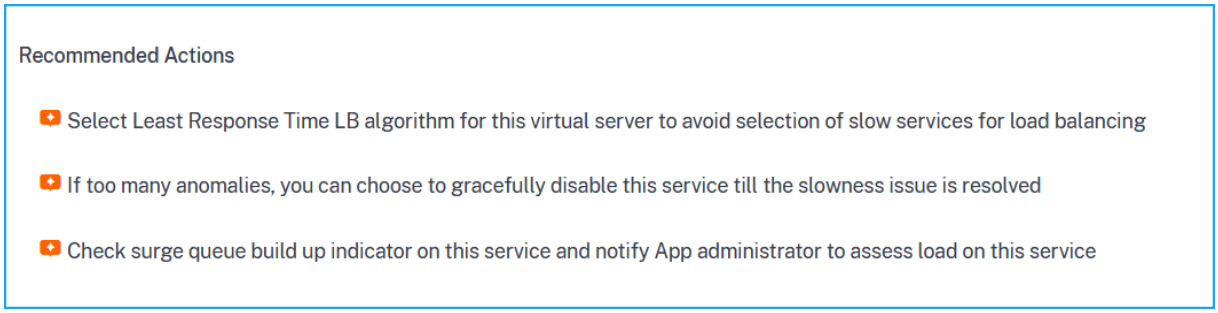
アプリケーションに異常がある場合は、異常がクライアントネットワーク遅延、サーバーネットワーク遅延、またはサーバー処理時間のどちらから発生しているかを確認できます。各タブをクリックして詳細を表示します。

応答時間

[異常の詳細] で、をクリックして、応答時間のコントリビュータの詳細を表示します (クライアントからサーバーへ)。次の例では、クライアントネットワーク遅延、サーバーネットワーク遅延、およびサーバー処理時間の異常があります。また、期待される範囲および期待範囲を超えて発生した違反も表示できます。



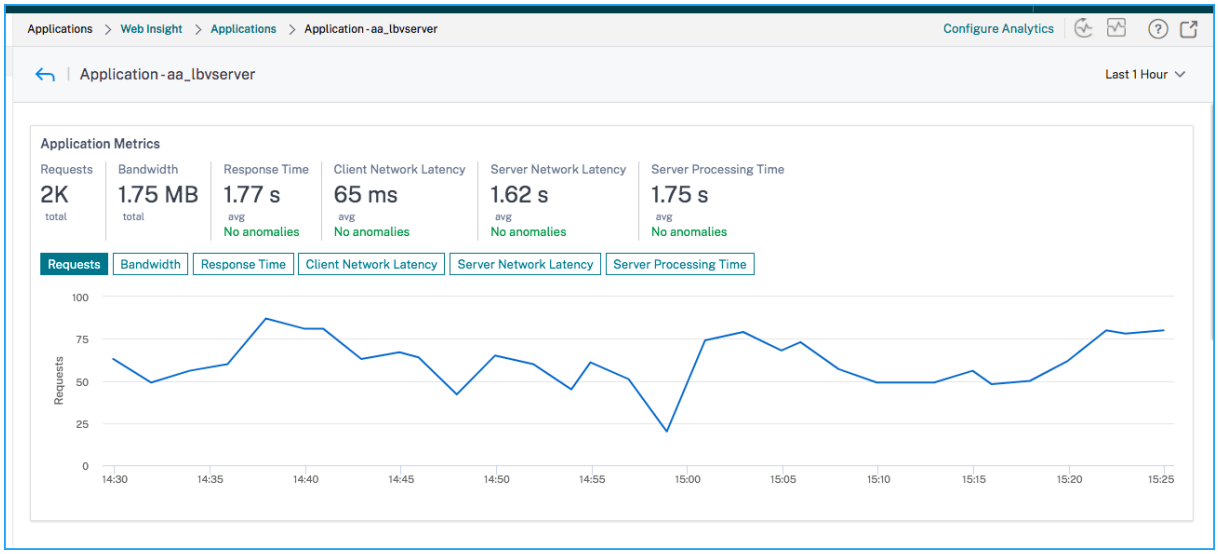
推奨アクションは、異常の解決方法を示します。



同様に、[クライアントネットワーク遅延]、[サーバーネットワーク遅延]、[サーバー処理時間] タブをクリックして、次の項目を表示できます。

- 期待範囲に違反した異常。
- 可能な解決策を示唆する推奨アクション。

アプリケーションのパフォーマンスが良好であれば、アプリケーションメトリックを異常なしとして表示できます。



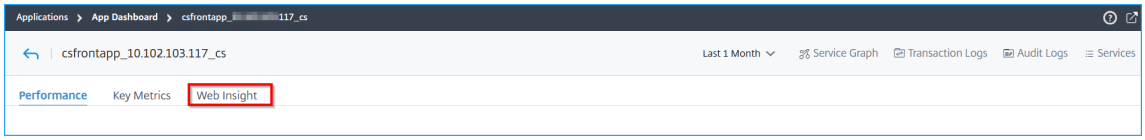
アプリケーション使用状況の分析

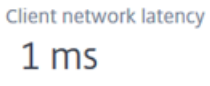
May 7, 2021

アプリケーション所有者は、パフォーマンスと使用の観点からアプリケーション全体を評価し、視覚化する能力を持っている必要があります。

即興の **App Dashboard** では、すべてのアプリケーションのパフォーマンスと使用状況指標をまとめて表示できます。既存のアプリケーション・パフォーマンス・メトリックとは別に、アプリケーションをクリックすると、「**Web Insight**」タブにメトリックの詳細が表示され、次のことができます。

- アプリケーションの使用状況を理解します。
- パフォーマンスの偏差と使用状況の指標を関連付けます。

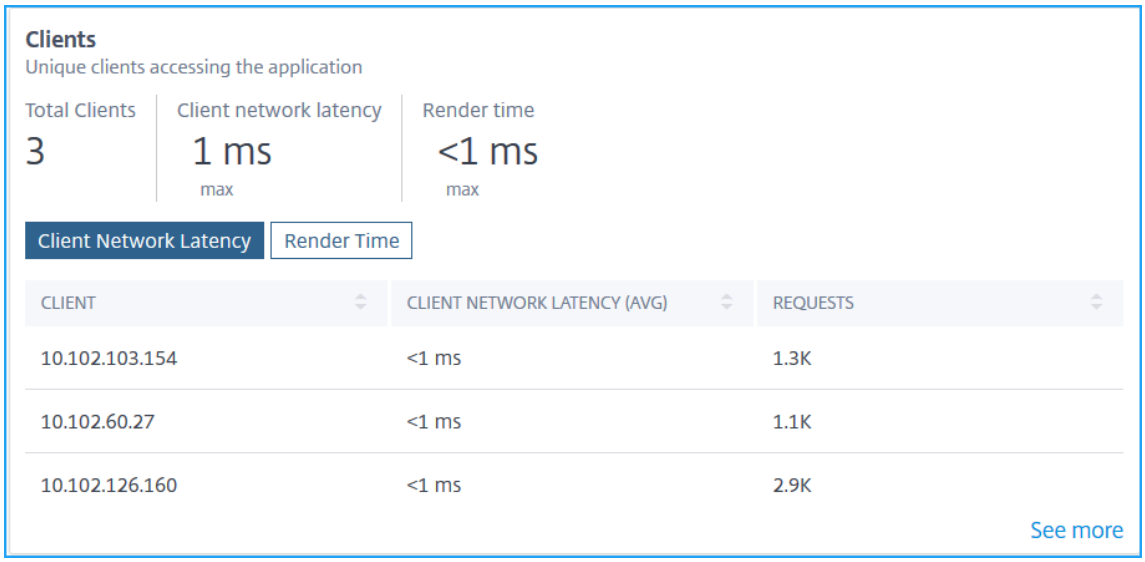


> 注
>
> 各メトリックについて、最大値と合計値を示すオプションを表示できます。次に例を示します:
>
> - 
>
> ：選択した期間における最大クライアントネットワーク待ち時間。クライアント 1 = 30 ミリ秒、クライアント 2 = 15 ミリ秒、クライアント 3 = 3 ミリ秒のネットワーク遅延があるとします。このシナリオでは、クライアントネットワーク遅延は 30 ミリ秒と表示されます。

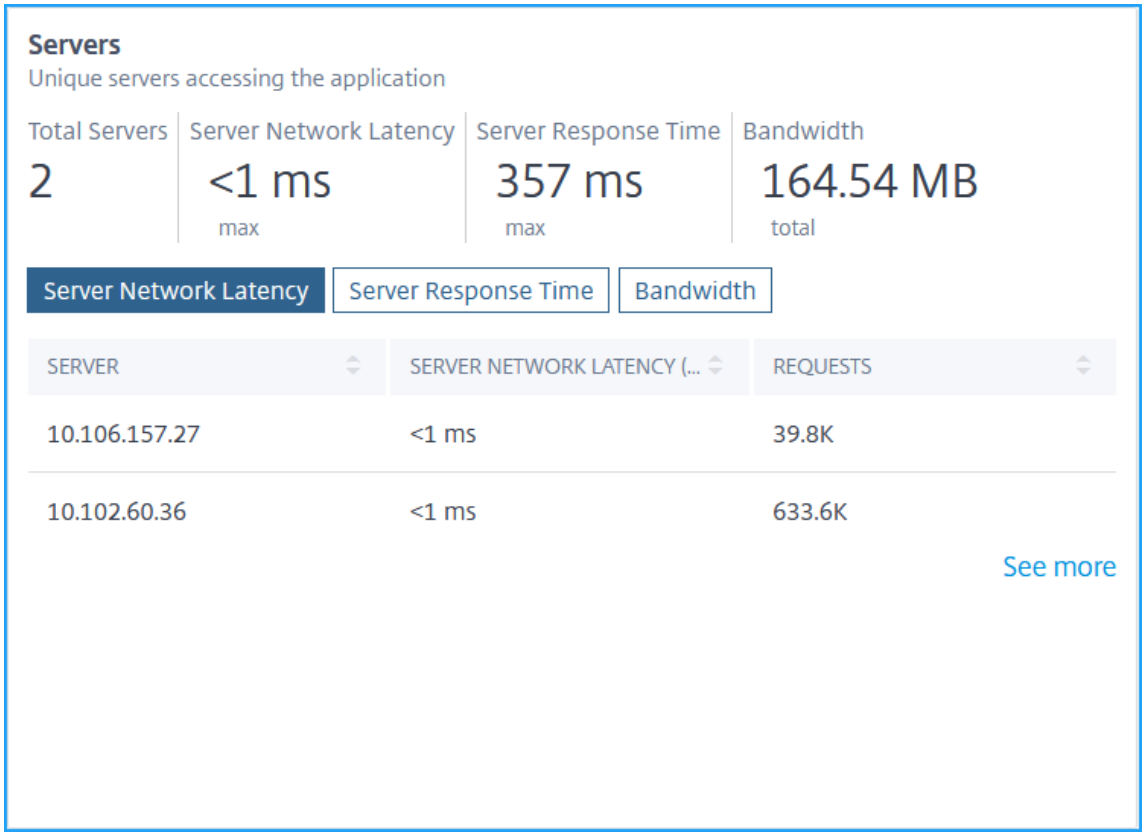
> Bandwidth
> 164.54 MB
> - total ：選択した期間において、使用可能なすべてのクライアント/サーバで消費された合計帯域幅。クライアント 1 = 30 MB、クライアント 2 = 45 MB、クライアント 3 = 40 MB の帯域幅消費があるとします。このシナリオでは、帯域幅が表示されます (30 MB + 45 MB + 40 MB) = 115 MB。

[使用状況] タブに表示できる Web Insight メトリックスを次に示します。

- 「クライアント」— アプリケーションにアクセスするクライアントのインサイトを表示します。

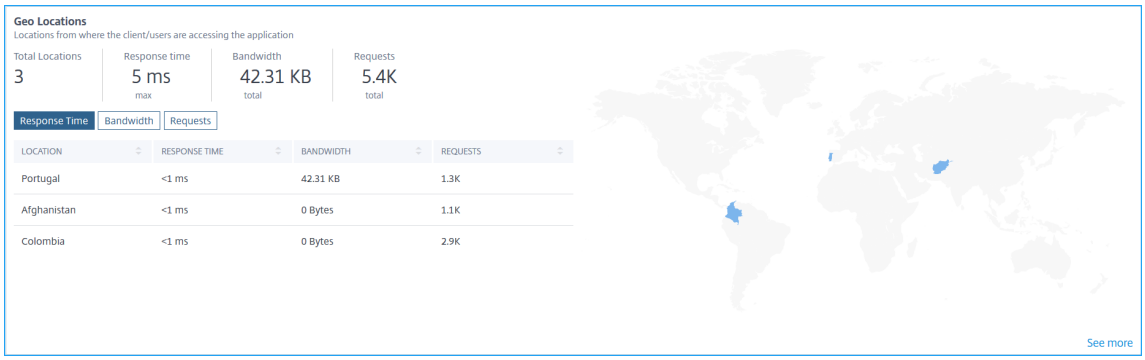


  - 「合計クライアント」— アプリケーションにアクセスしているクライアントの合計が表示されます。
  - [クライアントネットワーク遅延]： クライアントから Citrix ADC へのネットワーク遅延を表示します。[クライアントネットワーク遅延] タブをクリックして、次の項目を表示します。
    * クライアント： クライアントの IP アドレス。
    * クライアントネットワーク遅延 **(**平均**)** — クライアントからの平均ネットワーク遅延です。
    * [**Requests**] — クライアントからのリクエストの合計です。
  - 「レンダリング時間」(Render Time) — サーバーの応答をレンダリングするのにかかった時間を表示します。[レンダリング時間] タブをクリックして、次の項目を表示します。
    * クライアント： クライアントの IP アドレス。
    * **[** レンダリング時間 **(**平均**)**] — クライアントからの平均レンダリング時間。
    * [**Requests**] — クライアントからのリクエストの合計です。
- サーバー — アプリケーションにアクセスするサーバーのインサイトを表示します。



- [**Total Servers**]: アプリケーションにアクセスしているサーバの合計が表示されます。
- 「サーバーのネットワーク遅延」— サーバーから Citrix ADC へのネットワーク遅延を表示します。[サーバーネットワーク遅延] タブをクリックして、次の項目を表示します。
  - サーバー — サーバーの IP アドレス。
  - サーバーネットワーク遅延 **(**平均**)** — サーバーからの平均ネットワーク遅延です。
  - [要求] — サーバーからのリクエストの合計です。
- 「サーバー応答時間」— サーバーが要求に応答するのに要した時間を表示します。[サーバ応答時間] タブをクリックして、次の項目を表示します。
  - サーバー — サーバーの IP アドレス。
  - 応答時間（平均）: サーバからの平均応答時間。
  - [要求] — サーバーからのリクエストの合計です。
- [**Bandwidth**]: サーバによって消費された合計帯域幅を表示します。[帯域幅] タブをクリックして、次の項目を表示します。
  - サーバー — サーバーの IP アドレス。
  - 帯域幅: サーバから消費された合計帯域幅。
  - [要求] — サーバーからのリクエストの合計です。

- 地理的場所 — 特定の場所からアプリケーションにアクセスするクライアントのインサイトを表示します。

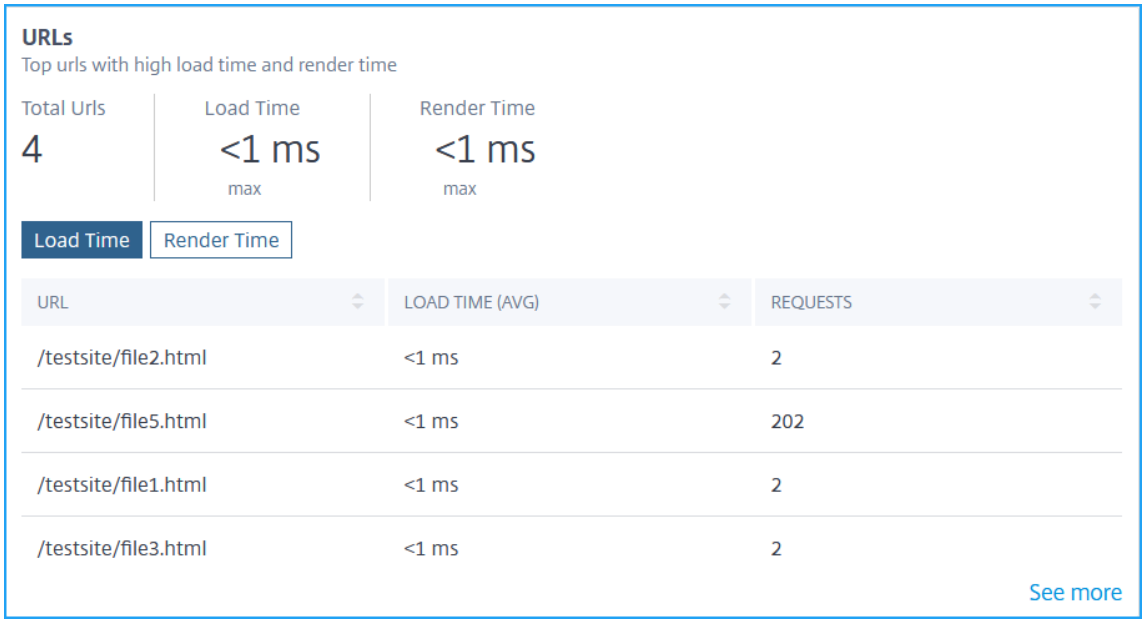


  - 合計ロケーション— アプリケーションにアクセスするクライアントのロケーションの合計が表示されます。
  - [応答時間]：クライアントの場所からの応答時間を表示します。
  - **Band width**：すべてのロケーションでクライアントが消費した合計帯域幅を表示します。
  - [**Requests**]：すべてのクライアントロケーションからの要求の合計を表示します。

    各タブをクリックすると、次の項目が表示されます。

    * 「場所」— 場所の名前。
    * [応答時間]：クライアントの場所からの平均応答時間。
    * **Bandwidth**： クライアントのロケーションから消費される帯域幅。
    * [**Requests**] — クライアントロケーションからのリクエストの合計です。

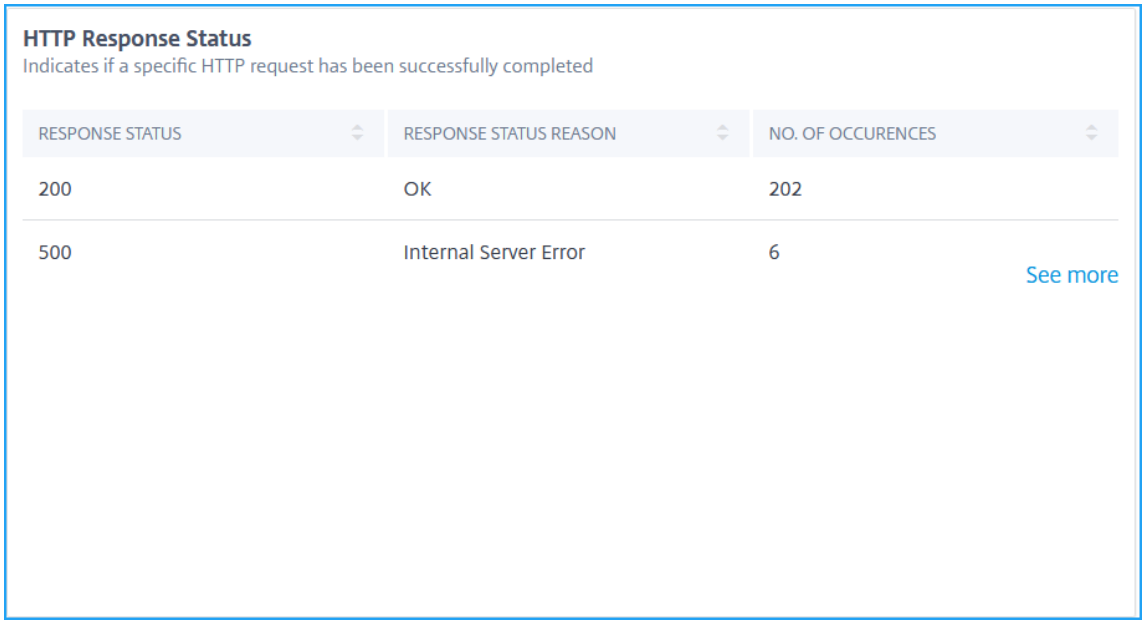
- 「**URL** 」— 負荷とレンダリング時間が長い URL のインサイトを表示します。



  - 「合計 **URL** 」— 合計 URL を表示します。

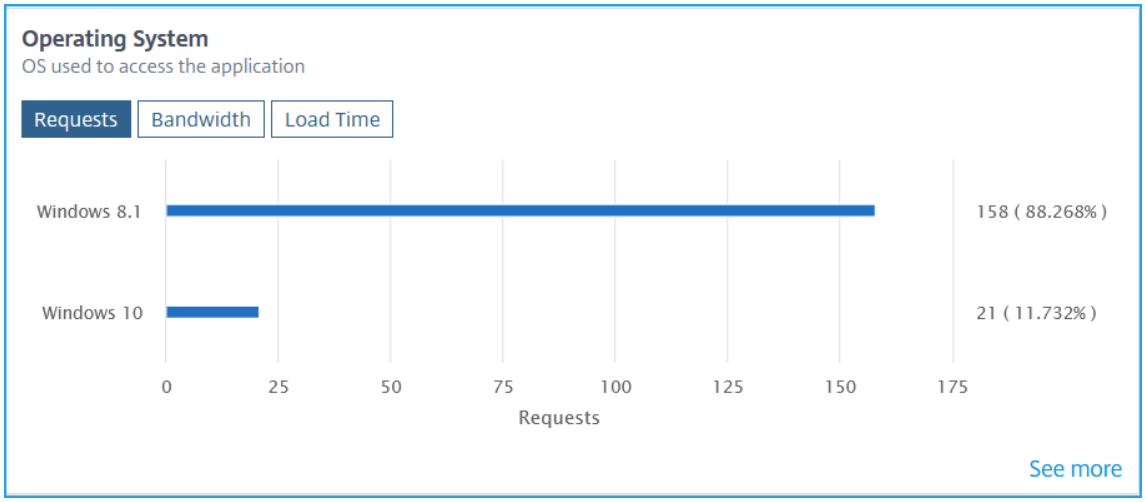
- 「読み込み時間」— URL のロードにかかった時間が表示されます。[ロード時間] タブをクリックして、次の項目を表示します。
  - 「**URL** 」— URL 名。
  - 読み込み時間 **(**平均**)** — URL の読み込みにかかった平均時間。
  - リクエスト — URL からのリクエストの合計です。
- 「レンダリング時間」(Render Time)-URL のレンダリングおよび表示にかかった時間を表示します。[レンダリング時間] タブをクリックして、次の項目を表示します。
  - 「**URL** 」— URL 名。
  - レンダリング時間 **(**平均**)** — URL のレンダリングにかかった平均時間。
  - リクエスト — URL からのリクエストの合計です。

- 「**HTTP** 応答ステータス」— 完了した HTTP リクエストのインサイトを表示します。



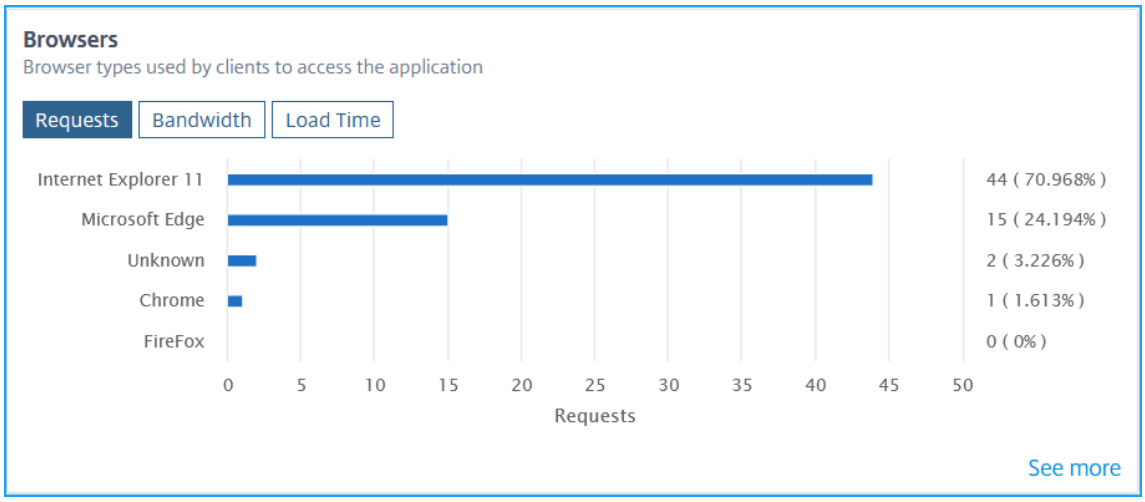
- [応答ステータス]: 2xx、4xx、5xx などの応答コードを表示します。
- 「応答ステータスの理由」— 内部サーバーエラー、見つからないなどの応答理由を表示します。
- 「オカレンスの数」-オカレンスの合計数を表示します。

- オペレーティングシステム — アプリケーションにアクセスする OS のインサイトを表示します。



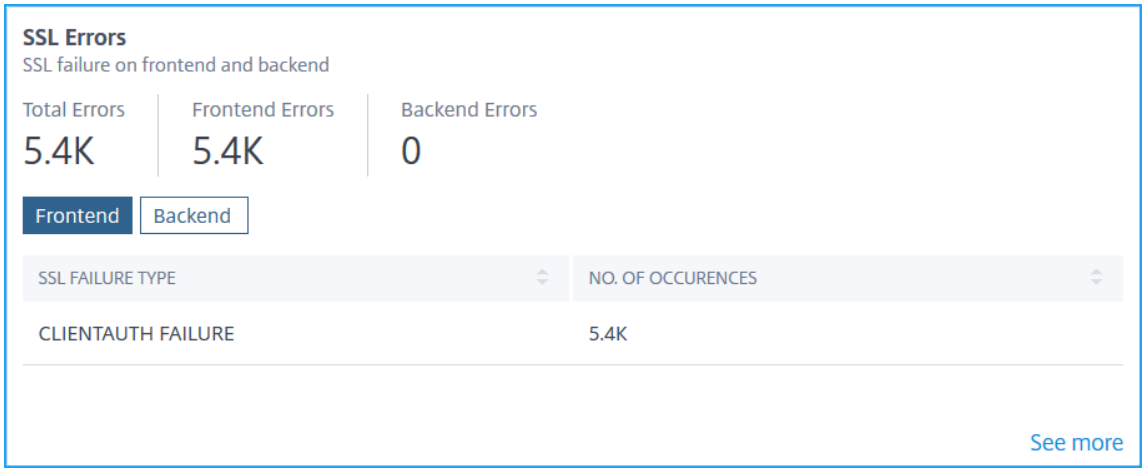
- 「**Requests** 」— 各オペレーティングシステムからのリクエストの合計を表示します。
- [**Bandwidth**]: 各オペレーティングシステムによって消費された合計帯域幅を表示します。
- 「ロード時間」— 各オペレーティングシステムからサーバーからロードされた合計時間が表示されます。

- 「ブラウザ」— アプリケーションにアクセスするためにクライアントが使用するブラウザーの種類に関するインサイトが表示されます。



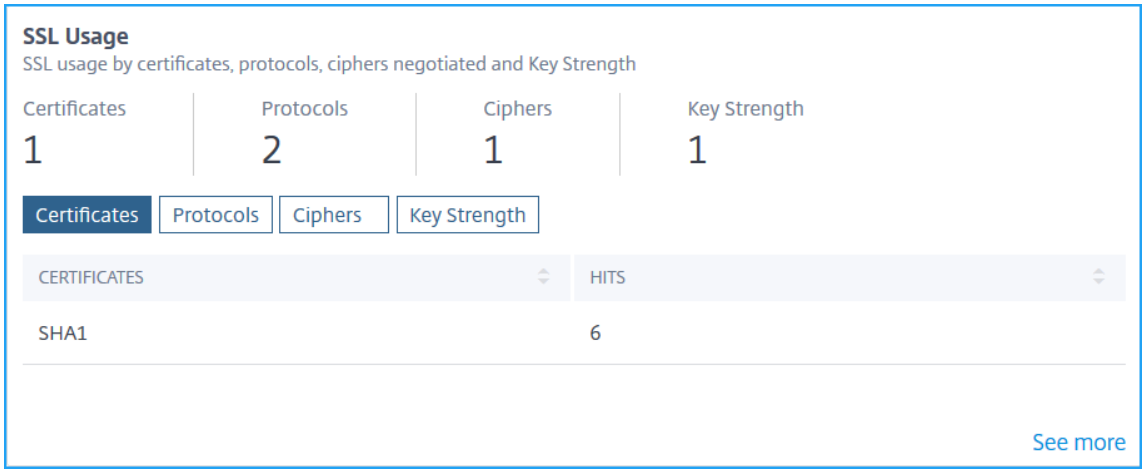
- 「要求」— 各ブラウザからのリクエストの合計を表示します。
- [**Bandwidth**]: 各ブラウザによって消費された合計帯域幅が表示されます。
- 「読み込み時間」— ブラウザーがサーバーからロードされるまでに要した合計時間を表示します。

- [**SSL** エラー] — フロントエンドサーバーとバックエンドサーバーからの SSL エラーに関するインサイトを表示します。



- 「エラーの合計」— SSL エラー発生の合計を表示します。
- 「フロントエンド」— フロントエンドサーバーからの SSL エラーの合計を表示します。[フロントエンド] タブをクリックして、SSL エラータイプと合計発生回数を表示します。
- バックエンド：バックエンドサーバからの SSL エラーの合計を表示します。[バックエンド] タブをクリックして、SSL エラータイプと発生の合計を表示します。

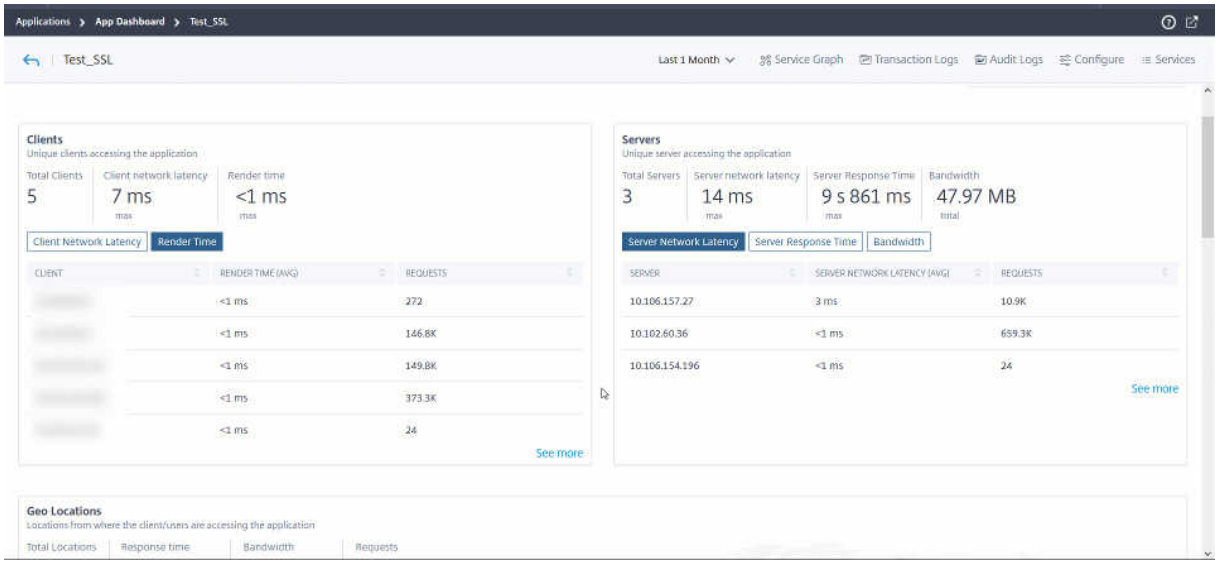
- [**SSL** 使用状況] — SSL 証明書、プロトコル、暗号、キー強度などの SSL 使用状況に関するインサイトを表示します。



- 「証明書」— SSL 証明書の合計を表示します。[**Certificates**] タブをクリックして、証明書の名前と合計ヒット数を表示します。
- [**Protocols**]: SSL プロトコルの合計を表示します。[**Protocols**] タブをクリックして、SSL/TSL プロトコルと合計ヒット数の詳細を表示します。
- 「暗号」-暗号の合計を表示します。[**Ciphers**] タブをクリックして、各暗号スイート名と合計ヒット数の詳細を表示します。
- 「キー強度」— SSL 証明書で使用されるキーの強度の合計を表示します。[キー強度] タブをクリックして、各キー強度とヒット数の合計の詳細を表示します。

メトリックスの詳細をグラフ形式で表示

各指標について、[詳細を表示] オプションをクリックすると、詳細をグラフィカル形式で表示できます。詳細をグラフィカル形式で表示するには、[**>**] をクリックします。



[詳細を表示] オプションをクリックした後、各メトリックについて表示できる詳細を次に示します。

インサイト名	メトリック	説明
クライアント	クライアント	クライアントリストを示します
	レンダリング時間 (平均)	クライアントがサーバの応答をレンダリングするのにかかった平均時間を示します
	クライアントネットワーク遅延 (AVG)	クライアントから Citrix ADC インスタンスまでの平均ネットワーク遅延を示します。
	要求	クライアントからのリクエストの合計を示します。
サーバー	サーバー	サーバーリストを示します
	サーバー処理時間 (平均)	サーバーが要求を処理するのに要した平均時間を示します
	サーバーネットワーク遅延 (AVG)	サーバーから Citrix ADC インスタンスまでの平均ネットワーク待機時間を示します
	ヒット数	サーバーが受信した総ヒット数を示します
地理的場所	場所	クライアントの場所を示します
	応答時間	クライアントの場所からの合計応答時間を示します
	帯域幅	ロケーションから消費された合計帯域幅を示します。
	要求	ロケーションからのリクエストの合計を示します
URL	レンダリング時間 (平均)	サーバーからページをロードするのに要した平均時間を示します
	ロード時間 (平均)	URL のレンダリングと表示に要した平均時間を示します
	ヒット数	URL からの総ヒット数を示します
HTTP 応答の状態	Name	「OK」、「見つかりません」、「内部サーバーエラー」 などの応答ステータス名を表します。
	応答の状態	サーバから受信した応答ステータスコード（200、400、500 など）を示します。

	ヒット数	レスポンスコードからの総ヒット数を示します。
	帯域幅	消費された総帯域幅を示します
オペレーティングシステム	オペレーティングシステム	Windows、MAC などのオペレーティングシステム名を示します。
	ロード時間	オペレーティングシステムがサーバーからロードされるまでに要した合計時間を示します
	帯域幅	オペレーティングシステムによって消費された合計帯域幅を示します。
	要求	オペレーティングシステムからのリクエストの合計を示します
Web ブラウザー	Web ブラウザー	Mozilla Firefox や Chrome などのブラウザ名を表します
	ロード時間	ブラウザがサーバーからロードするのに要した合計時間を示します。
	帯域幅	ブラウザによって消費された総帯域幅を示します
	要求	ブラウザからのリクエストの合計を示します
SSL エラー	SSL 障害タイプ	CLIENTAUTH FAILURE などのエラー名を示します
	オカレンス	SSL エラーの総発生回数を示します。
SSL 使用法	プロトコル名とバージョン (TLS、SSL など) を示します
	ヒット	プロトコルからの総ヒット数を示します

Web インサイトのユースケースの詳細については、「Web Insight」を参照してください。

アプリダッシュボードのトラブルシューティング

May 7, 2021

アプリケーションダッシュボードにアプリケーションを追加すると、ダッシュボードにアプリケーションの基本構成の詳細がすぐに表示されます。アプリスコア、主要指標、問題などのアプリケーション分析の詳細が、数分 (約 10 ～ 15 分) 以内に読み込まれます。詳しくは、「アプリケーション」を参照してください。

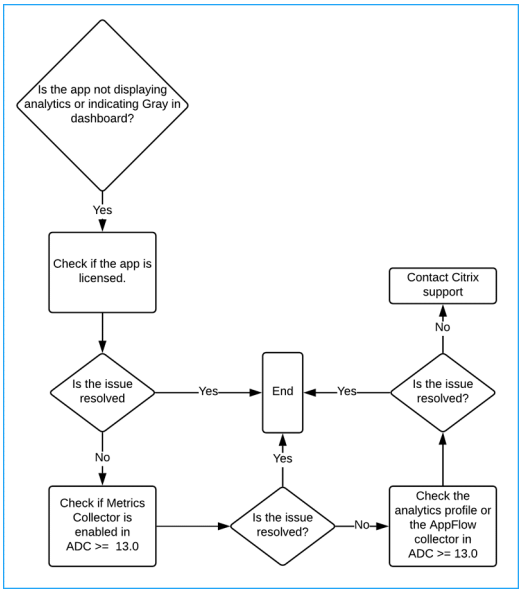
Citrix ADC インスタンスからのメトリックスデータフロー（AppFlow コレクターまたはアナリティクスプロファイル）に問題がないことを確認する必要があります。AppFlow コレクタと分析プロファイルの詳細については、このドキュメントを参照してください。

このドキュメントでは、次の場合に実行する必要があるトラブルシューティング手順について説明します。

- アプリケーションをクリックすると、指定した期間 (10 ～15 分) の後でも、選択したアプリケーションの分析に必要なデータが表示されません。
- CS または LB アプリケーションは、アプリケーションダッシュボードで常に灰色（適用不可ステータス）を示します。

> 注
>
> この文書に記載されているトラブルシューティング手順は、コンテンツスイッチングおよび負荷分散仮想サーバにのみ適用されます。

トラブルシューティングのシナリオ



アプリケーションはライセンス供与されています

アプリケーションがライセンスされているかどうかを確認する必要があります。

- **ADM** サービス - **[**アカウント**] > [**サブスクリプション**]** に移動し、[仮想サーバーライセンスの概要**]** でアプリケーションがライセンスされているかどうかを確認します。アプリケーションにライセンスが付与されていない場合は、仮想サーバーでのライセンスの管理および分析の有効化 を参照して仮想サーバのライセンスを取得してください。
- **ADM** オンプレム — **[**システム**] > [**ライセンス **&** 分析] に移動し、[仮想サーバーライセンスの概要**]** でアプリケーションがライセンスされているかどうかを確認します。アプリケーションにライセンスが付与されていない場合は、仮想サーバーでのライセンスの管理および分析の有効化 を参照して仮想サーバのライセンスを取得してください。

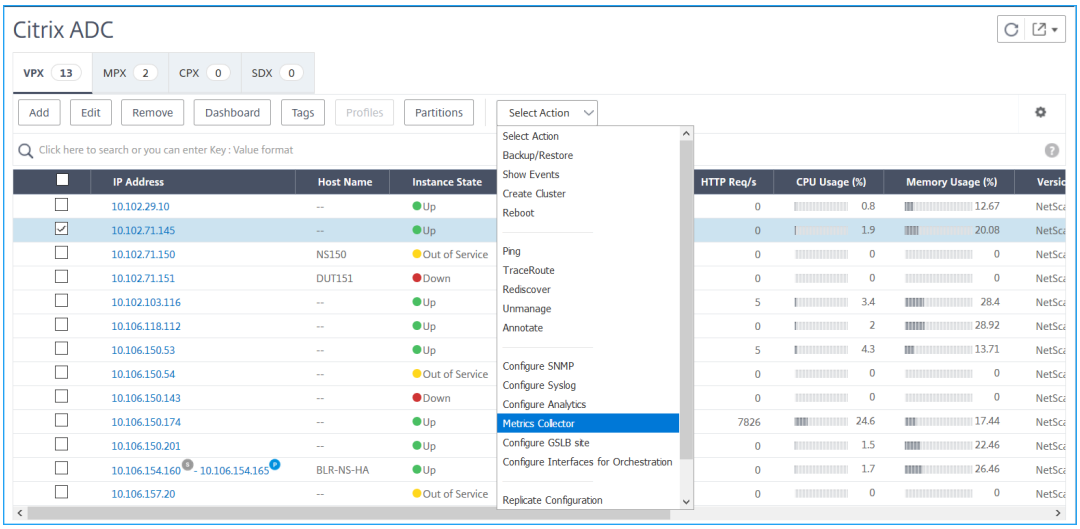
メトリックスコレクタが有効です

Citrix ADC インスタンスでメトリックスコレクタが有効になっているかどうかを確認する必要があります。

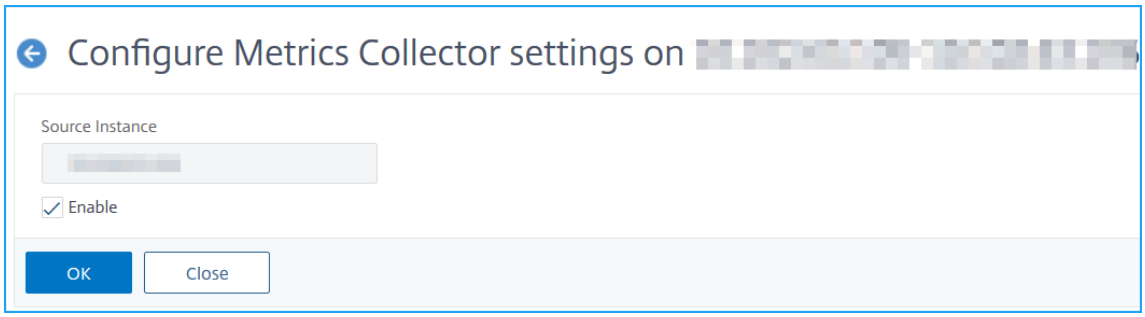
Citrix ADC バージョン 13.0 以降では、ADC インスタンスが ADM に正常に追加されると、メトリックコレクターがデフォルトで有効になります。メトリック・コレクタが有効になっているかどうかを確認するには、次の手順に従います。

1. [ネットワーク**] > [**インスタンス**]** に移動します。[インスタンス] で、インスタンスの種類（Citrix ADC VPX など）を選択します。
2. Citrix ADC インスタンスを選択します。

a)「アクションの選択」リストから、「メトリック・コレクター」を選択します。



3.「メトリック・コレクタ設定の構成」ページで、「有効」オプションが選択されていることを確認します。そうでない場合は、「有効」オプションを選択し、「**OK**」をクリックします。



メトリック・コレクタを有効にした後でデータを表示できない場合は、次のことを検証します。

- Citrix ADC インスタンスバージョン 13.0 **47.x** よりも前のビルドのAppFlow コレクタ。
- Citrix ADC インスタンスビルド **47.x** 以降の分析プロファイル。

Citrix ADC インスタンスの以前のビルド

Citrix ADC の場合:

1. 次のコマンドを実行して、コレクタが起動し、ポート 5563 で実行されていることを確認します。

```
sh appflow collector af_collector_rest_<adm_receiver_ip>
```

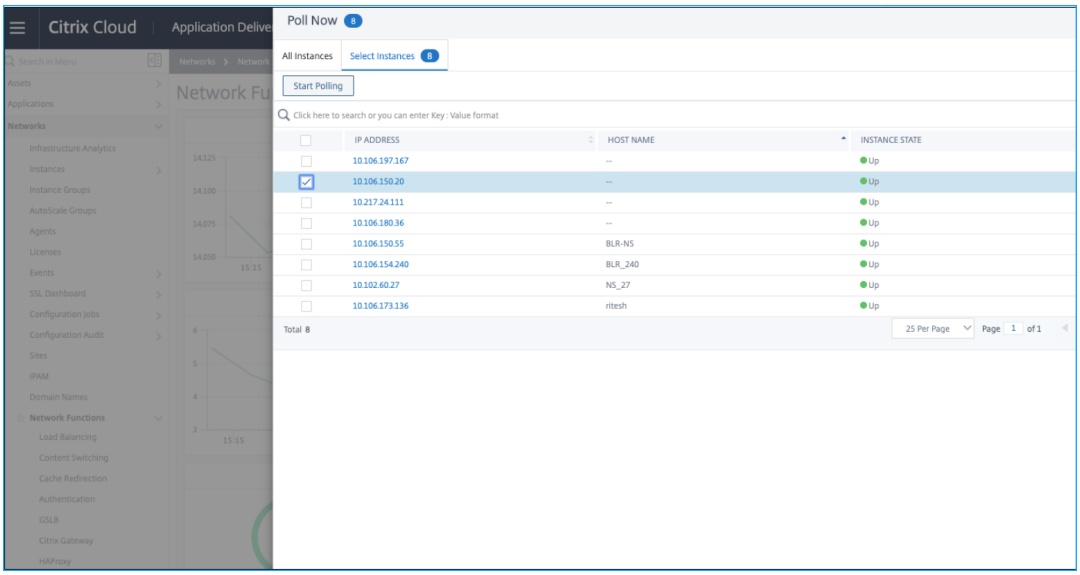


```
> sh appflow collector af_collector_rest_10.102.103.114
1) Name: af_collector_rest_10.102.103.114
IPv4 address: 10.102.103.114
Port: 5563
Netprofile:
Transport: rest
State: UP
Done
```

2. 使用可能なコレクタがない場合は、Citrix ADM でインスタンスの手動ポーリングを実行します。

   a) [ネットワーク] **>** [ネットワーク機能] **>** [今すぐ投票] に移動します

   b) インスタンスを選択し、[**Start Polling**] をクリックします。



   ポーリングに失敗した場合は、ADM から ADC インスタンスを削除してから、もう一度 ADC インスタンスを追加します。ADC インスタンスを追加すると、コレクタは ADC に追加されます。

コレクタに「**Down** 」ステータスが表示されている場合:

1. SNIP が構成されているかどうかを確認します。

```
> sh ip | grep SNIP
2)  10.106.150.34    0              SNIP            Active   Enabled  Enabled  NA       Enabled
```

   SNIP が構成されていない場合は、SNIP を構成する必要があります。詳しくは、「SNIP の構成」を参照してください。

2. ADC インスタンスが ADM に到達可能であることを確認してください。

   ping テストを実行することで検証できます。`ping -S <SNIP> <adm_receiver_ip>`を実行します。

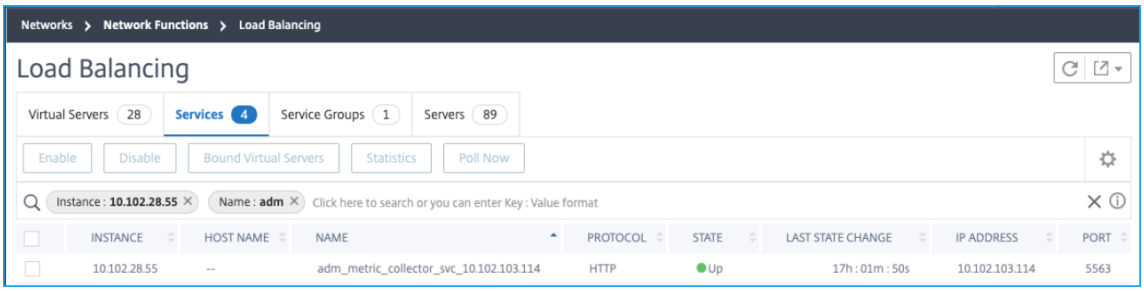

```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

Citrix ADC インスタンスは後でビルド

Citrix ADM で、メトリックスコレクタサービスが使用可能であることを確認します。

1. [ネットワーク**] > [**ネットワーク機能**] > [**負荷分散**] > [**サービス**]** に移動します。
2. 検索バーで、[インスタンス**:(IP** アドレス**)**] と [名前**:ADM**] でフィルタリングします。
3. `adm_metric_collector_svc_<adm_receiver ip>` が使用可能かどうか確認します。IP アドレスは、ADM 管理 IP またはエージェント IP のいずれかになります。

   このサービスが **UP** ステータスで、ポート 5563 で実行されていることを確認します。



それでもデータを表示できない場合は、コレクタサービスが Citrix ADC 時系列分析プロファイルにバインドされていることを確認します。

1. Citrix ADC にログオンする
2. 次のコマンドを実行します。

   `sh analytics profile ns_analytics_time_series_profile`

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```


コレクタに「**Down**」ステータスが表示されている場合:

1. SNIP が構成されているかどうかを確認します。

```
> sh ip | grep SNIP
2)  10.106.150.34    0              SNIP            Active   Enabled  Enabled  NA       Enabled
```

   SNIP が構成されていない場合は、SNIP を構成する必要があります。詳しくは、「SNIP の構成」を参照してください。

2. ADC インスタンスが ADM に到達可能であることを確認してください。

   ping テストを実行することで検証できます。`ping -S <SNIP> <adm_receiver_ip>`を実行します。

```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

3. Telnet を介したトラフィック接続がサービスを接続できることを確認します。

```
root@ns# telnet 10.102.103.114 5563
Trying 10.102.103.114...
Connected to 10.102.103.114.
Escape character is '^]'.
^]
telnet> q
Connection closed.
```

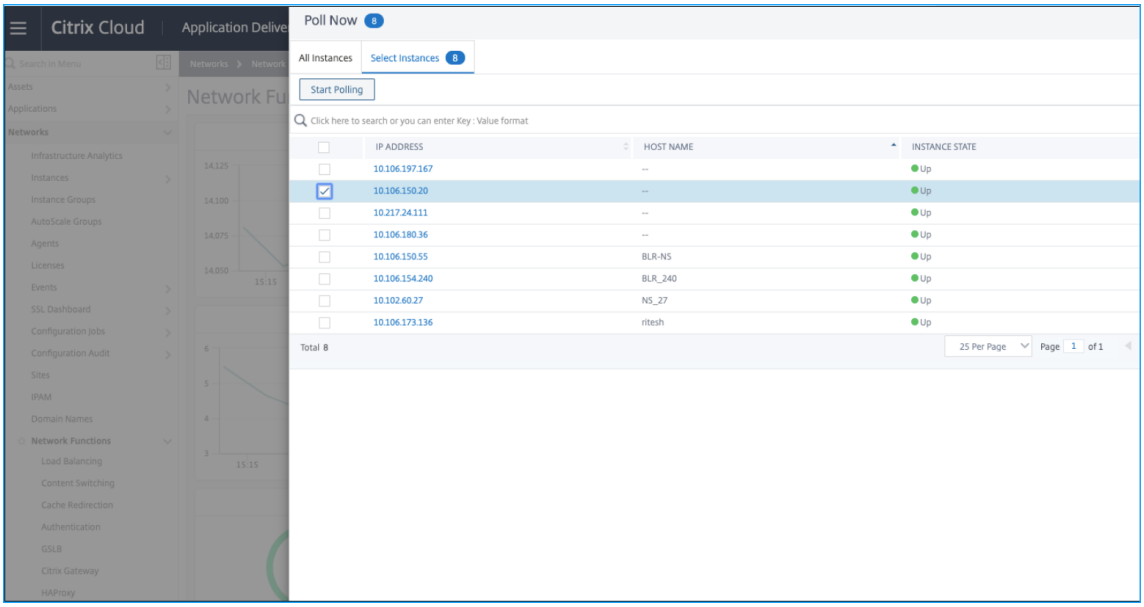
   telnet がサービスに接続できる場合は、ファイアウォールが存在し、メトリックデータフローをブロックしています。ファイアウォールブロックの問題を解決する必要があります。

Citrix ADC で時系列分析プロファイルにコレクタサービスがバインドされていない場合、コレクタは空白として表示されます。

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector:
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```


Citrix ADM でインスタンスの手動ポーリングを実行する必要があります。

1. [ネットワーク] **>** [ネットワーク機能] **>** [今すぐ投票] に移動します
2. インスタンスを選択し、[**Start Polling**] をクリックします。



ポーリングが失敗した場合は、次のコマンドを使用して、Citrix ADC インスタンスでコレクタサービスを直接追加します。

```
add service adm_metric_collector_svc_<adm_receiver_ip> <adm_receiver_ip
> HTTP 5563
```

```
unset analyticsprofile ns_analytics_time_series_profile -collectors
```

```
set analytics profile ns_analytics_time_series_profile -collectors
adm_metric_collector_svc_<adm_receiver_ip> -metrics enabled -events
enabled
```

分析時系列プロファイルが更新されます。

```
> add service adm_metric_collector_svc_10.102.103.114 10.102.103.114 HTTP 5563
 Done
> unset analyticsprofile ns_analytics_time_series_profile  -collectors
 Done
> set analytics profile ns_analytics_time_series_profile -collectors adm_metric_collector_svc_10.102.103.114 -metrics enab
 Done
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

上記のトラブルシューティング手順をすべて実行しても問題が解決しない場合は、**Citrix** サポートにお問い合わせください。

アプリケーション分析のしきい値およびアラートの作成

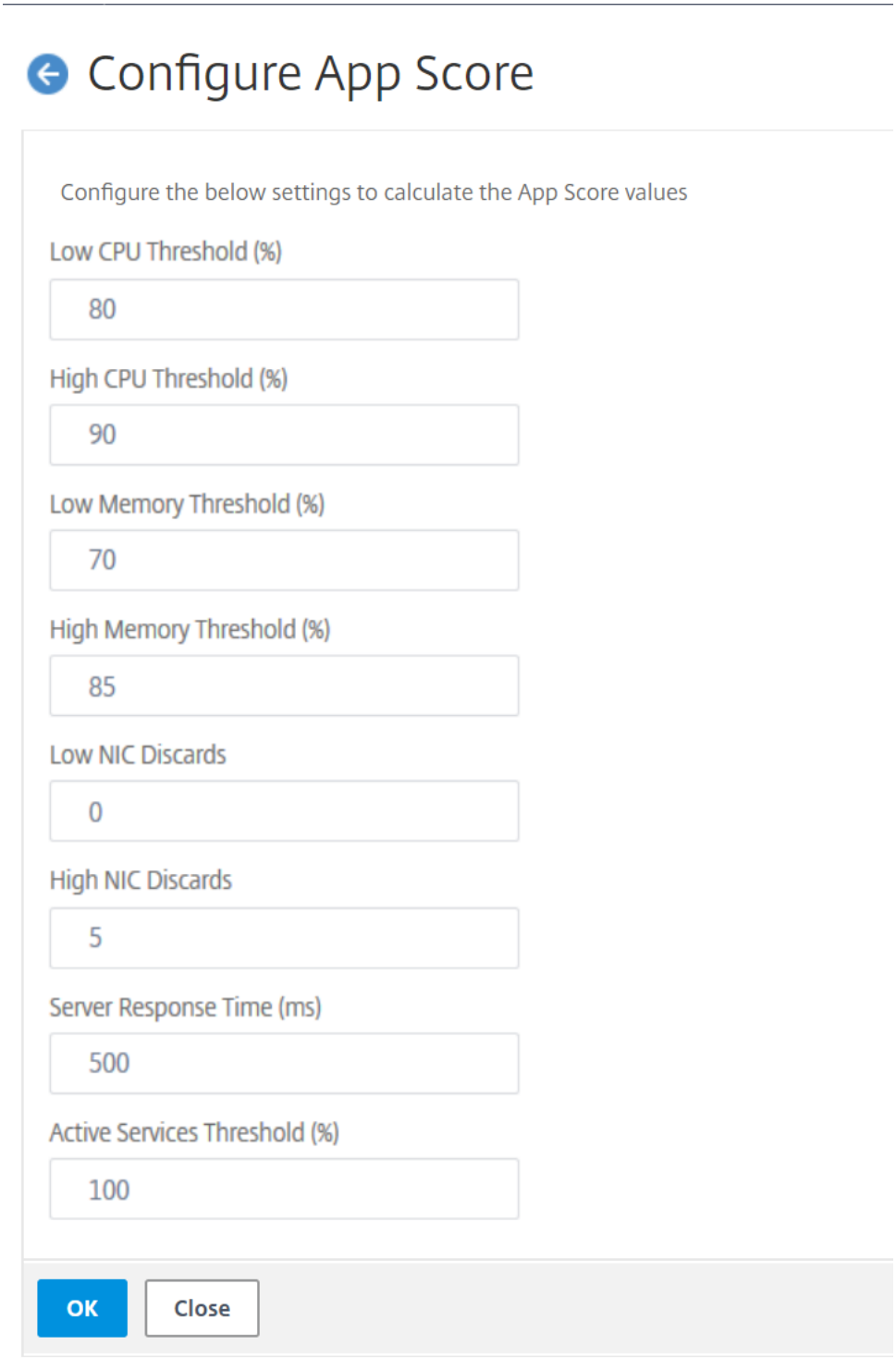
May 7, 2021

Citrix ADM アプリケーション分析では、Citrix ADC インスタンスを通過するさまざまな種類のトラフィックを監視できます。Citrix ADM では、次のカウンターのしきい値を設定して、トラフィックとアプリのスコアを監視できます。

しきい値を構成し、CPU、メモリ、NIC 廃棄および応答時間のアプリケーションスコアを監視できます。

Citrix ADM でアプリのスコアを構成するには:

1. Citrix ADM で、[**Analytics**] > [設定] に移動します。
2. [設定] ページで、[アプリスコアの構成] をクリックします。
3. [アプリスコアの構成] ページで、次のパラメータの値を入力します。
    a) **CPU** しきい値が低い。Citrix ADC インスタンスの合計 CPU 使用率の下限しきい値。
    b) 高い **CPU** しきい値。Citrix ADC インスタンスの合計 CPU 使用率の上限しきい値。
    c) メモリ不足のしきい値。Citrix ADC インスタンスの合計メモリ使用量の下限しきい値。
    d) 高いメモリしきい値。Citrix ADC インスタンスの合計メモリ使用量のより高いしきい値。
    e) **NIC** が低いと **SLA** が廃棄されます。インターフェイスによって廃棄されるパケットの下限しきい値。
    f) **NIC** が高いと **SLA** が廃棄されます。インターフェイスによって廃棄されるパケットの上限しきい値。
    g) 応答時間。要求パケットの送信から、仮想サーバ上で構成されたサービスからの最初の応答パケットを受信するまでの時間間隔。Citrix ADM で構成されたデフォルト値は 500 ミリ秒です。
    h) アクティブサービスのしきい値。仮想サーバーにバインドされているアクティブでなければならないサービスのパーセンテージのしきい値。



4. [**OK**] をクリックします。

インテリジェントなアプリケーション分析

May 7, 2021

インテリジェントなアプリケーション分析により、機械学習とルールアルゴリズムを使用して、アプリケーションのパフォーマンスの問題を特定できます。Citrix ADM インテリジェントアプリ分析機能:

- Citrix ADC インスタンスを介して配信されるアプリケーションの監視とトラブルシューティングを行うための、簡単でスケーラブルなソリューションを提供します。
- すべてのレベルのアプリケーションを監視して、問題のトラブルシューティングに要する時間を短縮し、アプリケーション全体のアップタイムを向上させます。

通常の展開では、数千台のサーバーがユーザーのデータニーズに対応します。これらのサーバーに送信されるトラフィックは、負荷分散され、Citrix ADC アプライアンスに構成された仮想サーバーによって監視されます。各仮想サーバーは、バックエンドサーバーを表す複数のサービスにバインドされます。このような展開では、インテリジェント App Analytics 機能によって次のことが実現されます。

- 停止やその他のイベントの監視、管理、意思決定を行う
- アプリケーション用に構成された仮想サーバおよびサービスの監視
- 仮想サーバおよびサービスに関する重要な情報を表示します。これにより、アプリケーションの最適なパフォーマンスを実現するために必要な構成を変更できます。

「アプリケーション」>「ダッシュボード」に移動し、「問題」セクションのパフォーマンス・インディケータを表示するアプリケーションを選択します。

インテリジェントアプリ分析の構成

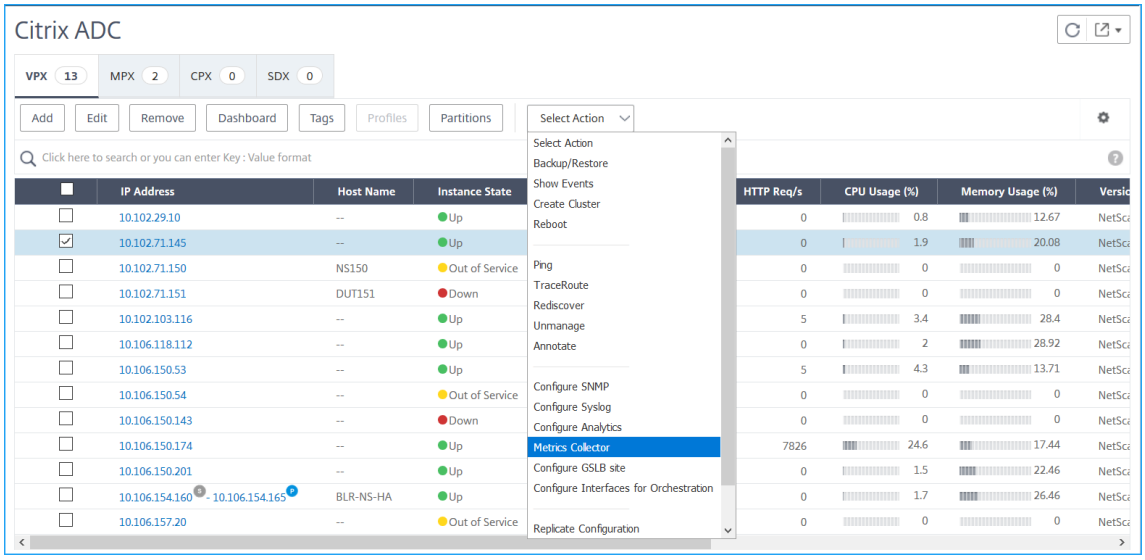
May 7, 2021

インテリジェントアプリ分析機能は、**Citrix ADC 12.1** ビルド **50.28** 以降でのみサポートされます。メトリックコレクターは、Citrix ADC カウンターデータを Citrix ADM にプッシュし、アプリケーションの問題を検出するために使用されます。インテリジェントアプリケーション分析機能を使用するには、各 Citrix ADC インスタンスで メトリックコレクターを構成する必要があります。Citrix ADM にインスタンスを追加している間、メトリックスコレクターはデフォルトで Citrix ADC で有効になっています。

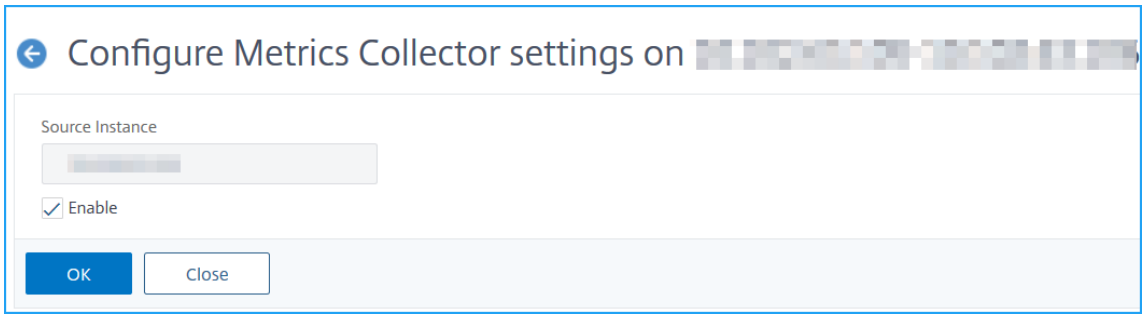
メトリック・コレクタが有効になっているかどうかを確認するには、次の手順に従います。

1. [ネットワーク**] > [**インスタンス**]** に移動します。[インスタンス］で、監視するインスタンスのタイプ（Citrix ADC VPX など）を選択します。
2. Citrix ADC インスタンスを選択します。

3.「アクションの選択」リストから、「メトリック・コレクター」を選択します。



4.「メトリック・コレクタ設定の構成」ページで、「有効」オプションが選択されていることを確認します。そうでない場合は、「有効」オプションを選択し、「**OK**」をクリックします。



Citrix **ADC** インスタンスでメトリックスコレクタオプションが有効になったら、［アプリケーション］>［ダッシュボード］に移動します。[問題] セクションで異常を表示するインスタンスを選択します。

また、分析を有効にして、サーバーエラーの詳細な Web トランザクションなどの問題を視覚化することをお勧めします (5xx)。詳しくは、「Analytics の有効化」を参照してください。

アプリケーション分析用のパフォーマンス・インディケータ

May 7, 2021

パフォーマンス指標と、Citrix ADC Web アプリケーションで発生するカテゴリを表示できます。これらのインジケータを表示するには、ADC インスタンス メトリックコレクター で分析を有効にする必要があります。

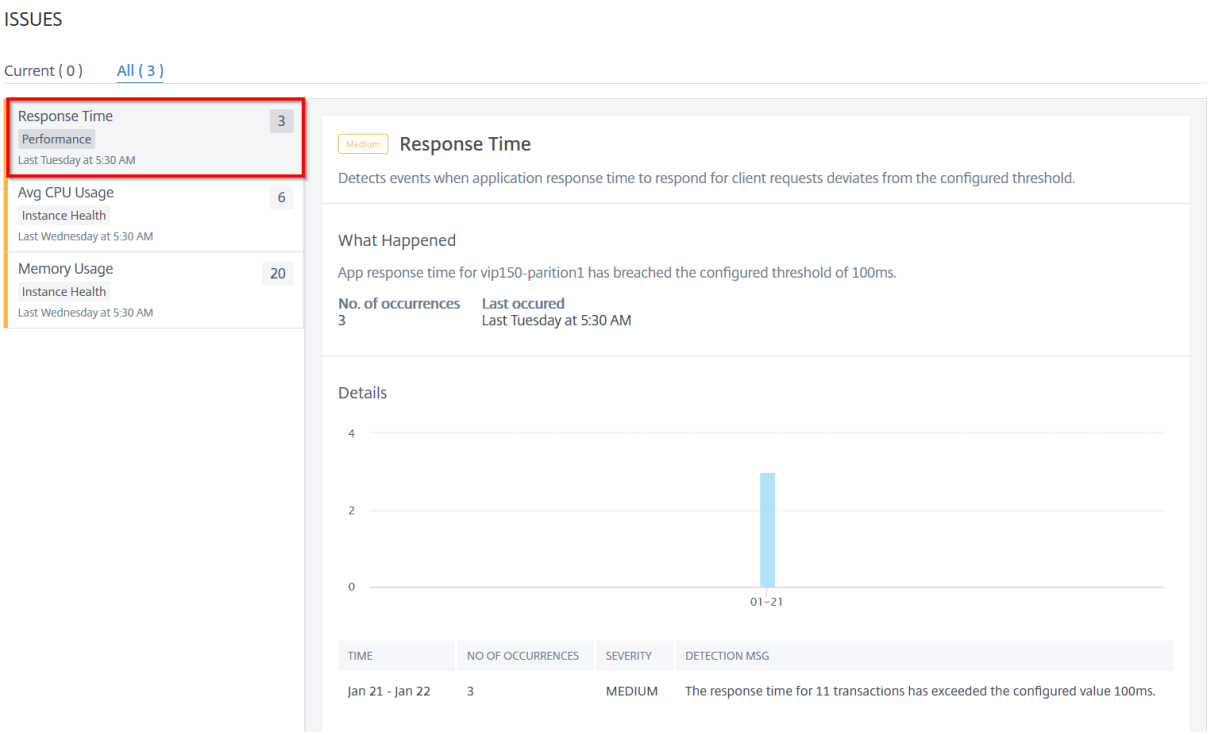
分析およびメトリック・コレクターを有効にした後、「アプリケーション」>「ダッシュボード」に移動してアプリケーションを選択し、「問題」セクションまでスクロールダウンすると、次のインジケータを表示できます。

- 応答時間
- アクティブなサービス
- 平均 CPU 使用率
- メモリ使用率
- NIC カードの飽和
- サービスフラップ
- サーバーの応答時間
- セッションの再利用が低い
- 不適切な永続性タイプ
- 不安定なサーバー (5xx)
- SSL リアルタイムトラフィック
- 異常に大きい HTTP パケット
- TCP 再構成キュー制限ヒット
- サージキューのビルダップ

応答時間

July 7, 2020

この問題は、クライアント要求に応答するアプリケーションの応答時間が、設定されたしきい値から逸脱した場合に検出されます。「応答時間」タブをクリックして、問題の詳細を表示します。



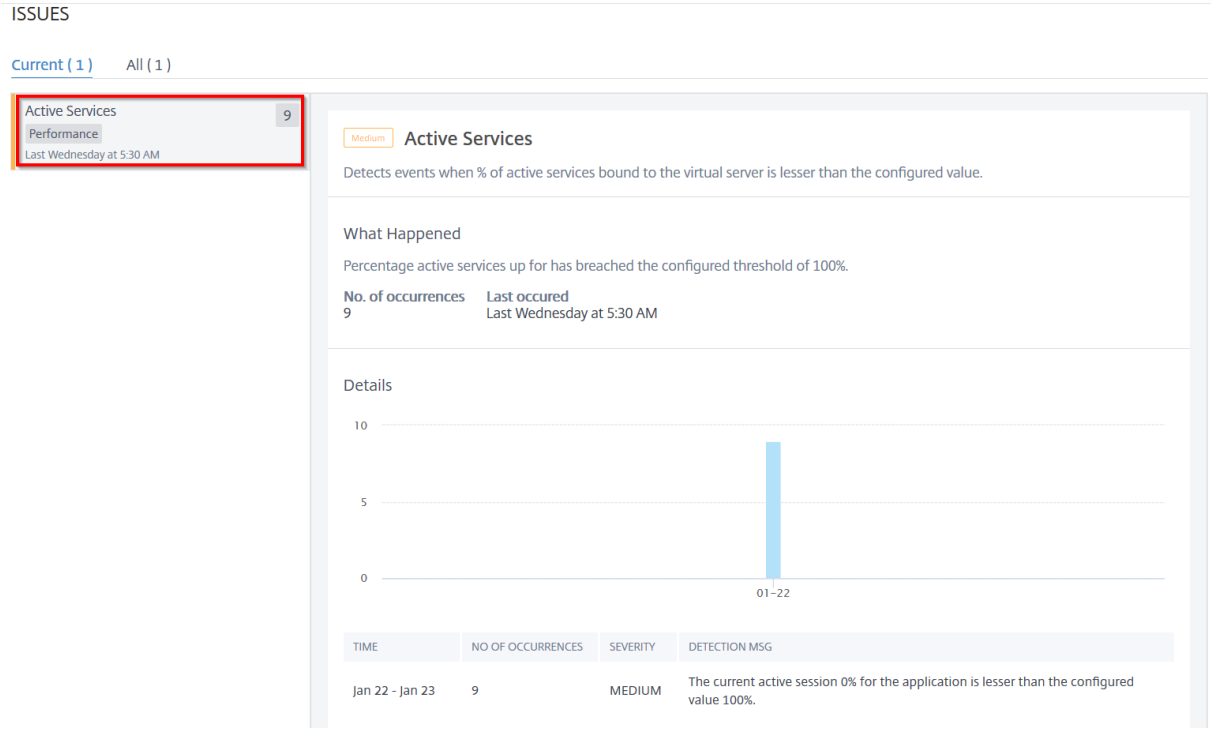
[詳細] では、次の項目を表示できます。

- 選択した時間の合計イベントを示すグラフ。クリックしてフィルタを適用し、詳細を表示します。
- 問題が発生した日時
- 選択した時間の合計オカレンス
- 「低」、「中」、「高」などの問題の重大度
- 設定されたしきい値を超えた合計トランザクション応答時間を示す検出メッセージ

アクティブなサービス

July 7, 2020

この問題は、仮想サーバにバインドされているアクティブサービスの割合が、設定されたしきい値よりも小さい場合に検出されます。[アクティブなサービス] タブをクリックして、問題の詳細を表示します。



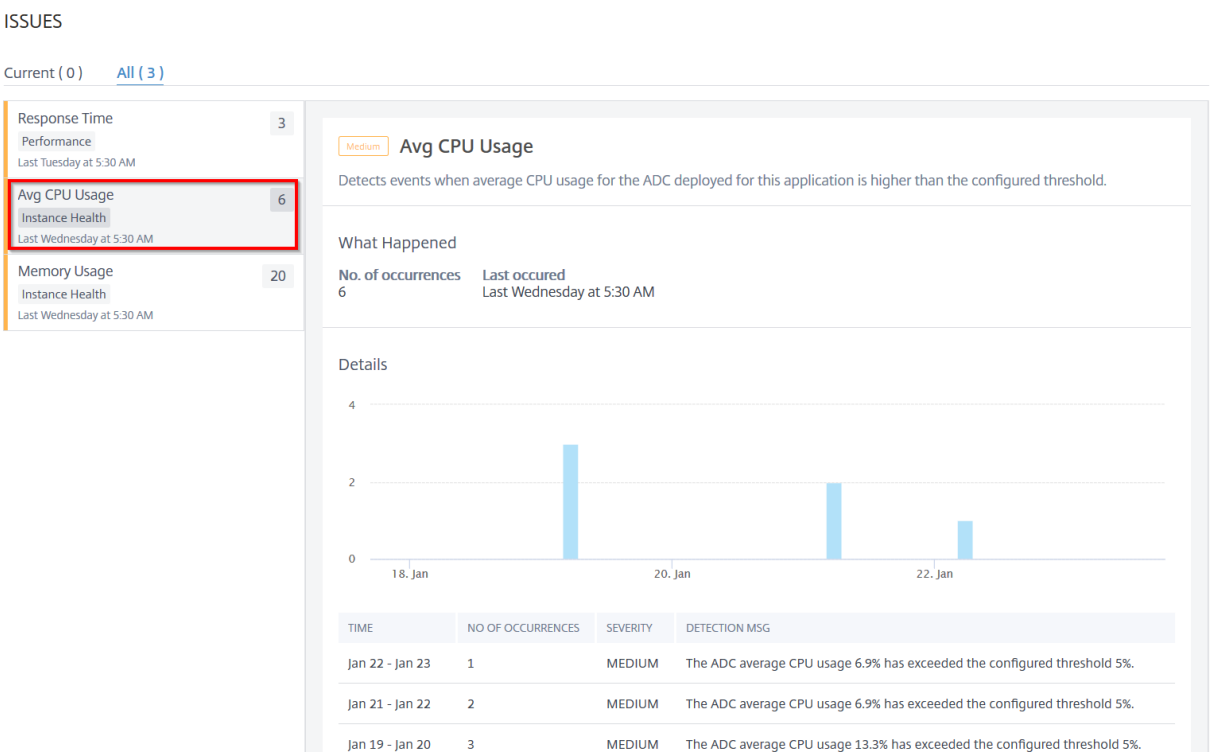
[詳細] では、次の項目を表示できます。

- 選択した期間の合計イベントを示すグラフ。クリックしてフィルタを適用し、詳細を表示します。
- 問題が発生した日時
- 選択した期間の合計オカレンス
- 「低」、「中」、「高」などの問題の重大度
- アクティブなサービスセッションの割合、および設定されたしきい値を示す検出メッセージ

平均 **CPU** 使用率

July 7, 2020

この問題は、このアプリケーションの ADC CPU 使用率が設定されたしきい値を超えた場合に検出します。[平均 **CPU** 使用率] タブをクリックして、問題の詳細を表示します。



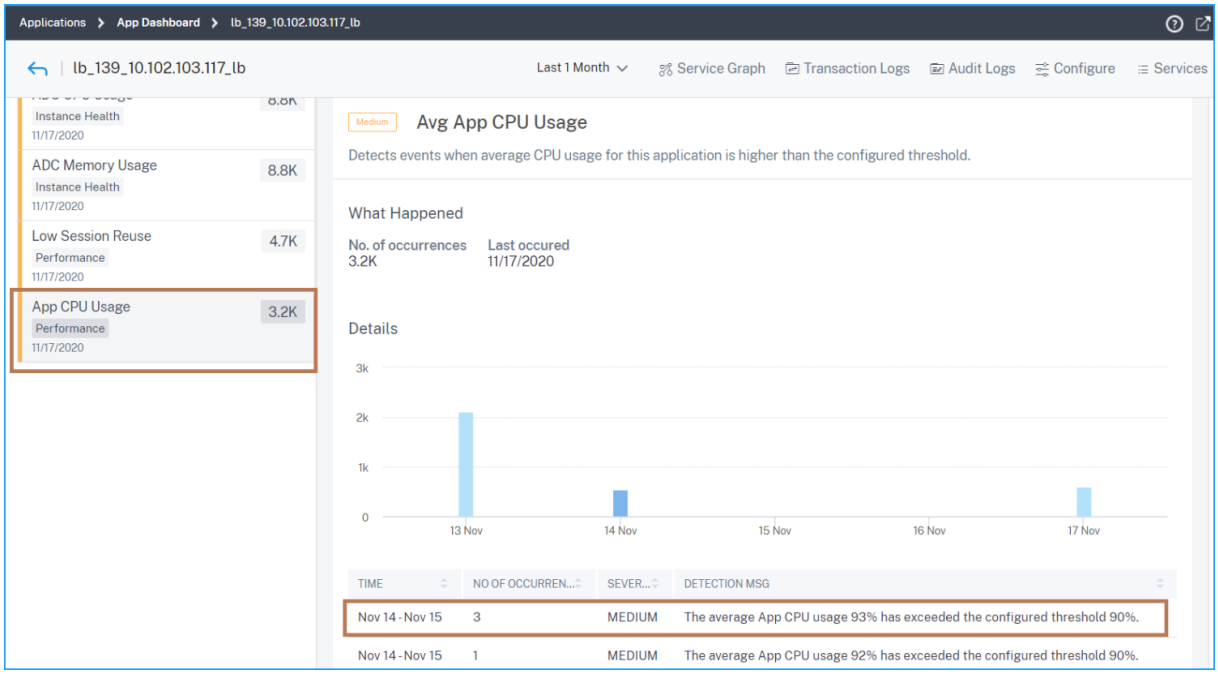
[詳細] では、次の項目を表示できます。

- 選択した期間の合計イベントを示すグラフ。クリックしてフィルタを適用し、詳細を表示します。
- 問題が発生した日時
- 選択した期間の合計オカレンス
- 「低」、「中」、「高」などの問題の重大度
- ADC 平均 CPU 使用率（%）と設定されたしきい値を示す検出メッセージ

アプリケーションの平均 **CPU** 使用率

May 7, 2021

この問題は、アプリケーションの CPU 使用率が設定されたしきい値を超えた場合に検出されます。[アプリ **CPU** 使用率] タブをクリックして、問題の詳細を表示します。



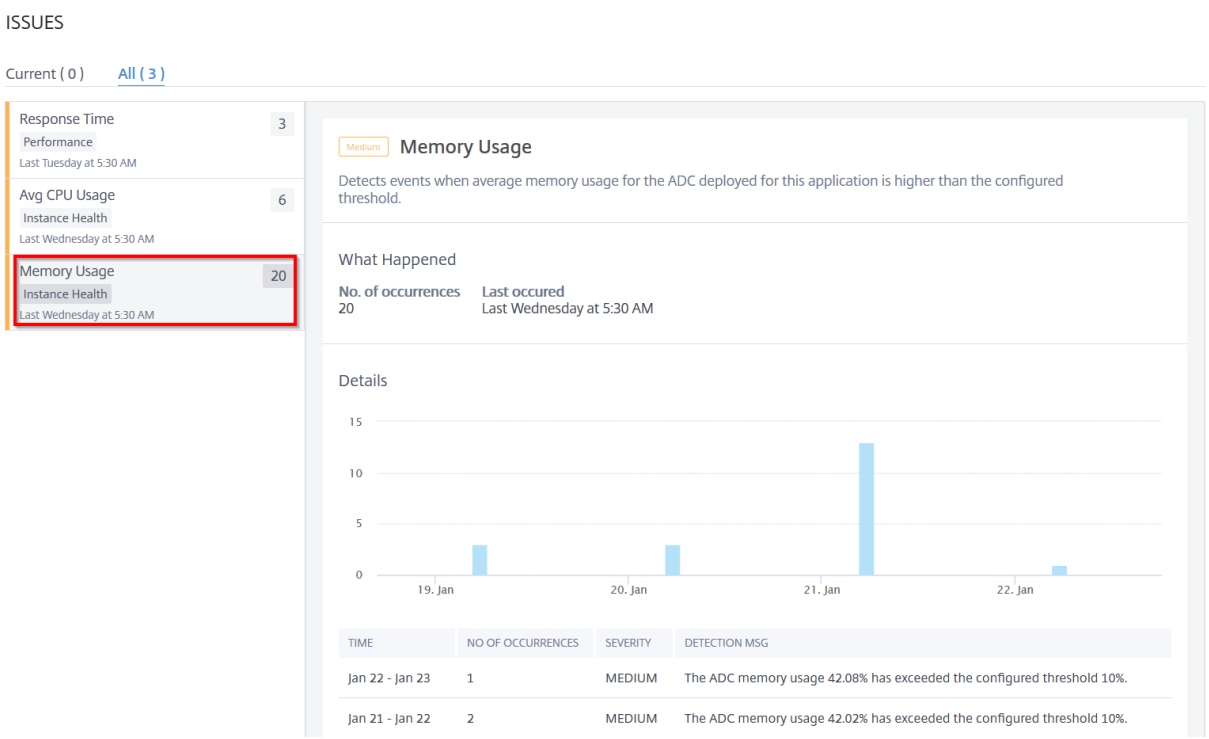
[詳細] では、次の項目を表示できます。

- 選択した期間の合計イベントを示すグラフ。クリックしてフィルタを適用し、詳細を表示します。
- 問題が発生した日時
- 選択した期間の合計オカレンス
- 「低」、「中」、「高」などの問題の重大度
- アプリケーションの平均 CPU 使用率（%）と設定されたしきい値を示す検出メッセージ

メモリ使用率

May 7, 2021

この問題は、このアプリケーションの ADC メモリ使用量が設定されたしきい値を超えた場合に検出します。[メモリ使用量] タブをクリックして、問題の詳細を表示します。



[詳細] では、次の項目を表示できます。

- 選択した期間の合計イベントを示すグラフ。クリックしてフィルタを適用し、詳細を表示します。
- 問題が発生した日時
- 選択した期間の合計オカレンス
- 「低」、「中」、「高」などの問題の重大度
- ADC 平均メモリ使用率（%）と設定されたしきい値を示す検出メッセージ

サービスフラップ

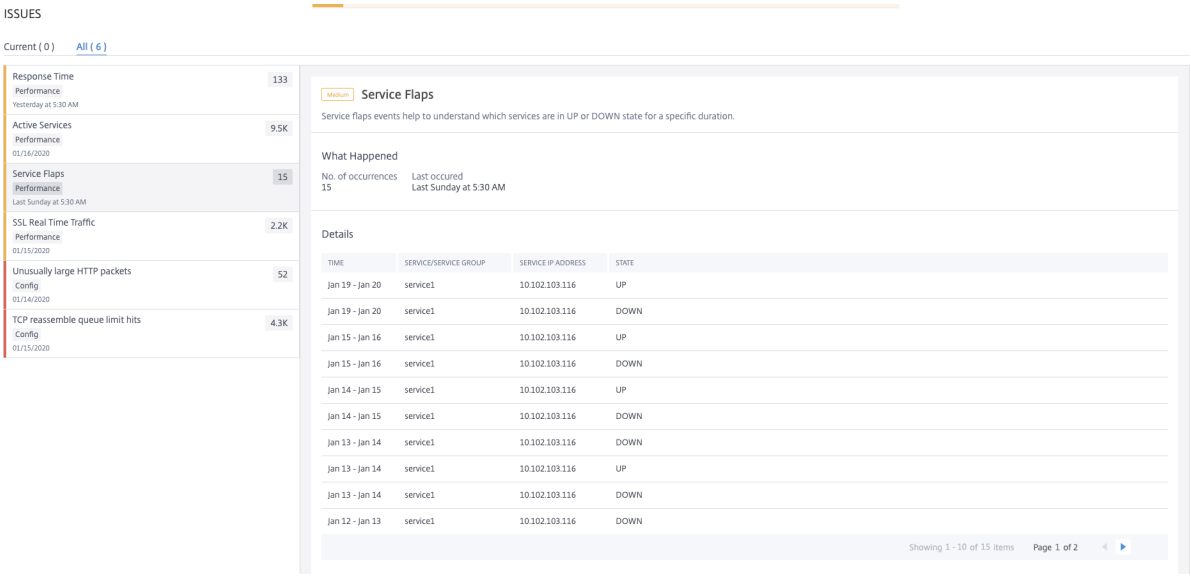
July 7, 2020

ネットワーク管理者は、アプリケーションの可用性を最適に保つ必要があります。ネットワークの問題や構成の問題がある場合、アプリケーションサーバーのステータスと可用性が全体的なパフォーマンスに影響を与える可能性があります。

サービスフラップイベントを使用して、問題のあるアプリケーションを特定できます。サービスフラップイベントは、次の点にも役立ちます。

- 特定の期間中 DOWN ステータスになっているサービスを理解する
- 特定の期間に UP または DOWN 状態にあるサービスの数を把握する

[**Service Flaps**] タブをクリックして、サービスフラップの詳細を表示します。



出現回数や最後に出現した時刻などの詳細を表示できます。

[詳細] では、次の項目を表示できます。

- サービスフラップ異常が発生した時刻
- サービス/サービスグループ名
- サービスの IP アドレス
- 現在のサービス状態

不安定なサーバ

May 7, 2021

一部のシナリオでは、無効な要求、一時的な過負荷、またはサーバーのメンテナンスなどの理由で要求を処理できない場合、Web サーバーはステータスコードで応答します。これらのエラーは、エラーのさまざまなシナリオを定義するエラーコードとともに表示されます。例:

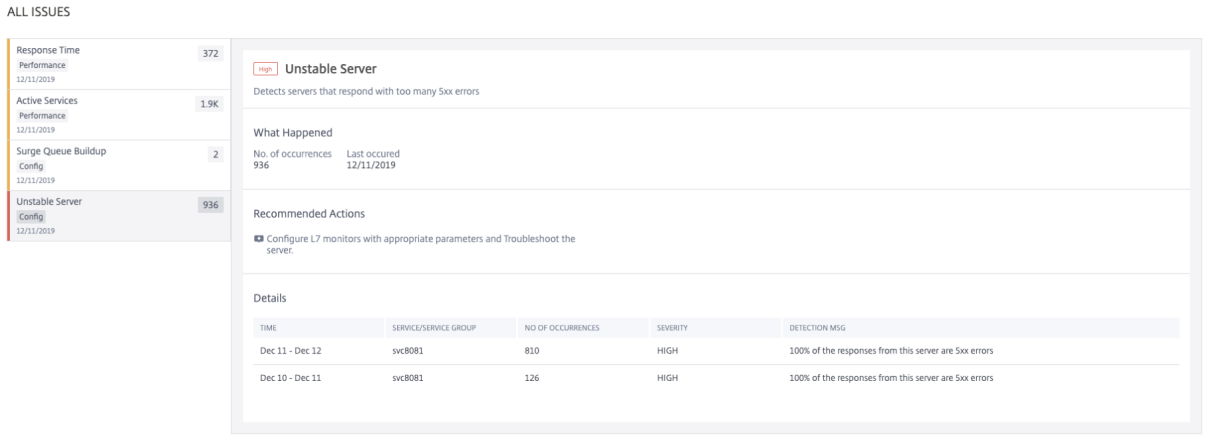
- **502** 不正な **Gateway**
  サーバーはゲートウェイまたはプロキシとして機能しており、アップストリームサーバーから無効な応答を受信しました。
- **503** サービス利用不可
  サーバーは現在利用できません。サーバーは過負荷またはメンテナンスのためにダウンしている可能性があります。

- **504 Gateway** タイムアウト
  サーバーはゲートウェイまたはプロキシとして機能しており、アップストリームサーバーからタイムリーな応答を受信しませんでした。

これらは一時的な条件ですが、Web ページをアップして利用できるようにするために、Web サーバーに修正措置を実装する必要があります。

不安定なサーバーインジケーターを使用すると、これらの障害を表示し、問題を解決するための修正アクションに関する決定を下し、クライアント要求が処理され、Web ページが常に利用可能であることを確認できます。

「不安定なサーバー」タブを選択して、問題の詳細を表示します。



問題のトラブルシューティングに 推奨される対処方法は次のとおりです。

- 5xx エラーで応答するサーバに適したパラメータを使用して L7 モニタを設定します。モニターは、サービスの状態を追跡するエンティティです。アプライアンスは、各サービスにバインドされたモニターを使用して、サーバーを定期的にプローブします。指定された応答タイムアウト内にサーバーが応答せず、指定されたプローブが失敗した場合、サービスは DOWN とマークされます。その後、アプライアンスは残りのサービス間で負荷分散を実行します。モニターの構成について詳しくは、カスタムモニターを参照してください。
- サーバーのトラブルシューティング

[詳細] では、次の項目を表示できます。

- 不安定なサーバー異常が発生した時刻
- サービス/サービスグループ名
- 総発生数
- 高、低、中などの異常の重症度
- 5xx エラーを報告する本サービスからの応答の% を示す検出メッセージ

サーバーエラー Web トランザクションについて詳しくは、サーバーエラーの Web トランザクション分析を参照してください。

サーバの応答時間

May 7, 2021

アプリケーションの遅さは、ビジネスへの影響や生産性につながるため、あらゆる組織にとって大きな懸念事項です。管理者は、ビジネスへの影響を避けるために、すべてのアプリケーションが最適に動作するようにする必要があります。

アプリケーションごとに動作が異なり、応答時間の期待値が異なります。大規模なサーバファームがある場合、管理者が各アプリケーションを評価し、サーバの応答時間のしきい値を設定することは、時間のかかる作業になります。

サーバー応答時間インジケータは、管理者は機械学習アルゴリズムに基づいてすべてのアプリケーションを評価するのに役立ちます。このインジケータは、次のことを報告します。

- 異常な高応答時間
- 異常な低応答時間

[サーバーの応答時間] タブをクリックして、問題の詳細を表示します。

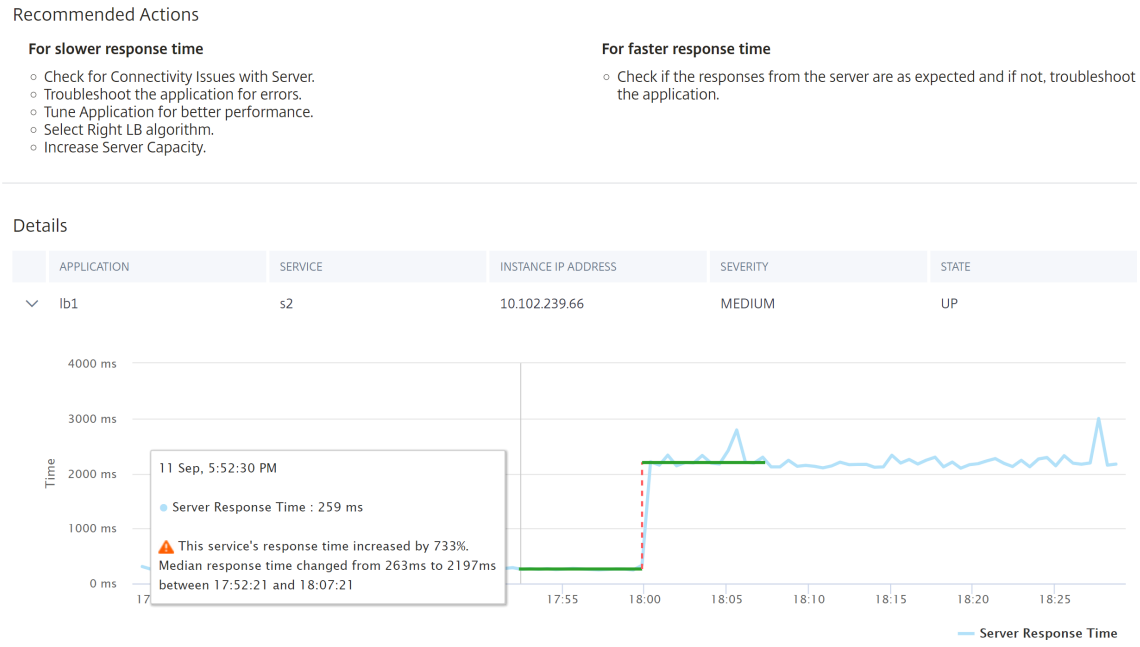
推奨アクションでは、これらの異常をトラブルシューティングすることをお勧めします。

[詳細] では、次の項目を表示できます。

- 異常があるアプリケーション
- アプリケーションにバインドされているサービス
- Citrix ADC インスタンスの IP アドレス
- 異常重大度タイプ
- アプリケーションのステータス
- 選択した期間のサーバー応答時間グラフ
- サーバーの応答時間に基づくローリング中央値グラフ
- 異常の詳細

Citrix ADM は、異常な高応答時間と異常な低応答時間の異常を検出します。

- 異常な高いサーバー応答時間に対する異常

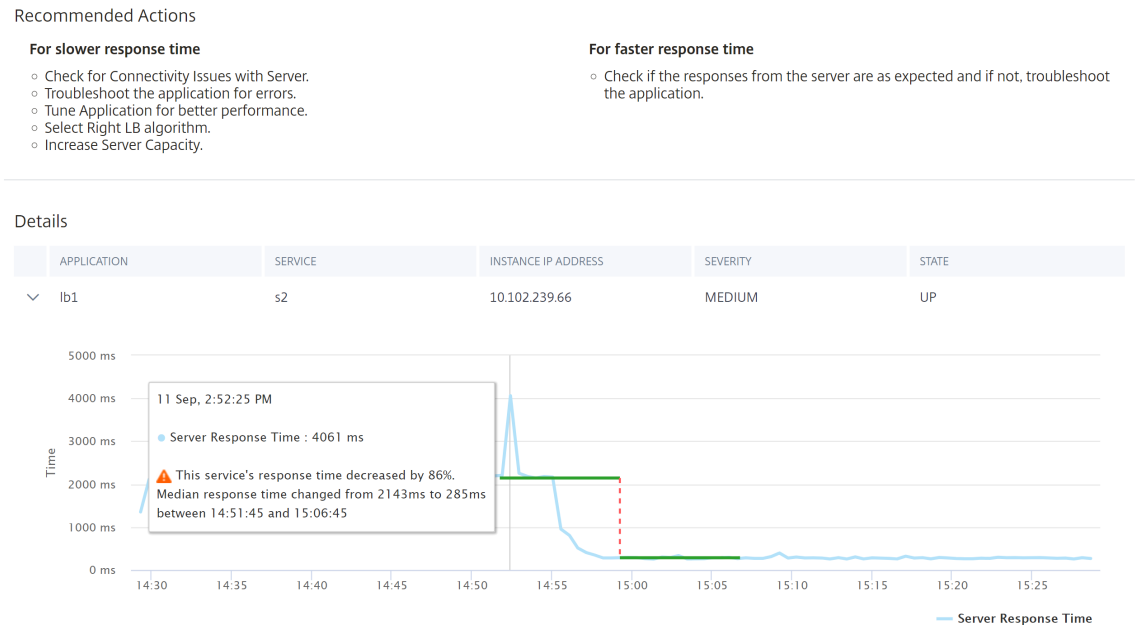


Citrix ADM は、特定の期間におけるサーバーの平均応答時間を比較します。この図に示されているように、Citrix ADM は、サーバーの平均応答時間を 17:50 ～18:20 の間で比較します。

サーバーの応答時間が増加し始めると、Citrix ADM はサーバーの応答時間をさらに監視し、サーバーの応答時間が増加し始めた時間の異常を検出します。

この図に示されている例によると、17:52 から 18:07 までの平均サーバ応答時間を比較すると、サーバの応答時間が 733% 増加していることがわかります。

- 異常な低いサーバー応答時間に対する異常



Citrix ADM は、特定の期間におけるサーバーの平均応答時間を比較します。この図に示されているように、Citrix ADM は 14:51 から 15:06 までの平均サーバー応答時間を比較します。

サーバーの応答時間が減少し始めると、Citrix ADM はサーバーの応答時間をさらに監視し、サーバーの応答時間が減少し始めた時間の異常を検出します。

この図に示されている例によると、14:51 ～15:06 の平均サーバの応答時間を比較すると、サーバの応答時間が 86% 減少していることがわかります。

セッションのビルダップ

May 7, 2021

セキュリティで保護されたすべてのトランザクションについて、Citrix ADC は最初のトランザクションに対して SSL オフロード処理を実行し、セッション の再利用構成に基づいて **SSL** セッションを保存します。

トラフィックレートに基づいて、一定期間にわたってセッションがビルドアップする可能性があり、Citrix ADC では、これらのセッションで大量のメモリが保持される可能性があります。

セッションのビルドアップイベントは、管理者に警告し、このイベントを解決するための推奨アクションを提供します。「セッションの構築」タブをクリックして、問題の詳細を表示します。

[詳細] では、次の項目を表示できます。

- セッションのビルドアップ異常が発生した時刻
- 仮想サーバ名
- 高、低、中などの異常の重症度
- 仮想サーバで使用可能な **X** 個の SSL セッションと、現在のところ、設定されたタイムアウトセッション内に 1 秒あたり **Y** 個の SSL ハンドシェイクがあることを示すメッセージ。

この異常を修正するための 推奨アクションは、セッションのタイムアウトを減らすか、セッションの再利用を無効にすることです。詳しくは、「セッションのタイムアウト」を参照してください。

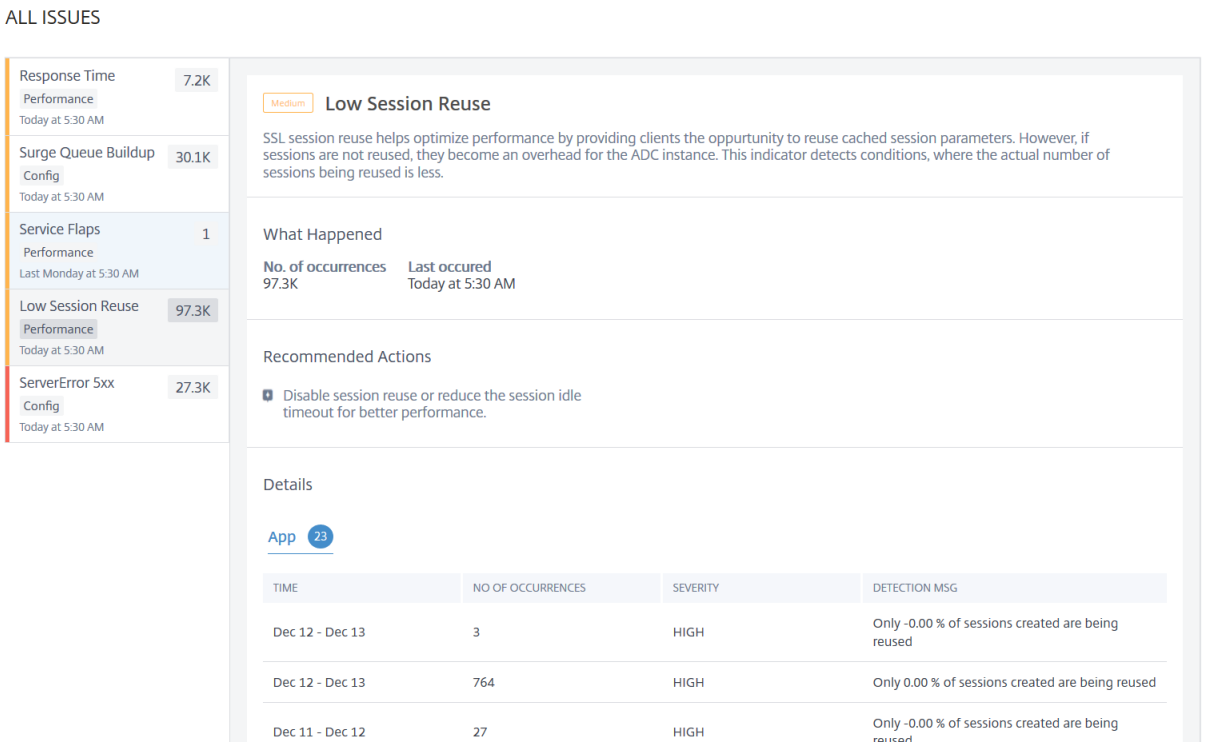
セッションの再利用が低い

July 7, 2020

Citrix ADC インスタンスは、サーバーから SSL ハンドシェイクプロセスをオフロードすることによって、SSL トランザクションを処理します。サーバーから応答を受信すると、Citrix ADC インスタンスはクライアントとの安全なトランザクションを完了します。Citrix ADC インスタンスは、キャッシュされたセッションパラメーターを使用して、連続した要求の SSL ハンドシェイクプロセスを完了します。

これらのセッションが再利用されない場合は、Citrix ADC インスタンスのオーバーヘッドになります。「**Low Session Reuse**」インジケータを使用すると、再利用される実際のセッション数が少ないかどうかを識別できます。

「低セッションの再利用」タブをクリックして、問題の詳細を表示します。



問題のトラブルシューティングに 推奨されるアクションは、セッションの再利用を無効にするか、セッションのタイムアウトを減らすことです。詳しくは、「セッションの再利用」を参照してください。

[詳細] では、次の項目を表示できます。

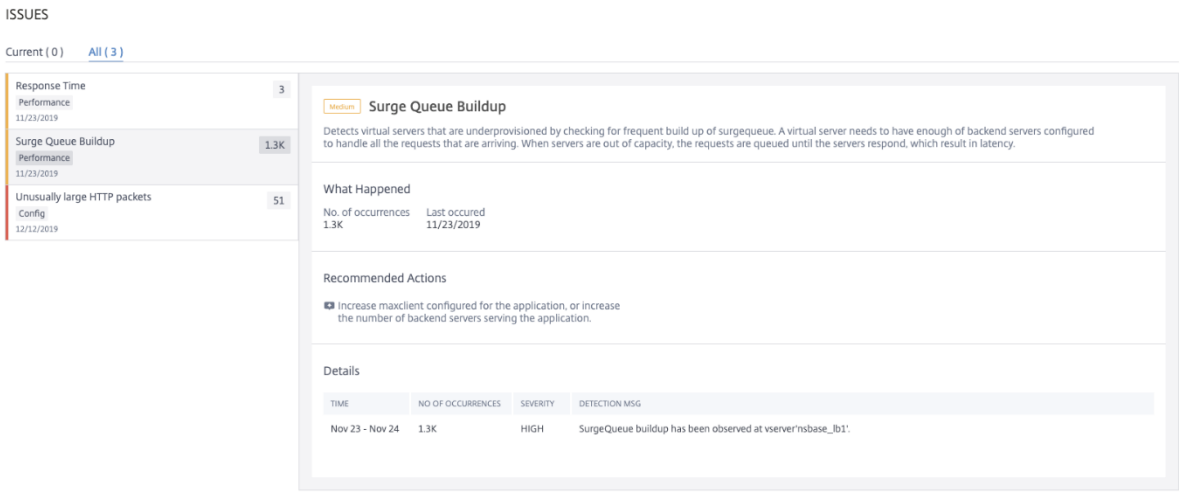
- セッションの再利用率が低いアプリケーションの合計
- 低セッションの再利用異常が発生した時間
- 総発生数
- 高、低、中などの異常の重症度
- 設定済みセッションの% のみが再利用されていることを示す検出メッセージ

サージキューのビルダップ

May 7, 2021

サーバーが要求の急増を受信すると、サーバーはクライアントへの応答が遅くなります。多くの場合、オーバーロードにより、クライアントはエラーページを受信します。仮想サーバーには、着信要求を処理するための十分なバックエンドサーバーを構成する必要があります。

サージキューのビルドアップインジケータを使用すると、サージキューのビルドアップがある仮想サーバーを表示できます。[サージキューのビルダップ] タブをクリックして、問題の詳細を表示します。



問題のトラブルシューティングに 推奨される対処方法は次のとおりです。

- クライアント接続の制限数を増やします。詳しくは、「クライアント接続数の制限を設定する」を参照してください。
- アプリケーション要求を処理するためにバックエンドサーバーを増やす

[詳細] では、次の項目を表示できます。

- サージキューの蓄積異常が発生した時間
- 総発生数
- 高、低、中などの異常の重症度
- 仮想サーバ上のサージキューの蓄積を示す検出メッセージ

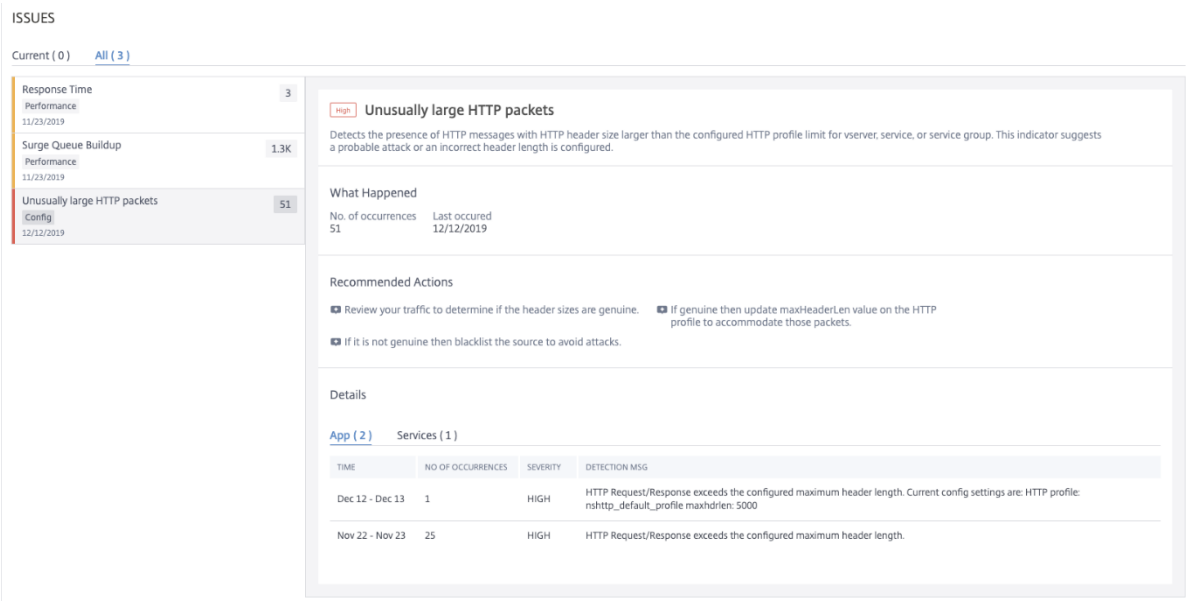
異常に大きい **HTTP** パケット

May 7, 2021

HTTP トランザクションは、クライアントとサーバー間の要求応答メッセージを使用します。要求メッセージと応答メッセージでは、HTTP ヘッダーは HTTP プロトコルに表示される値です。仮想サーバ、サービス、またはサービスグループで HTTP ヘッダー長を設定して、4xx エラーを回避できます。

HTTP 要求/応答がヘッダーの最大長を超えると、攻撃の可能性があります。[異常に大きい **HTTP** パケット] インジケータを使用すると、HTTP ヘッダーサイズの HTTP メッセージが設定値を超えている状況を表示できます。

[異常に大きい **HTTP** パケット] タブをクリックして、問題の詳細を表示します。



問題のトラブルシューティングに 推奨される対処方法は次のとおりです。

- トラフィックを確認して、ヘッダーサイズが正規のものかどうかを判断します。ヘッダーサイズが正規の場合は、HTTP プロファイルのヘッダー値を更新します。詳しくは、「バッファオーバーフローチェック」を参照してください。
- ヘッダーのサイズが正規でない場合は、攻撃を避けるためにソースをブロックリストに追加します。

[詳細] では、次の項目を表示できます。

- 異常発生した時間
- 総発生数
- 高、低、中などの異常の重症度
- 仮想サーバ、サーバ、またはサービスグループに設定されている現在の HTTP ヘッダー長を示す検出メッセージ

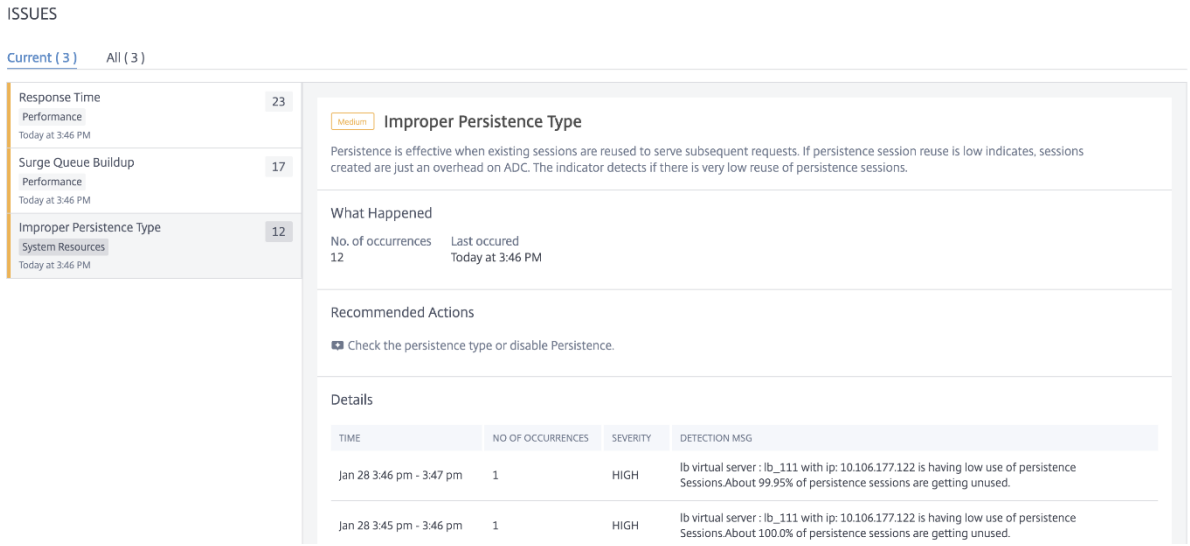
不適切な永続性タイプ

May 7, 2021

仮想サーバーにより実行されるサービスへの接続を維持したい場合（電子商取引で使用される接続など）は、その仮想サーバーに対してパーシステンスを構成する必要があります。アプライアンスは、まず構成されている負荷分散方式に基づいてサーバーを選択しますが、それ以降は同じクライアントからのすべての要求を同じサーバーに転送します。

永続性は、既存のセッションが後続のリクエストを処理するために再利用される場合に有効です。持続性セッションの再利用が少ない場合、ADC で作成されるセッションはオーバーヘッドに過ぎません。

不適切な永続性の種類インジケータを使用すると、仮想サーバーでの永続性の使用率が低いかどうかを判断できます。「不適切な持続性タイプ」タブをクリックして、問題の詳細を表示します。



問題のトラブルシューティングに 推奨されるアクションは、永続性タイプを確認するか、永続性を無効化することです。詳しくは、「持続性設定」を参照してください。

[詳細] では、次の項目を表示できます。

- 異常発生した時間
- 総発生数
- 高、低、中などの異常の重症度
- 未使用のセッションの割合（%）を示す検出メッセージ

TCP 再構成キュー制限ヒット

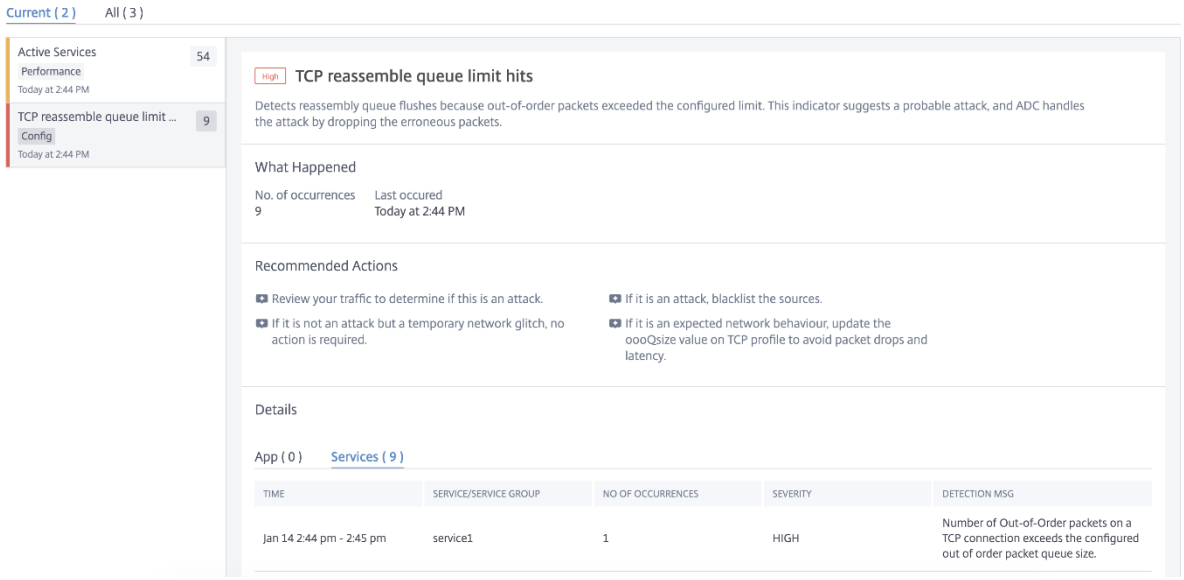
May 7, 2021

TCP は、OOO パケットを TCP 通信に保持するために、アウトオブオーダーキューを維持します。この設定は、パケットをランタイムメモリに保持する必要がある場合にキューサイズが長くなると、Citrix ADC メモリに影響します。

これは、ネットワークの種類とアプリケーション特性に基づいて最適化されたレベルで維持する必要があります。

TCP 再構成キュー制限ヒットインジケータを使用すると、TCP 接続上のアウトオブオーダーパケットが、設定されたアウトオブオーダーパケットキューサイズを超えているかどうかを確認できます。

[**TCP** 再構成キュー制限ヒット] タブをクリックして、問題の詳細を表示します。



問題のトラブルシューティングに 推奨される対処方法は次のとおりです。

- トラフィックを確認し、攻撃の場合は、送信元をブロックリストに追加します
- これが予想されるネットワーク動作の場合は、TCP プロファイルのアウトオブオーダーパケットサイズ値を更新します。詳しくは、「TCP 最適化」を参照してください。
- 一時的なネットワークグリッチであれば、それ以上の操作は必要ありません

[詳細] では、次の項目を表示できます。

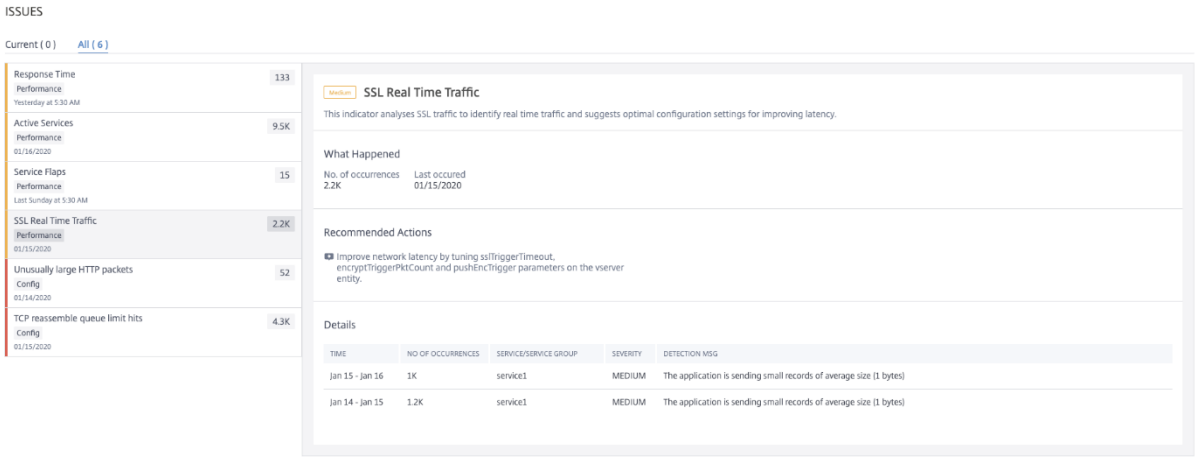
- 異常発生した時間
- 総発生数
- 低、中、高などの異常の重症度
- 現在の TCP プロファイルと OOQSize 設定を示す検出メッセージ

SSL リアルタイムトラフィック

July 7, 2020

Citrix ADC インスタンスでは、SSL トラフィックを処理するために SSL プロファイルを使用できます。SSL プロファイルは、仮想サーバ、サービス、およびサービスグループの特定の SSL パラメータで構成されます。**SSL Real Time Traff** ic インジケータは、SSL トラフィックを分析してリアルタイムトラフィックを識別し、遅延を改善するための最適な構成設定を提案します。

[**SSL** リアルタイムトラフィック] タブをクリックして、問題の詳細を表示します。



この問題をトラブルシューティングするための 推奨処置は、SSL パラメータを更新してネットワークの遅延を改善することです。詳しくは、「グローバル SSL パラメータ」を参照してください。

[詳細] では、次の項目を表示できます。

- 異常発生した時間
- サービス/サービスグループ名
- 低、中、高などの異常の重症度
- アプリケーションの現在の設定を含む検出メッセージ

アプリケーションセキュリティダッシュボード

May 7, 2021

App Security ダッシュボードには、検出済みまたはライセンス済みアプリケーションのセキュリティメトリックの概要が表示されます。このダッシュボードには、同期攻撃、スモールウィンドウ攻撃、DNS フラッド攻撃など、検出/ライセンスされたアプリケーションのセキュリティ攻撃情報が表示されます。

アプリのセキュリティダッシュボードでセキュリティメトリックを表示するには、次の操作を行います。

1. 「アプリケーション」>「アプリケーションセキュリティダッシュボード」に移動します。
2. [Instance] リストからインスタンスの IP アドレスを選択します。

   このレポートには、アプリケーション別に次の情報が含まれています。

   - 脅威インデックス。アプリケーションに対する攻撃の重要度を示す 1 桁の評価システム。アプリケーションに対する攻撃の重大度が高いほど、そのアプリケーションの脅威指数は大きくなります。値の範囲は 1 ～7 です。

     脅威指数は攻撃情報に基づいています。違反の種類、攻撃カテゴリ、場所、クライアントの詳細などの攻撃関連の情報は、アプリケーションに対する攻撃の洞察を提供します。違反情報は、違反または攻撃

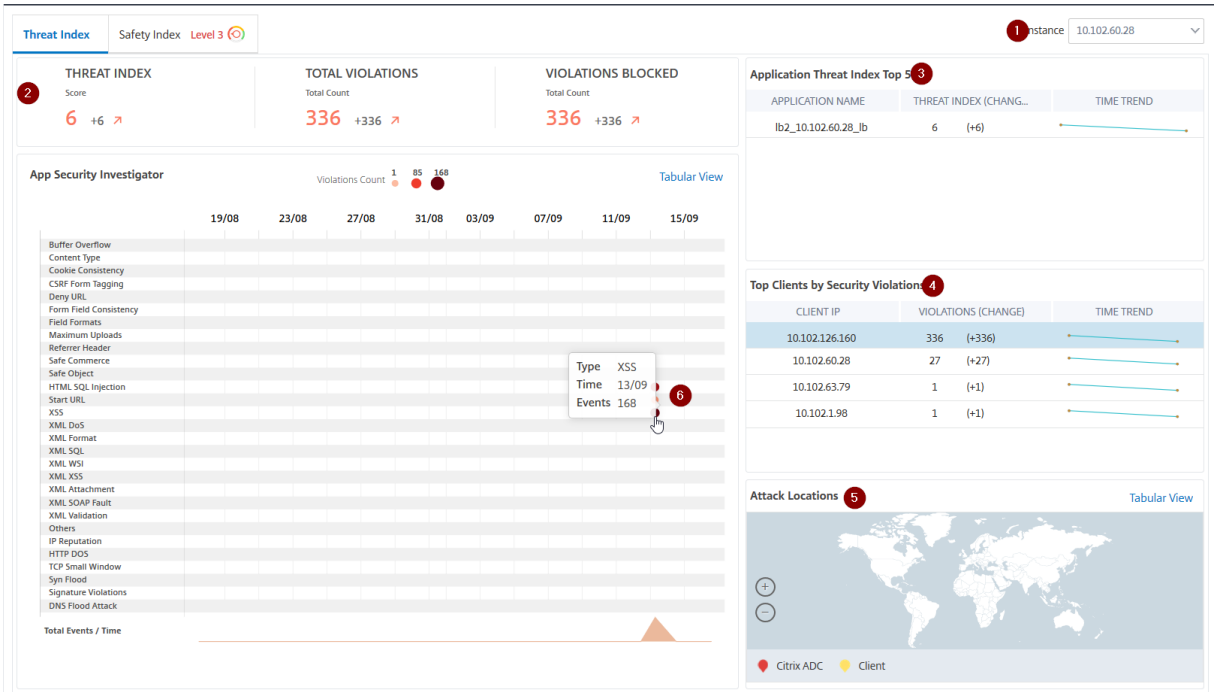
が発生した場合にのみ Citrix ADM に送信されます。多くの侵害や脆弱性は、高い脅威指数の値につながります。

- 安全指数。外部からの脅威や脆弱性からアプリケーションを保護するために、Citrix ADC インスタンスをどのように安全に構成したかを示す 1 桁の評価システム。アプリケーションのセキュリティリスクが小さいほど、安全性指数は高くなります。値の範囲は 1 ～7 です。

  安全指標では、アプリケーションファイアウォール構成と Citrix ADC システムセキュリティ構成の両方が考慮されます。高い安全性指数値を得るためには、両方の構成を堅牢にする必要があります。たとえば、アプリケーションのファイアウォールの厳格なチェックが行われていても、nsroot ユーザーに強力なパスワードなどの Citrix ADC システムのセキュリティ対策が提供されていない場合、アプリケーションには低い安全性インデックス値が割り当てられます。

App Security Investigator で報告された不一致を表示できます。

脅威インデックスの詳細



1 -詳細を表示できる Citrix ADC インスタンスの IP アドレスが表示されます。

2 -脅威インデックスのスコア、発生した違反合計、ブロックされた違反合計などの詳細を表示します。

3 -選択したインスタンスの仮想サーバーを表示します。

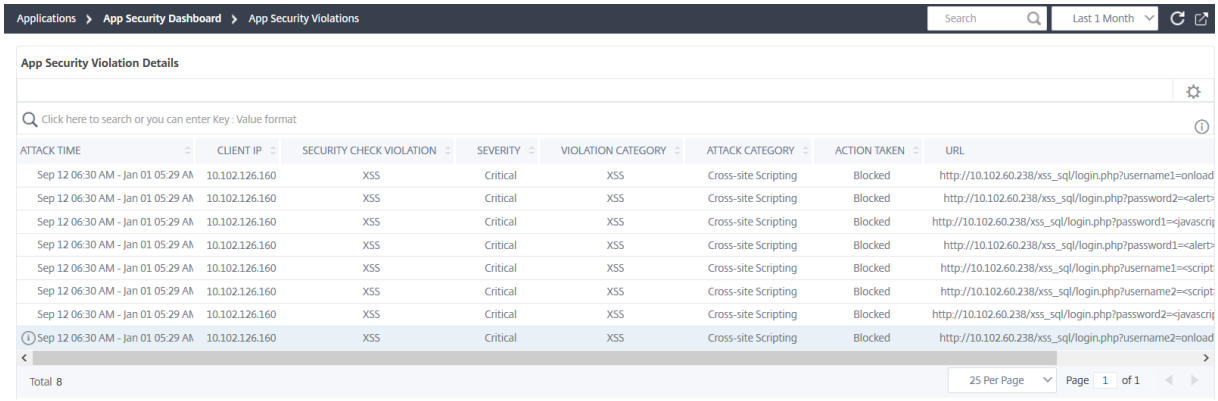
4 -クライアントに基づいてセキュリティ違反を表示します。アプリケーションセキュリティ調査者のグラフは、クライアントごとに表示されます。各クライアント IP をクリックすると、結果を表示できます。

5 -違反をマップビューと表形式で表示します。

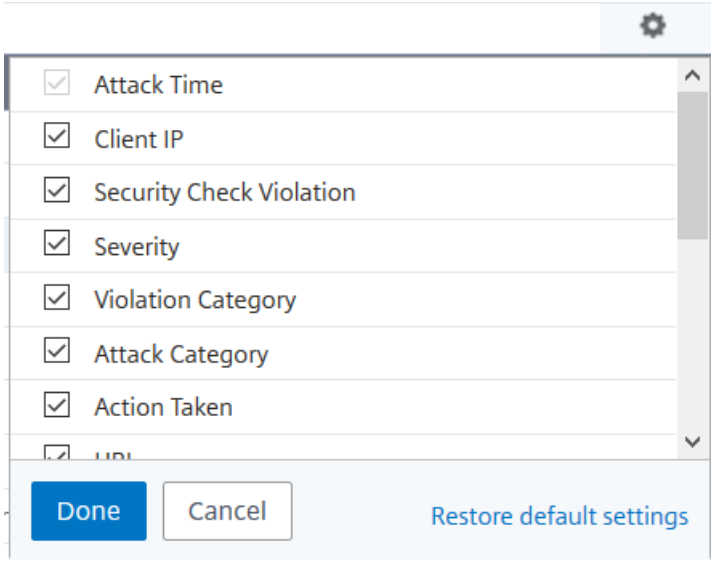
6 -違反の詳細を表示します。グラフ上にマウスポインタを置くと、違反の種類、攻撃時間、合計イベントなどの詳細が表示されます。

バブルグラフをクリックすると、詳細が [アプリセキュリティ違反の詳細] ページに表示されます。たとえば、クロスサイトスクリプト違反の詳細をさらに表示する場合は、[**App Security Investigator**] で **XSS** に設定されたグラフをクリックします。

[アプリのセキュリティ違反の詳細] には、攻撃時間、攻撃カテゴリ、重大度、URL などの違反の詳細が表示されます。



[設定] オプションをクリックして、表示させるオプションを選択することもできます。



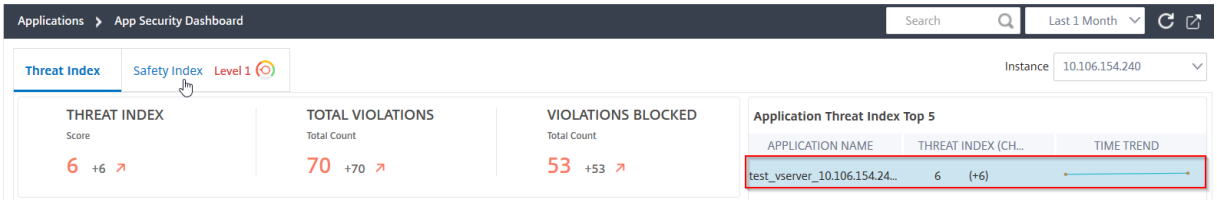
安全指数の詳細

アプリケーションの脅威への露出度を確認したら、そのアプリケーションに設定されているセキュリティ構成と欠落しているセキュリティ構成を確認します。この情報は、アプリケーション安全指数のサマリーにドリルダウンして取得できます。

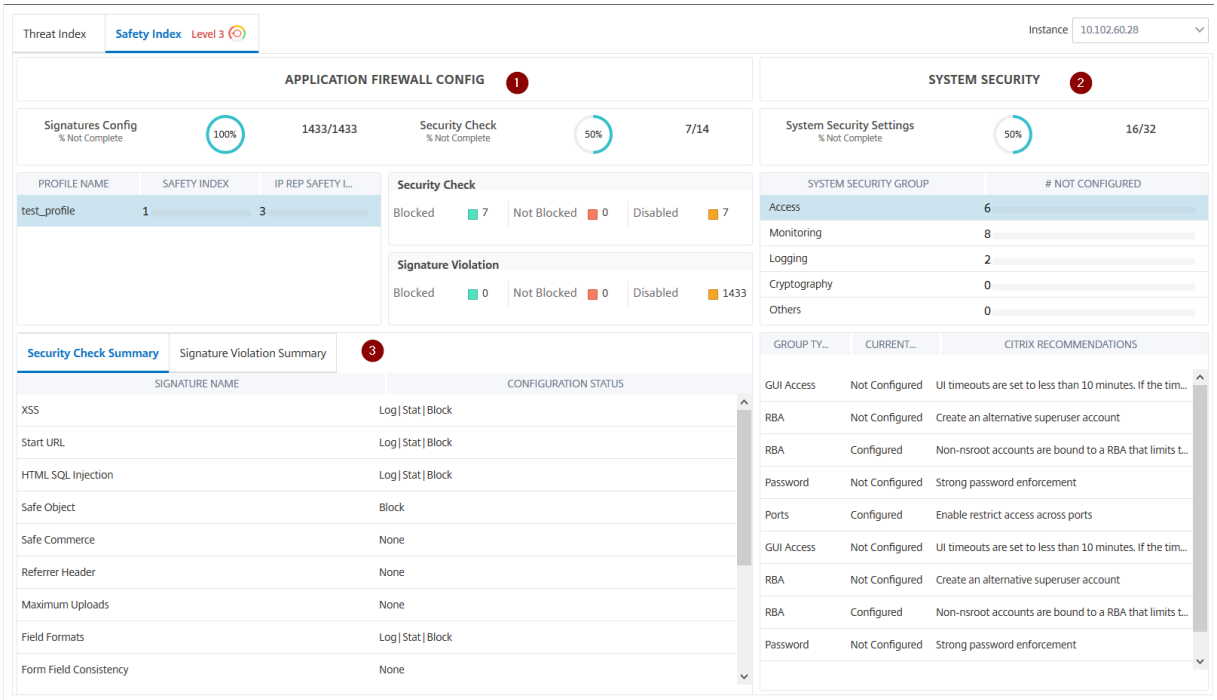
安全性指数概要には、次のセキュリティ構成の有効性に関する情報が表示されます。

- アプリケーションファイアウォールの設定。構成されていないシグネチャおよびセキュリティエンティティの数を表示します。
- **Citrix ADM** システムセキュリティ。構成されていないシステムセキュリティ設定の数を表示します。

安全指数の詳細を表示するには、仮想サーバーまたはアプリケーションを選択し、[安全指数] タブをクリックします。



詳細が表示されます。



1 -アプリケーションファイアウォールの設定の詳細情報を表示します。

2 -システムセキュリティの詳細情報を表示します。各セキュリティグループをクリックすると、ステータスと Citrix 推奨の詳細が表示されます。

3 -セキュリティチェックと署名違反のサマリーを表示します。

仮想サーバーのSecurity Insightを有効にしてから［**Analytics**］>［**Security Insight**］に移動して、脅威環境の概要を表示することもできます。安全指数のユースケースについて詳しくは、Security Insightを参照してください。

API Gateway

May 7, 2021

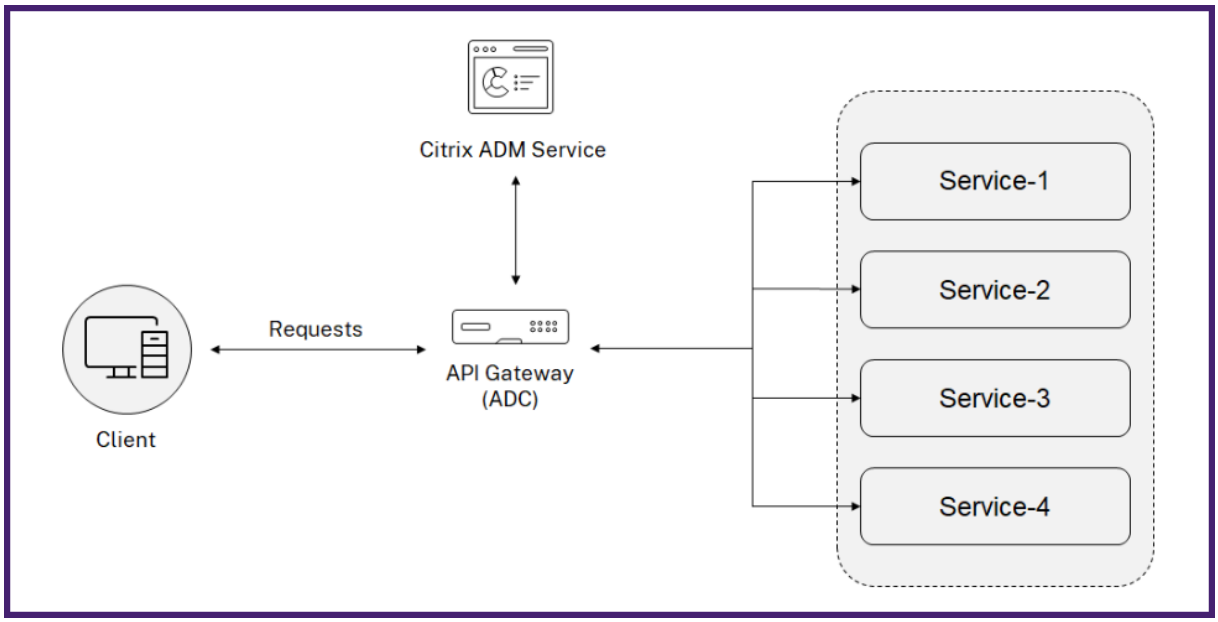
API ゲートウェイは、API エンドポイントへのすべてのリクエストのエントリポイントとして機能します。また、システム内のすべての API エンドポイントとマイクロサービスへの安全で信頼性の高いアクセスを保証します。

API ゲートウェイは、API クライアント/アプリケーション、およびバックエンド API サービス間のすべてのリクエストと応答をプロキシします。API エンドポイントの構成、管理、セキュリティ保護に役立ちます。次のいずれかの方法で API 定義を作成および管理することもできます。

- Swagger OAS 仕様ファイルのアップロード
- 独自の API 定義を作成する

詳しくは、「API 定義を作成またはアップロードする」を参照してください。

次の図は、API ゲートウェイがクライアント要求を受信し、バックエンド API サービスから応答を送信する方法を示しています。



> 注:
>
> Citrix Application Delivery Management では、この機能は Premium または Advanced ライセンスを持っているユーザーが利用できます。

API ゲートウェイの利点

API ゲートウェイには、次の利点があります。

- **API** エンドポイントを保護する: API ゲートウェイはセキュリティレイヤーを追加し、API エンドポイントとバックエンド API サーバーを次のような攻撃から保護します。

  - バッファオーバーフロー
  - SQL インジェクション
  - クロスサイトスクリプティング
  - サービス拒否 (DoS)

- **API** パフォーマンスの監視と向上: API ゲートウェイは、SSL オフロード、認証、認可、レート制限などのサービスを提供します。これらのサービスは、API のパフォーマンスと可用性を向上させます。

  API 分析により、API パフォーマンスメトリックスと API エンドポイントに対する脅威を可視化できます。詳しくは、「API アナリティクスの表示」を参照してください。

- **API** トラフィックを管理します。API ゲートウェイは、バックエンド API インフラストラクチャの複雑さを抽象化します。

- **API** エンドポイントの検出: API ゲートウェイは組織内の API エンドポイントを検出し、[**API Discovery**] ページに追加します。

API ゲートウェイの管理

管理者は、API 定義を作成し、Citrix ADM API ゲートウェイ（ADC）に API インスタンスをデプロイできます。詳しくは、次のトピックを参照してください:

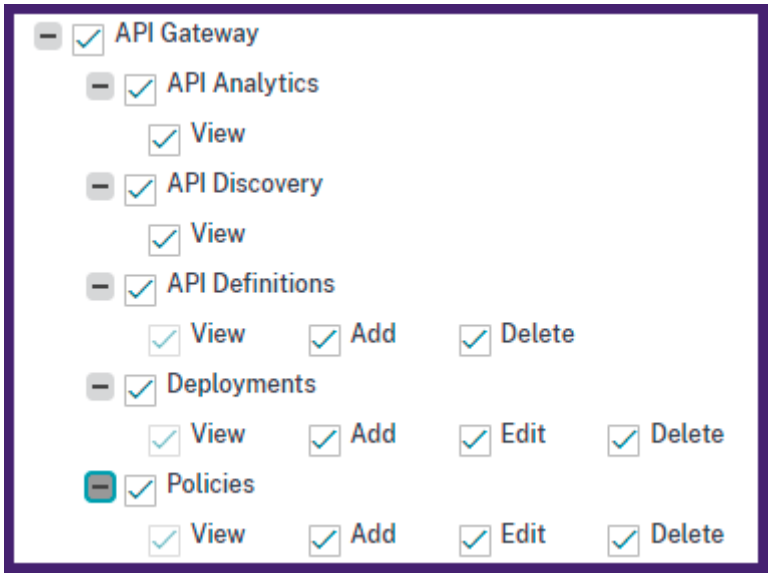
- API 定義を追加する
- API インスタンスのデプロイ

API ゲートウェイでは、セキュリティポリシーを適用できます。API ポリシーの作成方法については、「API デプロイへのポリシーの追加」を参照してください。

API ゲートウェイの設定と管理権限の付与

管理者は、アクセスポリシーを作成して、API ゲートウェイの設定と管理に対するアクセス許可をユーザーに付与できます。ユーザー権限は、表示、追加、編集、および削除できます。アクセス許可を付与するには、次の操作を実行します。

1. [アカウント**] > [**ユーザー管理**] > [**アクセスポリシー] に移動します。
2. [追加] をクリックします。
3. **[** アクセスポリシーの作成] で、ポリシーの名前と説明を指定します。
4. [アクセス許可] フィールドで、[アプリケーション]、[**API** ゲートウェイ] の順に展開します。
5. 必要な **API** ゲートウェイページを選択します。次に、付与するアクセス許可を選択します。



> 重要
>
> API ゲートウェイを使用するために必要な機能に対するアクセス許可を必ず付与してください。たとえば、[**Deployments**] ページへのユーザーアクセスを許可する場合、次の機能にもユーザーアクセスが必要です。
>
> - StyleBook
> - IPAM
> - 負荷分散 ([ネットワーク機能] の下)
> - コンテンツスイッチング（ネットワーク機能下）
> - デバイス API プロキシ (**API** の下)

アクセスポリシーの詳細については、「ADM でのアクセスポリシーの設定」を参照してください。

API アナリティクスの表示

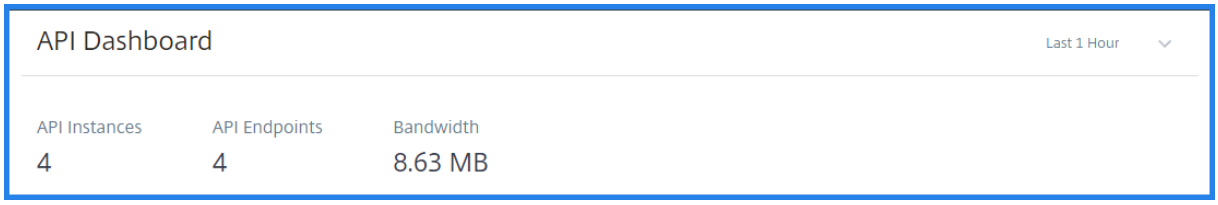
May 7, 2021

API 分析により、API トラフィックを可視化できます。この分析により、IT 管理者は API ゲートウェイによって提供される API インスタンスおよびエンドポイントを監視できます。これは、API リクエストの統合された定期的な監視を提供します。

API 分析を監視する前に、次のことを必ず完了してください。

1. API 定義を追加する
2. API 定義のデプロイ
3. API 定義へのポリシーの追加
4. API インスタンスへのライセンスの適用
5. API インスタンスで Web Insight を有効にする

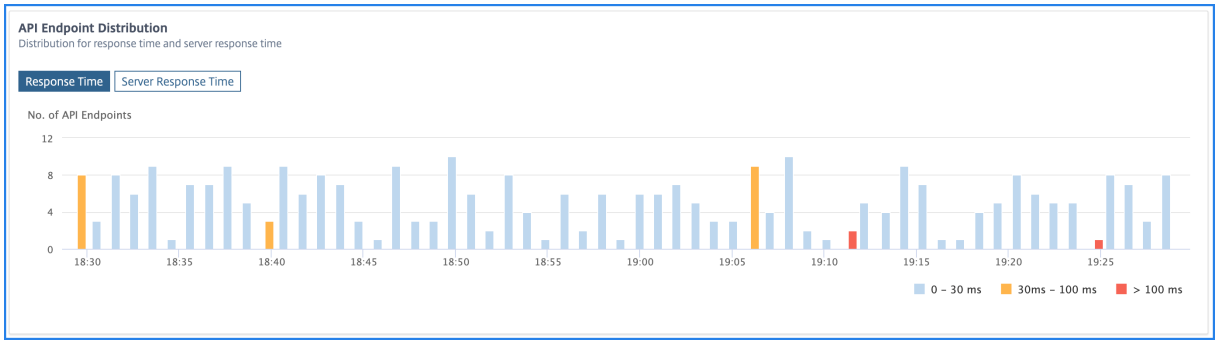
API Analytics では、API 定義の一部として追加された API インスタンスおよびエンドポイントの応答時間を監視できます。また、API インスタンスおよびエンドポイントによって消費された帯域幅も表示されます。



デフォルトでは、ダッシュボードには過去 1 時間の API 分析が表示されます。期間を選択して、その間隔の API 分析を表示できます。リスト全体を表示するには、各タイルの [詳細を表示] をクリックします。このビューでは、[地理的場所] タイルを除く名前の一部で API インスタンスとエンドポイントを検索できます。

API エンドポイントの配布

このグラフには、API エンドポイントのアプリケーションとサーバーの応答時間の分布が表示されます。応答時間が長い API エンドポイントを特定し、必要なアクションを実行できます。

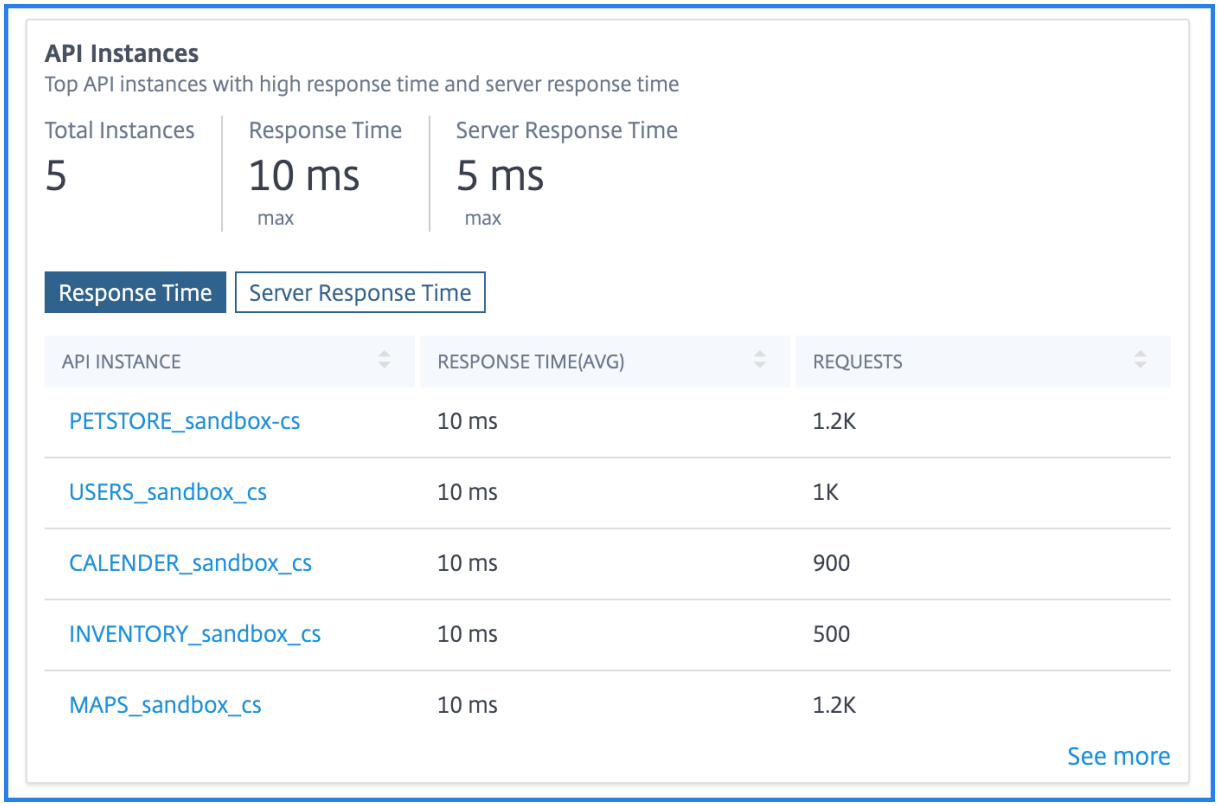


API エンドポイントは、応答時間の制限に応じて、次のいずれかの色で表示されます。

- 青：応答時間が 30 ミリ秒未満の場合。
- オレンジ：応答時間が 30 ～100 ミリ秒の間にある場合。
- 赤：応答時間が 100 ミリ秒を超える場合。

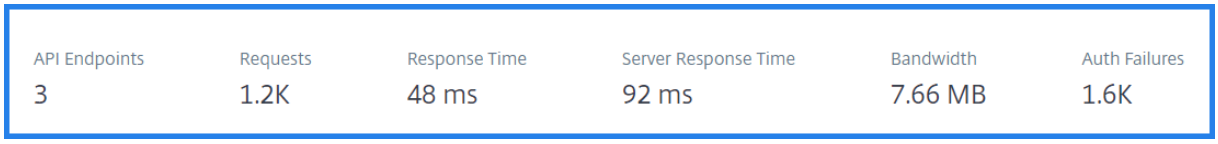
API インスタンス

[**API Instances**] タイルには、アプリケーションとサーバーの応答時間が長い上位 API インスタンスが表示されます。



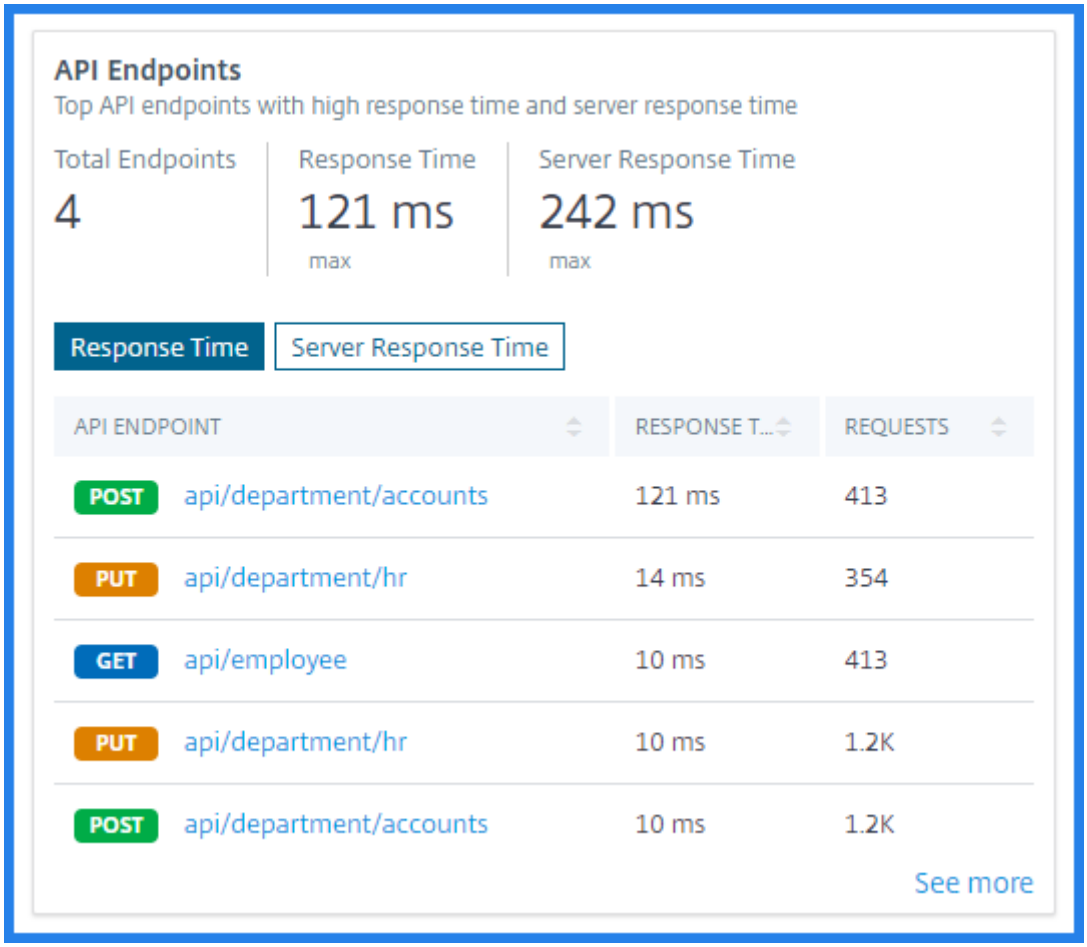
API インスタンスを選択し、パフォーマンス、使用状況、セキュリティの詳細を表示します。選択した API インスタンスには、次の情報が表示されます。

- API エンドポイント数
- リクエスト数
- アプリケーションとサーバーの応答時間
- 消費された帯域幅
- 認証の失敗



API エンドポイント

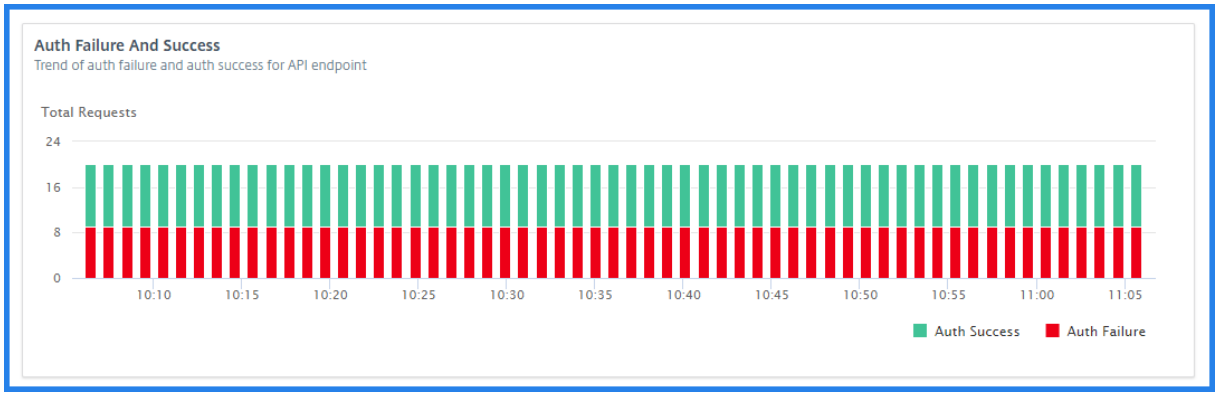
[**API Endpoints**] タイルには、アプリケーションとサーバーの応答時間が長い最上位のエンドポイントが表示されます。



API エンドポイントを選択して、パフォーマンス、使用状況、セキュリティの詳細を表示します。

認証の失敗

[**Auth Failures**] タイルには、認証に失敗した上位の API エンドポイントが表示されます。認証の失敗または成功は、API 定義に追加されたポリシーに基づいて発生します。



API エンドポイントで認証失敗と成功率を表示するには、次の手順を実行します。

1. [**API** エンドポイント] からエンドポイントを選択します。
2. [セキュリティ] タブを選択します。このタブには、選択したエンドポイントの認証失敗と成功が表示されます。

インスタンスの API エンドポイントで認証失敗と成功率を表示するには、次の手順を実行します。

1. [**API** インスタンス] からインスタンスを選択します。
2. [セキュリティ] タブを選択します。このタブには、選択したインスタンスのエンドポイントにおける認証の失敗と成功が表示されます。

さまざまな **API** インサイトを表示する

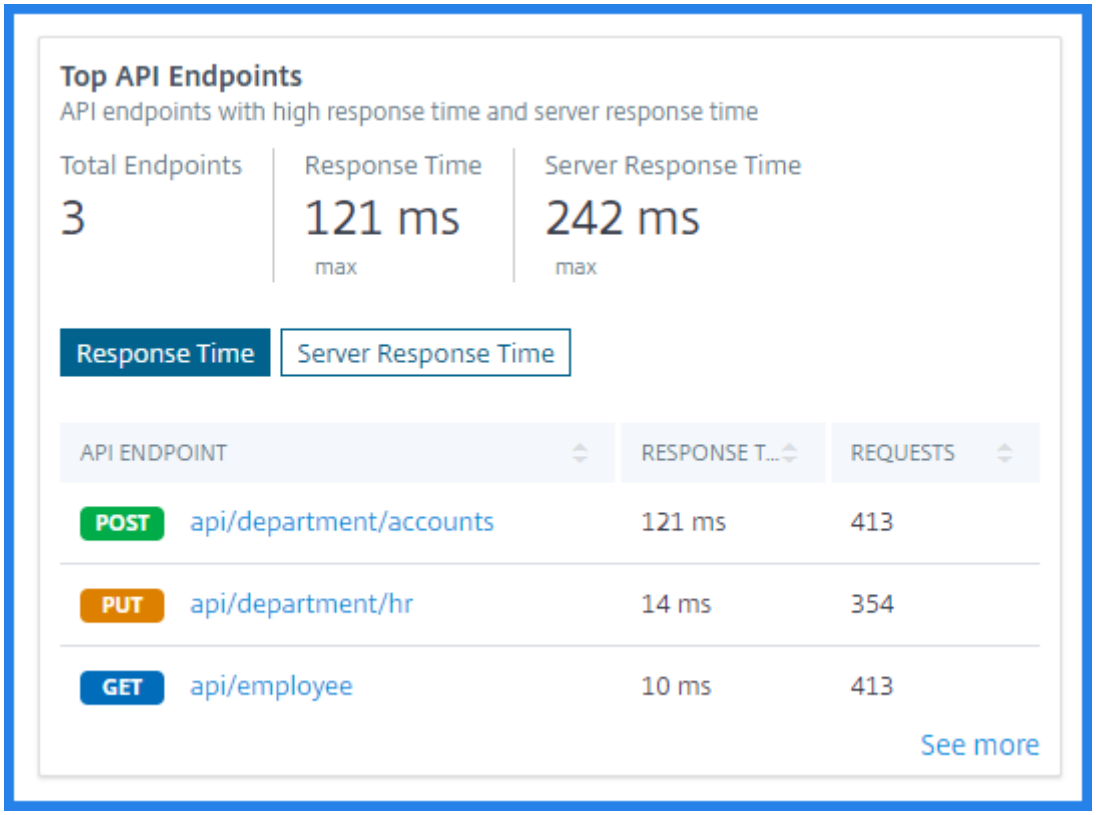
API Analytics をナビゲートして、以下に関する特定の情報を表示します。

- インスタンスの上位 API エンドポイント
- アクセス頻度の高い API
- エンドポイントの地上位置
- HTTPS 応答ステータス
- API リクエストの傾向
- エンドポイントの帯域幅消費
- SSL エラーと使用法

インスタンスの上位 **API** エンドポイントを表示する

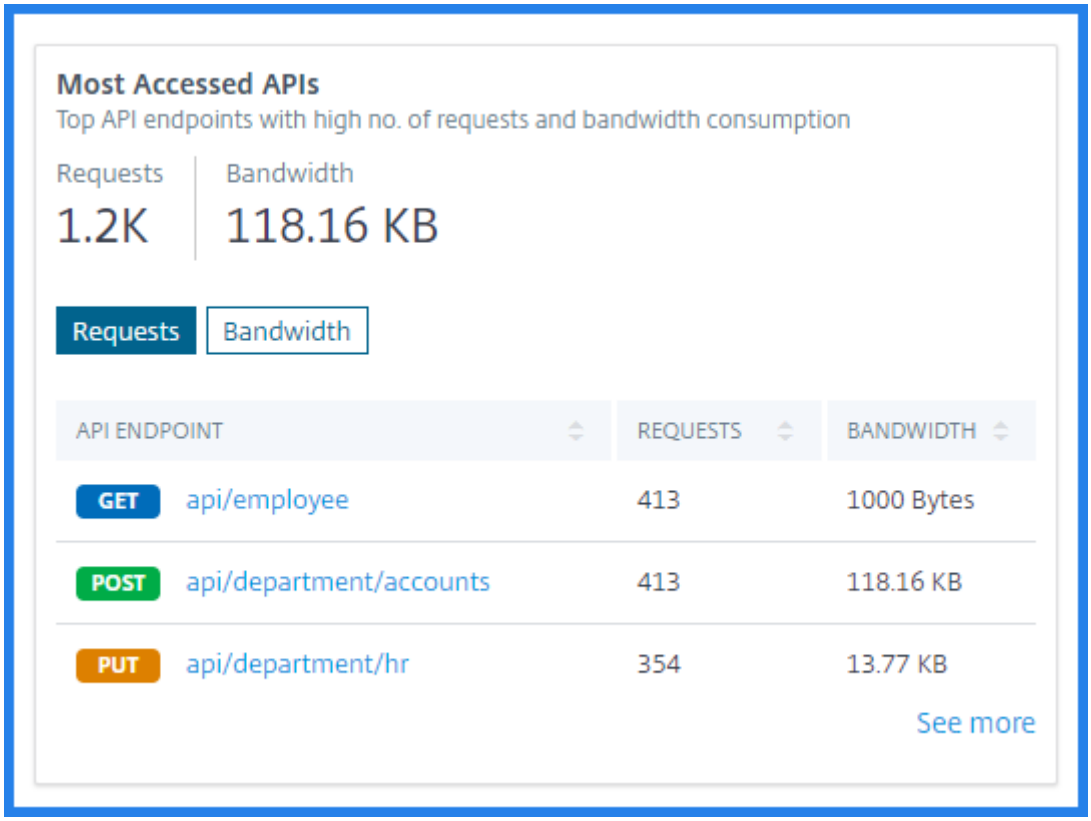
[**API Analytics**] ページには、応答時間が長い上位のエンドポイントが表示されます。インスタンスの類似エンドポイントを表示するには、[**API Instances**] からインスタンスを選択します。

[上位 **API** エンドポイント] タイルには、アプリケーションとサーバーの応答時間が長いエンドポイントが表示されます。



最もアクセスされた **API** を表示する

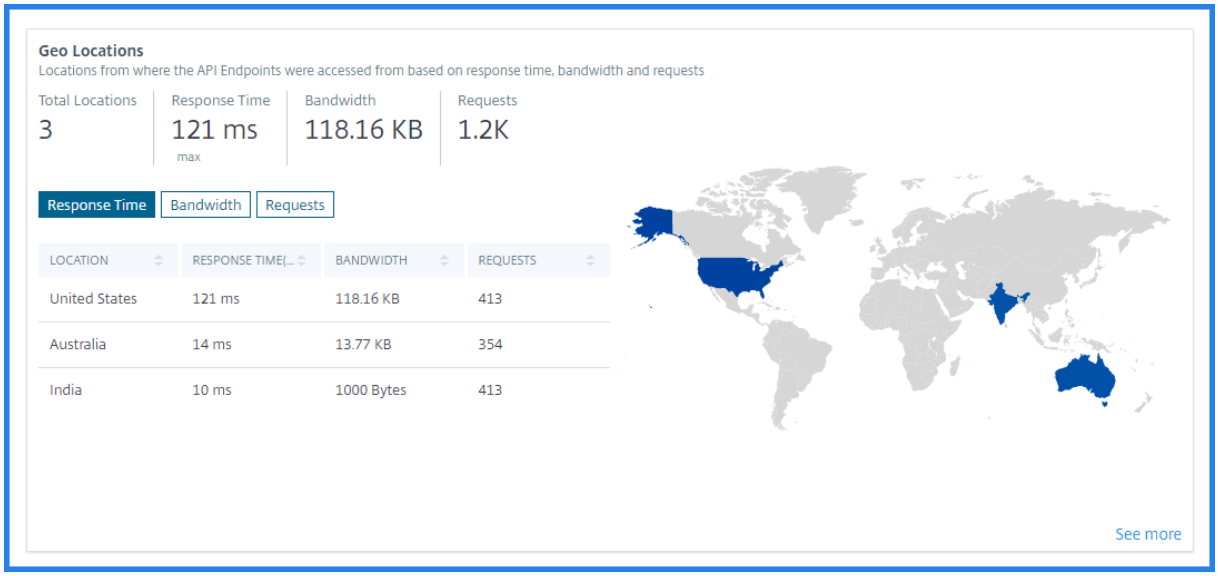
[**API** 分析] で、API インスタンスから API インスタンスを選択します。[最もアクセスされた **API**] タイルには、より多くの要求と帯域幅を持つ上位エンドポイントが表示されます。



エンドポイントの地情報の表示

1. [**API** 分析] で、次のいずれかを選択します。
   - [**API Instances]** からインスタンスを選択し、選択したインスタンスのエンドポイントがリクエストを受信した場所を表示します。
   - [**API Endpoints]** からエンドポイントを選択し、エンドポイントがリクエストを受信した場所を表示します。
2. [パフォーマンスと使用法] に、[地理的位置] タイルが表示されます。

   応答時間、帯域幅、要求に基づいて場所を並べ替えることができます。

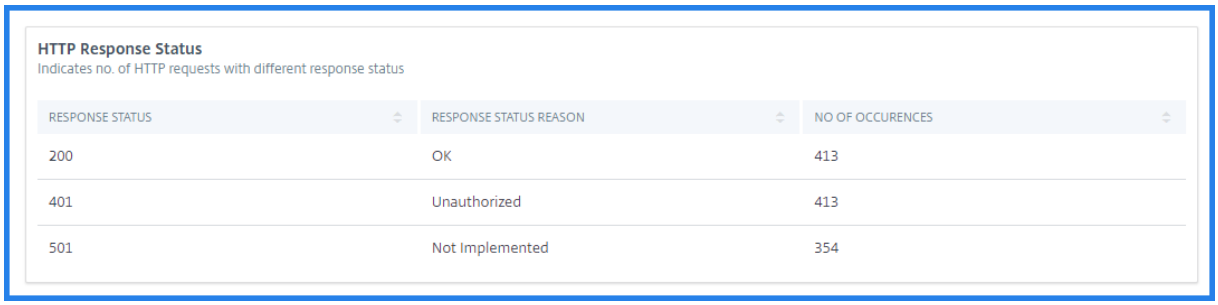


HTTPS 応答ステータスの表示

[**HTTPS** 応答ステータス] タイルには、応答ステータスとその理由と発生状況が表示されます。HTTPS 応答ステータスは、次のいずれかの方法で表示できます。

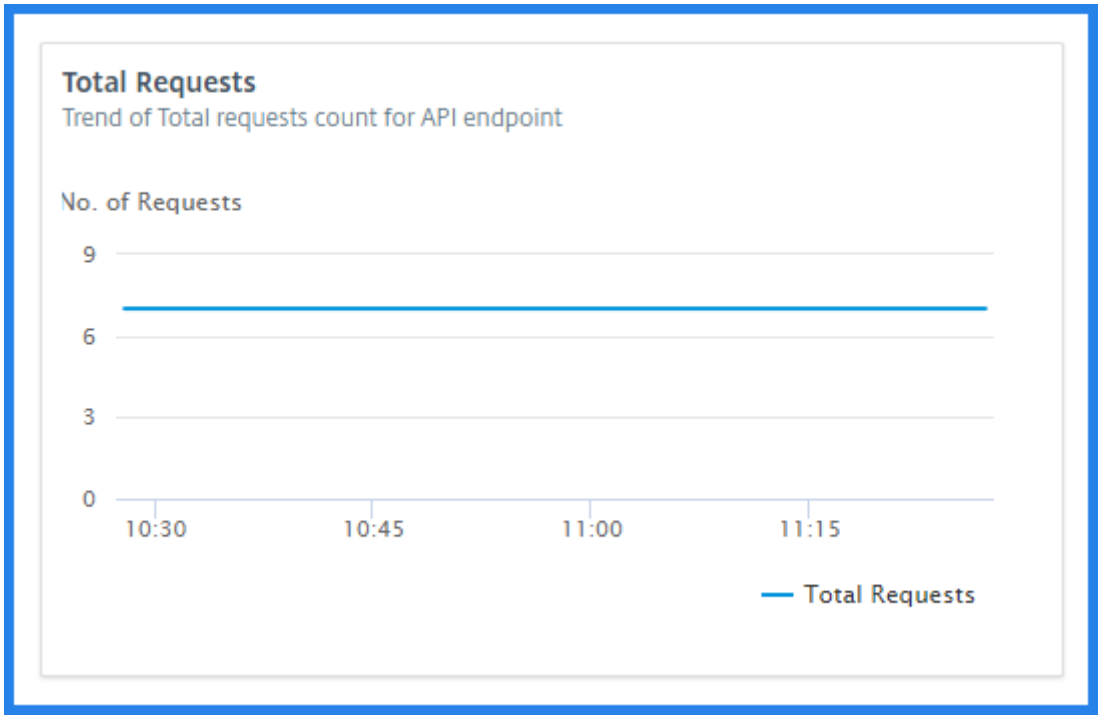
- [**API** インスタンス] からインスタンスを選択します。
- [**API** エンドポイント] からエンドポイントを選択します。

このタイルは、[パフォーマンスと使用状況] タブに表示されます。

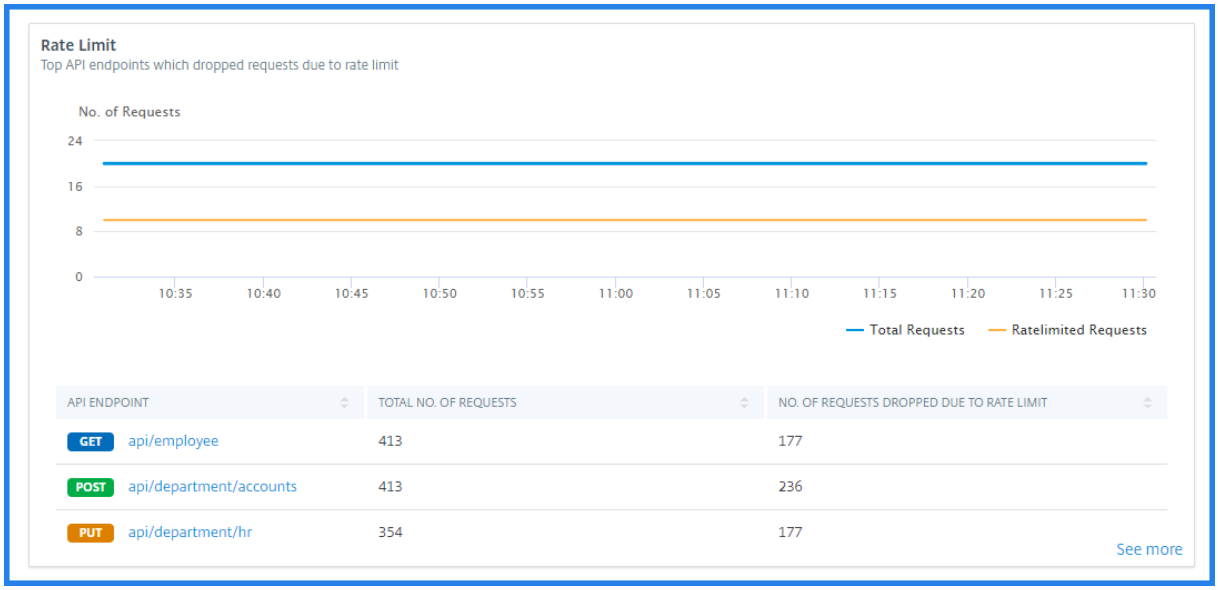


API リクエストの傾向の表示

[**API** エンドポイント] からエンドポイントを選択します。[パフォーマンスと使用状況] の [合計リクエスト数] タイルには、エンドポイントが受信したリクエスト数の合計の傾向が表示されます。



レート制限のために削除されたリクエストの傾向を表示するには、[**API Instances]** からインスタンスを選択します。[セキュリティ] の [レート制限] タイルには、削除された要求の傾向が表示されます。また、エンドポイントが受信したリクエストの合計の傾向も表示されます。



この比較により、合計リクエスト間のレート制限が原因でドロップされるリクエストの数を判断できます。

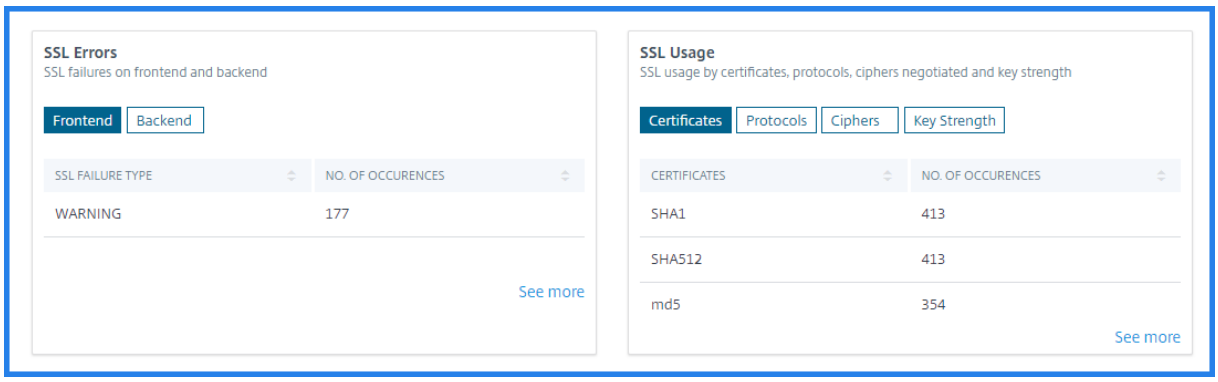
エンドポイントの帯域幅消費の表示

エンドポイント別の帯域幅消費傾向を表示するには、API エンドポイントからエンドポイントを選択します。[**Bandwidth**] タイルには、帯域幅消費グラフが表示されます。

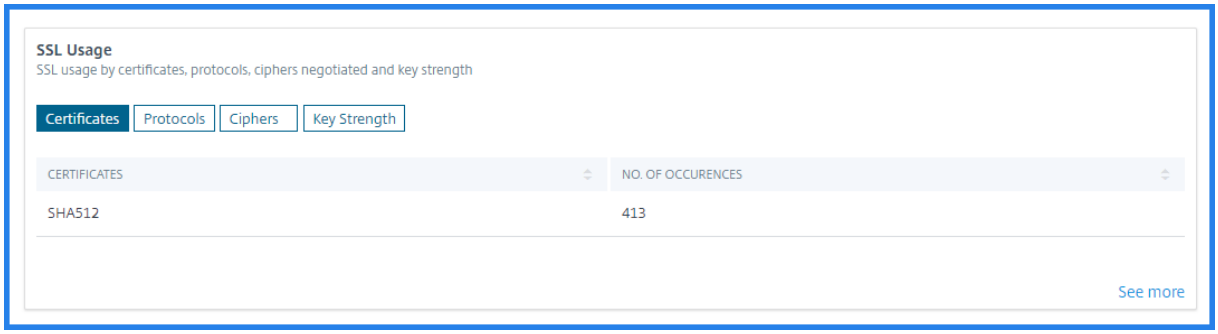
SSL エラーと使用状況を表示する

[**API** インスタンス] からインスタンスを選択します。[セキュリティ] には、次のタイルが表示されます。

- 「**SSL** エラー」— クライアントおよびアプリケーションサーバーで発生した SSL エラーを表示します。
- [**SSL Usage**]: SSL 証明書、プロトコル、暗号、およびキーの強度をそれぞれ表示します。



エンドポイントでの SSL の使用状況を表示するには、API エンドポイントからエンドポイントを選択します。[セキュリティ] タブに [**SSL** 使用] タイルが表示されます。



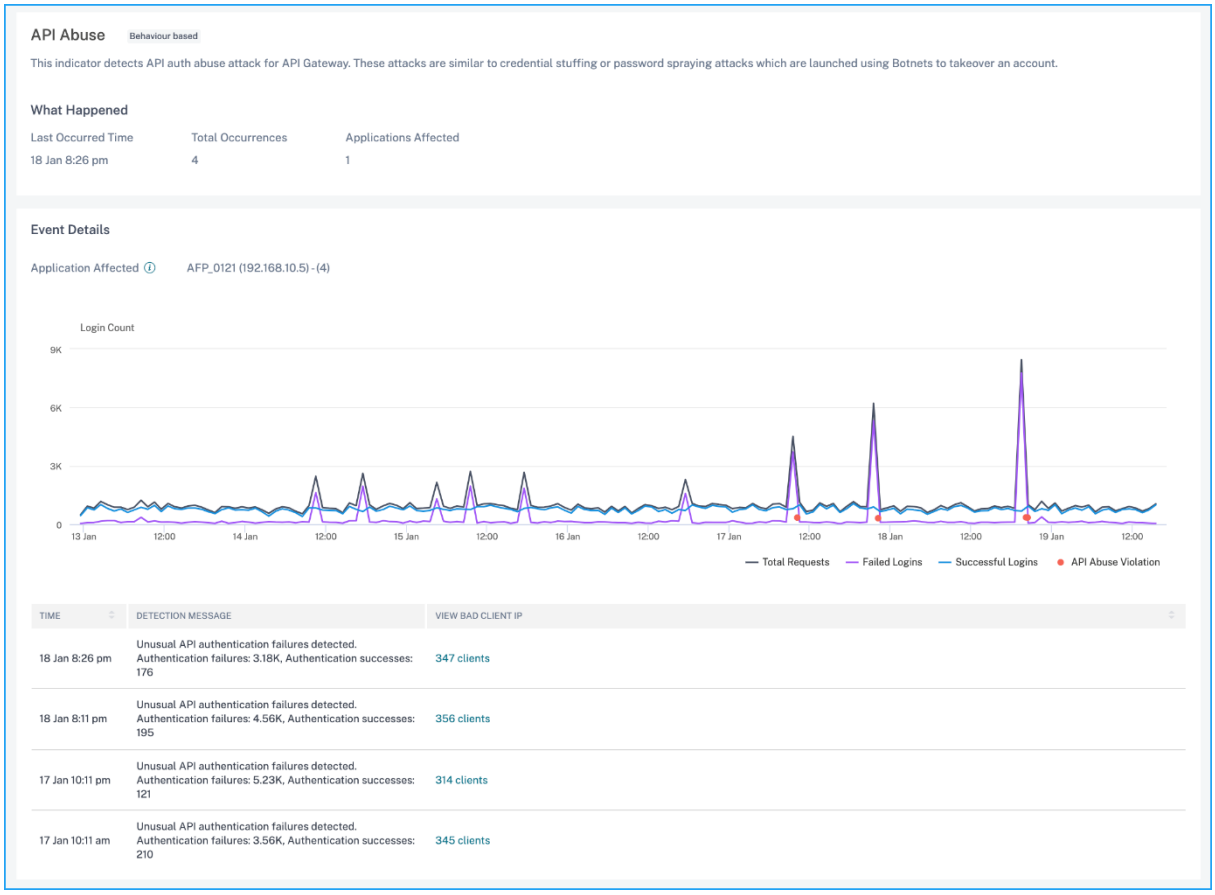
API セキュリティ違反の表示

Citrix ADM は、API ゲートウェイのセキュリティ違反を表示します。セキュリティの脅威は、ネットワーク、WAF、または Bot からのものです。この情報を使用して、インスタンスをセキュリティで保護するための適切なアクションを実行できます。ADM GUI には、次の API セキュリティ違反が表示されます。

API 乱用

不正なボットは、API 認証を使用または盗み、資格情報の詰め込みやパスワードスプレーなどのさまざまな種類のサイバー攻撃を実行できます。Citrix ADM では、API のこのような異常なログオンアクティビティを分析できます。

API 不正使用インジケータを使用して、管理者として API 認証を使用して、不正なボットがターゲットリソースを引き継ぐことを試みたかどうかを分析できます。

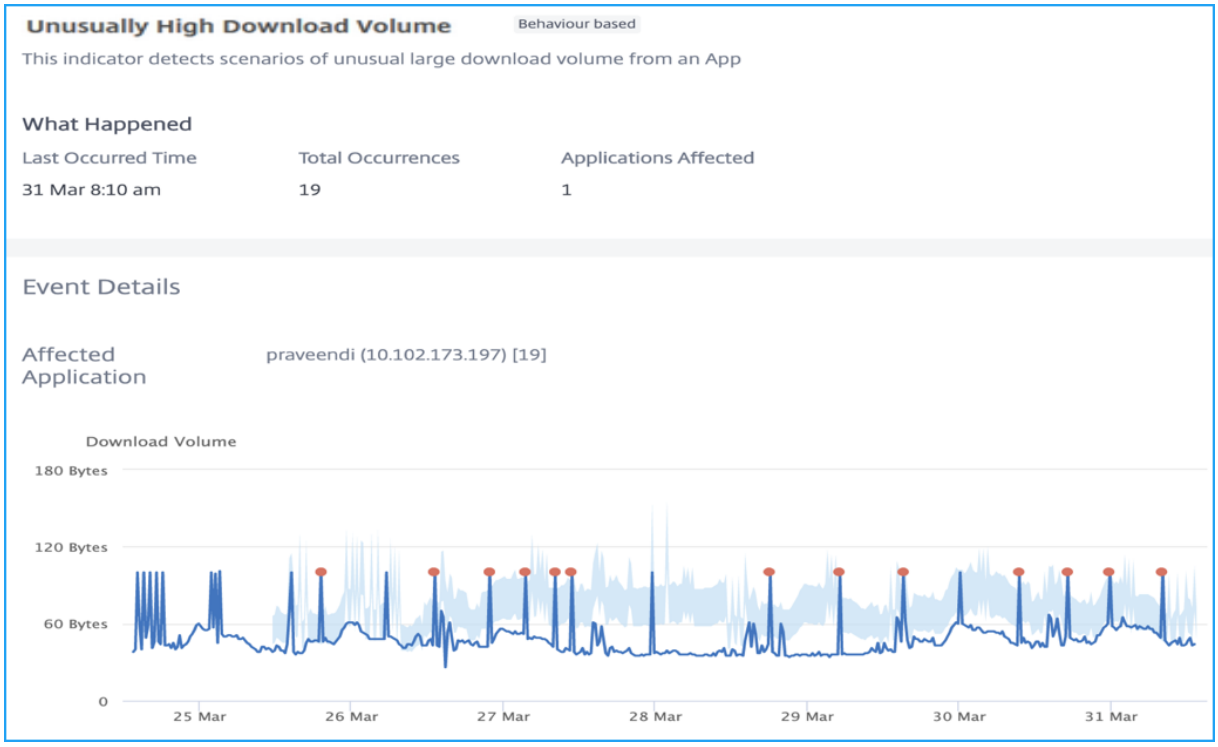


詳しくは、「API 乱用」を参照してください。

過度なデータ消失の危険性

API エンドポイントは、クライアント要求に対する応答が大きい場合があります。この状態は、過剰なデータ消失と呼ばれます。攻撃者は、このような抜け穴を特定して、エンドポイントからより多くの情報を取得することができます。

Citrix ADM では、通常よりも大きい応答サイズを分析できます。また、過剰なデータ漏洩を防ぐために、適切なアクションを実行することもできます。ADM GUI では、このような違反が [異常に高いダウンロードボリューム] インジケータの下に表示されます。影響を受けるエンドポイントからの過剰なデータ消失を分析し、適切なアクションを実行できます。



詳しくは、「ダウンロードボリュームが異常に高い」を参照してください。

API 定義を作成またはアップロードする

May 7, 2021

API 定義は、OpenAPI 仕様規格（Swagger 2.0、OpenAPI 3.0.x）を用いて API を記述した文書である。この定義には、API リソースパスとそれらを操作するメソッドを含めることができます。API 定義を ADM に追加し、API ゲートウェイ（Citrix ADC）に展開できます。

API 定義は、次のいずれかの方法で作成できます。

- Swagger OAS 仕様ファイルのアップロード
- 独自の API 定義を作成する

> 注:
>
> 現在、ADM は **Swagger 2.0** または **openapi 3.0.1** を使用する OAS 仕様ファイルの解析をサポートしています。

OAS 仕様をアップロードする

OAS 仕様は ADM GUI にアップロードできます。

1. 「アプリケーション」**>**「**API Gateway**」**>**「**API** 定義」に移動します。
2. ［追加］をクリックします。
3. 「**OAS** 仕様のアップロード」を選択します。

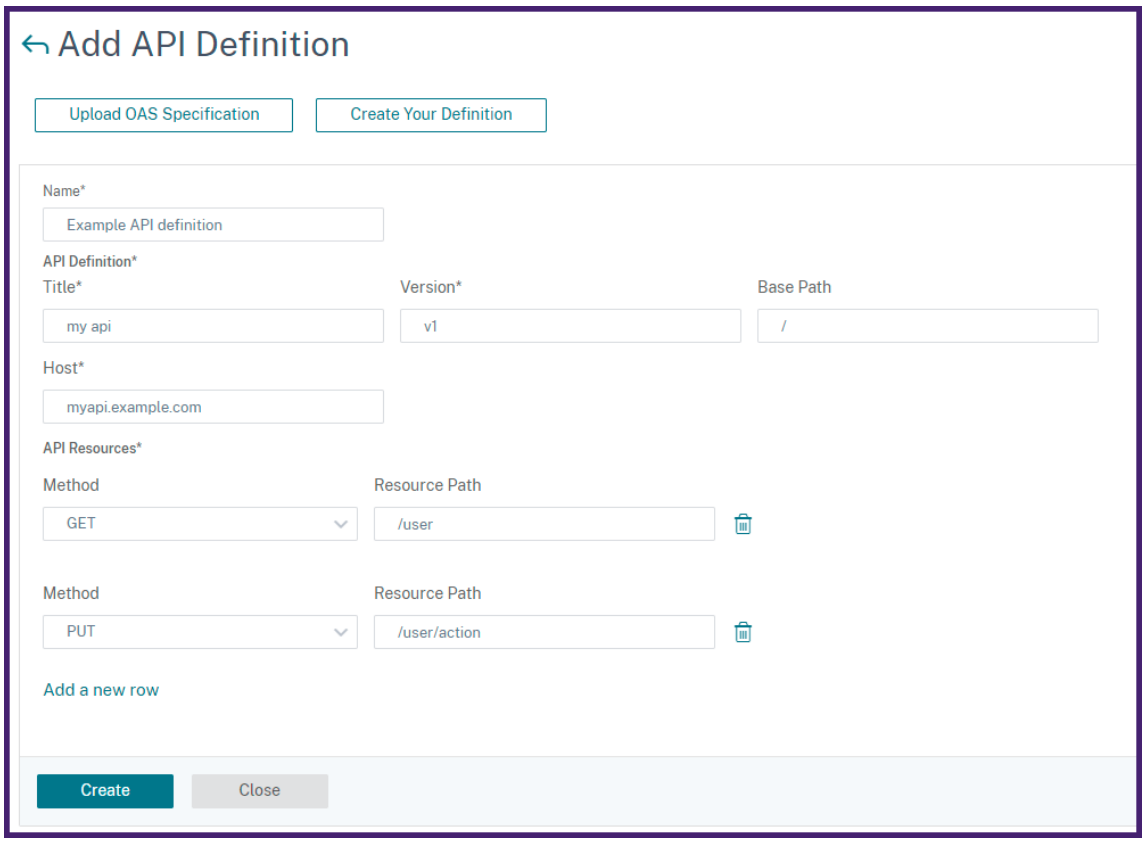
   > 注**:**
   >
   > OAS 仕様ファイルが YAML または JSON 形式であることを確認します。また、このファイルに外部参照を含めることはできません。現在、ADM は Swagger バージョン 2.0 をサポートしています。

4. ローカルコンピュータから OAS 仕様を参照し、ADM にアップロードします。

API 定義を作成する

ADM GUI で独自の API 定義を作成できます。

1. 「アプリケーション」**>**「**API Gateway**」**>**「**API** 定義」に移動します。
2. ［追加］をクリックします。
3. [定義を作成] を選択し、次の項目を指定します。
   - 名前 -API 定義の名前。
   - **API** 定義 -定義には、タイトル、バージョン、ベースパス、およびホストを含める必要があります。[**Host**] フィールドで、ドメイン名または IP アドレスを指定できます。
   - **API** リソース -定義に複数の API リソースを追加します。各リソースには、パスとサポートされているメソッドがあります。



4. [作成] をクリックします。

API 定義の表示

[**API** 定義] ページには、アップロードされた定義が一覧表示されます。[表示] をクリックして、次の API 定義の詳細を表示します。

- 「名前」-API 定義の名前を表示します。
- 「**API** 定義」**-**定義のタイトル、バージョン、ベースパス、ホストを表示します。
- **API** リソース — API 定義内の API リソースと、それらを操作するためのメソッドを一覧表示します。

次に、この定義を API ゲートウェイにデプロイします。

API インスタンスのデプロイ

May 7, 2021

API インスタンスをデプロイするには、次の手順を実行します。

1. [アプリケーション] **> [API** ゲートウェイ**] > [**配備**]** に移動します。

2. [追加] をクリックします。
3. 「配置の基本情報」で、
   a) 配置名を指定します。
   b) [ターゲット **API** ゲートウェイ] で、API ゲートウェイとして ADC インスタンスを選択します。
   c) 「**API** 定義」で、必要な API 定義を選択します。
   d) [**API** プロキシ] で、API ゲートウェイを使用する API プロキシを追加します。API プロキシは、API ゲートウェイがクライアントからの API トラフィックを受信するフロントエンドの仮想 IP アドレスです。次の詳細を指定します。
      - **IP** アドレス
      - ポート
      - [**TLS** セキュリティプロファイル] — リストから [高] または [中] を選択します。[High] を選択すると、ADC インスタンス上のセキュア SSL プロファイルにマップされます。
      - **TLS** 証明書
      - **TLS** キー

      > 注:
      >
      > TLS 証明書とキーを PEM 形式でアップロードします。

      または、IPAM ネットワークを選択して IP アドレスを割り当てることもできます。IPAM ネットワークから割り当てられた IP アドレスを表示するには、**[**ネットワーク**] > [IPAM**] に移動します。IPAM の詳細については、IPAM の設定を参照してください。
4. [アップストリームサービス] で、[追加] をクリックして、API トラフィックを転送するバックエンド API サーバーを追加します。ドメイン名または IP アドレスを使用して、アップストリームサービスを設定できます。
   a) アップストリームサービスの名前を指定します。
   b) ドメインを指定します。
   c) 「サービス」で、IP アドレスとポート値を指定します。IP アドレスを追加するには、[新しい行の追加] をクリックします。
   d) [追加] をクリックします。
5. [**Routing**] で、リソースパスプレフィックスに基づいて API トラフィックを転送するには、次の詳細を指定します。
   a) ルート名を指定します。
   b) **API** リクエストを受信する **API** リソースを選択します。
   c) API トラフィックを転送するアップストリームサービスをリストから選択します。

6. [保存] をクリックして、配置設定を保存します。

   設定を API ゲートウェイにデプロイする場合は、[**Save and Deploy**] をクリックします。

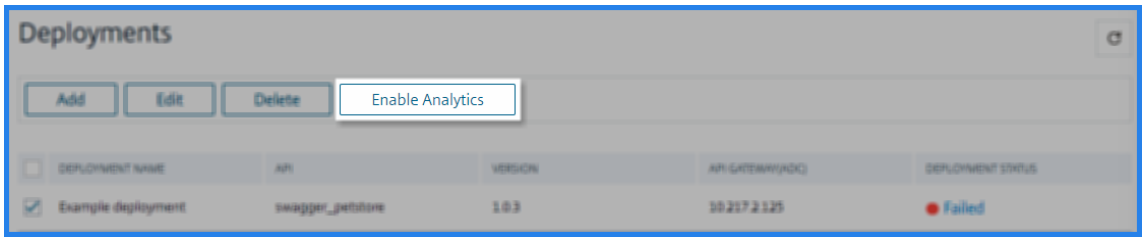
API アナリティクスを有効にする

デプロイの分析を有効にするための前提条件を次に示します。

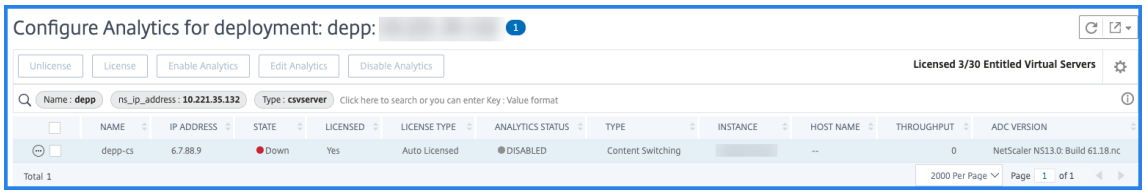
- 仮想サーバの ライセンスが付与されていることを確認する
- 分析ステータスが [無効] であることを確認します。
- 仮想サーバのステータスが **UP** であることを確認します。

デプロイの API 分析を有効にするには、次の手順を実行します。

1. API 分析を有効にするデプロイを選択します。
2. [アナリティクスの有効化] をクリックします。



3. [**Analytics** のデプロイの設定] ページで、仮想サーバーを選択し、[**Analytics** を有効にする] をクリックします。



4. **[Analytics** の有効化] ウィンドウで、次の操作を行います。

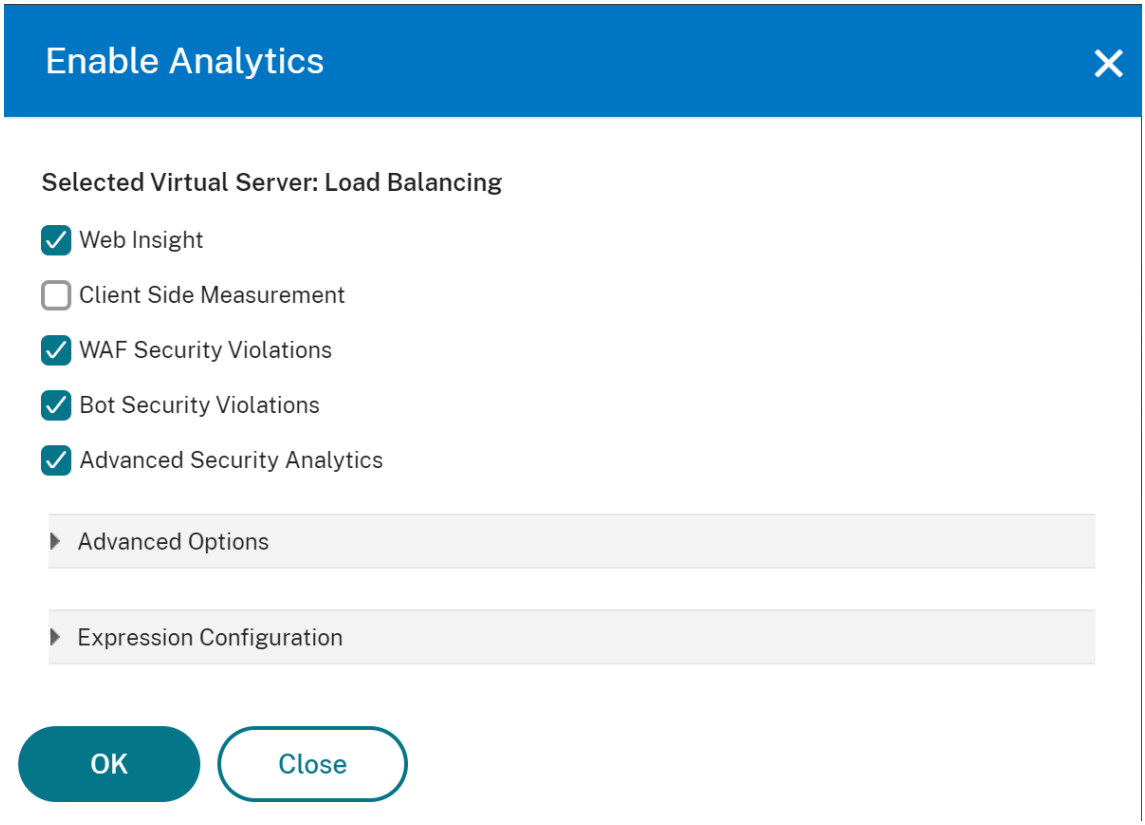
   a) インサイトタイプ (Web Insight、Security Insight、ボットインサイト) を選択します

   b) 転送モードとして [ログストリーム] または [**IPFIX**] を選択します。

      IPFIX とログストリームについて詳しくは、ログストリームの概要を参照してください。

   c) デフォルトでは、エクスプレッションは true です。

   d) [**OK**] をクリックします。



Citrix ADM は、選択した仮想サーバーで分析を有効にする処理を行います。

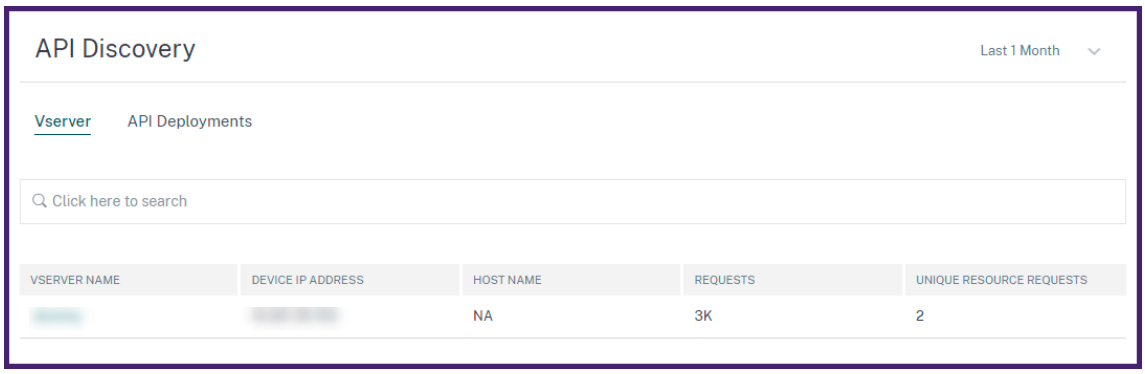
API エンドポイントの検出

May 7, 2021

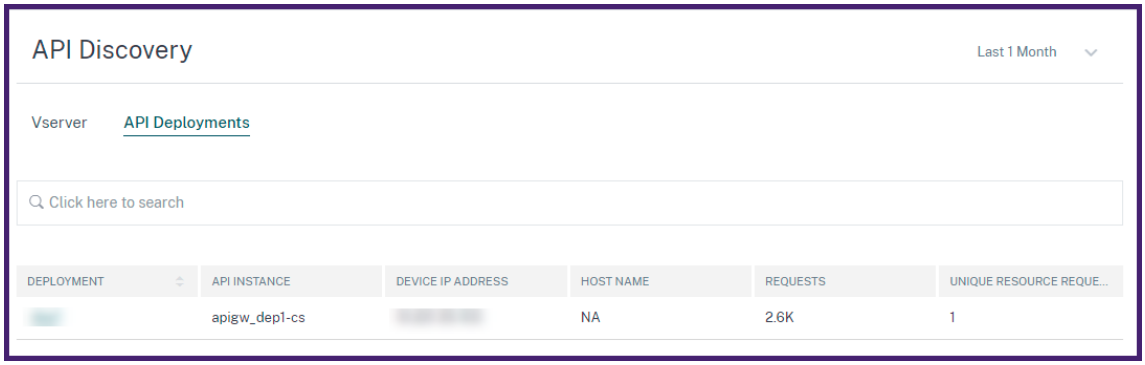
API Gateway を使用して、組織内に検出された API エンドポイントを表示できます。Citrix ADM は、ADC インスタンスおよび API 展開で受信した API トラフィックに基づいて、API エンドポイントを検出します。

Citrix ADM では、［アプリケーション］**>**［**API** ゲートウェイ］**>**［**API** 検出］ページに、検出された API エンドポイントが表示されます。

- 仮想サーバー -[仮想サーバー] タブには、ADC インスタンスの仮想サーバーが表示されます。仮想サーバーは、指定された期間の API リクエストを受信すると、このタブに表示されます。



- **API** デプロイ - このタブには、API 定義を使用して ADM からデプロイされた API デプロイメントが表示されます。このタブは、API デプロイが指定された期間の API リクエストを受信したときに API エンドポイントを検出します。API 定義を追加およびデプロイするには、「API 定義を追加する」および「API 定義のデプロイ」を参照してください。



> 注
>
> - 分析を構成し、仮想サーバーで Web インサイトを有効にしてください。API インスタンスで Web Insight を有効にするを参照してください。
> - ポリシーを追加できるのは、[API **deployments**] タブで検出された **API** エンドポイントのみです。

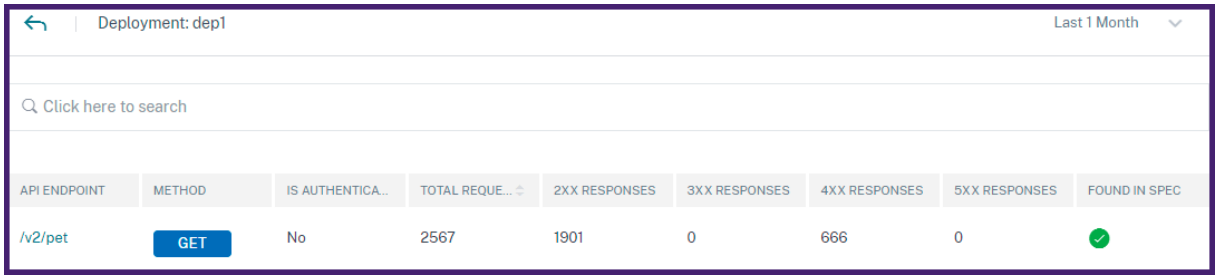
API エンドポイントの表示

[**API Discovery**] で、仮想サーバーまたは API 配置を選択すると、ADM GUI に API エンドポイントとその詳細が表示されます。

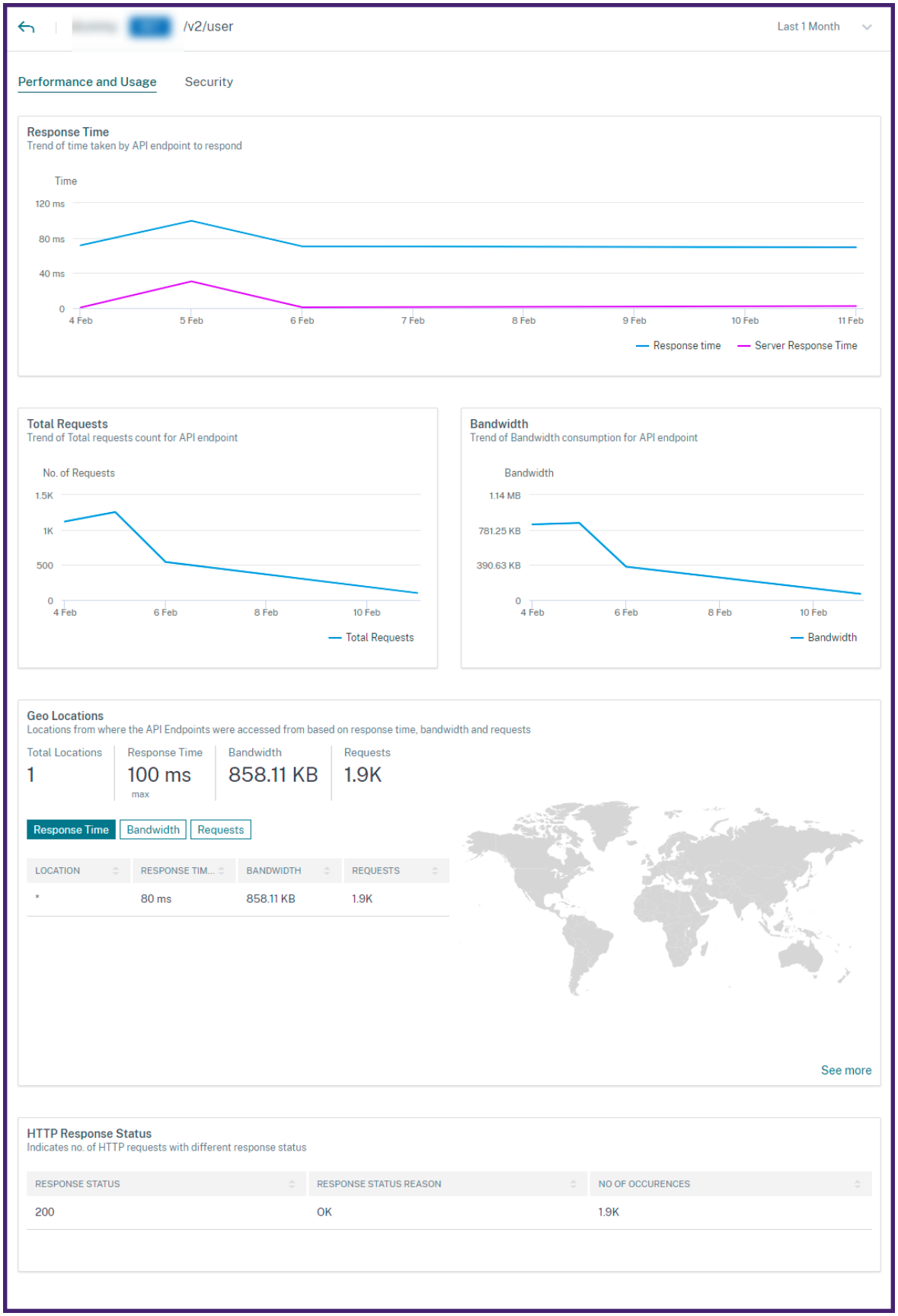
- メソッド -それは、API エンドポイントで使用されるメソッドを表示します。たとえば、GETおよびPOSTメソッド
- リクエスト合計 -それは、API エンドポイント上の API リクエストの数を表示します。
- 応答ステータス -それは、各応答ステータスのカウントを表示します。たとえば、2xx、3xx、4xx、5xxなどです。
- 仕様で見つかりました -この列は API デプロイにのみ表示されます。場合によっては、API 定義の一部ではない内部 API が外部からのトラフィックを受信することがあります。この列は、API エンドポイントと観測されたメソッドが API 定義の一部であるかどうかを識別するのに役立ちます。

仮想サーバ:

API デプロイ**:**



必要な API エンドポイントを選択して、詳細な分析レポートを表示することもできます。



各セクションの詳細については、API アナリティクスの表示を参照してください。

API デプロイへのポリシーの追加

May 7, 2021

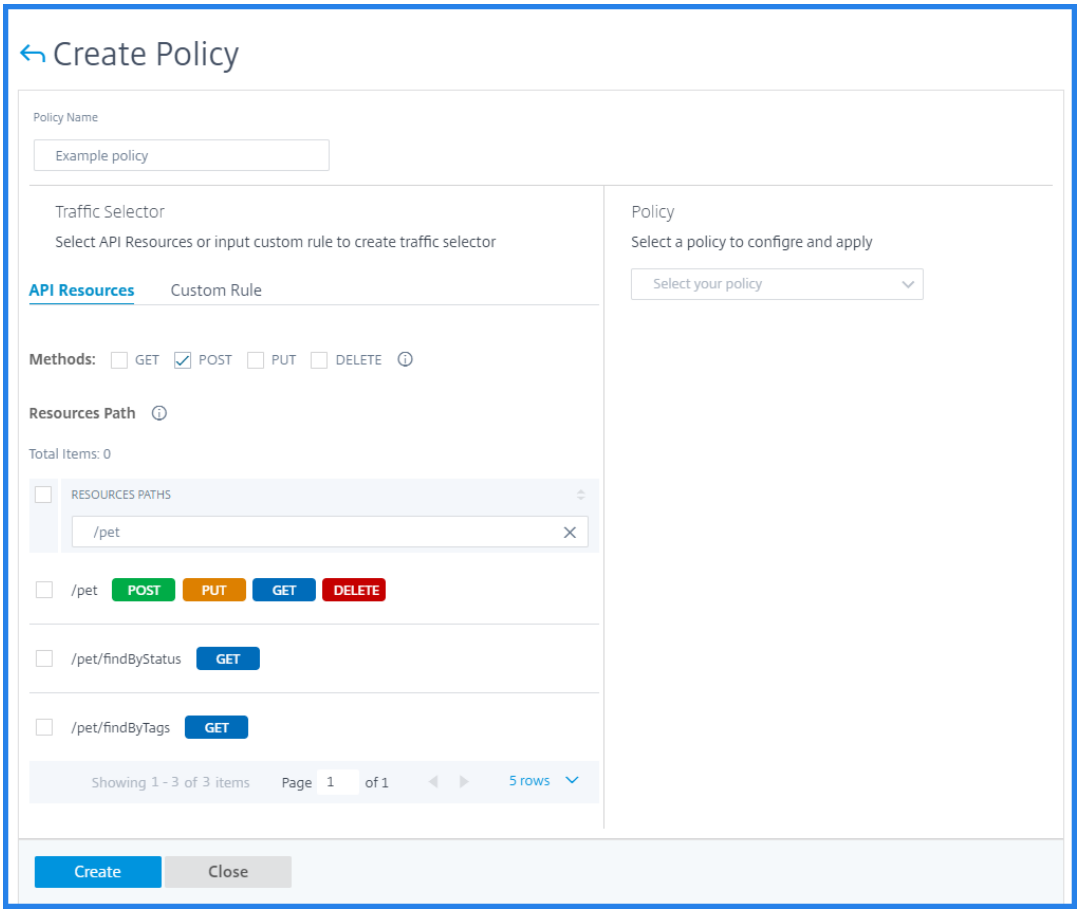
API トラフィックに対してさまざまなセキュリティポリシーを設定できます。この設定では、ポリシーに必要なトラフィック選択基準とパラメータを指定する必要があります。API 定義にポリシーを追加するには、次の手順を実行します。

1. [アプリケーション**] > [API Gateway] > [**ポリシー**]** に移動します。
2. ［追加］をクリックします。
3. ポリシーグループの名前を指定します。
4. リストから配置を選択します。
5. ポリシーを設定するアップストリームサービスをリストから選択します。
6. [**Add**] をクリックして、トラフィックセレクタとポリシータイプを選択します。

   トラフィックセレクタ -トラフィック選択基準には、API リソースパスまたはパスプレフィックス、メソッド、ポリシーが含まれます。

   トラフィック選択基準を指定するには、次のいずれかのオプションを使用できます。

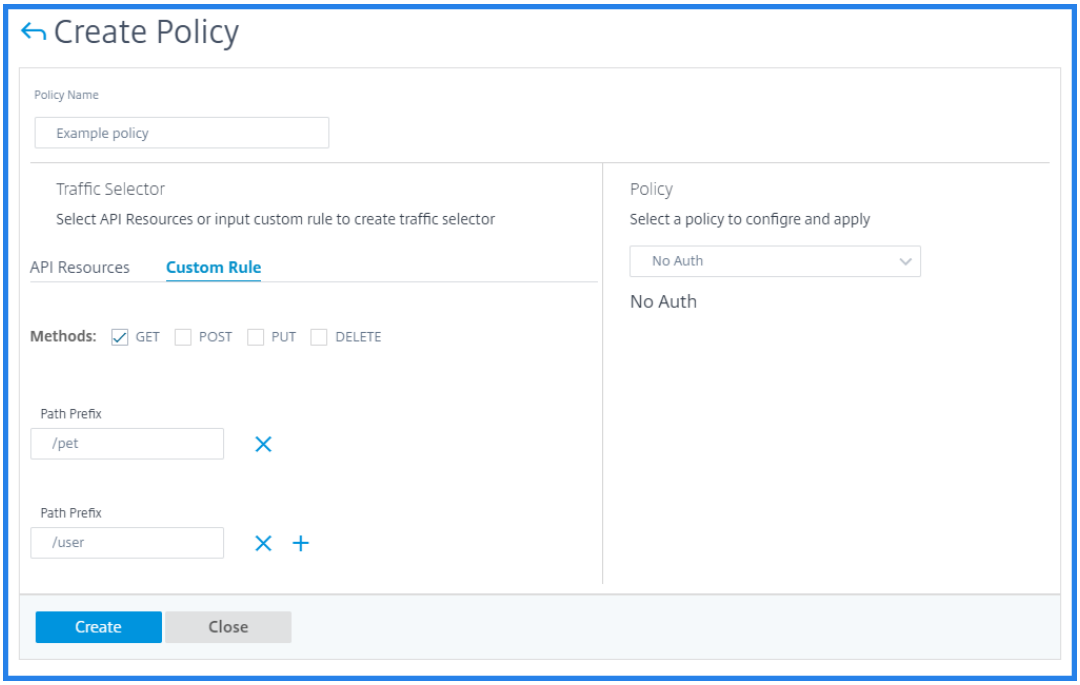
   - 「**API** リソース」— ポリシーを適用する API リソースとそのメソッドを選択します。キーワードを使用して API リソースとメソッドを検索できます。



この例では、POSTメソッドを持つ/userの API リソースが一覧表示されます。

- [カスタムルール] — このタブでは、カスタムパスプレフィックスと複数の方法を指定できます。

  設定したポリシーは、API トラフィック選択のカスタムルールに一致する着信 API リクエストに適用されます。



この例では、認証なしポリシーは、/petプレフィックスとPOSTメソッドを持つ API リソースに適用されます。

[**Policy**] で、選択した API リソースおよびメソッドに適用するポリシーをリストから選択します。各ポリシーの詳細については、「ポリシータイプ」を参照してください。

7. オプションで、ポリシータイプを移動して優先順位を設定できます。優先度の高いポリシータイプが最初に適用されます。
8. [保存] をクリックしてポリシーを追加します。ポリシーをすぐに適用する場合は、[保存して適用] をクリックします。

ポリシータイプ

API ポリシーを設定する場合、API リソースおよびメソッドに適用する次のポリシーを選択できます。

- 認証と承認
- レート制限
- **WAF**
- ボット
- ヘッダー書き換え

認証と承認

API リソースは、アプリケーションまたは API サーバーでホストされます。このような API リソースにアクセス制限を適用する場合は、認証ポリシーと承認ポリシーを使用できます。これらのポリシーは、着信 API リクエストにリソースへのアクセスに必要なアクセス許可があるかどうかを確認します。

次のポリシーを使用して、選択した API リソースの認証と承認を定義します。

‘No-Auth’

選択したトラフィックの認証をスキップするには、このポリシーを使用します。

‘Auth-Basic’

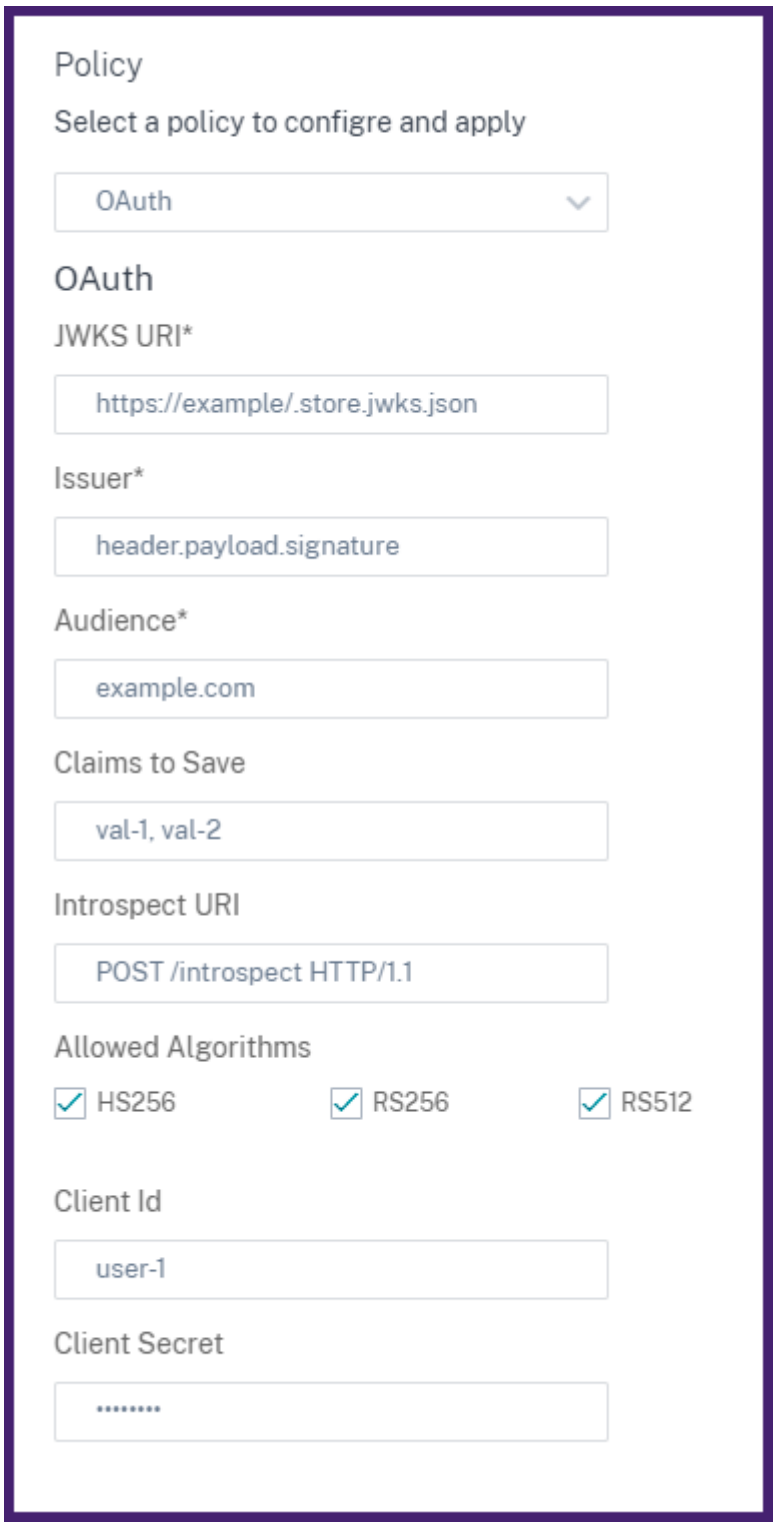
このポリシーは、ローカル認証を HTTP 基本認証スキームで使用するように指定します。ローカル認証を使用するには、Citrix ADC でユーザーアカウントを作成する必要があります。

OAuth

OAuth では、OAuth2 を使用してクライアントを認証し、アクセストークンを発行するために、外部 ID プロバイダーが必要です。クライアントがこのトークンを API ゲートウェイのアクセスクレデンシャルとして提供すると、設定された値に基づいてトークンが検証されます。

- **JWKS URI** -JWT（JSON ウェブトークン）検証用の JWK（JSON ウェブキー）を持つエンドポイントの URL
- 発行者 -認証サーバの ID（通常は URL）。
- 対象ユーザー -トークンが適用可能なサービスまたはアプリケーションの ID。
- **[** 保存する要求**]** : アクセス許可は、要求と期待される値のセットとして表されます。クレームの値を CSV 形式で指定します。
- イントロスペクト **URI** -認証サーバーのイントロスペクションエンドポイントの URL。この URL は、不透明なアクセストークンを確認するために使用されます。これらのトークンの詳細については、「不透明なアクセストークンの OAuth 設定」を参照してください。

  イントロスペクト **URI** を指定した後、認証サーバにアクセスするためのクライアント **ID** とクライアントシークレットを指定します。
- 許可されたアルゴリズム -このオプションを使用すると、着信トークン内の特定のアルゴリズムを制限できます。デフォルトでは、サポートされているすべてのメソッドが許可されています。ただし、選択したトラフィックに必要なアルゴリズムを確認することはできます。



検証が成功すると、API ゲートウェイはクライアントへのアクセスを許可します。

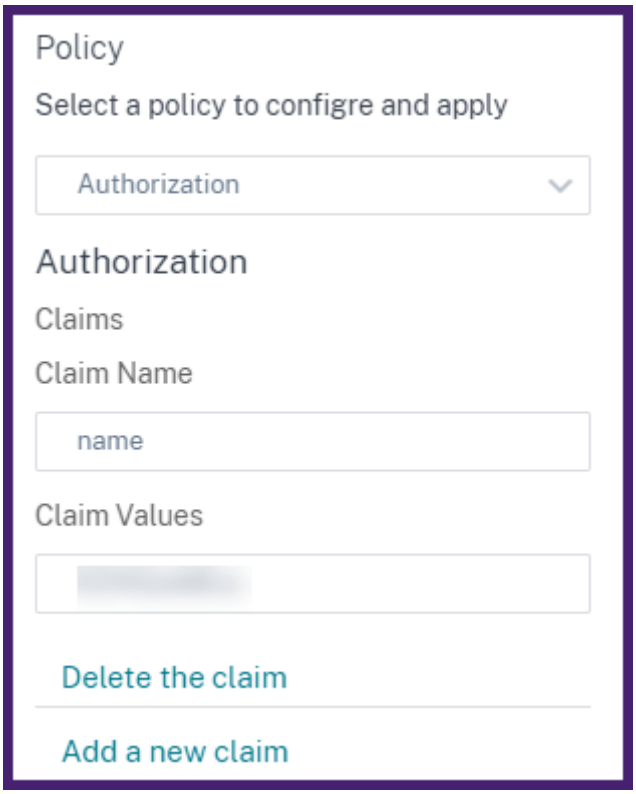
> 重要:
>
> 選択した API リソースの OAuth または**Auth-Basic**ポリシーを設定する場合は、残りの API リソースの**No**

> **Auth**ポリシーを構成します。この設定は、残りのリソースの認証をスキップすることを明示的に示します。

承認

このポリシーは、API リソースにアクセスするために必要なアクセス許可を確認します。アクセス許可は、要求と期待される値のセットとして表されます。このポリシーを構成するには、[新しい要求の追加] を選択し、以下を指定します。

- クレーム名
- クレームの値

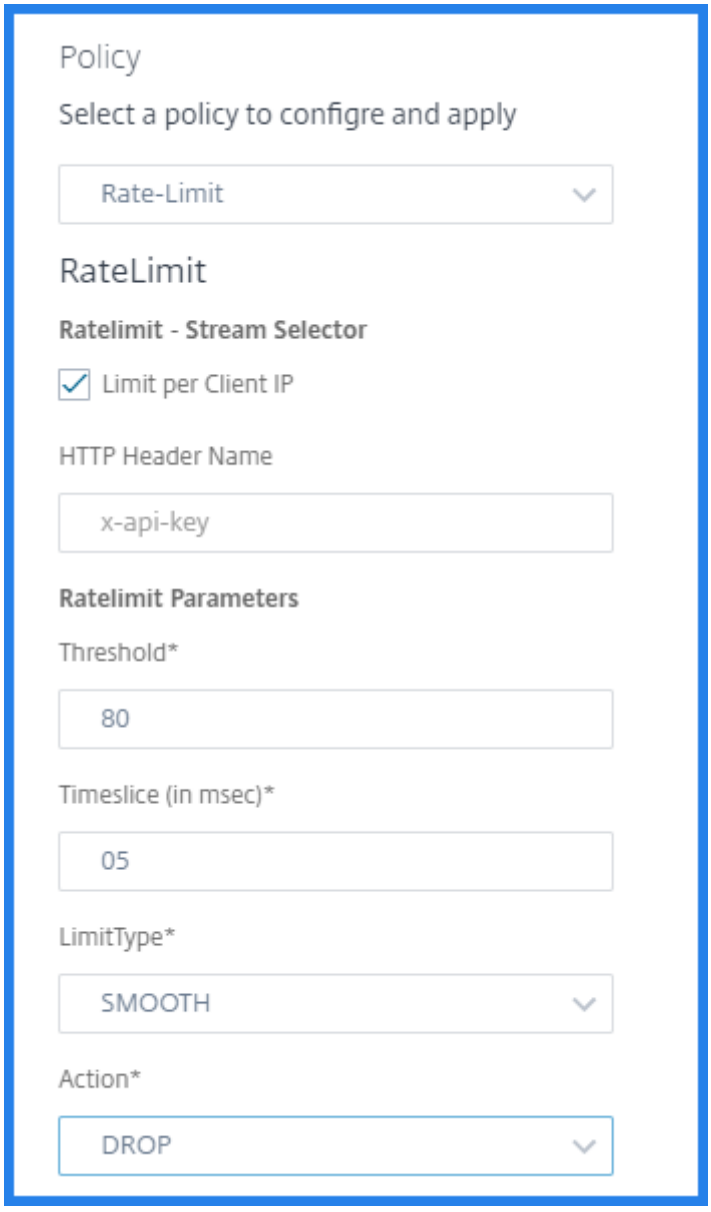


> 重要
>
> API ゲートウェイでは、API トラフィックの認証ポリシーと承認ポリシーの両方が必要です。したがって、認証ポリシーを使用して認可ポリシーを設定する必要があります。認証ポリシーは、OAuth または [Auth-Basic] (#auth-basic) にすることができます。
>
> 承認チェックがない場合でも、空の要求を持つ承認ポリシーを作成する必要があります。それ以外の場合、要求は 403 エラーで拒否されます。

レート制限ポリシー

選択した API リソースに与えられる最大負荷を指定します。このポリシーを使用すると、API トラフィックレートを監視し、予防措置を講じることができます。このポリシーを構成するには、以下を指定します。

- **HTTP** ヘッダー名 -これは、API リクエストを識別するためにトラフィックをフィルタリングするトラフィックセレクタキーです。また、レート制限ポリシーは、そのような API リクエストにのみ適用および監視します。
- **Threshold**： 指定された間隔で許可できる要求の最大数。
- タイムスライス -マイクロ秒単位で指定された間隔。この間隔の間、要求は設定された制限に対して監視されます。デフォルトでは、1000 マイクロ秒 (1 ミリ秒) に設定されています。
- **Limit type**： レート制限ポリシーを適用する方法を示すモード。[バースト] または [スムーズ] の制限タイプを選択できます。
- **[Action**]: しきい値を超えるトラフィックに対して実行するアクションを定義します。次のいずれかのアクションを指定できます。
  - **DROP:** 設定されたトラフィック制限を超える要求をドロップします。
  - **RESET:** 要求の接続をリセットします。
  - **REDIRECT:** 設定された **redirect_url** にトラフィックをリダイレクトします。
  - 応答: 標準応答 (429 `Too many requests`) で応答します。

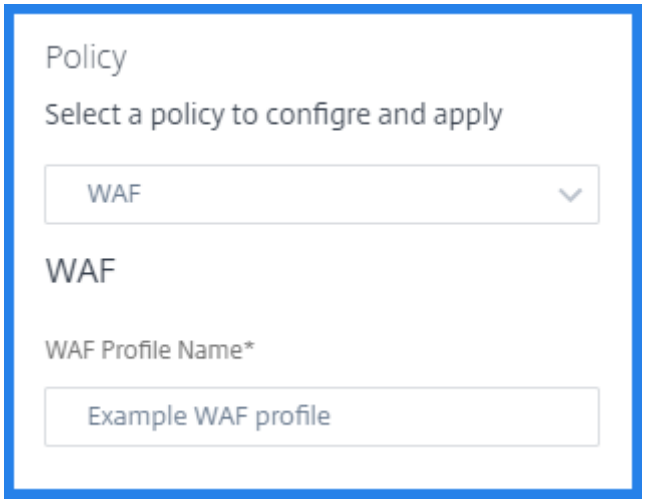


WAF ポリシー

このポリシーは、セキュリティ侵害、データの損失、および機密性の高いビジネス情報や顧客情報にアクセスする Web サイトへの不正変更を防止します。

WAF ポリシーを設定する前に StyleBook を使用して Citrix ADM で WAF プロファイルを作成する。

[**WAF** プロファイル名] で、作成した WAF プロファイルを選択または指定します。

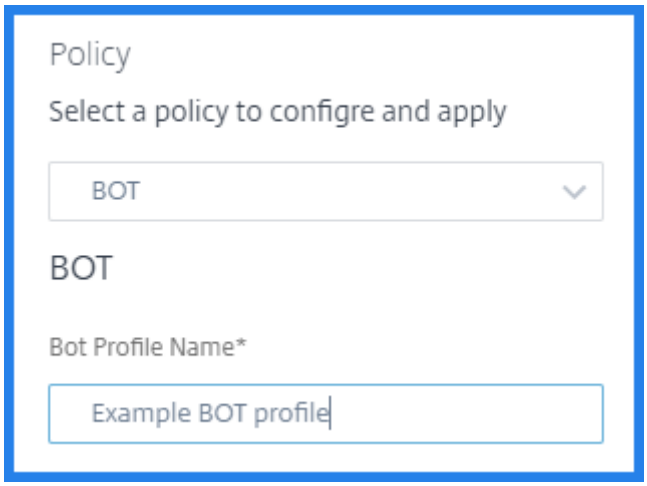


BOT ポリシー

このポリシーは、不正なボットを特定し、高度なセキュリティ攻撃からアプライアンスを保護します。

BOT ポリシーを設定する前に、StyleBook を使用して Citrix ADM で BOT プロファイルを作成する。

[ボットプロファイル名] で、作成した BOT プロファイルを指定します。



ヘッダー書き換え

このポリシーは、API リクエストとレスポンスのヘッダーを変更するのに役立ちます。HTTP ヘッダーの値を置き換える場合は、次のように指定します。

- **HTTP** ヘッダー名: リクエストヘッダーで変更するファイル名です。

  例: `Host`

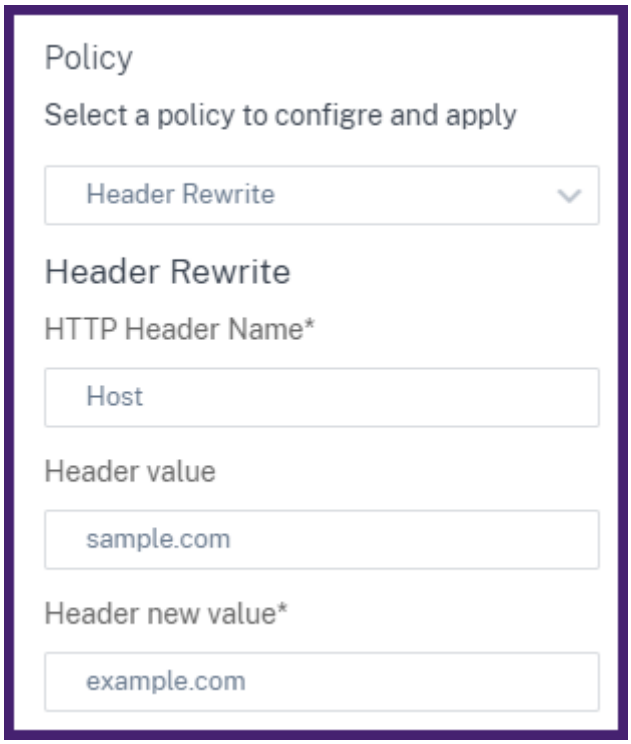
- **Header value**: オプション、指定したヘッダー名で変更する値文字列。

  例: `sample.com`

- ヘッダー新しい値: 指定されたヘッダー値を置き換える新しい値。

  Header 値が指定されていない場合は、受信した値を指定された値に置き換えて **HTTP** ヘッダー名にします。

  例: `example.com`



この例では、API リクエストの`Host`フィールドで、ヘッダー書き換えポリシー`sample.com`が`example.com`に置き換わります。

サービスグラフ

May 7, 2021

Citrix ADM サービスグラフ機能を使用すると、すべてのサービスをグラフィカルに監視できます。この機能では、サービスの詳細な分析と実用的なメトリックを表示することもできます。「アプリケーション」**>**「サービスグラフ」の順にナビゲートして、次のサービスグラフを表示します。

- すべての Citrix ADC インスタンスで構成されたアプリケーション
- Kubernetes アプリケーション
- 3 層の Web アプリケーション

すべての **Citrix ADC** インスタンスにおけるアプリケーションのサービスグラフ

グローバルサービスグラフ機能を使用すると、`clients to infrastructure to application`ビューの全体的な視覚化を取得できます。この単一ペインのサービスグラフビューでは、管理者として、次の操作を実行できます。

- ユーザーが特定のアプリケーション (3 層の Web アプリとマイクロサービスアプリ) にアクセスしているリージョンを理解する
- クライアント要求が処理されたというインフラストラクチャ（Citrix ADC インスタンス）ビューの視覚化
- 問題がクライアント、インフラストラクチャ、またはアプリケーションから発生しているかどうかを把握
- さらにドリルダウンして、問題のトラブルシューティングを行います。

「アプリケーション」**>**「サービスグラフ」の順に選択し、「グローバル」タブをクリックして以下を表示します。

- クライアントからバックエンドサーバに接続されたすべてのアプリケーションのエンドツーエンドの詳細
- 各データセンターに接続されているすべての Citrix ADC インスタンス

  > 注
  >
  > GSLB アプリがある場合にのみ、データセンターを表示できます。

- クライアントのメトリック情報
- Citrix ADC メトリックス情報
- 個別のアプリケーション、カスタムアプリケーション、および個別のマイクロサービスアプリケーションを持つすべての Citrix ADC インスタンス
- カスタムアプリ、個別アプリ、マイクロサービスアプリに属する上位 4 つの低スコアアプリケーション
- 上位 4 台の低スコア仮想サーバのメトリック情報
- クリティカル、レビュー、良い、適用できないなどのアプリケーション (個別のアプリ、カスタムアプリ、マイクロサービスアプリ) のステータス。

詳しくは、「サービスグラフでのアプリケーションの総合的なビュー」を参照してください。

Kubernetes アプリケーションのサービスグラフ

[アプリケーション**] > [**サービスグラフ] に移動し、[マイクロサービス] タブをクリックして以下を表示します。

- エンド・ツー・エンドのアプリケーション全体のパフォーマンスを確保
- アプリケーションのさまざまなコンポーネントの相互依存性によって生み出されるボトルネックの特定
- アプリケーションのさまざまなコンポーネントの依存関係に関するインサイトを収集
- Kubernetes クラスタ内のサービスの監視
- どのサービスに問題があるかを監視する
- パフォーマンスの問題に寄与する要因を確認する

- サービス HTTP トランザクションの詳細な可視性の表示
- HTTP、TCP、SSL メトリックの分析
- クライアント・メトリックとクライアント・トランザクション・サマリーの詳細の表示

Citrix ADM でこれらのメトリックを視覚化することで、問題の根本原因を分析し、必要なトラブルシューティングアクションを迅速に行うことができます。サービスグラフは、アプリケーションをさまざまなコンポーネントサービスに表示します。Kubernetes クラスター内で実行されるこれらのサービスは、アプリケーション内外のさまざまなコンポーネントと通信できます。はじめに、「サービスグラフの設定」を参照してください。

3 層 **Web** アプリケーションのサービスグラフ

[アプリケーション**] > [**サービスグラフ] に移動し、[**Web** アプリケーション] タブをクリックして以下を表示します。

- アプリケーションの構成方法の詳細（コンテンツスイッチング仮想サーバーと負荷分散仮想サーバーを使用）

  GSLB アプリケーションの場合は、データセンター、ADC インスタンス、CS、および LB 仮想サーバーを表示できます。
- クライアントからサービスへのエンド・ツー・エンドのトランザクション
- クライアントがアプリケーションにアクセスしている場所
- クライアント要求が処理されるデータセンターの名前と、関連するデータセンター Citrix ADC メトリック（GSLB アプリケーションのみ）
- クライアント、サービス、仮想サーバーのメトリックの詳細
- エラーがクライアントまたはサービスからのものである場合
- 「重大」、「レビュー」、「良好」などのサービスステータス。Citrix ADM は、サービスの応答時間とエラー数に基づいてサービスのステータスを表示します。
  - クリティカル（赤色）：平均サービス応答時間が 200 ミリ秒を超える場合とエラー数が 0 より大きいことを示します。
  - 確認（オレンジ）：平均サービス応答時間が 200 ミリ秒を超えるか、エラー数が 0 より大きいことを示します。
  - 良好（緑）：エラーがなく、平均サービス応答時間が 200 ミリ秒未満であることを示します。
- 「重大」、「レビュー」、「良好」などのクライアントのステータス。Citrix ADM は、クライアントのネットワーク遅延とエラー数に基づいてクライアントのステータスを表示します。
  - **Critical**（赤色）-平均クライアントネットワーク遅延が 200 ミリ秒を超える場合とエラーカウントが 0 より大きいことを示します。
  - 確認（オレンジ） -クライアントのネットワーク遅延の平均が 200 ミリ秒を超えるか、エラー回数が 0 を超えることを示します。

  - 良好（緑）: エラーがなく、クライアントのネットワーク遅延の平均が 200 ミリ秒未満であることを示します。

- 「重大」、「確認」、「良好」などの仮想サーバのステータス。Citrix ADM は、アプリのスコアに基づいて仮想サーバーのステータスを表示します。
  - クリティカル（赤） -アプリのスコアが 40 未満であることを示します。
  - レビュー（オレンジ） -アプリのスコアが 40 から 75 の間であることを示します。
  - **Good**（緑） -アプリのスコアが 75 を超えることを示します。

注意事項**:**

- 負荷分散、コンテンツスイッチング、GSLB 仮想サーバーのみがサービスグラフに表示されます。
- カスタムアプリケーションにバインドされた仮想サーバーがない場合、そのアプリケーションのサービスグラフに詳細は表示されません。
- 仮想サーバーと Web アプリケーションの間でアクティブなトランザクションが発生した場合にのみ、サービスグラフでクライアントとサービスのメトリックを表示できます。
- 仮想サーバーと Web アプリケーション間で有効なトランザクションがない場合は、負荷分散、コンテンツスイッチング、GSLB 仮想サーバー、サービスなどの構成データに基づいて、サービスグラフの詳細のみを表示できます。
- アプリケーション構成に変更が加えられた場合、サービスグラフに反映されるまで 10 分かかることがあります。

詳しくは、「アプリケーションのサービスグラフ」を参照してください。

サービスグラフの設定

May 7, 2021

ソフトウェア要件

Kubernetes 配布	Kubernetes バージョン	コンテナーネットワークインターフェイス (CNI)	CPX バージョン	CIC バージョン	Citrix ADM エージェントのバージョン
オープンソース	v1.16.3	Flannel、Calico または Canal	13.0—47.103 以降	1.6.1 以降	13.0—49.x 以降

Kubernetes クラスターはさまざまな配置トポロジを設定できます。次の表に、サービスグラフでサポートされているトポロジを示します。

トポロジ	サービスグラフでサポート
シングルティア入力または統合入力	はい
デュアルティア	はい
クラウド	はい。ただし、クラウドロードバランサーはグラフに表示されません
サービスメッシュライト	はい
サービスメッシュ	はい
ロードバランサーの種類のサービス	いいえ
NodePort タイプのサービス	いいえ

Citrix ADM でのサービスグラフの設定を完了するには、Kubernetes クラスター用に構成したトポロジの種類をクリックし、上記の手順を完了します。

- 単一層または統合入力トポロジ
- デュアルティアまたはサービスメッシュ Lite トポロジ
- サービスメッシュトポロジ

> 注
>
> 2 層トポロジとサービスメッシュ Lite トポロジ用のサービスグラフを設定する手順は同じです。

単一層または統合入力トポロジ

次の手順を実行して、単一層または統合入力トポロジを設定します。詳しくは、「単一層または統合入力トポロジを設定するための詳細な手順」を参照してください。

- 単一層またはユニファイド入力トポロジで Kubernetes クラスターを構成しました。

- Citrix ADM でVPX、MPX、SDX、BLX インスタンスが追加され、**Web Insight** を有効にしました。
- Citrix ADM Kubernetes クラスター で追加。

デュアルティアまたはサービスメッシュ **Lite** トポロジ

次の手順を実行して、デュアルティアまたはサービスメッシュ Lite トポロジを設定します。詳しくは、「デュアルティアまたはサービスメッシュ Lite トポロジを設定するための詳細な手順」を参照してください。

- サポートされているトポロジのいずれかで Kubernetes クラスターを構成しました。
- Citrix ADM エージェント をインストールし、データセンターまたはクラウド内の Citrix ADM と Kubernetes クラスターまたはマネージドインスタンス間の通信を有効にするように構成されています。

  Citrix ADM エージェントをマイクロサービスとして展開することもできます。詳細については、はじめにの「**Citrix ADM** エージェントのインストール」セクションを参照してください。
- Citrix ADM エージェント上でスタティックルートを構成して、Citrix ADM と Citrix ADC CPX 間の通信を有効にします。

  > 注
  >
  > Citrix ADM エージェントを同じクラスタにマイクロサービスとして展開している場合は、この手順を無視できます。
- GitHub リポジトリからサンプル配置ファイルをダウンロードしました。
- Citrix ADM への CPX 登録が正常に行われるように、CPX YAML ファイルに必須パラメータが追加されました。
- Citrix ADM にVPX、MPX、SDX、または BLX インスタンスを追加しました。
- Citrix ADM にKubernetes クラスターを追加しました。
- サンプルマイクロサービスアプリケーションをデプロイしました。
- Citrix ADC CPX とCPX を ADM に登録しましたを展開しました（2 層アーキテクチャにのみ適用）。
- 仮想サーバの自動選択を有効にして CPX 仮想サーバのライセンスを取得できるようにしました。
- Citrix ADM エージェントが HTTP トランザクションと TCP トランザクションを取得するために、すべてに設定したWeb トランザクションと TCP トランザクション設定を有効にしました。
- トラフィックがマイクロサービスに送信されます。

サービスメッシュトポロジ

サービスメッシュトポロジをセットアップするには、次の手順を完了してください。詳しくは、「サービスメッシュトポロジを設定するための詳細な手順」を参照してください。

- 次のいずれかのサービスメッシュトポロジで Kubernetes クラスターバージョン`1.14.0`を構成しました。

  - Istio のサイドカープロキシとしての Citrix ADC CPX
  - Istio の入力ゲートウェイとしての Citrix ADC

  詳しくは、「Citrix ADC Istio アダプタの展開アーキテクチャ」を参照してください。

- admissionregistration.k8s.io/v1beta1API を有効にしました。API を確認するには、以下を使用します。

  ```
  kubectl api-versions | grep admissionregistration.k8s.io/v1beta1
  ```

  次の出力は、API が有効になっていることを示しています。

  ```
  admissionregistration.k8s.io/v1beta1
  ```

- Istio `istio v.1.3.0`をインストールしました。
- Helm バージョン 3.xをインストールしました。
- Citrix ADM エージェント をインストールし、データセンターまたはクラウド内の Citrix ADM と Kubernetes クラスターまたはマネージドインスタンス間の通信を有効にするように構成されています。

  Citrix ADM エージェントをマイクロサービスとして展開することもできます。詳細については、はじめにの「**Citrix ADM** エージェントのインストール」セクションを参照してください。

- Citrix ADM エージェント上でスタティックルートを構成して、Citrix ADM と Citrix ADC CPX 間の通信を有効にします。

  > 注
  >
  > Citrix ADM エージェントを同じクラスタにマイクロサービスとして展開している場合は、この手順を無視できます。

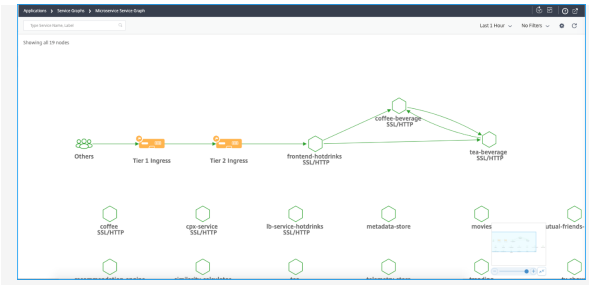
- サービスメッシュトポロジデータを入力するように必須パラメータを設定しました。
- サンプルアプリケーションをデプロイしました。
- Citrix ADM にKubernetes クラスターを追加しました。
- 仮想サーバの自動選択を有効にして仮想サーバのライセンスを取得できます。
- Citrix ADM エージェントが HTTP トランザクションと TCP トランザクションを取得するために、すべてに設定したWeb トランザクションと TCP トランザクション設定を有効にしました。
- トラフィックがマイクロサービスに送信されます。

必要なセットアップ手順を完了すると、[アプリケーション] > **[**サービスグラフ**]** および [マイクロサービス**]** タブで設定されたサービスグラフを表示できます。詳しくは、「サービスグラフの詳細」を参照してください。

サービスグラフで詳細を表示

May 7, 2021

Citrix ADM で Kubernetes クラスターを追加した後、サービスグラフにデータを取り込むまでに約 10 分かかります。[アプリケーション] > [サービスグラフ] に移動し、[マイクロサービス] タブをクリックして、サービスグラフの詳細を表示します。

2 階層/サービスメッシュ Lite トポロジ	シングルティア/統合型入力トポロジ
	

- 階層 **1** の入力 — Kubernetes クラスタ内の CitrixIngress Controller は、Kubernetes クラスタ外の Citrix ADC インスタンス（VPX/MPX/SDX/BLX）を構成します。
- 階層 **2** の入力 — Kubernetes クラスター内の Citrix ADC CPX インスタンスとともにサイドカーとして動作する CitrixIngress Controller です。
- [**Ingress**]: 他のすべての配置トポロジを表示します。

サービスグラフダッシュボード

1 -コンポーネントサービスの通信方法を示す、アプリケーションのエンドツーエンドのネットワークマップ

2 — 特定の期間のヒットとエラーを示すグラフ

3 — サービスを検索するための検索バー

4 — 期間を選択するための時間リスト

5 -サービスの表示にフィルタを適用する

6 — 設定アイコン

7 — ズームインおよびズームアウト

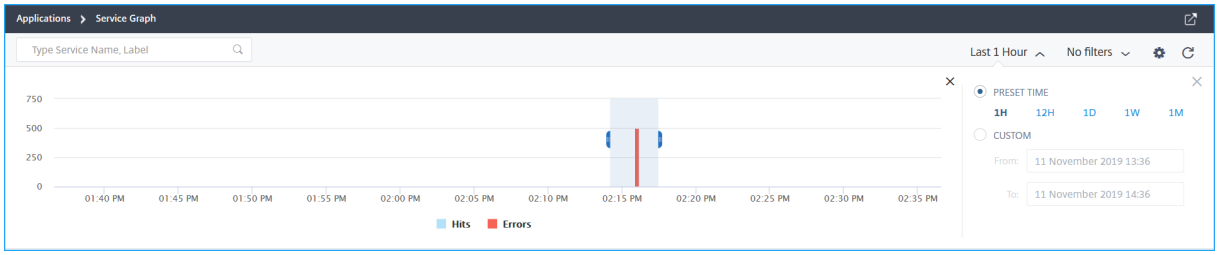
8 — グラフビューまたは表形式ビュー

選択した期間に基づいて、サービスグラフを表示できます。

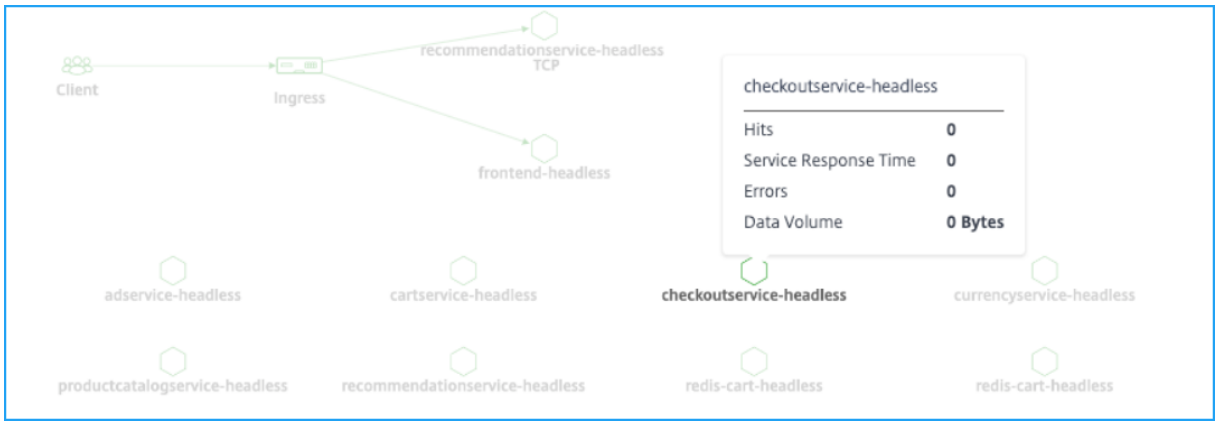
サービスアイコン	説明
	エッジの幅は、ヒット数を示します。エッジの幅が大きいほど、ヒット数が多くなることを示します。
	警告アイコンが付いたサービスは、サービスにエラーがあることを示します。
	ストップウォッチアイコンが付いたサービスは、サービスにレイテンシーまたは応答時間の問題があることを示します。
	ストップウォッチと警告アイコンの両方があるサービスは、サービスにエラーと遅延/応答時間の問題の両方があることを示します。

> 注:
>
> サービスに警告アイコンまたはストップウォッチアイコンがない場合は、そのサービスに Hits の異常またはしきい値違反があることを示します。

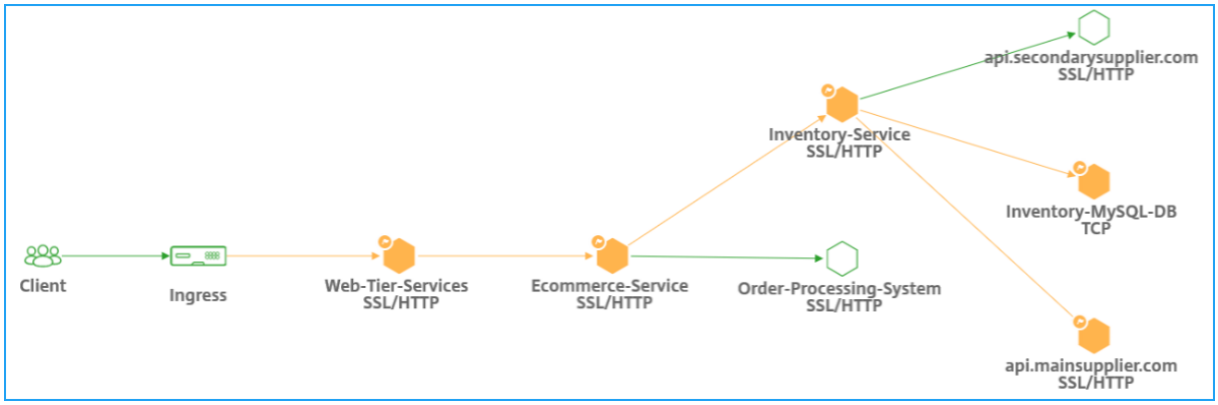
グラフからヒットを示す期間を選択し、さらにドリルダウンして追加情報を表示します。



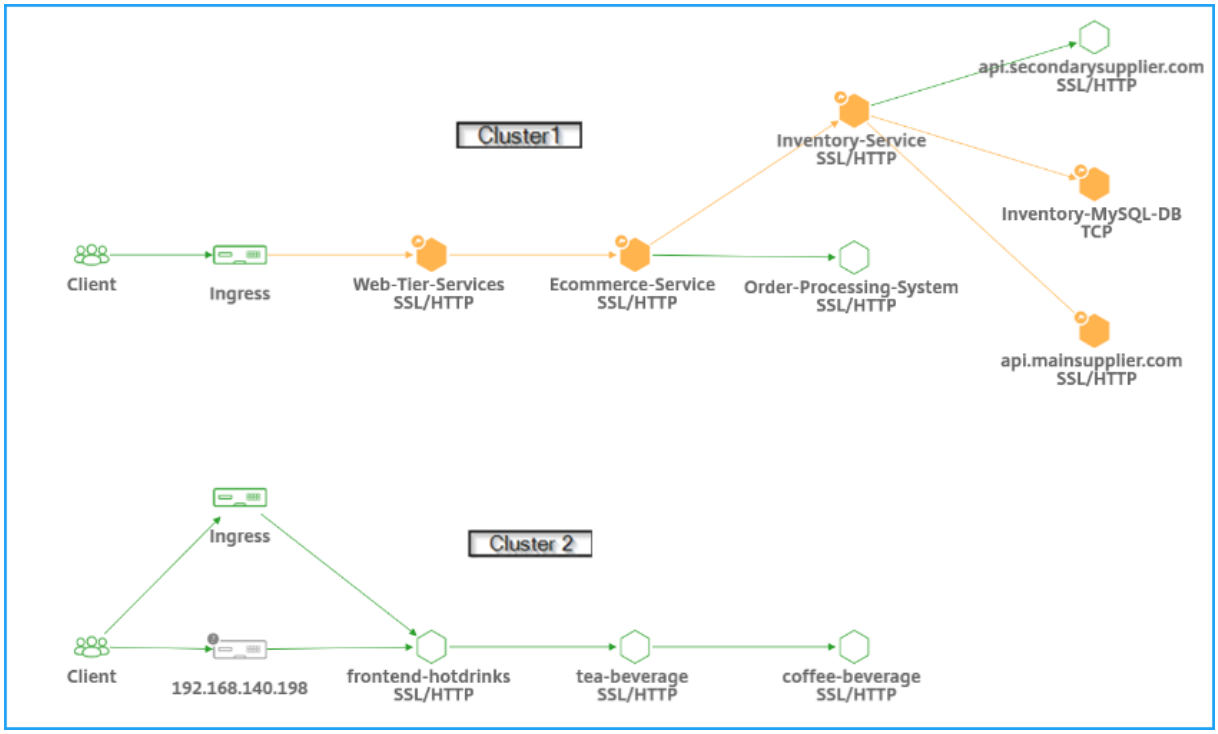
> 注
>
> Citrix ADM でアクティブなトランザクションが受信されない場合は、Citrix ADC インスタンスによって負荷分散されたサービスのみを表示できます。サービスの上にマウスポインタを置くと、すべてのメトリックが 0 として表示されます。



これで、サービスで使用されるプロトコルとともにサービスグラフが表示されます。次の図に示すように、Kubernetes クラスターで次のサービスが実行されているとします。



> 注
>
> オーケストレーション > **Kubernetes** > **Clusters** で複数のクラスターを追加した場合は、各クラスターに関連付けられたサービスを表示できます。



サービスの次のステータスを表示できます。

- クリティカル（赤） -複数のメトリックに異常またはしきい値違反があるサービス。デフォルトのしきい値の場合、Critical ステータスは平均サービス応答時間が 200 ミリ秒より長く、エラーカウントが 0 より大きいことを示します。
- **Review**（オレンジ色） -サービスのいずれかのメトリックに異常またはしきい値違反があります。デフォルトのしきい値の場合、[Review] ステータスは平均サービス応答時間が 200 ミリ秒より長いか、エラーカウントが 0 より長い
- 良好（緑） -異常またはしきい値違反のないサービス。デフォルトのしきい値の場合、[Good] ステータスはエラーがなく、平均サービス応答時間が 200 ミリ秒未満であることを示します。

  異常の詳細については、ゴールデンシグナルのメトリックを使用してサービスを監視するを参照してください。

  しきい値の詳細については、サービスグラフでのしきい値の設定を参照してください。

サービスで使用されるプロトコルを識別するためのプロトコルは次のとおりです。

- **TCP** — サービスが TCP プロトコルを使用していることを示します。
- **SSL, HTTP** — サービスが SSL over HTTP プロトコルを使用していることを示します。
- **SSL, TCP** — サービスが SSL over TCP プロトコルを使用していることを示します。

> 注
>
> プロトコルのないサービスは、サービスが HTTP プロトコルを使用していることを示します。

表形式ビューを使用した主要なメトリックの傾向の表示

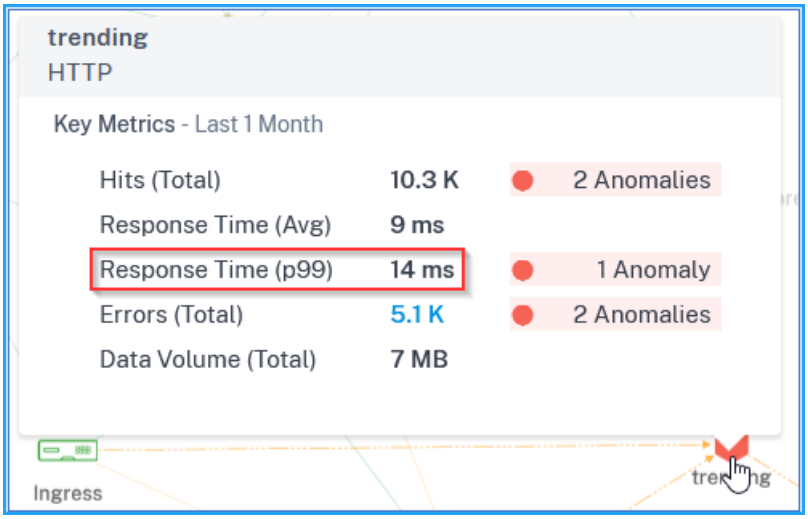
表形式ビューを使用すると、次の項目を確認できます。

- サービスの主なメトリック
- ソースサービスと宛先サービス間の主要なメトリック

管理者は、これらの主要なメトリックを使用して、選択した期間におけるゴールデンシグナルの傾向を分析できます。詳しくは、「サービス詳細の表示」を参照してください。

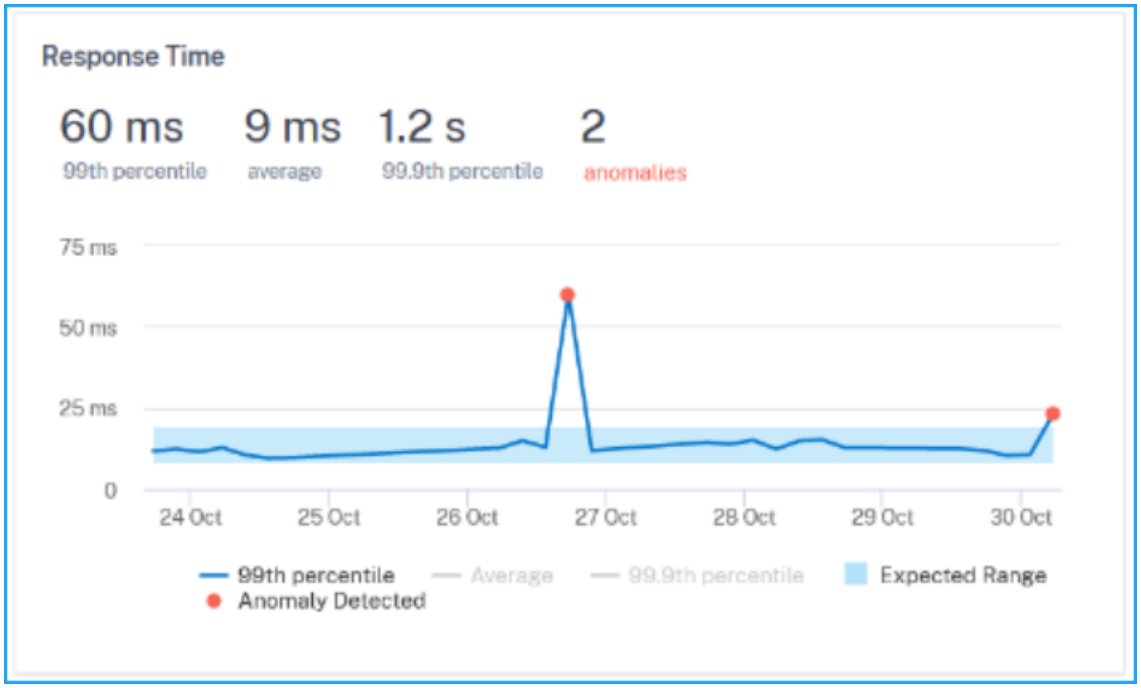
サービス応答時間の **Pxx** 値の表示

サービスの上にマウスを置くと、応答時間の Pxx 値が表示されます。



[応答時間]（**P99**）：選択した期間の 99% の要求が P99 値未満であることを示します。

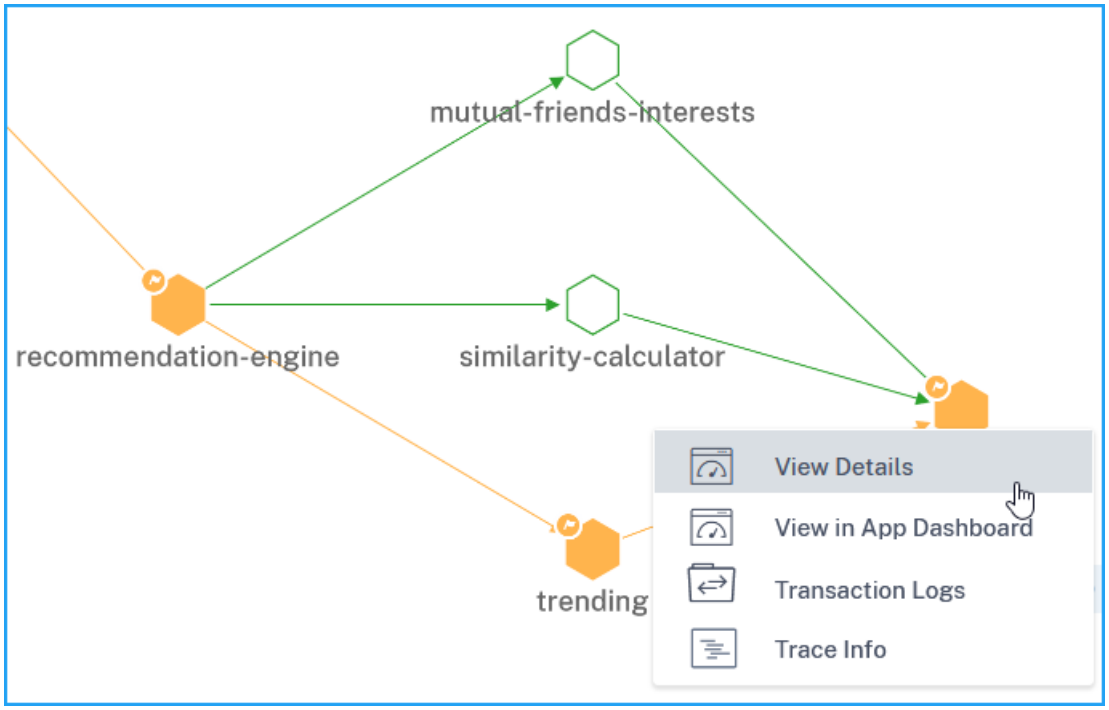
ドリルダウンしてサービスの詳細を表示する場合、選択した期間におけるレスポンス時間の 99 パーセンタイルおよび 99.9 百分位数も表示できます。



管理者は、pxx 値を使用すると、サービスの応答時間をよりよく理解できます。詳しくは、「サービス詳細の表示」を参照してください。

サービス詳細の表示

サービスをクリックすると、次のオプションが表示されます。

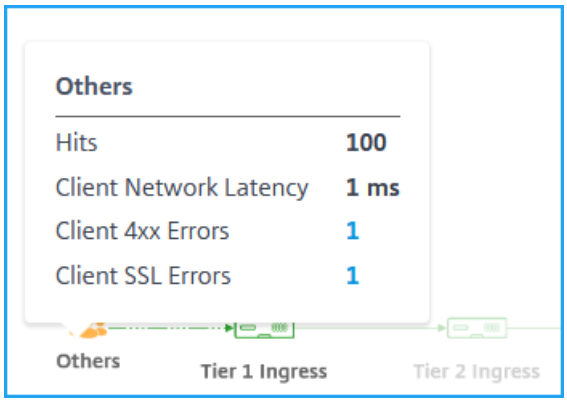


- 詳細の表示 -名前空間、ラベル、サービスがホストされているクラスターなどのサービスの詳細を表示できます。詳しくは、「サービス詳細の表示」を参照してください。
- アプリダッシュボードで表示 -アプリのスコア、Kubernetes サービスの詳細、ポッドの詳細など、選択したアプリケーションの詳細を表示できます。詳しくは、「Kubernetes アプリケーションの詳細」を参照してください。
- トランザクション・ログ：HTTP および SSL over HTTP トランザクションの詳細を表示できます。詳しくは、「Web トランザクションの分析の表示」を参照してください。
- トレース情報 -サービスの分散トレースを表示できます。詳しくは、「分散トレース」を参照してください。

クライアントメトリックの表示

クライアントがサービスにアクセスしている場所を表示できます。管理者は、クライアントメトリックスを視覚化し、クライアントから発生する問題を分析できます。

クライアントリージョンにマウスポインタを合わせると、メトリックスが表示されます。



- **Hits** -クライアントが受信したヒット数の合計を示します。
- クライアントネットワーク待ち時間 -平均クライアントネットワーク遅延を示します。
- クライアント **4xx** エラー -クライアントの 4xx エラーの合計を示します。
- クライアント **SSL** エラー -クライアントの SSL エラーの合計を示します。

Citrix ADM の **IP** ブロック -クライアントがパブリック IP アドレスを使用している場合、Citrix ADM はクライアントの場所を認識できます。Citrix ADM には組み込みの場所 CSV ファイルがあり、これはクライアントの IP アドレス範囲に基づいて場所と一致します。

Citrix ADM は、IP アドレスが Citrix ADM サーバーに追加される場合にのみ、プライベート IP アドレスを使用してクライアントの場所を認識できます。たとえば、クライアント IP アドレスが市 A に関連付けられたプライベート IP アドレス範囲内にある場合、Citrix ADM は、トラフィックがこのクライアントの都市 A から発信されていることを認識します。

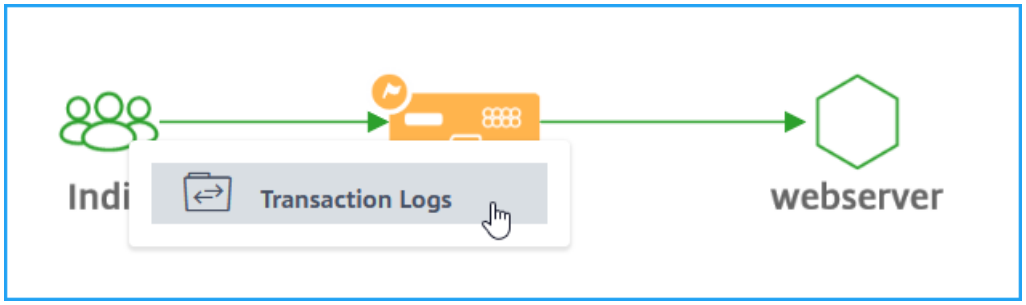
詳しくは、「プライベート IP ブロックを作成する」を参照してください。

クライアント・トランザクション・サマリーを表示

詳細なクライアント・トランザクション・サマリーでは、次の項目を表示できます。

- 応答時間 > 500 ミリ秒
- 5xx エラー

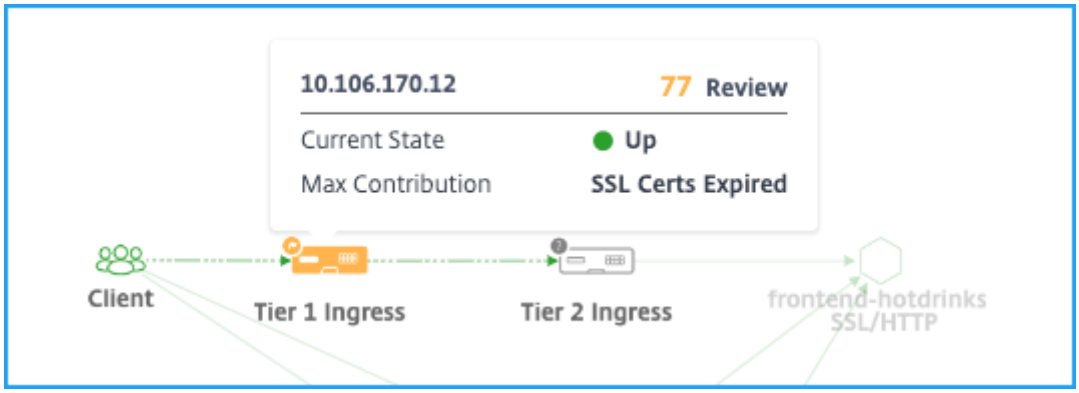
クライアントの場所をクリックし、[トランザクションログ] を選択します。



詳しくは、「Web トランザクション分析」を参照してください。

入力メトリックの表示

Kubernetes クラスターで使用されている入力のタイプを表示できます。



- Citrix ADC IP アドレスとそのスコア
- 現在の状態：Citrix ADC インスタンスが稼働中、停止中、または状態外のいずれであるかを示す
- **[** 最大コントリビューション] ― インスタンススコアに影響している問題を示します。

単一層トポロジでは、単一の **Ingress** だけを表示できます。

[**Ingress**] をクリックして、さらにドリルダウンして詳細を表示します。詳しくは、「問題のトラブルシューティングに関する進入の詳細の表示」を参照してください。

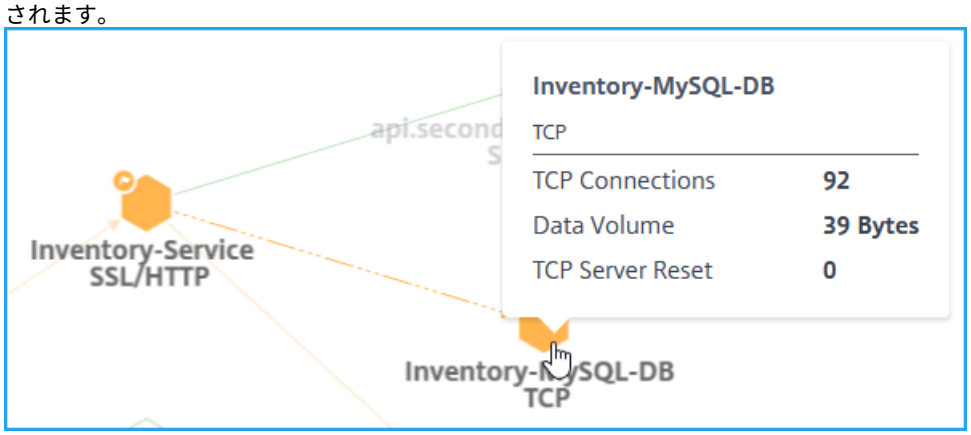
TCP および **SSL** メトリックの表示

TCP メトリックと SSL メトリックを使用すると、次のことができます。

- サービス間の TCP 接続の詳細を表示する
- TCP 関連の問題が送信元サービスまたは宛先サービスにあるかどうかを確認します。
- SSL エラーが送信元サービスまたは宛先サービスからのものであるかを表示する
- SSL サービスが使用する SSL プロトコルのバージョンの表示

TCP メトリック

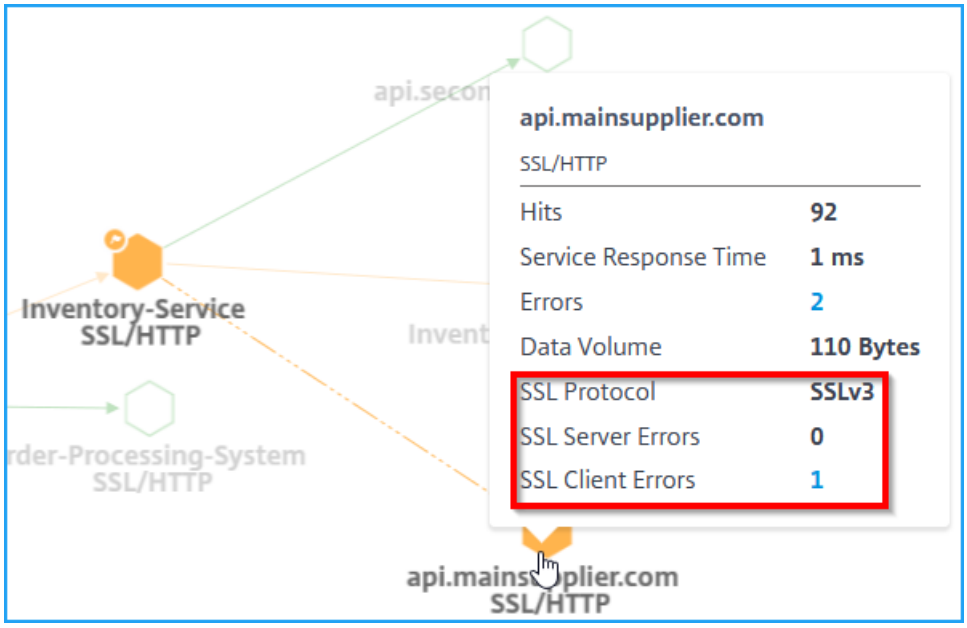
TCP サービスまたはその関連付けられた着信サービスの上にマウスポインタを合わせると、TCP メトリックが表示されます。



- **TCP** 接続 — サービス間で確立された接続の合計
- **Data Volume**： サービスによって処理されたデータの合計
- **TCP** サーバのリセット — サーバから開始された TCP リセットの合計

SSL メトリック

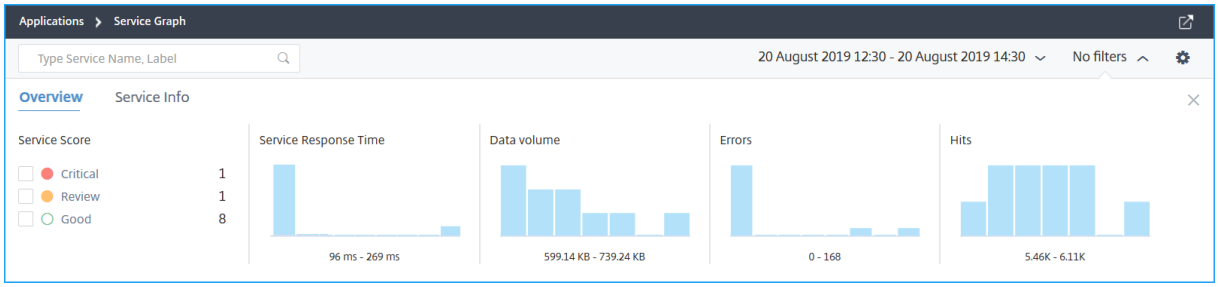
SSL プロトコルを使用するサービスにマウスポインタを合わせて、SSL メトリックを表示します。



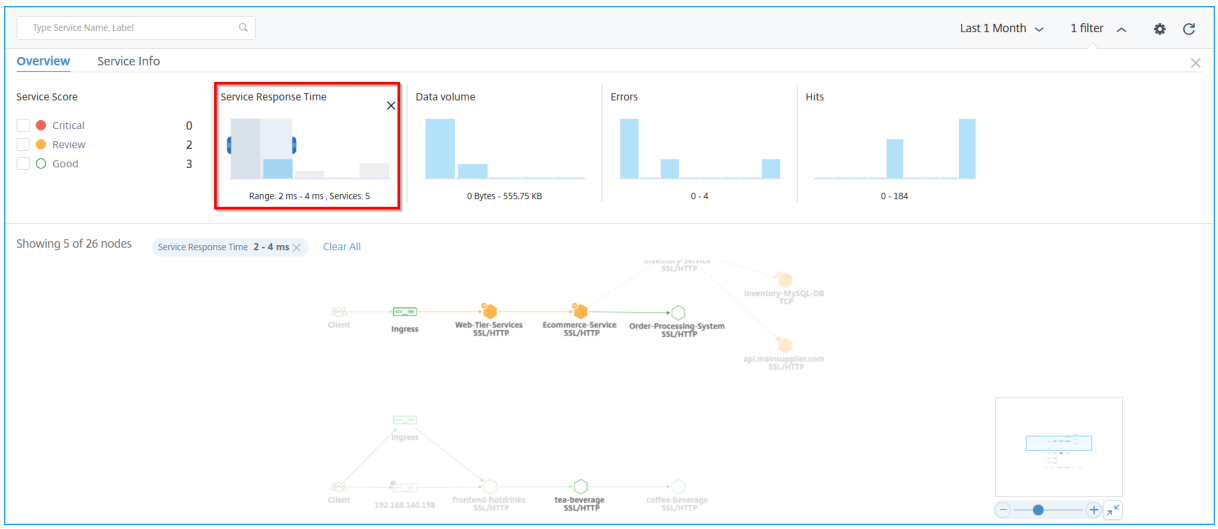
- 「**SSL** サーバーエラー」— サーバーからの SSL エラーの合計を示します。(SSL 証明書が不明など)
- **SSL** プロトコル — サービスが使用する SSL プロトコルのバージョンを示します。
- **SSL** クライアントエラー -クライアントからの SSL エラーの合計を示します。(SSL クライアント認証エラーなど)

フィルタの適用

フィルタを適用して、特定のサービス情報を表示できます。フィルタオプションを取得するには、**[**フィルタなし] リストをクリックします。

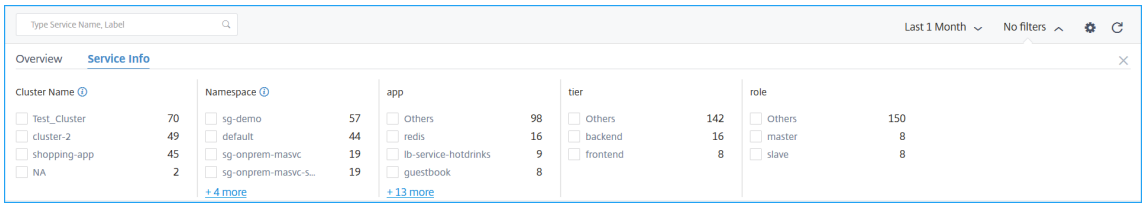


たとえば、レイテンシーが 150 ミリ秒未満のサービスを表示する場合は、[サービス応答時間] の下の棒グラフをクリックして結果を表示します。



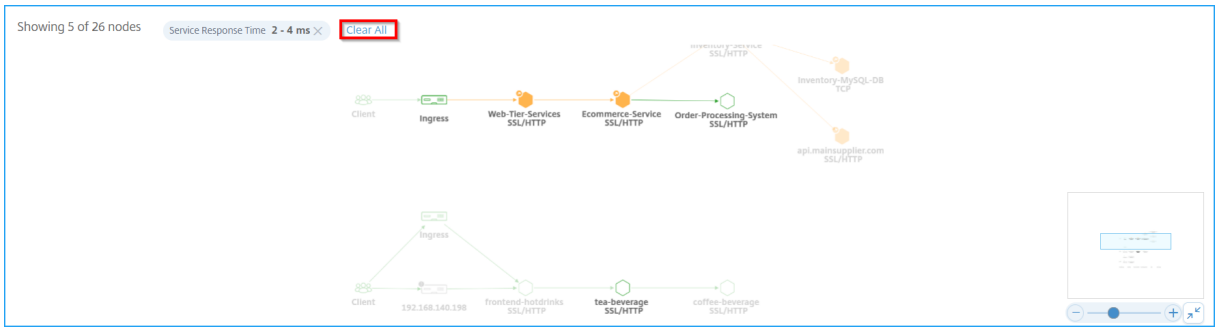
[サービス情報] をクリックして、次のフィルタを選択して適用します。

- [**Cluster**]: 選択した 1 つまたは複数のクラスタに適用可能なすべてのサービスが表示されます。
- [**Namespace**]: 選択したネームスペースに適用可能なすべてのサービスが表示されます。

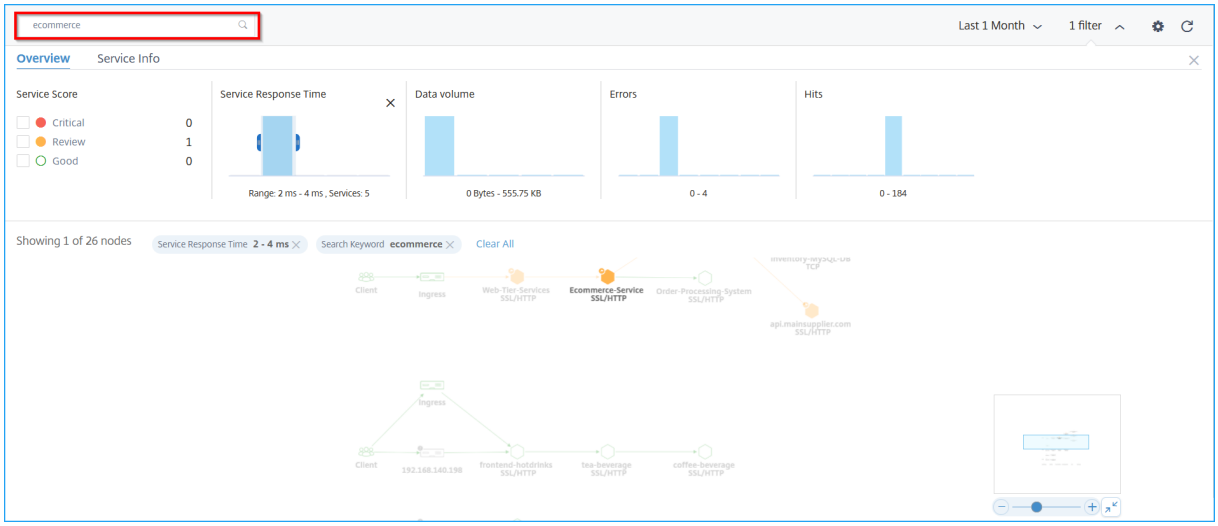


> 注
>
> Kubernetes サービス定義 YAML でサービスに対して構成されたラベルによっては、より多くのフィルターオプションを表示することもできます。

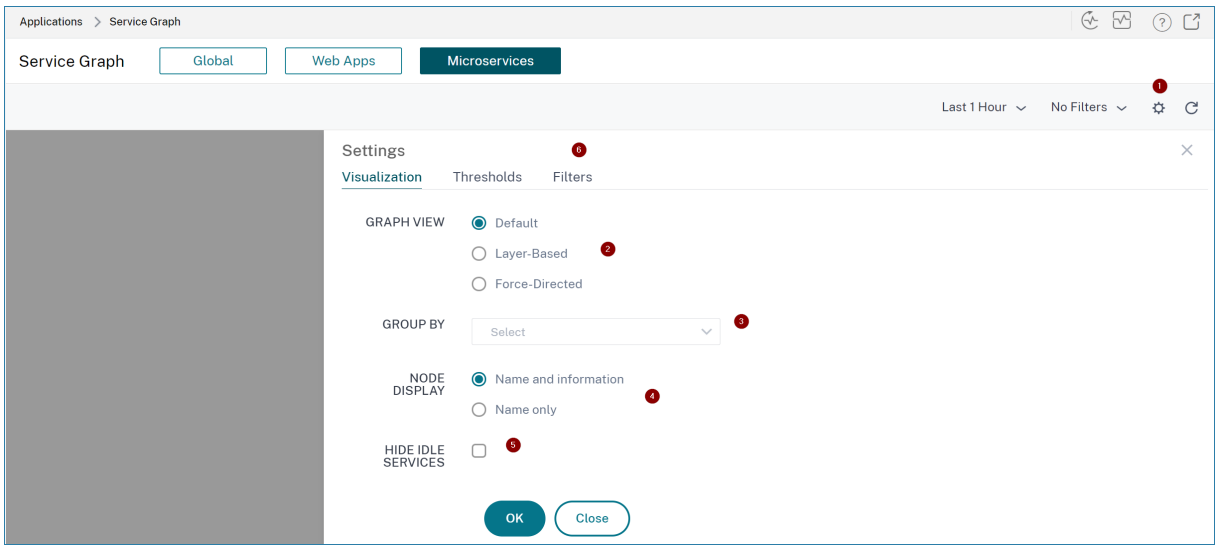
すべてのフィルタをクリアするには、[すべてクリア] をクリックします。



または、検索テキストボックスを使用してサービス名を入力して、サービスグラフに結果を表示することもできます。



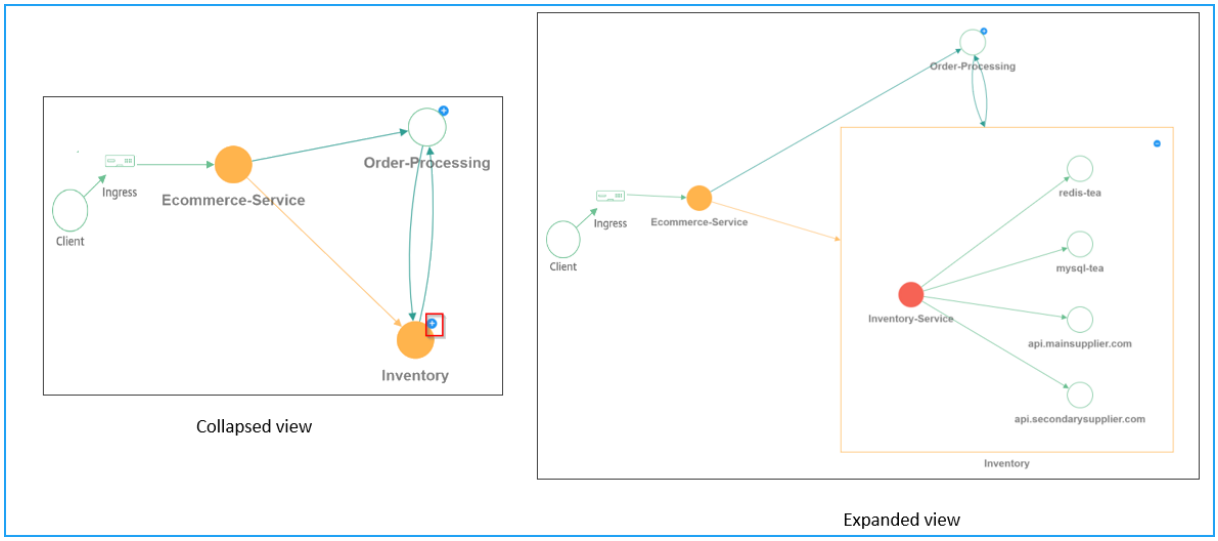
設定オプションの使用



1 — 設定アイコン

2 — サービスグラフをデフォルト、レイヤーベース、または強制方向ビューとして表示するオプション

3： リストからオプションを選択し、カテゴリに基づいてサービスを表示します。リストからカテゴリを選択した後、グラフの [**+**] をクリックして、すべてのサービスを表示します。

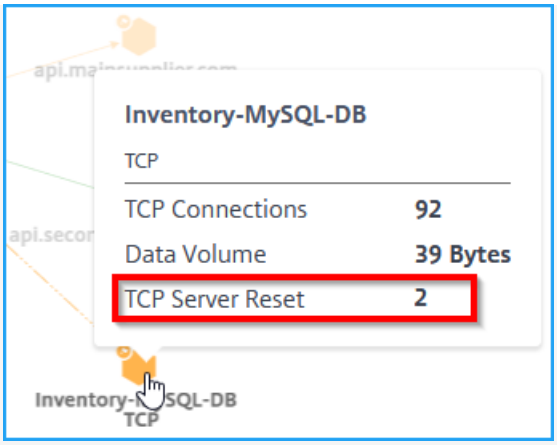


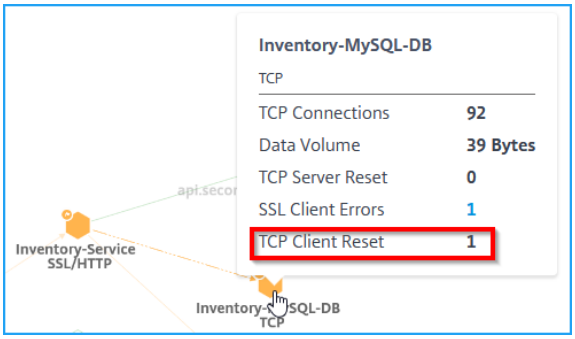
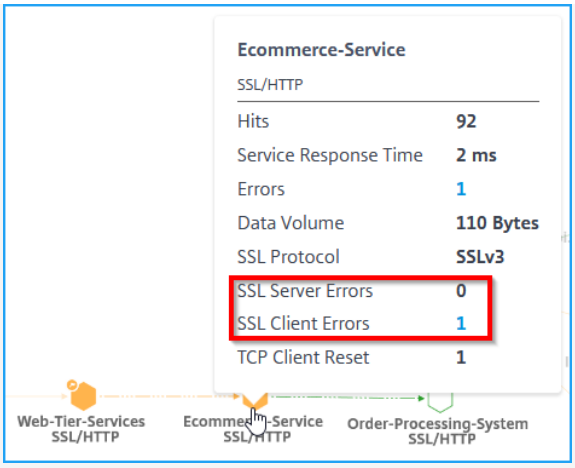
4： サービスの表示方法に関するオプションを選択できます。

5 -設定を保存するか、デフォルトにリセットするオプション。

エラーを分析する

エラーを示すサービスにマウスポインタを合わせます。

エラー	説明
	**TCP** サーバのリセットは、サーバから開始された TCP リセットの合計を示します。

エラー	説明
	**TCP** クライアントのリセットは、クライアントによって開始された TCP リセットの合計を示します。
	SSL クライアントエラーは、クライアントからの SSL エラーの合計を示します。(SSL クライアント認証エラーなど)。 SSL サーバエラー: サーバからの SSL エラーの総数を示します。(SSL 証明書が不明など)

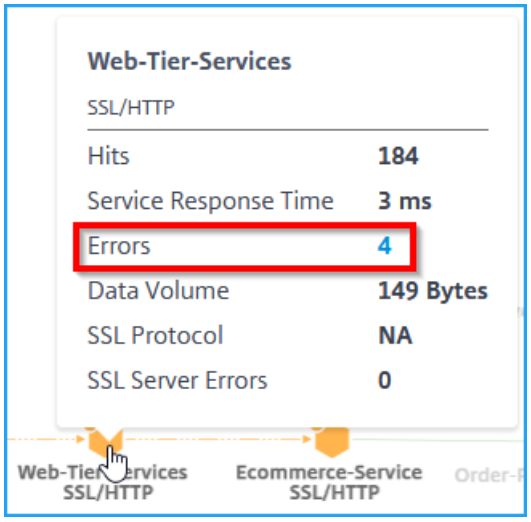
注

- クライアントエラー数が **1** 以上の場合、クライアントエラー数（プロトコルタイプに関係なく）は、どのサービスにも表示されます。
- 任意のサービスに対して表示されるクライアントのエラー数は、そのエラーがクライアント側からのものであることを示します。

HTTP トランザクションの詳細を表示する

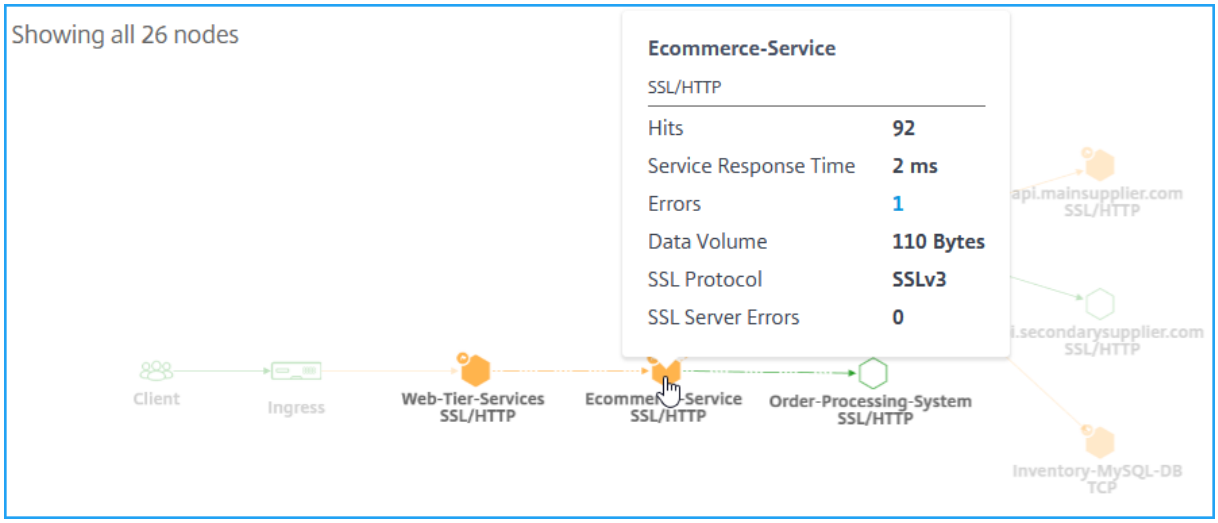
注

エラーを表示するには、誤ったサービスの上にマウスポインタを置いて、問題数をクリックします。

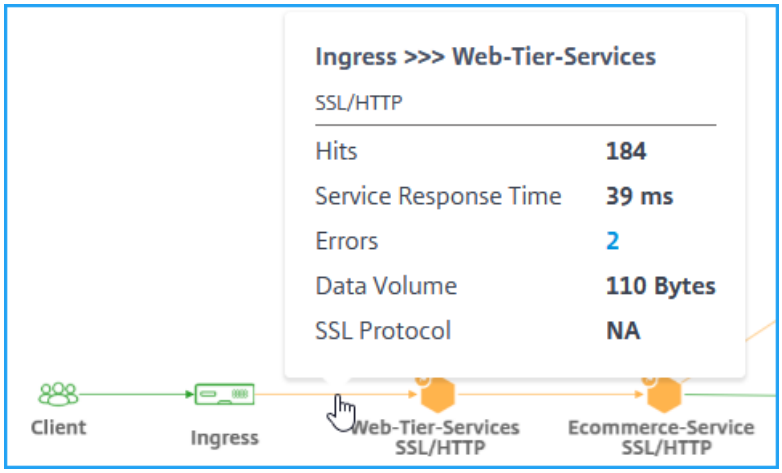


この図に示されている例では、コンポーネントサービスの通信方法を示すアプリケーションのエンドツーエンドのネットワークマップを表示できます。

e コマースサービスの上にマウスポインターを置くと、**e** コマースサービスの指標の詳細を表示できます。



Citrix ADM では、Ingress とサービスの間のトランザクションの詳細を表示することもできます。マウスポインタを合わせると、Ingress とサービスの間のエラー合計、平均サービスレスポンス時間などの詳細が表示されます。



「ヒット」(Hits) — サービスが受信したヒットの合計数を示します。

サービス応答時間 — 最初のバイトまでの時間（TTFB）の応答にサービスから要した平均応答時間を示します。

[**Err** ors]：4xx、5xx などの合計エラーを示します。

「データボリューム」— サービスによって処理されるデータの合計量を示します。

「**SSL** プロトコル」— SSL プロトコルのバージョンを示します。

[**Ingress**] と [**service**] の間の矢印をクリックして、詳細なトランザクションを表示します。

詳しくは、「Web トランザクションの分析の表示」を参照してください。

サービスグラフでのしきい値の設定

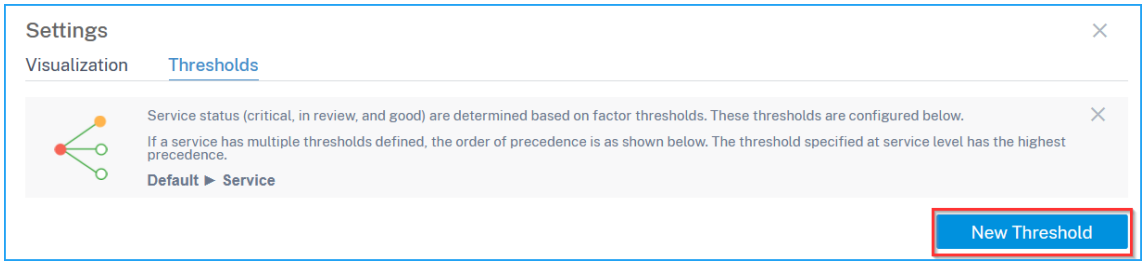
May 7, 2021

管理者は、Kubernetes サービスのしきい値を設定できます。Citrix ADM では、サービスの応答時間とエラー数に基づいて、サービスの状態（重大、レビュー、および良好）が表示されます。デフォルトでは、すべてのサービスに適用される デフォルトのしきい値（サービス応答時間 = 200 ms、エラー数 = 0）を表示できます。

> 注
>
> デフォルトのしきい値は削除できません。

新しいしきい値を設定するには、次の手順を実行します。

1. [アプリケーション**] > [**サービスグラフ] で、[マイクロサービス] タブをクリックします。
2. 設定アイコンをクリックし、[しきい値] タブを選択します。
3. 新しいしきい値を設定するには、[New Threshold] をクリックします。



「新しいしきい値」ページが表示されます。

4. 次のパラメータを設定します。

   a)「名前」— しきい値の名前を指定します。

   b) [マイクロサービス] で、しきい値を適用するサービスを選択します。

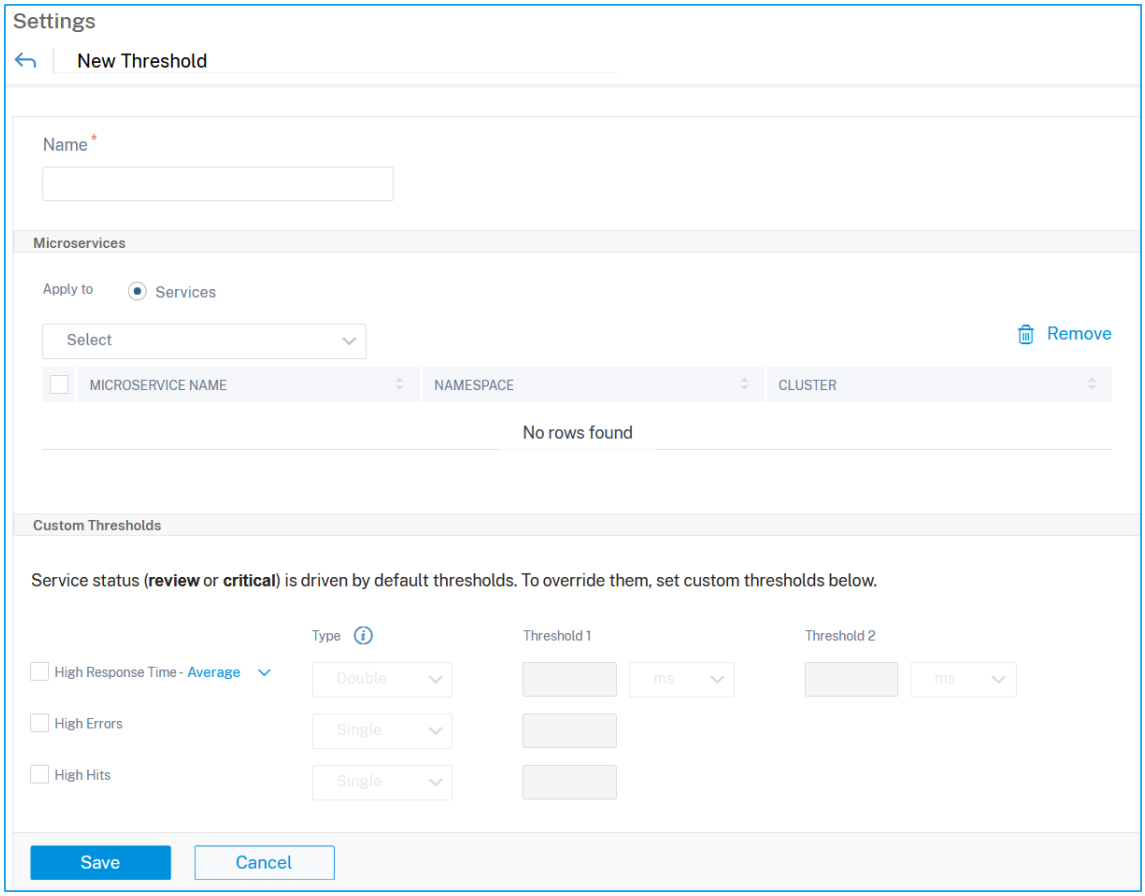
   c) [しきい値] で、[シングル] または [ダブル] を選択します。

      - 高い応答時間（平均、P99、P99.9）
      - エラーが高い
      - ハイヒット

   d) しきい値を指定します。

   > 注
   >
   > 二重しきい値を選択した場合は、次のことを確認します。
   >
   > ```
   > 1    - しきい値 1 の値が、しきい値 2 の値より小さくなっています。たとえば、しきい値 1 を 250 ミリ秒に設定する場合、しきい値 2 は 251 ミリ秒以上にする必要があります。
   > 2
   > 3    - しきい値 1 の値は、しきい値 2 の値と同じにすることはできません。
   > ```

5. [保存] をクリックします。



しきい値が正常に作成されました。しきい値の詳細は ⊠ しきい値 | Thresh **old** s | emdw⊠・ページで表示できます。

> 注
>
> Citrix ADM は、選択したメトリックに基づいてサービスの最終スコアとステータスを計算します。たとえば、しきい値の構成で［**High** Hits］のみを選択した場合、Citrix ADM はデフォルトのしきい値（応答時間 = 200 ミリ秒、エラーカウント = 0）と高いヒットを使用してサービススコアとステータスを計算します。

単一しきい値

すべてのメトリックスまたは選択したメトリックスに対して単一のしきい値を構成すると、Citrix ADM:

- 各メトリックの現在の値を、各メトリックで設定されたしきい値を比較します。
- 各メトリックで超過したしきい値に基づいて、ペナルティの合計を計算します。

  > 注
  >
  > いずれかのメトリックスがしきい値に違反していない場合、ペナルティはそれに応じて計算されます。

- ペナルティ計算に基づくサービススコアとサービスステータスを表示します。

二重しきい値

すべてのメトリックスまたは選択したメトリックの二重しきい値を構成すると、Citrix ADM:

- 各メトリックの現在の値を、各メトリックで設定されたしきい値を比較します。
- 現在の値が次の値であるかどうかを調べます。
  - しきい値 1 より小さい
  - しきい値 1 としきい値 2 の間
  - しきい値 2 より大きい
- 各メトリックで超過したしきい値に基づいて、ペナルティの合計を計算します。

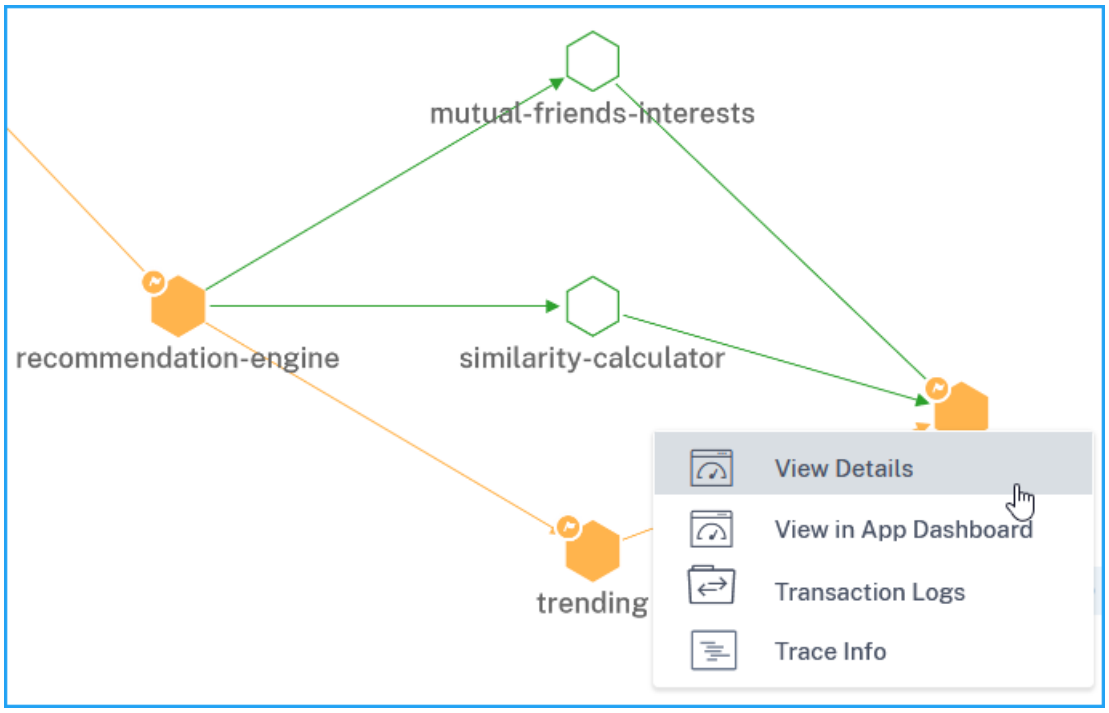
  > 注
  >
  > いずれかのメトリックスがしきい値に違反していない場合、ペナルティはそれに応じて計算されます。

- ペナルティ計算に基づくサービススコアとサービスステータスを表示します。

サービス詳細の表示

May 7, 2021

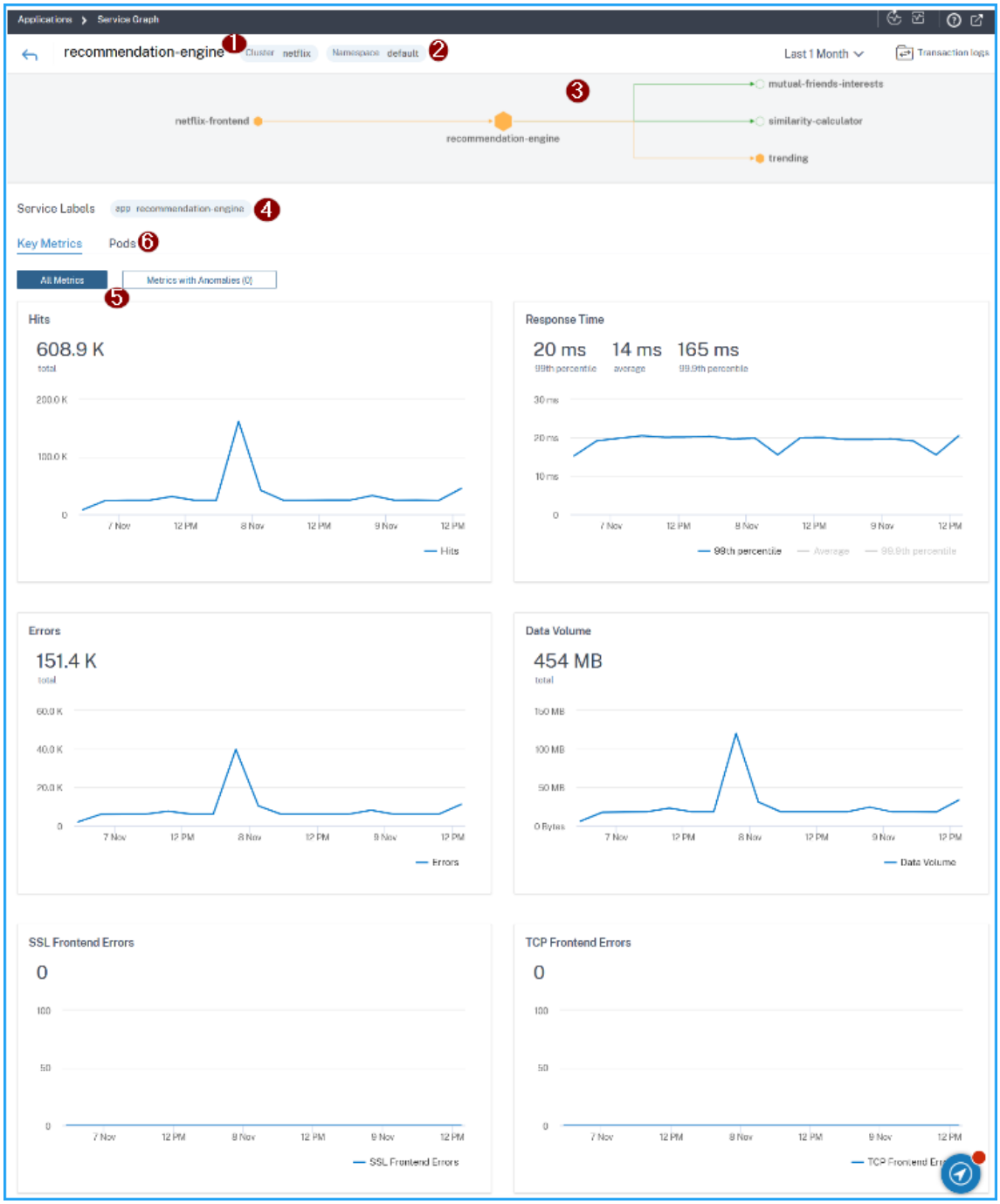
サービスをクリックし、[詳細の表示] を選択します。



サービスの詳細ページでは、次の項目を表示できます。

- サービスがホストされているクラスター名 (1)
- サービスの名前空間とサービスラベル (2) (4)
- 選択したサービスに接続されているすべての関連する着信および発信サービス (3)
- ヒット、レスポンス時間、エラー、データ量、SSL フロントエンドエラー、TCP フロントエンドエラーなどのグラフ形式のサービスキーメトリック。[異常のあるメトリック] タブでは、特定の期間 (5) の異常を表示できます。

  詳しくは、「ゴールデンシグナルのメトリックを使用してサービスを監視する」を参照してください。
- サービスに関連付けられたバックエンド Pod (6)。



これらの主要なメトリックの傾向を使用して、特定の期間におけるサービスのパフォーマンスを分析できます。

たとえば、サービスが、すべての要求に対してサービス応答時間が 700 ミリ秒を超えると示しているとします。管理者は、次の操作を実行できます。

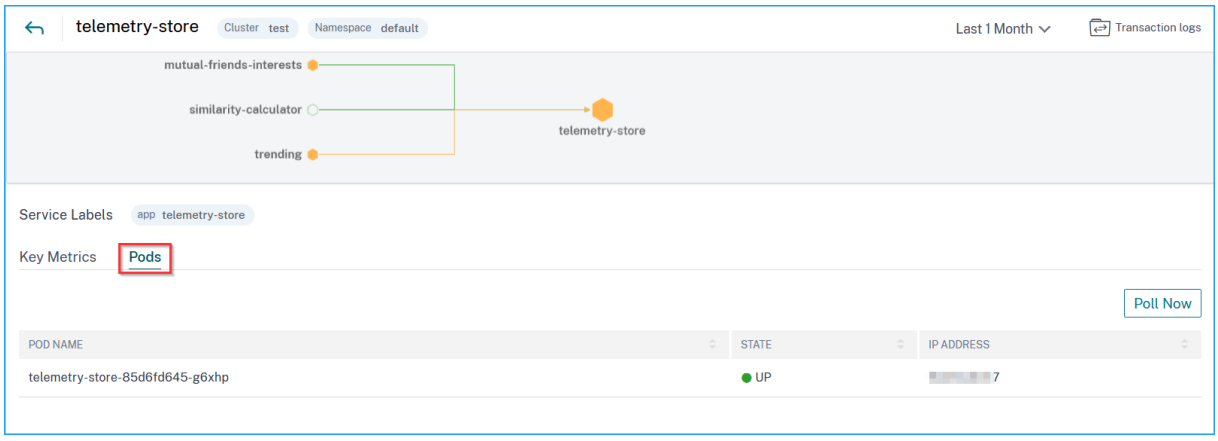
- 特定の期間におけるサービス応答時間メトリックの傾向を分析する
- 問題のトラブルシューティング
- サービス応答時間メトリックを再度確認して、応答時間が改善されたかどうかを分析します。

メトリックスの詳細

メトリック	説明
ヒット数	サービスによって受信されたリクエストの総数
エラー	サービスからの HTTP エラーの合計
サービス応答時間	最初のバイトまでの時間（TTFB）の応答にサービスから要した平均応答時間。
データ量	サービスによって処理された合計データ量
SSL フロントエンドエラー	サービスからの SSL フロントエンドエラーの総数。例:SSL クライアントの失敗
SSL バックエンドエラー	サービスからの SSL バックエンドエラーの合計。例:SSL クライアントエラー
TCP バックエンドエラー	サービスからの TCP バックエンドエラーの合計。例:TCP サーバのリセット
TCP フロントエンドエラー	サービスからの TCP フロントエンドエラーの合計。例:TCP クライアントのリセット

バックエンドポッドの詳細を表示する

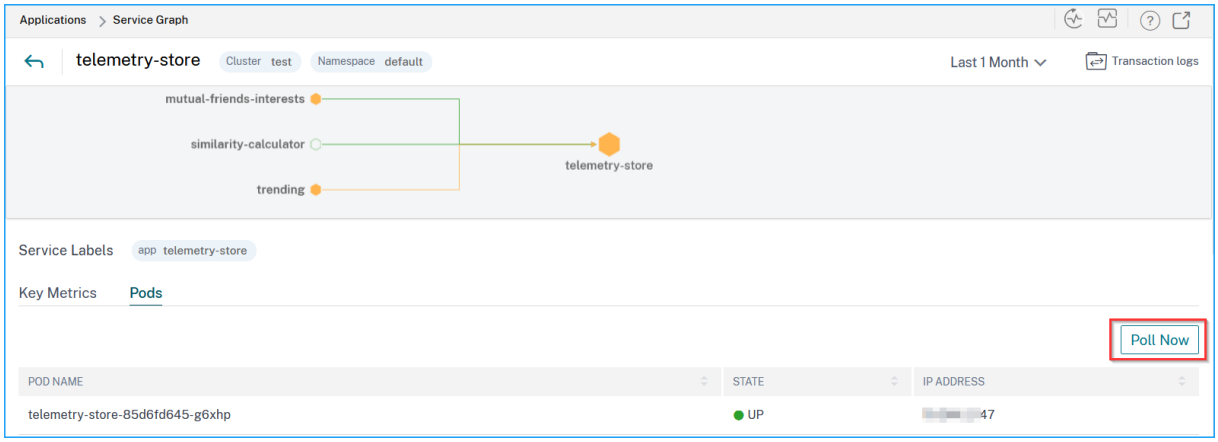
[**Pods**] タブをクリックして、サービスに関連付けられたバックエンド Pod を表示します。



- ポッド名 — ポッド名を示します
- **Status** — Pod が実行中 (UP) かそうでないか (DOWN) を示します。
- **IP** アドレス — ポッドの IP アドレスを表します。

[今すぐ投票] オプションを使用して **Pod** のステータスを取得します

[今すぐポーリングする] オプションは、クラスターから最新の Pod ステータスをフェッチします。



ゴールデンシグナルのメトリックを使用してサービスを監視する

Kubernetes クラスターで実行されているサービスのゴールデンシグナルメトリックは、特定の期間における潜在的な異常を検出できる一連のメトリックのことです。Kubernetes クラスターに 100 個のマイクロサービスがある場合、頻繁な問題があるサービスを特定するのは難しい場合があります。次の 3 つの主要なメトリックは、Citrix ADM サービスグラフが Kubernetes サービスの潜在的な異常を特定するのに役立つゴールデンシグナル指標です。

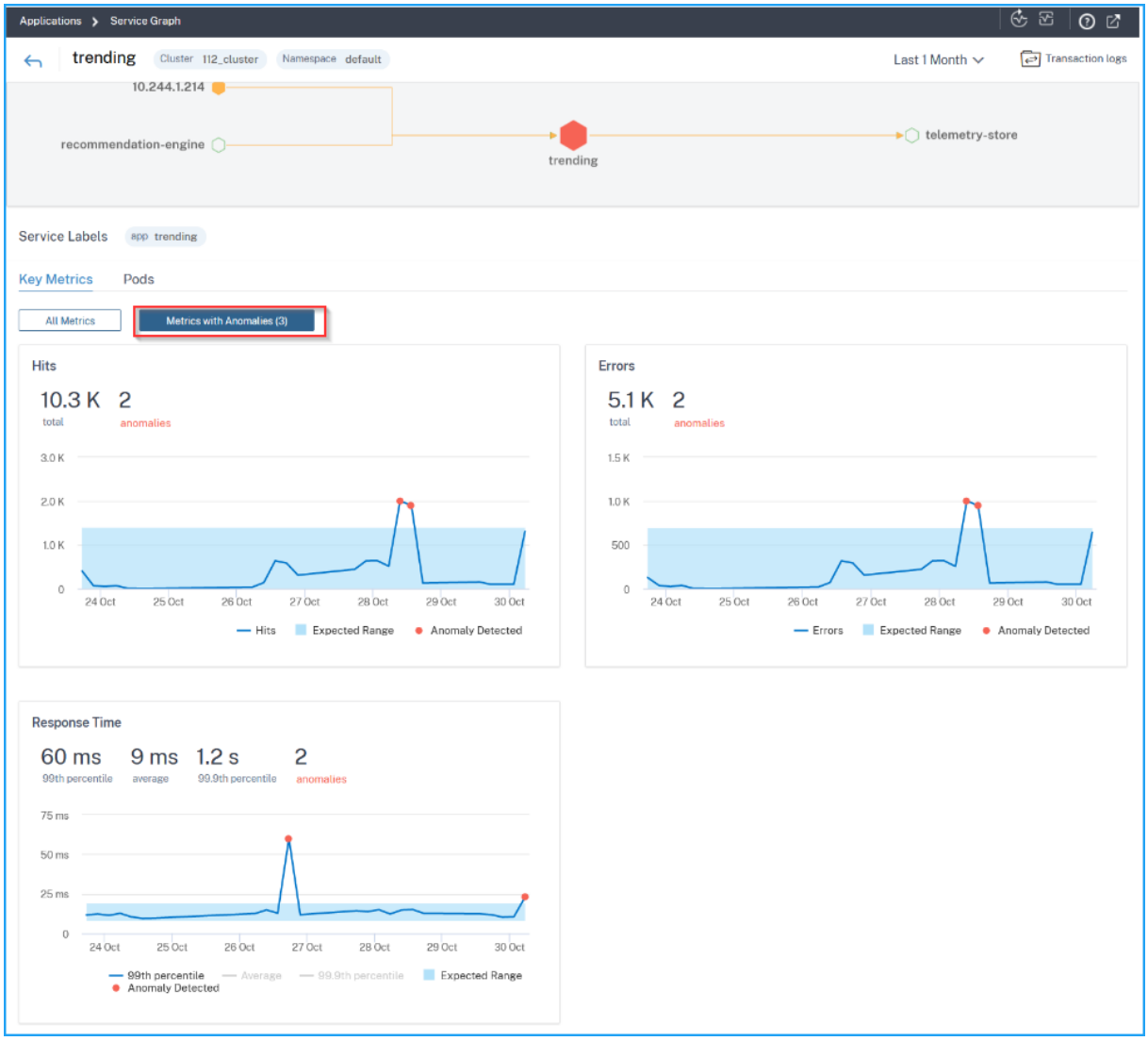
- ヒット数
- 応答時間（平均）と応答時間（P99）
- エラー

管理者は、これらのメトリックを使用して、次の操作を実行できます。

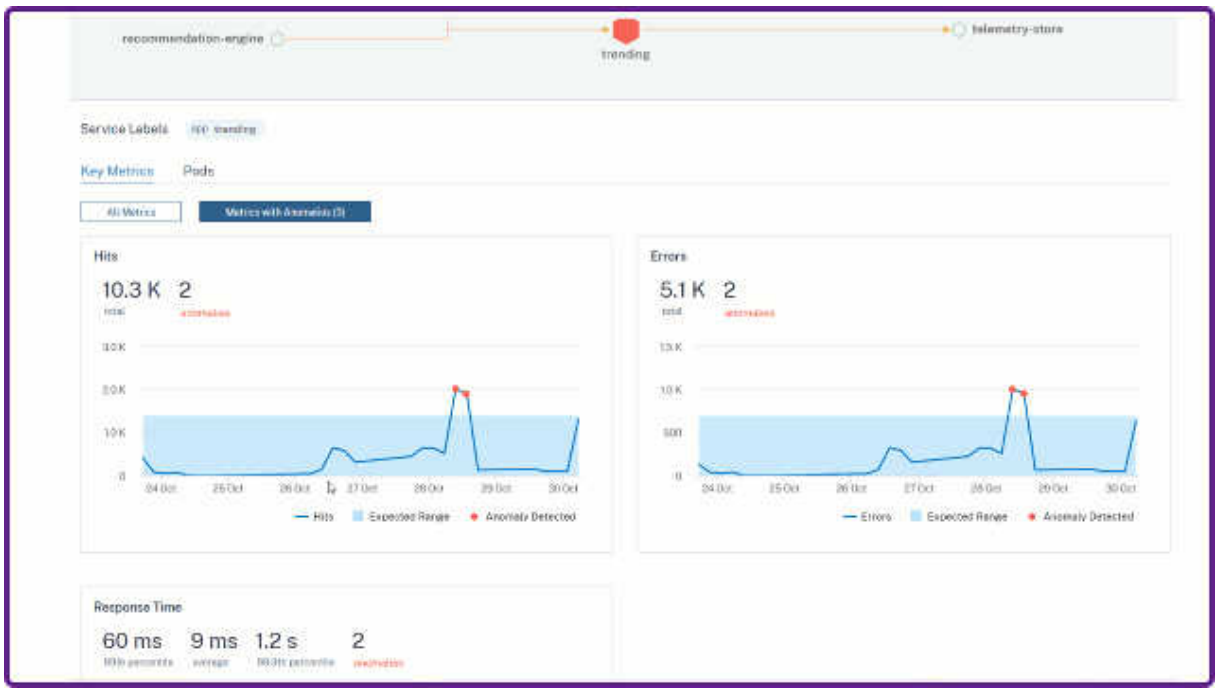
- サービスステータスの識別
  - **Critical** — サービスの複数のメトリックに異常またはしきい値違反がある
  - 確認 — サービスのいずれかのメトリックに異常またはしきい値違反がある
  - 良好 — 異常なし、またはしきい値違反のないサービス
- 各メトリックで識別される異常の数を分析する
- 問題のトラブルシューティングを行い、大きな影響を回避する

異常の特定

サービスをクリックして [**View Details**] を選択すると、サービスの詳細ページにすべてのメトリックの概要が表示されます。「異常のあるメトリック」タブをクリックして、異常の詳細を表示します。

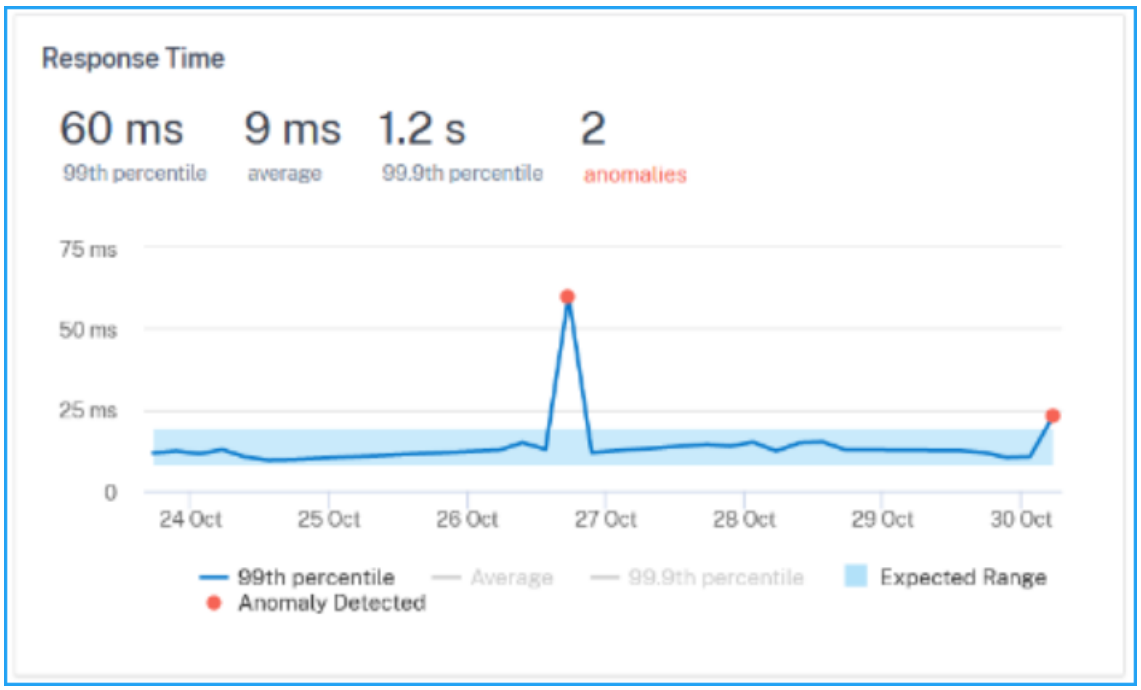


各メトリックについて、予測される範囲を超えるたびに検出された異常をグラフで表示できます。オプションをクリックすると、グラフ内のビューをフィルタできます。



サービスの応答時間（P99）の異常を分析することを検討してください。

[応答時間] では、選択した期間の次の詳細を表示できます。



- **99** パーセンタイル：選択した期間の要求の 99% が 60 ミリ秒未満であることを示します。
- **Average**： サービスからの平均応答時間を示します。
- **99.9** パーセンタイル — サービスからの応答時間が最も高いことを示します

- [**Anomalies**]: 検出された異常の総数を示します

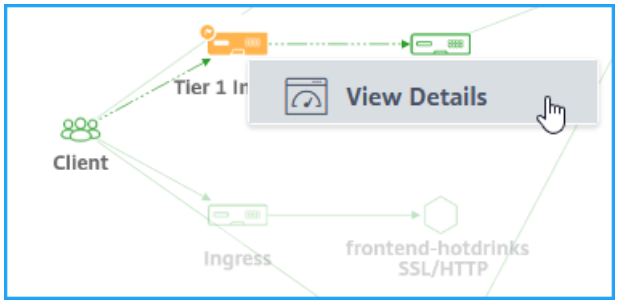
グラフでは、選択した期間の予測範囲を表示することもできます。例によると、次のものを表示できます。

- 期待される応答時間の範囲は、1 ミリ秒から 9 ミリ秒です。
- サービス応答時間が期待される範囲（1 ミリ秒から 9 ms）を超えているため、サービスに対して 2 つの異常（60 ミリ秒と 25 ミリ秒）が検出されました。

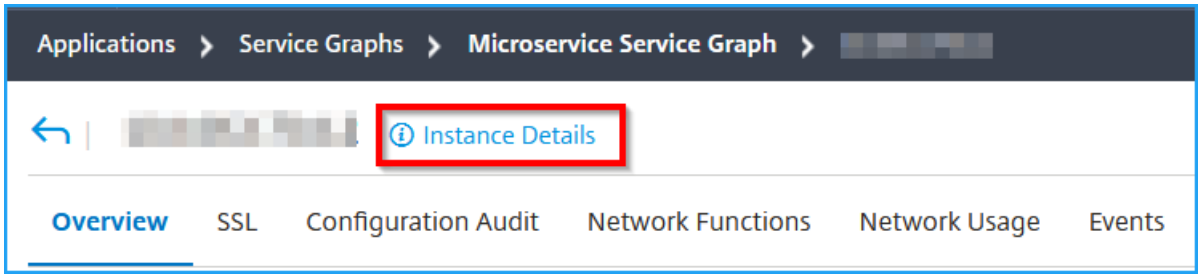
問題のトラブルシューティングに関する進入の詳細の表示

May 7, 2021

サービスグラフで、入力をクリックし、［詳細の表示］を選択して、Kubernetes クラスター用に構成されている Citrix ADC インスタンスの詳細を視覚化します。

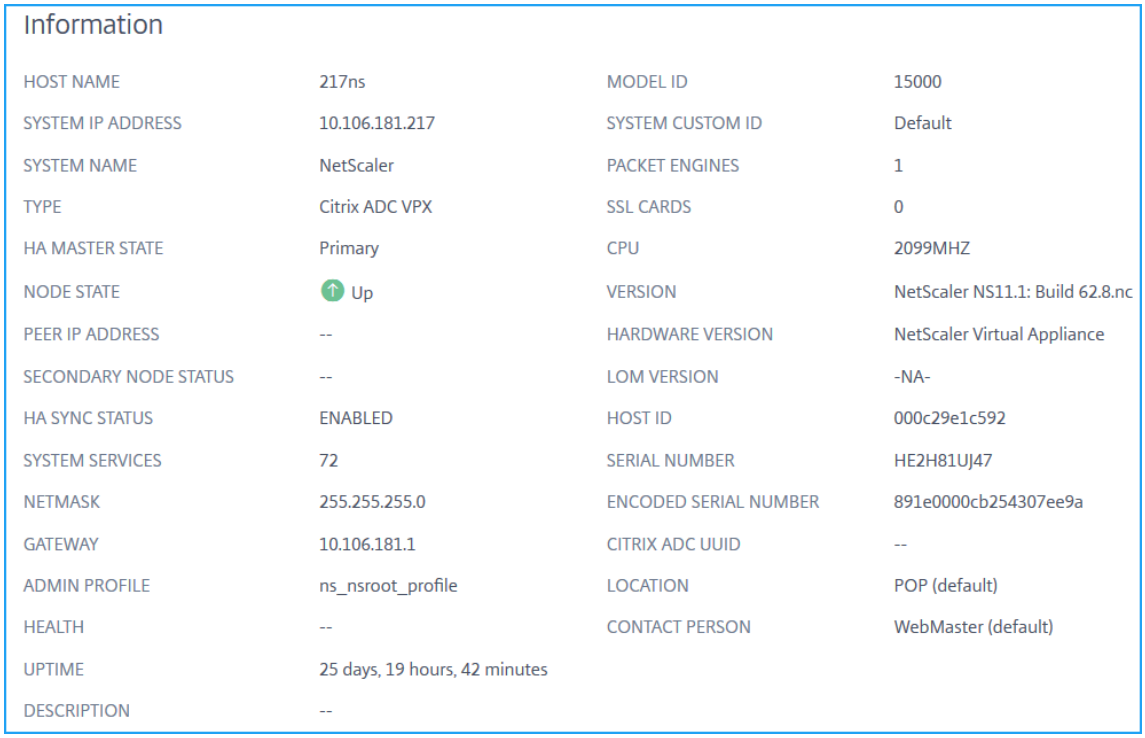


[インスタンスの詳細] をクリックして詳細を表示します。

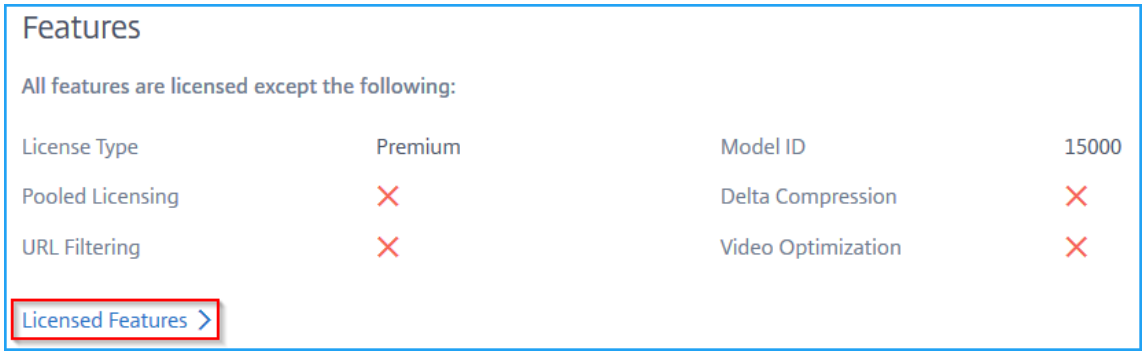


次の詳細が表示されます。

- 情報 -インスタンスタイプ、デプロイタイプ、バージョン、モデルなどのインスタンスの詳細。



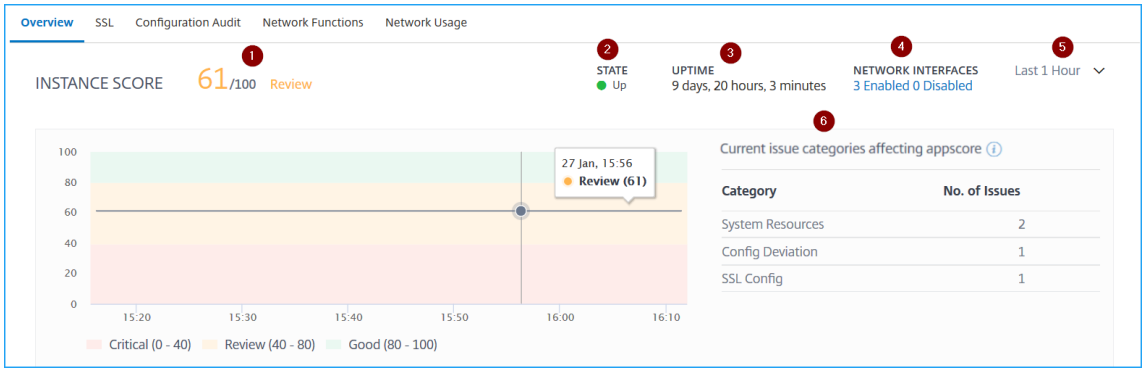
- 機能：デフォルトでは、ライセンスされていない機能が表示されます。ライセンスされた機能を表示するには、[ライセンスされた機能] をクリックします。



- **Modes** — デフォルトでは、インスタンスで無効になっているすべてのモードが表示されます。[**View Enabled Modes**] をクリックして、インスタンスの有効なモードを表示します。

インスタンスダッシュボードにはインスタンスの概要が表示され、次の詳細を確認できます。

- インスタンススコア

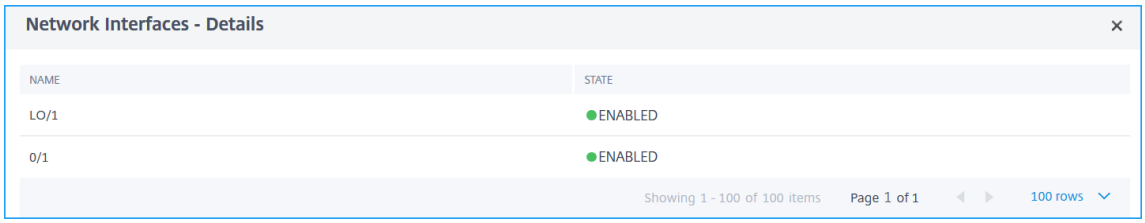


1 — 選択した期間の現在の Citrix ADC インスタンススコアを示します。最終的なスコアは、**100** からペナルティ合計を差し引いたものとして計算されます。グラフには、選択した期間のスコア範囲が表示されます。

2： Citrix ADC インスタンスの現在のステータス（[アップ]、[停止]、[サービス外] など）を示します。

3 — Citrix ADC インスタンスが起動して実行されている期間を示します。

4 — インスタンスに対して有効または無効になっているネットワークインターフェイスの合計を示します。クリックすると、ネットワークインターフェイス名やステータス (有効または無効) などの詳細が表示されます。



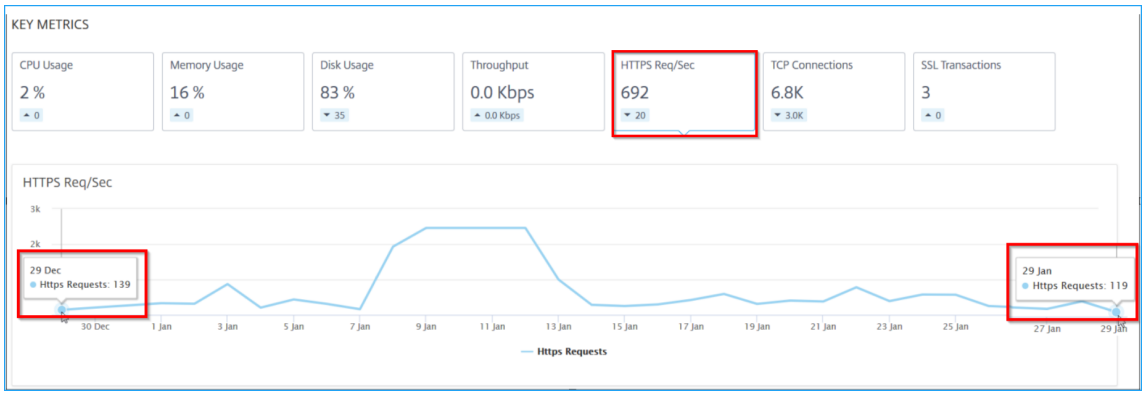
5 — インスタンスの詳細を表示するには、リストから期間を選択します。

6 — ADC インスタンスの問題と問題のカテゴリ合計を表示します。

- 主要メトリック

  各タブをクリックして詳細を表示します。各指標で、選択した時間の平均値と差分値を表示できます。

  次の図は、HTTPS 要求/秒の例で、選択した期間は過去 1 か月間です。値 **692** は過去 1 か月の平均 HTTPS 要求/秒で、値 **20** は差の値です。グラフでは、最初の値は **139** 、最後の値は **119** です。差の値は **139** ～**119** **= 20** です。



  選択した期間について、次のインスタンスメトリックスをグラフ形式で表示できます。

  - **CPU** 使用率 — 選択した期間におけるインスタンスからの平均 CPU%（パケット CPU と管理 CPU の両方で表示）。
  - 「メモリ使用量」— 選択した期間におけるインスタンスからの平均メモリ使用率 (%)。
  - [**Disk Usage**] — 選択した期間におけるインスタンスからの平均ディスク容量%。
  - スループット — 選択した期間にインスタンスによって処理された平均ネットワークスループット。
  - **HTTPS** リクエスト/秒 — 選択した期間にインスタンスが受信した HTTPS リクエストの平均値。
  - **TCP** 接続 — 選択した期間にクライアントとサーバーによって確立された平均 TCP 接続。
  - **SSL** トランザクション — 選択した期間にインスタンスによって処理された平均 SSL トランザクションです。

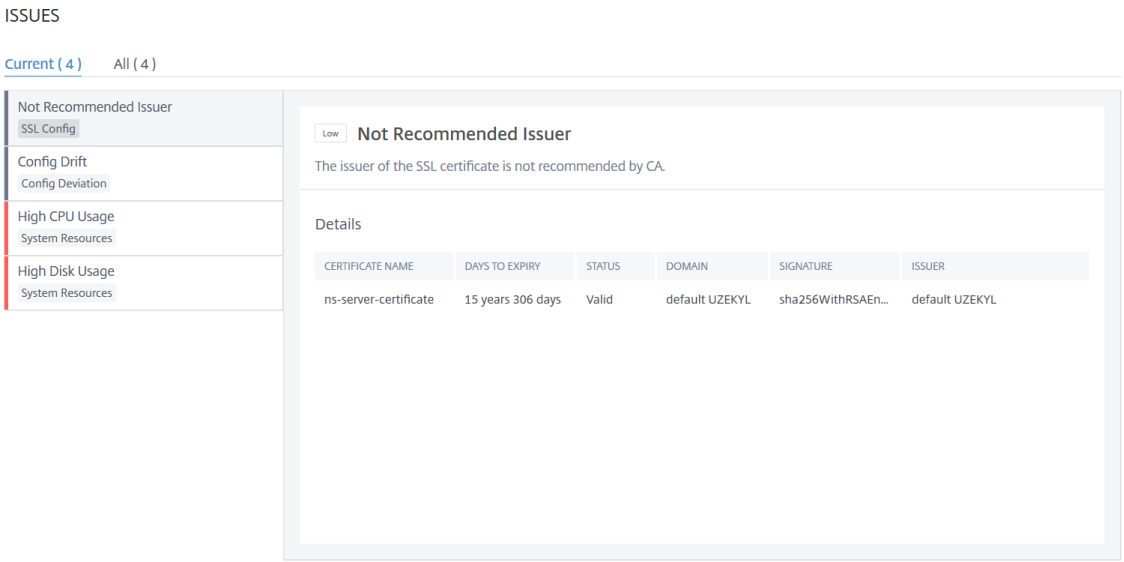
- 問題

  Citrix ADC インスタンスで発生する次の問題を表示できます。

問題カテゴリ	説明	問題
システムリソース	CPU、メモリ、ディスク使用率など、Citrix ADC システムリソースに関連するすべての問題を表示します。	- 高い CPU 使用率 - 高いメモリ使用量

問題カテゴリ	説明	問題
		- 高いディスク使用率
		- SSL カードの障害
		- 電源障害
		- ディスクエラー
		- フラッシュエラー
		- NIC を破棄します。
SSL 設定	Citrix ADC インスタンスの SSL 構成に関連するすべての問題を表示します。	-SSL 証明書の有効期限が切れました
		- 推奨されない発行者
		- 推奨されていないアルゴリズム
		- 推奨しないキー強度。
設定偏差	Citrix ADC インスタンスで適用された構成ジョブに関連するすべての問題を表示します。	-コンフィグドリフト
		- 実行とテンプレート
容量の問題	ADC 容量の問題を表示します。ADM は、ADC インスタンスから 5 分ごとにこれらのイベントをポーリングし、パケットドロップまたはレート制限カウンタが存在する場合は、その増加を表示します。問題は、次の容量パラメータに分類されます。	- スループット制限に達しました
		- PE CPU 制限に達しました
		- PPS 制限に達しました
		- SSL スループットレート制限
		- SSL TPS レート制限
ネットワーク	インスタンスで発生する運用上の問題を表示します。	詳しくは、「新しいインジケータによるインフラストラクチャ分析の強化」を参照してください。

各タブをクリックして、問題を分析し、トラブルシューティングします。たとえば、選択した期間について、インスタンスに次のエラーがあるとします。



- [**Current**] タブには、インスタンススコアに影響している現在の ADC 運用上の問題が表示されます。
- [すべて] タブには、選択した期間に検出されたすべてのインフラストラクチャの問題が表示されます。

分散トレース

May 7, 2021

サービスグラフでは、分散トレーシングビューを使用して、次のことができます。

- サービス全体のパフォーマンスを分析します。
- 選択したサービスとその相互依存サービス間の通信フローを視覚化します。
- エラーを示しているサービスを特定し、誤ったサービスをトラブルシューティングします。
- 選択したサービスとその相互依存サービス間のトランザクションの詳細を表示します。

前提条件

サービスのトレース情報を表示するには、次の操作を行う必要があります。

- east-west トラフィックを送信しながら、アプリケーションが次のトレースヘッダーを維持していることを確認します。

- x-request-id
- x-b3-traceid
- x-b3-spanid
- x-b3-parentspanid
- x-b3-sampled
- x-b3-flags
- x-ot-span-context

- **1.7.23** より前の **CIC** ビルドの場合、CPX `NS_DISTRIBUTED_TRACING` YAML ファイルをおよび値として更新します `yes`


```
# Add cic as a sidecar
- name: cic
  image: "quay.io/citrix/citrix-k8s-ingress-controller:1.5.6"
  env:
  - name: "EULA"
    value: "yes"
  - name: "NS_IP"
    value: "127.0.0.1"
  - name: "NS_PROTOCOL"
    value: "HTTP"
  - name: "NS_PORT"
    value: "80"
  - name: "NS_DEPLOYMENT_MODE"
    value: "SIDECAR"
  - name: "NS_ENABLE_MONITORING"
    value: "YES"
  - name: "NS_DISTRIBUTED_TRACING"
    value: "yes"
  - name: "NS_LOGPROXY"
    value: "coe-tracing.default.svc.cluster.local"
  - name: POD_NAME
    valueFrom:
      fieldRef:
        apiVersion: v1
        fieldPath: metadata.name
  - name: POD_NAMESPACE
    valueFrom:
      fieldRef:
        apiVersion: v1
        fieldPath: metadata.namespace
  args:
    - --ingress-classes
      watches-ingress
  imagePullPolicy: Always
```

- **1.7.23** 以降の **CIC** ビルドでは、ConfigMap を使用する必要があります。

  ConfigMaps を使用すると、Pod から設定を分離し、ワークロードを移植することができます。ConfigMaps を使用すると、ワークロード構成を簡単に変更および管理でき、構成データを Pod 仕様にハードコードする必要性を軽減できます。

  ConfigMap サポートでは、Citrix ingress controller ポッドを実行したまま構成を自動的に更新できます。更新後に Pod を再起動する必要はありません。詳しくは、「入力コントローラの ConfigMap サポート」を参

照してください。

ConfigMap を使用すると、分散トレース、イベント、監査ログなどを有効または無効にできます。コンフィグマップを使用するには、次の手順に従います。

1. 必要なパラメータを使用して YAML ファイルを作成します。

   次の YAML ファイルの例では、分散トレースが有効になり、監査ログ、イベント、トランザクションなどのその他の変数が無効になっています。

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cic-configmap
  namespace: default
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG: |
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <ADM-AgentIP> / <ADM-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'false'
      events:
        enable: 'false'
    transactions:
      enable: 'false'
      port: 5557
<!--NeedCopy-->
```

   > 注
   >
   > 0 から 100 Samplingrate までの値を指定できます。Citrix ADM には、上記のトレーストランザクション数が表示されます。

2. 以下を使用して ConfigMap を展開します。

```
kubectl create -f <configmap-yaml>.yaml
```


3. CPX YAML ファイルを編集し、envFromまたはargsを使用して次の引数を指定します。

```
envFrom:
 - configMapRef:
     name: cic-configmap
<!--NeedCopy-->
```

または

```
args:
   - --configmap
     default/cic-configmap
```

ConfigMap の YAML 設定は CIC にデプロイされます。

4. 任意の変数の値を変更する場合は、ConfigMap で値を編集します。この例では、他のすべての変数を**false**から**true**に変更しています。

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cic-configmap
  namespace: default
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG: |
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <ADM-AgentIP> / <ADM-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'true'
      events:
        enable: 'true'
    transactions:
      enable: 'true'
      port: 5557
```



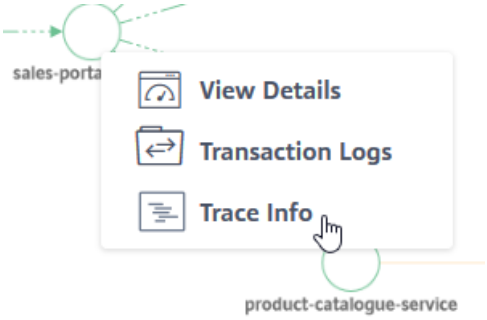
```
29      <!--NeedCopy-->
```

5. 次のコマンドを使用して ConfigMap を再適用します。

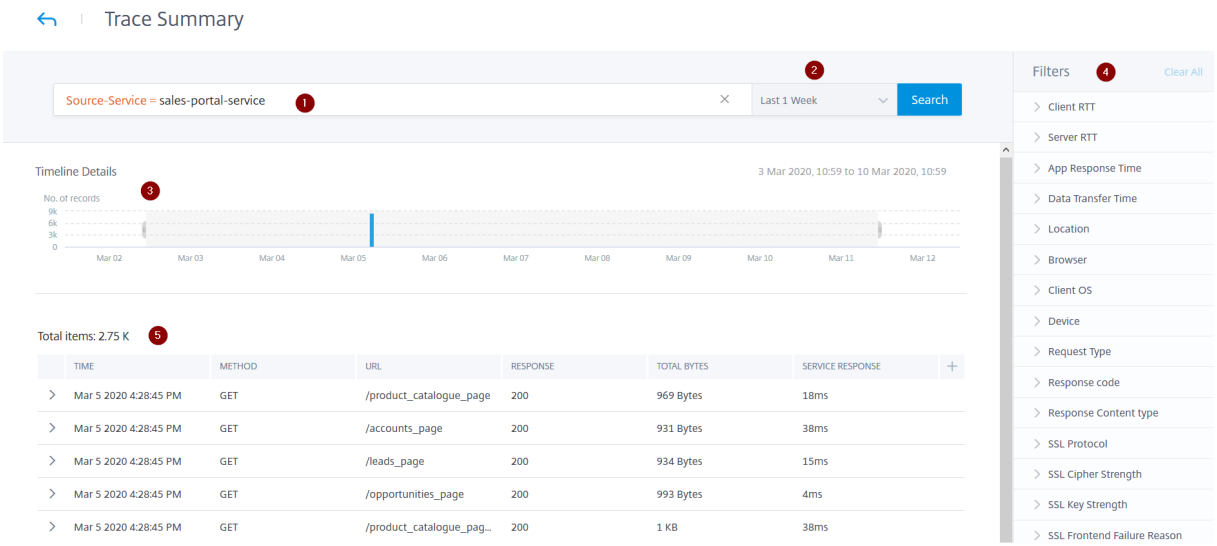
   ```
   kubectl apply -f <yaml-file>.yaml
   ```

サービストレースの詳細の表示

サービスグラフでサービスをクリックし、[トレース情報] を選択します。



選択したサービスの [トレースの概要] ページが表示されます。



[トレースの概要] には、次の情報が表示されます。

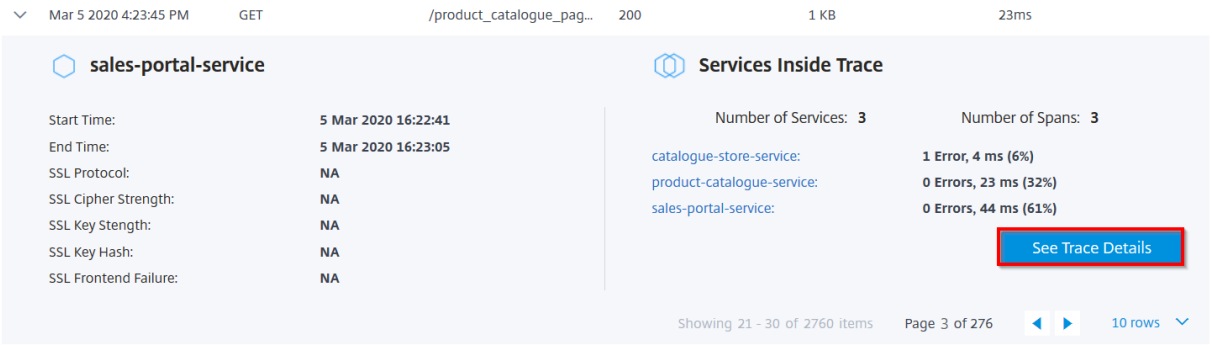
- 提案と演算子を使用したトランザクションを検索できる拡張検索 (1)。詳しくは、「高度な検索」を参照してください。
- 1 時間、12 時間、1 日、1 週間、1 ヶ月、カスタム時間 (2) などの期間を選択できる期間リスト。
- 「タイムラインの詳細」グラフ。ドラッグして選択して、特定の期間 (3) の結果を表示できます。
- 各メトリックからオプションを選択できる [フィルタ] パネル (4)。
- 選択したサービスのトランザクション詳細 (5)。

取引の詳細の表示

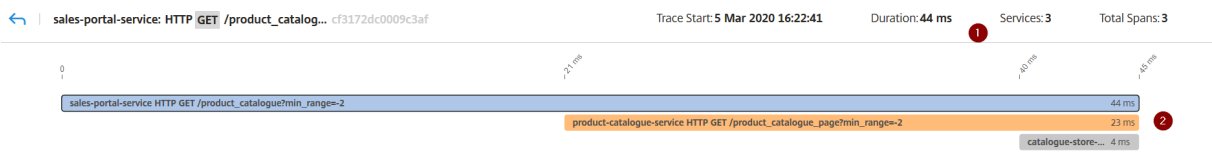
トランザクションをクリックして、詳細情報をドリルダウンします。次のような、選択したサービスの取引詳細を表示できます。

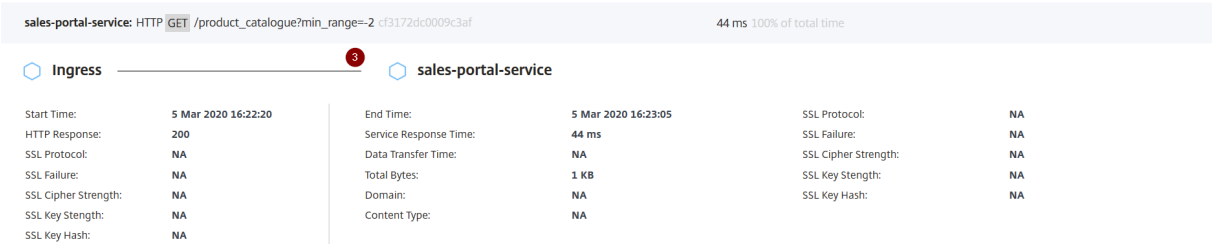
- 開始日時
- 終了時間
- SSL メトリック
- 相互依存サービスとの通信（各サービスとのエラーおよび応答時間とともに）。

次の例は、`catalogue-store-service`からのエラーを示しています。詳しくは、[トレースの詳細を表示] をクリックします。



「トレースの詳細」ページが表示されます。



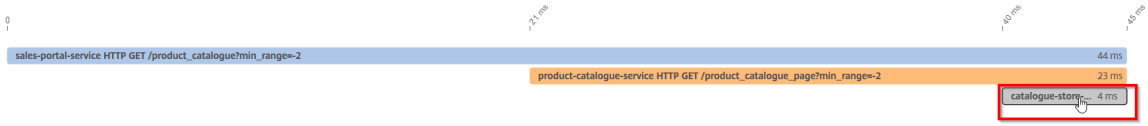


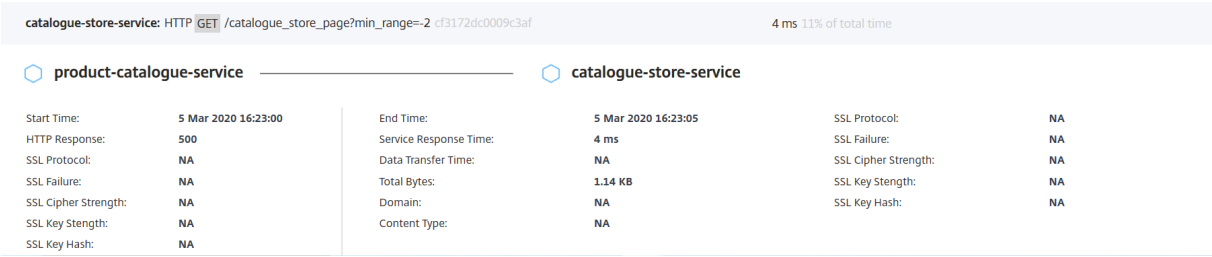
1 — トランザクションの開始時間、応答時間、サービスの合計、および合計スパンが表示されます。

2 — 依存関係間のサービスと通信した、選択したサービスの詳細を表示します。各トランザクションをクリックすると、詳細を表示できます。

3 — 各サービスのトランザクションの詳細を表示します。

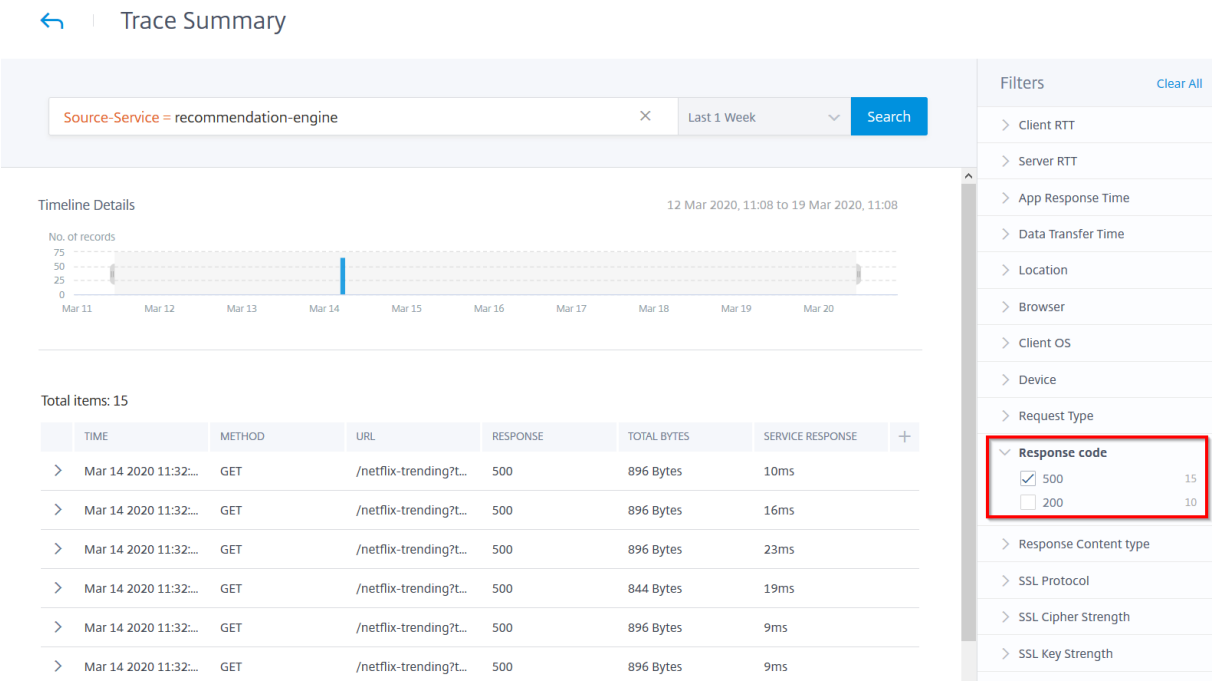
例の画像によると、catalogue-store-serviceはエラーを示しました.catalogue-store-serviceで利用可能なトランザクションをクリックします。





product-catalogue-serviceとcatalogue-store-serviceの間のトランザクションの詳細は、HTTP 応答を 500 と示します。これらの詳細情報を使用して、管理者として、誤ったサービスを分析し、解決方法product-catalogue-service としてトラブルシューティングできます。

また、フィルターパネルの各指標からオプションを選択して、結果を フィルターすることもできます。たとえば、すべての 5xx トランザクションを表示する場合は、[応答コード] をクリックし、[**500**] を選択します。



- クライアント **RTT**: パケットがクライアントから転送される時間。
- サーバ **RTT**: パケットがサーバから転送される時間。

- アプリの応答時間: アプリケーションの平均応答時間
- データ転送時間：データ転送サイズと、サービスとの間で送信が行われる速度。
- 場所: クライアントの場所
- ブラウザ：クライアントが使用するブラウザのタイプ。例：Chrome、Firefox です。
- クライアント **OS**：ブラウザからのユーザーエージェントの詳細に基づくクライアント OS。
- デバイス：ブラウザからのユーザーエージェントの詳細に基づくデバイス。例：タブレット、モバイル。
- 要求タイプ: 取引要求タイプ。例:GET。
- 応答コード：サーバーから受信した応答コード。例：501、404、200。
- 応答コンテンツ・タイプ: 取引コンテンツ・タイプ。クライアント要求が text/html の場合、サーバーからの応答は text/html でなければなりません。
- **SSL** プロトコル: クライアントが使用する SSL プロトコルのバージョン。例:SSLv3。
- **SSL** 暗号の強度: SSL 証明書キーサイズ (高、中、低) に基づく暗号の強度。
- **SSL** キーの強度: SSL 暗号の強さは、SSL 証明書のキーサイズから計算されます。キーの長さは、SSL アルゴリズムのセキュリティを定義します。例:2048
- **SSL** フロントエンド失敗の理由: フロントエンド SSL ハンドシェイクのエラーメッセージ。例：SSL CLIENTAUTH FAILURE

サービスグラフで部分的なデータまたはデータがないかの診断詳細の表示

May 7, 2021

必要なサービスグラフ構成を完了し、Citrix ADM で Kubernetes クラスターを追加すると、サービスグラフがデータを入力し始めます。状況によっては、サービスグラフに部分的なデータが表示されているか、データが表示されないことがあります。サービスグラフに部分的なデータまたはデータがない理由のいくつかは、次のとおりです。

- スタティックルートが設定されていません
- Kubernetes クラスターのステータスが停止しています
- CPX 登録が失敗しました
- CPX 仮想サーバにはライセンスがありません
- サービスグラフがすべてのデータをロードできないように、必要な分析構成が設定されていません

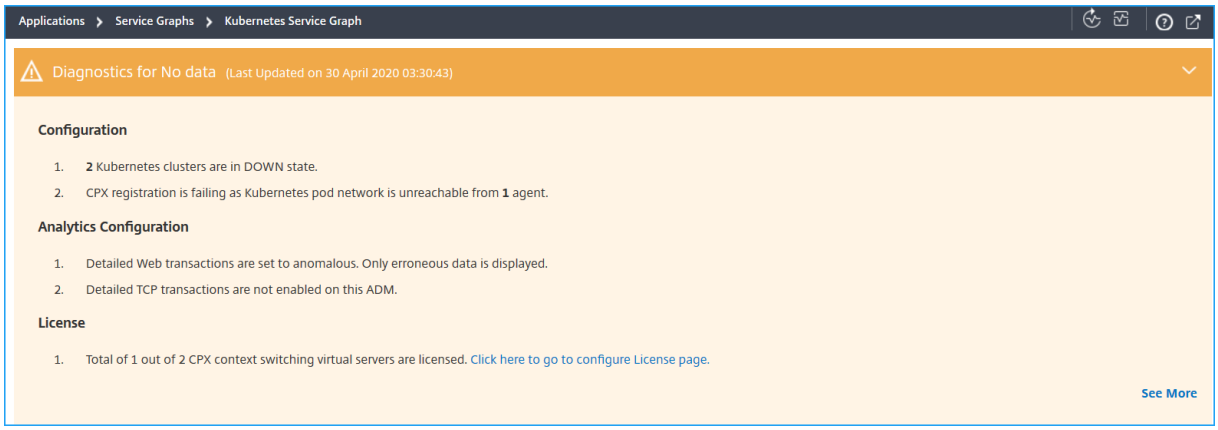
管理者として、サービスグラフに部分的なデータが表示されている場合やデータがない場合に、その理由を分析することが困難な場合があります。サービスグラフページの診断情報を使用すると、データの一部またはデータがない問題のトラブルシューティングに必要な理由と必要なアクションを確認できます。

Citrix ADM で、[アプリケーション] > [サービスグラフ] の順に選択し、[マイクロサービス] タブをクリックします。

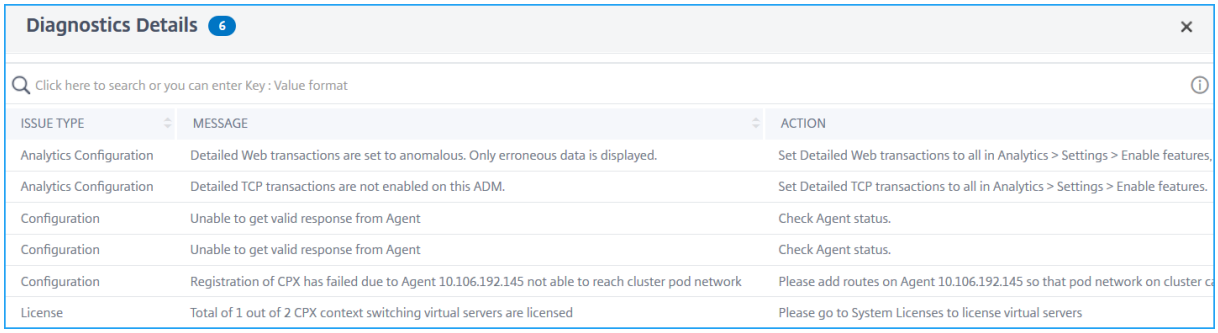
データなしの診断

サービスグラフにデータが表示されない場合は、次の診断メッセージが表示されます。

[**>**] をクリックして詳細を表示します。サービスグラフにデータが表示されない原因を確認できます。次の図は、サービスグラフにデータがない場合の例です。



問題の詳細を表示するには、[詳細を表示] をクリックします。

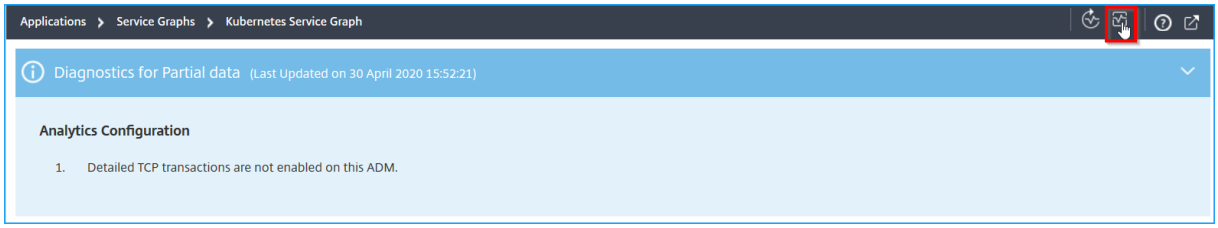


- **[** 問題の種類**]** — 構成、分析設定、またはライセンスから発生する問題を示します。
- 「メッセージ」— 問題の原因を示します。
- **[** アクション] — 問題のトラブルシューティングを行うために実行する必要があるアクションを示します。

部分データの診断

サービスグラフが部分的なデータだけで表示される場合は、[**Show Diagnostics**] ボタンをクリックして診断情報を表示します。

次に、TCP トランザクションが無効になっている例を示します。

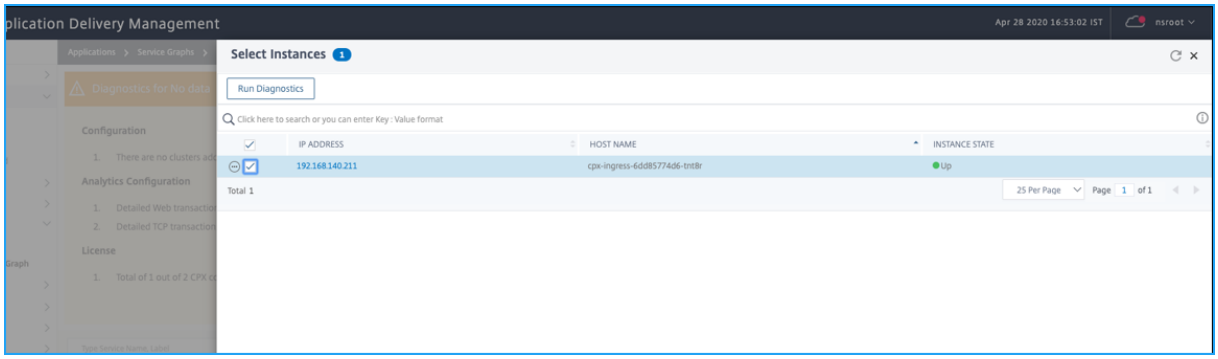


この例では、**[** 分析**]** > **[**設定**]** に移動して **[TCP** トランザクション設定**]** を **[** すべて**]** に設定する必要があります。

トラブルシューティング

管理者は、これらの診断メッセージを使用して、これらの問題を検証し、これらの問題のトラブルシューティングを試みることができます。トラブルシューティング後、Citrix ADM は定期的な診断チェックを定期的に自動的に実行します。診断チェックが完了すると、サービスグラフ内のデータの一部またはデータがない問題が解決されます。

[診断の実行] をクリックし、**CPX** インスタンスを選択し、[診断の実行] をクリックすることもできます。



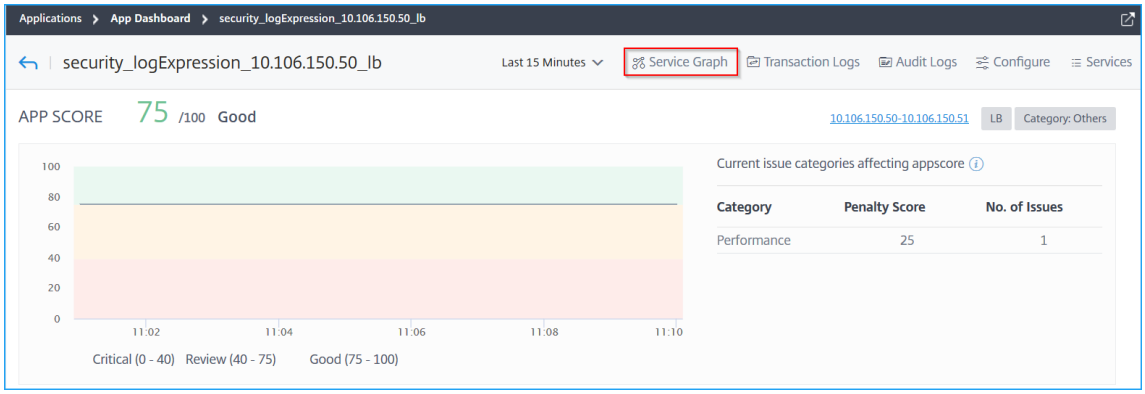
3 層 Web アプリケーションのサービスグラフ

May 7, 2021

アプリケーションのサービス・グラフを表示するには、次の手順に従います。

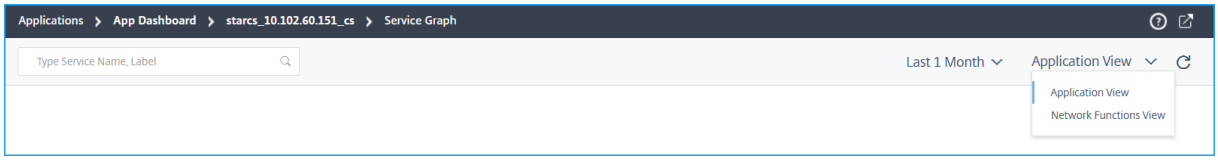
1. 「アプリケーション」>「ダッシュボード」にナビゲートします。
2. アプリケーションを選択します。

   アプリケーションの詳細ページが表示されます。
3. 期間を選択し、[**Service Graph**] をクリックします。



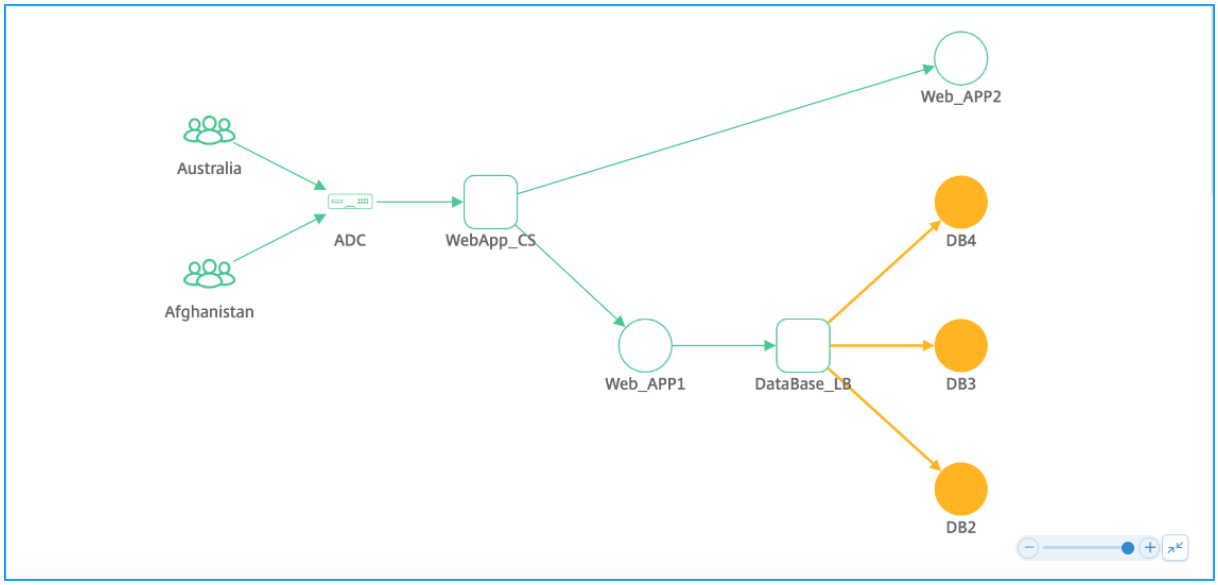
選択したアプリケーションのサービスグラフページが表示されます。

サービス・グラフは、アプリケーション・ビューまたは ネットワーク機能ビューで表示できます。

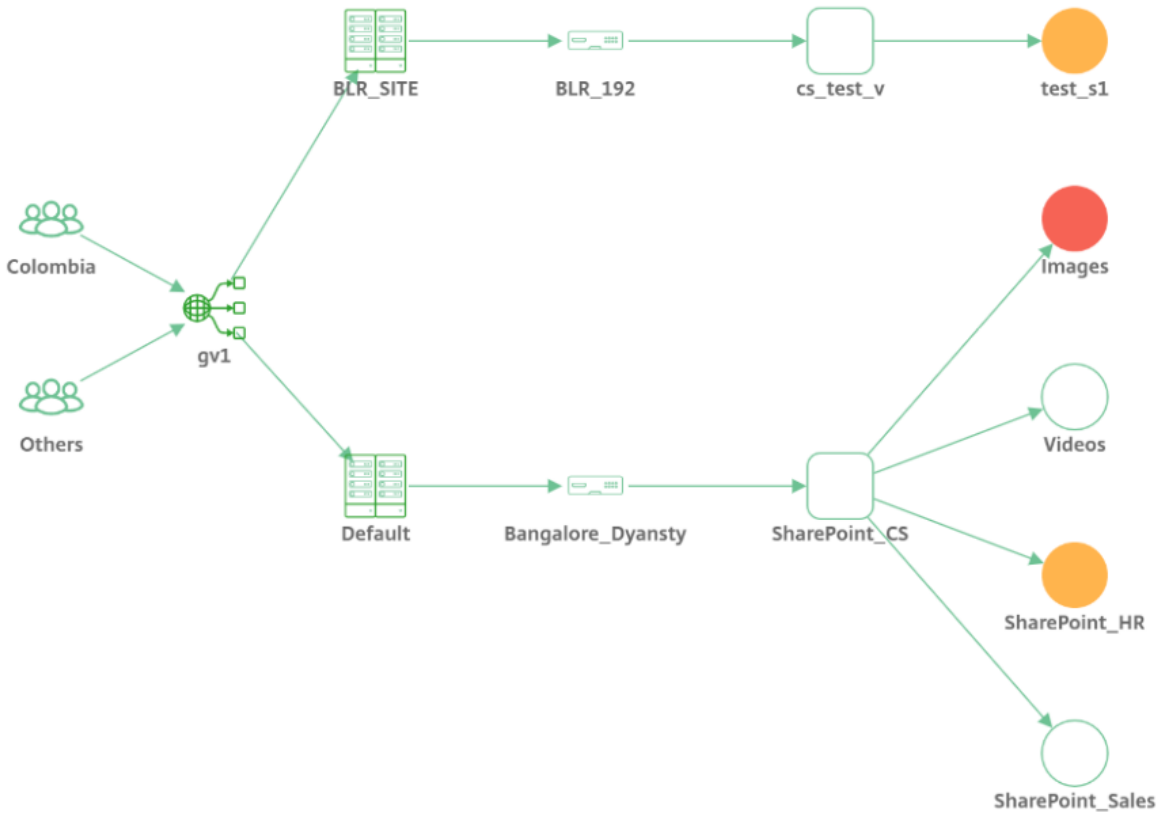


アプリケーションビュー

アプリケーション構成の概要を表示します。このビューでは、クライアント、ADC、Web アプリケーション間の通信を視覚化できます。



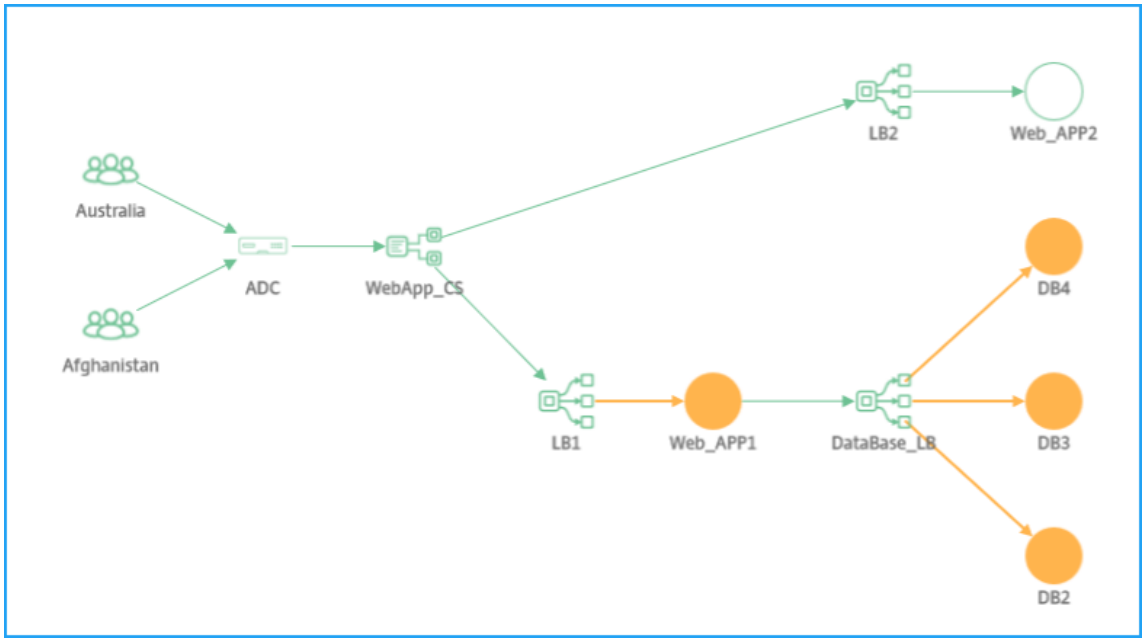
GSLB アプリケーションでは、クライアント、データセンター、ADC、サービス間の通信を視覚化できます。



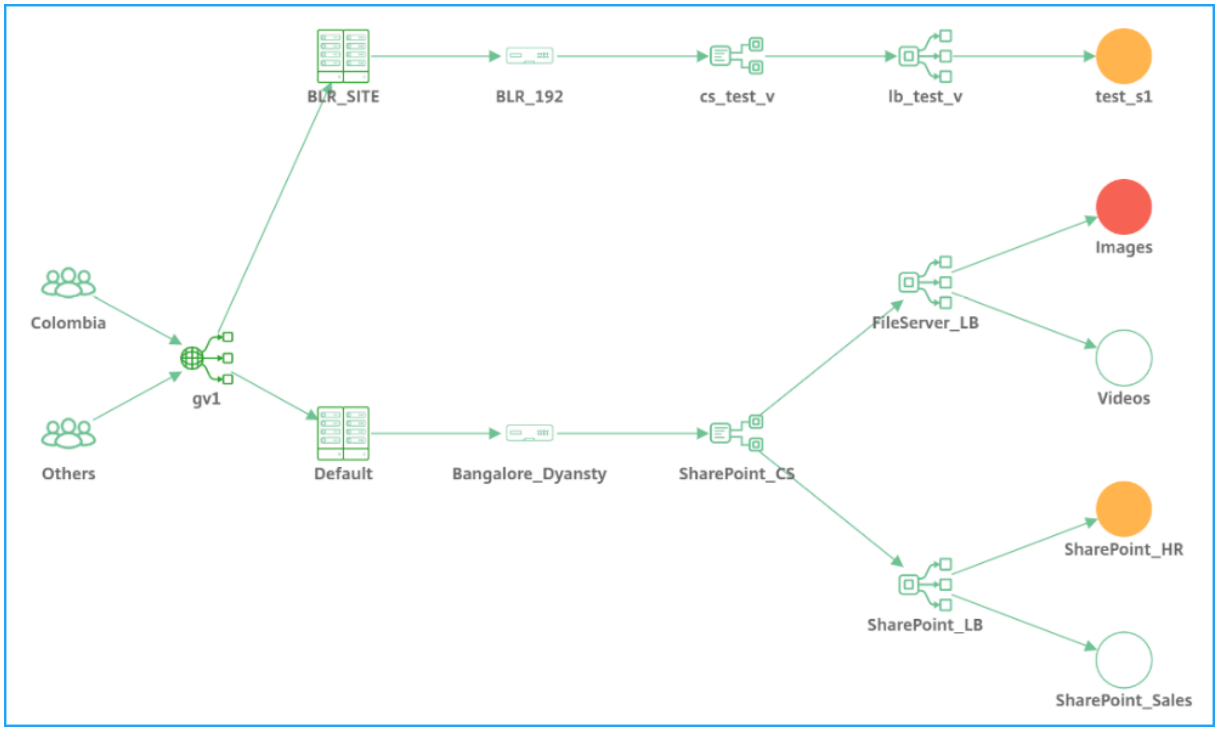
ネットワーク機能ビュー

アプリケーションに関連付けられている仮想サーバーを表示します。このビューでは、ADC が次のものと通信しているかどうかを視覚化できます。

- アプリケーションにアクセスするためのコンテンツスイッチング仮想サーバー
- アプリケーションにアクセスするための負荷分散仮想サーバー
- コンテンツスイッチングと負荷分散の両方の仮想サーバーによるアプリケーションへのアクセス

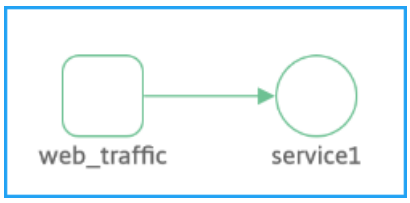


GSLB アプリケーションでは、データセンターおよび Citrix ADC とともに詳細が表示されます。

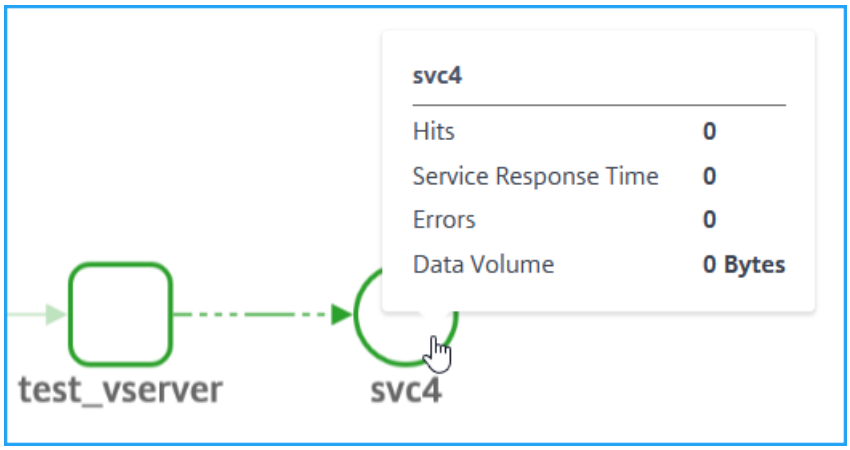


アクティブなトランザクションがないサービスグラフビュー

ADC と Web アプリケーション間でアクティブなトランザクションが発生しない場合、サービスグラフにはアプリケーションの基本構成のみが表示されます（クライアントと ADC なし）。



サービスまたは仮想サーバーにマウスポインタを置くと、トランザクションがないためにすべてのメトリックについて詳細が 0 として表示されます。

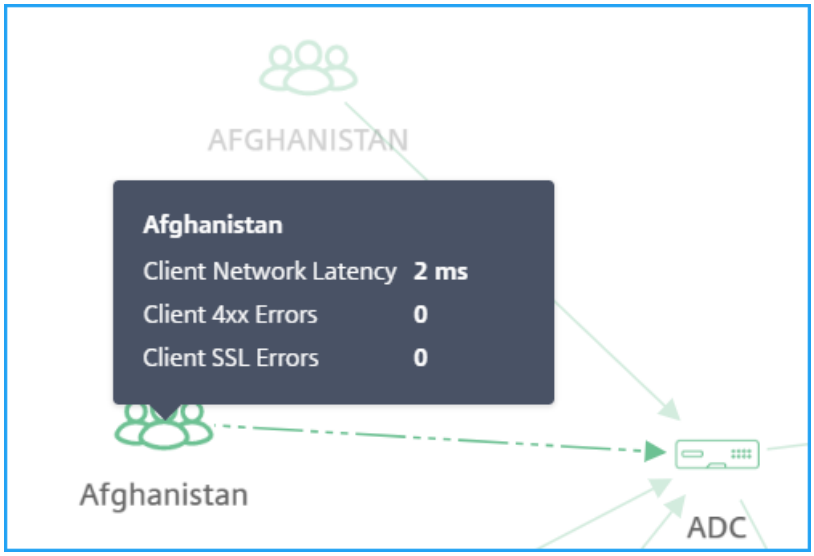


メトリックスの分析

各サービスの上にマウスポインタを置くと、アプリケーションビューまたはネットワーク機能ビューでメトリックの詳細が表示されます。

クライアント・メトリック

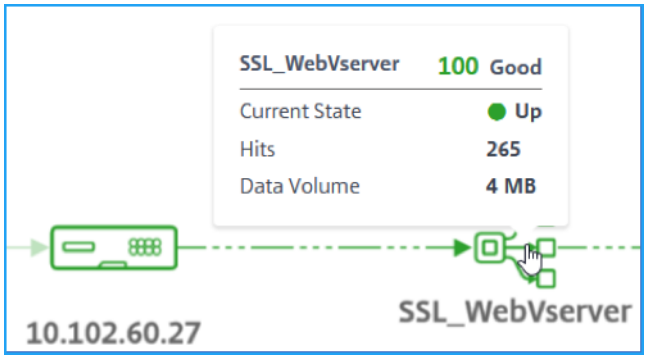
クライアント上にマウスポインターを合わせると、クライアントのメトリックが表示されます。



- 「クライアントネットワーク遅延」— クライアントからのネットワーク遅延を示します。
- クライアント **4xx** エラー：クライアントから発生した 4xx エラーの総数を示します。
- 「クライアント **SSL** エラー」— クライアントからの SSL エラーの総数を示します。

ネットワーク機能メトリック

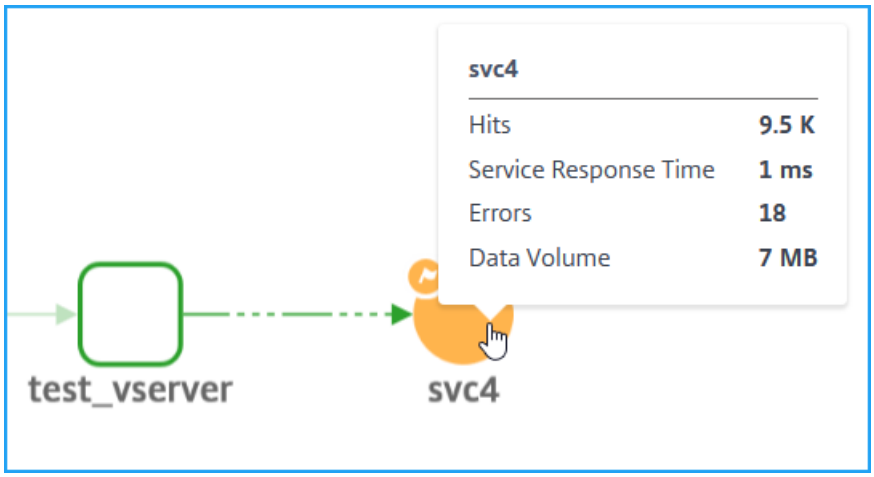
負荷分散サービスまたはコンテンツスイッチングサービスにマウスポインターを合わせると、メトリックの詳細が表示されます。



- **Current state**： 仮想サーバの現在のステータスを示します。
- **Hits** — 仮想サーバーが受信したヒットの合計数を示します。
- **Data Volume**： 仮想サーバによって処理された合計データ量を示します。

サービスメトリック

サービス (Web アプリケーション) にマウスポインターを合わせると、メトリックスが表示されます。

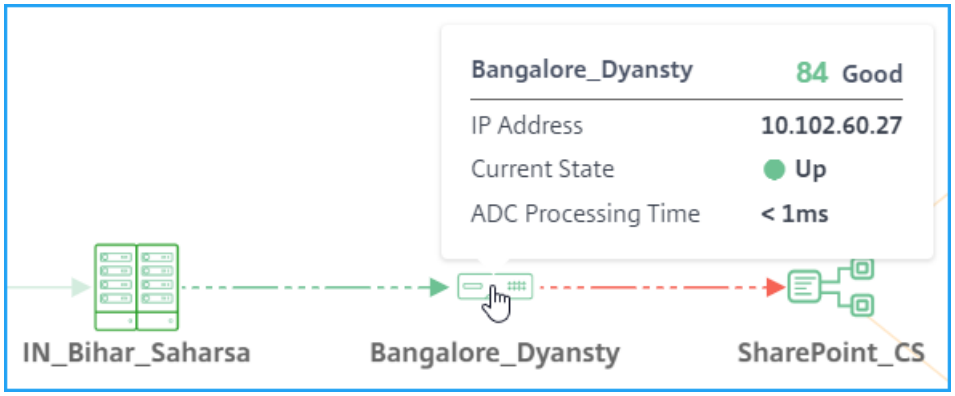


- **Hits** — サービスによって受信されたヒットの合計数を示します。
- サービス応答時間：サービスからの平均応答時間を示します。

- **Errors** — サービスから発生したエラーの総数を示します。
- **Data Volume**： サービスによって処理されたデータの合計を示します。

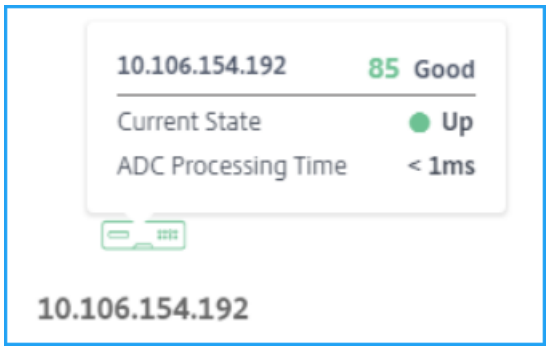
Citrix ADC メトリック（**GSLB** アプリケーションのみ）

ADC にマウスポインターを合わせると、メトリックが表示されます。



- ホスト名と現在の ADC スコアを表示します。スコアは、Citrix ADC 潜在的な問題に基づいて計算されます。詳しくは、「インスタンススコア」を参照してください。
- **IP** アドレス — Citrix ADC IP アドレスを示します。
- 現在の状態 — Citrix ADC 状態（稼働中、停止中、サービス停止中）を示します。
- **ADC** 処理時間 — ADC インスタンスによる平均処理時間を示します。

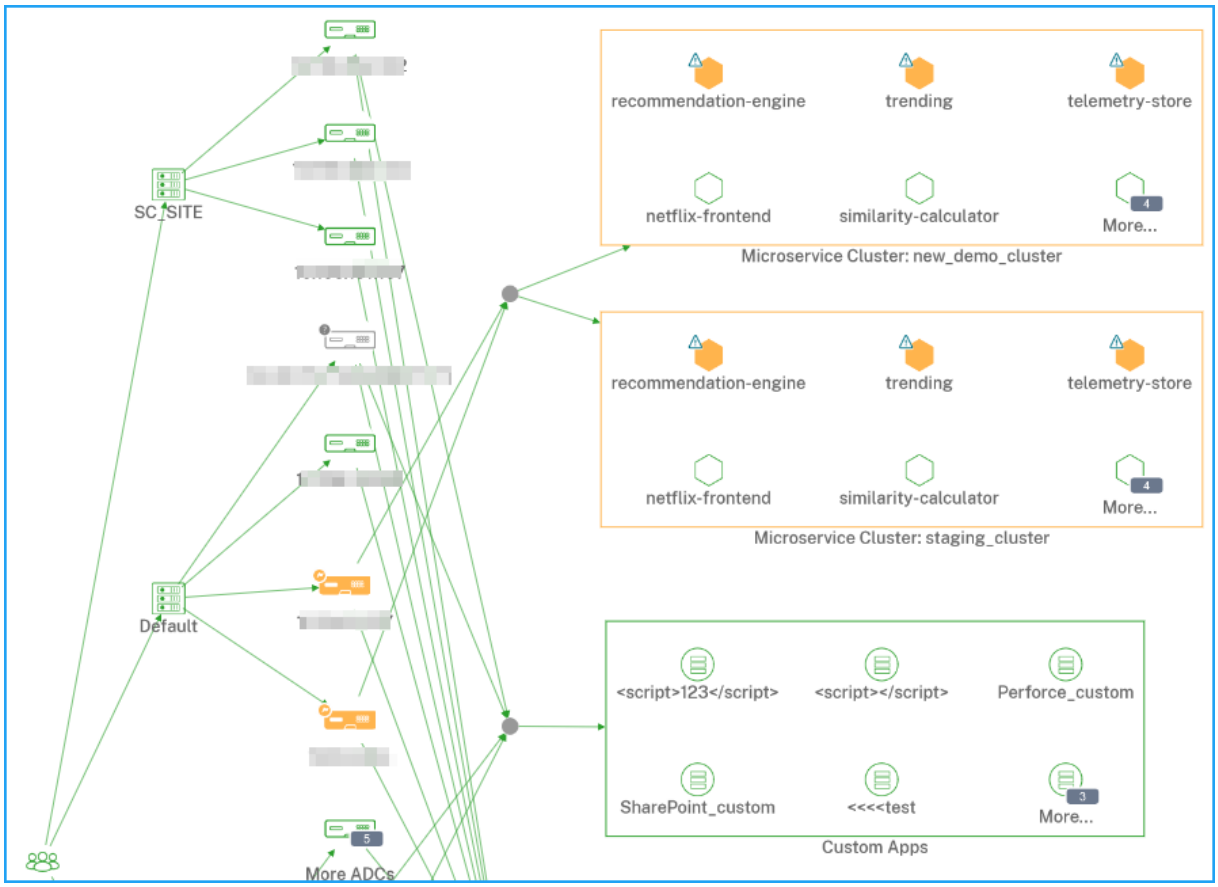
> 注
>
> ホスト名が Citrix ADC に割り当てられていない場合：
>
> -ホスト名の代わりに Citrix ADC の IP アドレスが表示される。
>
> -メトリックでは、Citrix ADC IP アドレス情報は表示されません。



サービスグラフ内のすべてのアプリケーションの全体的ビュー

May 7, 2021

[アプリケーション] > [サービスグラフ] に移動し、[グローバル] をクリックします。



サービスグラフには、選択した期間の次の情報が表示されます。

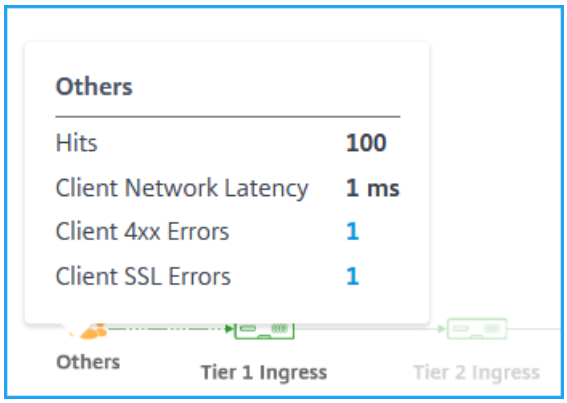
- ユーザーが特定のアプリケーションにアクセスするリージョン
- Citrix ADC インスタンスがホストされているデータセンター
- すべての Citrix ADC インスタンスからの個別のアプリケーションの合計

  > 注
  >
  > Citrix ADC インスタンスに個別のアプリケーションがない場合、Citrix ADC インスタンスから個別の仮想サーバーに向かう矢印端は表示されません。

- すべての Citrix ADC インスタンスからのカスタムアプリケーションの合計
- Citrix ADC CPX インスタンスからのマイクロサービスアプリケーションの合計

クライアントメトリックの表示

クライアントリージョンにマウスポインタを合わせると、メトリックスが表示されます。

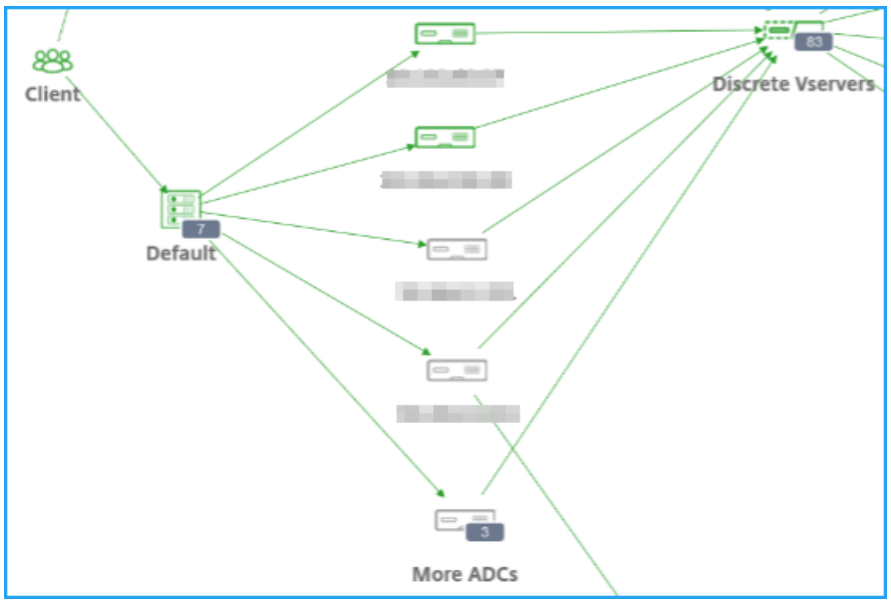


- クライアントネットワーク待ち時間 -平均クライアントネットワーク遅延を示します。
- クライアント **4xx** エラー -クライアントの 4xx エラーの合計を示します。
- クライアント **SSL** エラー -クライアントの SSL エラーの合計を示します。

Citrix ADC の詳細を表示する

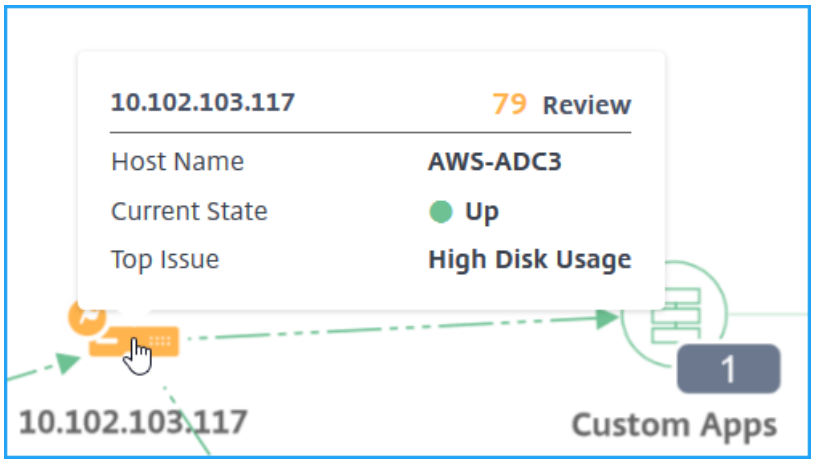
サービスグラフでは、次の項目を表示できます。

- Citrix ADC インスタンスの合計でグループ化されたデータセンター
- 各データセンターの上位 4 つの低スコアの Citrix ADC インスタンスのみ



[その他の **ADC**] をクリックして、それぞれのステータス（クリティカル、レビュー、良好および該当なし）タブを選択して、すべての Citrix ADC インスタンスを表示します。

Citrix ADC インスタンスにマウスポインタを置いて、メトリックを表示します。



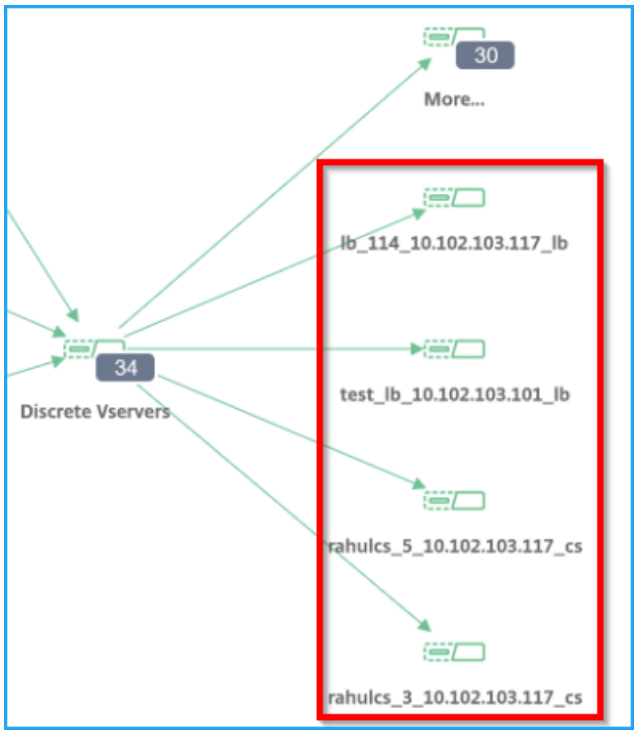
次の項目を表示できます。

- Citrix ADC インスタンスの IP アドレスとスコア
- ホスト名 — Citrix ADC インスタンスに割り当てられているホスト名を示します。
- 現在の状態：Citrix ADC インスタンスの現在のステータス（稼働中、停止、アウトオブサービスなど）を示します。
- 上位の問題 — 現在の Citrix ADC スコアに影響する上位の問題を示します

Citrix ADC インスタンスをクリックして、インスタンスのスコア、主要メトリック、および ADC インスタンスに関連付けられた問題などのインスタンスの詳細を表示します。詳しくは、「インフラストラクチャ分析でのインスタンスの詳細の表示」を参照してください。

ディスクリートアプリケーションの表示

サービス・グラフには、上位 4 つの低スコアディスクリートアプリケーションが表示されます。



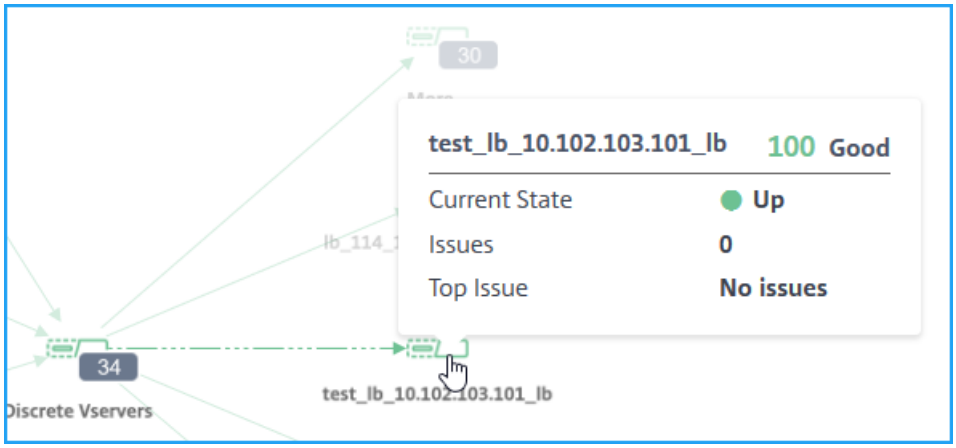
次の個別のアプリケーションがあるとします。

アプリ名	Citrix ADC	App Score	アプリのステータス
App1	10.102.29.50	35 (クリティカル)	実行中
App2	10.102.29.90	100 (いいね)	ダウン
App 3	10.102.32.40	49 (レビュー)	実行中
App4	10.102.113.208	92 (いいね)	ダウン
App5	10.102.25.25	86 (いいね)	実行中
App6	10.102.29.41	77 (よい)	実行中
App7	10.102.29.102	41 (レビュー)	実行中

このシナリオでは、サービスグラフの上位 4 つの低スコアアプリケーションとして App1、App3、App6、およびアプリケーション 7 を表示できます。

同様に、カスタムアプリケーションとマイクロサービスアプリケーションの上位 4 つの低スコアアプリケーションを表示することもできます。

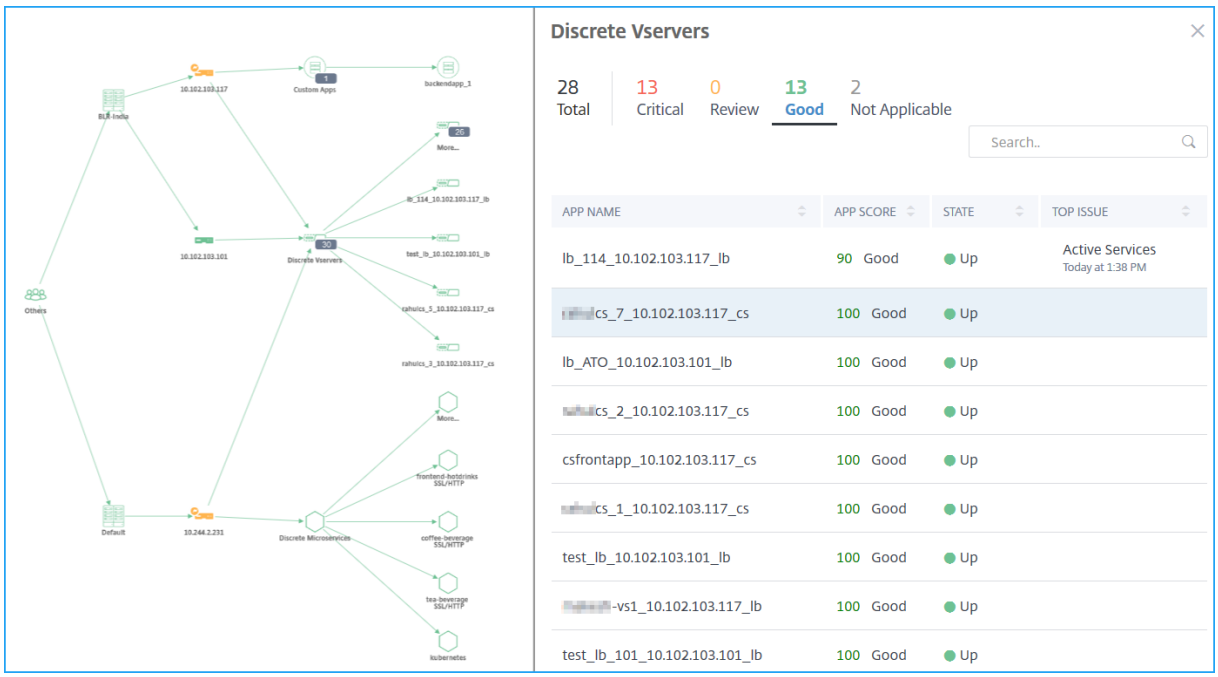
サービスの上にマウスポインタを置くと、メトリックス情報が表示されます。



次の項目を表示できます。

- アプリケーション名とスコア
- 現在の状態：アプリケーションの現在のステータス（Up、Down）を示します。
- **Issues** — アプリケーションに適用可能な問題の合計を示します。
- **Top Issue**： アプリケーション全体のスコアに影響する上位の問題を示します。

[詳細] をクリックして、すべての個別のアプリケーションを表示します。次の図に示すように、「離散仮想サーバー」ページが表示されます。

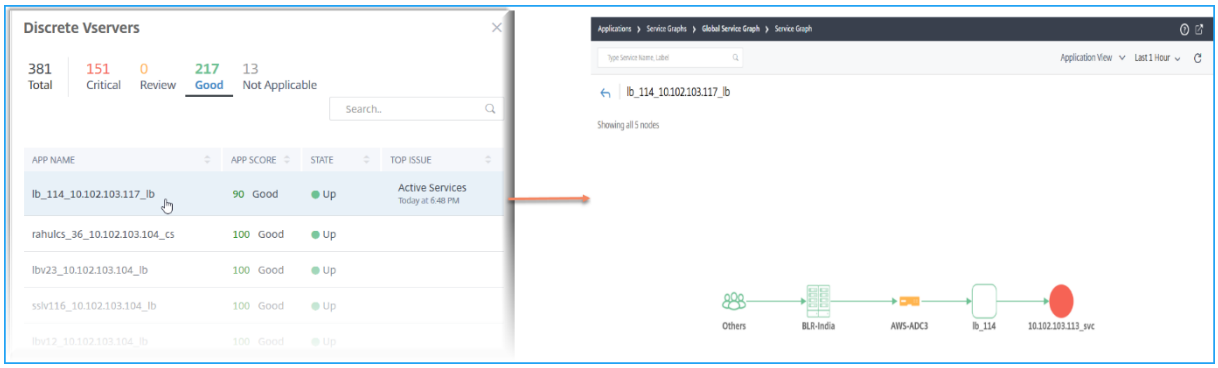


仮想サーバは、ステータスに応じて表示されます。

- 合計 — ディスクリートアプリケーションの合計
- クリティカル — アプリのスコアは 0 から 40 以下です

- レビュー — アプリのスコアは 40 から 75 未満です
- 良かった — アプリのスコアは > 75
- 該当なし — アプリは仮想サーバーにバインドされていません

各タブをクリックすると、仮想サーバを表示できます。アプリケーションをクリックすると、選択したアプリケーションのサービスグラフが表示されます。



詳しくは、「アプリケーションのサービスグラフ」を参照してください。

マイクロサービスアプリケーションの表示

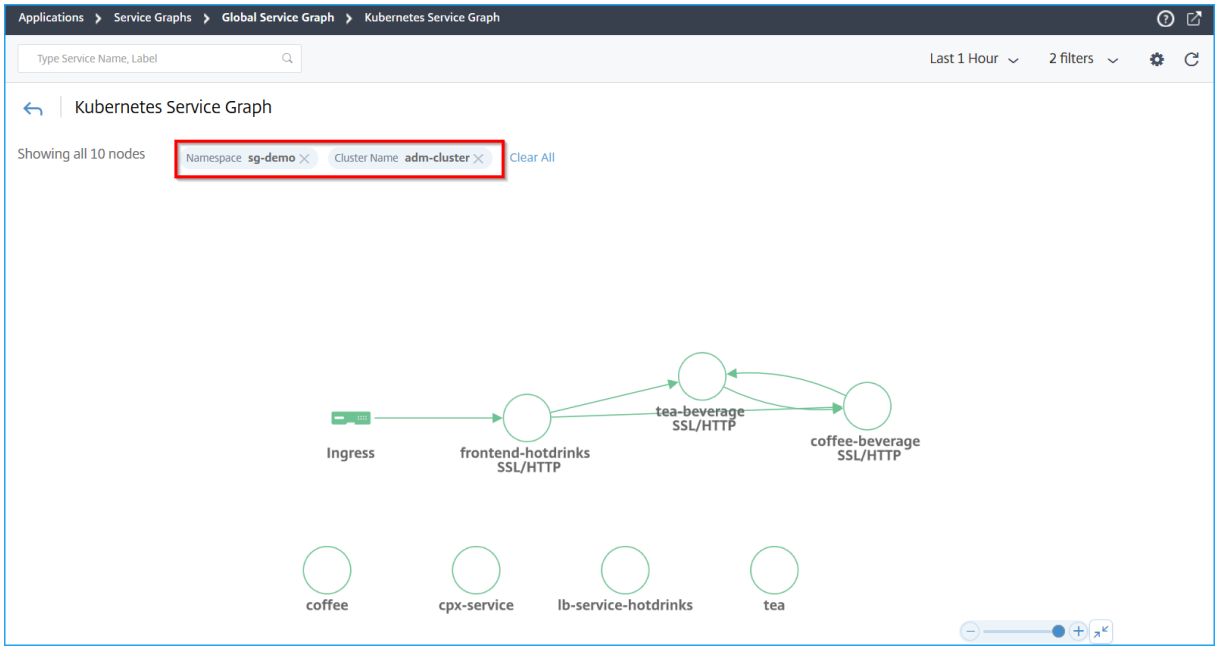
サービスグラフには、Kubernetes クラスターに属するすべてのマイクロサービスアプリケーションも表示されます。サービスの上にマウスポインタを置くと、メトリックスの詳細が表示されます。

次の項目を表示できます。

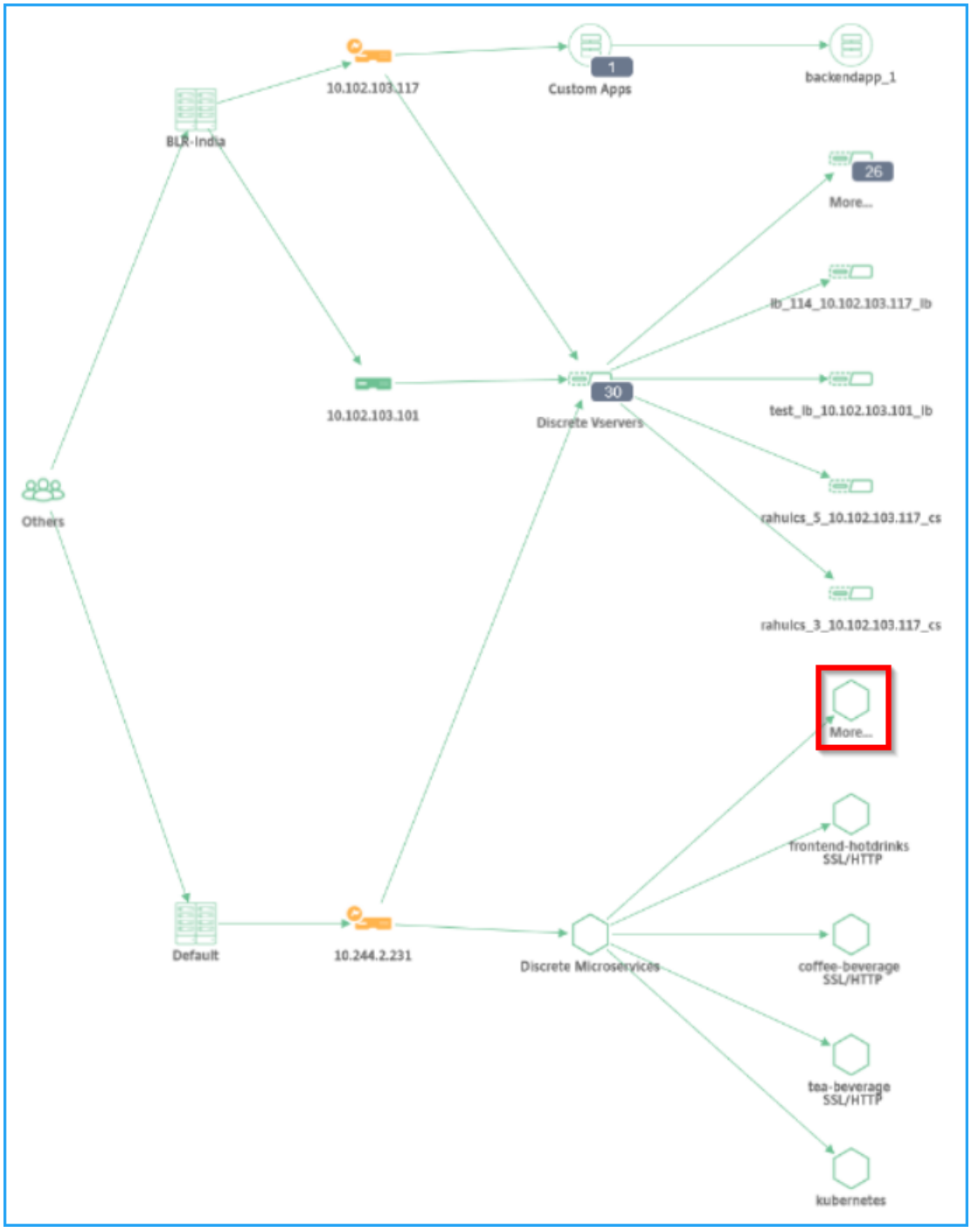
- サービス名
- SSL、HTTP、TCP、SSL over HTTP、SSL などのサービスで使用されるプロトコル
- **Hits** — サービスによって受信されたヒットの総数
- サービス応答時間 — サービスから取得した平均応答時間。

  (応答時間 = クライアント RTT + 要求の最後のバイト — 要求の最初のバイト)
- エラー — 4xx、5xx などのエラーの総数
- **Data Volume** — サービスによって処理されるデータの総量
- 名前空間 — サービスの名前空間
- クラスター名 — サービスがホストされているクラスター名
- **SSL** サーバーエラー — サービスからの SSL エラーの合計

サービスをクリックすると、選択したサービスの Kubernetes サービスグラフが、適用されたサービス名前空間とクラスター名フィルターと共に表示されます。



[詳細] をクリックして、すべてのサービスを持つ Kubernetes サービスグラフを表示します。Kubernetes サービスグラフの詳細については、クラウドネイティブアプリケーションのサービスグラフを参照してください。



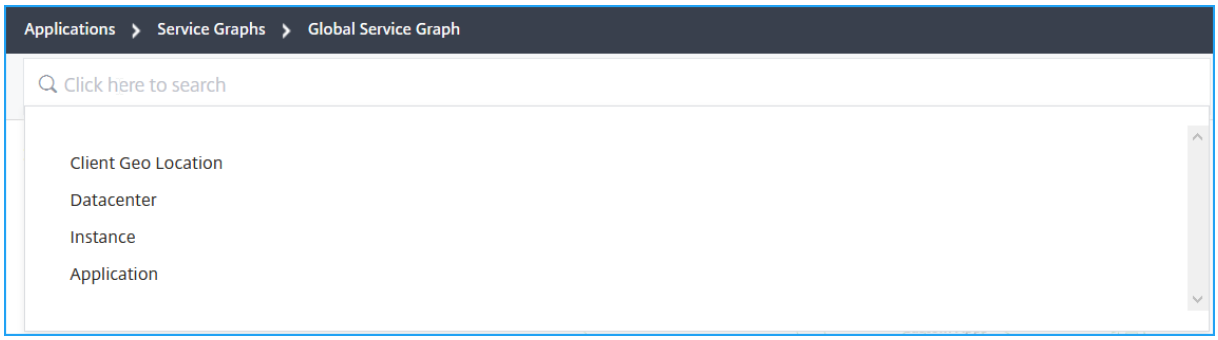
結果をフィルタする検索バー

検索バーを使用して結果をフィルタリングできます。管理者は、次の条件を満たす場合に、この検索バーを使用して、特定のインスタンス/クライアント/アプリケーション/データセンターにすばやく絞り込むことができます。

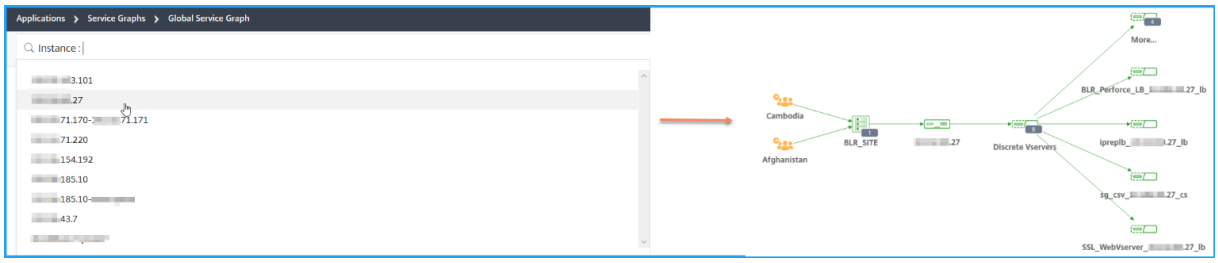
- 多数のデータセンターを持つ大企業

- データセンターごとに多数の Citrix ADC インスタンスを構成しました
- 各 Citrix ADC インスタンス経由で展開またはアクセスされる多数のアプリケーションを構成
- 異なる場所からアプリケーションにアクセスするクライアント

検索バーにマウスポインタを置き、フィルタを作成するカテゴリを選択します。



たとえば、特定の ADC インスタンスを表示する場合は、検索バーから [**Instance**] を選択し、インスタンスの IP アドレスを選択します。グローバルサービスグラフには、選択したインスタンスとその関連アプリケーション、データセンター、クライアントの場所が表示されます。



StyleBook

May 7, 2021

StyleBook は、アプリケーションの複雑な Citrix ADC 構成の管理作業を簡素化します。StyleBook は、Citrix ADC 構成の作成と管理に使用できるテンプレートです。Citrix ADC の特定の機能を構成するための StyleBook を作成することも、Microsoft Exchange や Lync などのエンタープライズアプリケーション展開用の構成を作成するための StyleBook を設計することもできます。

StyleBook は DevOps チームによって実践されているコードとしてのインフラストラクチャの原則によく適しています。コードとしてのインフラストラクチャの構成は宣言的でバージョン管理されるものです。構成は繰り返され全体として展開されるものでもあります。StyleBook には、次の利点があります。

- 宣言: **StyleBook** は、命令構文ではなく宣言構文で書かれています。StyleBook では、特定の ADC インスタンスで実現する方法に関するステップバイステップの手順ではなく、構成の結果や「望ましい状態」の説明に集中できます。Citrix ADM は、ADC 上の既存の状態と指定した目的の状態との差分を計算し、インフラスト

ラクチャに必要な編集を行います。StyleBook は YAML で記述された宣言構文を使用するため、StyleBook のコンポーネントは任意の順序で指定でき、Citrix ADM は計算された依存関係に基づいて正しい順序を決定します。

- **Atomic**：StyleBooks を使用して構成を展開すると、完全な構成が展開されるか、まったく展開されないため、インフラストラクチャは常に一貫した状態のままになります。
- バージョン対応：StyleBook には、システム内の他の StyleBook と一意に区別する名前、名前空間、およびバージョン番号があります。この特徴を保つために、StyleBook を変更した場合はそのバージョン番号（またはその名前または名前空間）を更新する必要があります。バージョンの更新では、同じ StyleBook の複数のバージョンを維持することもできます。
- コンポーザブル：StyleBook を定義した後、StyleBook を他の StyleBook を構築するためのユニットとして使用できます。共通の構成パターンの繰り返しを避けることができます。また、社内の標準の構成ブロックを確立することもできます。StyleBook はバージョン管理され、既存の StyleBook を変更すると新しい StyleBook になるため、依存する StyleBook が意図せずに壊されることはありません。
- アプリケーション中心：StyleBook を使用して、完全なアプリケーションの Citrix ADC 構成を定義できます。アプリケーションの構成はパラメーターを使用することで抽象化できます。したがって、StyleBook から構成を作成するユーザーは、いくつかのパラメータを入力することで複雑な ADC 構成を作成できるシンプルなインターフェースと対話することができます。StyleBooks から作成された構成は、インフラストラクチャに関連付けられていません。したがって、1 つの構成を 1 つまたは複数の ADC インスタンスに導入でき、インスタンス間で移動することもできます。
- 自動生成 **UI**：Citrix ADM は、Citrix ADM GUI を使用して構成を行うときに、StyleBook のパラメータを入力するために使用する UI フォームを自動生成します。StyleBook の作成者が新しい GUI 言語を学習したり、UI ページやフォームを個別に作成したりする必要はありません。
- **API** 駆動：すべての構成操作は、Citrix ADM GUI または REST API を使用してサポートされます。API は、同期モードまたは非同期モードで使用できます。StyleBook の API では、構成タスクに加えて、実行時に StyleBook のスキーマ（パラメーターの説明）を見つけることもできます。

1 つの StyleBook を使用して複数の構成を作成できます。各構成は構成パックとして保存されます。たとえば、通常の HTTP 負荷分散アプリケーションの構成を定義する StyleBook があるとします。負荷分散エンティティの値を含む構成を作成し、Citrix ADC インスタンスで実行できます。この構成は構成パックとして保存されます。同じ StyleBook を使用して、異なる値を持つ別の構成を作成し、同じインスタンスまたは別のインスタンスで実行できます。この構成には、新しい構成パックが作成されます。設定パックは、ADM と、構成が実行されている ADC インスタンスの両方に保存されます。

Citrix ADM に同梱されているデフォルトの StyleBook を使用して展開用の構成を作成するか、独自の StyleBook を設計して Citrix ADM にインポートすることができます。StyleBook を使用して、Citrix ADM GUI または API を使用して構成を作成できます。

このドキュメントでは、次の内容について説明します。

- スタイルブックを表示する方法
- デフォルトのスタイルブック
- ビジネスアプリケーション向けに開発された StyleBooks

- カスタムスタイルブック
- スタイルブックの API
- スタイルブックの文法

スタイルブックグループ

May 7, 2021

Citrix Application Delivery Management（ADM）には、2 つの StyleBook グループがあります。これらは、デフォルトの StyleBooks とカスタム StyleBook です。デフォルトでもカスタムでも、StyleBook はパブリックまたはプライベートの StyleBook です。Citrix ADM では、システムに存在する StyleBook の種類や表示状態に関係なく、すべての StyleBook を表示できます。また、StyleBook 同士がどのように接続されているかをグラフィカルに表示することもできます。

このドキュメントでは、StyleBook のさまざまなタイプについて説明します。また、Citrix ADM から StyleBooks に対して実行できる以下のアクションについても説明します。

- カスタム StyleBook をダウンロードして修正するか、既存の StyleBook に基づいて StyleBook を作成します。
- ADM のデフォルトの StyleBook を非表示にします。
- Citrix ADM からカスタム StyleBook を削除します。
- StyleBooks にタグを追加します。

デフォルトおよびカスタムスタイルブック

- デフォルトの **StyleBook** は、Citrix ADM に同梱されている StyleBook で、Citrix ADC インスタンスに展開できる構成を作成できます。デフォルトの StyleBooks は削除できませんが、ADM GUI からは非表示にできます。
- カスタムスタイルブックは、Citrix ADM にインポートした独自の StyleBook です。

デフォルトの StyleBook とカスタム StyleBook はどちらもパブリックまたはプライベートにすることができます。

パブリックおよびプライベートのスタイルブック

構成パックを作成できる StyleBooks は、パブリック StyleBooks に分類できます。つまり、これらはすべて、Citrix ADM GUI および API から構成を作成するために直接使用することができます。

しかし、一部の StyleBook は、他の StyleBook のビルディングブロックとして使用されます。そのような **StyleBook** はプライベートとしてマークされます。プライベート StyleBook は、Citrix ADM GUI から構成パックを直接作成することはできません。ただし、Citrix ADM でこれらの StyleBook を表示および表示することはできます。カスタム **StyleBook** のいずれかをプライベートとしてマークするには、**StyleBook** のプライベート属性を

true に設定します。Citrix ADM API を使用して構成パックを作成するために、プライベート StyleBooks を使用できます。

プライベートとしてマークされた **StyleBook** の例

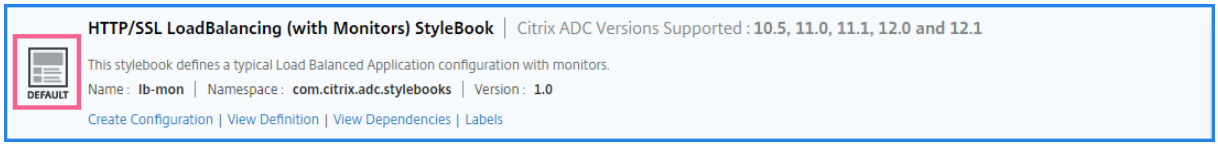
```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: |
    This StyleBook defines a simple load balancing configuration and is
        a building block to build other load balancing configurations.
schema-version: "1.0"
private: true
<!--NeedCopy-->
```

スタイルブックを見る

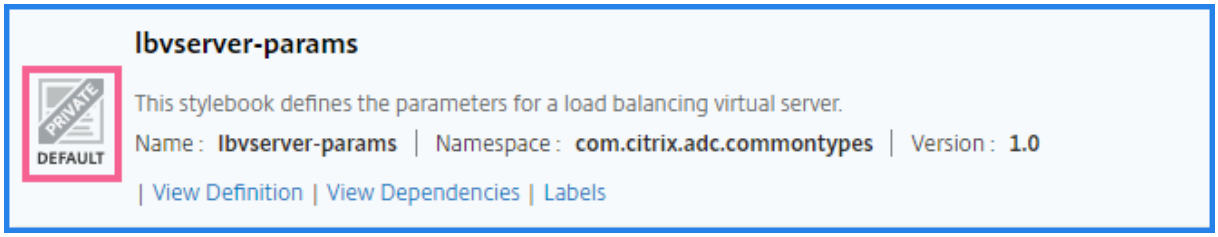
Citrix ADM では、StyleBook の数がデフォルトとプライベートの両方で増加しています。アクセスしたい特定の StyleBook を検索することもできます。また、両方のタイプの StyleBook を別々に表示することもできます。

Citrix ADM で、[アプリケーション] > [**StyleBooks**] に移動すると、システムに存在する StyleBook のリストを表示できます。

デフォルトのパブリック StyleBook のパネルには、次のアイコンがあります。

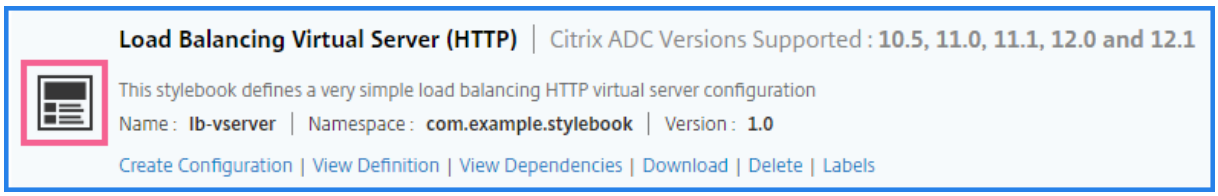


デフォルトのプライベート StyleBook には、プライベート StyleBook として宣言するアイコンがあります。

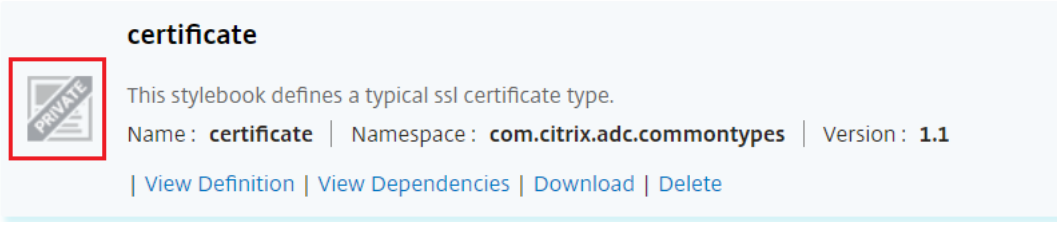


プライベート StyleBook の定義と依存関係を表示できますが、GUI を使用してプライベート StyleBook から構成パックを作成することはできません。プライベート StyleBook の主な目的は、別の StyleBook のビルディングブロックとして使用することです。Building-blocks-StyleBooks を使用すると、一般的な構成パターンの再利用を促進します。

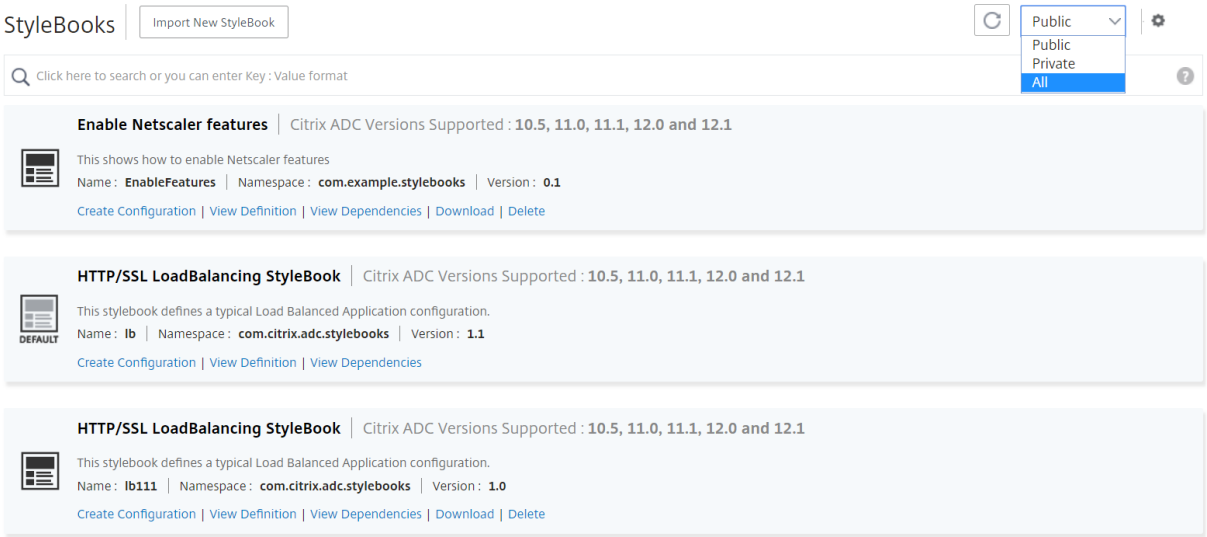
カスタムパブリック StyleBook には、次の図に示すように別のアイコンが表示されます。



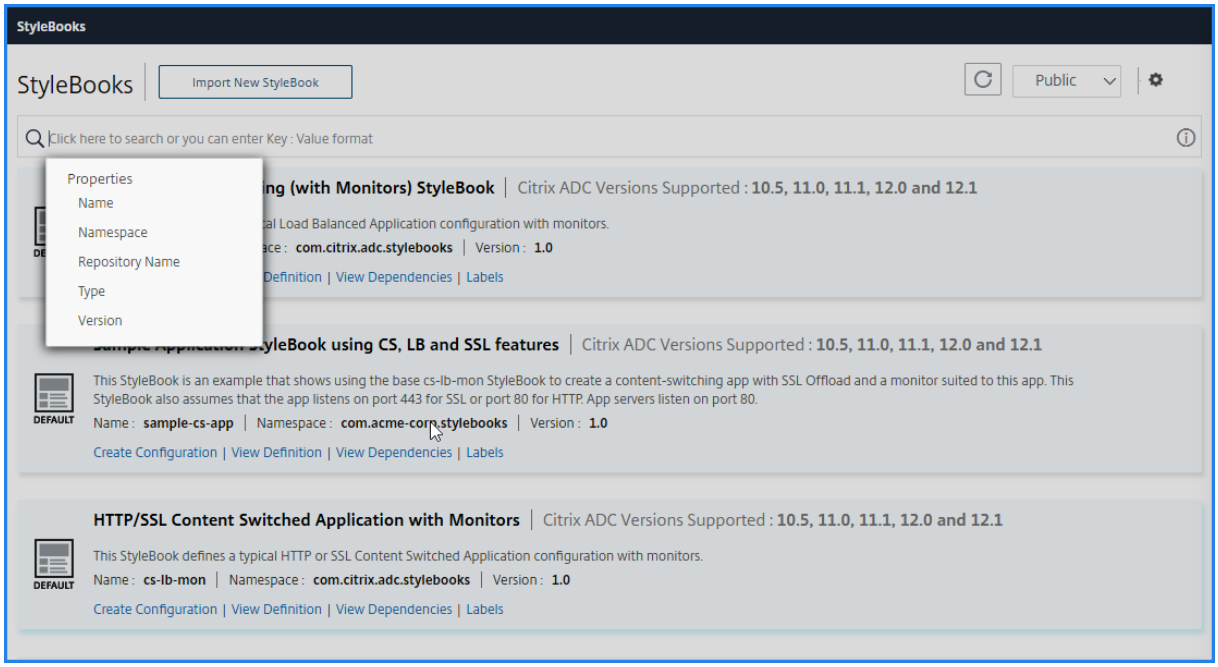
カスタムプライベート StyleBook は次のアイコンで表示されますが、



ページの右上には、表示する StyleBook の種類を選択するオプションが表示されます。StyleBook には、すべて、パブリック、またはプライベートの 3 つのオプションがあります。オプションの 1 つをクリックします。



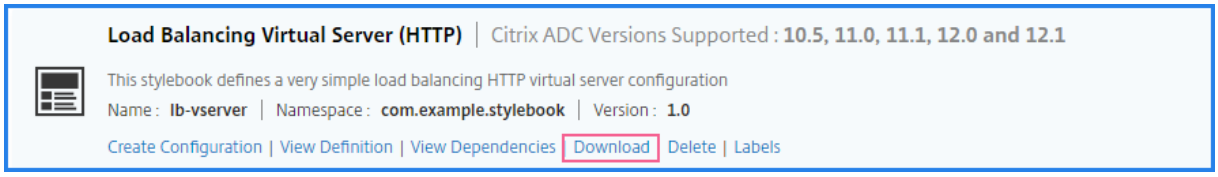
検索アイコンをクリックして、特定の StyleBook を検索することもできます。名前、名前空間、バージョン属性、またはこれらのオプションの組み合わせで検索できます。検索操作では、大文字と小文字は区別されません。



カスタム **StyleBook** をダウンロードする

Citrix ADM からカスタム StyleBook をダウンロードするには、［アプリケーション］>［**StyleBooks** ］>［構成］に移動します。右側のパネルに表示される StyleBook のリストで、カスタム定義の StyleBook をダウンロードするオプションをオンにします。［**Download**］をクリックします。StyleBook に依存するカスタム StyleBook がある場合は、ダウンロードしたバンドルに依存する StyleBook を含めることができます。

> 注:
>
> 公開または非公開としてマークされたカスタム StyleBooks をダウンロードできます。



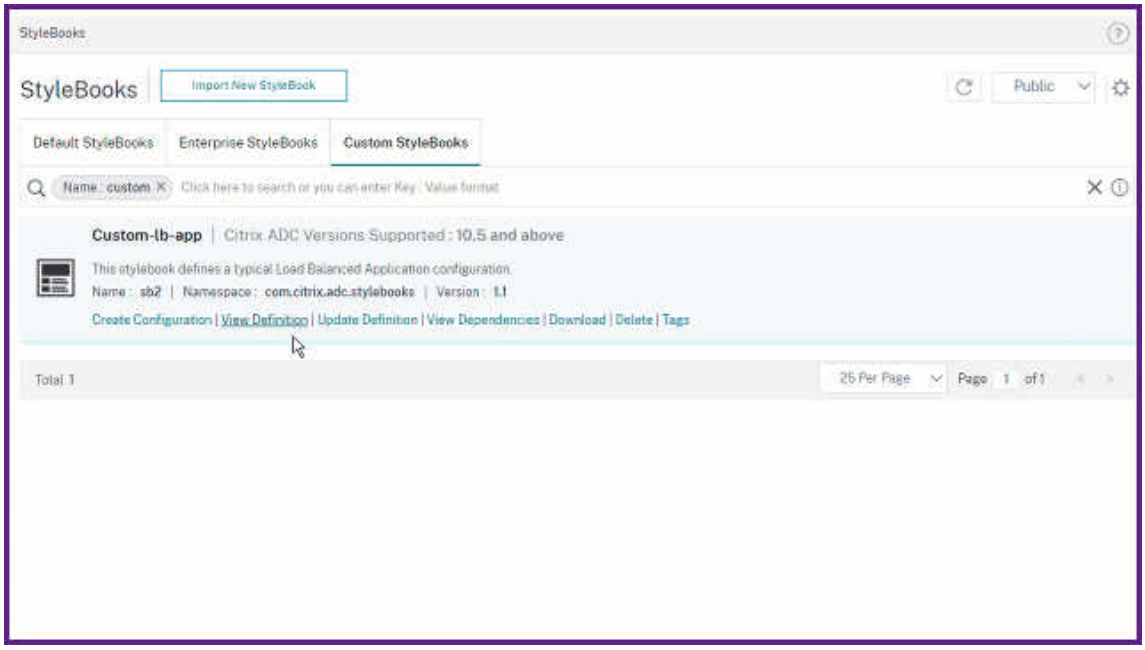
> 注
>
> Citrix ADM デフォルトのスタイルブックをダウンロードすることはできません。それらの定義と依存関係を表示できます。これを行うには、StyleBook パネルの「表示定義」および「依存関係の表示」リンクをクリックします。

カスタム **StyleBook** を更新する

カスタム StyleBook 定義は、ADM GUI 自体から更新できます。

1. 「アプリケーション」**>**「**StyleBooks**」に移動します。

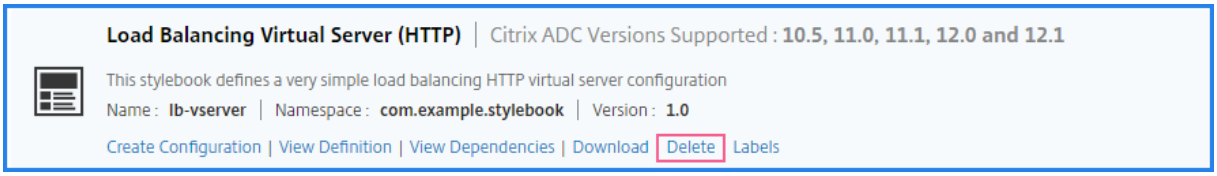
2. カスタムスタイルブックタブを選択します。
3. 更新する **StyleBook** で「定義の更新」を選択します。
4. 必要に応じて定義を更新し、[更新] をクリックします。

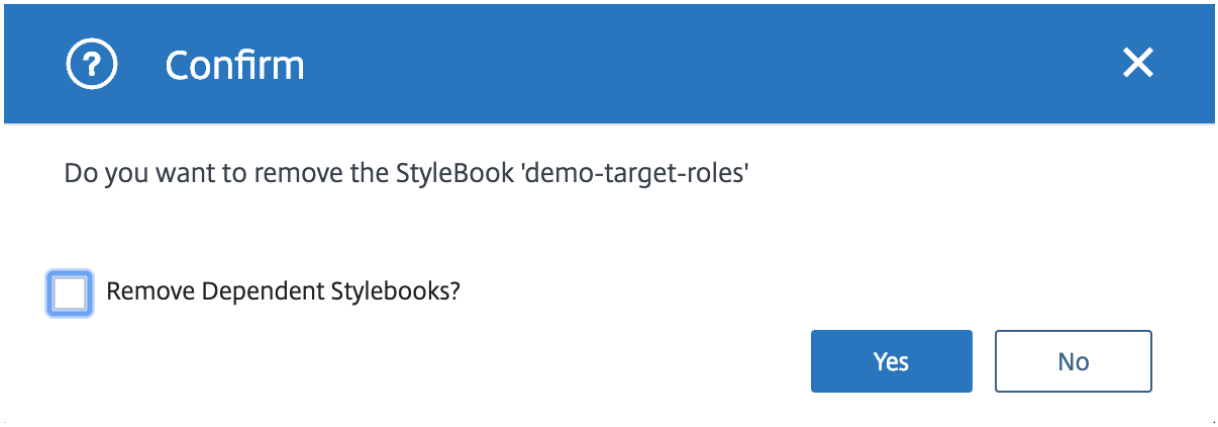


5. ページを更新して、最新の変更を確認します。

カスタムスタイルブックを削除する

削除ボタンをクリックして、カスタム **StyleBook** を削除することもできます。Citrix ADM から StyleBook を削除するかどうかを確認するポップアップウィンドウが表示されます。StyleBook で他のカスタム StyleBook が使用されている場合は、チェックボックスをオンにしてその StyleBook を削除できます。





> 注
>
> Citrix ADM に依存する StyleBook がある場合は、カスタム StyleBook を削除しないでください。そうしないと、既存の StyleBook が壊れます。

StyleBook の依存関係を表示する

StyleBook の重要かつ便利な特徴の 1 つは、別の StyleBook の構築ブロックとして使用できる点です。StyleBook を別の StyleBook にインポートできます。インポートされた StyleBook は型として宣言され、2 番目の StyleBook のコンポーネントまたはパラメータで使用されます。Citrix ADM で既存のデフォルトの StyleBook を調べて、1 つの StyleBook を別の StyleBook の上に構築する方法を学ぶことができます。

Citrix ADM では、StyleBook の相互接続方法をグラフィカルに表示できます。この表現は、他の StyleBook をビルディングブロックとして使用して構築された複雑な StyleBook に特に便利です。ディペンデンシーグラフを見ると、複数の StyleBook 間の関係や依存関係を確認できます。

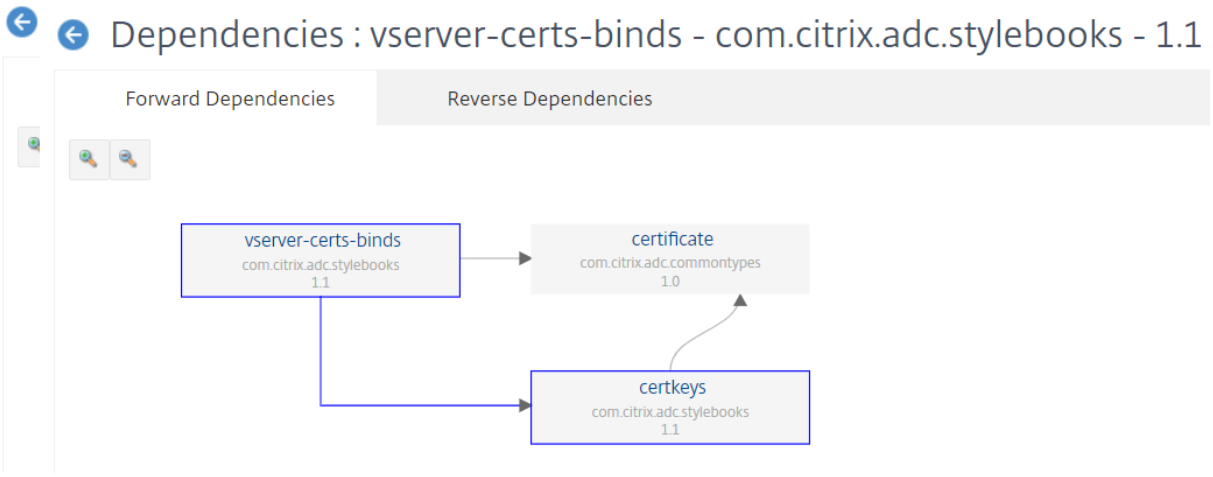
他の StyleBook で使用されている StyleBook は、既存の StyleBook が壊れるため、システムから削除することはできません。ディペンデンシーグラフ表示を使用して、StyleBook の削除を妨げている StyleBook を特定できます。

StyleBook の依存関係を表示するには

Citrix ADM で、[アプリケーション] > [スタイルブック] に移動します。[スタイルブック] ページには、Citrix ADM で使用可能なすべてのスタイルブックが表示されます。下にスクロールして、StyleBook を見つけます。**StyleBook** タイルには、構成の作成、StyleBook の定義の表示、StyleBook の依存関係の表示へのリンクが表示されます。[依存関係の表示] をクリックします。

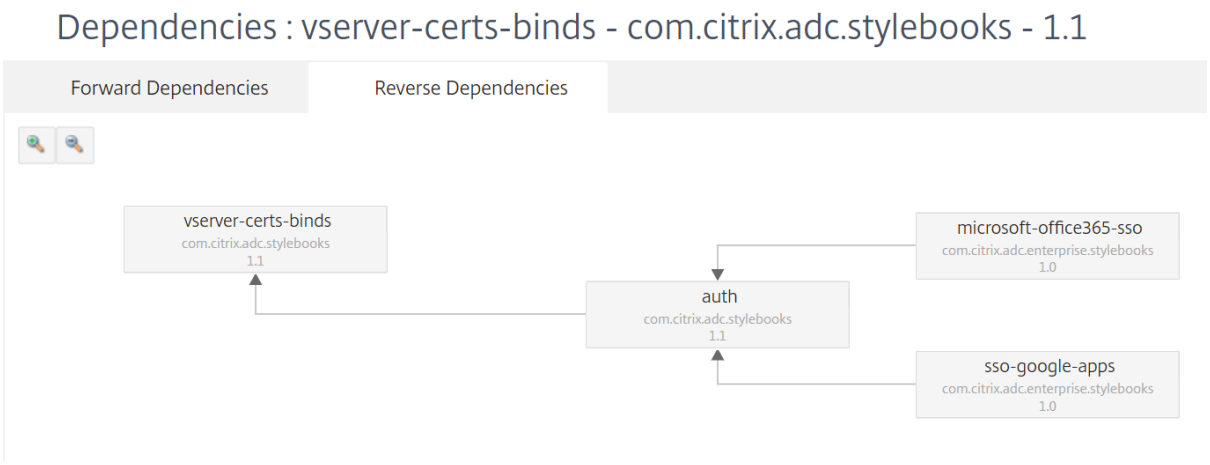
フォワード依存関係

「順方向の依存関係」タブでは、StyleBook が使用しているさまざまなデフォルトの StyleBook を表示できます。矢印に従って、StyleBook が使用している StyleBook を見つけます。マウスを矢印の 1 つにポイントすると、矢印と StyleBook がハイライト表示されます。StyleBook の名前をクリックして、その StyleBook の定義を表示することもできます。



逆依存関係

「逆依存関係」タブでは、StyleBook を使用している StyleBook をグラフィカルに表示できます。矢印に従えば、表示内のすべての StyleBook が StyleBook の方向を指していることがわかります。StyleBook が直接使用している場合や、StyleBook が別の StyleBook を介して StyleBook を使用している場合があります。



構成パックに対する **ADC** 構成の監査

StyleBook 構成パックで行った変更を、現在の ADC 構成と比較できます。この比較では、次の操作を実行できます。

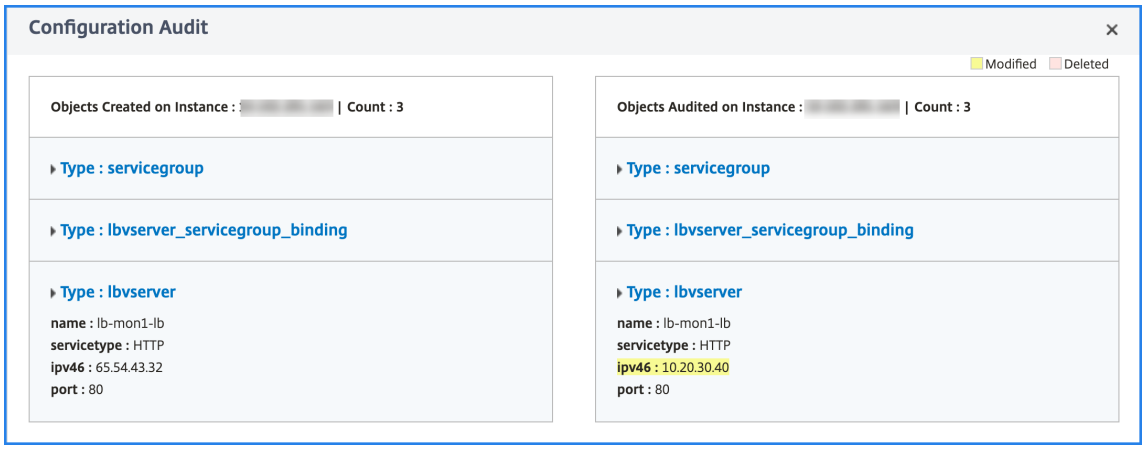
- StyleBook 構成パックと ADC 構成間の構成ドリフトを検出します。
- ADC 上で変更または削除されたオブジェクトで、構成パックによって加えられた変更を反映していないオブジェクトを特定します。

構成パックの変更と ADC の設定を比較するには、次の手順に従います。

1. 「アプリケーション」>「スタイルブック」>「構成」に移動します。

2. [構成] **[**監査] をクリックします。

   「構成の監査」ページには、作成および監査されたオブジェクトが表示されます。

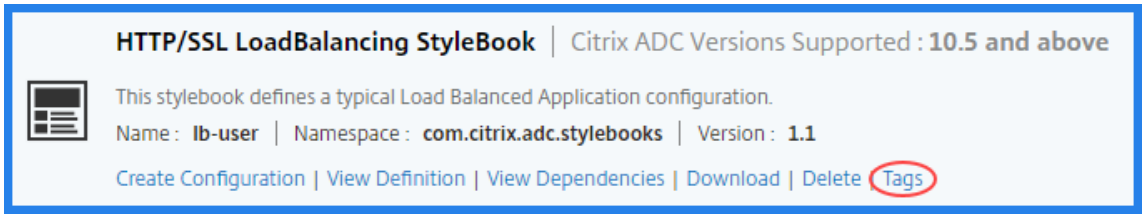


StyleBook のタグを作成する

Citrix ADM では、任意の StyleBook にタグを追加できます。タグは、異なる条件を使用して StyleBook をグループ化できるキーと値のペアです。これらのタグは、Citrix ADM で StyleBook を検索またはフィルタリングするときに使用できます。

StyleBook にタグを追加するには:

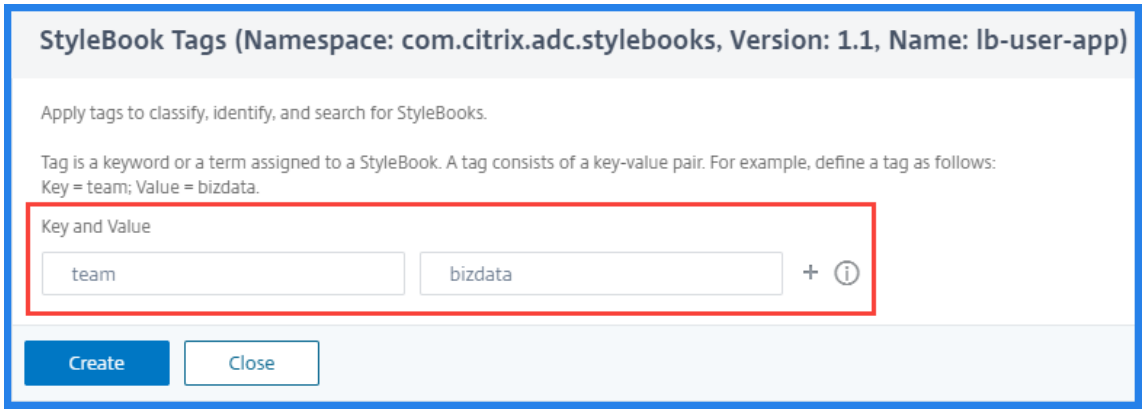
1. 「アプリケーション」>「スタイルブック」に移動します。
2. **StyleBook** で、タグを追加するタグを選択します。



   すべてのタイプの StyleBook にタグを追加できます。

3. StyleBook をフィルタリングするのに役立つ、必要な キーと値の情報を指定します。

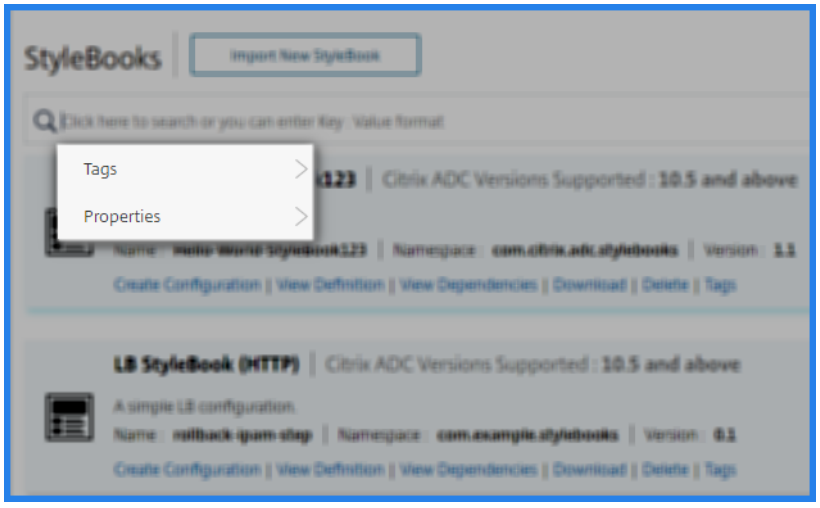
   たとえば、キー = チームと値 =BizData



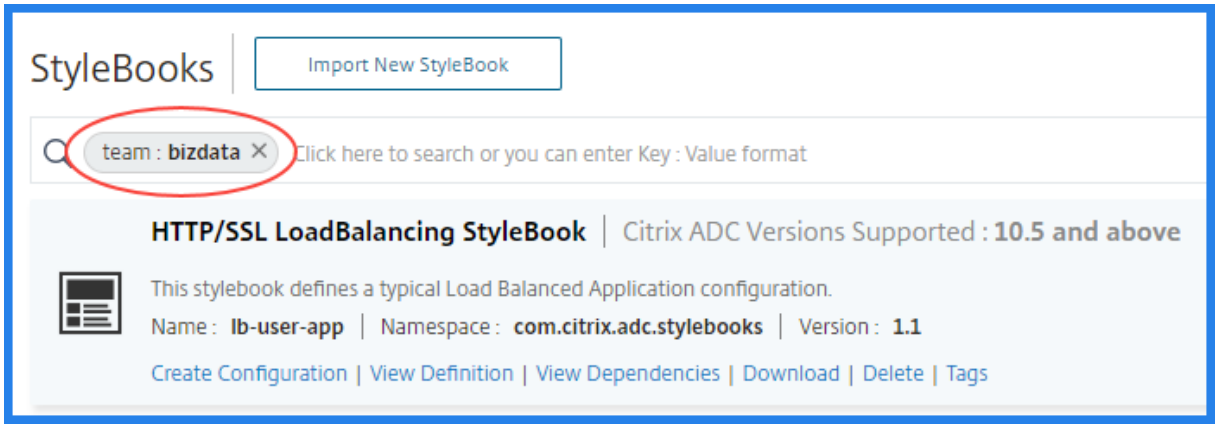
タグを追加するには、[**+**] をクリックします。

4. ［作成］ をクリックします。

タグを使用して StyleBooks をフィルタするには、検索バーで [タグ] をクリックし、リストからキーと値を選択します。指定したタグに一致する StyleBooks が表示されます。



次に、`key=team`および`value=bizdata`というタグを持つ StyleBooks を検索する例を示します。

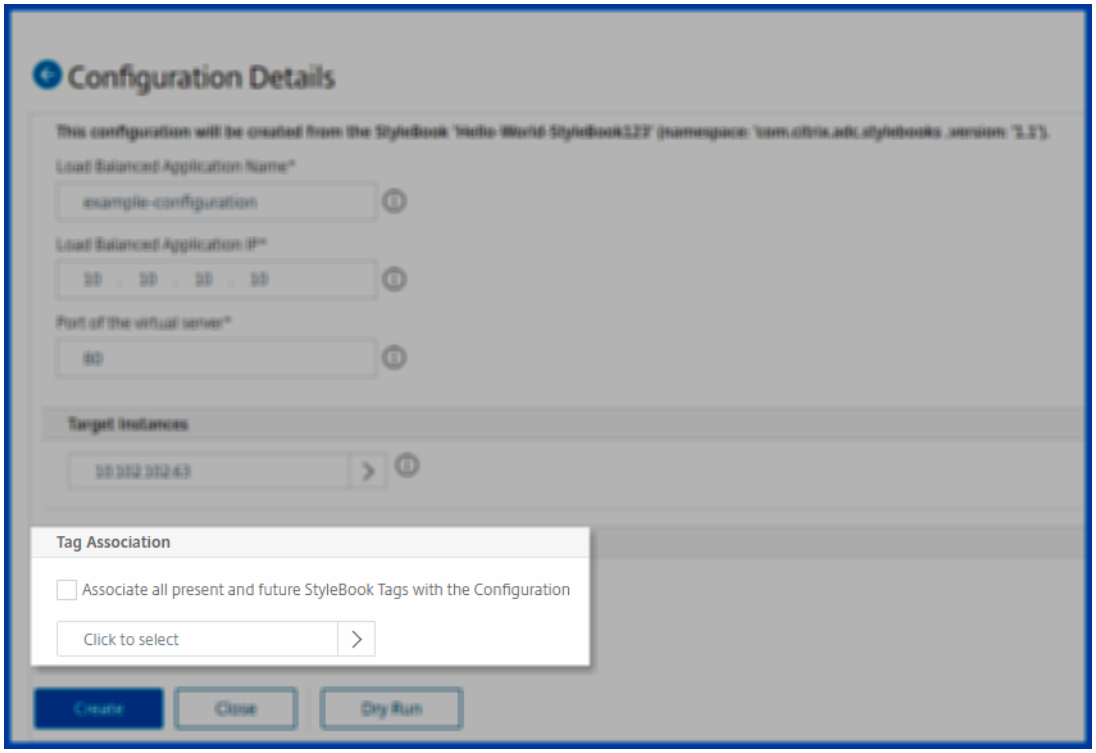


StyleBook タグを構成パックに関連付けることができます。そのため、StyleBook タグ自体を使用して構成パック

を検索できます。

構成パックを作成するときは、[タグの関連付け] セクションで次のいずれかのオプションを使用します。

- 現在および将来のすべての **StyleBook** タグを構成に関連付ける — このオプションは、すべての StyleBook タグを構成パックに関連付けます。また、今後 StyleBooks に追加する可能性のある新しいタグを必ず関連付けます。
- 「タグの選択」 -このオプションは、選択した StyleBook のタグを表示します。必要な StyleBook タグを選択し、構成パックに関連付けることができます。



GitHub リポジトリからのスタイルブックのインポートと同期

May 7, 2021

開発に CI/CD プロセスを使用しているシナリオを考えてみましょう。または、GitHub ですべてのアプリケーションのソースコードとデプロイメントオブジェクトを管理するシナリオです。

GitHub リポジトリでは、Citrix ADC 構成を展開してこれらの StyleBook を管理するために、いくつかの StyleBook を作成している可能性があります。これらのスタイルブックは、Citrix アプリケーションおよび配信管理（ADM）でも必要です。これで、これらのスタイルブックを Citrix ADM に直接インポートできるようになりました。GitHub から手動でコピーして Citrix ADM にアップロードしたり、ADM と GitHub の両方でファイルを手動で同期したりする必要はありません。

GitHub リポジトリを表すリポジトリを Citrix ADM で定義できるようになりました。GitHub リポジトリの URL と、GitHub で作成されたユーザ名、または API トークンを指定します。つまり、GitHub で有効なアカウントを持つ権限のあるユーザーのみが StyleBook をインポートおよび同期できます。

リポジトリを作成したら、Citrix ADM を GitHub リポジトリと同期できます。Citrix ADM は GitHub に接続し、そのリポジトリにある StyleBook をインポートします。次に、ADM によってスタイルブックが検証され、Citrix ADM スタイルブックのリストに追加されます。検証に失敗した場合、スタイルブックは Citrix ADM に追加されません。エラーを修正し、更新されたバージョンを GitHub リポジトリにコミットします。その後、それらをインポートするか、Citrix ADM に再度同期してみてください。

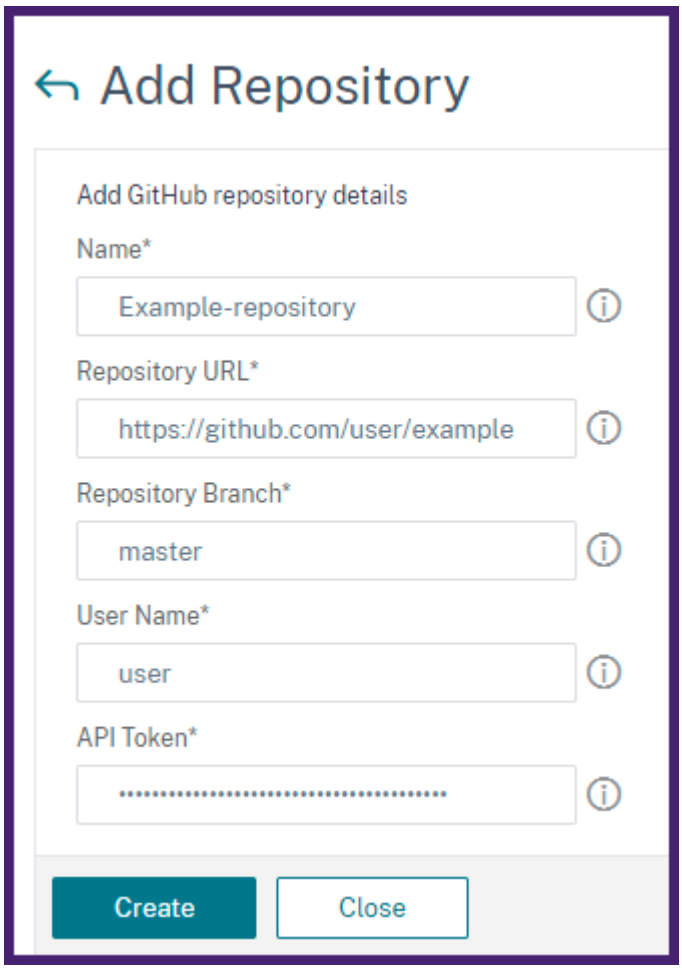
> 注
>
> - StyleBooks ファイルは、GitHub リポジトリの任意のブランチからインポートおよび同期できます。
> - 依存する StyleBook が関連付けられている StyleBook もインポートおよび同期できます。
> - GitHub リポジトリからの StyleBook の同期は、Citrix ADM GUI または API から手動で開始する必要があります。つまり、現在、StyleBook のインポートと同期は、GitHub コミットアクティビティに基づいて自動的に行われません。

リポジトリを追加し、**GitHub** リポジトリから **StyleBooks** をインポートする

開始する前に、GitHub に有効なアカウントがあることを確認してください。

GitHub リポジトリ内の任意のフォルダから、StyleBook ファイルを ADM にインポートできます。

1. Citrix ADM で、「アプリケーション」>「スタイルブック」>「リポジトリ」に移動します。
2. ［追加］をクリックします。「リポジトリの追加」ウィンドウで、次のパラメータを入力します。
   - [名前]-リポジトリの名前を入力します。この名前は、GitHub のリポジトリ名と同じでもかまいません。
   - [リポジトリ **URL**]-GitHub リポジトリの URL を入力します。
   - ユーザー名 -GitHub アカウントへのアクセスに使用するユーザー名を入力します。
   - **API** トークン -このトークンは、GitHub リポジトリにアクセスするために使用されます。GitHub リポジトリの API トークンを作成する方法については、作成, パーソナルアクセストークンの GitHub のドキュメントを参照してください。
3. ［作成］をクリックします。



リポジトリは Citrix ADM で作成されます。

4. StyleBook をインポートまたは同期するには、「リポジトリ」ページで リポジトリを選択し、「同期」をクリックします。

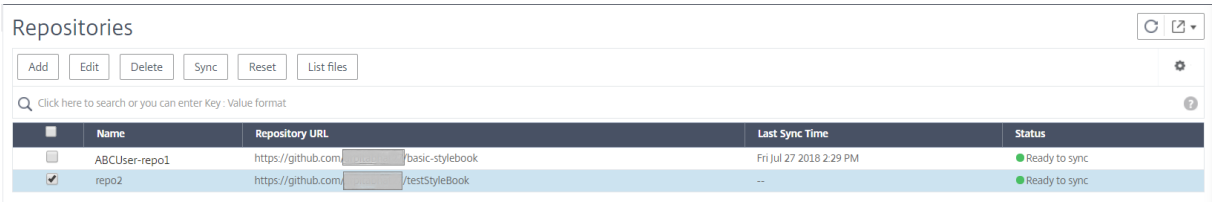
ここで使用できる他のアクションは次のとおりです。

- 編集。リポジトリの URL、ユーザー名、および API トークンを編集できます。
- **[** 削除**]:** リポジトリは、GitHub リポジトリから以前にインポートされた Citrix ADM に存在するすべての StyleBook とともに削除できます。

  > 注:
  >
  > ConfigPack が関連付けられている StyleBook がある場合は、Citrix ADM からリポジトリを削除できません。まず、これらの StyleBook のすべての構成パックを削除します。後で Citrix ADM からリポジトリを削除して、そのリポジトリから StyleBook をクリーンアップできます。

- リセット。Citrix ADM からリポジトリエントリを実際に削除しなくても、そのリポジトリから同期された Citrix ADM 内のすべての StyleBook を削除できます。
- ファイルを一覧表示します。Citrix ADM に存在する、GitHub リポジトリからのすべての StyleBook のリス

トが表示されます。



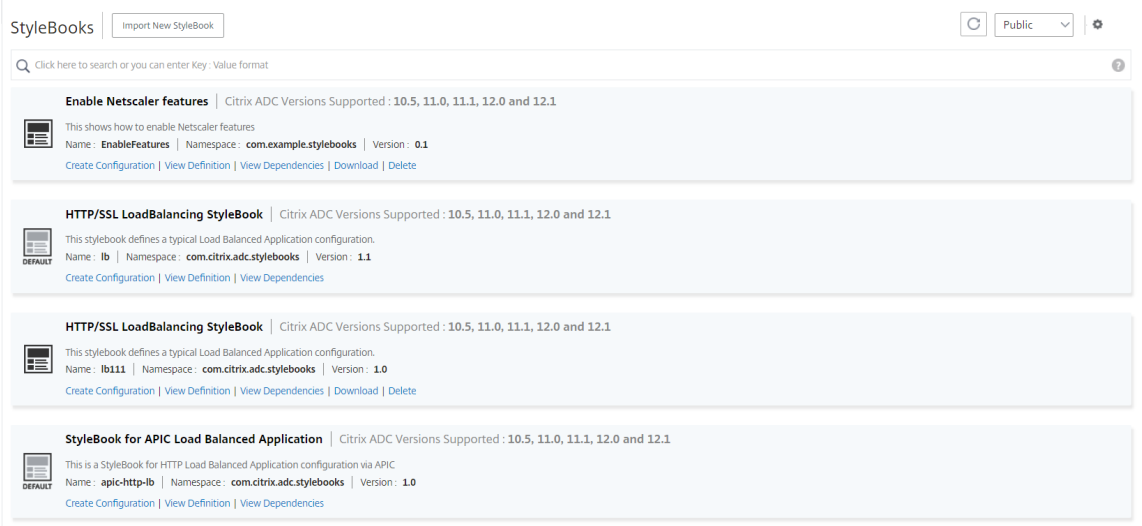
デフォルトのスタイルブックを使用する

May 7, 2021

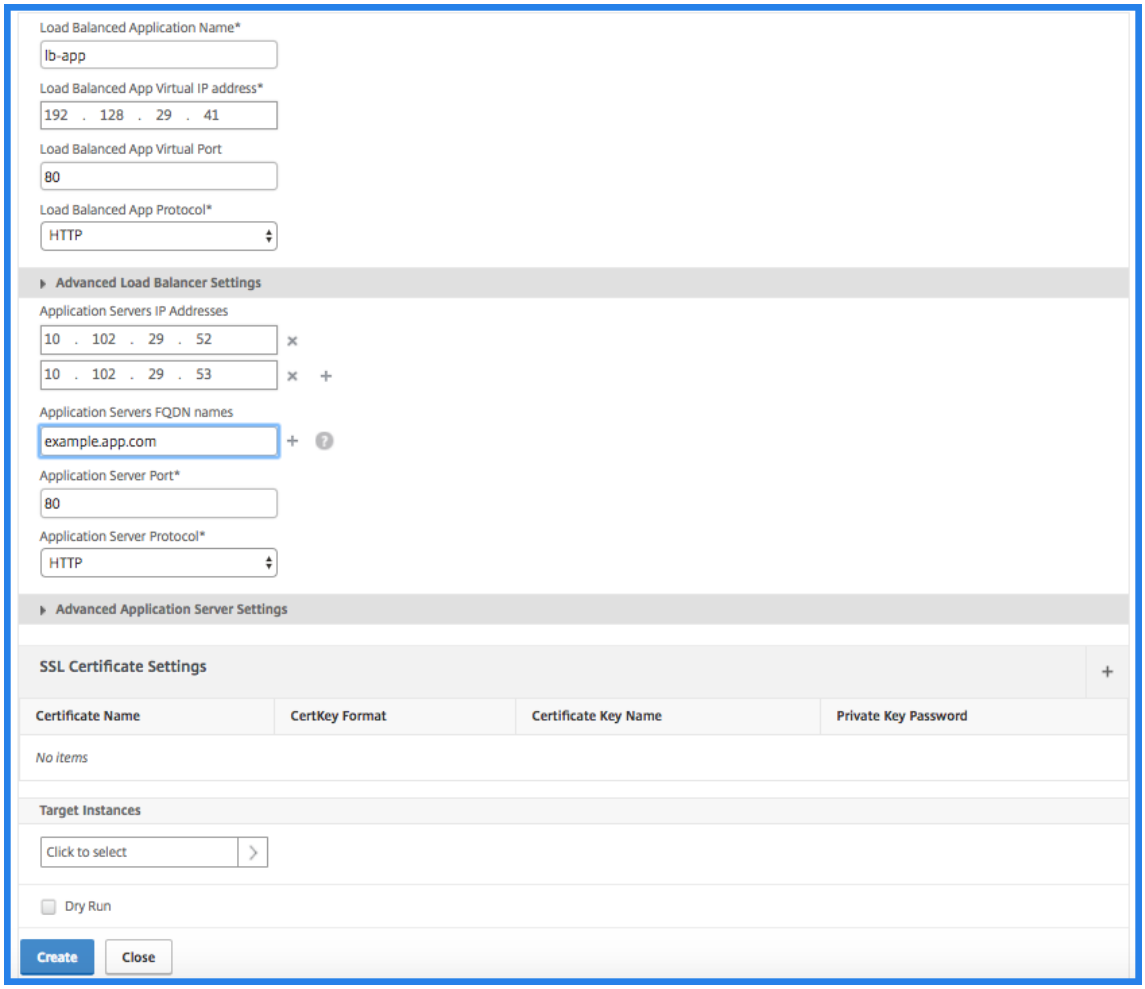
デフォルトの StyleBook のセットは、Citrix Application Delivery Management（ADM）とともに提供されます。デフォルトの StyleBook を使用する場合は、StyleBook でパラメータの値を指定し、構成を実行する Citrix ADC インスタンスの IP アドレスを選択する必要があります。構成を送信すると、Citrix ADM は指定したパラメータ値を検証し、構成のグラフを作成し、Citrix ADC インスタンスに接続し、インスタンス上で構成を実行します。

デフォルトの **StyleBook** から設定を作成するには

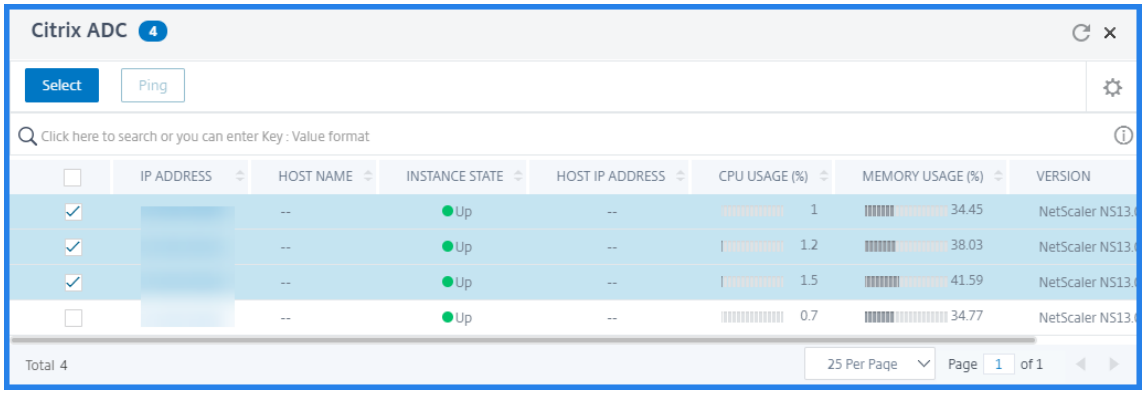
1. アプリケーション > 構成 **> StyleBooks** に移動します。[StyleBooks] ページには、Citrix ADM のすべての StyleBook が表示されます。このリストには、デフォルトの StyleBook とカスタム StyleBook の両方が含まれています。検索フィールドに StyleBook の名前 を入力し、Enter キーを押します。それ以外の場合は、リストを下にスクロールして StyleBook を見つけることができます。



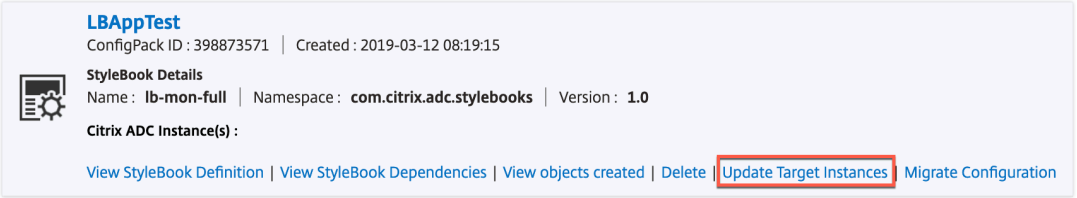
2. [構成を作成] をクリックします。パラメータに必要な値を指定します。



3. ［ターゲットインスタンス］で、構成を実行する Citrix ADC インスタンスの IP アドレスを選択します。この設定を実行するには、複数のインスタンスを選択できます。

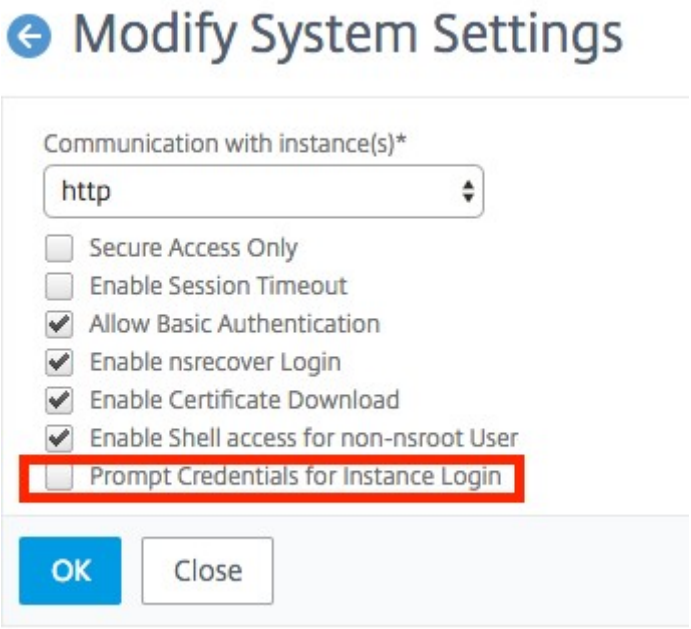


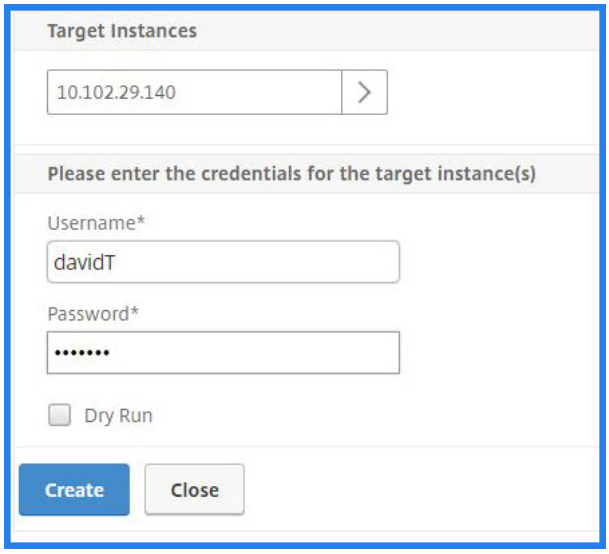
> 注:
>
> インスタンスを選択せずに構成パックを作成することもできます。その後、構成をデプロイするターゲットインスタンスを選択して、後で構成パックを更新できます。同様に、構成パック自体を削除せずに、構成パックのターゲットインスタンスをすべて削除できます。

> ユースケース: インスタンスにアクセスできない場合でも、アプリケーション用の設定パックを作成できます。
>
> 次の図は、特定のインスタンスを選択せずに作成されたこのような構成パックを示しています。[**Update Target Instances**] をクリックし、この設定をデプロイするターゲットインスタンスを選択します。
>
> 
>

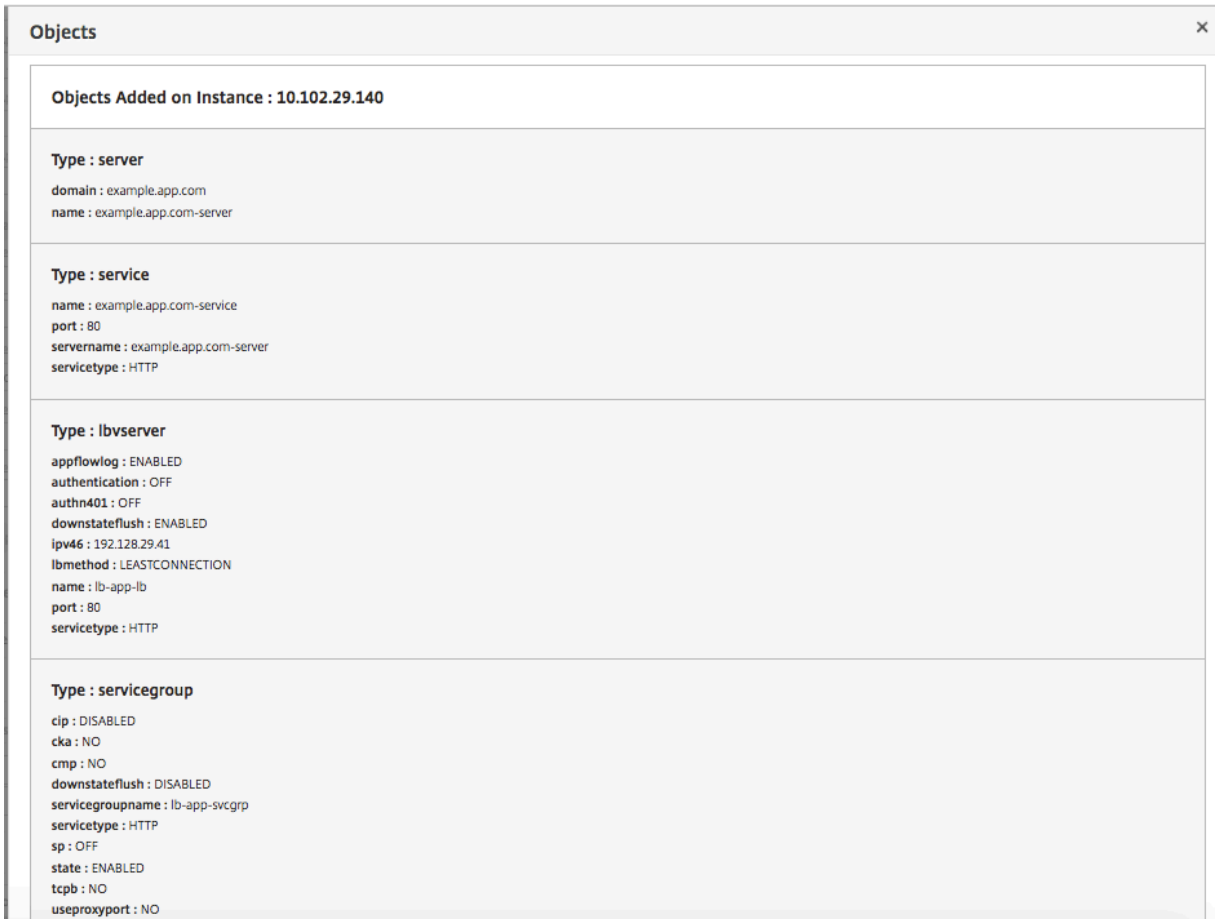
[**Citrix ADM**] > [システム] > [システム設定の変更] > [システム設定の変更] で [インスタンスログインの資格情報を要求する] オプションが有効になっている場合は、選択した Citrix ADC インスタンスで構成を実行すると Citrix ADC インスタンスの資格情報の入力を求められます。それ以外の場合、Citrix ADM はインスタンスプロファイルに格納されているインスタンス認証情報を使用してインスタンスにログインします。

ユースケース: インスタンスにアクセスできない場合でも、アプリケーション用の設定パックを作成できます。





Citrix ADC インスタンスで実行する前に構成をテストまたは検証する場合は、［ドライ実行］を選択し、［作成］をクリックします。構成が有効の場合は、指定した値に基づいて作成されたオブジェクトが表示されます。



1. ［**Dry Run**］チェックボックスをオフにし、［作成］をクリックして構成パックを作成し、Citrix ADC インスタンスで構成を実行します。以下に示すように、作成した StyleBook 構成（構成パック）が構成のリストに表

示されます。

> 注
>
> 更新アイコンをクリックして、Citrix ADM で最近検出された Citrix ADC インスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。

Citrix ADM を使用して、この構成（構成パック）を確認、更新、または削除できます。

すべてのデフォルトスタイルブックを非表示にする

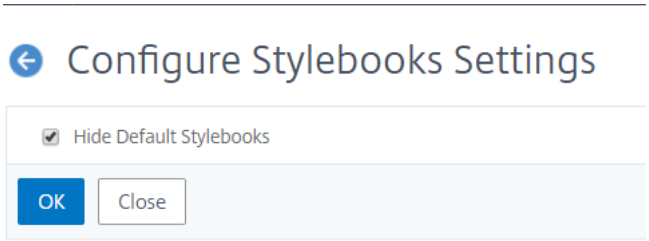
May 7, 2021

Citrix ADM には、Citrix ADM フォルダシステム内に存在するすべての StyleBook が一覧表示されます。StyleBook のリストには、プライベートとパブリックの両方に使用できるデフォルトの StyleBook とカスタム StyleBook が含まれています。管理者は、デフォルトの StyleBook をすべて非表示にすることができます。ユーザーは、自分またはユーザーが作成したカスタム StyleBook のみを表示およびアクセスすることを許可できます。

Citrix ADM では、カスタムスタイルブックを表示したり、Citrix ADM に同梱されているデフォルトのスタイルブックをすべて非表示にしたりできます。すべてのデフォルトの StyleBook を非表示にできる、新しい GUI オプションが用意されています。

すべてのデフォルト **StyleBook** を非表示にするには:

1. Citrix ADM で、［アプリケーション］>［構成］**>**［設定］に移動します。
2.「設定」ページには、デフォルトの StyleBook がユーザーに表示されるかどうかが表示されます。
3. デフォルトの StyleBook を非表示にするには、右上にある編集アイコンをクリックします。
4. **StyleBook** の設定ページで、「デフォルトの **StyleBook** を非表示にする」オプションを選択します。
5.［**OK**］をクリックします。

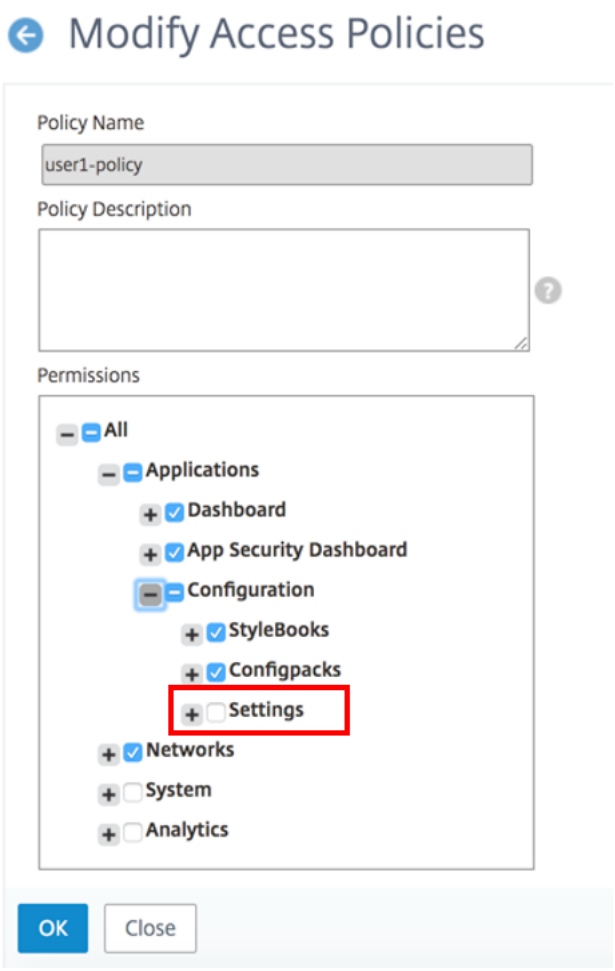


RBAC 機能を使用してページを非表示にしない場合でも、**StyleBook** 設定の設定ページは引き続き表示されます。ユーザーには、デフォルトの StyleBook を再表示するためのオプションが残っている場合があります。

StyleBook 設定の構成ページを非表示にするには、ポリシーを作成し、デフォルトの StyleBook を表示しないユーザーにそのポリシーを割り当てる必要があります。

RBAC ポリシーを作成するには、次の手順を実行します。

1. Citrix ADM で、［アカウント］ > ［ユーザー管理］ > ［アクセスポリシー］ に移動します。
2. [**Add**] をクリックしてポリシーを作成します。
3. ポリシー名を入力します。
4. [アクセス許可] セクションで、[すべて] > [アプリケーション] > [構成] > [設定] が選択されていないことを確認し、[**OK**] をクリックします。



ポリシーを作成したら、ロールを作成し、各ロールを 1 つ以上のポリシーにバインドし、ロールをユーザグループに割り当てる必要があります。ポリシーをユーザーに関連付ける方法の詳細については、「ロールベースのアクセス制御の設定」を参照してください。

StyleBooks 構成ビルダーを使用した Citrix ADC アプリケーション構成の移行

May 7, 2021

StyleBooks 構成ビルダーは、既存の ADC 設定を StyleBooks に移行するために使用されます。この機能により、ある Citrix ADC インスタンスから別のインスタンスまたは AutoScale グループへのアプリケーション構成の移行も自動化されます。

構成ビルダーは、ADC 構成の任意のバリアントに使用できる構造化アプリケーション StyleBook を提供します。この機能により、StyleBooks の文法や構造に関する深い知識がなくても、StyleBooks の使用を開始できます。それ以外の場合は、StyleBooks の作成には StyleBooks の文法と構文の知識が必要です。

また、構成ビルダーは、新しい ADC インスタンス上で同じ ADC 構成を反映する構成パックも作成します。この構成

パックを使用すると、ある ADC インスタンスの初期 ADC 設定を別の ADC インスタンスに複製できます。初期設定ソースは、次のいずれかになります。

- **Citrix ADC** インスタンス：複製するアプリケーション構成をホストするインスタンスを指定します。

  ターゲット・インスタンスを指定しない場合でも、構成ビルダーは、ADC 構成を StyleBook および構成パックに変換します。後でこの構成パックを使用して、ADC 設定を他の ADC インスタンスに移行できます。

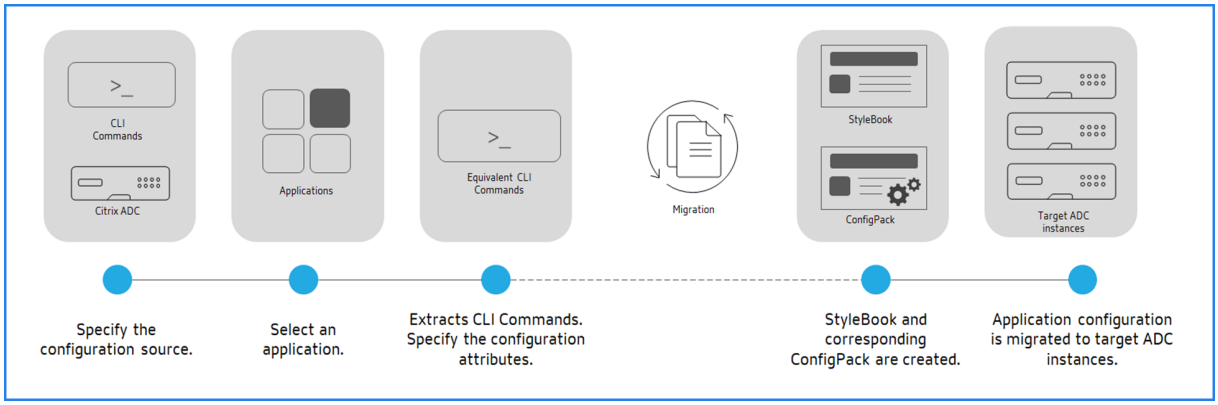
  ターゲットインスタンスが AutoScale グループの場合、構成パックは **[**ネットワーク**] > [AutoScale** グループ] ページに表示されます。[構成] タブの下にあります。

- **CLI** コマンドのセット： `ns.conf`または`Application config`から設定を貼り付けます。

構成ビルダーは、ソース構成に埋め込まれた個別のアプリケーションのリストを識別します。目的のアプリケーション設定を選択すると、構成ビルダーは、選択したアプリケーションの CLI コマンドのセットを抽出します。これらの CLI コマンドは、ソース構成から抽出されます。また、入力を必要とする可能性のあるデプロイメントおよび構成属性も識別します。

- **IP** アドレス/ポート：元の構成から仮想サーバ、サービス、サービスグループメンバーの IP アドレスとポートを表示および編集できます。
- 設定ファイル/シークレット -これらの属性は、ソース構成で指定されたパスワードまたは証明書にすることができます。

必要な情報を指定したら、ターゲット ADC インスタンスでアプリケーション構成の移行または複製を開始します。



アプリケーションの作成と移行後、`adc_nitro_application`StyleBook を使用して Citrix ADM に構成パックが作成されます。この StyleBook は、ADC の NITRO リソースに基づいて作成されます。この構成パックは、ターゲット ADC インスタンス上のアプリケーション構成を表します。作成した構成パックを表示するには、[アプリケーション] > [**StyleBooks**] > [構成] に移動します。

サポートされている **Citrix ADC** 機能

StyleBook 構成ビルダーは、ソース構成で次の Citrix ADC 機能を認識し、サポートします。

- コンテンツスイッチ

- 負荷分散
- 監視
- SSL オフロード
- レート制限
- 書き換え
- レスポンダー
- Web アプリケーションファイアウォール (WAF)

Citrix ADC アプリケーション構成を移行するための **StyleBook** の作成

以下の手順では、Citrix ADM で Citrix ADC アプリケーションの移行を移行する StyleBook を作成します。

1. 「アプリケーション」>「スタイルブック」>「構成」に移動します。
2. [**ADC** 構成の移行] をクリックします。
3. [開始] をクリックします。
4. 「構成の指定」で、構成ソースを選択します。
   - **ADC** からインポート: このオプションは、選択した ADC インスタンス上のアクティブなアプリケーションを検出します。
   - **CLI** コマンドを使用したインポート： このオプションは、CLI コマンドを分析し、CLI コマンドからアプリケーションを抽出します。
5. アプリケーション構成の移行 元または複製元の **ADC** インスタンスを指定します。

   アプリケーション構成を Autocale グループに移行するには、次の情報がソース構成に含まれていないことを確認します。

   - `IPset`
   - デバイスプロファイル
   - プロトコル
   - ポート
6. アプリケーション構成の移行先または複製先となる ターゲット **ADC** インスタンスを指定します。

   アプリケーション構成を Autocale グループに移行するには、リストから AutoScale グループを選択します。
7. 「アプリケーションの定義」で、

   a) 「アプリケーション名」で、アプリケーションの名前を指定します。

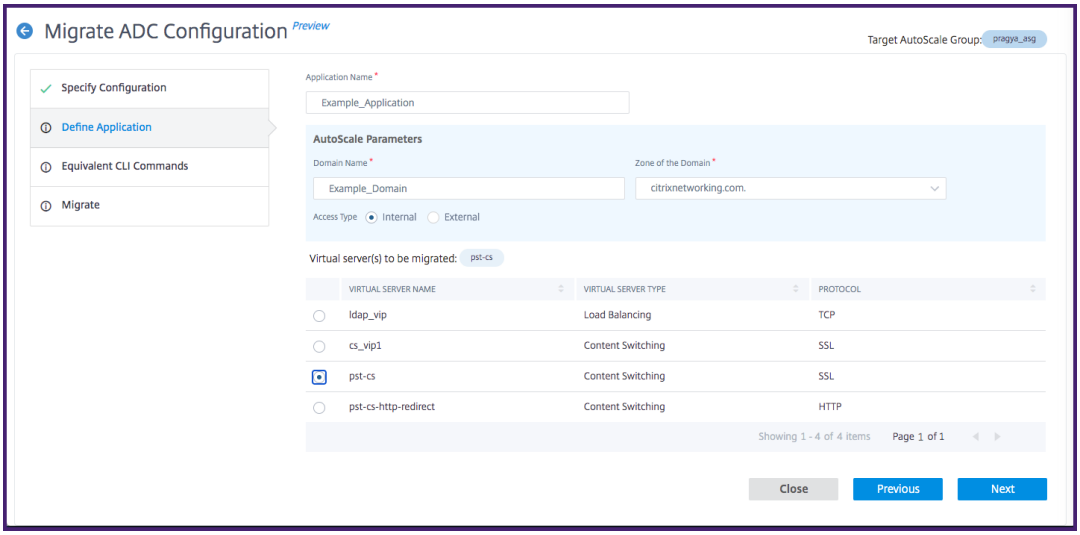
   ターゲットインスタンスが AutoScale グループの場合は、次の AutoScale パラメータを指定します。

   - アクセスタイプ -ADM Auto Scaling ソリューションは外部アプリケーションと内部アプリケーションの両方に使用できます。必要なアプリケーションアクセスタイプを選択します。

- ドメイン名 -アプリケーションのドメイン名を指定します。このオプションは、[ユーザー定義 FQDN タイプ] を選択した場合にのみ適用されます。
- **[** ドメインのゾーン]: リストからアプリケーションのゾーン名を選択します。このオプションは、[ユーザー定義 FQDN タイプ] を選択した場合にのみ適用されます。

  このドメイン名とゾーン名は、Azure の仮想サーバーにリダイレクトされます。たとえば、`app.example.com`でアプリケーションをホストする場合、`app`はドメイン名、`example.com`はゾーン名です。

b) 移行する仮想サーバーを選択します。



c) [次へ] をクリックします。

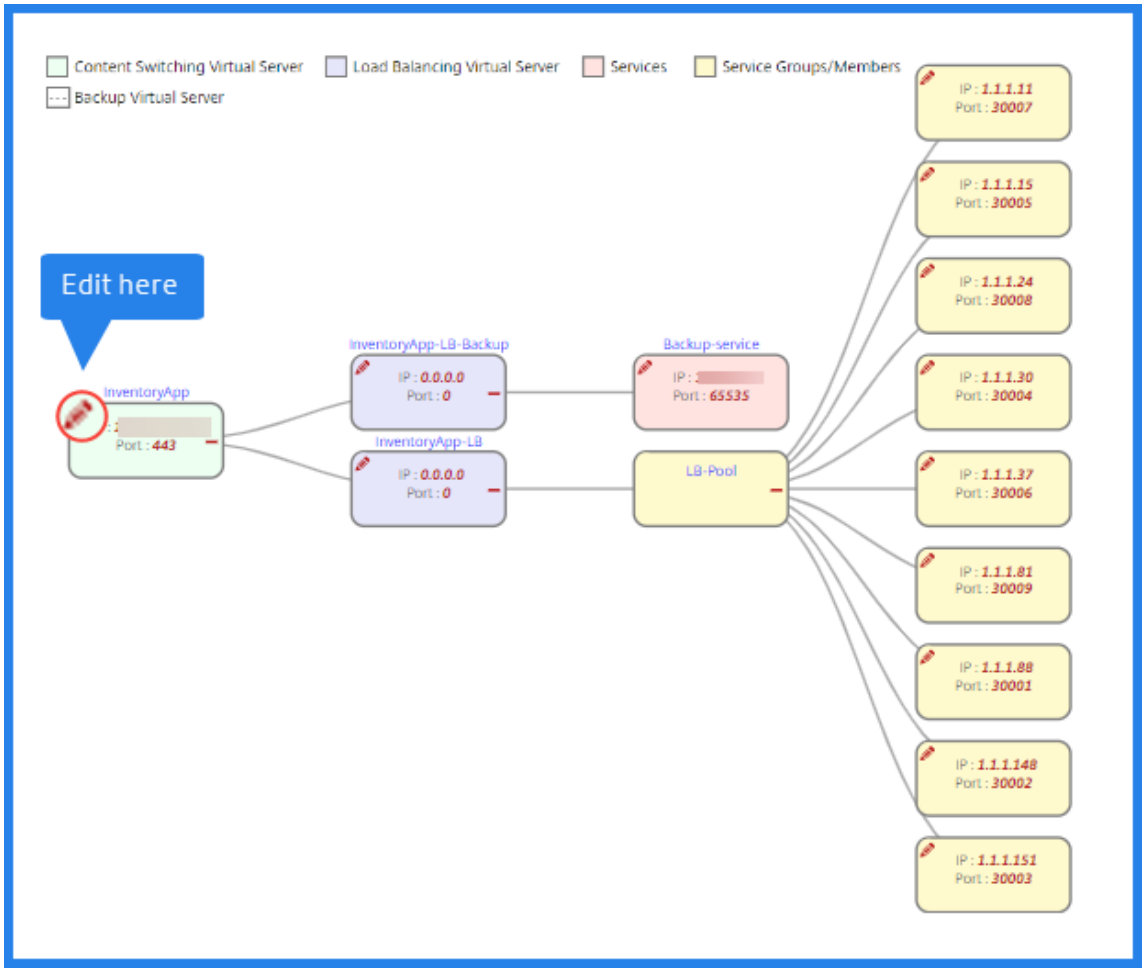
8. [同等の **CLI** コマンド] で、コマンドを確認し、[次へ] をクリックします。

   これらのコマンドは、選択したアプリケーション構成に固有です。

   > 注:
   >
   > 必要に応じて、構成を追加または編集することもできます。

9. 展開属性では、仮想サーバー、サービス、およびサービスグループメンバーの IP アドレスとポートを表示および編集できます。

   IP アドレスとポートを編集するには、フロー図の仮想サーバー、サービス、またはサービスグループメンバーの編集アイコンをクリックします。



> 注:
>
> ターゲットインスタンスが Autosale グループの場合、フロントエンド IP アドレスの編集は無効になります。

このタブは、次の場合にのみ表示されます。

- ソースインスタンスとターゲットインスタンスは異なります。
- CLI コマンドを使用して設定をインポートします。

10. 「構成属性」で必要な詳細を指定し、「次へ」をクリックします。

このタブには、パスワードや証明書を解読するためのキーなどの秘密が一覧表示されます。

> 注 移行を開始する前に、次のタブのいずれかに、欠落またはサポートされていない構成が表示されます。
>
> - サポートされていない構成
> - サポートされていないグローバル構成これらの設定を正常に移行するには
>
> 、移行先インスタンスで欠落またはサポートされていない構成を個別に適用する必要があります。次に、[次へ] をクリックします。

11. [移行] で、[移行] をクリックします。

制限事項

- ソースインスタンスで言及されている名前付き式とresponderhtmlpagesは識別されません。移行の前に、ターゲットインスタンスで名前付き式とresponderhtmlpagesを設定してください。
- ソースに、servicegroup およびモニタバインディングの設定が次のように設定されている場合。

  ```
  bind serviceGroup <Name> <Port> -monitorName <Monitor_Name>
  ```

  次のエラーが表示されます。

  ```
  1  CLI Command conversion failed: 100 - No such command [{
  2   "errorcode": 1090, "message": "No such argument [XXX]", "
         severity": "ERROR"  }
  3  ]
  4  <!--NeedCopy-->
  ```

  このエラーは、Citrix ADC がサービスグループとモニターの間のバインドを無効な形式で保存するために発生します。この問題は、Citrix ADC 12.1.52.15 ビルドから修正されます。

SSO Google Apps スタイルブック

May 7, 2021

Google Apps は、Google が開発したクラウドコンピューティング、生産性、コラボレーションツール、ソフトウェア、製品のコレクションです。シングルサインオン (SSO) を使用すると、ユーザーは、エンタープライズ資格情報を使用してすべてのサービスに対して 1 回サインインすることで、管理コンソールへのサインインを含め、すべてのエンタープライズクラウドアプリケーションにアクセスできます。

Citrix Application Delivery Management（ADM）SSO Google Apps StyleBook を使用すると、Citrix ADC インスタンスを介して Google Apps SSO を有効にすることができます。StyleBook は、ユーザーが Google Apps にアクセスできるように認証するための SAML アイデンティティプロバイダとして Citrix ADC インスタンスを構成します。

この StyleBook を使用して Citrix ADC インスタンスで Google アプリの SSO を有効にすると、以下の手順が実行されます。

1. 認証仮想サーバーの構成
2. SAML IdP ポリシーとプロファイルの設定
3. 認証仮想サーバーへのポリシーとプロファイルのバインド
4. インスタンスでの LDAP 認証サーバーおよびポリシーの構成
5. インスタンスで設定された認証仮想サーバーへの LDAP 認証サーバーおよびポリシーのバインド

構成の詳細:

次の表に、この統合を正常に動作させるために最低限必要なソフトウェアバージョンを示します。統合プロセスは、同じのより高いバージョンもサポートします。

製品	最低限必要なバージョン
Citrix ADC	リリース 11.0、アドバンス/プレミアムライセンス

以下の手順は、認証要求を Citrix ADC が監視する IP アドレスにルーティングするために、適切な外部および内部 DNS エントリをすでに作成していることを前提としています。

SSO Google アプリの **StyleBook** 設定をデプロイする:

次のタスクは、Microsoft SSO Google Apps StyleBook をビジネスネットワークに展開する際に役立ちます。

SSO Google アプリのスタイルブックをデプロイするには

1. Citrix ADM で、[アプリケーション] > [構成] > [スタイルブック] に移動します。[スタイルブック] ページには、Citrix ADM で使用可能なすべてのスタイルブックが表示されます。下にスクロールして、**SSO Google Apps** スタイルブックを見つけます。[構成を作成] をクリックします。
2. StyleBook がユーザーインターフェイスページとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。
3. 次のパラメーターの値を入力します。
   a) アプリケーション名。ネットワークにデプロイする SSO Google アプリ設定の名前。
   b) 認証仮想 **IP** アドレス。Google アプリ SAML IdP ポリシーがバインドされている Citrix ADC AAA 仮想サーバーで使用される仮想 IP アドレス。
   c) **SAML** ルール式。デフォルトでは、HTTP.REQ.HEADER（「参照元」）.CONTAINS（「グーグル」）という Citrix ADC ポリシー（PI）式が使用されます。要件が異なる場合は、このフィールドを別の式で更新します。このポリシー式は、これらの SAML SSO 設定が適用されるトラフィックに一致し、リファラーヘッダーが Google ドメインから来ていることを確認します。
4. [SAML IdP 設定] セクションでは、手順 3 で作成した Citrix ADC AAA 仮想サーバーで使用される SAML IdP プロファイルとポリシーを作成して、Citrix ADC インスタンスを SAML ID プロバイダーとして構成できます。
   a) **SAML** 発行者名。このフィールドには、認証仮想サーバのパブリック FQDN を入力します。例: `https://<Citrix_ADC_VIP>/saml/login`
   b) **SAML** サービスプロバイダー **(SP) ID**。（オプション）Citrix ADC アイデンティティプロバイダは、この ID に一致する発行者名からの SAML 認証要求を受け入れます。

c) アサーションコンシューマサービスの **URL**。ユーザー認証が成功した後、Citrix ADC ID プロバイダーが SAML アサーションを送信する必要があるサービスプロバイダーの URL を入力します。アサーション・コンシューマ・サービス URL は、アイデンティティ・プロバイダ・サーバー・サイトまたはサービス・プロバイダ・サイトで開始できます。

d) このセクションには、その他のオプションのフィールドを入力できます。たとえば、次のオプションを設定できます。

i. SAML バインディングプロファイル (デフォルトは「POST」プロファイル)。

ii. SAML 要求/応答を検証/署名する署名アルゴリズム (デフォルトは”RSA-SHA1”)。

iii. SAML 要求/応答のハッシュをダイジェストする方法 (デフォルトは「SHA-1」)。

iv. 暗号化アルゴリズム（デフォルトは AES256）およびその他の設定。

> 注
>
> これらの設定は Google Apps をサポートするためにテストされているため、デフォルト設定のままにすることをお勧めします。

e)「ユーザー属性」チェック・ボックスを有効にして、次のようなユーザー詳細を入力することもできます。

i. ユーザー属性の名前

ii. 属性の値を抽出するために評価される Citrix ADC PI 式

iii. 属性のわかりやすい名前

iv. ユーザー属性の形式を選択します。

これらの値は、発行された SAML アサーションに含まれます。この StyleBook を使用して Citrix ADC が発行するアサーションには、最大 5 セットのユーザー属性を含めることができます。

5. [LDAP 設定] セクションで、次の詳細を入力して Google Apps ユーザーを認証します。ドメインユーザーが企業のメールアドレスを使用して Citrix ADC インスタンスにログオンできるようにするには、以下を構成する必要があります。

a) **LDAP**（**Active Directory**）ベース。認証を許可する Active Directory（AD）内にユーザーアカウントが存在するドメインの基本ドメイン名を入力します。例: `dc=netscaler,dc=com`

b) **LDAP**（**Active Directory**）バインド **DN**。AD ツリーを参照する権限を持つドメインアカウント (構成を容易にするために電子メールアドレスを使用) を追加します。例: `cn=Manager,dc=netscaler,dc=com`

c) **LDAP (Active Directory)** バインド **DN** パスワード。認証用のドメインアカウントのパスワードを入力します。

d) このセクションで入力する必要があるその他のフィールドは次のとおりです。

i. ユーザー認証のために Citrix ADC が接続する LDAP サーバー IP アドレス

ii. LDAP サーバーの FQDN 名

> 注:
>
> 上記の 2 つのうち少なくとも 1 つ、LDAP サーバーの IP アドレスまたは FQDN 名を指定する必要があります。

iii. Citrix ADC がユーザーを認証するために接続する LDAP サーバーポート（デフォルトは 389 です）。

iv. LDAP ホスト名。これは、検証がオンになっている場合（デフォルトではオフになっています）、LDAP 証明書を検証するために使用されます。

v. LDAP ログイン名属性。ログイン名の抽出に使用されるデフォルトの属性は`samAccountname`です。

vi. その他のオプションの LDAP 設定

6.「SAML IdP SSL 証明書」セクションでは、SSL 証明書の詳細を指定できます。

a) 証明書名。SSL 証明書の名前を入力します。

b) 証明書ファイル。ローカルシステムまたは **Citrix ADM** 上のディレクトリから、**SSL** 証明書ファイルを検索します。

c) 証明書キーの形式。ドロップダウンリストボックスから、証明書と秘密キーファイルの形式を選択します。サポートされている形式は、`.pem`および`.der`拡張子です。

d) 証明書キー名。証明書の秘密キーの名前を入力します。

e) 証明書キーファイル。ローカルシステムまたは Citrix ADM から、証明書の秘密キーを含むファイルを選択します。

f) 秘密キーのパスワード。秘密鍵ファイルがパスフレーズで保護されている場合は、このフィールドに入力します。

g) [証明書の詳細設定] チェックボックスをオンにして、証明書の有効期限通知期間などの詳細を入力したり、証明書の有効期限モニターを有効または無効にすることができます。

7. 上記の SAML IdP 証明書で Citrix ADC に CA パブリック証明書をインストールする必要がある場合は、必要に応じて、IdP SSL CA 証明書を選択できます。詳細設定で「CA 証明書です」を選択してください。

8. 必要に応じて、[SAML SP SSL 証明書] を選択して、Google Apps (SAML SP) からの認証要求の検証に使用される Google SSL 証明書 (公開キー) を指定できます。

9.［ターゲットインスタンス］をクリックし、この Google Apps SSO 構成を展開する Citrix ADC インスタンスを選択します。［作成］をクリックして構成を作成し、選択した Citrix ADC インスタンスに構成を展開します。

> 注
>
> 更新アイコンをクリックして、Citrix ADM で最近検出された Citrix ADC インスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。

また、

> ヒント
>
> > Citrix では、実際の構成を実行する前に、［ドライ実行］を選択して、StyleBook によってターゲット Citrix ADC インスタンス上に作成された構成オブジェクトを視覚的に確認することをお勧めします。

SSO Office 365 StyleBook

May 7, 2021

Microsoft™ Office 365 は、Microsoft がサブスクリプションベースで提供する、クラウドベースの生産性およびコラボレーションアプリケーションのスイートです。これは、Exchange、SharePoint、Office、および Skype for Business などの Microsoft の一般的なサーバーベースのアプリケーションが含まれています。シングル・サインオン（SSO）により、ユーザーはすべてのエンタープライズ・クラウド・アプリケーションにアクセスできます。

- 管理コンソールにサインインする管理者を含める
- エンタープライズ資格情報を使用して、すべての Microsoft Office 365 サービスに対して 1 回限りのサインオンを行います。

SSO Office 365 スタイルブックを使用すると、Citrix ADC インスタンスを介して Microsoft Office 365 用の SSO を有効にすることができます。SAML アイデンティティプロバイダ（IdP）として Citrix ADC を使用して、SAML サービスプロバイダとして Microsoft Office 365 を使用して SAML 認証を構成できるようになりました。

このスタイルブックを使用して Citrix ADC インスタンスで Microsoft Office 365 用の SSO を有効にするには、次の手順に従います。

1. 認証仮想サーバーの構成
2. SAML IdP ポリシーとプロファイルの設定
3. 認証仮想サーバーへのポリシーとプロファイルのバインド
4. インスタンスでの LDAP 認証サーバーおよびポリシーの構成
5. LDAP 認証サーバーとポリシーを、インスタンスで設定した認証仮想サーバーにバインドします。

この統合が正常に機能するために最低限必要なソフトウェアバージョンを示します。統合プロセスは、同じのより高いバージョンもサポートします。

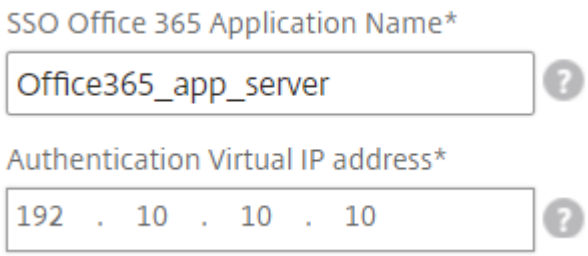
製品	最低限必要なバージョン
Citrix ADC	11.0, アドバンス/プレミアムライセンス

次の手順は、適切な外部および内部 DNS エントリが既に作成されていることを前提としています。これらのエントリは、認証要求を Citrix ADC で監視される IP アドレスにルーティングするために不可欠です。

次の手順は、SSO Office 365 StyleBook をビジネスネットワークに実装する際に役立ちます。

SSO Microsoft Office 365 スタイルブックを展開するには

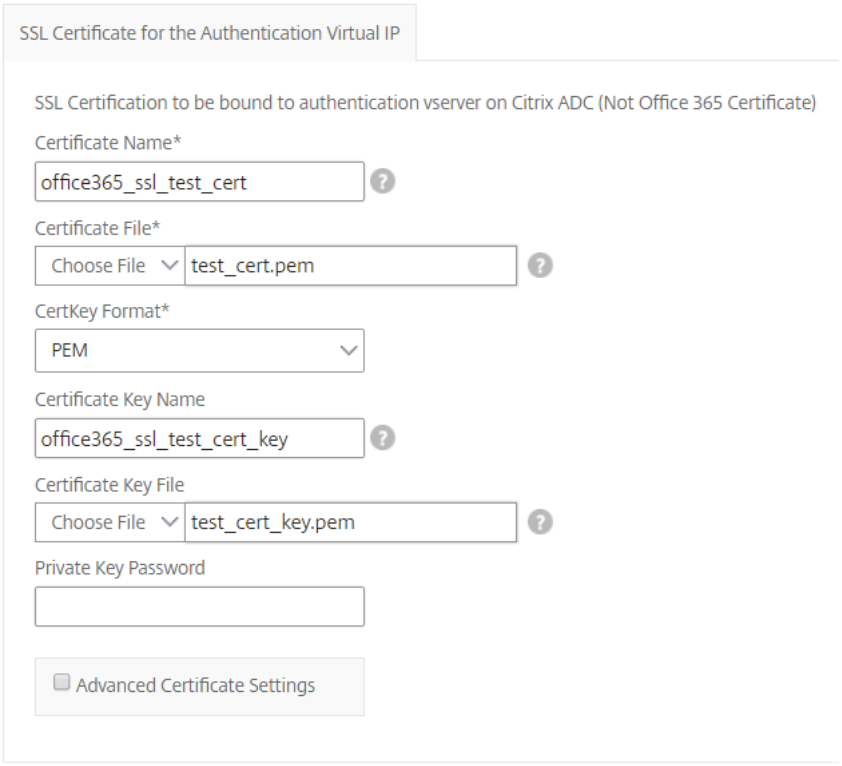
1. Citrix Application Delivery Management（ADM）で、［アプリケーション］>［スタイルブック］に移動します。［スタイルブック］ページには、Citrix ADM で使用可能なすべてのスタイルブックが表示されます。下にスクロールして、**SSO Office 365** スタイルブックを見つけます。[構成を作成] をクリックします。
2. StyleBook がユーザーインターフェイスページとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。
3. 次のパラメーターの値を入力します。
   a) アプリケーション名。ネットワークに展開する SSO Microsoft Office 365 構成の名前。
   b) 認証仮想 **IP** アドレス。Microsoft Office 365 SAML IdP ポリシーがバインドされている Citrix ADC AAA 仮想サーバーで使用される仮想 IP アドレス。



4. **[SSL** 証明書の設定**]** セクションで、SSL 証明書の名前と証明書キーを入力します。

   > 注
   >
   > これは Office 365 サービスプロバイダー証明書ではありません。この SSL 証明書は、Citrix ADC インスタンスの仮想認証サーバーにバインドされます。

5. ローカルストレージフォルダからそれぞれのファイルを選択します。また、秘密鍵パスワードを入力して、暗号化された秘密鍵を PEM 形式でロードすることもできます。



6. **[** 証明書の詳細設定] チェックボックスをオンにすることもできます。ここでは、証明書の有効期限通知期間などの詳細を入力したり、証明書の有効期限モニターを有効または無効にすることができます。
7. **SSL** 証明書で **Citrix ADC** に **CA** パブリック証明書をインストールする必要がある場合は、オプションで［認証仮想 IP の SSL CA 証明書］チェックボックスをオンにできます。上記の [証明書 の詳細設定**]** セクションで **[CA** 証明書です] を選択してください。
8. [**SSO Office 365** の **LDAP** 設定] セクションで、Office 365 ユーザーを認証するために次の詳細を入力します。ドメインユーザーが企業のメールアドレスを使用して Citrix ADC インスタンスにログオンできるようにするには、次のように構成します。

   a) **LDAP**（**Active Directory**）ベース。認証を許可する Active Directory（AD）内にユーザーアカウントが存在するドメインの基本ドメイン名を入力します。例：`dc=netscaler,dc=com`

   b) **LDAP**（**Active Directory**）バインド **DN**。AD ツリーを参照する権限を持つドメインアカウント (構成を容易にするために電子メールアドレスを使用) を追加します。例：`cn=Manager,dc=netscaler,dc=com`

   c) **LDAP (Active Directory)** バインド **DN** パスワード。認証用のドメインアカウントのパスワードを入力します。

   d) このセクションで入力する必要があるその他のフィールドは次のとおりです。

      i. Citrix ADC がユーザーを認証するために接続する LDAP サーバー IP アドレス。

      ii. LDAP サーバーの FQDN 名。

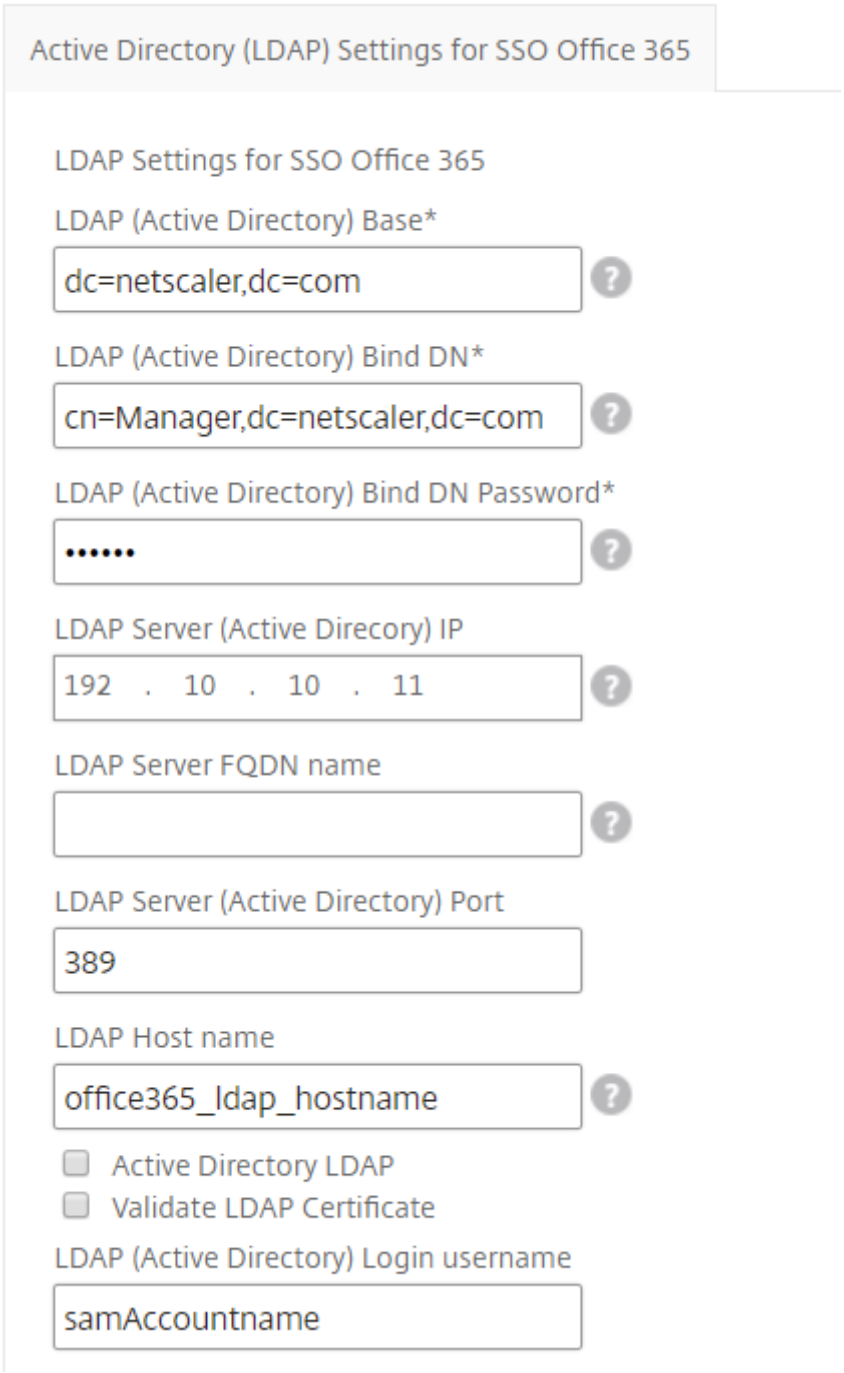
> 注:
>
> 上記の 2 つのうち少なくとも 1 つ、LDAP サーバーの IP アドレスまたは FQDN 名を指定する必要があります。

iii. Citrix ADC がユーザーを認証するために接続する LDAP サーバーポート（デフォルトは 389 です）。LDAPS は 636 を使用している。

iv. LDAP ホスト名。検証がオン（デフォルトではオフ）の場合、ホスト名を使用して LDAP 証明書を検証します。

v. LDAP ログイン名属性。ログイン名の抽出に使用されるデフォルトの属性は「sAMAccountName」です。

vi. その他のオプションの LDAP 設定。



9. **SAML IdP** 証明書セクションでは、SAML アサーションに使用される SSL 証明書の詳細を指定できます。

   a) 証明書名。SSL 証明書の名前を入力します。

   b) 証明書ファイル。ローカルシステム上のディレクトリから SSL 証明書ファイルを選択します。

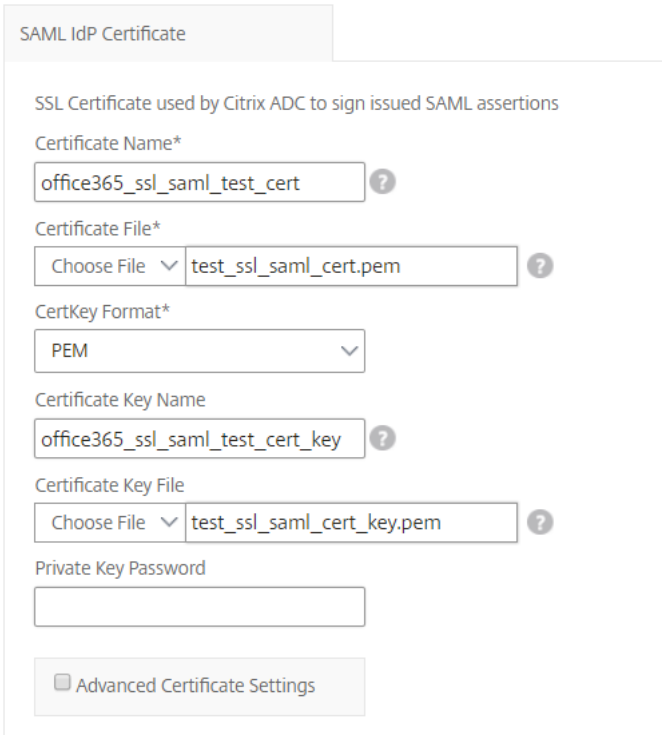
   c) 証明書キーの形式。ドロップダウンリストボックスから、証明書と秘密キーファイルの形式を選択します。サポートされている形式は、.pem と.der 拡張子です。

   d) 証明書キー名。証明書の秘密キーの名前を入力します。

e) 証明書キーファイル。ローカルシステムから証明書の秘密キーを含むファイルを選択します。

f) 秘密鍵パスワード: 秘密鍵ファイルを保護するパスフレーズを入力します。

[証明書の詳細設定] チェックボックスをオンにすることもできます。ここでは、証明書の有効期限通知期間などの詳細を入力したり、証明書の有効期限モニターを有効または無効にすることができます。



10. 上記の **SAML IdP** 証明書で **Citrix ADC** に **CA** パブリック証明書をインストールする必要がある場合は、オプションで「SAML IdP CA 証明書」を選択できます。上記の [証明書の詳細設定] セクションで **[CA** 証明書か] を選択してください。

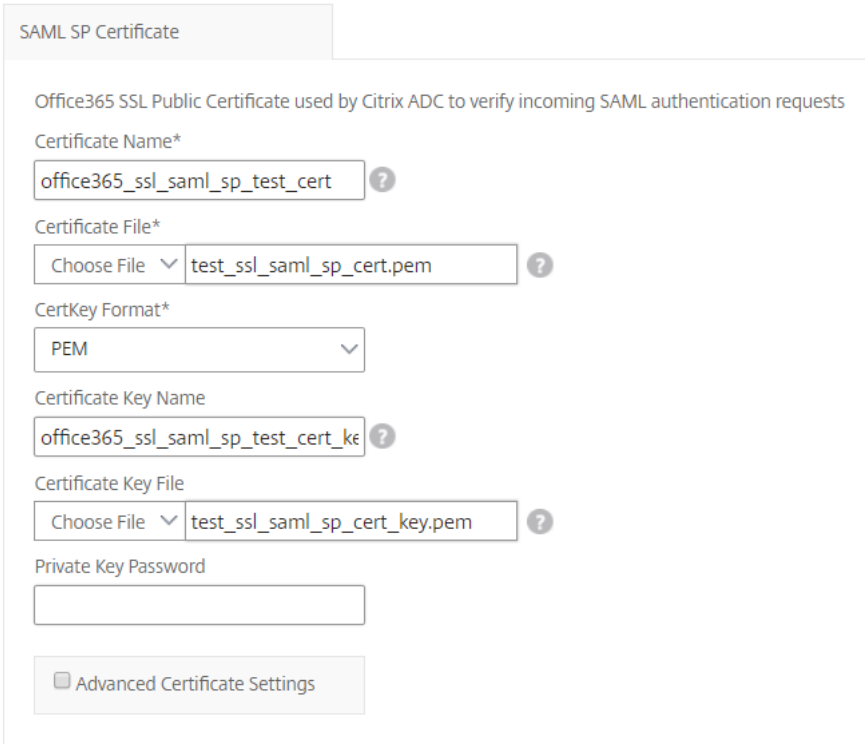
11. [**SAML SP** 証明書] セクションで、Office 365 SSL パブリック証明書について次の詳細を入力します。この証明書は、着信 SAML 認証要求を検証するために Citrix ADC インスタンスによって使用されます。

a) 証明書名。SSL 証明書の名前を入力します。

b) 証明書ファイル。ローカルシステム上のディレクトリから SSL 証明書ファイルを選択します。

c) 証明書キーの形式。ドロップダウンリストボックスから、証明書と秘密キーファイルの形式を選択します。サポートされている形式は、.pem と.der 拡張子です。

[証明書の詳細設定] チェックボックスをオンにすることもできます。ここでは、証明書の有効期限通知期間などの詳細を入力したり、証明書の有効期限モニターを有効または無効にすることができます。



12. [**SAML Idp** 設定] セクションでは、手順 3 で作成した Citrix ADC AAA 仮想サーバーで使用される SAML IdP プロファイルとポリシーを作成して、Citrix ADC インスタンスを SAML ID プロバイダーとして構成できます。

    a) **SAML** 発行者名。このフィールドには、認証仮想サーバーのパブリック FQDN を入力します。例: `https://\<Citrix ADC_VIP_Address\>/saml/login`

    b) 名前識別子式。SAML アサーションで送信された SAML 名識別子を抽出するために評価される Citrix ADC 式を入力します。例: `"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`

    c) 署名アルゴリズム: SAML 要求/応答を検証/署名するアルゴリズムを選択します (デフォルトは「RSA-SHA256」)。

    d) ダイジェスト方式。SAML 要求/応答のハッシュをダイジェストする方法を選択します (デフォルトは「SHA256」)。

    e) オーディエンスの名前。サービスプロバイダ (Microsoft Office 365) を表すエンティティ名または URL を入力します。

    f) **SAML** サービスプロバイダー **(SP) ID**。(オプション) Citrix ADC アイデンティティプロバイダは、この ID に一致する発行者名からの SAML 認証要求を受け入れます。

    g) アサーションコンシューマサービスの **URL**。ユーザー認証が成功した後、Citrix ADC ID プロバイダーが SAML アサーションを送信する必要があるサービスプロバイダーの URL を入力します。アサーション・コンシューマ・サービス URL は、アイデンティティ・プロバイダ・サーバー・サイトまたはサービス・プロバイダ・サイトで開始できます。

h) このセクションには、その他のオプションのフィールドを入力できます。たとえば、次のオプションを設定できます。

   i. **SAML** 属性名。SAML アサーションで送信されるユーザー属性の名前。

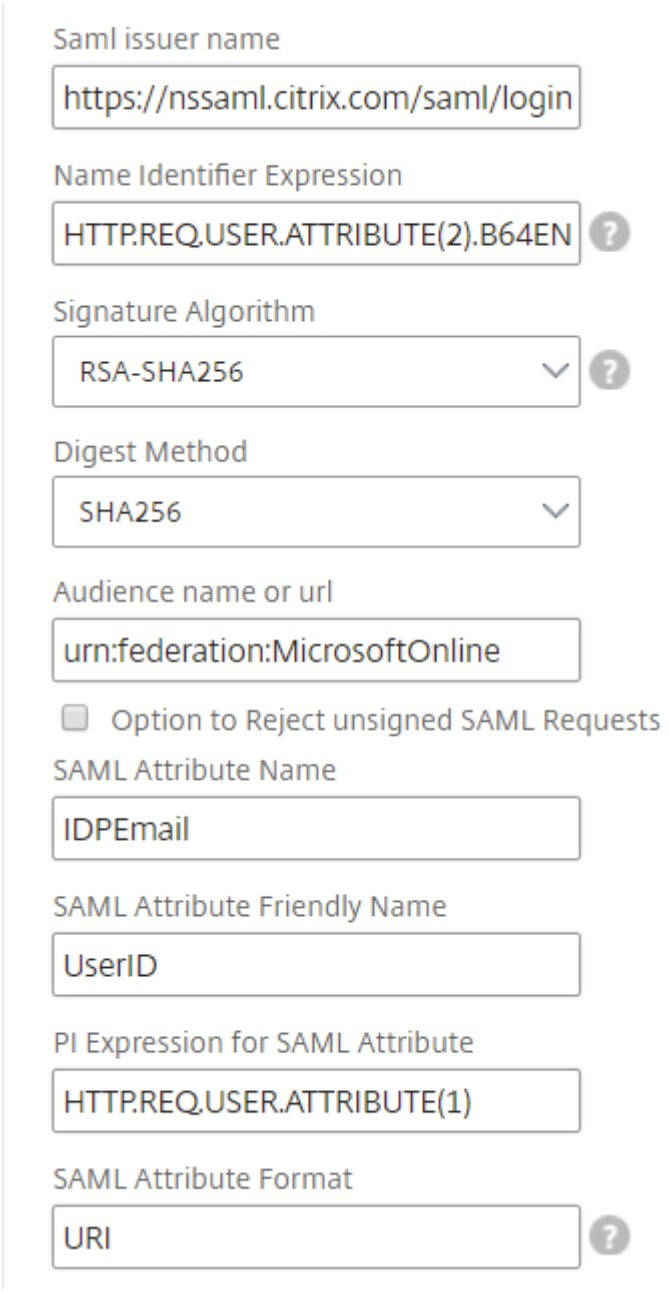
   ii. **SAML** 属性のフレンドリ名。SAML アサーションで送信されるユーザー属性のフレンドリ名。

   iii. **SAML** 属性の **PI** 式。デフォルトでは、次の Citrix ADC ポリシー（PI）式が使用されます: HTTP.REQ.USER.ATTRIBUE（1）。このフィールドは、LDAP サーバ（メール）から送信される最初のユーザー属性を SAML 認証属性として指定します。

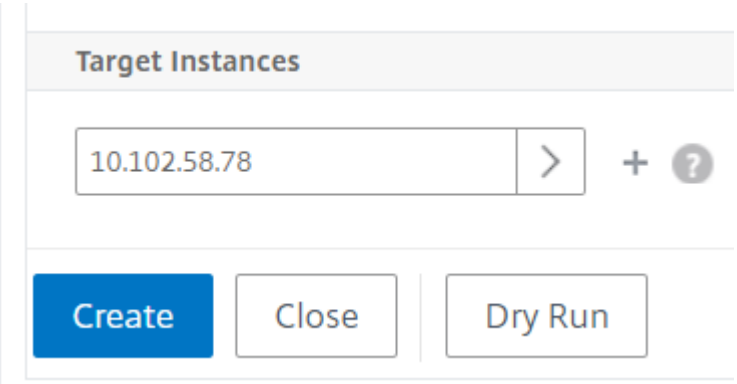
   iv. ユーザー属性の形式を選択します。

   これらの値は、発行された SAML アサーションに含まれます。

   > ヒント
   >
   > Microsoft Office 365 アプリをサポートするためにこれらの設定がテストされているため、デフォルト設定のままにすることをお勧めします。



13. ［ターゲットインスタンス］をクリックし、この Microsoft Office 365 SSO 構成を展開する Citrix ADC インスタンスを選択します。［作成］をクリックして構成を作成し、選択した Citrix ADC インスタンスに構成を展開します。



ヒント

実際の構成を実行する前に、［**Dry Run** ］を選択して、StyleBook によってターゲット Citrix ADC インスタンスに作成された構成オブジェクトを表示することをお勧めします。

スタイルブックのための **Microsoft Skype for Business**

May 7, 2021

Skype for Business 2015 アプリケーションは、機能するいくつかの外部コンポーネントに依存します。Skype for Business ネットワークは、サーバーとそれらのオペレーティングシステム、データベース、認証システムと承認システム、ネットワーキングシステムとインフラストラクチャ、および電話の PBX（Private Branch Exchange：構内交換機）システムなど、さまざまなシステムで構成されています。Skype for Business Server 2015 は、2 つのバージョン、スタンダードエディションと高度なエディションで利用可能です。主な違いは、Advanced Edition にのみ含まれる高可用性機能のサポートにあります。高可用性を実装するには、複数のフロントエンドサーバーをプールに展開し、SQL サーバーをミラーリングする必要があります。

Advanced Edition 展開では、異なる役割を持つ複数のサーバーを作成できます。

Skype for Business 2015 アプリケーションの主なコンポーネントは次のとおりです。

- フロントエンドサーバー
- エッジサーバー
- Director サーバー
- データベース（SQL）サーバー

フロントエンドサーバー:

Skype for Business アプリケーションでは、フロントエンドサーバーは、ネットワーク内の中核的なサーバーです。これは、ユーザー認証、登録、プレゼンス、アドレス帳、音声またはビデオ（Audio/Video：A/V）会議、アプリケーション共有、インスタントメッセージング、および Web 会議のためのリンクとサービスを提供します。Skype for Business 2015 エンタープライズ版を展開する場合、トポロジは通常、少なくとも 2 つのフロントエンドサーバーの負荷分散は、Skype for Business データベースを保持する SQL Server インスタンスをホストするデータベースサーバーとフロントエンドプールで構成されます。

エッジサーバー:

Skype for Business 用のエッジサーバーの展開は、外部ユーザーがログインしていない場合に必要です

内部ユーザーとやり取りできるようにする必要がある場合です。これらの外部ユーザーは、認証された匿名リモートユーザー、フェデレーションパートナー、またはその他のモバイルクライアントにすることができます。

ビジネスエッジサーバーの Skype の役割の 4 種類があります。

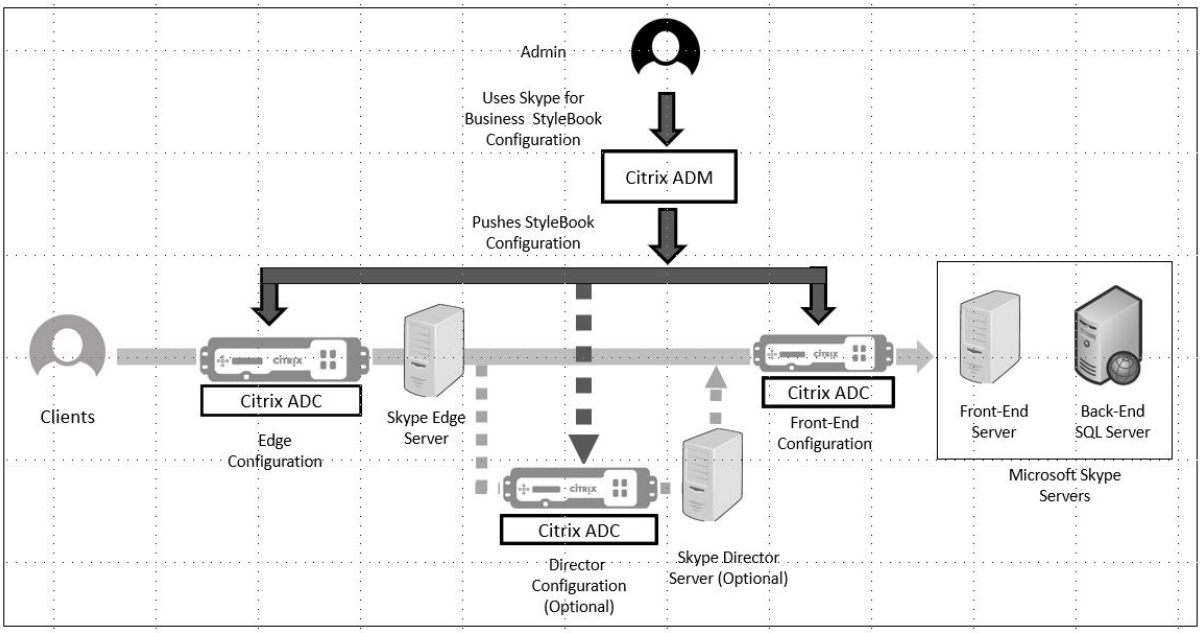
- Access Edge は、SIP トラフィックを処理し、外部接続を認証し、リモート接続を許可し、フェデレーション接続を許可します。
- Web Conferencing。これは、データ会議パケットを処理し、外部ユーザーに Skype for Business へのアクセスを許可します。
- A/V Conferencing。これは、A/V 会議パケットを処理し、音声とビデオ、アプリ共有、およびファイル転送の機能を外部ユーザーにも使用できるようにします。
- XMPP Proxy。これは、XMPP パケットを処理し、XMPP ベースのサーバーまたはクライアントに Skype for Business への接続を許可します。

ディレクターサーバー:

Skype for Business 2015 の Director サーバーの主な機能は、エンドポイントを認証し、ユーザーをアカウントを含むプールに「ダイレクト」することです。Skype for Business 2015 では、Director はスタンドアロンサーバー上で完全に専用の特定の役割ですが、オプションのサーバーです。これにより、構成の展開や削除がより簡単になることで、セキュリティが促進されます。

Director は、複数のプールが存在する場合に最も便利です。これは、エンドポイントを認証するための単一の連絡先を提供するためです。また、リモートユーザーについては、Director はエッジプールとフロントエンドプールとの間の追加のホップの役割を果たし、それによって攻撃に対する保護が強化されます。

次の図は、ネットワーク内の Skype サーバーの展開を示しています。



エンタープライズでの **Citrix ADC** インスタンスの構成

次の表は、以下の手順に含まれるサンプル構成で使用されている IP アドレスの一覧です。

Skype for Business Servers	仮想 IP アドレス	サーバー IP アドレス	Citrix ADC インスタンス
エッジサーバー	外部 VIP - 192.20.20.20	192.20.21; 192.20.22	102.29.141
	内部 VIP - 10.10.10.20	10.10.10.21; 10.10.10.22	
フロントエンド・サーバー	10.10.10.10	10.10.10.11; 10.10.12	10.102.29.60
ディレクターサーバー	10.10.10.30	10.10.10.31; 10.10.10.32	10.102.29.93

フロントエンドサーバーを構成するには

1. Citrix Application Delivery Management（ADM）で、［アプリケーション］>［構成］の順に選択し、［新規作成］をクリックします。［スタイルブックの選択］ページには、Citrix ADM で使用可能なすべてのスタイルブックが表示されます。下にスクロールして、**Microfost Skype for Business 2015** のスタイルブックを選択します。StyleBook がユーザーインターフェイスページとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。
2. [エッジサーバー] セクションで、ネットワーク内のすべてのエッジサーバーの次の仮想 IP (VIP) アドレスと IP アドレスを入力します。
   a) アクセスエッジ、Web 会議エッジ、および音声ビデオエッジに使用されるエッジサーバーの外部 VIP アドレスと IP アドレス。
   b) 内部ネットワークに接続されるエッジサーバーの内部 VIP アドレスと IP アドレス。
   c) ネットワーク内の 2 つの外部エッジサーバーと 2 つの内部エッジサーバー
3. [フロントエンドサーバー] セクションで、Skype for Business フロントエンドサーバー用に作成する仮想フロントエンドサーバー (VIP) の IP アドレスを入力します。また、ネットワーク内のすべての Skype for Business フロントエンドサーバーの IP アドレスを入力します。
4. [ディレクターサーバー] セクションで、Skype for Business アプリケーション用に作成される Director サーバーの仮想 IP アドレス (VIP) を入力します。また、ネットワーク内のすべての Skype for Business Director サーバーの IP アドレスを入力します。高可用性のためには、少なくとも 2 台の Director サーバーを作成します。
5. ［詳細設定］セクションには、3 つの Skype サーバーの Citrix ADC インスタンスに構成されているすべてのデフォルトポートが表示されます。

次の表に、すべてのデフォルトポートとプロトコルのリストを示します。

ラベル	ポート	プロトコル	説明
HTTP Port	80	HTTP	HTTPS が使用されないときに、フロントエンドサーバーから Web ファームの完全修飾ドメイン名（Fully Qualified Domain Name: FQDN）への通信のために使用されます。
HTTPS ポート	443	HTTPS	フロントエンドサーバーから Web ファームの FQDN への通信のために使用されます。
内部ポートの自動検出	4443	HTTPS	HTTPS (リバースプロキシからの) および HTTPS フロントエンドプール間通信 (自動検出サインイン用)
RPC Port	135	DCOM およびリモートプロシージャコール（Remote Procedure Call：RPC）	ユーザーの移動、ユーザーレプリケーターの同期、アドレス帳の同期など、DCOM ベースの操作のために使用されます。
SIP Port	5061	TCP（TLS）	すべての内部 SIP 通信のためにフロントエンドサーバーによって使用されます。
SIP Focus Port	444	HTTPS、TCP	Focus（Skype 会議状態を管理するコンポーネント）と個々のサーバーとの間の HTTPS 通信のために使用されます。
SIP Group Port	5071	TCP	応答グループアプリケーションの受信 SIP 要求のために使用されます。

ラベル	ポート	プロトコル	説明
SIP AppSharing Port	5065	TCP	アプリケーション共有の受信 SIP リスニング要求のために使用されます。
SIP Attendant Port	5072	TCP	出席者の受信 SIP 要求のために使用されます（つまり、ダイヤルイン会議用）。
SIP Conf Announcement Port	5073	TCP	Skype for Business サーバーの会議お知らせサービスの受信 SIP 要求のために使用されます（つまり、ダイヤルイン会議用）。
SIP CallPark Port	5075	TCP	CallPark アプリケーションの受信 SIP 要求のために使用されます。
SIP Call Admission Port	448	TCP	Skype for Business サーバーの帯域幅ポリシーサービスによる通話受付管理のために使用されます。
SIP Call Admission TURN Port	5080	TCP	音声/ビデオエッジ TURN トラフィックの帯域幅ポリシーサービスによる通話受付管理のために使用されます。
SIP Audio Test Port	5076	TCP	音声テストサービスの受信 SIP 要求のために使用されます。

ラベル	ポート	プロトコル	説明
HTTPS External Port	443	HTTPS	内部 Web 会議へのリモートユーザーアクセスのための SIP/TLS 通信用、および内部メディアおよび A/V セッションにアクセスするための STUN/TCP 送受信メディア通信用の外部ポートとして使用されます。
HTTPS Internal Port	443	HTTPS	内部 Web 会議へのリモートユーザーアクセスのための SIP/TLS 通信用、および内部メディアおよび A/V セッションにアクセスするための STUN/TCP 送受信メディア通信用の内部ポートとして使用されます。
SIP External Remote Access Port	5061	TCP	リモートユーザーアクセスまたはフェデレーションのための SIP/MTLS 通信用の外部ポートとして使用されます。
SIP Internal Remote Access Port	5061	TCP	リモートユーザーアクセスまたはフェデレーションのための SIP/MTLS 通信用の内部ポートとして使用されます。
SIP External STUN UDP Port	3478	UDP	STUN/UDP 送受信メディア通信のための外部ポートとして使用されます。
SIP Internal STUN UDP Port	3478	UDP	STUN/UDP 送受信メディア通信のための内部ポートとして使用されます。

ラベル	ポート	プロトコル	説明
SIP Internal IM Port	5062		内部ファイアウォールを通過して送信方向に流れる IM 通信の SIP/MTLS 認証のための内部ポートとして使用されます。
HTTP Port	80	TCP	Director から Web ファームの FQDN への初期通信のために使用されます。
HTTPS ポート	443	HTTPS	Director から Web ファームの FQDN への通信のために使用されます。
内部ポートの自動検出	4443	HTTPS	自動検出サインイン用の HTTPS (リバースプロキシからの) および HTTPS Director プール間通信に使用されます。
SIP Internal Port	5061	TCP	サーバー間の通信とクライアント接続のために使用されます。

1. [ターゲットインスタンス] セクションで、3 つの Skype for Business サーバーを展開する 3 つの異なる Citrix ADC インスタンスを選択します。

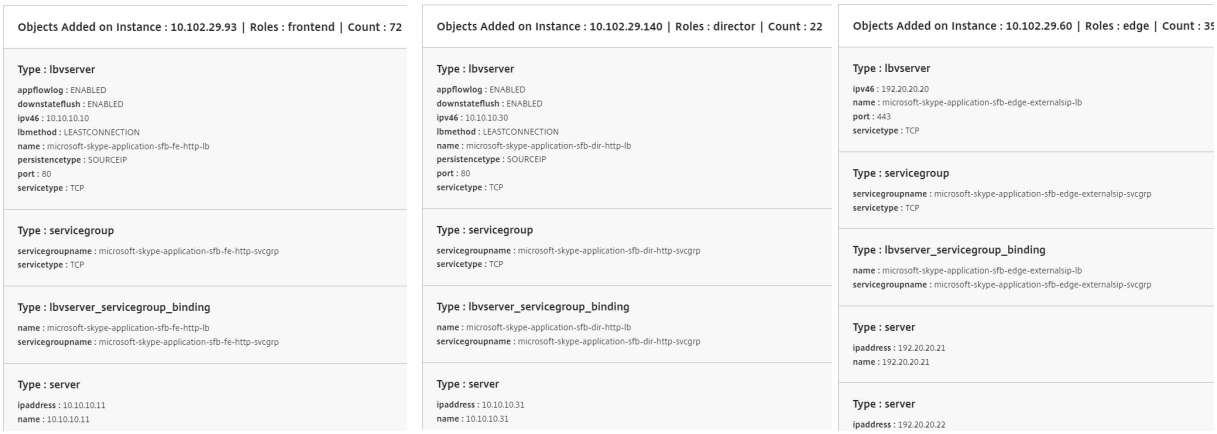
   > 注
   >
   > 更新アイコンをクリックして、Citrix ADM で最近検出された Citrix ADC インスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。

2. ［作成］をクリックして、選択した Citrix ADC インスタンスで構成を作成します。

   > ヒント
   >
   > インスタンスで実際の構成を実行する前に、［**Dry Run** ］を選択して、ターゲットインスタンスに作成する必要がある構成オブジェクトを確認することをお勧めします。

構成が正常に作成されると、StyleBook により、25 台の負荷分散仮想サーバーが作成されます。つまり、ポートごとに、1 台の負荷分散仮想サーバーが 1 つのサービスグループとともに定義されます。そのサービスグループは、その負荷分散仮想サーバーにバインドされています。また、その構成では、フロントエンドサーバーがサービスグループのメンバーとして追加され、それらがそのサービスグループにバインドされます。作成されたサービスグループメンバーの数は、作成されたフロントエンドサーバーの数と等しくなります。

次の図は、各サーバーで作成されるオブジェクトを示しています。



Microsoft Exchange StyleBook

May 7, 2021

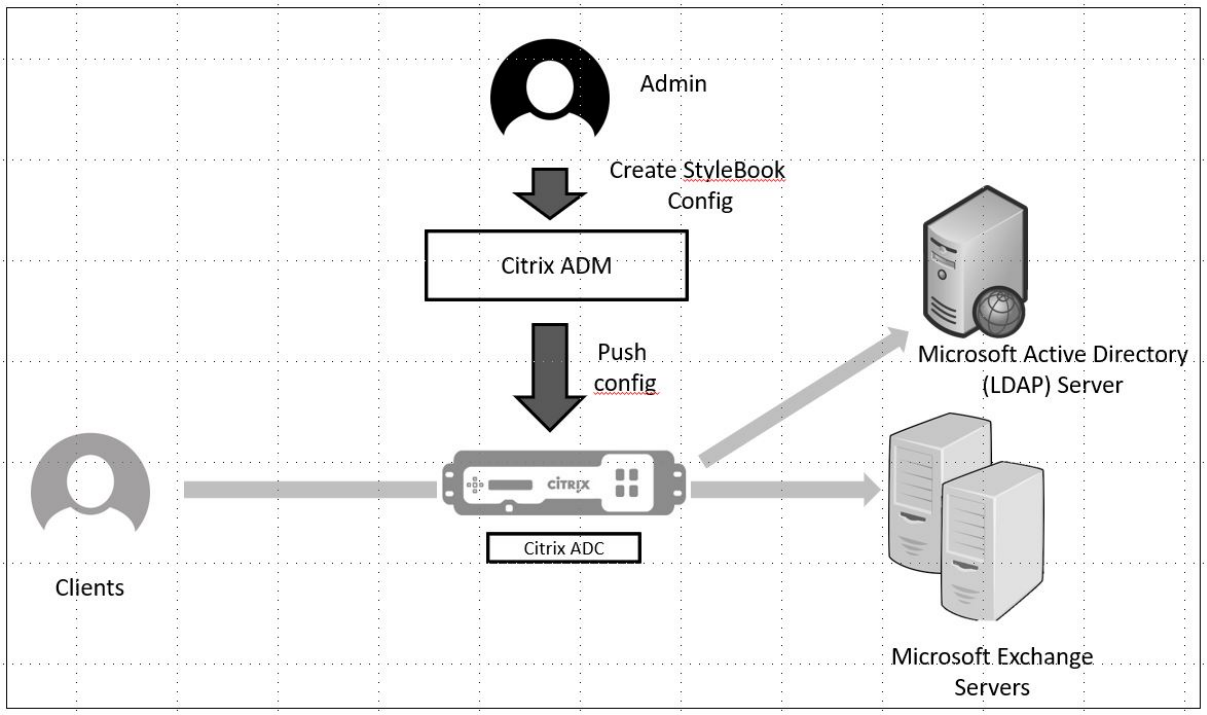
Microsoft Exchange 2016 スタイルブックを使用して、ネットワーク内の Microsoft Exchange 2016 エンタープライズアプリケーションを最適化してセキュリティ保護する Citrix ADC 構成を展開できます。Microsoft Exchange 2016 は、従業員やその他の利害関係者にメール、個人情報管理、およびメッセージングのサービスを提供するための主要なエンタープライズアプリケーションです。

Microsoft Exchange スタイルブックを使用して構成された **Citrix ADC** 機能

Microsoft Exchange 2016 StyleBook は、Microsoft Exchange 2016 サーバーの次の Citrix ADC 機能を有効化および構成します。

- 負荷分散 - 複数の Exchange サーバーを負荷分散できる、基本的な負荷分散です。
- コンテンツスイッチ - シングル IP アクセス、および正しい負荷分散仮想サーバーへのクエリのリダイレクトができるようになるコンテンツスイッチです。
- 書き換え - ユーザーを安全なページにリダイレクトします。
- SSL オフロード: SSL 処理を Citrix ADC にオフロードするため、Exchange サーバーの負荷が軽減されます。

次の図は、ネットワーク内の Exchange サーバーの展開を示しています。



前提条件

- 証明書ベースの認証の場合は、ネットワーク設定に含まれているアドレス可能なすべてのホストに、IP アドレスのみでなく解決できるドメイン名が必要となります。
- 必ず Microsoft Exchange 2016 サーバーの SIP ポートにアクセスできるようにしてください。

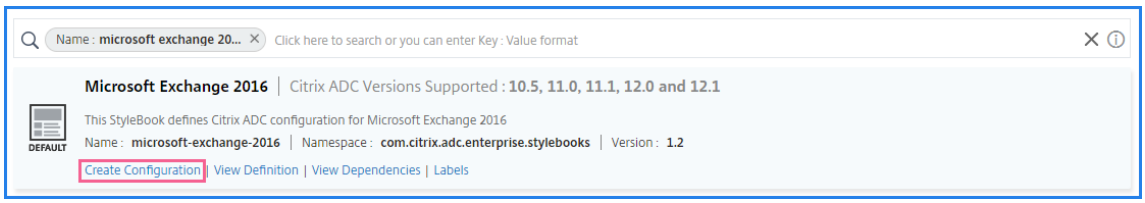
Microsoft Exchange スタイルブックの構成

企業内の Microsoft Exchange スタイルブックを構成して、Citrix ADC 構成を展開します。

Exchange アプリケーションを構成するには、次の手順に従います

1. Citrix ADM で、［アプリケーション］>［スタイルブック］に移動します。
2. **Microsoft Exchange 2016** スタイルブックを検索し、[構成の作成] をクリックします。

   StyleBook がユーザーインターフェイスフォームとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。



3. 以下のパラメーターに対して詳細を入力します。

   - **Exchange** アプリケーション名 -ネットワーク内の Microsoft Exchange アプリケーションの名前
   - **Exchange VIP** : Microsoft Exchange アプリケーションに対するクライアント要求を受信する Citrix ADC 上の仮想 IP アドレス
   - **Exchange Server** IP：ネットワーク内のすべての Exchange サーバの IP アドレス。

     IP アドレスをさらに追加する場合は、プラス（**+**）アイコンをクリックします。通常は、ネットワーク内で 2 つの Exchange サーバーが構成されます。

4. [**Exchange** 証明書］セクションで、Citrix ADM に交換証明書をアップロードします。証明書とキーファイルの両方の名前を入力し、ローカルストレージからアップロードします。キーファイルを暗号化するための秘密キーパスワードも指定できます。

   > 注**:**
   >
   > 証明書ファイルが「.pem」または「.der」形式であることを確認します。Citrix ADM は、他の形式のファイルを拒否します。

   証明書の有効期限の詳細または詳細設定を指定する場合は、[証明書の詳細設定] を選択します。

5. **Exchange Active Directory** 認証の構成セクションで、データを入力して AD 設定を構成します。

   - **Active Directory** 認証 **VIP** -Citrix ADC アプライアンス上で AD（LDAP）仮想サーバーを作成および構成するために使用される仮想 IP アドレス。
   - **Active Directory** サーバー **IP** -Active Directory ドメインコントローラの IP アドレス。
   - **Active Directory** ベース文字列 -Active Directory 内の LDAP ベース文字列。たとえば、CN=Users,DC=CTXNSSFB,DC=COM などです。
   - **Active Directory LDAP** バインド識別名 **(DN)** -LDAP バインド識別名 (DN) は、このオブジェクトを LDAP サーバー (AD) にバインドするために使用されます。たとえば、「cn=Administrator,cn=Users,dc=acme,dc=com」などです。
   - **Active Directory LDAP** バインド識別名 **(DN)** パスワード -LDAP バインド識別名 (DN) は AD 認証のパスワードです。
   - **Active Directory** ユーザー名属性 -ユーザー名の AD 属性。Citrix ADC は、LDAP 属性を使用して外部の Active Directory y サーバーを照会します。たとえば、「samAccountName」
   - **Active Directory** グループ属性名 -LDAP サーバ上で構成されている LDAP グループ属性名。たとえば、LDAP のグループ属性には「memberOf」を指定します。
   - **Active Directory** サブ属性名 -LDAP サーバーで構成された LDAP サブ属性名。たとえば、LDAP のサブ属性には「cn」を指定します。
   - **Active Directory** 認証ドメイン -認証に使用される AD/LDAP ドメイン名。たとえば、ctxnssfb.com などです。

6. ［ターゲットインスタンス］セクションで、この Exchange 構成を展開する Citrix ADC インスタンスを選択します。

   > 注
   >
   > 最近検出された Citrix ADC インスタンスを表示する場合は、更新アイコンをクリックします。

7. ［作成］をクリックして、構成ファイルを作成し、選択した Citrix ADC インスタンスで構成を実行します。

   インスタンスで実際の構成を実行する前に、ターゲットインスタンスに作成された構成オブジェクトを確認するために **[Dry Run**] を選択することをお勧めします。

構成が正常に作成されると、StyleBook はコンテンツスイッチング仮想サーバー、5 つの負荷分散仮想サーバー、1 つの LDAP 認証仮想サーバーにバインドされた 1 つの LDAP ポリシーを作成します。また、対応するサービスグループが作成され、負荷分散仮想サーバーにバインドされます。

Microsoft SharePoint StyleBook

May 7, 2021

Microsoft SharePoint 2016 は、主にドキュメント管理機能とストレージシステムを提供する、主要なエンタープライズアプリケーションです。高度に構成可能であり、すべての主要 Web ブラウザーでサポートされています。

Microsoft SharePoint 2016 スタイルブックを使用して、ネットワーク内の Microsoft SharePoint 2016 エンタープライズアプリケーションを最適化してセキュリティ保護する Citrix ADC 構成を展開できます。

前提条件

- Microsoft SharePoint 2016
- Citrix Application Delivery Management（ADM）、バージョン 12.0 以降
- Citrix ADC、バージョン 10.5 以降

Microsoft SharePoint 2016 スタイルブックによって構成される **Citrix ADC** の機能

Microsoft SharePoint 2016 スタイルブックを使用して、Microsoft SharePoint 2016 の次の Citrix ADC 機能を有効にして構成できます。

- 負荷分散
- コンテンツスイッチ
- レスポンダー
- 書き換え
- 圧縮
- 統合キャッシュ

負荷分散

Citrix ADC 負荷分散は、バックエンド SharePoint サーバーに要求を均等に分散します。バックエンドサーバーをインテリジェントに監視して、誤動作しているサーバーに要求を送信することを防ぎます。

SharePoint 用 StyleBook では、12 台の負荷分散仮想サーバーが構成され、各仮想サーバーは、ドキュメント、画像、オーディオ、ビデオ、およびその他のファイルタイプなど、特定の種類のコンテンツの負荷分散要求専用となります。

Citrix ADM は、SSL ベースの LB 仮想サーバーを構成することにより、SharePoint アプリケーションの SSL モードをサポートするようになりました。フロントエンドプロトコルとして SSL を選択してください。仮想ポートは、デフォルトで 443 に設定されています。

コンテンツの切り替え

コンテンツスイッチ機能は、要求された特定種類の SharePoint コンテンツ（たとえば、ドキュメント、画像、およびオーディオまたはビデオファイル）に基づいて複数の負荷分散仮想サーバーにわたりクライアント要求を分散するために使用されます。コンテンツスイッチモジュールにより、受信トラフィックが、その種類のコンテンツを処理できる最適な負荷分散仮想サーバーに送られます。それにより、さまざまな最適化ポリシーをさまざまな種類のトラフィックに適用できます。たとえば、テキストドキュメントよりもさまざまな圧縮ポリシーやキャッシュポリシーをビデオに使用できます。

レスポンダー

Citrix ADC インスタンスのレスポンダー機能を使用して、ユーザーを HTTP から HTTPS にシームレスにリダイレクトできます。レスポンダーは、カスタマイズされたエラーページを提供するように構成することもできます。Responder ポリシーは、アクションを実行する必要がある要求（トラフィック）を決定し、各ポリシーを負荷分散仮想サーバーにバインドします。SharePoint 用 StyleBook には、ユーザーを HTTP の URL から HTTPS の URL にリダイレクトする構成が含まれています。

書き換え

書き換えモジュールは、要求/応答のヘッダー、URL、またはコンテンツを即座に変更するために使用されます。このモジュールは、トラフィック処理でインラインで動作します。それにより、特定のユースケースに応じてトラフィックフローを変更できます。たとえば、書き換えにより、Web サイトのサーバーについて不要な情報が公開されることなく、要求されたコンテンツにアクセスできるようになります。

SharePoint 用 StyleBook では、書き換え機能は、ユーザーの要求から不要なヘッダーを削除するために使用されます。

圧縮

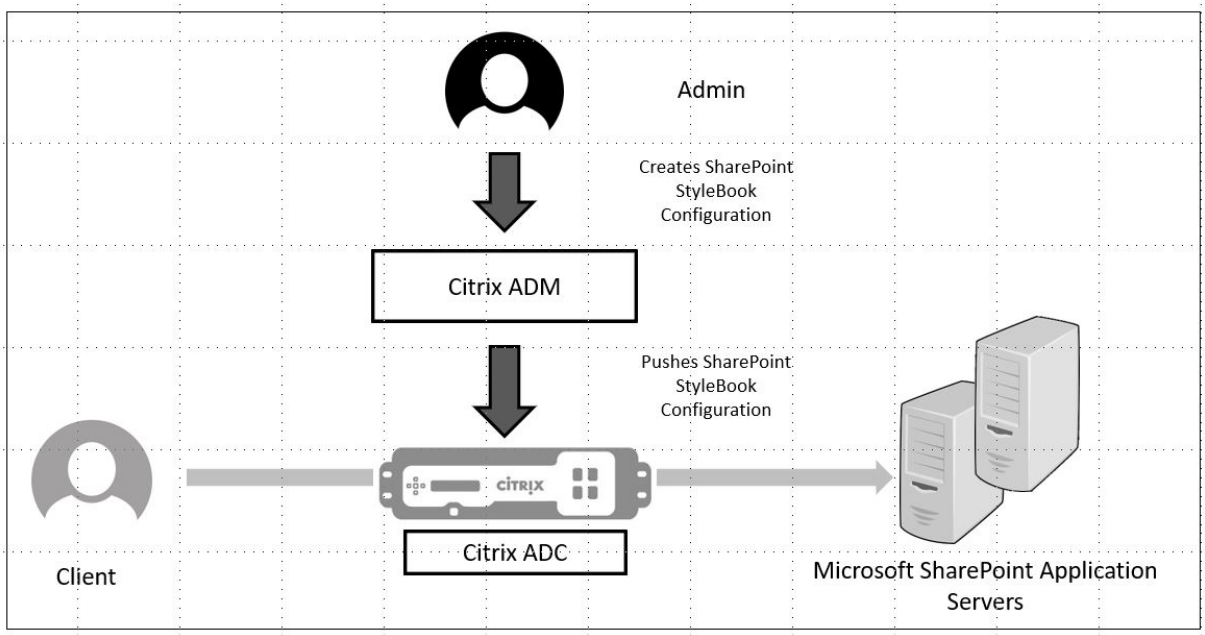
Citrix ADC 圧縮エンジンは、圧縮可能なコンテンツを識別して圧縮します。このプロセスにより、データ転送時間が短縮され、クライアントに対するネットワーク帯域幅要件が減少するとともに、SharePoint コンテンツサーバー上の CPU サイクルが節約されます。Citrix ADC インスタンスは、静的データと動的に生成されたデータの両方を圧縮できます。GZIP または DEFLATE 圧縮アルゴリズムが適用されることで、無関係で反復的な情報がサーバー応答から削除され、より簡潔で効率的な形式で元の情報が表されます。クライアントのブラウザーのデータ展開機能は、サポートされているアルゴリズム（GZIP、DEFLATE、またはこれら両方）によって異なります。

Citrix ADC インスタンスは、HTML、XML、プレーンテキスト、カスケードスタイルシート（CSS）、および Microsoft Office ドキュメントでテキストを圧縮するように構成されますが、GIF または JPG 形式の画像は圧縮されません。トラフィック圧縮の主な利点には、帯域幅コストの減少、WAN（Wide Area Network：ワイドエリアネットワーク）の遅延の減少、サーバーパフォーマンスの向上があります。

統合されたキャッシング

Citrix ADC インメモリキャッシュは、頻繁に要求されるコンテンツをユーザーにすばやく配信するために、SharePoint オブジェクトを格納できます。キャッシュされるコンテンツには、ダウンロードしたドキュメントや、オーディオ、ビデオ、および画像ファイルなどがあります。

次の図は、Citrix ADM を使用して SharePoint スタイルブック構成を展開する Citrix ADC インスタンスによるネットワークフロントエンドでの SharePoint サーバーの展開を示しています。



SharePoint スタイルブックの構成を展開する

次のタスクは、ビジネスネットワークに Microsoft SharePoint 2016 StyleBook を展開する際に役立ちます。

Microsoft SharePoint 2016 スタイルブックを展開するには、次の操作を行います。

1. Citrix ADM で、［アプリケーション］>［管理］>［構成］の順に選択し、［新規作成］をクリックします。

   ［スタイルブックの選択］ページには、Citrix ADM で使用可能なすべてのスタイルブックが表示されます。

2. 下にスクロールして、**Microsoft SharePoint 2016** スタイルブックを選択します。

   > 注:
   >
   > Citrix ADM で、「アプリケーション」>「構成」>「**StyleBooks**」の順に選択します。下にスクロールして、**Microsoft SharePoint 2016** スタイルブックを見つけます。[**Microsoft SharePoint 2016** スタイルブック] パネルで、[構成の作成] をクリックします。

   StyleBook は、この StyleBook で定義されているすべてのパラメータの値を入力できるユーザーインタフェースフォームとして開きます。

   次のパラメーターの値を入力します。

   a) **SharePoint** アプリケーション名。ネットワーク内で展開する SharePoint 構成の名前です。

   b) **SharePoint** の仮想 **IP** です。Citrix ADC インスタンスが Microsoft SharePoint アプリケーションに対するクライアント要求を受信する仮想 IP アドレス。

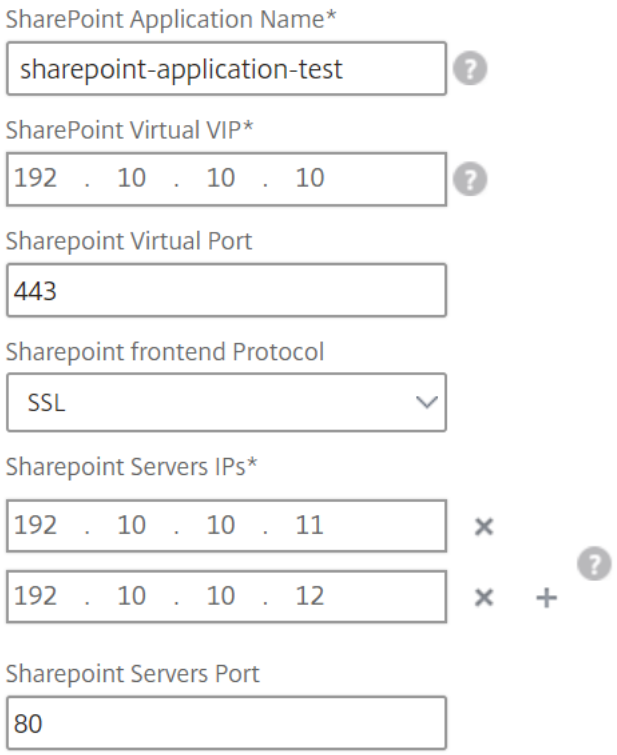
   c) **SharePoint** 仮想ポート。SharePoint アプリケーションへのアクセス時にユーザーが使用する TCP ポート

   d) **SharePoint** フロントエンドプロトコル。ドロップダウンリストから SharePoint フロントエンドプロトコルを選択します。使用可能なオプションは、HTTP または SSL です。

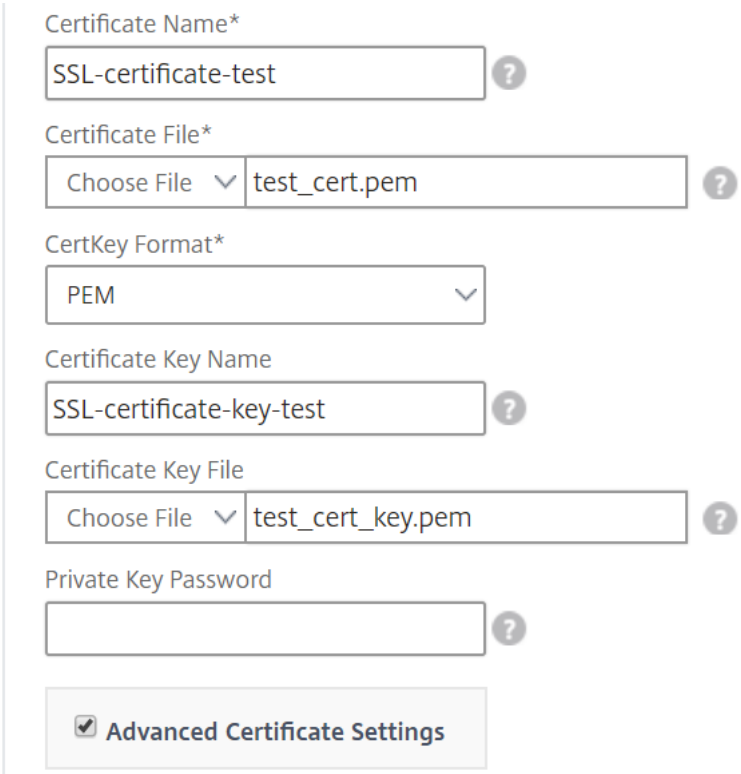
      > 注:
      >
      > SSL を選択した場合は、この StyleBook の「SharePoint の詳細設定」セクションで「書き換え構成」パラメータが有効になっていることを確認してください。

   e) **SharePoint** サーバーの **IP** です。ネットワーク内のすべての SharePoint サーバーの IP アドレス。

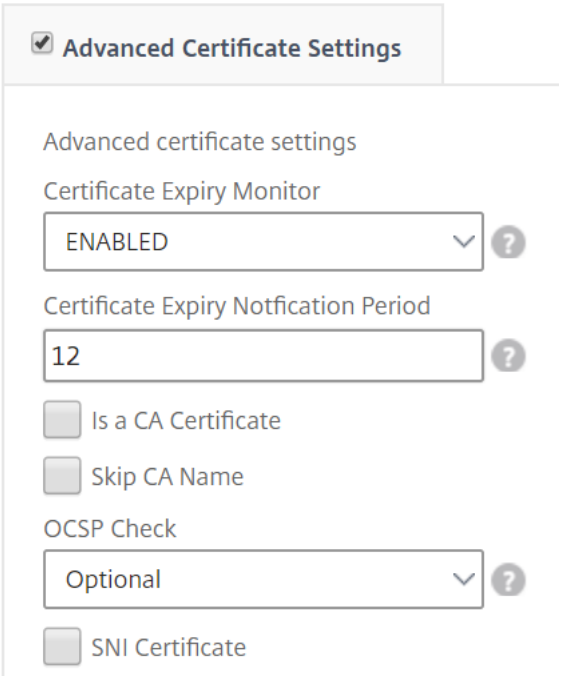
   f) **SharePoint** サーバーポート。SharePoint サーバーで使用される TCP ポート番号です。デフォルト値は、80 です。必要な場合はこの値を編集できますが、必ず Microsoft SharePoint 2016 サーバー上でこのポートにアクセスできることを確認してください。



3. [**SSL** 証明書の設定] セクションで、[+] をクリックして SSL 証明書の名前と証明書キーを入力し、ローカルストレージフォルダからそれぞれのファイルを選択します。



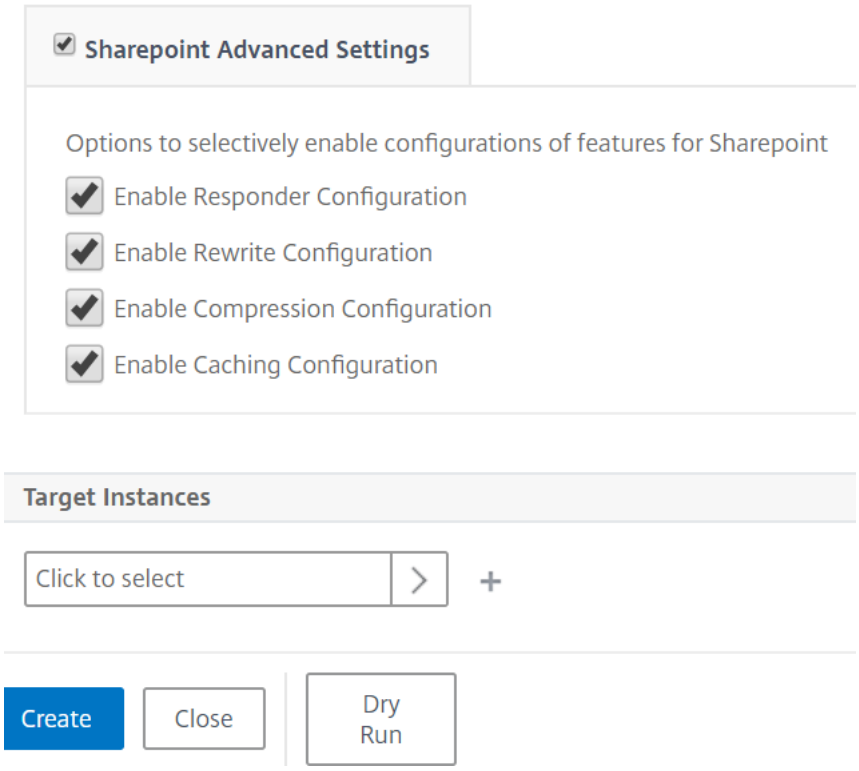
4. 必要に応じて、[証明書の詳細設定] をクリックして、SSL 証明書の有効期限の監視を有効または無効にします。証明書の有効期限の監視を有効にする場合は、証明書の有効期限が近づくと Citrix ADM がアラームを発行するように、日数を設定します。OCSP チェックをオプション機能または必須機能にするオプションもあります。



5. [SharePoint の詳細設定] セクションでは、Citrix ADC インスタンスで構成する Citrix ADC 機能を有効にできます。負荷分散機能とコンテンツスイッチ機能はインスタンス上でデフォルトで構成されますが、その他の機能（つまり、インスタンス上で構成する必要がある、レスポンダー構成、書き換え構成、圧縮構成、および統合キャッシュ構成）を選択できます。

6. [ターゲットインスタンス] をクリックし、この SharePoint 構成を展開する Citrix ADC インスタンスを選択します。[作成] をクリックして構成を作成し、選択した Citrix ADC インスタンスに構成を展開します。

> 注
>
> 更新アイコンをクリックして、Citrix ADM で最近検出された Citrix ADC インスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。



> 注:
>
> 実際の構成を実行する前に、［**Dry Run** ］を選択して、ターゲットインスタンスに作成される構成オブジェクトを確認することをお勧めします。

構成が作成され、正常に展開されると、SharePoint 用 StyleBook により、1 台のコンテンツスイッチ仮想サーバーと 12 台の負荷分散仮想サーバーが作成されます。ポリシーとサービスグループも作成され、それらが負荷分散仮想サーバーにバインドされます。作成されるポリシーは、構成パックの作成中に StyleBook で選択した機能によって異なります。

Citrix ADC インスタンスに定義されているオブジェクトの表示

構成パックが Citrix ADM で作成されると、SharePoint スタイルブックの Citrix ADC インスタンスに作成されたすべてのオブジェクトを表示できます。「アプリケーション」>「管理」>「構成」に移動し、「作成されたオブジェクトの表示」をクリックします。次の図は、作成されたオブジェクトの一部を示しています。この例では、「Citrix ADM から SharePoint スタイルブック構成を展開する」に示されている IP アドレスが指定されています。

Type : lbvserver

appflowlog : DISABLED
backuppersistencetimeout : 20
downstateflush : DISABLED
ipv46 : 0.0.0.0
lbmethod : LEASTCONNECTION
name : sharepoint application test frontpage services lb
persistencebackup : SOURCEIP
persistencetype : COOKIEINSERT
port : 0
servicetype : HTTP
timeout : 20

Type : servicegroup

cip : DISABLED
cka : YES
cmp : NO
downstateflush : DISABLED
healthmonitor : NO
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp
servicetype : HTTP
sp : ON
state : ENABLED
tcpb : NO
useproxyport : NO
usip : NO

Type : lbvserver_servicegroup_binding

name : sharepoint-application-test-frontpage-services-lb
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.11
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.12
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : csaction

name : sharepoint-application-test-cs-frontpage-services-csaction
targetlbvserver : sharepoint-application-test-frontpage-services-lb

Type : cspolicy

action : sharepoint-application-test-cs-frontpage-services-csaction
policyname : sharepoint-application-test-cs-frontpage-services-cspol
rule : HTTP.REQ.HEADER("X-Vermeer-Content-Type").EXISTS

Type : csvserver_cspolicy_binding

name : sharepoint-application-test-cs
policyname : sharepoint-application-test-cs-frontpage-services-cspol
priority : 10

Microsoft ADFS proxy StyleBook

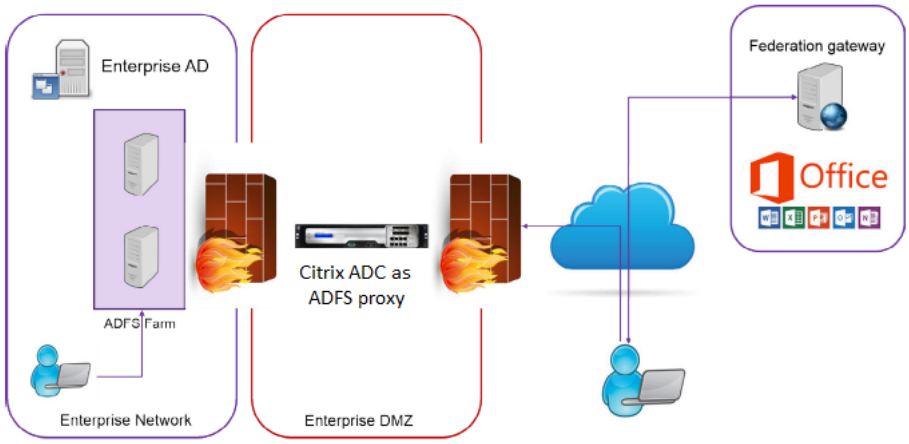
May 7, 2021

Microsoft™ ADFS プロキシは、内部フェデレーション対応リソースとクラウドリソースの両方にシングルサインオンアクセスを提供することで、重要な役割を果たします。クラウドリソースのこのような例の 1 つは Office 365 です。ADFS プロキシサーバーの目的は、インターネットからアクセスできない ADFS サーバーに要求を受信および転送することです。ADFS プロキシはリバースプロキシであり、通常は組織の境界ネットワーク (DMZ) に存在します。ADFS プロキシは、リモートユーザーの接続とアプリケーションアクセスにおいて重要な役割を果たします。

Citrix ADC には、フェデレーション ID の安全な接続、認証、および処理を可能にする正確なテクノロジーがあります。ADFS プロキシとして Citrix ADC を使用すると、DMZ に余分なコンポーネントを展開する必要がなくなります。

Citrix Application Delivery Management（ADM）の Microsoft ADFS プロキシスタイルブックを使用すると、Citrix ADC インスタンスで ADFS プロキシサーバーを構成できます。

次の図は、Citrix ADC インスタンスを ADFS プロキシサーバーとしてエンタープライズ DMZ に展開する方法を示しています。



ADFS プロキシとして Citrix ADC を使用する利点

1. 負荷分散と ADFS プロキシの両方のニーズに対応
2. 内部と外部の両方のユーザー・アクセス・シナリオをサポート
3. 事前認証のための豊富な方法をサポート
4. ユーザーにシングルサインオンエクスペリエンスを提供します。
5. アクティブプロトコルとパッシブプロトコルの両方をサポート
    a) アクティブなプロトコルアプリケーションの例としては、— Microsoft Outlook、Microsoft Skype for Business
    b) パッシブプロトコルアプリケーションの例としては、Microsoft Outlook Web アプリケーション、Web ブラウザなどがあります。

6. DMZ ベースの展開のための強化されたデバイス
7. 追加のコア Citrix ADC 機能を使用して価値を追加
    a) コンテンツスイッチ
    b) SSL オフロード
    c) 書き換え
    d) セキュリティ (Citrix ADC AAA)

アクティブなプロトコルベースのシナリオでは、Office 365 に接続して資格情報を提供できます。Microsoft フェデレーションゲートウェイは、アクティブなプロトコルクライアントに代わって (ADFS プロキシを介して) ADFS サービスにアクセスします。次に、Gateway は基本認証（401）を使用してクレデンシャルを送信します。Citrix ADC は、ADFS サービスにアクセスする前にクライアント認証を処理します。認証後、ADFS サービスは SAML トークンをフェデレーションゲートウェイに提供します。次に、フェデレーションゲートウェイはトークンを Office 365 に送信し、クライアントアクセスを提供します。

パッシブクライアントの場合、ADFS プロキシスタイルブックは Kerberos 制約付き委任 (KCD) ユーザーアカウントを作成します。KCD アカウントは、Kerberos SSO 認証が ADFS サーバーに接続するために必要です。StyleBook は、LDAP ポリシーとセッションポリシーも生成します。これらのポリシーは、パッシブ・クライアントの認証を処理する Citrix ADC AAA 仮想サーバーに後でバインドされます。

StyleBook では、Citrix ADC 上の DNS サーバーが ADFS 用に構成されていることを確認することもできます。

以下の構成セクションでは、アクティブとパッシブの両方のプロトコルベースのクライアント認証を処理するために Citrix ADC を設定する方法について説明します。

構成の詳細

次の表に、この統合を正常に展開するために必要な最低限のソフトウェアバージョンを示します。

製品	最低限必要なバージョン
Citrix ADC	11.0, アドバンス/プレミアムライセンス

次の手順は、適切な外部および内部 DNS エントリが既に作成されていることを前提としています。

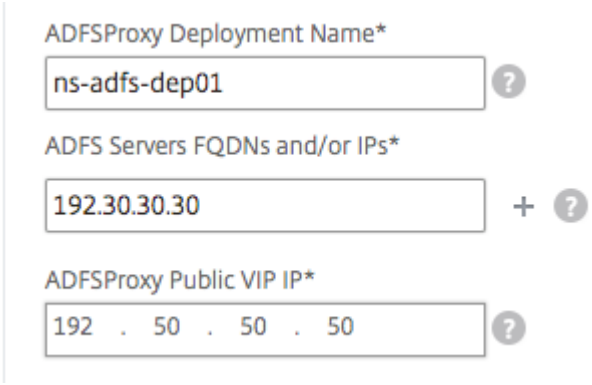
Citrix ADM から **Microsoft ADFS** プロキシのスタイルブック構成を展開する

次の手順は、Microsoft ADFS プロキシ StyleBook をビジネスネットワークに実装する際に役立ちます。

Microsoft ADFS プロキシスタイルブックを展開するには

1. Citrix ADM で、［アプリケーション］>［スタイルブック］に移動します。［スタイルブック］ページには、Citrix ADM で使用可能なすべてのスタイルブックが表示されます。

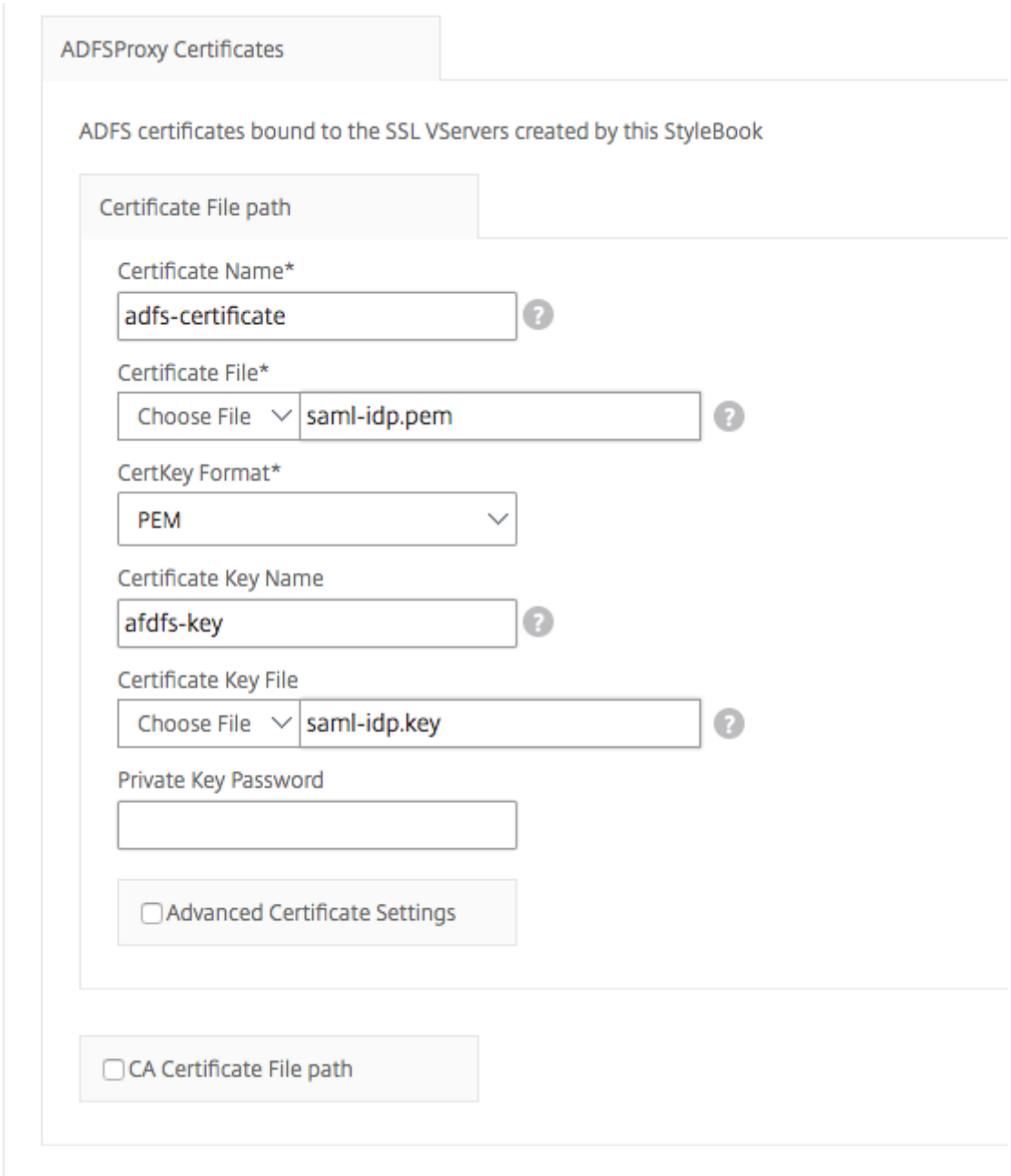
2. 下にスクロールして、**Microsoft ADFS** プロキシのスタイルブックを見つけます。[構成を作成] をクリックします。
   StyleBook がユーザーインタフェースページとして開きます。このページには、この StyleBook で定義されているすべてのパラメータの値を入力できます。
3. 次のパラメータの値を入力します。
   a) **ADFS** プロキシ展開名。ネットワークにデプロイされた ADFS プロキシ設定の名前を選択します。
   b) **ADFS** サーバー **FQDN** または **IP**。ネットワーク内のすべての ADFS サーバーの IP アドレスまたは FQDN (ドメイン名) を入力します。
   c) **ADFS** プロキシパブリック **VIP IP**。ADFS プロキシサーバーとして Citrix ADC 上のパブリック仮想 IP アドレスを入力します。



4. [**ADFS** プロキシ証明書] セクションで、SSL 証明書と証明書キーの詳細を入力します。

   この SSL 証明書は、Citrix ADC インスタンスで作成されたすべての仮想サーバーにバインドされます。

   ローカルストレージフォルダからそれぞれのファイルを選択します。また、秘密キーのパスワードを入力して、暗号化された秘密キーを.pem 形式でロードすることもできます。



[証明書の詳細設定] チェックボックスをオンにすることもできます。ここでは、証明書の有効期限通知期間などの詳細を入力したり、証明書の有効期限モニターを有効または無効にすることができます。

5. **SSL** 証明書で **Citrix ADC** に **CA** パブリック証明書をインストールする必要がある場合は、オプションで [SSL CA 証明書] チェックボックスをオンにできます。[証明書の詳細設定] セクションで [CA 証明書か] を選択していることを確認します。
6. アクティブクライアントおよびパッシブクライアントの認証を有効にします。Active Directory でユーザー認証に使用する DNS ドメイン名を入力します。その後、アクティブクライアントまたはパッシブクライアント、またはその両方に対して認証を構成できます。

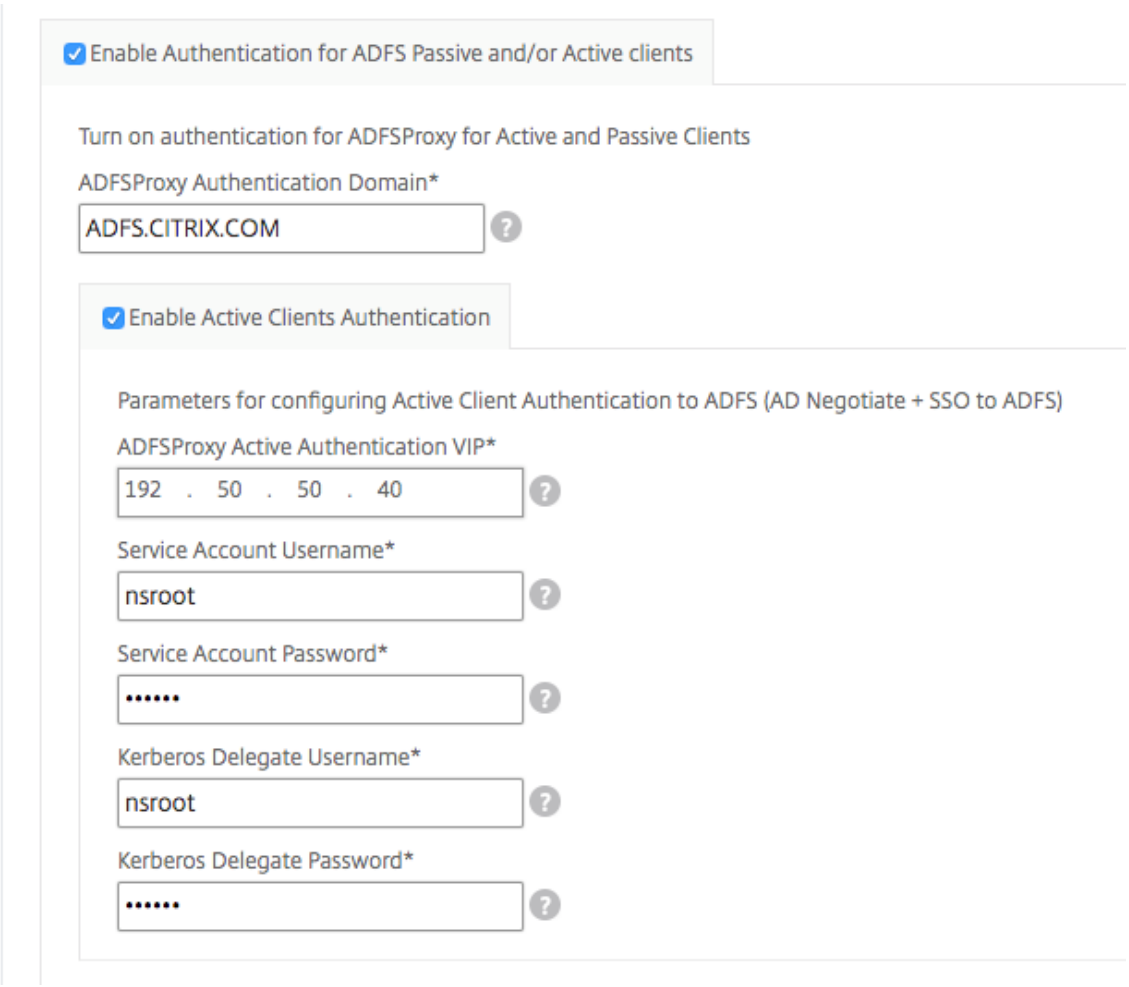
7. アクティブなクライアントの認証を有効にするには、次の詳細を入力します。

> 注:
>
> アクティブクライアントのサポートを構成することはオプションです。

a) **ADFS** プロキシアクティブ認証 **VIP**。アクティブなクライアントが認証用にリダイレクトされる Citrix ADC インスタンス上の仮想認証サーバーの仮想 IP アドレスを入力します。

b) サービスアカウントのユーザー名。Active Directory に対するユーザーを認証するために Citrix ADC が使用するサービスアカウントのユーザー名を入力します。

c) サービスアカウントパスワード。Active Directory に対するユーザーを認証するために Citrix ADC が使用するパスワードを入力します。



8. 対応するオプションを有効にし、LDAP 設定を構成して、パッシブクライアントの認証を構成します。

> 注:
>
> パッシブクライアントのサポートを構成することはオプションです。

パッシブクライアントの認証を有効にするには、次の詳細を入力します。

a) **LDAP**（**Active Directory**）ベース。認証を許可する Active Directory (AD) 内にユーザーアカウントが存在するドメインの基本ドメイン名を入力します。例：`dc=netscaler,dc=com`

b) **LDAP**（**Active Directory**）バインド **DN**。AD ツリーを参照する権限を持つドメインアカウント (構成を容易にするために電子メールアドレスを使用) を追加します。たとえば、CN= マネージャー、`dc=netscaler,dc=com`

c) **LDAP (Active Directory)** バインド **DN** パスワード。認証用のドメインアカウントのパスワードを入力します。

このセクションの値に入力する必要があるその他のフィールドは次のとおりです。

d) **LDAP** サーバ（**Active Directory**）**IP**。AD 認証が正しく機能するように、Active Directory サーバーの IP アドレスを入力します。

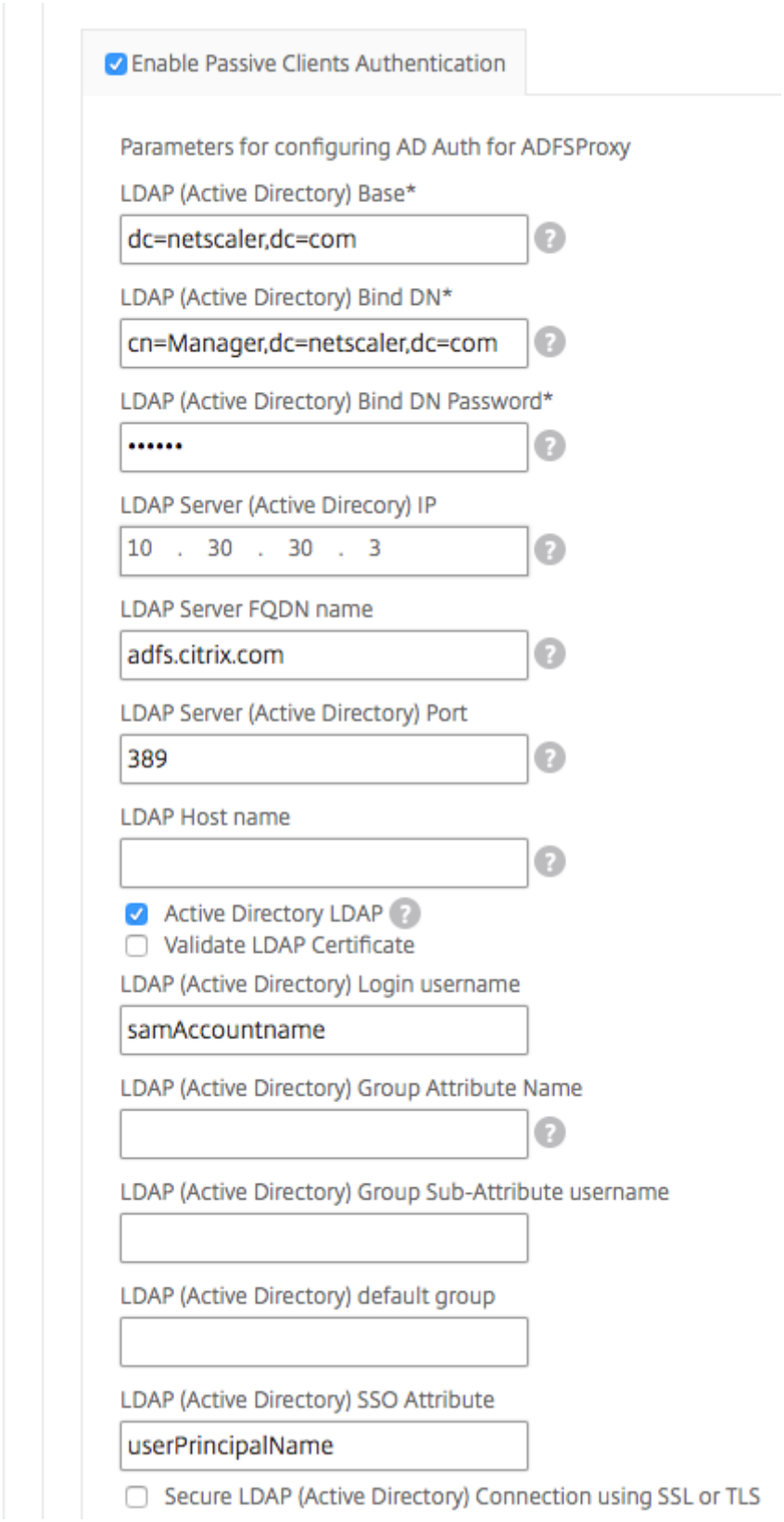
e) **LDAP** サーバの **FQDN** 名。アクティブディレクトリサーバーの FQDN 名を入力します。FQDN 名はオプションです。手順 1 のように IP アドレスまたは FQDN 名を指定します。

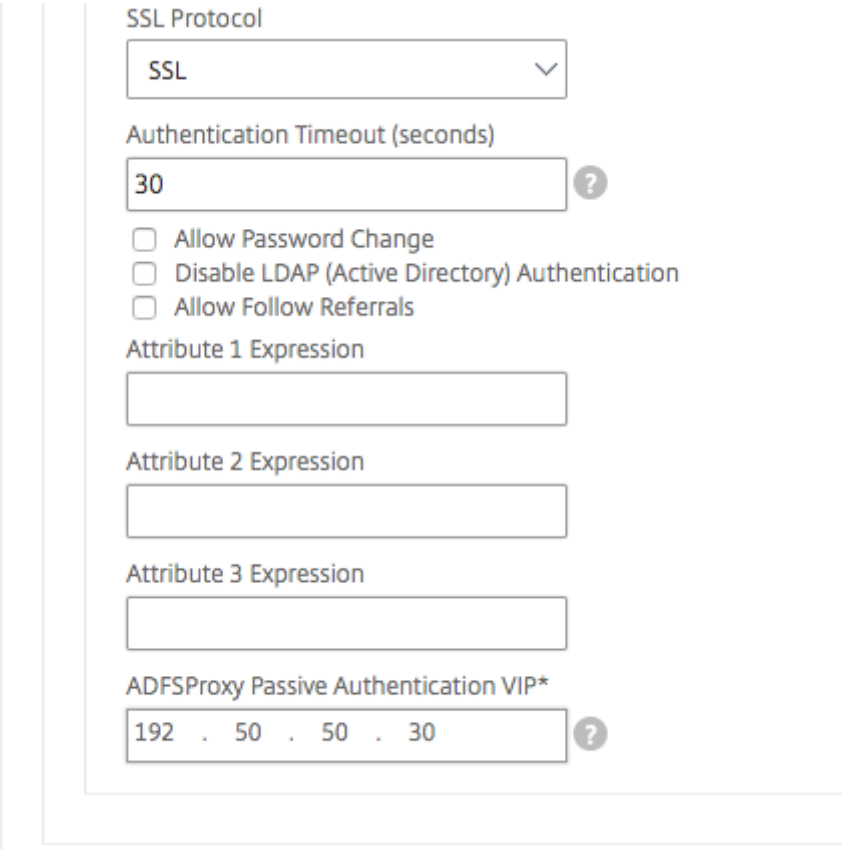
f) **LDAP** サーバの **Active Directory** ポート。デフォルトでは、LDAP プロトコルの TCP ポートと UDP ポートは 389 ですが、セキュア LDAP の TCP ポートは 636 です。

g) **LDAP**（**Active Directory**）ログインユーザ名。ユーザー名を「samAccountName」として入力します。

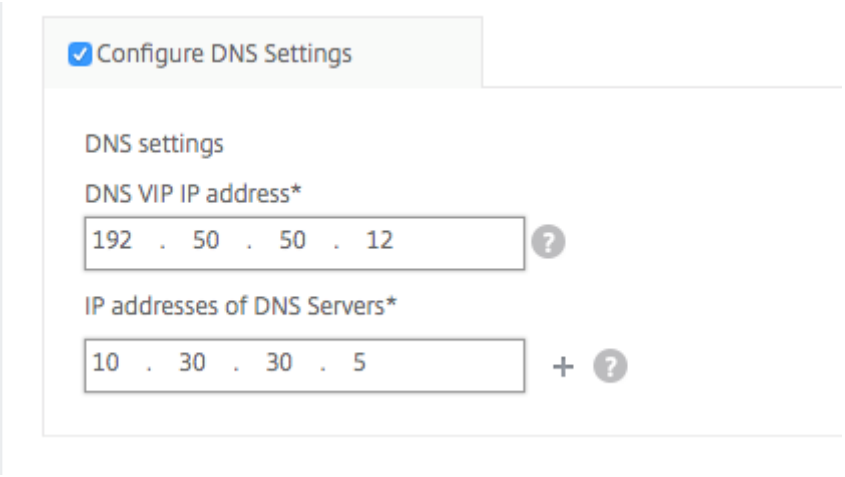
h) **ADFS** プロキシパッシブ認証 **VIP**。パッシブクライアントの ADFS プロキシ仮想サーバーの IP アドレスを入力します。

> 注:
>
> 「*」の付いたフィールドは必須です。

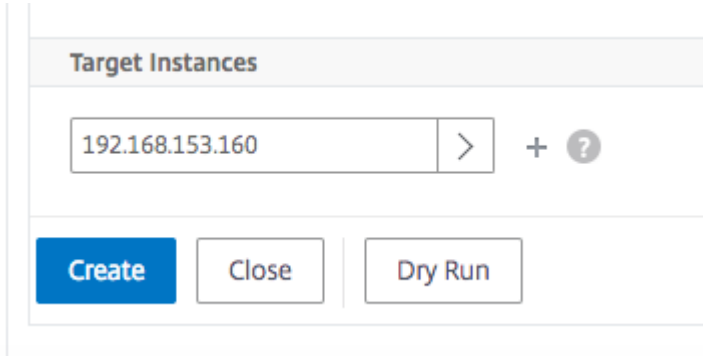




9. 必要に応じて、DNS サーバーの DNS VIP を構成することもできます。



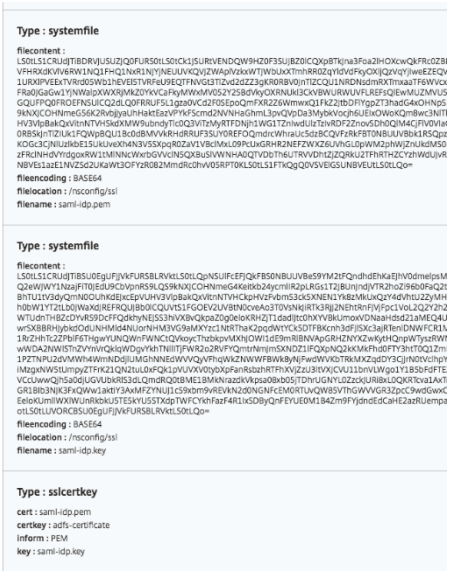
10. ［ターゲットインスタンス］をクリックし、この Microsoft ADFS プロキシ構成を展開する Citrix ADC インスタンスを選択します。［作成］をクリックして構成を作成し、選択した Citrix ADC インスタンスに構成を展開します。

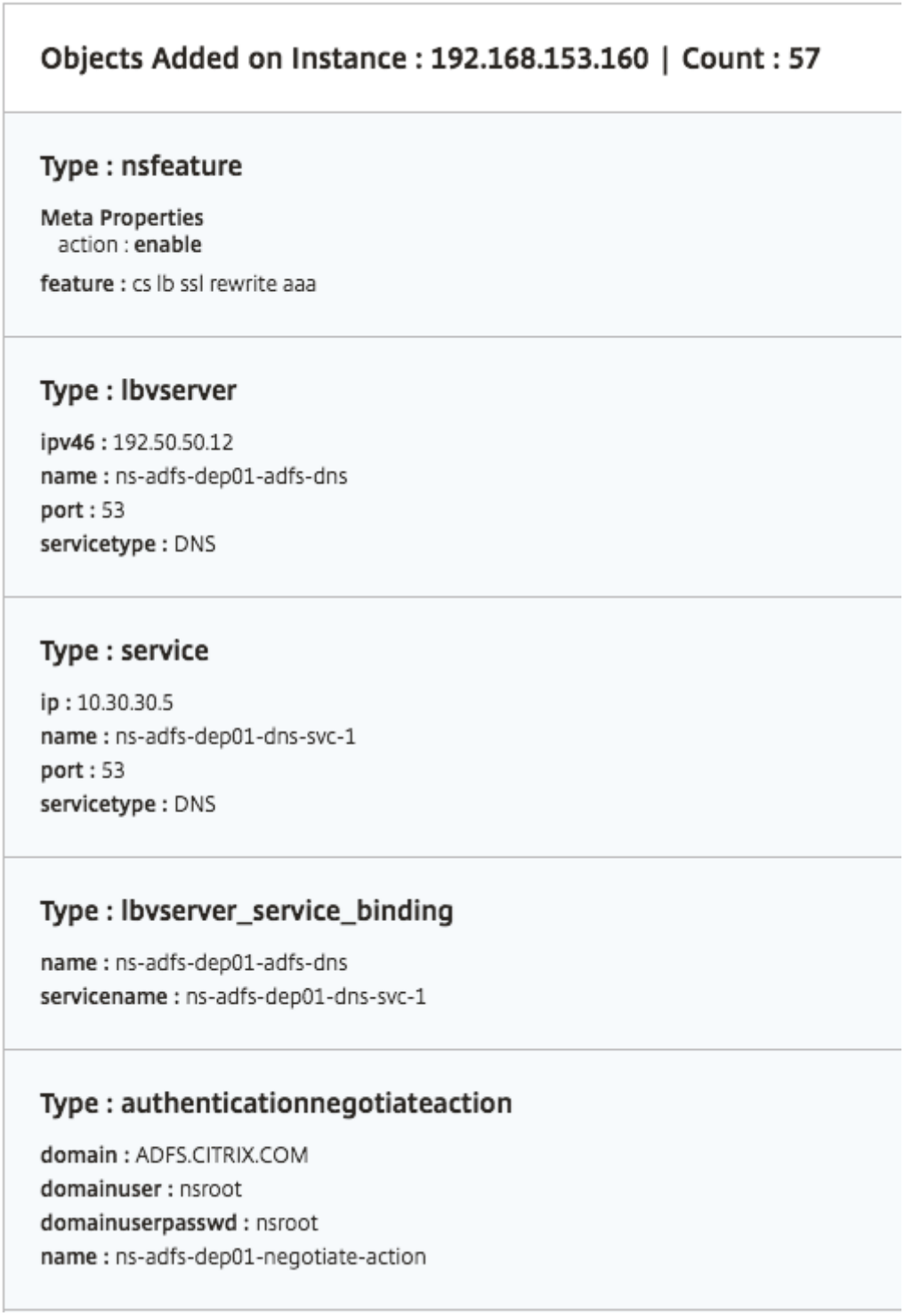


> 注:
>
> 実際の構成を実行する前に、[ドライ実行] を選択することをお勧めします。まず、StyleBook によってターゲットの Citrix ADC インスタンスに作成された構成オブジェクトを表示できます。その後、[**Create**] をクリックして、選択したインスタンスに設定をデプロイできます。

作成されたオブジェクト

ADFS プロキシ構成が Citrix ADC インスタンスに展開されると、いくつかの構成オブジェクトが作成されます。次の図は、作成されたオブジェクトのリストを示しています。





Type : authenticationpolicy

action : ns-adfs-dep01-negotiate-action
name : ns-adfs-dep01-negotiate-policy
rule : true

Type : aaakcdaccount

delegateduser : nsroot
kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
kcdpassword : nsroot
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
name : ns-adfs-dep01-adfs-auth401-tmsession-action
persistentcookie : ON
persistentcookievalidity : 3
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-auth401-tmsession-action
name : ns-adfs-dep01-adfs-auth401-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.40
maxloginattempts : 255
name : ns-adfs-dep01-adfs-auth401-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-auth401-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-negotiate-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-adfs-auth401-tmsession-policy
priority : 10

Type : authenticationldapaction

authentication : ENABLED
authtimeout : 30
followreferrals : OFF
ldapbase : dc=netscaler,dc=com
ldapbinddn : cn=Manager,dc=netscaler,dc=com
ldapbinddnpassword : nsroot
ldaploginname : samAccountname
name : ns-adfs-dep01-ldap-action
passwdchange : DISABLED
sectype : PLAINTEXT
serverip : 10.30.30.3
serverport : 389
ssonameattribute : userPrincipalName
svrtype : AD
validateservercert : NO

Type : authenticationpolicy

action : ns-adfs-dep01-ldap-action
name : ns-adfs-dep01-ldap-policy
rule : true

Type : aaakcdaccount

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
name : ns-adfs-dep01-adfs-ldap-tmsession-action
persistentcookie : OFF
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-ldap-tmsession-action
name : ns-adfs-dep01-adfs-ldap-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.30
maxloginattempts : 255
name : ns-adfs-dep01-adfs-ldap-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-ldap-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-ldap-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-adfs-ldap-tmsession-policy
priority : 10

Type : csvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-cs
port : 443
servicetype : SSL

Type : lbvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
port : 445
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : server

ipaddress : 192.30.30.30
name : 192.30.30.30

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") || HTTP.REQ.URL.CONTAINS("/federa

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
priority : 9800

Type : lbvserver

appflowlog : ENABLED
authentication : ON
authenticationhost : ADFS.CITRIX.COM
authn401 : OFF
authnvsname : ns-adfs-dep01-adfs-ldap-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
port : 446
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/ls/auth/integrated") || HTTP.REQ.URL.CONTAINS("/adfs/ls/wia")

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
priority : 9900

Type : lbvserver

appflowlog : ENABLED
authentication : OFF
authn401 : ON
authnvsname : ns-adfs-dep01-adfs-auth401-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
port : 444
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
rule : true

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
priority : 10000

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-cs

Type : rewritepolicylabel

labelname : ns-adfs-dep01-request-rewritepolicylabel
transform : HTTP_REQ

Type : rewritepolicylabel

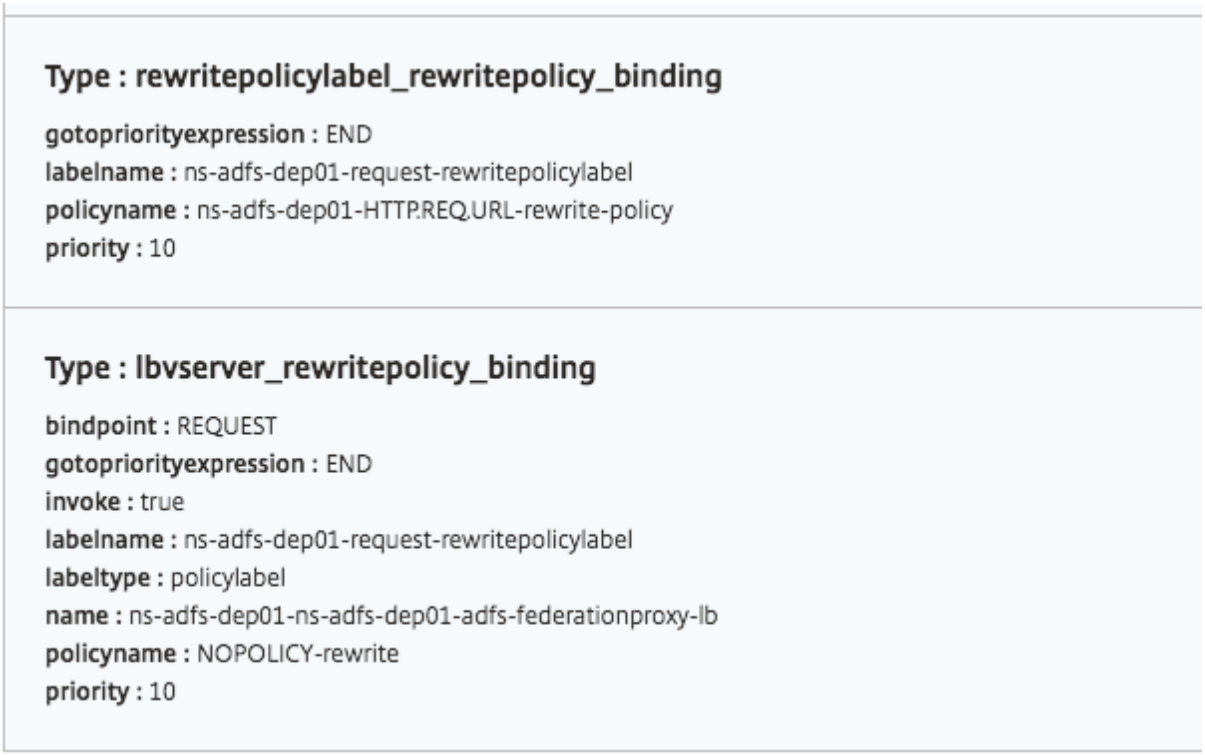
labelname : ns-adfs-dep01-response-rewritepolicylabel
transform : HTTP_RES

Type : rewriteaction

name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
stringbuilderexpr : "/adfs/services/trust/proxymex"
target : HTTP.REQ.URL
type : REPLACE

Type : rewritepolicy

action : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-policy
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") && (!HTTP.REQ.URL.CONTAINS("/trust/proxymex"))



Oracle 電子ビジネススタイルブック

May 7, 2021

Oracle E-Business Suite は、統合されたグローバルなビジネス・アプリケーションの最も包括的なスイートです。このスイートは、組織がより良い意思決定、コストの削減、パフォーマンスの向上を可能にし、次のアプリケーションで構成されています。

- ERP（エンタープライズ・リソース・プランニング）
- 顧客関係管理（CRM）
- サプライチェーン管理（SCM）

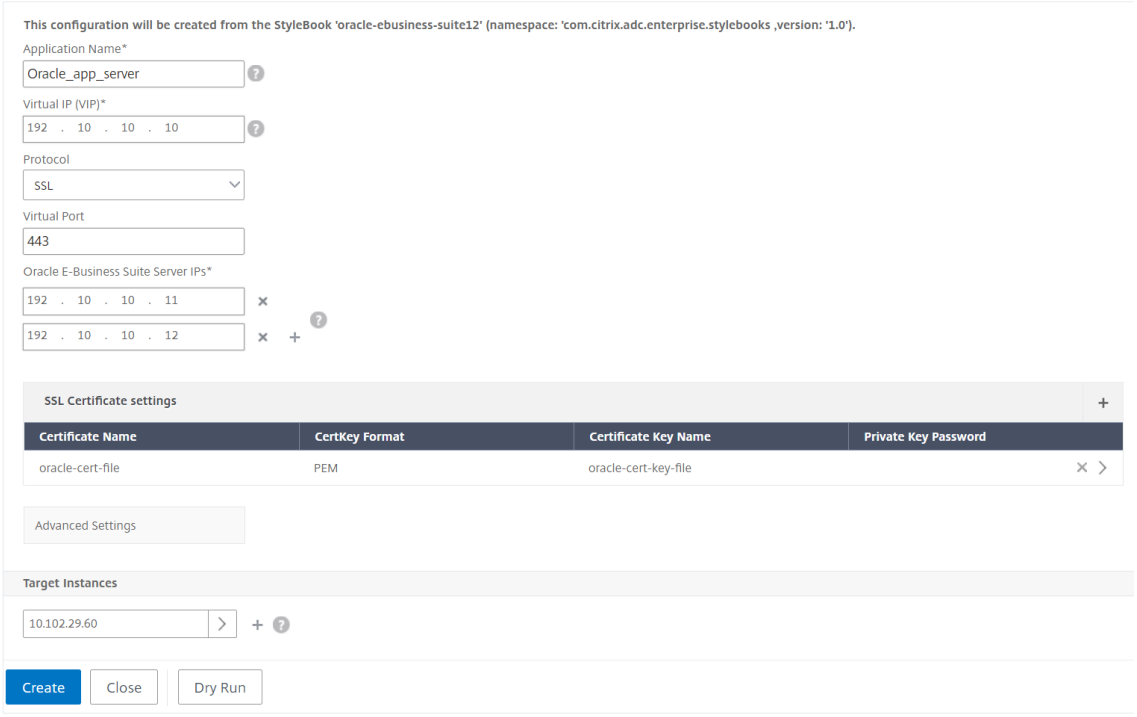
これらのコンピュータ・アプリケーションは、Oracle によって開発または買収されています。Oracle E-Business Suite 12.2 StyleBook では、選択した Citrix ADC インスタンスに構成を展開できます。

この StyleBook は、負荷分散仮想サーバー、サービスグループ、およびサービスのリストを含む負荷分散構成を作成します。また、サービスをサービスグループにバインドし、サービスグループを仮想サーバーにバインドできます。SSL を選択し、ローカルシステムから SSL ファイルとキーファイルを提供することで、暗号化された通信を選択できます。

Oracle E-ビジネス・スイート **12.2** の構成を作成する手順は、次のとおりです

1. Citrix Application Delivery Management（ADM）で、［アプリケーション］>［構成］**>**［**StyleBooks**］に移動します。［スタイルブック］ページには、Citrix ADM で使用可能なすべてのスタイルブックが表示されます。下にスクロールして、「**Oracle E-Business Suite 12.2**」を選択します。検索オプションを使用して、StyleBook を検索することもできます。
2. StyleBook パネルで「設定を作成」をクリックします。
3. ロードバランサーの設定セクションに、ロードバランサーアプリケーションの名前と仮想 IP アドレスを入力します。
4. 必要なプロトコルを選択します。HTTP と HTTPS/SSL の 2 つのオプションがあります。ポート番号を入力することもできます。
5. 負荷分散を行うネットワーク内のすべての Oracle E-Business Suite アプリケーション・サーバーの IP アドレスを入力します。サーバーの IP アドレスを追加するには、[**+**] をクリックします。
6. [**SSL** 証明書の設定] セクションで、ローカルストレージからそれぞれのファイルを選択します。**[** 証明書の詳細設定] チェックボックスをオンにすることもできます。ここでは、証明書の有効期限の通知期間などの詳細を設定できます。また、証明書の有効期限モニターを有効または無効にすることができます。

   構成を作成する対象の Citrix ADC インスタンスを選択し、［作成］をクリックします。



> ヒント
>
> 更新アイコンをクリックして、Citrix ADM で最近検出された Citrix ADC インスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。更新アイコンは、Citrix ADM でのみ

> 使用できます。

Web アプリケーションファイアウォール StyleBook

May 7, 2021

Citrix Web App Firewall wall は、Web アプリケーションファイアウォール（WAF）で、アプリケーション層およびゼロデイ脅威を含む既知の攻撃と未知の攻撃の両方から Web アプリケーションとサイトを保護します。

Citrix ADM は、Citrix ADC インスタンスでアプリケーションファイアウォール構成をより便利に作成できるデフォルトの StyleBook を提供します。

アプリケーションファイアウォール構成の展開

以下のタスクは、ビジネスネットワーク内の Citrix ADC インスタンスで、アプリケーションファイアウォールと IP レピュテーションポリシーとともに負荷分散構成を展開するのに役立ちます。

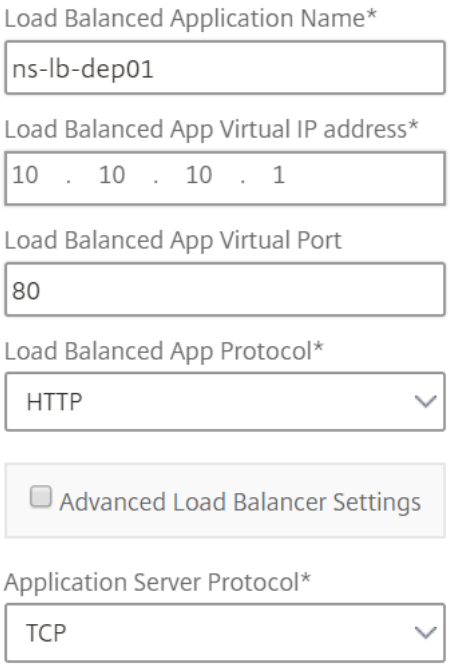
アプリケーション・ファイアウォール設定を使用して **LB** 構成を作成するには、次の手順に従います。

1. Citrix ADM で、［アプリケーション］>［構成］>［スタイルブック］に移動します。［スタイルブック］ページには、Citrix ADM で使用可能なすべてのスタイルブックが表示されます。下にスクロールして、アプリケーションファイアウォールポリシーと IP レピュテーションポリシーを使用した HTTP/SSL 負荷分散 StyleBook を見つけます。StyleBook は、`lb-appfw`という名前を入力して検索することもできます。[構成を作成] をクリックします。

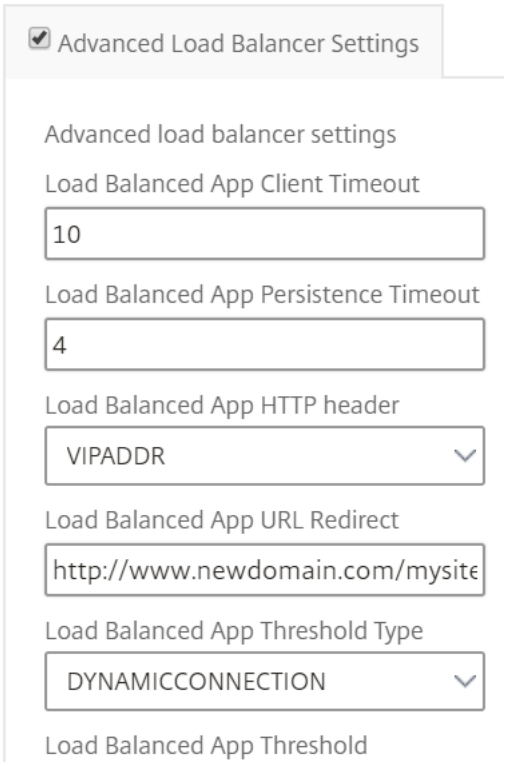
   StyleBook がユーザーインターフェイスページとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。

2. 次のパラメーターの値を入力します。

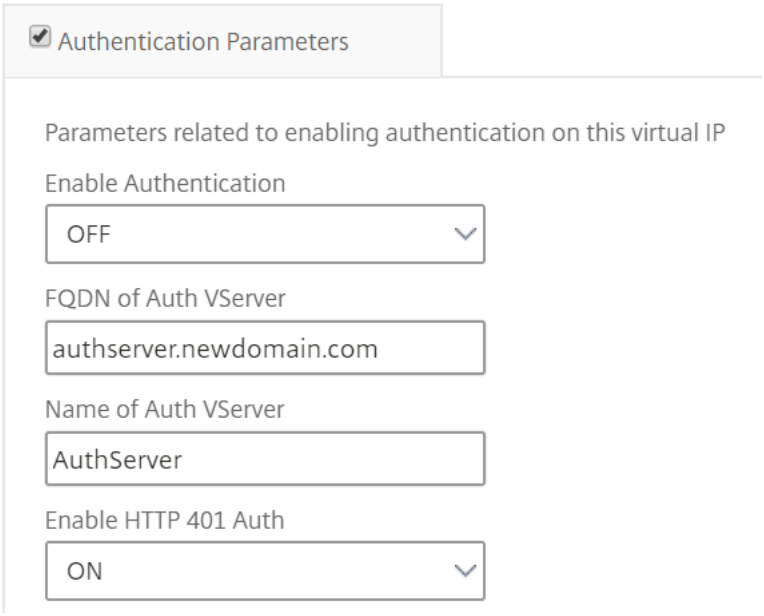
   - 負荷分散されたアプリケーション名。ネットワークに展開するアプリケーションファイアウォールを使用した負荷分散設定の名前。
   - 負荷分散されたアプリケーションの仮想 **IP** アドレス。Citrix ADC インスタンスがクライアント要求を受信する仮想 IP アドレス。
   - 負荷分散されたアプリケーション仮想ポート。負荷分散されたアプリケーションにアクセスする際にユーザーが使用する TCP ポート。
   - 負荷分散されたアプリケーションプロトコル。リストからフロントエンドプロトコルを選択します。
   - アプリケーションサーバープロトコル。アプリケーションサーバーのプロトコルを選択します。



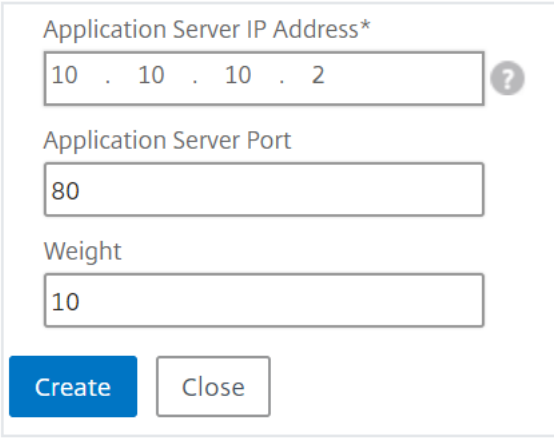
3. オプションとして、ロードバランサーの詳細設定を有効にして構成できます。



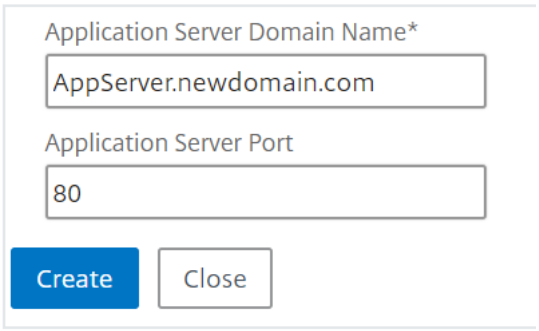
4. オプションで、負荷分散仮想サーバのトラフィックを認証するための認証サーバを設定することもできます。



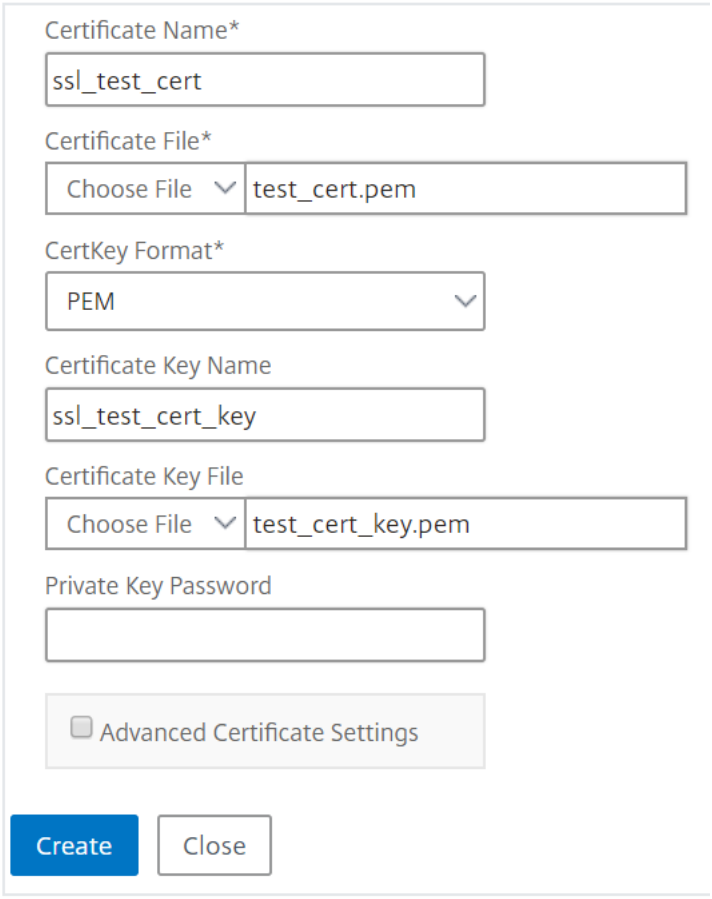
5. [サーバー IP とポート] セクションの [+] をクリックして、アプリケーションサーバーと、それらにアクセス可能なポートを作成します。



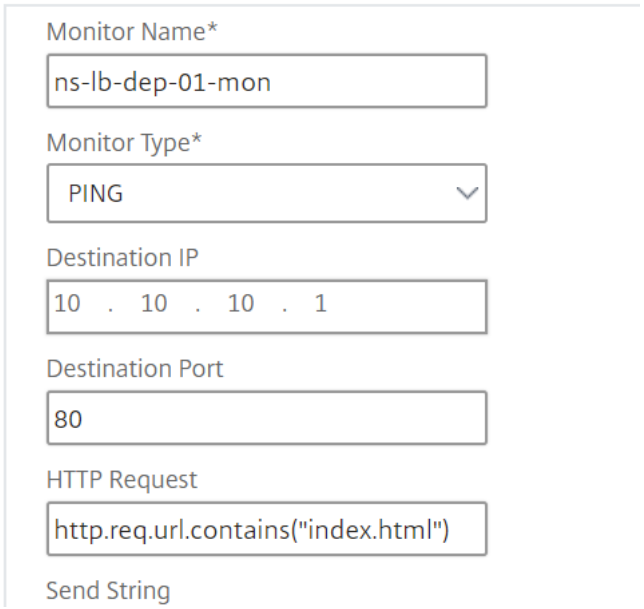
6. アプリケーションサーバーの FQDN 名を作成することもできます。



7. SSL 証明書の詳細を指定することもできます。



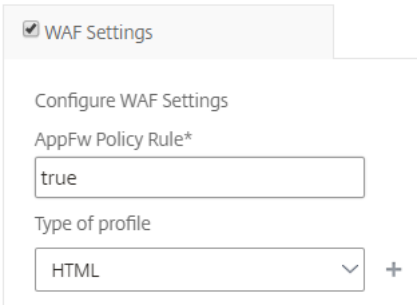
8. ターゲット Citrix ADC インスタンスでモニターを作成することもできます。



9. 仮想サーバでアプリケーションファイアウォールを設定するには、WAF 設定を有効にします。

   その VIP 上のすべてのトラフィックにアプリケーションファイアウォール設定を適用する場合は、アプリケ

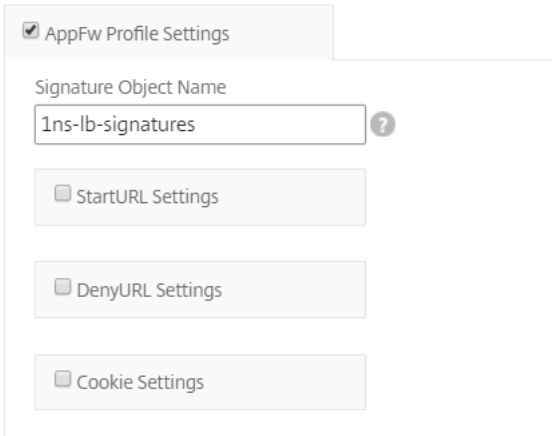
ーションファイアウォールポリシールールが true であることを確認します。それ以外の場合は、Citrix ADC ポリシールールを指定して、アプリケーションファイアウォール設定を適用する要求のサブセットを選択します。次に、適用する必要があるプロファイルのタイプ (HTML または XML) を選択します。



10. オプションで、アプリケーションファイアウォールの [プロファイル設定] チェックボックスをオンにして、アプリケーションファイアウォールプロファイルの詳細設定を構成できます。
11. 必要に応じて、アプリケーションファイアウォール署名を構成する場合は、仮想サーバーを展開する Citrix ADC インスタンス上に作成される署名オブジェクトの名前を入力します。

    > 注:
    >
    > この StyleBook を使用して署名オブジェクトを作成することはできません。

12. 次に、StartUrl 設定、denyURL 設定など、他のアプリケーションファイアウォールプロファイル設定を構成することもできます。



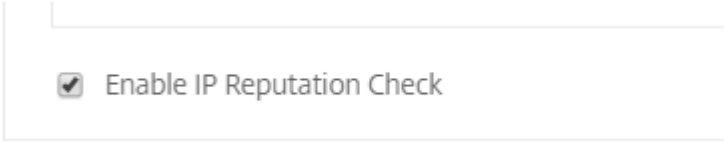
アプリケーションファイアウォールと構成設定の詳細については、「アプリケーションファイアウォール」を参照してください。

13. [ターゲットインスタンス] セクションで、アプリケーションファイアウォールで負荷分散仮想サーバーを展開する Citrix ADC インスタンスを選択します。

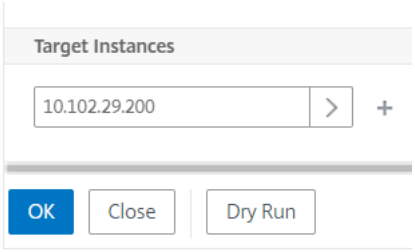
    > 注:
    >
    > 更新アイコンをクリックして、Citrix ADM で最近検出された Citrix ADC インスタンスを、このウィン

> ドウで使用可能なインスタンスの一覧に追加することもできます。

14. **IP** レピュテーションチェックを有効にして、不要な要求を送信している IP アドレスを特定することもできます。IP レピュテーションリストを使用すると、不正なレピュテーションを持つ IP からの要求をプリエンプティブに拒否できます。



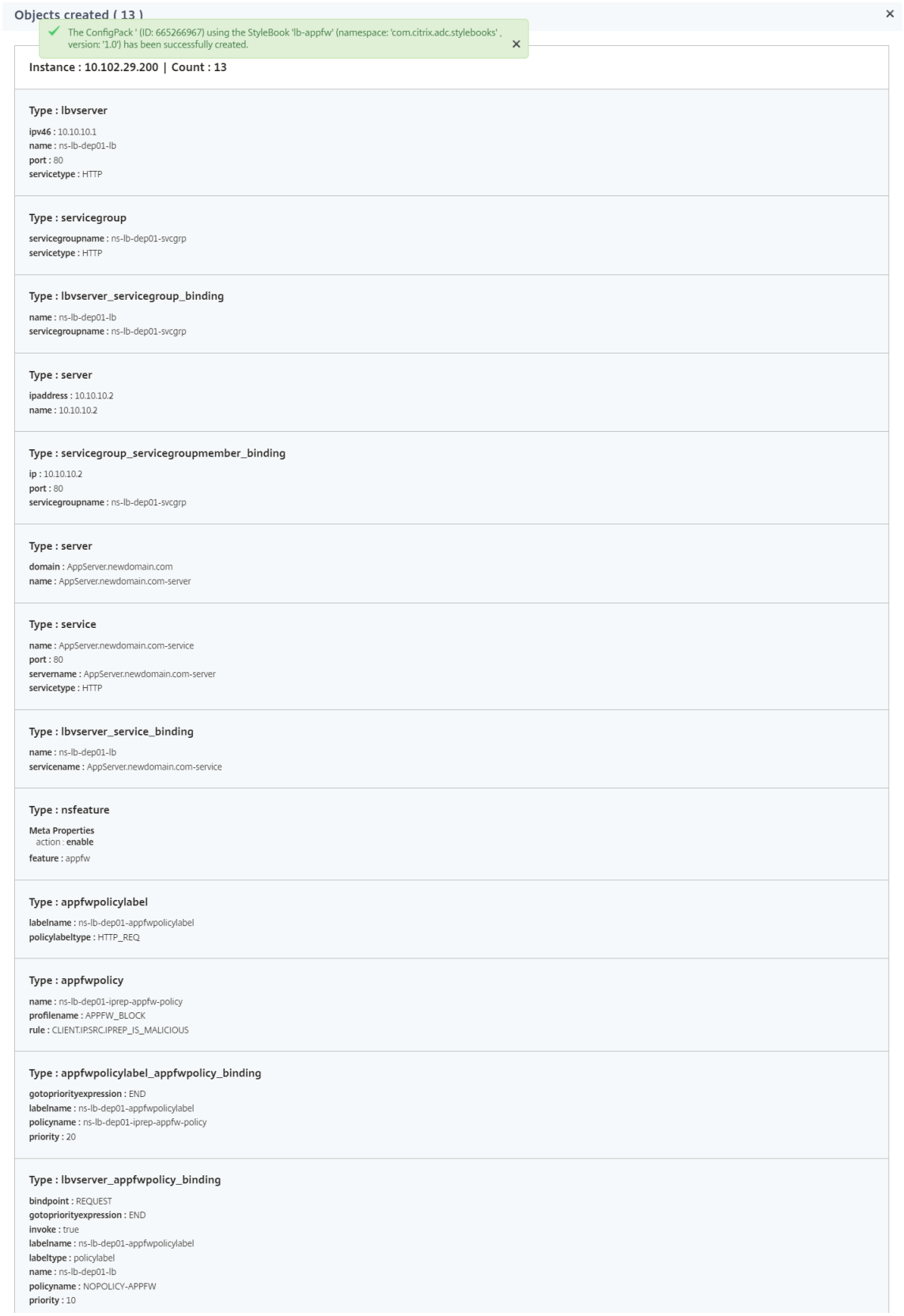
15. ［作成］をクリックして、選択した Citrix ADC インスタンスで構成を作成します。



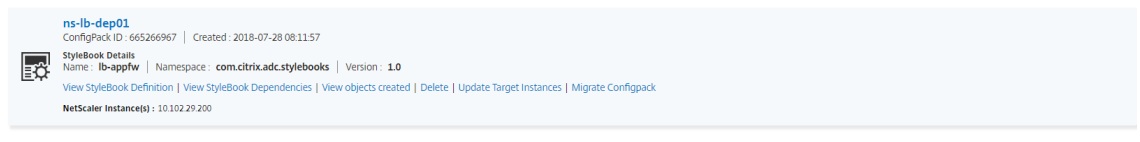
> ヒント
>
> インスタンスで実際の構成を実行する前に、［Dry Run］を選択して、ターゲットインスタンスに作成する必要がある構成オブジェクトを確認することをお勧めします。

構成が正常に作成されると、StyleBook は必要な負荷分散仮想サーバー、アプリケーションサーバー、サービス、サービスグループ、アプリケーションファイアウォールラベル、アプリケーションファイアウォールポリシーを作成し、負荷分散仮想サーバーにバインドします。

次の図は、各サーバーで作成されるオブジェクトを示しています。



16. Citrix ADM で作成された ConfigPack を表示するには、［アプリケーション］>［構成］に移動します。



StyleBook を使用して WAF と BOT プロファイルを作成する

May 7, 2021

API **Gateway** で **API** リソースに対するポリシーを選択できる場合、API リクエストを認証するためのトラフィック選択基準を定義できます。また、API トラフィックに対して API セキュリティポリシーを設定することもできます。詳しくは、「API ゲートウェイの管理」を参照してください。

WAF ポリシーと BOT ポリシーを API リソースに設定できます。ポリシーを構成する前に、Citrix Application Delivery Management（ADM）でプロファイルを作成してください。プロファイルを作成するには、次のデフォルトの StyleBooks を使用します。

- API WAF 検出スタイルブック
- API ボット検出 StyleBook

StyleBook を使用して WAF プロファイルを作成する

WAF プロファイルを作成するには、次の手順を実行します。

1. Citrix ADM で、[アプリケーション] > [構成] > [スタイルブック] に移動します。StyleBook を検索するには、`api-waf-profile`という名前を入力します。[構成を作成] をクリックします。

   StyleBook がユーザーインターフェイスページとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。

2. 次のパラメータの値を指定します。

   - **API WAF** プロファイル名 -WAF プロファイルを識別するための名前。
   - アプリケーションタイプ -プロファイルへのアプリケーションの種類を追加します。WAF プロファイルは、JSON および XML アプリケーションタイプをサポートします。

3. オプション、セキュリティ設定を有効にして、HTTP、JSON、または XML の保護チェックを指定します。Citrix Web App Firewall へのエラー URL を指定することもできます。詳しくは、「Web App Firewall プロファイルの作成」を参照してください。

4. この構成を展開するターゲット Citrix ADC インスタンスまたはインスタンスグループを選択します。

5. [作成] をクリックします。

WAF ポリシーを設定するには、API デプロイへのポリシーの追加を参照してください。

StyleBook を使用して **BOT** プロファイルを作成する

BOT プロファイルを作成するには、次の手順を実行します。

1. Citrix ADM で、［アプリケーション］>［構成］>［スタイルブック］に移動します。StyleBook を検索するには、`api-bot-profile`という名前を入力します。[構成を作成] をクリックします。

   StyleBook がユーザーインターフェイスページとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。

2.「**BOT** プロファイル名」で、BOT プロファイルを識別する名前を指定します。

3. 必要に応じて、要件に応じて次のオプションを有効にします。

   - **IP** レピュテーションチェックを有効にする -このオプションは、不要な要求を送信している IP アドレスを識別します。IP レピュテーションリストを使用すると、不正なレピュテーションを持つ IP からの要求をプリエンプティブに拒否できます。
   - **BOT** 署名を有効にする -BOT 署名名を指定します。これは、指定された署名からのリクエストをブロックします。
   - 許可リスト -IPv4 またはサブネット (CIDR) アドレスを指定します。このオプションを使用すると、BOT プロファイルは、指定した IPv4 アドレスまたはサブネットアドレスからの要求をバイパスできます。
   - 拒否リスト -IPv4 またはサブネット (CIDR) アドレスを指定します。このオプションを使用すると、BOT プロファイルは、指定した IPv4 アドレスまたはサブネットアドレスからの要求をブロックできます。

4. この構成を展開するターゲット Citrix ADC インスタンスまたはインスタンスグループを選択します。
5.［作成］をクリックします。

BOT ポリシーを設定するには、API デプロイへのポリシーの追加を参照してください。

カスタムスタイルブックの作成と使用

May 7, 2021

展開用に独自の StyleBook を作成し、Citrix Application Delivery Management（ADM）にインポートして、構成オブジェクトを作成できます。また、API を使用して、StyleBook から構成を作成することもできます。

このドキュメントでは、次の内容について説明します。

はじめに

StyleBook の作成を始める前に、次の知識があることを確認してください。

- NITRO API。詳しくは、「NITRO API ドキュメント」を参照してください。
- YAML

StyleBook ファイルでは YAML 形式を使用します。YAML 形式について詳しくは、YAML 構文を参照してください。

StyleBook を作成するときは、次に示す YAML のガイドラインに注意する必要があります。

- YAML では、大文字と小文字が区別されます。
- YAML では、インデントを適切に使用する必要があります。
- 適切なインデントを作成するには、<spacebar> キーを使用します。<tab>キーは使用しないでください。<tab> キーを使用すると、StyleBook を MA Service にインポートする際にコンパイルエラーが発生します。
- 文字列を引用符で囲まないでください。文字列が句読点（ダッシュ、コロン、その他）を含む場合にのみ、文字列を引用符で囲ってください。数字を文字列として解釈する必要がある場合は、数字を引用符で囲むか、または StyleBook の組み込み関数 str() を使用します。
- Yes/Yes/Yes/Y/Y/No/No/N/N、ON/ON/ON/OFF/OFF、および真/真/真/真/偽/偽/偽のようなリテラルはブール値とみなされ、それぞれ真と偽に相当します。これらのリテラルを文字列として解釈するには、引用符で囲んでください。例:
  - 「YES」
  - 「いいえ」
  - 「真」
  - 「偽」など。

> 注
>
> StyleBook ファイルを Citrix ADM にインポートする前に、ファイルが YAML 形式に準拠しているかどうかを確認することをお勧めします。StyleBooks に組み込みの YAML バリデータを使用して、YAML コンテンツを検証およびインポートすることをお勧めします。
>
> StyleBooks の設定中は、作成および削除操作（**POST** および **DELETE** HTTP メソッド）をサポートする NITRO 構成リソースのみを使用できます。詳しくは、「NITRO API のドキュメント」を参照してください。

StyleBook の構造

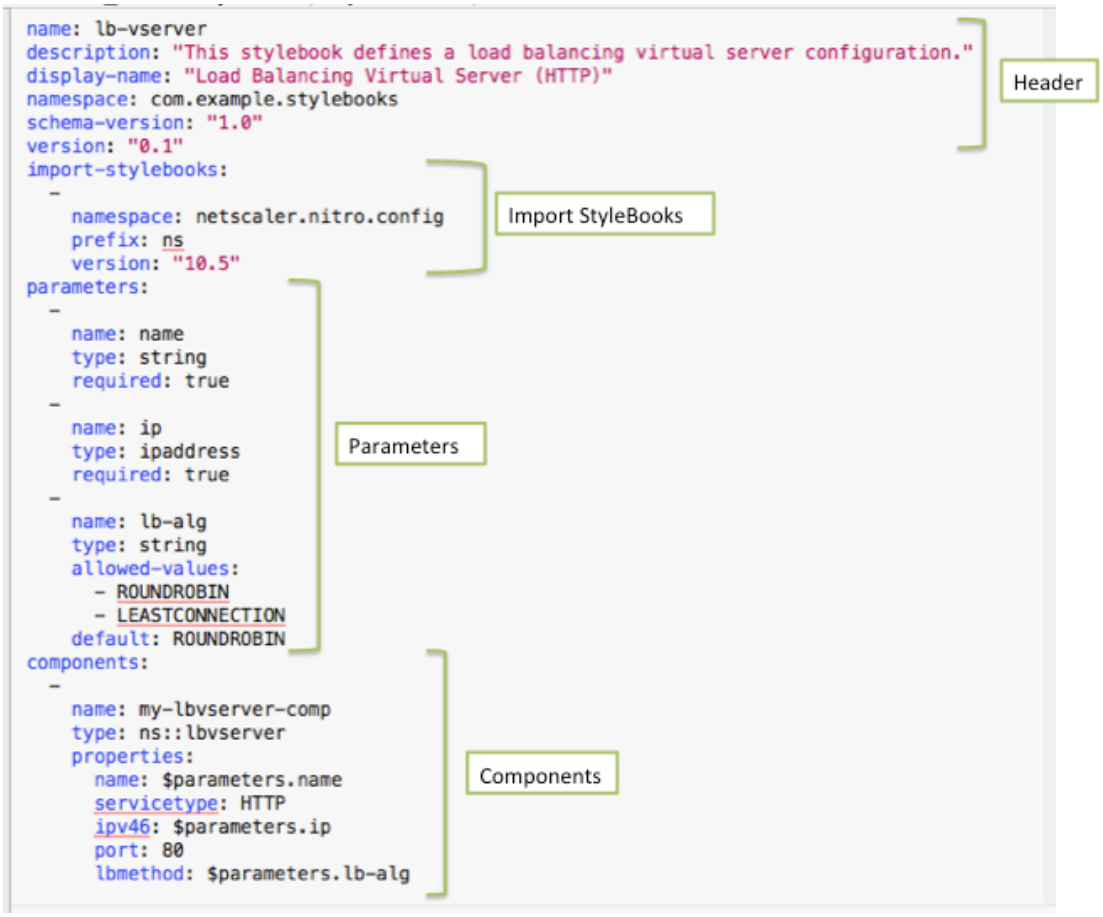
StyleBook を作成するには、StyleBook の文法、構文、および構造を理解する必要があります。通常、StyleBook には、次のセクションが含まれます。

- ヘッダー: このセクションでは、StyleBook のアイデンティティを定義し、それが何をしているのかを説明します。これは必須セクションです。
- **Import StyleBooks**: このセクションでは、現在の StyleBook から参照する他の StyleBook を宣言できます。スタイルブックを作成するためには、Citrix ADC NITRO 構成スタイルブックまたはその他のスタイルブックをインポートする必要があります。これは必須セクションです。

- **Parameters**: このセクションでは、構成を作成するために必要な StyleBook のパラメーターを定義します。StyleBook では、このセクションに記述された入力が使用されます。これはオプションのセクションです。
- コンポーネント: このセクションでは、StyleBook によって特定の構成に対して作成されるエンティティ（構成オブジェクト）を定義できます。このセクションは、StyleBook の中核です。Components では通常、Parameters セクションの入力値を使用して、StyleBook で生成される構成に適応させます。これはオプションのセクションです。

  StyleBook には、Parameters セクションと Components セクションのいずれか、または両方を記述できます。他の StyleBook で使用可能なパラメーターの一覧を定義する場合、Parameters セクションのみを含む StyleBook を作成すると便利です。これにより、一連の StyleBook 全体で、パラメーターグループが再利用しやすくなります。ユーザー入力を取得するパラメーターを定義せずに、StyleBook の属性値を指定する場合は、Components セクションのみを含む StyleBook を使用します。
- **Outputs**: Parameters セクションでは、StyleBook の入力を定義しましたが、この省略可能な Outputs セクションでは StyleBook の出力を定義します。構成を作成するユーザーは、この省略可能な Outputs セクションで指定したコンポーネントを、この StyleBook から、この StyleBook をインポートする他の StyleBook に公開できます。これにより、ユーザーおよびインポートする側の StyleBook は、公開されたコンポーネントのプロパティを参照できます。
- 操作: StyleBook には、StyleBook の一部である仮想サーバー上で Citrix ADM で Analytics を有効にするオプションのセクションを含めることができます。

次の図は、StyleBook の概略を簡単に示したものです。



次の例は、StyleBook の文法と構文について学び、より複雑な StyleBook の作成方法を理解するのに役立ちます。

- 負荷分散仮想サーバーを作成する StyleBook
- StyleBook による基本的な負荷分散構成の作成
- 複合スタイルブックの作成
- GUI 属性を使用して StyleBook をカスタマイズする

負荷分散仮想サーバーを作成する **StyleBook**

May 7, 2021

この例で設計する基本的な StyleBook では、プロトコルのタイプが HTTP で、ポート 80 でリッスンする負荷分散仮想サーバーを作成します。仮想サーバーの名前、IP アドレス、負荷分散方式の各パラメーターには、ユーザーが定義した値を指定できます（これらは StyleBook のパラメーターです）。

ヘッダー

StyleBook の先頭の 6 行は、Header セクションです。この例の場合、Header セクションは、次のように記述されています。

```
name: lb-vserver
namespace: com.example.stylebook
version: "1.0"
display-name: Load Balancing Virtual Server (HTTP)
description: "This stylebook defines a very simple load balancing HTTP
   virtual server configuration"
schema-version: "1.0"
<!--NeedCopy-->
```

Header セクションには、次の情報が記述されています。

- **name**：この StyleBook の名前。
- **description**：この StyleBook の実行内容を示す説明。この説明は、Citrix Application Delivery Management（ADM）に表示されます。
- 表示名：Citrix ADM に表示されるスタイルブックの説明的な名前。
- **namespace**：名前空間は、StyleBook の一意の識別子の一部で、これにより名前の衝突を回避できます。
- スキーマバージョン: このリリースでは常に「1.0」の値を取ります。
- **version**：StyleBook のバージョン番号。バージョン番号は、StyleBook の更新時に変更できます。

name、**namespace**、および **version** の組み合わせにより、システム内で StyleBook が一意に識別されます。Citrix ADM では、名前、名前空間、およびバージョンの同じ組み合わせを持つ 2 つの StyleBook を使用することはできません。ただし、name と version が同じであっても namespace が異なる場合、または namespace と version が同じであっても name が異なる場合は、それらの 2 つの StyleBook を使用できます。

> 注
>
> StyleBook を更新して、version の番号が更新された場合を想定してください。別の StyleBook でこの StyleBook を参照している（つまりインポートしている）場合は、インポート元の StyleBook の正しいバージョン番号が使用されるように、別の StyleBook を確実に更新して、インポートされる StyleBook の正しいバージョンが使われるようにしてください。

StyleBook のインポート

ヘッダーの後のセクションは「インポートスタイルブック」と呼ばれます。このセクションで、現在の StyleBook で参照する他の StyleBook の名前空間とバージョン番号を宣言する必要があります。このセクションを記述すると、他の StyleBook をインポートして再利用できるため、StyleBook で同じ構成を再作成する必要がなくなります。

この例の場合、import-stylebooks セクションは、次のように記述されています。

```
import-stylebooks:
```



```
  -
   namespace: netscaler.nitro.config
   prefix: ns
   version: "10.5"
<!--NeedCopy-->
```

いずれかの NITRO 構成オブジェクトを直接使用する場合、StyleBook では、netscaler.nitro.config 名前空間を必ず参照する必要があります。この名前空間には、LBVServer など、すべての Citrix ADC NITRO タイプが含まれています。ソフトウェアバージョン 10.5 以降がサポートされるため、StyleBook を使用して、リリース 10.5 以降を実行するすべての Citrix ADC インスタンス上で構成を作成および実行できます。

import-stylebooks セクションで使用されるプレフィックスは、名前空間とバージョンの組み合わせを示すための略語です。この場合、ns はバージョン 10.5 の netscaler.nitro.config を指します。StyleBook の以降のセクションでは、名前空間とバージョンを使用して、インポートされる StyleBook を示す代わりに、選択したプレフィックス文字列（上記の例では ns）を使用できます。

スタイルブックで使用されるバージョンは、Citrix ADC NITRO バージョンです。NITRO バージョン X に基づく StyleBook を使用して、バージョン X 以上の Citrix ADC を構成できます。

> 注
>
> StyleBook を使用してバージョン 10.5 以降の Citrix ADC インスタンスを構成できるようにするには、互換性を最大化するために、NITRO 組み込み StyleBooks（名前空間：netscaler.NITRO .config、バージョン：10.5）を直接使用する StyleBook に NITRO 10.5 名前空間をインポートすることをお勧めします。

他の StyleBook をインポートする StyleBook は、インポートする StyleBook と同等またはそれ以上のバージョンの NITRO バージョンに基づいている必要があることが重要です。たとえば、NITRO バージョン 10.5 をベースにした StyleBook は、11.1 をベースにした StyleBook に依存したり、使用したり、インポートしたりすることはできません。しかし、バージョン 11.1 に基づく StyleBook は、11.1 未満のバージョンに基づく StyleBook をインポートすることができます。

また、NITRO 名前空間をまったくインポートしない StyleBook もあります。つまり、StyleBook は NITRO コンポーネントを直接定義する必要はなく、NITRO コンポーネントを定義する StyleBook をインポートすることができます。他の StyleBook をインポートする StyleBook は、常に依存関係の階層内で最も高い NITRO バージョンを取得します。また、そのバージョン以上の Citrix ADC を構成するために使用されます。

パラメーター

Parameters セクションでは、StyleBook で必要なすべてのパラメーターを宣言できます。StyleBook の作成者は、StyleBook のユーザーが指定する入力項目を決定する必要があります。この例の場合、ユーザーが、仮想サーバーの名前、IP アドレス、負荷分散方式を指定するように StyleBook を設計しました。

Parameters セクションは、次のようになっています。

```
parameters:
```



```
 -
  name: name
  label: "Application Name"
  description: "Give a name to the application configuration."
  type: string
  required: true
 -
  name: vip-ipaddress
  label: "Load Balancer IP Address"
  description: "The Application VIP that clients access"
  type: ipaddress
  required: true
 -
  name: lb-alg
  label: LB Algorithm
  description: Load Balancing Algorithm
  type: string
  default: ROUNDROBIN
  allowed-values:
   - ROUNDROBIN
   - LEAST-CONNECTION
<!--NeedCopy-->
```

> 注
>
> パラメーターのラベルを指定しない場合、Citrix ADM はこのパラメーターの表示時に name 属性を使用します。Citrix ADM での表示方法を制御できるように、パラメーターのラベルを常に定義する必要があります。
>
> ただし、API で使われる場合、パラメーターはその name で指定されます。

このセクションでは、**name** 属性の値で示される 3 つのパラメーターが宣言されています。**name** は仮想サーバー名、**ip** は仮想サーバーの IP アドレス、**lb-alg** は負荷分散方式を表します。

- **type** は、そのパラメーターで使用できる値のタイプを示します。たとえば、名前および`lb-alg`は文字列値を取ることができます。IP 値は IP アドレスのタイプである必要があります。StyleBook のパラメーターには、次のいずれかの組み込みタイプを指定できます。
- **string**: 文字の配列。長さが指定されていない場合、文字列値には、任意の数の文字を使用できます。ただし、min-length 属性と max-length 属性を使用すれば、文字列タイプの長さを制限できます。
- **number**: 整数。min-value 属性と max-value 属性により、このタイプで使用できる最小数と最大数を指定できます。
- **boolean**: true と false のいずれかを設定できます。YAML では、すべてのリテラルがブール値（例: Yes または No）と見なされることに注意してください。
- **ipaddress**: 有効な IPv4 アドレスまたは IPv6 アドレスを示す文字列。
- **tcp-port**: TCP ポートまたは UDP ポートを示す 0～65535 の数値。
- パスワード: Opaque/シークレット文字列値。Citrix ADM でこのパラメータの値が表示される場合は、アス

タリスク（*****）として表示されます。

- **certfile**: 証明書ファイル。
- **keyfile**: 証明書の秘密鍵ファイル。
- **file**：このパラメータータイプを指定すると、ユーザーは、証明書やキーファイルなどのファイルをアップロードする必要があります。
- **object**：複数の要素から構成されます。これらの各要素はパラメーターです。このタイプを使用すると、関連する複数のパラメーターを 1 つの親パラメーターの下にグループ化できます。
- **required**: パラメータが必須かオプションかを示します。true に設定すると、パラメーターは必須になります。その場合、ユーザーは、StyleBook を使った構成の作成時にこのパラメーターの値を指定する必要があります。デフォルトでは、すべてのパラメーターが任意です。この例では、**name** と **ip** は必須のパラメータで、**lb-alg** はオプションのパラメータです。デフォルト値は「ROUNDROBIN.「

任意のパラメーターにデフォルト値を割り当てるには、**default** 属性を使用します。構成の作成時、ユーザーが値を指定しない場合は、デフォルト値が使用されます。たとえば、**lb-alg** パラメーターのデフォルト値は、ROUNDROBIN です。

構成の作成時にユーザーが選択できる値を定義するには、**allowed-values** 属性を使用します。この例の場合、**lb-alg** パラメーターには、ROUNDROBIN および LEASTCONNECTION という 2 つの値が指定されています。

StyleBook をインポートして使用すると、Citrix ADM はこれらの 3 つのパラメータを含むフォームが表示されます。[名前] と [IP] に表示されるフィールドでは、文字列と`ipaddress`タイプの値を入力できます。`lb-alg`フィールドは ROUNDROBIN がデフォルト値として選択されたドロップダウンリストとして表示されます。

> 注
>
> 組み込みタイプに加えて、パラメーターには他の StyleBook をタイプにすることができます。こうして他の StyleBook で定義されたパラメーターを再利用できます。

コンポーネント

この StyleBook の最後のセクションは、Components セクションです。Components セクションは、StyleBook で最も重要なセクションです。このセクションでは、StyleBook で作成する必要がある設定オブジェクトを定義します。

この例の場合、Components セクションは、次のように記述する必要があります。

```
components:
 -
  name: lbvserver-comp
  description: This StyleBook component (a Builtin Nitro StyleBook)
     builds a Citrix ADC lbvserver configuration object.
  type: ns::lbvserver
  properties:
   name: $parameters.name
   ipv46: $parameters.vip-ipaddress
```



```
    lbmethod: $parameters.lb-alg
    servicetype: HTTP
    port: 80
<!--NeedCopy-->
```

この例では、コンポーネントが 1 つのみ含まれています。コンポーネントの主要な属性は、name、type、および properties です。このコンポーネントで指定するプロパティは、コンポーネントのタイプによって決まります。コンポーネントには、次の 2 つのタイプがあります。

- 組み込み型: このタイプはシステムによって提供され、NITRO エンティティタイプlbvserverやservicegroupなど、定義する必要はありません。この例では、組み込みコンポーネントタイプを使用しています。
- 複合タイプ: このタイプは、作成して Citrix ADM にインポートした StyleBook、または Citrix ADM に同梱されているデフォルトの StyleBook です。複合 StyleBook について詳しくは、複合 StyleBook の作成を参照してください。

この例では、**lbvserver-comp** というコンポーネントを定義しました。このコンポーネントは、**ns lbvserver**（組み込みの NITRO タイプ）です。ここで、「ns」は、import-stylebooks セクションで指定した名前空間 netscaler.nitro.config およびバージョン 10.5 を参照する接頭辞であり、lbvserverはこの名前空間の NITRO リソースです。

ここで定義されたプロパティは、lbvserverリソースの属性です。利用可能なすべての Citrix ADC NITRO リソースとその属性の詳細については、Citrix ADC NITRO REST API ドキュメントを参照してください。

このセクションのプロパティには、lbvserverリソースの必須属性が含まれており、これらの属性の値を指定できます。この例では、servicetype およびポートに静的値を指定し、名前、ipv46、lbmethod およびプロパティは入力パラメータから値を取得します。StyleBook の残りの部分では、を使用して、パラメータ・セクションで定義されたパラメータ名を参照できます。**$parameters.<parameter-name>** 式 (例: **$** パラメータ**.ip**) です。

> 注
>
> 慣例により、「インポートスタイルブック」セクションで Citrix ADC NITRO 名前空間を指定するには、「ns」というプレフィックスが常に使用されます。これは必須ではありませんが、一貫性を保つためにお使いの StyleBook で慣例に従うことをお勧めします。

スタイルブックを構築する

StyleBook の必須セクションをすべて定義しました。これらのセクションをまとめて、最初の StyleBook を作成します。StyleBook の内容をコピーして、テキストエディターに貼り付け、**lb-vserver.yaml** という名前でファイルを保存します。StyleBooks で組み込みの YAML バリデータを使用して、YAML コンテンツを検証およびインポートすることをお勧めします。

lb-vserver.yaml ファイルのすべての内容を次に示します。

```
name: lb-vserver
```



```
namespace: com.example.stylebook
version: "1.0"
display-name: Load Balancing Virtual Server (HTTP)
description: "This stylebook defines a very simple load balancing HTTP
   virtual server configuration"
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
 -
  namespace: com.citrix.adc.stylebooks
  version: "1.0"
  prefix: stlb

parameters:
 -
  name: name
  label: "Application Name"
  description: "Give a name to the application configuration."
  type: string
  required: true
 -
  name: vip-ipaddress
  label: "Load Balancer IP Address"
  description: "The Application VIP that clients access"
  type: ipaddress
  required: true
 -
  name: lb-alg
  label: LB Algorithm
  description: Load Balancing Algorithm
  type: string
  default: ROUNDROBIN
  allowed-values:
   - ROUNDROBIN
   - LEAST-CONNECTION

components:
 -
  name: lbvserver-comp
  description: This StyleBook component (a Builtin Nitro StyleBook)
     builds a Citrix ADC lbvserver configuration object.
```



```
45    type: ns::lbvserver
46    properties:
47     name: $parameters.name
48     ipv46: $parameters.vip-ipaddress
49     lbmethod: $parameters.lb-alg
50     servicetype: HTTP
51     port: 80
52  <!--NeedCopy-->
```

StyleBook を使用して構成を作成するには、Citrix ADM にインポートしてから使用する必要があります。詳しくは、「ユーザー定義スタイルブックの使用方法」を参照してください。

またこの StyleBook を他の StyleBook に（import-stylebooks 構造を使って）インポートすることもできます。または、次のセクションで説明されるように、より多くのパラメーターとコンポーネントを含むようにこの StyleBook を修正することもできます。

StyleBook による基本的な負荷分散構成の作成

May 7, 2021

前の例では、負荷分散仮想サーバーを作成するための基本的な StyleBook を構築しました。この StyleBook を別名で保存した後、基本的な負荷分散を構成するためのパラメーターとコンポーネントを追加して、StyleBook を更新します。この StyleBook ファイルを **basic-lb-config.yaml** という名前で保存します。

このセクションでは、負荷分散仮想サーバー、サービスグループ、およびサービス一覧からなる負荷分散の構成を作成する新しい StyleBook を設計します。また、サービスをサービスグループにバインドし、サービスグループを仮想サーバーにバインドできます。

ヘッダー

この StyleBook を作成するには、最初に Header セクションを更新する必要があります。このセクションは、負荷分散仮想サーバーの StyleBook 用に作成したセクションと似ています。Header セクションで、**name** の値を basic-lb-config に変更します。また、この StyleBook の適切な説明を記述して、**description** と **display-name** を更新します。**namespace** と **version** の値は、変更する必要はありません。name を変更したため、name、namespace、および version の組み合わせにより、この StyleBook の一意の識別子がシステム内に作成されます。

```
1  name: basic-lb-config
2  namespace: com.example.stylebooks
3  version: "0.1"
4  display-name: Load Balancing Configuration
5  description: This StyleBook defines a simple load balancing
       configuration.
```



```
schema-version: "1.0"
<!--NeedCopy-->
```

StyleBook のインポート

import-stylebooks セクションは、同じままです。このセクションでは、NITRO 構成オブジェクトを使用するために、netscaler.nitro.config 名前空間が指定されています。

```
import-stylebooks:
 -
 namespace: netscaler.nitro.config
 prefix: ns
 version: "10.5"
<!--NeedCopy-->
```

パラメーター

Parameters セクションを更新して、サービスまたはサーバーの一覧を定義するパラメーターと、サービスをリッスンするポートを定義するパラメーターを追加する必要があります。最初の 3 つのパラメータ name、ip、lb-alg およびは同じままです。

```
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the loadbalancing algorithm (method) used for
     loadbalancing client requests between the application servers.
  allowed-values:
     - ROUNDROBIN
     - LEASTCONNECTION
```



```
    default: ROUNDROBIN
  -
    name: svc-servers
    type: ipaddress[]
    label: Application Server IPs
    description: The IP addresses of all the servers of this application
    required: true
  -
    name: svc-port
    type: tcp-port
    label: Server Port
    description: The TCP port open on the application servers to receive
       requests.
    default: 80
<!--NeedCopy-->
```

この例では、パラメータ **svc-servers** が追加され、アプリケーションのバックエンドサーバーを表すサービスの IP アドレスのリストを受け付けます。これは、**required: true** からわかるように、必須パラメーターです。2 番目のパラメーター、**svc-port** は、サーバーがリッスンするポート番号を示しています。`svc-port` パラメータがユーザーによって指定されていない場合、デフォルトのポート番号は 80 です。

コンポーネント

また、Components セクションを更新して、新しい 2 つのパラメーターを使用して完全な負荷分散構成を作成する追加コンポーネントを定義する必要があります。

この例の場合、Components セクションは、次のように記述する必要があります。

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg

components:
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
```



```
17     name: $parameters.name + "-svcgrp"
18     servicetype: HTTP
19
20 components:
21  -
22   name: lbvserver-svg-binding-comp
23   type: ns::lbvserver_servicegroup_binding
24   properties:
25    name: $parent.parent.properties.name
26    servicegroupname: $parent.properties.name
27  -
28   name: members-svcg-comp
29   type: ns::servicegroup_servicegroupmember_binding
30   repeat: $parameters.svc-servers
31   repeat-item: srv
32   properties:
33    ip: $srv
34    port: str($parameters.svc-port)
35    servicegroupname: $parent.properties.name
36 <!--NeedCopy-->
```

この例では、(前の例の) 元のコンポーネント **lbvserver-comp** に **svcg-comp** という子コンポーネントがあります。また、**svcg-comp** コンポーネントには 2 つの子コンポーネントがあります。コンポーネントを別のコンポーネント内にネストした場合、ネストされたコンポーネントは、親コンポーネントの属性を参照して構成オブジェクトを作成できます。ネストされたコンポーネントは、親コンポーネントでオブジェクトが作成されるたびに、1 つまたは複数のオブジェクトを作成できます。

svcg-comp コンポーネントは、リソース`servicegroup`の属性に指定された値を使用して、Citrix ADC インスタンス上にサービスグループを作成するために使用されます。この例では、`servicetype`の静的値を指定し、name は入力パラメータから値を取得します。**$parameters.name+**「**-svcgrp**」表記を使用して、パラメータセクションで定義されているパラメータ名を参照します。ここで、ユーザー定義の名前に「**-svcgrp**」が付加されます (連結)。

コンポーネント **svcg-comp** には、**lbvserver-svg-binding-comp** と **members-svcg-comp** という 2 つの子コンポーネントがあります。

最初の子コンポーネント **lbvserver-svg-binding-comp** は、親コンポーネントによって作成されたサービスグループと、親の親コンポーネントによって作成された負荷分散仮想サーバー (`lbvserver`) との間で設定オブジェクトをバインドするために使用されます。$parent 表記 (親参照とも呼ばれる) は、親コンポーネントのエンティティを参照するために使用されます。たとえば、**servicegroupname: $parent.properties.name** は、親コンポーネント **svcg-comp** によって作成されたサービスグループを指し、名前**:$parent.parent.parent.properties.name** は、親の親コンポーネント **lbvserver-comp** によって作成された仮想サーバーを指します。

members-svcg コンポーネントは、親コンポーネントによって作成されたサービスグループにサービスのリスト間の設定オブジェクトをバインドするために使用されます。複数のバインディング設定オブジェクトを作成するには、StyleBook の **re** peat 構造を使用して、パラメータ **svc-**servers で指定されたサーバーのリストを反復処理しま

す。反復処理中、この StyleBook コンポーネントはサービスグループ内の各サービス（**repeat-item** 構造の`srv`）に対してサービスグループで **servicegroup_servicegroupmember_binding** タイプの NITRO 設定オブジェクトを作成し、各 NITRO 設定オブジェクト **ip** 属性を対応するサーバの IP アドレスに設定します。

通常、コンポーネント内で **repeat** および **repeat-item** 構造を使用して、そのコンポーネントが同じタイプの複数の設定オブジェクトを構築できます。たとえば、`srv`のように **repeat-item** 構造に変数名を割り当てて、反復の現在の値を指定できます。この変数名は、同じコンポーネントのプロパティまたは子コンポーネントで、**$<varname>**として参照されます（例：$srv）。

上記の例では、お互いの内部でコンポーネントのネスティングを使って、簡単に構成を組み立てています。この特定のケースでは、構成を構築する唯一の方法は、コンポーネントのネストではありませんでした。以下に示すように、ネストせずに同じ結果を得ることができます。

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
    servicegroupname: $parameters.name + "-svcgrp"
    servicetype: HTTP
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
   name: $components.lbvserver-comp.properties.name
   servicegroupname: $components.svcg-comp.properties.servicegroupname
 -
  name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: 80
   servicegroupname: $components.svcg-comp.properties.servicegroupname
<!--NeedCopy-->
```


ここでは、すべてのコンポーネントが同じレベル（つまり、ネストされていない）ですが、達成された結果（Citrix ADC 構成が生成される）は、以前に使用されたネストされたコンポーネントと同じになります。また、StyleBook のコンポーネントを宣言する順序が、構成オブジェクトの作成順序に影響を与えることはありません。この例では、**svcg-comp** および **lbvserver-comp** コンポーネントは、最後に宣言されていても、2 番目のコンポーネントにはこれらのコンポーネントへの前方参照があるため、2 番目のコンポーネント **lbvserver-svg-binding-comp** を構築する前に構築する必要があります。

> 注
>
> 慣例によって、StyleBooks、パラメーター、置換、コンポーネント、出力の名前は小文字です。複数の単語を含む場合は「-」文字で区分されます。たとえば`lb-bindings`、`app-name`、`rewrite-config`などです。もう 1 つの規則は、コンポーネント名の末尾に`-comp`文字列を付けることです。

結果

新しい StyleBook に最後に追加するセクションは Outputs セクションです。Outputs セクションでは、この StyleBook を使用して構成を作成した後にユーザーに（または他の StyleBook で）公開する情報を指定します。たとえば、outputs セクションでを指定して、この StyleBook によって作成される`lbvserver`および`servicegroup`設定オブジェクトを公開できます。

```
outputs:
-
  name: lbvserver-comp
  value: $components.lbvserver-comp
  description: The component that builds the Nitro lbvserver
     configuration object
-
  name: servicegroup-comp
  value: $components.svcg-comp
  description: The component that builds the Nitro servicegroup
     configuration object
<!--NeedCopy-->
```

StyleBook の Outputs セクションは、必要に応じて記述します。StyleBook で必ずしも出力を返す必要はありません。ただし、内部コンポーネントを出力として返すと、この StyleBook をインポートするすべての StyleBook の柔軟性が向上します。このことは、複合 StyleBook の作成時にわかります。

> 注
>
> outputs セクションで、コンポーネントの単一のプロパティだけでなく、StyleBook のコンポーネントの全体を公開することが推奨されます（たとえば、$components.lbvserver-comp.properties.name という名前だけでなく、$components.lbvserver-comp 全体を公開します）。また出力には、特定の出力が何を表すかを説明する記述が追加されます。

スタイルブックを構築する

StyleBook の必須セクションをすべて定義したので、それらをまとめて 2 番目の StyleBook を作成します。この StyleBook ファイルは、**basic-lb-config.yaml** という名前で既に保存されています。StyleBooks に組み込みの YAML バリデータを使用して、YAML コンテンツを検証およびインポートすることをお勧めします。

basic-lb-config.yaml のすべての内容を次に示します。

```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: This StyleBook defines a simple load balancing
   configuration.
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the loadbalancing algorithm (method) used for
     loadbalancing client requests between the application servers.
  allowed-values:
     - ROUNDROBIN
     - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: svc-servers
```



```
37    type: ipaddress[]
38    label: Application Server IPs
39    description: The IP addresses of all the servers of this application
40    required: true
41   -
42    name: svc-port
43    type: tcp-port
44    label: Server Port
45    description: The TCP port open on the application servers to receive
          requests.
46    default: 80
47
48  components:
49   -
50    name: lbvserver-comp
51    type: ns::lbvserver
52    properties:
53     name: $parameters.name + "-lb"
54     servicetype: HTTP
55     ipv46: $parameters.ip
56     port: 80
57     lbmethod: $parameters.lb-alg
58   -
59    name: svcg-comp
60    type: ns::servicegroup
61    properties:
62      servicegroupname: $parameters.name + "-svcgrp"
63      servicetype: HTTP
64   -
65    name: lbvserver-svg-binding-comp
66    type: ns::lbvserver_servicegroup_binding
67    properties:
68     name: $components.lbvserver-comp.properties.name
69     servicegroupname: $components.svcg-comp.properties.servicegroupname
70   -
71    name: members-svcg-comp
72    type: ns::servicegroup_servicegroupmember_binding
73    repeat: $parameters.svc-servers
74    repeat-item: srv
75    properties:
76     ip: $srv
77     port: 80
78     servicegroupname: $components.svcg-comp.properties.servicegroupname
79
80  outputs:
```



```
81 -
82   name: lbvserver-comp
83   value: $components.lbvserver-comp
84   description: The component that builds the Nitro lbvserver
        configuration object
85 -
86   name: servicegroup-comp
87   value: $components.svcg-comp
88   description: The component that builds the Nitro servicegroup
        configuration object
89 <!--NeedCopy-->
```

StyleBook を使用して構成を作成するには、Citrix ADM にインポートしてから使用する必要があります。詳しくは、「ユーザー定義スタイルブックの使用方法」を参照してください。

この StyleBook を他の StyleBook にインポートして、そのプロパティを使用することもできます。詳しくは、次のセクションで説明します。

複合スタイルブックの作成

May 7, 2021

StyleBook の重要かつ便利な特徴の 1 つは、別の StyleBook の構築ブロックとして使用できる点です。StyleBook は別の StyleBook にインポートすることができ、それは NITRO 組み込み **StyleBook** に似た **2** 番目の **StyleBook** のコンポーネントで使用されるタイプと呼ぶことができます。

たとえば、前のセクションで構築した **basic-lb-config StyleBook** を使用して、複合例と呼ばれる別の **StyleBook** を作成できます。「basic-lb-config」StyleBook を使用するには、新しい StyleBook のインポート・スタイルブックセクションにインポートする必要があります。

スタイルブックを構築する

新しい StyleBook は、次のようになります。

```
1 name: composite-example
2 namespace: com.example.stylebooks
3 version: "0.1"
4 display-name: Load Balancing Virtual Server (HTTP/RoundRobin)
5 description: This StyleBook defines a RoundRobin load balancing
     configuration with a monitor.
6 schema-version: "1.0"
7 import-stylebooks:
8   -
```



```
    namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
  -
    namespace: com.example.stylebooks
    version: "0.1"
    prefix: stlb
parameters:
  -
    name: name
    type: string
    label: Application Name
    description: Give a name to the application configuration.
    required: true
  -
    name: ip
    type: ipaddress
    label: Application Virtual IP (VIP)
    description: The Application VIP that clients access
    required: true
  -
    name: svc-servers
    type: ipaddress[]
    label: Application Server IPs
    description: The IP addresses of all the servers of this
       application
    required: true

  -
    name: response-code
    type: string[]
    label: List of Response Codes
    description: List of Response Codes - Provide a list of response
       codes in integer.

components:
  -
    name: basic-lb-comp
    type: stlb::basic-lb-config
    description: This component's type is another StyleBook that builds
        the NetScaler lbvserver, servicegroups and services
       configuration objects.
    properties:
     name: $parameters.name
     ip: $parameters.ip
```



```
50      svc-servers: $parameters.svc-servers
51    -
52      name: monit-comp
53      type: ns::lbmonitor
54      description: This component is a basic Nitro type (a Builtin
            StyleBook) that builds the NetScaler monitor configuration
            object.
55      properties:
56        monitorname: $parameters.name + "-mon"
57        type: HTTP
58        respcode: $parameters.response-code
59        httprequest: "'GET /'"
60        lrtm: ENABLED
61        secure: "YES"
62
63      components:
64        -
65          name: monit-svcgrp-bind-comp
66          type: ns::servicegroup_lbmonitor_binding
67          properties:
68            servicegroupname: $components.basic-lb-comp.outputs.
                  servicegroup-comp.properties.servicegroupname
69            monitor_name: $parent.properties.monitorname
70  <!--NeedCopy-->
```

import-stylebooks セクションでは、プレフィックス`stlb`で参照される名前空間とバージョンを使用して、基本の lb-config StyleBook をインポートします。

Components セクションでは、2 つのコンポーネントが定義されています。最初のコンポーネントは **stlb::basic-lb-config** 型です。ここで、「basic-lb-config」はStyleBook による基本的な負荷分散構成の作成で作成したスタイルブックの名前です。このコンポーネントで定義されているプロパティは、basic-lb-config StyleBook で宣言されている必須パラメーターに対応しています。ただし、StyleBook の任意のパラメータを使用できます（必須とオプションの両方）。`lbvserver`、サービスグループ、サービスおよびサービスグループバインディングを再構築する代わりに、これらすべてをコンポーネントとして実行する StyleBook をインポートし、それを使用して新しい StyleBook にこれらの設定オブジェクトを作成します。

StyleBook は、NITRO リソース`lbmonitor`の属性（組み込み StyleBook）を使用してモニター設定オブジェクトを作成する 2 番目のコンポーネント`monit-comp`を追加します。また、最初のコンポーネントで作成された`servicegroup`にモニターをバインドするバインディング設定オブジェクトを作成するためのサブコンポーネント`monit-svcgrp-bind-comp`もあります。「basic-lb-config」StyleBook 作成されたコンポーネント`servicegroup`は出力として公開されるため、この **StyleBook** は **$components.basic-lb-comp.outputs.servicegroup-comp** という式を使用してアクセスできます。この例では、インポート先の StyleBook が、Outputs セクションを使用してインポート元の StyleBook のコンポーネントにアクセスする方法を示しています。この方法以外でアクセスすることはできません。

次に、StyleBook の内容をコピーしてテキストエディタに貼り付け、ファイルを コンポジット**-example.yaml** として保存します。Citrix ADM でファイルをインポートする前に、必ず YAML の内容を検証してください。次に、それを Citrix ADM にインポートし、この StyleBook を使用して 1 つまたは複数の構成を作成します。

StyleBooks に組み込みの YAML バリデータを使用して、YAML コンテンツを検証およびインポートすることをお勧めします。

カスタムスタイルブックでの **GUI** 属性の使用

May 7, 2021

StyleBook のパラメータセクションに GUI 属性を追加して、Citrix Application Delivery Management（ADM）に表示されるフィールドを直感的に表示できます。

例：パラメーターの説明的な名前を追加するには、label 属性を使用します。このパラメーターのツールチップを追加するには、description 属性を使用します。

```
name: ip
label: Virtual Server IP Address
description: IP address of the virtual server that represents the load
   balanced application.
type: ipaddress
required: true
<!--NeedCopy-->
```

例：使用するパラメーターのタイプがオブジェクトの場合は、**gui** 属性を使用してレイアウトを定義できます。この例の場合、レイアウトは折りたたみ可能なオブジェクトで、フィールドが 2 列で表示されます。

```
name: svcg-advanced
label: Advanced Application Server Settings
type: object
required: false
gui:
 collapse_pane: true
 columns: 2
<!--NeedCopy-->
```

例。また、タイプがオブジェクト [] (オブジェクトのリスト) のパラメータの概要ビューを、列を表す内部パラメータを持つテーブルとして表示することもできます。概要ビューに内部パラメーターを含めるか、除外するには、`gui`セクション内の`summary_display`属性を次のように使用します。

```
name: settings
label: Settings
```



```
type: object[]
parameters:
  -
    name: name
    label: Name
    description: Name of this setting
    type: string
    gui:
      summary_display: true
<!--NeedCopy-->
```

例: Citrix ADM の一部の StyleBook は、他の StyleBook のビルディングブロックとしてのみ使用されます。また、ユーザーがこれらの StyleBook から直接構成を作成しないようにすることもできます。これらの StyleBook は他の StyleBook の一部として使用されるためです。StyleBook をプライベートとしてマークして、Citrix ADM GUI で構成を作成するために StyleBook を直接使用しないようにします。

```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: This StyleBook defines a simple load balancing
   configuration.
schema-version: "1.0"
<!--NeedCopy-->
```

カスタム **StyleBook** をインポートする

May 7, 2021

StyleBook を構築したら、それを Citrix Application Delivery Management（ADM）にインポートして使用する必要があります。Citrix ADM では、単一のスタイルブックを YAML 形式でインポートすることも、複数のスタイルブック YAML ファイルを.zip、.tgz、または.gz 形式でバンドルとしてインポートすることもできます。Citrix ADM システムは、インポート時にスタイルブックを検証します。これで、StyleBook を使用して構成を作成できるようになりました。

Citrix ADM には、StyleBook YAML コンテンツの作成に使用できる組み込みの YAML エディタもあります。YAML エディタを使用すると、Citrix ADM GUI 自体から YAML 構造を検証できます。これらの検証チェックに個別のツールを使用する必要はありません。コンテンツは YAML 標準に照らして検証され、偏差が強調表示されます。その後、コンテンツを修正し、StyleBook を Citrix ADM にインポートできます。独自のスタイルブックを作成しながら、組み込みの YAML エディタは、2 つの利点を提供します。

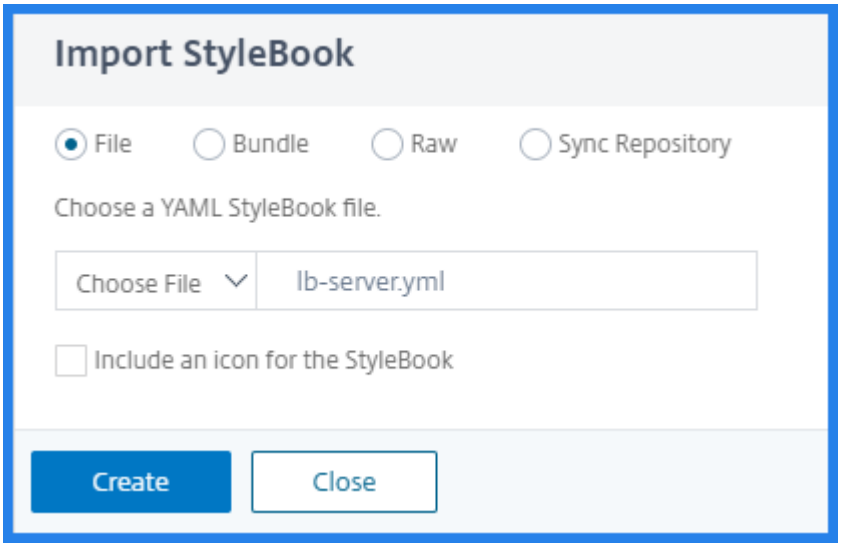
- 色分けされています。エディタは、YAML ガイドラインに従って解析された StyleBook コンテンツを表示し、色分けを使用すると、YAML コンテンツで定義されているキーと値を簡単に区別するのに役立ちます。
- **YAML** 検証です。入力時にコンテンツが YAML エラーに対して検証され、偏差が即座に強調表示されます。この検証により、Citrix ADM に StyleBook をインポートする前でも、YAML ガイドラインに準拠したテキストを作成できます。

> 注:
>
> 現在、エディタは YAML ガイドラインに従ってコンテンツを検証します。コードの正確性と誤植は検証されません。

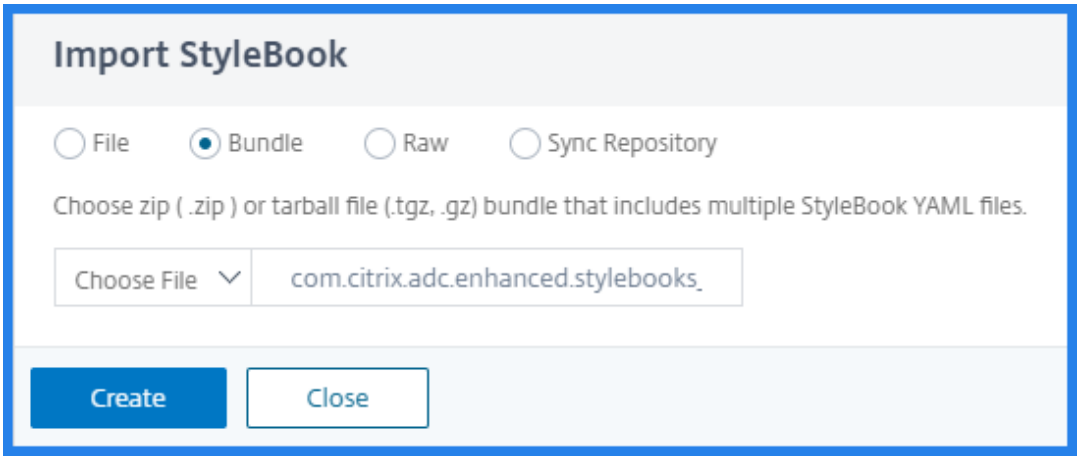
StyleBook をインポートするには

1. Citrix ADM で、[アプリケーション] > [構成] > [スタイルブック] の順に選択し、[新しいスタイルブックのインポート] をクリックします。
2. 次のいずれかのオプションをクリックして、StyleBook をインポートします。
   - ファイル -ローカルストレージから必要なファイルまたはファイルのバンドルを選択します。

     > 注:
     >
     > この例では、負荷分散仮想サーバーを作成するための StyleBookで作成したlb-vserver.yml StyleBook をインポートします。

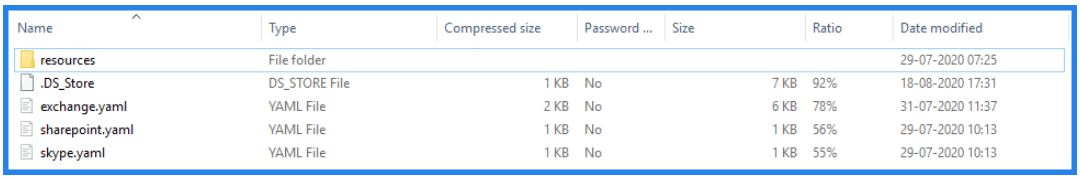
   - バンドル -Citrix ADM では、複数のスタイルブックを YAML 形式でインポートできます。zip（.zip）形式または tarball（.tgz、.gz）形式で圧縮された複数の YAML StyleBook ファイルをインポートできます。



バンドル内の各 StyleBook にアイコンを追加できるようになりました。これを行うには、アイコンと`icon_mapping.json`ファイルを`resources`フォルダにアップロードします。アイコンファイル名と StyleBook 名が一致する場合、アイコンは自動的に StyleBook にマッピングされます。それ以外の場合は、StyleBooks とアイコンを`icon_mapping.json`ファイルに次のようにマップします。

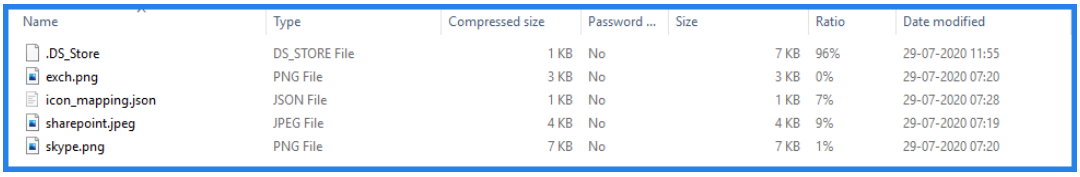
```
<StyleBook file name> : <icon file name>
<!--NeedCopy-->
```

StyleBook バンドルの例を次に示します。



Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
resources	File folder					29-07-2020 07:25
.DS_Store	DS_STORE File	1 KB	No	7 KB	92%	18-08-2020 17:31
exchange.yaml	YAML File	2 KB	No	6 KB	78%	31-07-2020 11:37
sharepoint.yaml	YAML File	1 KB	No	1 KB	56%	29-07-2020 10:13
skype.yaml	YAML File	1 KB	No	1 KB	55%	29-07-2020 10:13

`resources` フォルダには、必要なアイコンが含まれています。



Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
.DS_Store	DS_STORE File	1 KB	No	7 KB	96%	29-07-2020 11:55
exch.png	PNG File	3 KB	No	3 KB	0%	29-07-2020 07:20
icon_mapping.json	JSON File	1 KB	No	1 KB	7%	29-07-2020 07:28
sharepoint.jpeg	JPEG File	4 KB	No	4 KB	9%	29-07-2020 07:19
skype.png	PNG File	7 KB	No	7 KB	1%	29-07-2020 07:20

この例では、`sharepoint.yaml`および`skype.yaml`ファイルはそれぞれ`sharepoint.jpeg`および`skype.png`に自動的にマップされます。

`exchange.yaml`を`exch.png`にマッピングするには、`icon_mapping.json` ファイルに次のように指定します。

```
{

"exchange.yaml":"exch.png"
 }

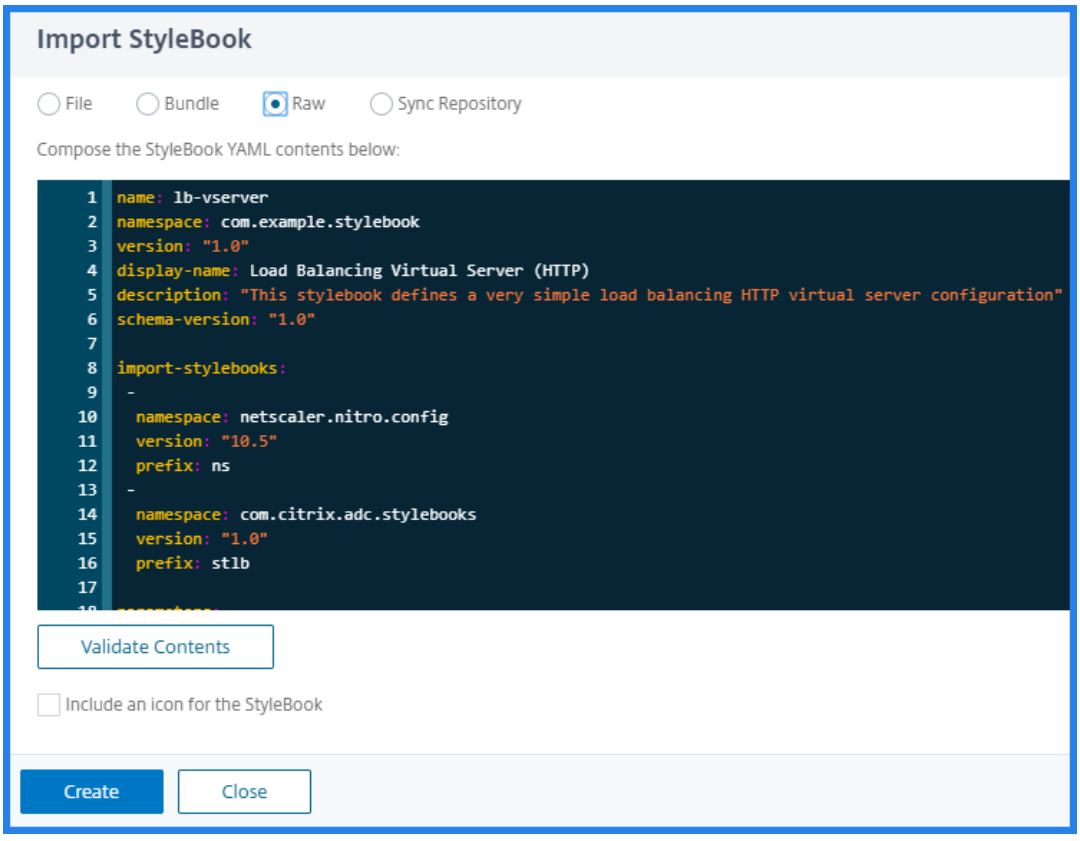
<!--NeedCopy-->
```


- **Raw** -YAML エディタでスタイルブックのコンテンツを作成します。

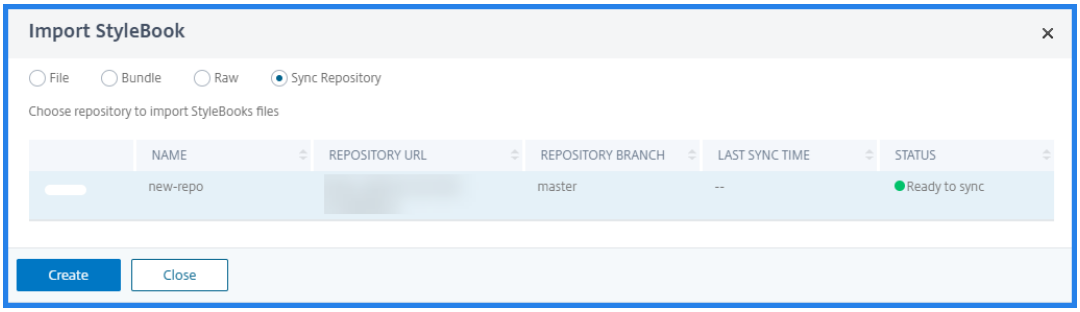
  StyleBook の内容を検証して、StyleBook の文法エラーをチェックできます。StyleBook の内容を検証するには、「内容を検証」をクリックします。

  > 注:
  >
  > StyleBook を作成する際には、次の概念を確認してください。
  >
  > - NITRO API
  > - YAML

  独自の StyleBook を作成する方法について詳しくは、「独自の StyleBook の作成方法」を参照してください。



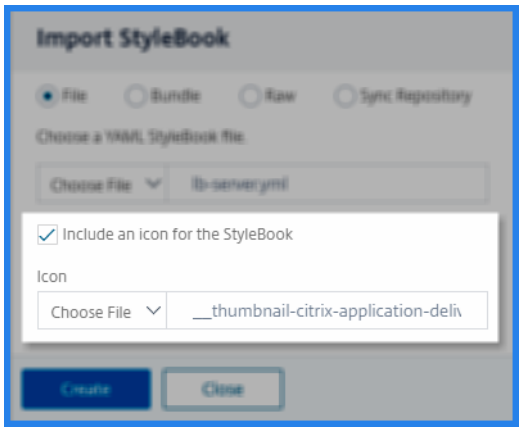
- リポジトリを同期 -このオプションは、ADM に追加されたリポジトリを一覧表示します。ADM と同期するリポジトリを選択します。



> 注:
>
> StyleBook YAML ファイルから YAML エディタにコンテンツをコピーして貼り付けることもできます。

3. 必要に応じて、StyleBook のアイコンを選択します。

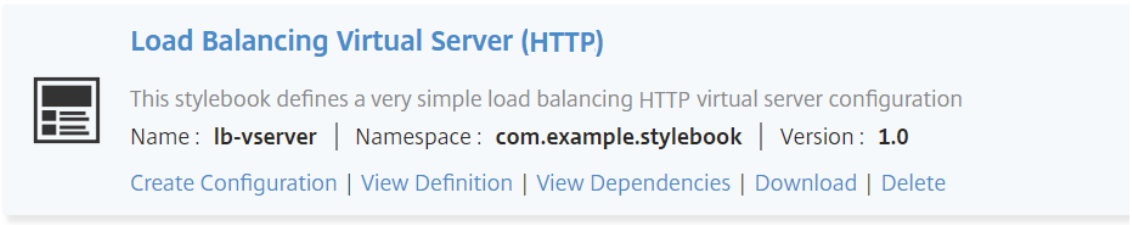
   アプリケーション／ **StyleBook** では、インポートされた StyleBook がこのアイコンとともに表示されます。



4. [作成] をクリックします。

   Citrix ADM は、StyleBook の文法に従って、すべての構文エラーと意味エラーについて StyleBook を検証するようになりました。エラーが発生した場合、StyleBook は Citrix ADM にインポートされません。

   エラーがなければ、StyleBook は正常にインポートされ、**StyleBook** ページにリストされます。StyleBook のヘッダーセクションで定義した表示名で StyleBook を識別できます。



> 注:
>
> ファイルのバンドルをインポートする場合、Citrix ADM は圧縮されたフォルダーを解凍し、すべての StyleBook を検証します。

> 1 つの StyleBook ファイルが検証テストに失敗しても、バンドルはインポートされません。

StyleBook の文法および構文について詳しくは、「スタイルブックの文法」を参照してください。

5. この **StyleBook** から構成を作成するには、「構成の作成」リンクをクリックします。

   StyleBook がユーザーインターフェイスページとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。

6. パラメータに必要な値を指定します。

   次の例では、

   1. アプリケーション名とロードバランサの **IP** アドレスの必須フィールドを指定します。

      a) リストから **LoadBalancing Algorithm** を選択します。デフォルトでは、**ROUNDROBIN** が選択されています。

   ![設定の展開例] (/en-us/citrix-application-delivery-management-service/media/nmas-stylebooks-yaml-editor-4.png)

7. ［ターゲットインスタンス］で、構成を展開する Citrix ADC インスタンスの IP アドレスを選択します。

   ターゲットインスタンスを必要な数だけ指定して、複数の Citrix ADC で構成を展開することもできます。

8. 構成を展開する前に、Citrix ADC（NITRO）構成オブジェクトをテストする場合は、［ドライ実行］をクリックします。

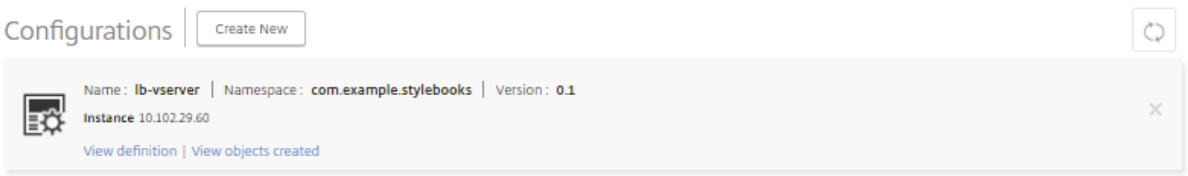
   構成が有効な場合、設定オブジェクトは指定された値に基づいて作成されます。

   この例では、StyleBook はタイプ`lbvserver`のオブジェクトを 1 つだけ作成します。この負荷分散サーバーは、この基本的な例 StyleBook で定義されている唯一のコンポーネントでした。

   その後、［作成］をクリックして、選択した Citrix ADC インスタンスに構成を展開します。

構成を正常に展開すると、[構成] ページに新しい構成パックが表示されます。

> 注
>
> 更新アイコンをクリックして、Citrix ADM で最近検出された Citrix ADC インスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。



カスタムスタイルブックの検索

Citrix ADM では、タイプに基づいて StyleBook を検索できるようになりました。つまり、デフォルトの StyleBook またはカスタム StyleBook のいずれかを検索できるようになりました。このオプションは、多くのデフォルト

StyleBook の中からユーザー定義の StyleBook を検索する必要がある場合に特に便利です。

カスタムスタイルブックを検索するには

1. Citrix ADM で、［アプリケーション］>［構成］>［スタイルブック］に移動します。
2. 右上にある検索アイコンをクリックします。
3. 検索バーで、[種類] を選択し、サブリストから [カスタム] を選択します。
4. Citrix ADM では、ユーザー定義のスタイルブックのみが表示されます。

StyleBook をインポートして、**AutoScale** グループのアプリケーションを構成する

May 7, 2021

ADM のデフォルトの StyleBooks を使用して、ADC AutoScale グループにアプリケーションを設定できます。詳細については、次のリンクを参照してください。

- AWS
- Microsoft Azure

または、独自の StyleBook を作成またはインポートして、アプリケーションを作成することもできます。AutoScale グループ StyleBooks は、従来の StyleBooks に似ています。ただし、ADC Autocale グループとインスタンス上でアプリケーションを設定するための StyleBooks には、いくつかのバリエーションがあります。この記事では、StyleBook ルールについて理解し、AutoScale アプリケーションを構成するのに役立ちます。

開始する前に、ADM で ADC AutoScale グループが作成されていることを確認します。

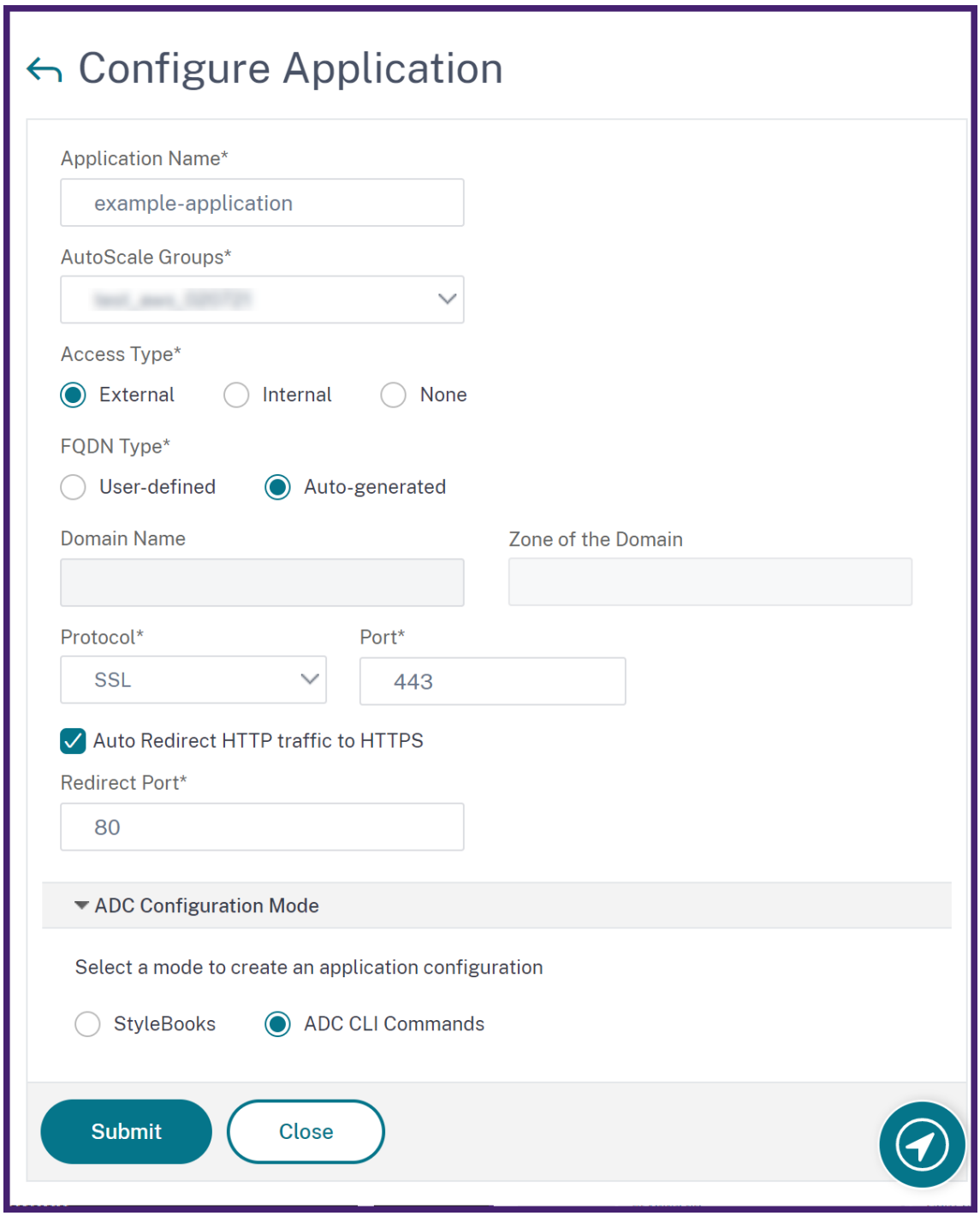
カスタム StyleBook をインポートして AutoScale アプリケーションを構成するには、次の操作を行います。

1. [ネットワーク**] > [AutoScale** グループ] に移動します。
2. 設定する [AutoScale] グループを選択します。
3. [環境設定] をクリックします。
4. 次の詳細を指定します。
    - アプリケーション名 -アプリケーションの名前を指定します。
    - アクセスタイプ -ADM Auto Scaling ソリューションは外部アプリケーションと内部アプリケーションの両方に使用できます。必要なアプリケーションアクセスタイプを選択します。
    - **FQDN** タイプ -ドメイン名とゾーン名を割り当てるモードを選択します。

      手動で指定する場合は、[ユーザー定義] を選択します。ドメイン名とゾーン名を自動的に割り当てるには、[自動生成] を選択します。

- ドメイン名 -アプリケーションのドメイン名を指定します。このオプションは、[ユーザー定義 FQDN タイプ] を選択した場合にのみ適用されます。
- **[** ドメインのゾーン]: リストからアプリケーションのゾーン名を選択します。このオプションは、[ユーザー定義 FQDN タイプ] を選択した場合にのみ適用されます。

  このドメイン名とゾーン名は、Azure の仮想サーバーにリダイレクトされます。たとえば、`app.example.com`でアプリケーションをホストする場合、`app`はドメイン名、`example.com`はゾーン名です。
- **Protocol**： リストからプロトコルタイプを選択します。設定されたアプリケーションは、選択したプロトコルタイプに応じてトラフィックを受信します。
- [ポート]: ポート値を指定します。指定されたポートは、アプリケーションと Autosale グループ間の通信を確立するために使用されます。



5. 「**StyleBook** を選択」をクリックします。
6. 「**StyleBook** を選択」ページで、「新規 **StyleBook** を読み込む」をクリックします。
   読み込みオプションの詳細については、「StyleBook のインポートと使用」を参照してください。

AutoScale グループ StyleBooks には、いくつかの必須パラメータがあります。次の属性リストでは、AutoScale グループと従来の StyleBooks のバリエーションについて説明します。

- **Type** -ヘッダーセクションで、値:autoscaleを持つtype属性を含めます。

```
type: autoscale
<!--NeedCopy-->
```

この属性により、StyleBook は ADC Autocale グループでのアプリケーションの設定にのみ使用されます。また、**StyleBook** がアプリケーション／ **StyleBook** のリストに表示されないように制限します。

次に、AutoScale グループ StyleBook のヘッダーの例を示します。

```
name: autoscale-params
namespace: com.citrix.adc.commontypes
version: "1.0"
description: "This StyleBook defines the parameters required for
    Autoscale Deployment"
display-name: "Autoscale Parmeters StyleBook"
private: true
type: autoscale
schema-version: "1.0"
<!--NeedCopy-->
```

- アプリケーション名 -このパラメータは、アプリケーションの名前と説明を記述します。ADM GUI にパラメータを表示するラベルフィールドを指定します。このフィールドは文字列型です。

```
-
    name: app_name
    label: "Application Name"
    description: "Name of the Application"
    type: string
    key: true
    gui:
      updatable: false
      required: true
<!--NeedCopy-->
```

- 仮想 **IP** アドレス -このパラメータは、仮想サーバーの IP アドレスを記述します。[AutoScale] 領域では、このパラメータが自動的に更新されます。

```
-
    name: ip_address
    label: "IP Address of the LoadBalancer"
    description: "IP Address of the LoadBalancer"
    type: ipaddress
    gui:
      hidden: true
<!--NeedCopy-->
```


- **IPSet** -アプリケーションをデプロイすると、各アベイラビリティーゾーンのクラスターにIPsetが作成されます。
  - AWS では、ドメインとインスタンスの IP アドレスが DNS/NLB に登録されます。
  - Azure では、ドメインとインスタンスの IP アドレスは、Azure トラフィックマネージャーまたは ALB に登録されます。

  StyleBook では、IP アドレスまたは IP セットを、AutoScale グループで指定できます。

```
-
    name: ipset
    label: "IPSet"
    description: "Configuration for network ipset resource"
    type: string
    gui:
      hidden: true
<!--NeedCopy-->
```

Citrix ADM にファイルをアップロードするスタイルブックを作成する

May 7, 2021

Citrix Application Delivery Management（Citrix ADM）スタイルブックでは、Citrix ADC M GUI または API を使用して、ローカルファイルシステムから Citrix ADC インスタンスに任意の種類のファイルをアップロードする際に、さまざまな種類の Citrix ADC 構成を作成できます。これらのファイルには、サンプル証明書ファイルまたはジオロケーションファイルを使用できます。これらのファイルをアップロードするディレクトリを指定することもできます。

スタイルブックの設定

以下は、Citrix ADC インスタンスで地理位置情報ファイルをアップロードする方法を説明した StyleBook の例です。地理ファイルは、地理的位置に基づいて静的近接を定義するために、GSLB 設定で通常使用されます。

StyleBook を構築する-1

```
name: upload-geolocations
namespace: com.citrix.adc.stylebooks.samples
version: "1.0"
display-name: GeoLocation File Upload
```



```
description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
schema-version: "1.0"

import-stylebooks:
-
 namespace: netscaler.nitro.config
 version: "11.1"
 prefix: ns

parameters:
-
 name: locationfile
 label: Location File
 description: The system file path of the geolocation file on Citrix
    ADM
 type: file
 required: true

components:
-
 name: upload-file-comp
 type: ns::systemfile
 properties:
    filename: $parameters.locationfile.filename
    filelocation: "/var/netscaler/inbuilt_db/"
    filecontent: base64.encode($parameters.locationfile.contents)
<!--NeedCopy-->
```

> 注:
>
> この例で使用されるパラメータは、タイプファイルです。この StyleBook を Citrix ADM にインポートして、ジオロケーションファイルをアップロードできます。

この StyleBook では、ファイルが Citrix ADM にすでに存在している必要があります（たとえば、SCP などのユーティリティを使用して Citrix ADM にコピー済みなど）。
Citrix ADM ファイルシステムにファイルをコピーせずに、Citrix ADM 経由で Citrix ADC にファイルをアップロードする場合は、2 つの「文字列」パラメータを持つ StyleBook を構築できます。1 つは Citrix ADC で使用するファイル名を指定し、もう 1 つは Citrix ADC の内容を指定するものです。ファイルを作成し、upload-file-comp コンポーネントでこれら 2 つのパラメータを使用します。以下は、地理位置ファイルをアップロードする代替の StyleBook です。

あなたのスタイルブックを作成する**-2**


```
name: upload-geolocations-alt
namespace: com.citrix.adc.stylebooks.samples
version: "1.0"
display-name: GeoLocation File Upload
description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "11.1"
  prefix: ns

parameters:
 -
  name: filename
  label: Location Filename
  description: The name of the location file on the Citrix ADC
  type: string
  required: true
 -
  name: filecontents
  label: Location File Contents
  description: The contents of the location file
  type: string
  required: true

components:
 -
  name: upload-file-comp
  type: ns::systemfile
  properties:
   filename: $parameters.filename
   filelocation: "/var/Citrix ADC/inbuilt_db/"
   filecontent: base64.encode($parameters.filecontents)
<!--NeedCopy-->
```

ファイルをアップロードするための設定を作成する

以下の手順では、選択した Citrix ADC インスタンスに構成を作成し、上記の最初の StyleBook を使用してジオロケーションファイルをアップロードします。

ファイルをアップロードするための設定を作成するには:

1. Citrix ADM で、［アプリケーション］>［構成］の順に選択し、［新規作成］をクリックします。［スタイルブックの選択］ページには、Citrix ADM で使用可能なすべてのスタイルブックが表示されます。下方向にスクロールして、インポートした StyleBook を選択します。

   StyleBook パラメータは、この StyleBook で定義されているすべてのパラメータの値を入力できるユーザーインタフェースページとして表示されます。

2. ロードバランサーの名前と仮想 IP アドレスを基本ロードバランサーの設定セクションに入力します。
3. [ロケーションファイル] セクションで、ファイルの名前または場所を入力します。

   > 注:
   >
   > Citrix ADM では、ファイルが現在のテナントのフォルダーにのみ配置されていることを確認します。任意の FTP を使用してファイルを Citrix ADM ファイルシステムにコピーします。

4. ターゲットインスタンスにアクセスする前に、ユーザー認証情報を入力するように求められる場合があります。
5. 構成を作成する対象の Citrix ADC インスタンスを選択し、［作成］をクリックします。

> 注:
>
> インスタンスで実際の構成を実行する前に、［**Dry Run** ］を選択して、ターゲットインスタンスに作成された構成オブジェクトを確認することをお勧めします。

構成パックが正常に作成されると、ファイルは Citrix ADC インスタンスファイルシステムの /var/netscaler/inbuilt_db/ という場所に保存されます。

> 注
>
> 更新アイコンをクリックして、Citrix ADM で最近検出された Citrix ADC インスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。

Citrix ADM API を使用した構成パックの作成

Citrix ADM API を使用して、選択した Citrix ADC インスタンスにファイルをアップロードする構成パックを作成することもできます。API の使用方法の詳細については、「あらゆるファイルタイプをアップロードするための構成を API を使用して作成する方法」を参照してください。

SSL 証明書と証明書キーファイルを **Citrix ADM** にアップロードするスタイルブックを作成する

May 7, 2021

SSL プロトコルを使用する StyleBook の構成を作成する場合、SSL 証明書ファイルと証明書キーファイルを StyleBook パラメーターの要求に応じてアップロードする必要があります。StyleBook では、Citrix Application Delivery Management（ADM）GUI を使用して、ローカルシステムから SSL ファイルとキーファイルを直接アップロードできます。Citrix ADM API を使用して、Citrix ADM によってすでに管理されている証明書ファイルとキーファイルをアップロードすることもできます。

スタイルブックの設定

このドキュメントは、SSL 証明書とキーファイルをアップロードするためのコンポーネントを備えた独自の StyleBook- 負荷分散仮想サーバー（**SSL**）
を作成する際に役立ちます。ここで紹介する StyleBook は、選択した Citrix ADC インスタンス上に基本的な負荷分散仮想サーバー構成を作成します。この構成は SSL プロトコルを使用します。この StyleBook を使用して構成を作成するには、仮想サーバーの名前と IP アドレスを指定し、負荷分散方式パラメータを選択し、仮想サーバーの証明書ファイルと証明書キーファイルをアップロードするか、すでに証明書ファイルと証明書キーファイルを使用する必要があります。Citrix ADM に存在します。これらは下記のとおり、「parameters」セクションで指定されます。

```
parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: certificate
  label: "SSL Certificate File"
  description: "The file name of the SSL certificate file"
  type: certfile
 -
  name: key
  label: "SSL Certificate Key File"
  description: "The file name of the server certificate's private key
     file"
  type: keyfile
```



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

下記のとおり、StyleBook のコンポーネントセクションに 2 つのコンポーネントが作成されます。`my-lbvserver-comp`コンポーネントの型は nsの lbvserver です。

- 「ns」は、インポートスタイルブックセクションで指定した、組み込みの名前空間 netscaler.nitro.config およびバージョン 10.5 を参照する接頭辞です。
- `lbvserver`は、この名前空間に組み込みの StyleBook です。これは、同じ名前の Citrix ADC NITRO `lbvserver` リソースに対応します。

2 番目のコンポーネント`lbvserver-certificate-comp`はタイプ`stlb::vserver-certs-binds`です。プレフィックス`stlb`は、StyleBook のインポートスタイルブックセクションで指定されている名前空間「com.citrix.adc.stylebooks」とバージョン 1.0 を指します。「com.citrix.adc.stylebooks」名前空間をフォルダと考えることができる場合、そのフォルダには別の StyleBook（またはファイル）`vserver-certs-binds`があります。名前空間「com.citrix.adc.stylebooks」にあるスタイルブックは、Citrix ADM の一部として出荷されます。

ユーザー定義の`vserver-certs-binds`StyleBook で使用される StyleBook を使用すると、証明書とキーファイルをターゲットの Citrix ADC インスタンスにアップロードし、証明書とキーファイルを適切な仮想サーバーにバインドして構成することで、証明書を簡単に構成できます。このコンポーネントのプロパティーは、lb 仮想サーバーの名前と、構成パックの作成時に提供する SSL 証明書の名前です。

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name
   servicetype: SSL
   ipv46: $parameters.ip
   port: 443
   lbmethod: $parameters.lb-alg
 -
  name: lbvserver-certificate-comp
  type: stlb::vserver-certs-binds
  description: Binds lbvserver with server certificate
  properties:
   vserver-name: $components.my-lbvserver-comp.properties.name
   certificates:
    -
     cert-name: $parameters.name + "-lb-cert"
     cert-file: $parameters.certificate
     ssl-inform: PEM
     key-name: $parameters.name + "-key"
     key-file: $parameters.key
```



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

API を使ってこういった StyleBook から構成を作成する場合は、ファイル名だけを使うようにしてください（フルファイルパスではなく）。これらのファイルは、Citrix ADM 証明書およびキーファイルフォルダーにすでに入手可能であることが予想されます。アップロードされた SSL 証明書ファイルは、Citrix ADM 上の/var/mps/テナント/…/ns_ssl_certs ディレクトリに保存され、SSL 証明書キーファイルは /var/mps/テナント/…/ns_ssl_keys ディレクトリ Citrix ADM。

SSL ファイルをアップロードするための設定を作成する

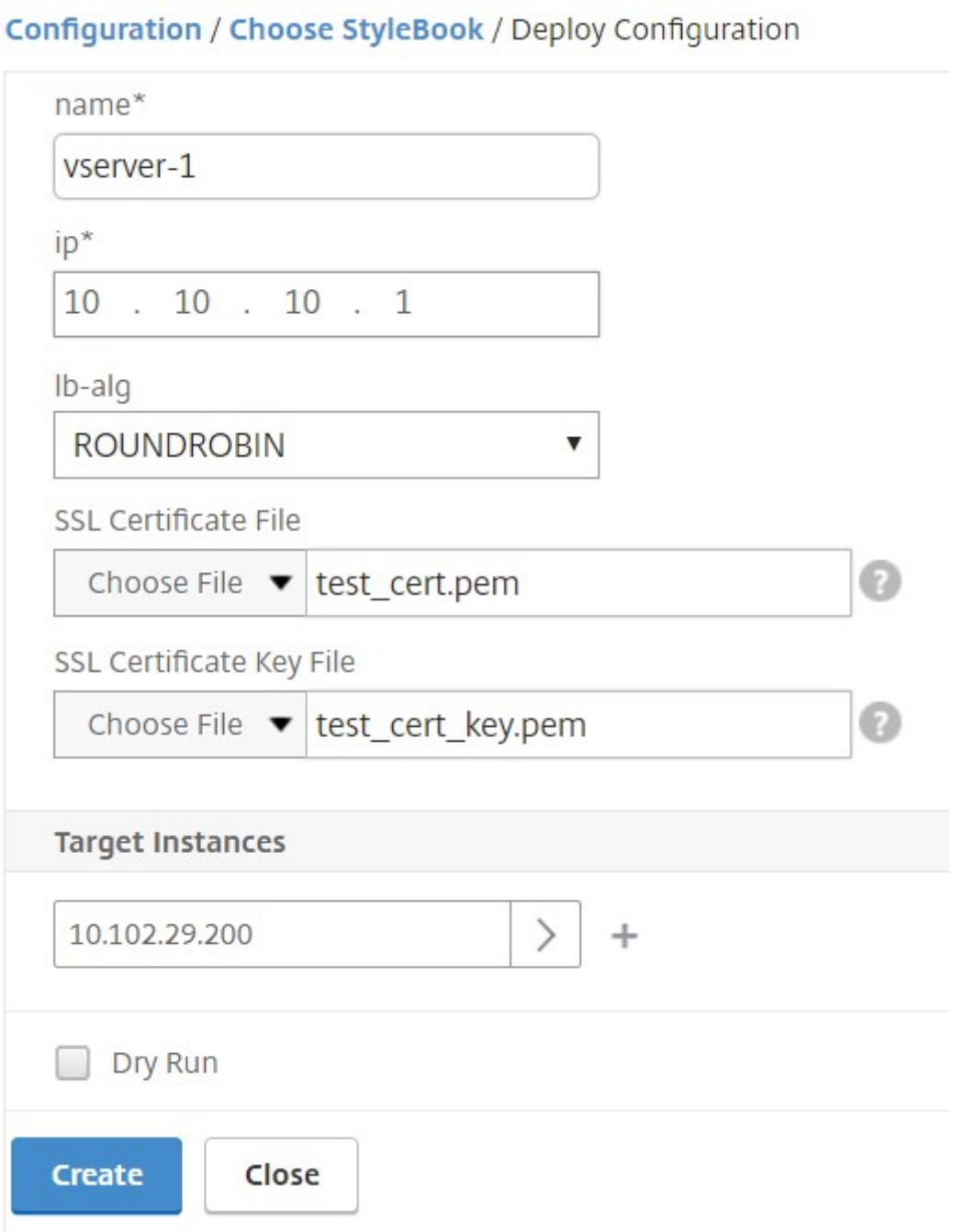
以下の手順では、上記の StyleBook の SSL プロトコルを使用して、選択した Citrix ADC インスタンス上に基本的な負荷分散仮想サーバー構成を作成します。この手順を使用して、Citrix ADM で SSL 証明書ファイルと証明書キーファイルをアップロードできます。

ファイルをアップロードするための設定を作成するには:

1. Citrix ADM で、［アプリケーション］>［構成］**>**［スタイルブック］に移動します。［スタイルブック］ページには、Citrix ADM で使用可能なすべてのスタイルブックが表示されます。
2. 下にスクロールして、[負荷分散仮想サーバー **(SSL)**] を選択するか、検索フィールドに [負荷分散仮想サーバー **(SSL)**] と入力し、**Enter** キーを押します。
3. StyleBook パネルで「設定を作成」リンクをクリックします。

   StyleBook パラメータは、この StyleBook で定義されているすべてのパラメータの値を入力できるユーザーインタフェースページとして表示されます。
4. ロードバランサーの名前と仮想 IP アドレスを基本ロードバランサーの設定セクションに入力します。
5. [**SSL** 証明書の設定] セクションで、ローカルストレージフォルダからそれぞれのファイルを選択します。または、Citrix ADM 自体に存在するファイルを選択することもできます。
6. 構成を作成する対象の Citrix ADC インスタンスを選択し、［作成］をクリックします。

> 注
>
> 更新アイコンをクリックして、Citrix ADM で最近検出された Citrix ADC インスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。



注:

Citrix ADM では、Citrix ADM の一部として出荷される次のデフォルトの StyleBook を使用すると、SSL 証明書とキーをアップロードして SSL サポートを作成できます。

- HTTP/SSL 負荷分散 StyleBook（lb）
- HTTP/SSL 負荷分散（モニタ付き）StyleBook (`lb-mon`)
- HTTPS/SSL コンテンツスイッチ付きアプリケーション (`cs-lb-mon`)

> - CS、LB、SSL 機能を使用したサンプルアプリケーション StyleBook（sample-cs-app）
>
> 上記の StyleBook で説明されたものと同じ方法で SSL 証明書を使用する、ご自身の StyleBook を作成することも可能です。

スタイルブックを構築する

lb-vserver-ssl.yaml ファイルのすべての内容を次に示します。

```
name: lb-vserver-ssl
description: "This stylebook defines a load balancing virtual server
   configuration."
display-name: "Load Balancing Virtual Server (SSL)"
namespace: com.example.ssl.stylebooks
schema-version: "1.0"
version: "0.1"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
 -
  namespace: com.citrix.adc.stylebooks
  prefix: stlb
  version: "1.0"

parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: certificate
```



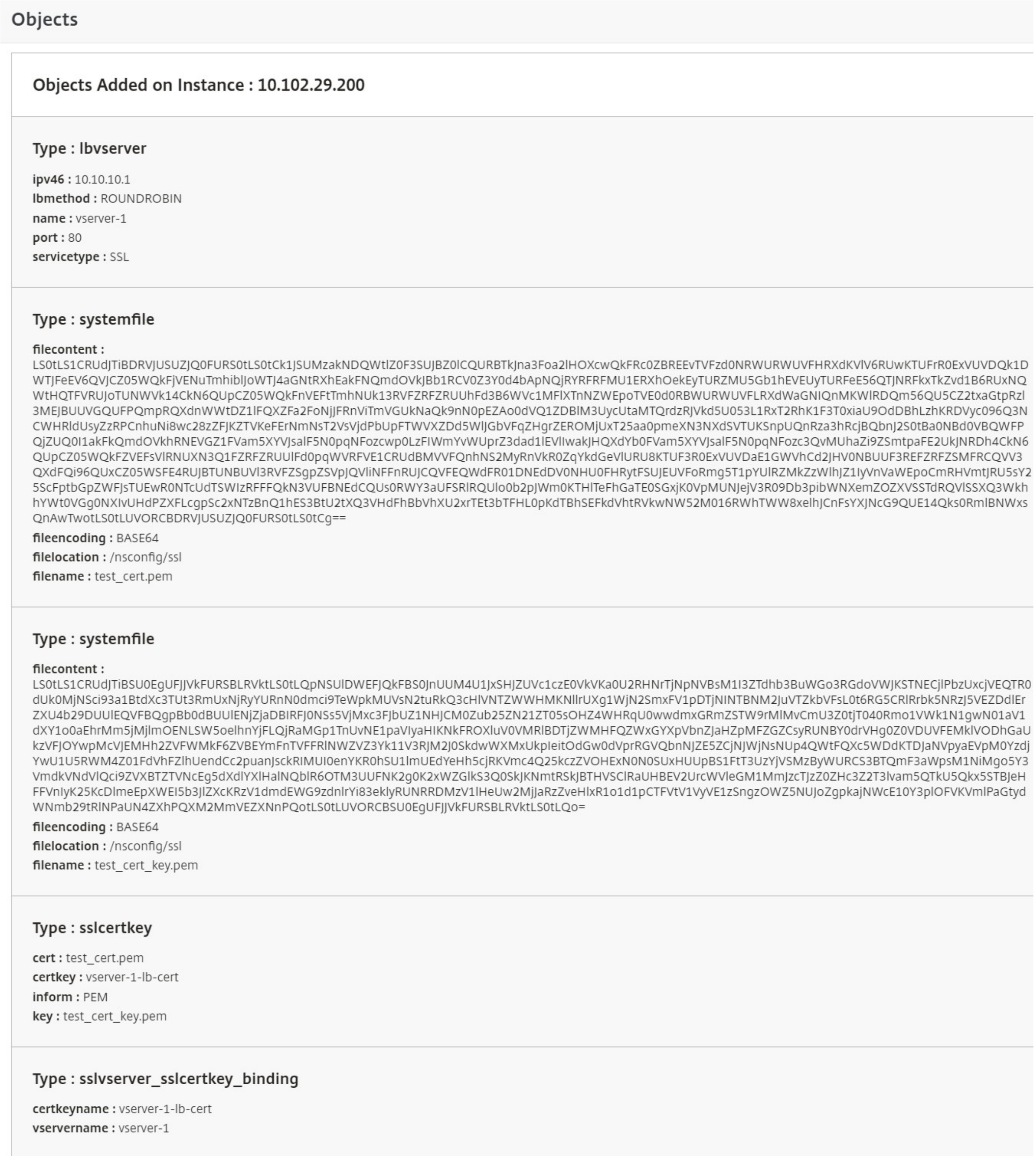
```
36    label: "SSL Certificate File"
37    description: "The file name of the SSL certificate file"
38    type: certfile
39   -
40    name: key
41    label: "SSL Certificate Key File"
42    description: "The file name of the server certificate's private key
          file"
43    type: keyfile
44
45  components:
46   -
47    name: my-lbvserver-comp
48    type: ns::lbvserver
49    properties:
50      name: $parameters.name
51      servicetype: SSL
52      ipv46: $parameters.ip
53      port: 443
54      lbmethod: $parameters.lb-alg
55   -
56    name: lbvserver-certificate-comp
57    type: stlb::vserver-certs-binds
58    description: Binds lbvserver with server certificate
59    properties:
60     vserver-name: $ components.my-lbvserver-comp.properties.name
61     certificates:
62      -
63       cert-name: $parameters.name + "-lb-cert"
64       cert-file: $parameters.certificate
65       ssl-inform: PEM
66       key-name: $parameters.name + "-key"
67       key-file: $parameters.key
68  <!--NeedCopy-->
```

Citrix ADM API を使用して構成パックを作成する:

Citrix ADM API を使用して、選択した Citrix ADC インスタンスに証明書ファイルとキーファイルをアップロードする構成パックを作成することもできます。API の使用方法の詳細については、「[API を使用して証明書とキーファイルをアップロードする設定を作成する方法。]」を参照してください。(/en-us/citrix-application-delivery-management-service/stylebooks/how-to-use-api-to-create-configuration-from-stylebooks/how-to-use-api-to-create-configurations-to-upload-cert-and-key-files.html)

Citrix ADC インスタンスに定義されているオブジェクトの表示

Citrix ADM で StyleBook 構成（構成パック）を作成したら、［作成されたオブジェクトの表示］をクリックして、ターゲットの Citrix ADC インスタンスで作成されたすべての Citrix ADC オブジェクトを表示します。



StyleBook で定義された仮想サーバーでの分析の有効化とアラームの設定

May 7, 2021

操作コンストラクトを使用して、Citrix Application Delivery Management（ADM）分析を構成して、StyleBook の一部である仮想サーバーコンポーネントによって処理されるトラフィックトランザクションの全部または一部のトラフィックトランザクションで AppFlow レコードを収集できます。また、このような操作構成を使用して、アラームを構成し、仮想サーバーが管理するトラフィックの詳細な情報を取得できます。

次の例は、StyleBook の Operations セクションを示しています。

```
operations:
  analytics:
   -
    name: lbvserver-ops
    properties:
      target: $components.basic-lb-comp
      filter: HTTP.REQ.URL.CONTAINS("catalog")
  alarms:
   -
    name: lbvserver-alarm
    properties:
      target: $components.basic-lb-comp
      email-profile: $parameters.emailprofile
      sms-profile: "MyProdSMS"
      rules:
       -
         metric: "total_requests"
         operator: "greaterthan"
         value: 25
         period-unit: $parameters.period
       -
         metric: "total_bytes"
         operator: "lessthan"
         value: 60
         period-unit: "day"
<!--NeedCopy-->
```

分析セクションの属性は、Citrix ADM 分析機能に、ターゲットプロパティによって識別される仮想サーバーコンポーネント上の AppFlow レコードを収集するように指示するために使用されます。オプションで、Citrix ADM ポリシー式を受け入れるフィルタプロパティを指定して、仮想サーバーで収集される AppFlow レコードに対する要求をフィルタリングすることもできます。

この StyleBook から構成パックを作成すると、Citrix ADM 分析機能は、構成パックの作成プロセスで仮想サーバー

が作成されたときに指定された AppFlow レコードを収集するように構成されます。

alarms セクションの属性は、アラーム生成のしきい値を設定し、ターゲットプロパティが指定する仮想サーバーの通知を送信するために使用されます。上記の例では、電子メールプロファイルと SMS プロファイルのプロパティは、通知を送信する必要がある場所を指定するために使用されます。rules セクションはしきい値を定義します。たとえば、ユーザーが定義した期間に、仮想サーバーが処理する要求の合計が 25 件を超えた場合、アラームが設定され、通知が送信されます。「period-unit」はアラームをトリガーする頻度を指定します。これは、日、時間、または毎週の値を取ることができます。

測定基準値としきい値の比較を用いる場合、次の演算子を使用できます。

- `greaterthan` 対象: >
- `lessthan` 対象: <
- `greaterthanequal` 対象: >=
- `lessthanequal` 対象: <=

StyleBook では、メトリックスに API 名が使用され、Citrix ADM 分析 GUI に表示される名前は使用されません。

構成パックの一部として作成された仮想サーバーで収集されたデータを表示および分析する方法については、Citrix ADM Analytics のドキュメントを参照してください。

インスタンスロール

May 7, 2021

Citrix Application Delivery Management（ADM）では、1 つのアプリケーションに対して複数の Citrix ADC インスタンスを構成する必要がある場合がありますが、各 ADC インスタンスで異なる構成を展開する必要がある場合もあります。このような場合の例は、Microsoft Skype for Business スタイルブックのデフォルトです。

StyleBooks は現在、構成パックを作成し、複数の Citrix ADC インスタンスに同じ構成を適用する機能をサポートしています。構成がすべての ADC インスタンスで同一であるようなシナリオを対称構成と呼ぶことができます。

StyleBooks の「インスタンスロール」機能を使用すると、非対称構成、つまり複数の ADC インスタンスに適用できる構成パックを作成できますが、異なる ADC インスタンスには異なる構成を使用できます。

インスタンスロール機能を備えた StyleBook を使用して構成パックを作成すると、構成パック内の各 ADC インスタンスに異なるロールを割り当てることができます。このロールは、ADC インスタンスが受け取る設定パックの設定オブジェクトを決定します。

注意事項**:**

- StyleBook のインスタンスロールのセットは、StyleBook の作成時に定義されます。
- ロールは、構成パックを作成または更新するときに、特定の ADC インスタンスに割り当てられます。

「ターゲットロール」セクション

StyleBook に「ターゲットロール」と呼ばれる新しいセクションが導入され、StyleBook でサポートされているすべてのロールが宣言されています。

このセクションは通常、StyleBook の「Import-StyleBooks」セクションの後とパラメータセクションの前に配置されます。

次の StyleBook の例では、「target-roles」セクション内で A と B の 2 つのロールが定義されています。

```
target-roles:

  -
   name: A
   name: B
     min-targets: 2
     max-targets: 5
<!--NeedCopy-->
```

ロール B は、min-target と max-target という 2 つのオプションのサブプロパティも定義していることがわかります。

これらの 2 つのサブプロパティはオプションですが、最小ターゲットは、この StyleBook から構成パックを作成するときにこのロールを割り当てる ADC インスタンスの最小必須数を指定します。max-targets は、構成パックの作成時にこのロールを割り当てることができる ADC インスタンスの最大数を指定しますこの StyleBook から。

これらのサブプロパティが指定されていない場合、そのロールに設定できる ADC インスタンスの数に制限はありません。min-targets = 0 の場合、そのロールに関連付けられた設定はオプションであり、min-targets = 1 の場合、その設定は必須であり、そのロールに対して少なくとも 1 つの ADC インスタンスを設定する必要があります。

ロール「デフォルト」

明示的に定義されたロールに加えて、すべての StyleBook が持つ暗黙的なロールがあり、そのロールはデフォルトロールとして呼び出されます。このロールは、StyleBook の他のロールと同様に使用できます。設定パックを作成するときに、ADC インスタンスに特定のロールが割り当てられていない場合、インスタンスは「デフォルト」ロールに暗黙的に割り当てられます。インスタンスは、「default」ロールを持つコンポーネントによって生成された設定オブジェクトを受け取ります。

ロールを持つコンポーネント

StyleBook がサポートできるロール（ロール「デフォルト」を含む）を定義すると、StyleBook のコンポーネントセクションでそのロールを使用できます。コンポーネントを特定の役割を果たす ADC インスタンスにのみデプロイする場合は、次のコンポーネントの例に示すように、コンポーネントの一部として roles 属性を指定できます。


```
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
<!--NeedCopy-->
```

上記の例では、コンポーネントが`lbvserver`を生成し、ロール A のインスタンスにデプロイされます。コンポーネントの roles 属性はリストであり、コンポーネントに複数のロールを割り当てることができます。これらのロールは、StyleBook の「ターゲットロール」セクションで宣言されているでしょう。

注：StyleBook のコンポーネントでロール属性が指定されていない場合、コンポーネントによって生成された構成オブジェクトは、その役割に関係なく、すべての Citrix ADC インスタンスに作成されます。この機能を効果的に使用して、構成パックのすべてのインスタンスに適用できる設定オブジェクトを作成できます。

A と B の 2 つのロールが定義され、4 つのコンポーネントを含む StyleBook があるとします。

- コンポーネント C1 にはロール A と B があります。
- コンポーネント C2 にはロール B があります。
- コンポーネント C3 にはロールが定義されていません
- コンポーネント C4 には「デフォルト」というロールがあります

この StyleBook のコンポーネントセクションを以下に示します。

```
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
```



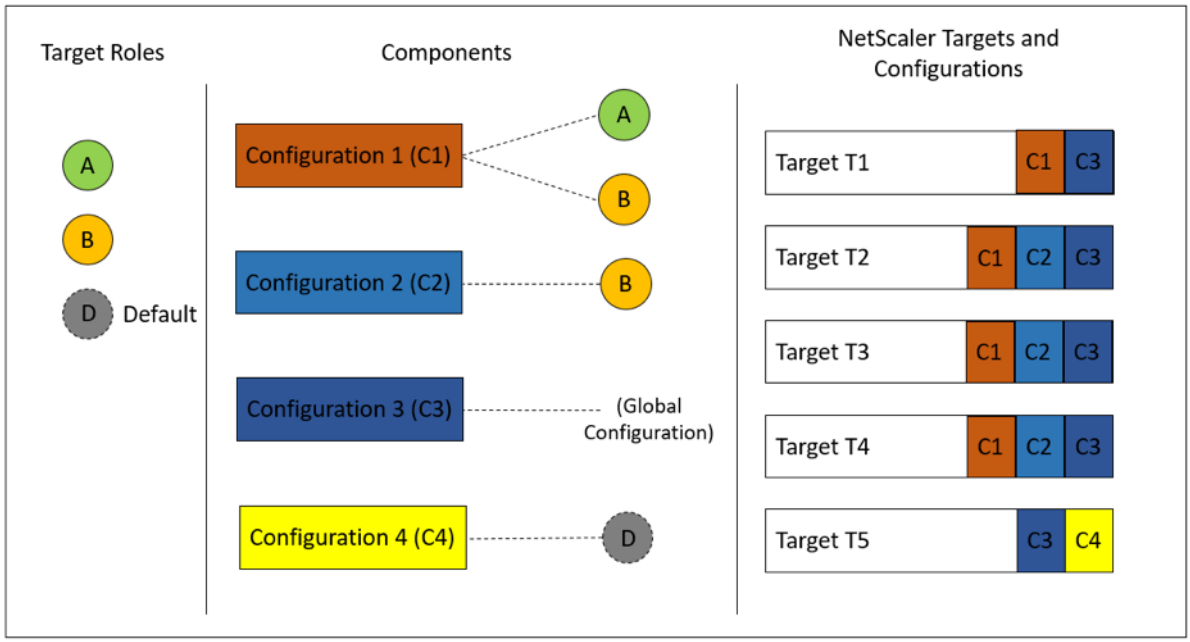
```
17        - B
18      properties:
19        name: lb2
20        servicetype: HTTP
21        ipv46: 12.12.12.12
22        port: 80
23    -
24      name: C3
25      type: ns::lbvserver
26      properties:
27        name: lb3
28        servicetype: HTTP
29        ipv46: 13.13.13.13
30        port: 80
31    -
32      name: C4
33      type: ns::lbvserver
34      roles:
35        - default
36      properties:
37        name: lb4
38        servicetype: HTTP
39        ipv46: 14.14.14.14
40        port: 80
41  <!--NeedCopy-->
```

コンポーネント C3 にはロールが定義されていないことに注意してください。つまり、コンポーネントはそのロールに関係なくすべてのインスタンスにデプロイされます。一方、コンポーネント C4 には「default」というロールがあります。つまり、明示的なロールが割り当てられていないインスタンスに適用されます。

ここで、この StyleBook を使用して構成パックを作成し、5 つの ADC インスタンスにデプロイすることを検討します。この段階では、次の方法でインスタンスにロールを割り当てることができます。

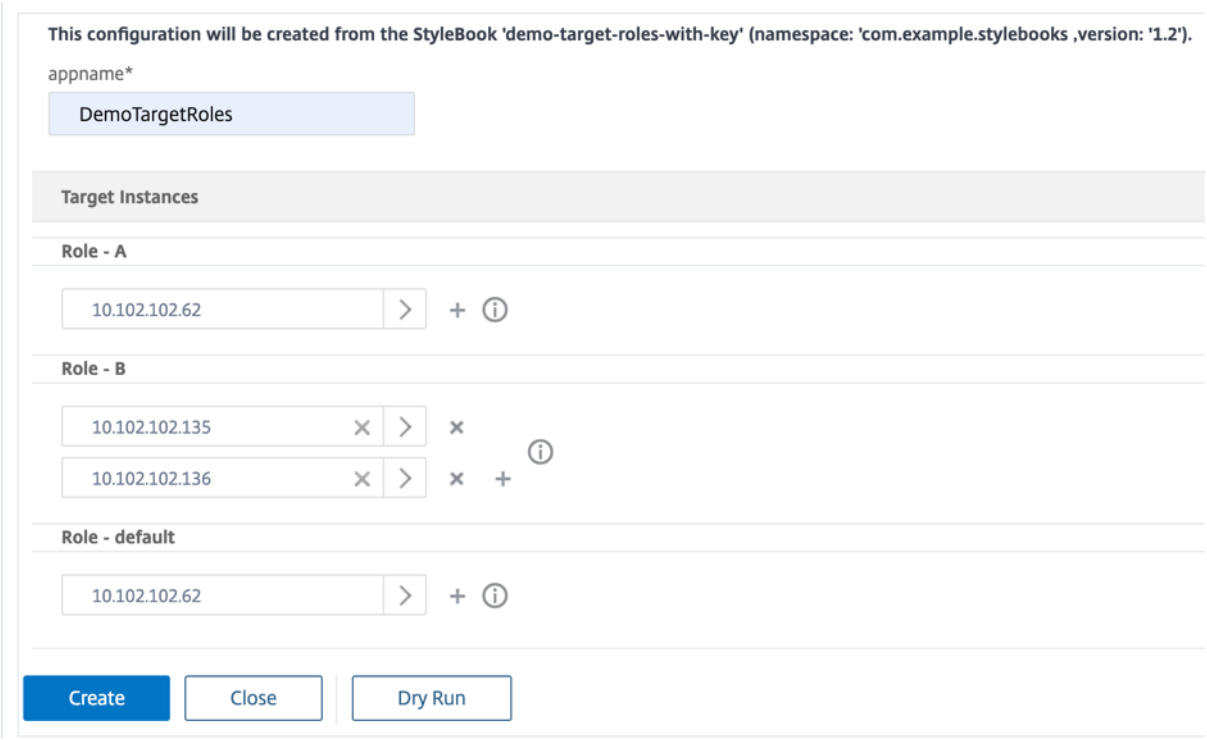
- ロール A はインスタンス T1、T2、T3、および T4 に割り当てられます。
- ロール B はインスタンス T2、T3、および T4 に割り当てられます。
- インスタンス T5 にはロールが割り当てられていません

次の図は、役割の割り当てをまとめたもので、各 ADC インスタンスが受け取る構成を示しています。



コンポーネント C3 は、ロールに関係なくすべてのインスタンスにデプロイされます。これは、このコンポーネントには roles 属性がないためです。

次の図は、サンプル構成パックを作成するときのロールの割り当てを示しています。



構成パックの作成時に「Dry Run」機能を使用して、各 ADC インスタンスに作成されるロールと設定オブジェクトの正しい割り当てを表示および検証することもできます。

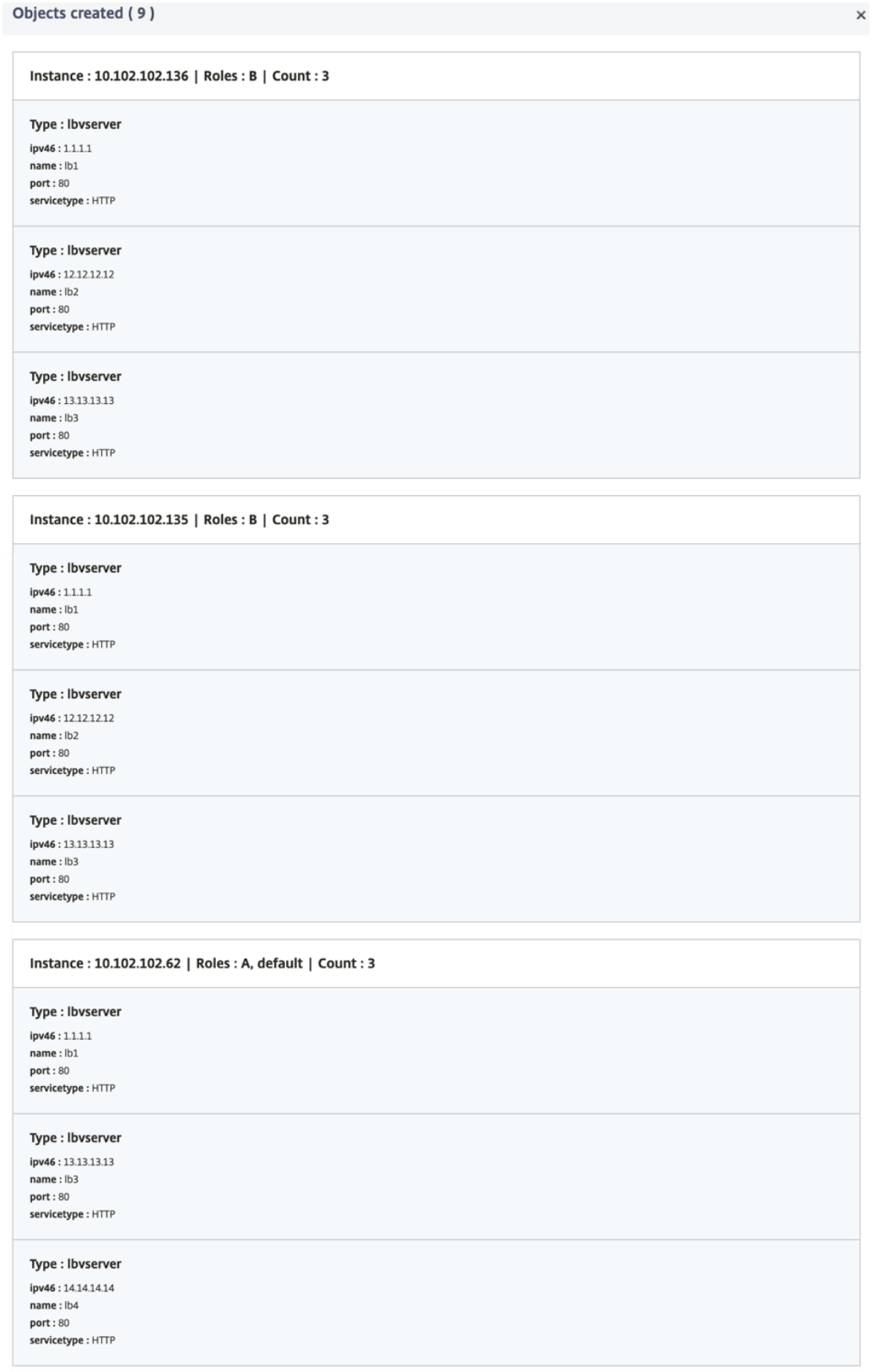
スタイルブックを構築する

StyleBook「デモターゲットロール」の全コンテンツを以下に示します。

```
---
name: demo-target-roles
namespace: com.example.stylebooks
version: "1.2"
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: appname
    type: string
    required: true
    key: true
target-roles:
  -
    name: A
  -
    name: B
    min-targets: 2
    max-targets: 5
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
```

```
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
      port: 80
<!--NeedCopy-->
```

次の図は、サンプル構成パック用に作成されたオブジェクトを示しています。



API の使用

REST API を使用する場合、次のように設定パックを作成または更新するときに、各 ADC インスタンスに対してロールを指定できます。[targets] ブロックで、個々のコンポーネントをデプロイする特定の Citrix ADC インスタンスの UUID を指定します。

```
"targets": [
            {

             "id": "<ADC-UUID>",
             "roles": ["A"]
             }
 ,
           ]
<!--NeedCopy-->
```

参考のために、完全なサンプル REST API が提供されています。

POST /<ADM-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks

```
{

  "configpack": {

     "parameters": {

     "appname": "app1"
     }
 ,
     "targets": [
        {

          "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",
        "roles": ["A"]
         }
 ,
        {

          "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",
          "roles": ["A", "B"]
         }
 ,
        {

          "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",
```

```
26             "roles": ["A", "B"]
27           }
28  ,
29          {
30
31             "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
32             "roles": ["A", "B"]
33           }
34  ,
35          {
36
37             "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
38             "roles": ["default"]
39           }
40
41        ]
42       }
43
44  }
45
46  <!--NeedCopy-->
```

StyleBook を作成して非 CRUD 操作を実行する

May 7, 2021

StyleBook は、Citrix ADC インスタンス上で必要な構成オブジェクトを計算することによって、Citrix ADC 構成を管理します。これらのオブジェクトは、ConfigPack を作成または更新するたびに、インスタンスから追加、更新、または削除されます。つまり、「望ましい状態」を指定するときです。

ただし、一部の Citrix ADC 構成オブジェクトは、作成、更新、削除（CRUD 操作）以外のいくつかの操作をサポートしています。たとえば、ロードバランサーオブジェクト（`lbvserver`）または Citrix ADC 機能オブジェクト（`nsfeature`）は、「有効化」または「無効」操作をサポートできます。同様に、Citrix ADC`certkeys`では、証明書を別の証明書にリンクまたはリンク解除するための「リンク」および「リンク解除」操作がサポートされています。Citrix ADC オブジェクトに対するこれらの操作は、非 CRUD 操作と呼ばれます。このセクションでは、StyleBook を使用して、それらをサポートする設定オブジェクトに対して非 CRUD 操作を実行する方法について説明します。

> 注:
>
> 設定オブジェクト間のバインド (たとえば、`certkey` を`lbvserver`にバインド) は、非 CRUD 操作とは見なされません。これは、NITRO バインディングが独自の構成オブジェクトとして表現されるためです。これらのオブジェクトは、他の Citrix ADC 構成オブジェクトと同様に作成および削除されます。

非 **CRUD** 操作のサポート

「meta-properties」と呼ばれる新しい構造が、「properties」構造と同じレベルでコンポーネントに追加されます。この構成でサポートされる唯一の属性は、現在「action」と呼ばれています。この属性は、その構成オブジェクトでサポートされている「enable」や「disable」のような値を取ることができます。

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  meta-properties
   action: enable
  properties:
    name: $parameters.name
    servicetype: HTTP
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

この例では、`my-lbvserver-comp`コンポーネントのタイプは`ns::lbvserver`です。「ns」は、import-stylebooks セクションで指定した名前空間 netscaler.nitro.config およびバージョン **10.5 を参照する接頭辞です。`lbvserver`は、この名前空間の NITRO リソースです。暗黙的なアクションとして、`lbvserver`が StyleBook によって最初に作成されます。次に、「有効」操作が実行されます。

メタプロパティで指定されたアクションは、ConfigPack の作成時にのみ構成オブジェクトに対して実行されます。ConfigPack の更新は、CRUD 以外のアクションを実行しません。

> 注:
>
> アクション属性の値は、動的に評価される StyleBook 式にすることはできません。

構成パックを作成および編集する

May 7, 2021

Citrix Application Delivery Management（ADM）では、StyleBook から構成パックを作成できます。また、構成パックは、作成元の StyleBook に関連付けられています。構成パックへの更新は、それが結び付けられている StyleBook を通じて行われます。

構成パックを作成する

StyleBook から構成パックを作成するには、次の手順に従います。

1. [アプリケーション**] > [StyleBooks] > [**構成**]** に移動します
2. ［追加］をクリックします。
3.「**StyleBooks**」で、構成パックを作成する必要な StyleBook を選択します。

   このページでは、StyleBook をデフォルトとカスタム StyleBook に分類しています。それぞれのタブを選択して、必要な StyleBook を見つけます。
4. アプリケーション名、IP アドレス、ポート、プロトコルタイプなど、必要な詳細を指定します。

   GUI フィールドは、ある StyleBook から別の StyleBook によって異なります。
5. [ターゲットインスタンス] で、設定を実行するインスタンスまたはインスタンスグループを選択します。

   > 注:
   >
   > 必要な数のターゲットインスタンスを指定することで、複数の Citrix ADC に構成を展開できます。
6. [ドライラン] をクリックします。

   ［オブジェクト］ページには、Citrix ADC インスタンスから作成、変更、または削除されたオブジェクトが表示されます。
7. [作成] をクリックします。

   設定パックは、**StyleBook > [**構成**]** ページに表示されます。

既存の構成パックを編集する場合は、構成パックを選択して [編集] をクリックします。

設定パックの **StyleBook** を変更する

機能を追加したり、問題を解決したりするために、StyleBook を更新する必要がある場合があります。古い StyleBook を使用して構成パックをすでに作成している場合は、新しい更新された StyleBook を使用するように構成パックを更新することができます。新しい StyleBook を使用するには、構成パックの既存の StyleBook を変更します。

ADC インスタンスに基本的なロードバランサー設定をデプロイする StyleBook **example-lb** の例を考えてみましょう。そして、この StyleBook から構成パック CP1 を作成します。

基本的なロードバランサー設定でモニターを構成する場合は、新しい StyleBook が必要です。したがって、基本的なロードバランサー設定とともにモニターを構成する機能を含む、例 **lb-mon StyleBook** を作成します。

StyleBook を作成したら、既存の構成パック CP1 を更新してモニターを追加します。これを行うには、次の手順を実行します。

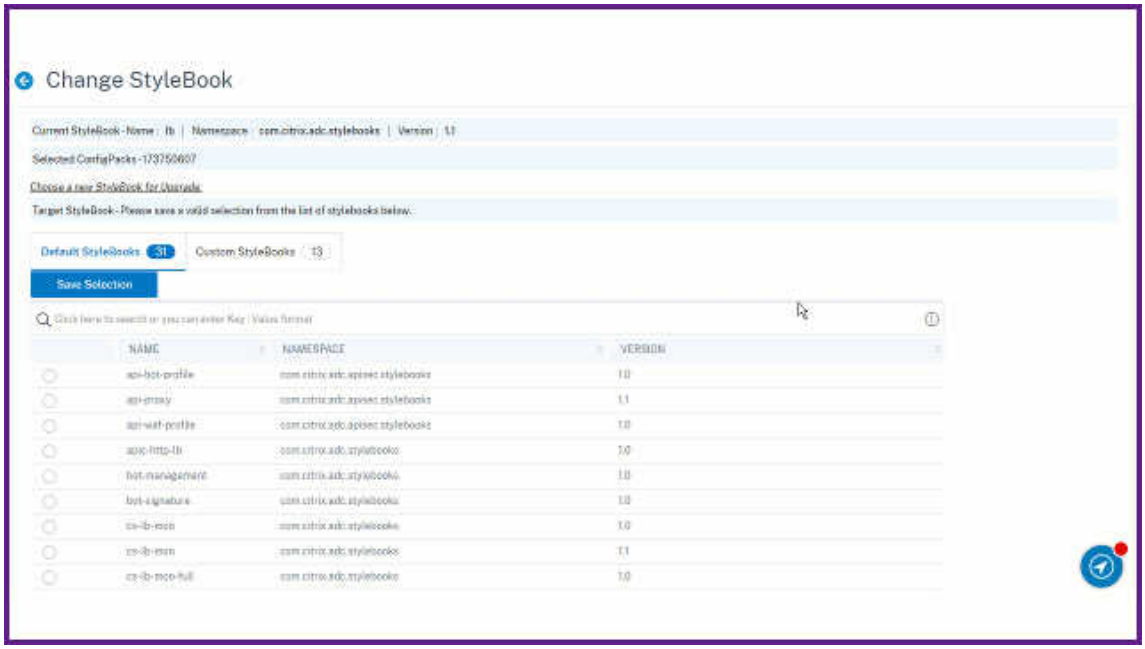
1. [アプリケーション**] > [StyleBooks] > [**構成**]** に移動します
2. StyleBook を変更する構成パックを選択します。

   この例では、リストから CP1 を選択します。
3.「**StyleBook** の変更」をクリックします。

4. リストから必要な StyleBook を選択します。次に、[選択を保存] をクリックします。
5. ［変更］をクリックします。

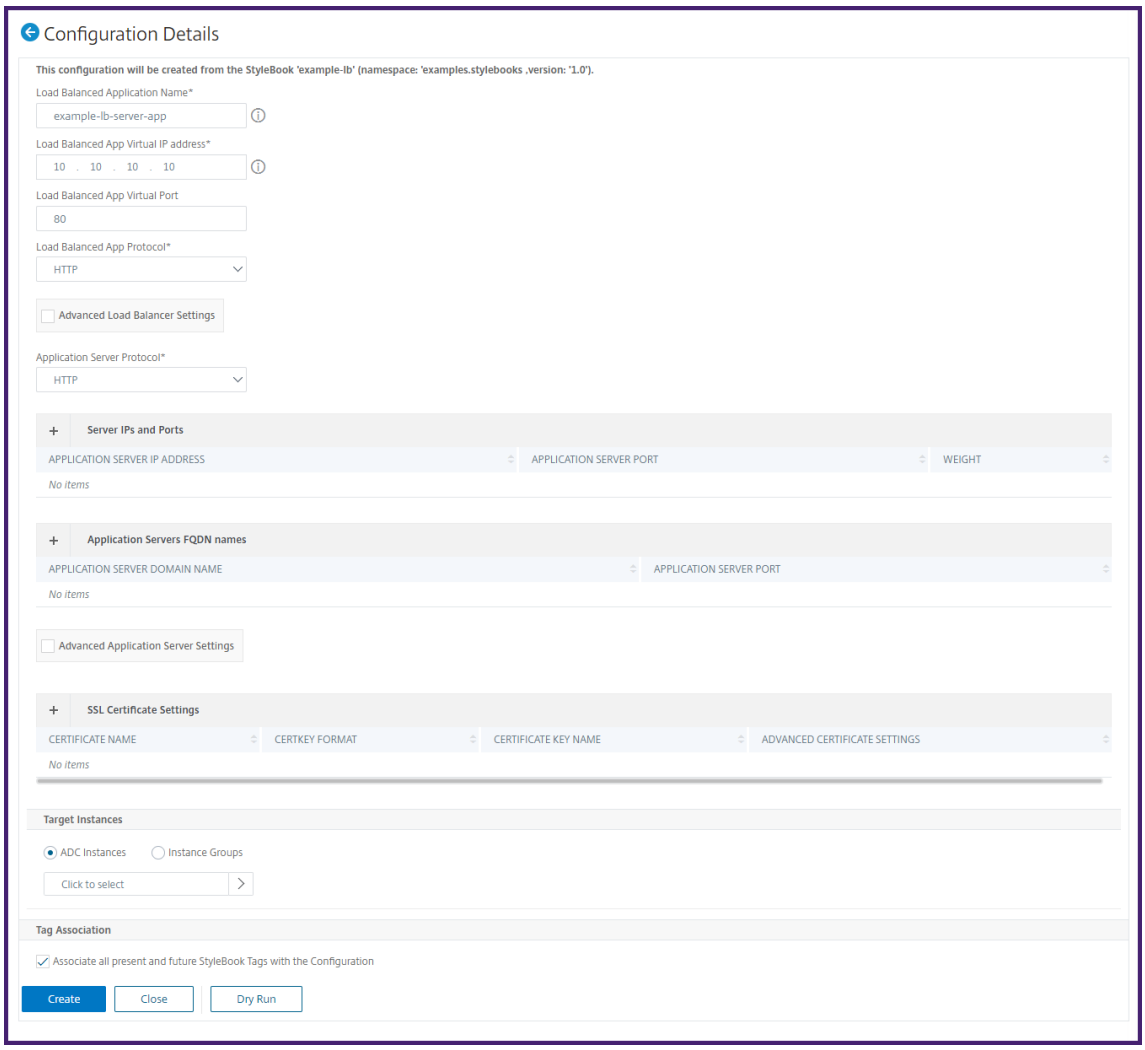
   この例では、リストから **example-lb-mon** を選択します。

   設定パックの StyleBook を変更すると、新しい StyleBook のパラメータが既存の StyleBook とは異なる構造になることがあります。パラメータ構造が以前の StyleBook に似ている場合、パラメータの値はそれぞれのフィールドに自動的に保持されます。それ以外の場合は、2 つの StyleBook 間で同じ構造を持つパラメータのみが転送されます。たとえば、同じパラメータ名、タイプ、パラメータの親など。

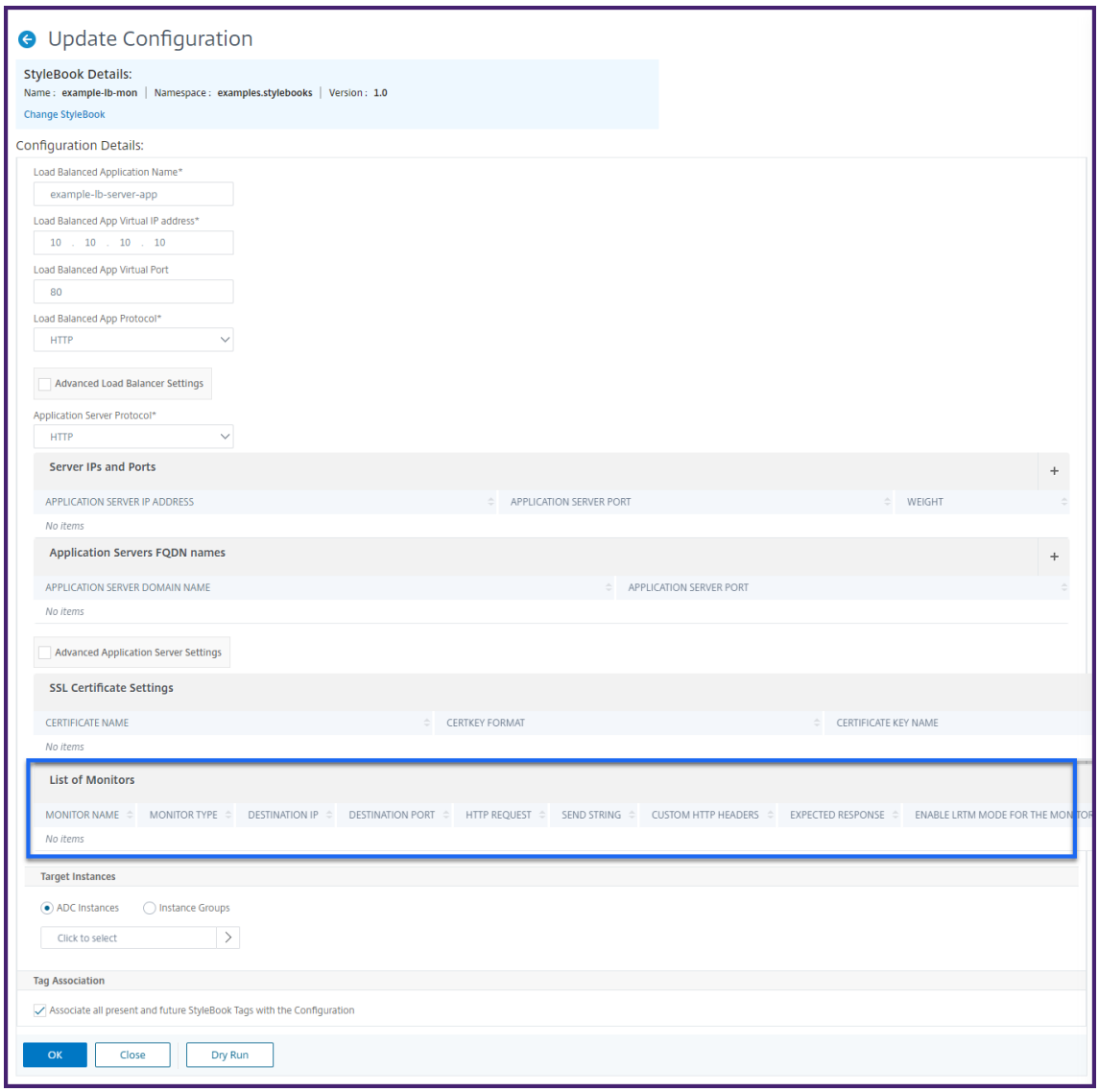


   新しい StyleBook に新しい必須パラメータを追加する場合は、StyleBook を変更した後、そのようなパラメータの値を手動で指定する必要があります。

   この例では、**example-lb** StyleBook の設定ページに表示されるパラメータは次のとおりです。



新しい **example-lb-mon StyleBook** の設定ページに表示されるパラメーターは次のとおりです。



この場合、新しい StyleBook は既存のパラメータを変更していないため、StyleBooks は基本的なロードバランサー設定の古い値を保持します。そして、それは新しいパラメータだけを追加します。モニタパラメータの場合は、必要な値を手動で指定します。

6. [ターゲットインスタンス] で、選択したインスタンスを確認し、必要に応じてリストを更新します。
7. [ドライラン] をクリックします。

   [オブジェクト] ページには、Citrix ADC インスタンスから作成、変更、または削除されたオブジェクトが表示されます。

8. [**OK**] をクリックします。

   「**StyleBook**」**>**「構成」ページの「**StyleBook** 名」列に、選択した構成パックの新しい StyleBook 名が表示されます。この場合、**example-lb-mon** と表示されます。

複数の構成パックがある **StyleBook** を変更する

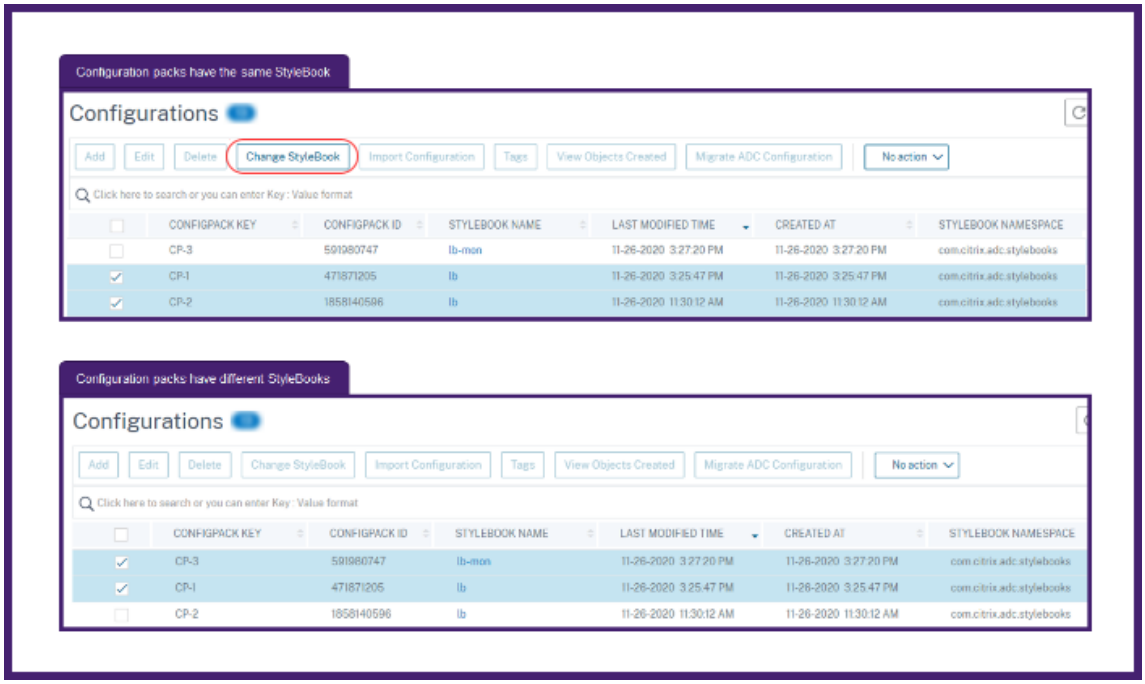
複数の構成パックを含む既存の StyleBook を変更する場合は、次の操作を行います。

1. 新しい StyleBook を ADM にインポートします。

   通常、新しい StyleBook の名前と名前空間は、既存の StyleBook よりも高いバージョンを持ちます。ただし、名前、名前空間、またはバージョンが異なる場合は、この手順を省略できます。

2. 既存の StyleBook に関連付けられている構成パックの StyleBook を変更します。

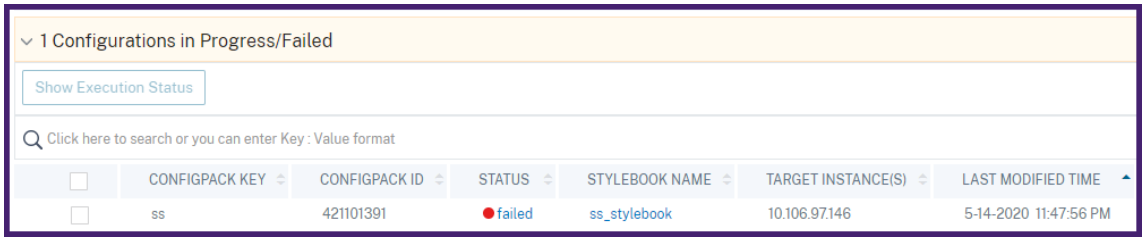
   選択した構成パックが同じ StyleBook に関連付けられている場合にのみ、**StyleBook** の変更を選択できます。



   選択した構成パックについて、次の条件が満たされると、ADM は StyleBook を正常に変更します。

   - 既存の StyleBook の設定パラメータはすべて、選択した StyleBook に存在する必要があります。
   - 選択した StyleBook の新しいパラメータはオプションです。

   選択した構成パックの進行状況を確認するには、[構成] ページの **[**進行中/失敗] の [構成] を選択します。



3. すべての構成パックを新しい StyleBook に関連付けたら、古い StyleBook を ADM から削除します。

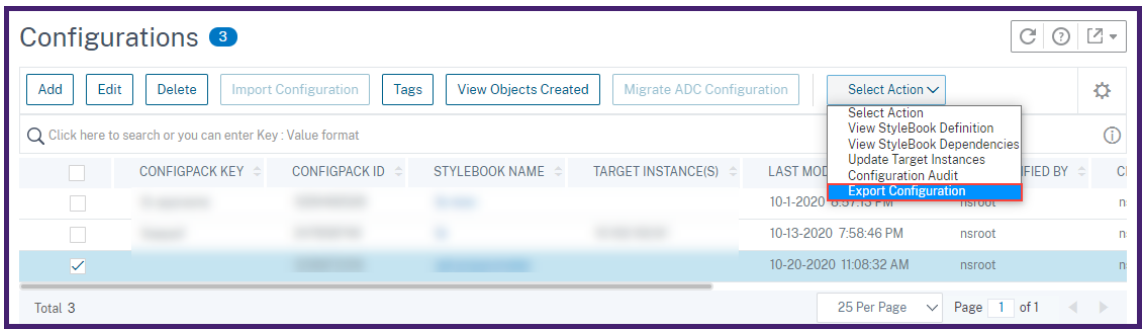
構成パックのエクスポートまたはインポート

StyleBooks のような構成パックをエクスポートまたはインポートできます。この機能を使用すると、StyleBook 設定を別の ADM サーバーに簡単に共有できます。構成パックをエクスポートすると、`tgz`または`zip`バンドルがローカルコンピュータにダウンロードされます。このバンドルには、設定パックで定義されたすべてのパラメーターを含む JSON ファイルが含まれます。

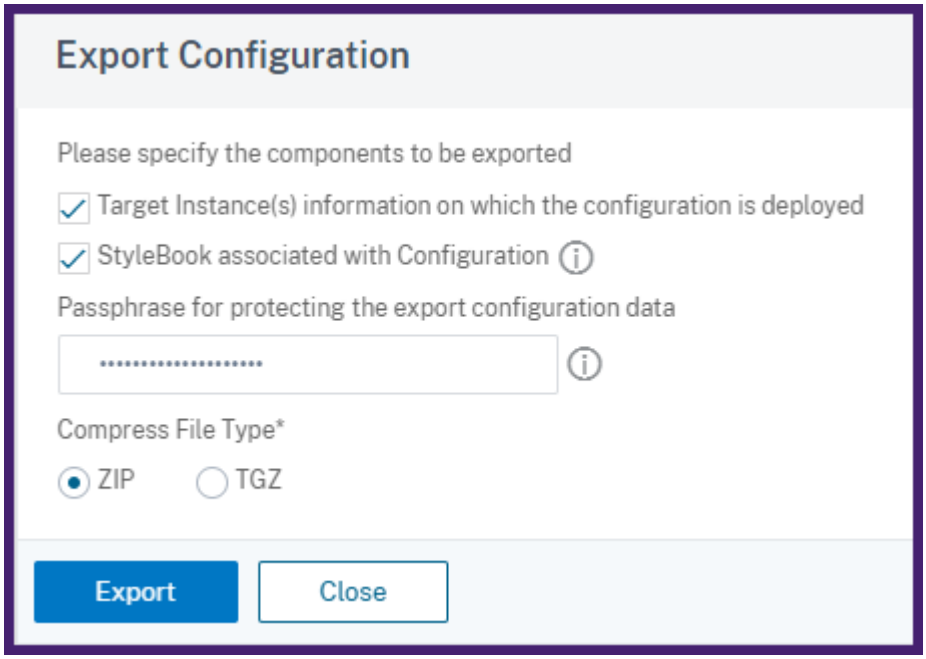
設定のエクスポート

構成パックをエクスポートするには、次の手順を実行します。

1. [アプリケーション] **> [StyleBooks] > [**構成**]** に移動します
2. エクスポートする構成パックを選択します。
3. 「アクションの選択」で、「構成のエクスポート」を選択します。



4. [構成のエクスポート] ペインで、次の項目を指定します。
   - 設定がデプロイされるターゲットインスタンス情報: エクスポートバンドルにターゲットインスタンスの情報を含めるには、このオプションを選択します。
   - 設定に関連付けられた **StyleBook**: StyleBook をエクスポートバンドルに含めるには、このオプションを選択します。
   - エクスポート設定データを保護するためのパスフレーズ: エクスポートバンドルを暗号化するためのパスフレーズを指定します。このパスフレーズは、構成パックの機密データを保護します。
   - 圧縮ファイルの種類: **ZIP** または **TGZ** ファイルタイプを選択します。



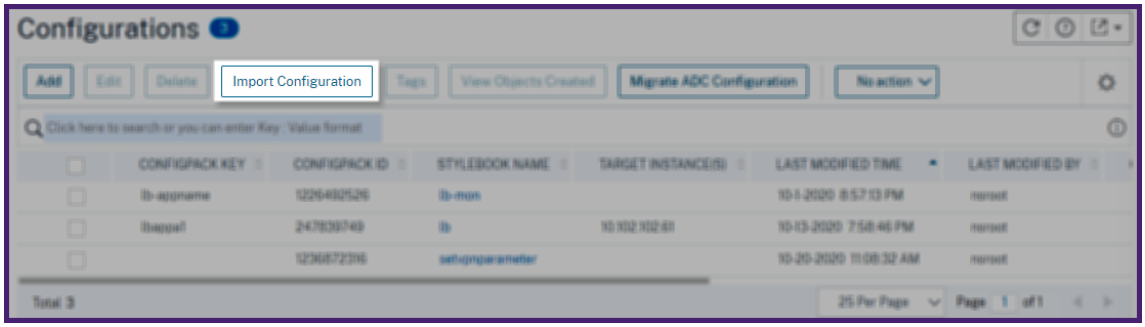
5. [エクスポート] をクリックします。

   エクスポートバンドルをローカルコンピューターに保存します。

設定のインポート

ローカルコンピューターから別の ADM サーバーに構成パックをインポートできます。構成パックをインポートするには、次の手順を実行します。

1. [アプリケーション] **> [StyleBooks] > [**構成] に移動します
2. [構成のインポート] を選択します。



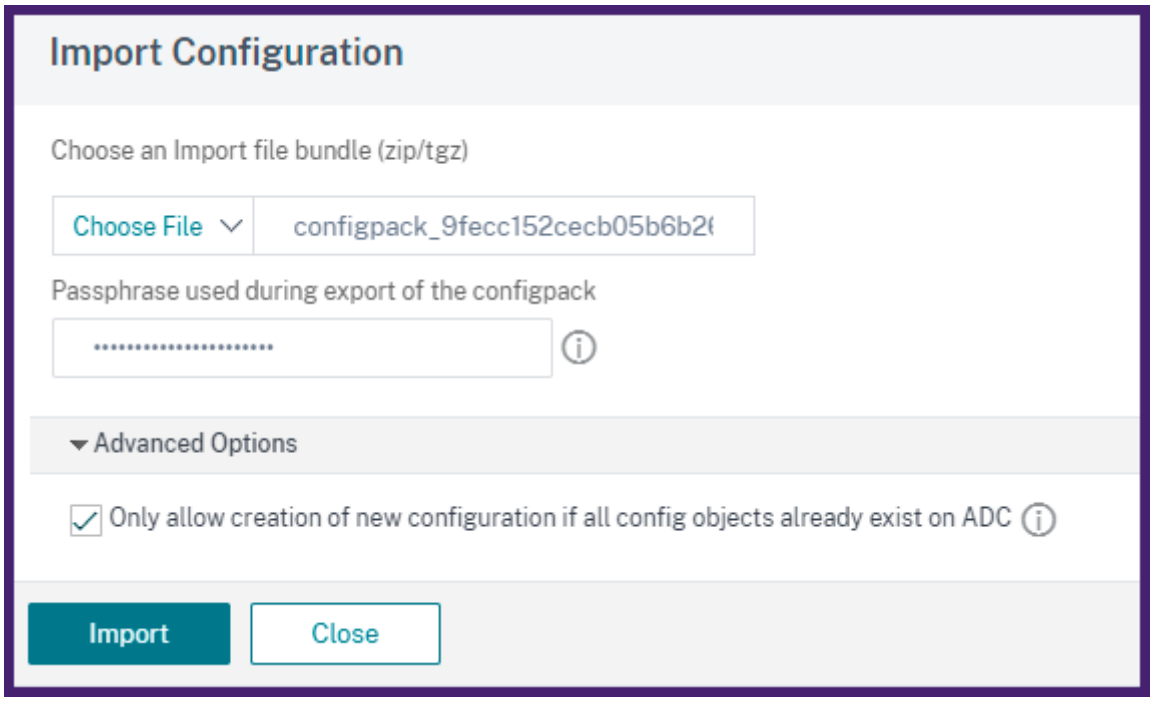
3. コンピュータからインポートファイルバンドルを選択します。
4. エクスポート時に指定したパスフレーズを使用します。
5. オプションで、[詳細オプション] で、[**ADC** にすべての設定オブジェクトが存在する場合にのみ、新しい構成の作成を許可する] を選択します。

   このオプションでは、ADC インスタンスにすでに作成されているオブジェクトは変更されません。

同じ ADC インスタンスを 2 つの ADM サーバに追加したとします。また、ある ADM サーバーから別のサーバーへ構成パックを移行する場合。このオプションは、ADC インスタンス上の設定オブジェクトを変更せずに構成パックをインポートする場合に使用します。

> 重要:
>
> このオプションを使用するには、指定された設定バンドルにターゲットインスタンス情報が含まれていることを確認してください。設定のエクスポートを参照してください。
>
> このオプションは、すべてのオブジェクトがターゲットインスタンスに存在する場合のみ、設定を移行します。

6. ［インポート］をクリックします。



構成パックをインポートすると、ADM は次のことを検証します。

- 関連した **StyleBook**: 関連する StyleBook が ADM にない場合、StyleBook を構成パックとともにインポートします。
- ターゲットインスタンス: ターゲットインスタンスをチェックし、指定したターゲットインスタンスに設定をデプロイします。上記の ADC インスタンスが ADM に存在しない場合、構成パックはターゲットインスタンスなしでインポートされます。
- ソース **ADM**: 同じ ADM サーバー上に構成パックをインポートする場合、選択したバンドルによって既存の構成パックが更新されます。

スタイルブックを構築する

example-lb StyleBook の全コンテンツは、以下の参照用に提供されています。


```
name: example-lb
namespace: examples.stylebooks
version: "1.0"
display-name: Basic Load Balancer App
description: This is an example StyleBook that creates a load balancer
   application
schema-version: "1.0"
import-stylebooks:
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
parameters-default-sources:
  - stlb::lb
components:
  -
    name: lb-comp
    type: stlb::lb
    description: Uses the default lb StyleBook to build the typical lb
       configuration objects
    properties-default-sources:
      - $parameters
<!--NeedCopy-->
```

example-lb-mon StyleBook の全コンテンツは、参照用に次のように提供されます。

```
name: example-lb-mon
namespace: examples.stylebooks
version: "1.0"
description: This is an example StyleBook that creates a load balancer
   application with monitors
display-name: Basic Load Balancer App with Monitors
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
  -
    namespace: com.citrix.adc.commontypes
```



```
18      prefix: cmtypes
19      version: "1.0"
20  parameters-default-sources:
21    - stlb::lb
22  parameters:
23    -
24      name: monitors
25      label: "List of Monitors"
26      description: "List of Monitors to monitor Application Servers"
27      type: cmtypes::monitor[]
28  substitutions:
29    mon-name(appname, monname): $appname + "-mon-" + $monname
30  components:
31    -
32      name: lb-comp
33      type: stlb::lb
34      description: Uses the default lb StyleBook to build the typical lb
           configuration objects
35      properties-default-sources:
36        - $parameters
37    -
38      name: monitors-comp
39      type: cmtypes::monitor
40      condition: $parameters.monitors
41      repeat: $parameters.monitors
42      repeat-item: mon
43      repeat-index: ndx
44      description: Builds a list of Citrix ADC monitor objects and binds
           them to the servicegroup of this LB config
45      properties-default-sources:
46        - $mon
47      properties:
48          monitorname: $substitutions.mon-name($parameters.lb-appname,
              $mon.monitorname)
49      components:
50        -
51          name: monitor-svcg-binding-comp
52          condition:  $parameters.svc-servers
53          type: ns::servicegroup_lbmonitor_binding
54          properties:
55            servicegroupname: $components.lb-comp.outputs.servicegroup.
                properties.servicegroupname
56            monitor_name: $parent.properties.monitorname
57  <!--NeedCopy-->
```

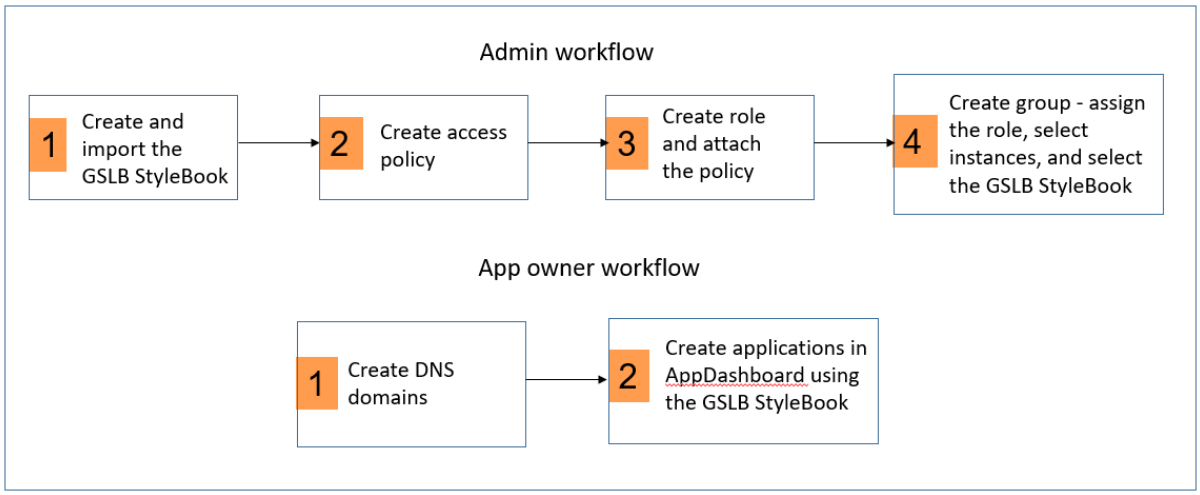

DNS ドメイン名を使用した GSLB 設定のデプロイ

May 7, 2021

Citrix Application Delivery Management（ADM）の新しい RBAC の機能強化により、承認されたアプリケーション所有者のみが Citrix ADM で自分の DNS ドメインを作成および管理できるようになります。これで、特定の StyleBook を使用して、アプリ所有者が所有する DNS ドメインから GSLB 設定を作成する権限を与えることができます。選択した DNS ドメイン名がユーザーが所有している場合は、Citrix ADM アプリケーションダッシュボードの GSLB StyleBooks を使用して GSLB 構成を作成するときに使用できます。
Citrix ADM には、GSLB 構成を構成するためのワークフローが 2 つあります。

1. 管理者のためのワークフロー。Citrix ADM で RBAC 環境を設定します。つまり、GSLB StyleBooks を作成してインポートするには、ユーザーグループ、ポリシー、ロールを作成し、ユーザーをグループに割り当てる必要があります。管理者として、このワークフローを実行する必要があります。
2. アプリケーション所有者のためのワークフロー。アプリケーション所有者は、所有するドメイン名を使用して GSLB 設定を作成する必要があります。

次のフローチャートは、両方のワークフローを示しています。



管理者のワークフロー

管理者として、Citrix ADM で RBAC 環境を作成するワークフローは、以下の手順で構成されます。

まず、StyleBook を作成して、Citrix ADC インスタンスに GSLB 構成を展開します。この文書では、独自の StyleBook-を作成するのに役立つサンプル YAML コンテンツを提供します。スタイルブックを構築する。

カスタムスタイルブックの作成方法の詳細については、「カスタムスタイルブックの作成と使用」を参照してください。

> 注:
>
> Citrix ADM は、StyleBooks で「許可された動的値」と呼ばれる新しい構造をサポートしています。この構造を使用すると、Citrix ADM に存在する DNS ドメイン値をユーザーが一覧表示および選択して、Citrix ADM GUI の StyleBook の「ドメイン名」パラメータを自動的に入力できます。

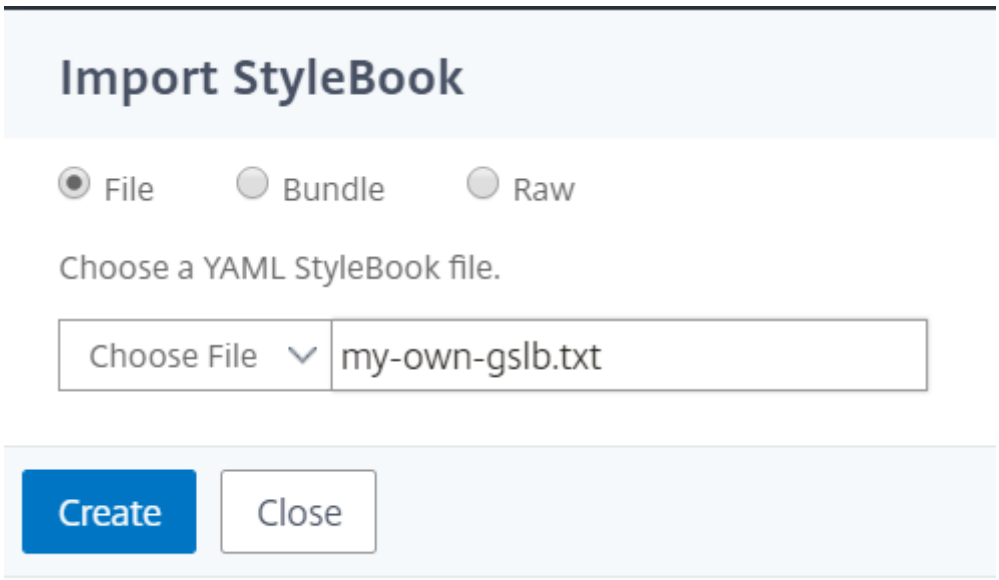
参考のために、「ドメイン名」パラメータセクションの例を提供しています。

ここで使用される「ドメイン名」パラメータは単なる例です。このパラメータは、カスタム StyleBook で異なる場合があります。

```
-
  name: domain-name
   label: DNS Domain Name
   description: GSLB DNS Domain Name
   type: string
   required: true
   allowed-dynamic-values:
      source: local
      resource-type: dns_domain_entry
<!--NeedCopy-->
```

> 注
>
> : 現在、Citrix ADM では、デフォルトの StyleBook では、「許可された動的値」コンストラクトは使用されません。デフォルトの GSLB StyleBook を使用して、新しいカスタム GSLB StyleBook を作成します。ドメイン名のパラメーターの部分は、上記のサンプルに置き換えます。新しい StyleBooks を作成するには、任意のテキストエディタを使用できます。

1. 管理者として Citrix ADM にログオンします。
2. アプリケーション > 構成 > **StyleBooks** に移動します。
3. [新しい **StyleBook** のインポート] をクリックし、新しい GSLB StyleBook を Citrix ADM にアップロードします。



Citrix ADM でスタイルブックをインポートする方法の詳細については、「カスタム StyleBook を使用する」を参照してください。

4. [システム] > [ユーザー] > [ポリシー] に移動し、[追加] をクリックして、アプリケーション所有者のアクセスポリシーを設定します。

   アプリケーション所有者が設定した RBAC ルールを回避しないように、アクセスポリシーを作成することをお勧めします。

5. ポリシーの名前と簡単な説明を入力します。[Permissions] セクションで、次のビュー編集権限が必須にチェックされていることを確認します。

   a) アプリケーション > ダッシュボード

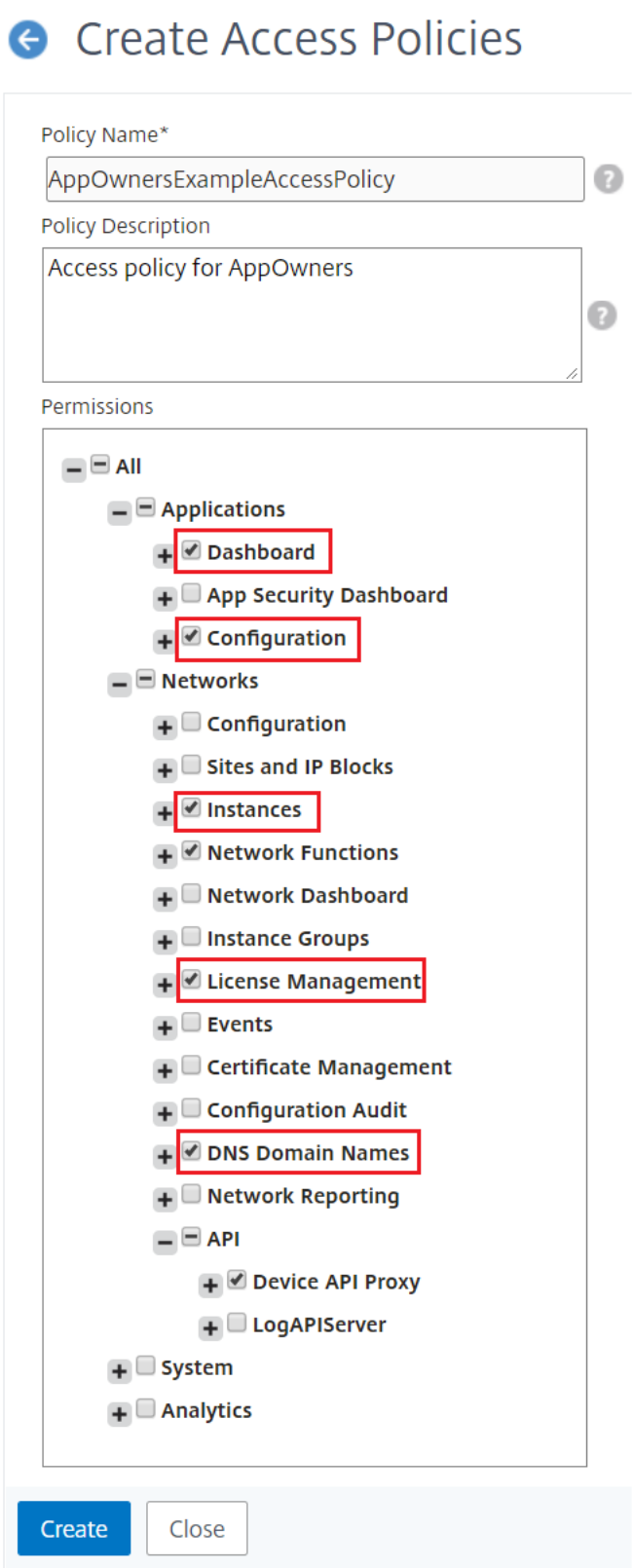
   b) アプリケーション > 構成

   c) ネットワーク > インスタンス

   d) ネットワーク > ライセンス管理

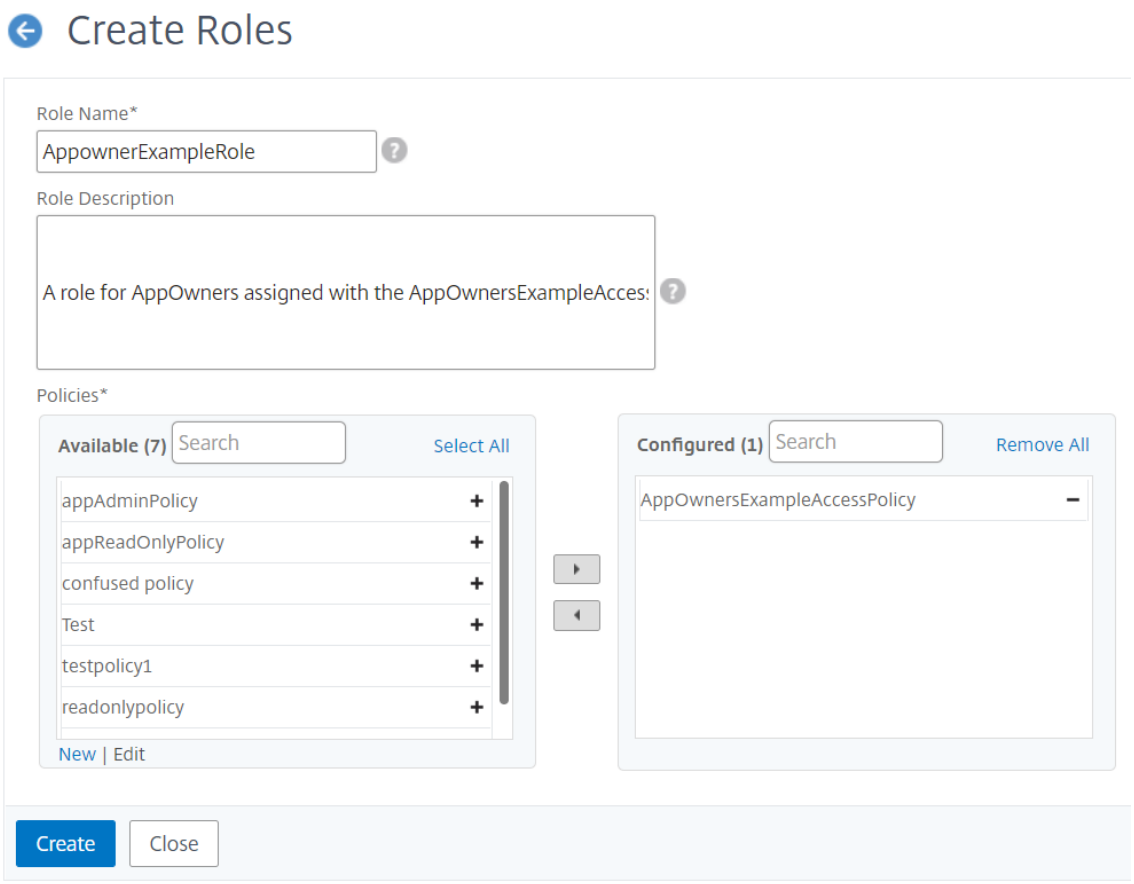
   e) [ネットワーク] > [DNS ドメイン名]

   必要に応じて他の権限を指定し、[**Create**] をクリックします。



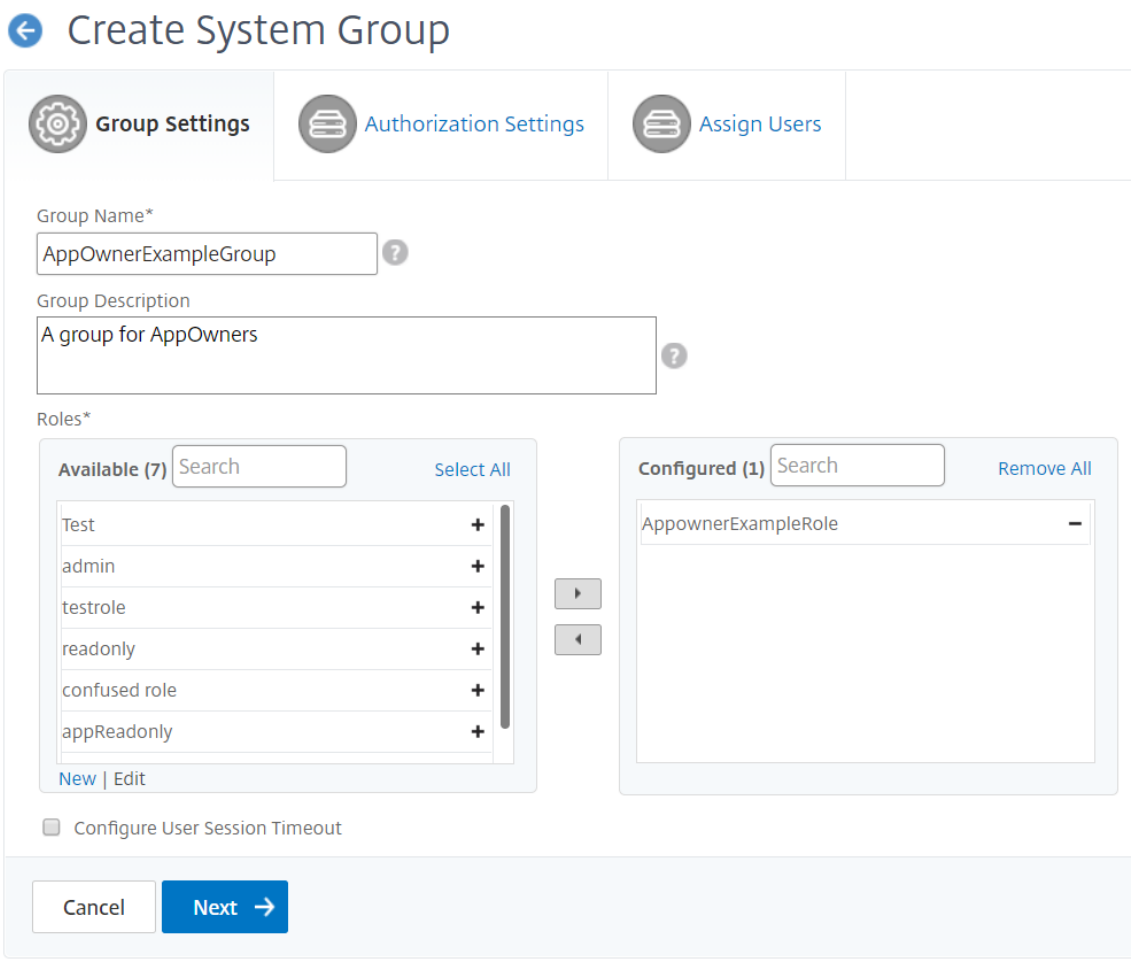
6. [システム] > [ユーザー] > [ロール] に移動し、ロールを作成し、前の手順で作成したポリシーを割り当てます。

7. ロールの名前を入力し、簡単な説明を入力します。[ポリシー] セクションで、[**appownereXampleAccessPolicy**] を選択します。

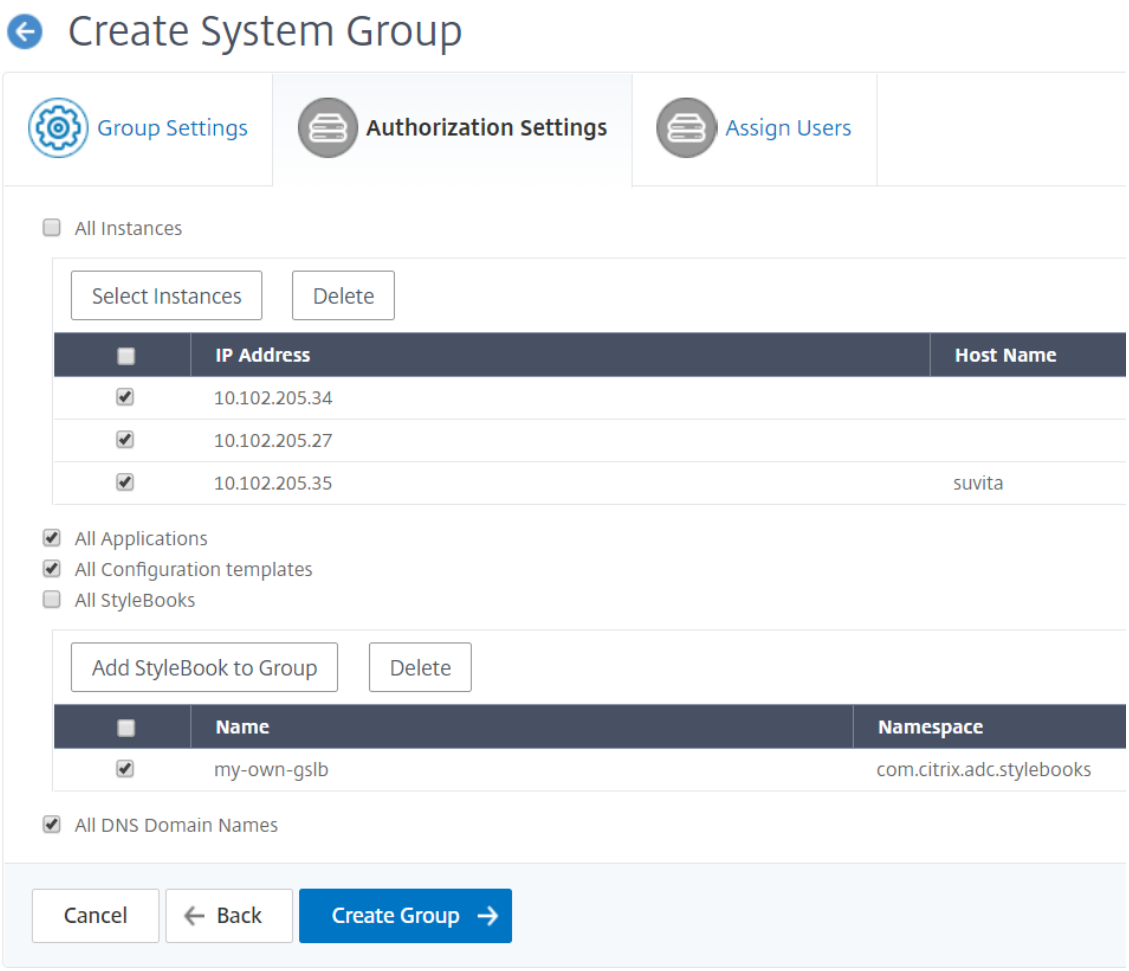


8. [システム] > [ユーザー] > [グループ] に移動し、グループを作成し、前の手順で作成したロールを関連付けます。

9. 名前と説明を入力し、[ロール] セクションで [**AppownereXampleRole**] を選択します。



10. ［次へ］をクリックします。
11. ［認証設定］タブで、アプリケーション所有者がアクセスできる Citrix ADC インスタンスと、新しい GSLB StyleBook を選択します。

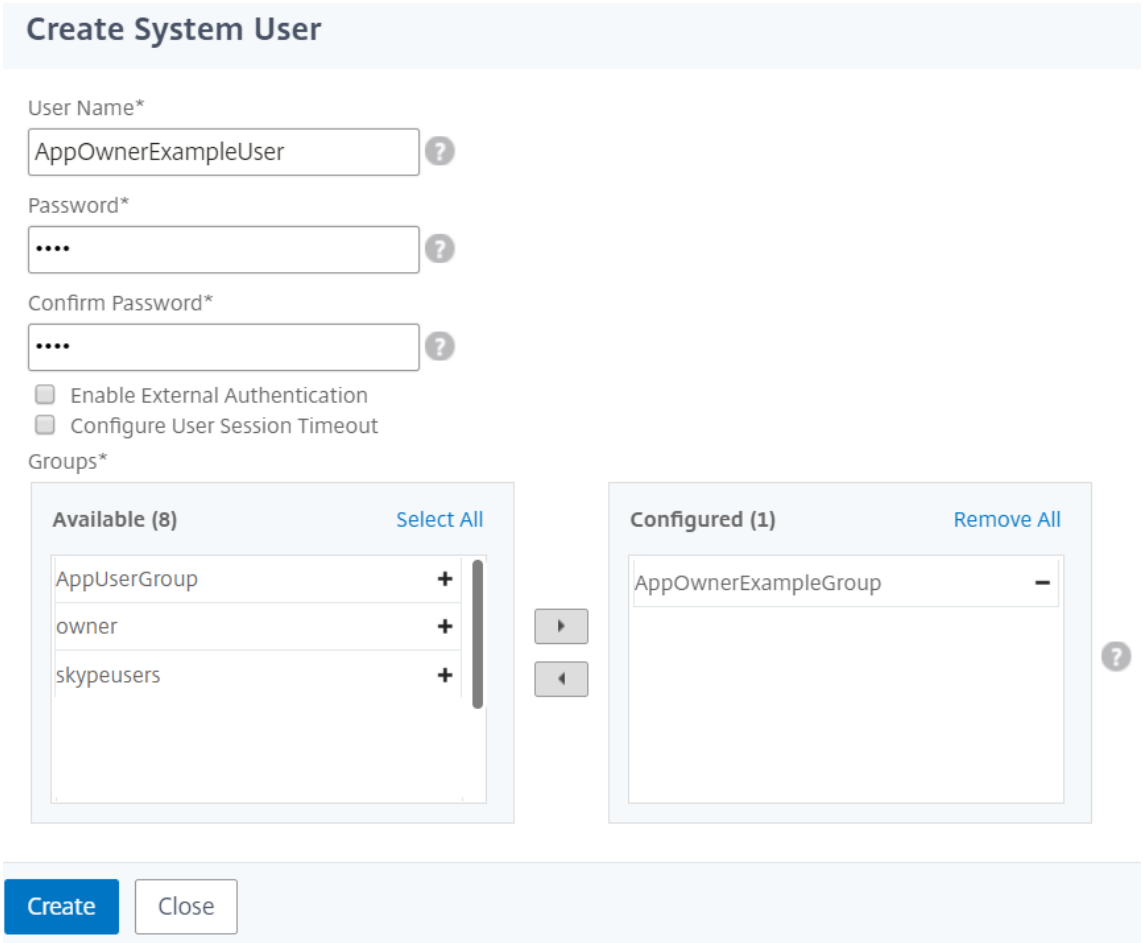


この手順を繰り返して、組織内で必要な数のユーザーグループを作成します。[**Create Group**] をクリックします。

12. システムユーザを作成し、そのユーザをユーザグループに割り当てます。このドキュメントは、ローカルに作成されたユーザーのみを参照します。Citrix ADM が外部認証（LDAP など）を使用するようにセットアップされている場合は、ユーザーグループにユーザーを作成する必要はありません。グループへのユーザーマッピングは、外部認証ディレクトリから取得されます。

    a) [システム] > [ユーザー**] > [**** ユーザー **] に移動します。

    b) システムユーザーのユーザー名とパスワードを入力し、ユーザーをグループに割り当てます。



> 注:
>
> ステップ 12 はオプションであり、LDAP などの外部認証を使用する場合は必須ではありません。

管理者ワークフロー用の **Citrix ADM REST API**

Citrix ADM にログオンするための **REST API**

```
URL: http: //<MAS_IP>/nitro/v2/config/login
HTTPMETHOD: POST

Body Payload:
{

  "login": {

    "username": "<USER_NAME>",
    "password": "<PASSWORD>",
    "session_timeout": 1800
   }
```



```
13
14  }
15
16
17 The response results in a session cookie header, that can be sent with
      the rest of the API requests below.
18
19 Set-Cookie: SESSID=##
      ED31F7C886E248CCDCA8F0E0AD2AA511ACCC5F46C48D6D2BCAA719A9DE62;path=/;
      secure;HttpOnly
20 <!--NeedCopy-->
```

REST API を使用してアクセスポリシーを作成する

```
1  URL: https://<MAS_IP>/nitro/v2/config/rba_policy
2  HTTP METHOD: POST
3
4  {
5
6    "rba_policy": {
7
8      "name": " AppOwnerAccessPolicy",
9      "description": " ExampleCompany AppOwner Access Policy",
10     "tenant_id": "7c12ec97-1472-4096-97e7-a5acb453cc5c",
11     "statement": [
12       {
13
14         "access_type": true,
15         "resource_type": "application",
16         "operation_name": "add",
17         "dependent_resources": "mail_profile,slack_profile,smtp_server,
               app_category"
18        }
19   ,
20       {
21
22         "access_type": true,
23         "resource_type": "application",
24         "operation_name": "get",
25         "dependent_resources": "download,smtp_server,ns_vserver_license
               ,app_category,app_summary,app_health_dashboard_details,
               haproxy_frontend,haproxy_backend,haproxy_frontend_stats"
26        }
27   ,
```

```
28        {
29
30          "access_type": true,
31          "resource_type": "si_app_unit",
32          "operation_name": "get",
33          "dependent_resources": "download,smtp_server,app_summary,
                si_app_summary,si_device,security_app_dashboard_details,
                si_geo_location,si_safety_app_firewall,si_safety_overview,
                si_safety_security_check,si_safety_system_security,
                si_safety_signature"
34         }
35  ,
36        {
37
38          "access_type": true,
39          "resource_type": "stylebooks",
40          "operation_name": "get",
41          "dependent_resources": "download,smtp_server,ns_vserver_license
                "
42         }
43  ,
44        {
45
46          "access_type": true,
47          "resource_type": "stylebooks",
48          "operation_name": "add",
49          "dependent_resources": "mail_profile,slack_profile,smtp_server"
50         }
51  ,
52        {
53
54          "access_type": true,
55          "resource_type": "configpacks",
56          "operation_name": "get",
57          "dependent_resources": "download,smtp_server,stylebooks,
                ns_vserver_license"
58         }
59  ,
60        {
61
62          "access_type": true,
63          "resource_type": "configpacks",
64          "operation_name": "add",
65          "dependent_resources": "mail_profile,slack_profile,smtp_server"
66         }
```



```
67  ,
68        {
69
70          "access_type": true,
71          "resource_type": "stylebooks_system_settings",
72          "operation_name": "get",
73          "dependent_resources": "download,smtp_server"
74         }
75  ,
76        {
77
78          "access_type": true,
79          "resource_type": "stylebooks_system_settings",
80          "operation_name": "add",
81          "dependent_resources": "mail_profile,slack_profile,smtp_server"
82         }
83  ,
84        {
85
86          "access_type": true,
87          "resource_type": "ns_crvserver",
88          "operation_name": "get",
89          "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                perf_cache_redirection_report,poll_activity_status,
                ns_emon_poll_policy,lb_export_report"
90         }
91  ,
92        {
93
94          "access_type": true,
95          "resource_type": "ns_crvserver",
96          "operation_name": "add",
97          "dependent_resources": "DeviceAPIProxy,mail_profile,
                slack_profile,smtp_server,poll_activity_status,
                ns_emon_poll_policy,lb_export_report"
98         }
99  ,
100       {
101
102         "access_type": true,
103         "resource_type": "haproxy_frontend",
104         "operation_name": "get",
105         "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                haproxy_backend,haproxy_server"
106        }
```



```
,
      {

        "access_type": true,
        "resource_type": "haproxy_frontend",
        "operation_name": "add",
        "dependent_resources": "DeviceAPIProxy,mail_profile,
           slack_profile,smtp_server"
       }
,
      {

        "access_type": true,
        "resource_type": "ns_server",
        "operation_name": "get",
        "dependent_resources": "download,DeviceAPIProxy,smtp_server,
           ns_emon_poll_policy,poll_activity_status,ns_server,
           lb_export_report"
       }
,
      {

        "access_type": true,
        "resource_type": "ns_server",
        "operation_name": "add",
        "dependent_resources": "DeviceAPIProxy,mail_profile,
           slack_profile,smtp_server,ns_emon_poll_policy,
           poll_activity_status,lb_export_report"
       }
,
      {

        "access_type": true,
        "resource_type": "ns_lbvserver",
        "operation_name": "get",
        "dependent_resources": "download,DeviceAPIProxy,smtp_server,
           perf_lb_vserver_report,ns_emon_poll_policy,
           poll_activity_status,lb_export_report"
       }
,
      {

        "access_type": true,
        "resource_type": "ns_lbvserver",
        "operation_name": "add",
```



```
145           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server,ns_emon_poll_policy,
                  poll_activity_status,lb_export_report"
146          }
147    ,
148          {
149
150           "access_type": true,
151           "resource_type": "ns_service",
152           "operation_name": "get",
153           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                  ns_emon_poll_policy,poll_activity_status,
                  ns_visualizer_lb_bindings,lb_export_report"
154          }
155    ,
156          {
157
158           "access_type": true,
159           "resource_type": "ns_service",
160           "operation_name": "add",
161           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server,ns_emon_poll_policy,
                  poll_activity_status,ns_visualizer_lb_bindings,
                  lb_export_report"
162          }
163    ,
164          {
165
166           "access_type": true,
167           "resource_type": "ns_servicegroup",
168           "operation_name": "get",
169           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                  ns_emon_poll_policy,poll_activity_status,
                  ns_servicegroupmember_binding,ns_visualizer_lb_bindings,
                  lb_export_report"
170          }
171    ,
172          {
173
174           "access_type": true,
175           "resource_type": "ns_servicegroup",
176           "operation_name": "add",
177           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server,ns_emon_poll_policy,
                  poll_activity_status,ns_servicegroupmember_binding,
```



```
                ns_visualizer_lb_bindings,lb_export_report"
178          }
179    ,
180          {
181
182            "access_type": true,
183            "resource_type": "ns_authenticationvserver",
184            "operation_name": "get",
185            "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                   perf_authentication_report,poll_activity_status,
                   ns_emon_poll_policy,lb_export_report"
186          }
187    ,
188          {
189
190            "access_type": true,
191            "resource_type": "ns_authenticationvserver",
192            "operation_name": "add",
193            "dependent_resources": "DeviceAPIProxy,mail_profile,
                   slack_profile,smtp_server,poll_activity_status,
                   ns_emon_poll_policy,lb_export_report"
194          }
195    ,
196          {
197
198            "access_type": true,
199            "resource_type": "syslog_messages",
200            "operation_name": "get",
201            "dependent_resources": "download,smtp_server"
202          }
203    ,
204          {
205
206            "access_type": true,
207            "resource_type": "ns_emon_poll_policy",
208            "operation_name": "get",
209            "dependent_resources": "download,poll_activity_status,
                   smtp_server"
210          }
211    ,
212          {
213
214            "access_type": true,
215            "resource_type": "ns_emon_poll_policy",
216            "operation_name": "add",
```



```
217           "dependent_resources": "download,poll_activity_status,
                  mail_profile,slack_profile,smtp_server"
218         }
219   ,
220         {
221
222           "access_type": true,
223           "resource_type": "ns_visualizer_gslb_bindings",
224           "operation_name": "add",
225           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server,poll_activity_status,
                  ns_emon_poll_policy,ns_gslbvserver_domain,lb_export_report"
226         }
227   ,
228         {
229
230           "access_type": true,
231           "resource_type": "ns_visualizer_gslb_bindings",
232           "operation_name": "get",
233           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                  poll_activity_status,ns_emon_poll_policy,
                  ns_gslbvserver_domain,lb_export_report"
234         }
235   ,
236         {
237
238           "access_type": true,
239           "resource_type": "ns_gslbservice",
240           "operation_name": "add",
241           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server,poll_activity_status,
                  ns_emon_poll_policy,lb_export_report"
242         }
243   ,
244         {
245
246           "access_type": true,
247           "resource_type": "ns_gslbservice",
248           "operation_name": "get",
249           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                  poll_activity_status,ns_emon_poll_policy,lb_export_report"
250         }
251   ,
252         {
253
```



```
254           "access_type": true,
255           "resource_type": "ns_gslbvserver",
256           "operation_name": "get",
257           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                 perf_global_server_load_balancing_report,
                 poll_activity_status,ns_emon_poll_policy,lb_export_report"
258          }
259   ,
260         {
261
262           "access_type": true,
263           "resource_type": "ns_gslbvserver",
264           "operation_name": "add",
265           "dependent_resources": "DeviceAPIProxy,mail_profile,
                 slack_profile,smtp_server,poll_activity_status,
                 ns_emon_poll_policy,lb_export_report"
266         }
267   ,
268         {
269
270           "access_type": true,
271           "resource_type": "ns_vpnvserver",
272           "operation_name": "add",
273           "dependent_resources": "DeviceAPIProxy,mail_profile,
                 slack_profile,smtp_server,poll_activity_status,
                 ns_emon_poll_policy,lb_export_report"
274          }
275   ,
276         {
277
278           "access_type": true,
279           "resource_type": "ns_vpnvserver",
280           "operation_name": "get",
281           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                 perf_ssl_vpn_report,poll_activity_status,ns_emon_poll_policy
                 ,lb_export_report"
282          }
283   ,
284         {
285
286           "access_type": true,
287           "resource_type": "ns_csvserver",
288           "operation_name": "get",
289           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                 perf_content_switching_report,ns_emon_poll_policy,
```



```
                poll_activity_status,ns_visualizer_cs_bindings,
                lb_export_report"
290          }
291    ,
292          {
293
294            "access_type": true,
295            "resource_type": "ns_csvserver",
296            "operation_name": "add",
297            "dependent_resources": "DeviceAPIProxy,mail_profile,
                   slack_profile,smtp_server,ns_emon_poll_policy,
                   poll_activity_status,ns_visualizer_cs_bindings,
                   lb_export_report"
298          }
299    ,
300          {
301
302            "access_type": true,
303            "resource_type": "dns_domain_entry",
304            "operation_name": "get",
305            "dependent_resources": ""
306          }
307    ,
308          {
309
310            "access_type": true,
311            "resource_type": "dns_domain_entry",
312            "operation_name": "add",
313            "dependent_resources": ""
314          }
315    ,
316          {
317
318            "access_type": true,
319            "resource_type": "devicewise_detail_summary",
320            "operation_name": "get",
321            "dependent_resources": "download,mps_user_heatmap,ns_event,
                   mps_agent,active_event,smtp_server,mps_datacenter,
                   event_severity_report,event_device_report,ns_conf,
                   device_event_summary"
322          }
323    ,
324          {
325
326            "access_type": true,
```



```
          "resource_type": "devicewise_detail_summary",
          "operation_name": "add",
          "dependent_resources": "mail_profile,slack_profile,smtp_server"
        }
  ,
      {

        "access_type": true,
        "resource_type": "cbwanopt",
        "operation_name": "get",
        "dependent_resources": "download,device_backup,traceroute,
            inventory,inventory_status,ping,mps_datacenter,
            cbwanopt_device_profile,sdwanvw_device_profile,
            sdwanvw_snmp_config,sdwanvw_appflowconfig,smtp_server,
            cbwanopt_snmp_config,cbwanopt_appflowconfig,sdwanvw,tag"
        }
  ,
      {

        "access_type": true,
        "resource_type": "cbwanopt",
        "operation_name": "add",
        "dependent_resources": "inventory,managed_device,device_backup,
            upload,cbwanopt_device_profile,mps_datacenter,mail_profile,
            slack_profile,smtp_server,sdwanvw_device_profile,
            sdwanvw_snmp_config,sdwanvw_appflowconfig,
            cbwanopt_snmp_config,cbwanopt_appflowconfig,sdwanvw,tag"
        }
  ,
      {

        "access_type": true,
        "resource_type": "device_login",
        "operation_name": "get",
        "dependent_resources": ""
        }
  ,
      {

        "access_type": true,
        "resource_type": "ns",
        "operation_name": "get",
        "dependent_resources": "download,ns_config_replicate,ns_conf,
            ns_ns_runningconfig,ns_ns_savedconfig,active_event,
            device_backup,traceroute,inventory,inventory_status,ping,
```



```
                ns_device_profile,nssdx_device_profile,sdx_snmp_config,
                sdx_syslog_config,smtp_server,ns_cluster,ns_snmp_config,
                ns_syslog_config,ns_l7_latency_config,ica_l7_latency_update,
                af_vserver_policy,ns_vserver_appflow_config,mps_datacenter,
                ns_appflow_param_config,ns_ns_license,ns_ns_mode,
                ns_network_interface,advanced_analytics_config,tag"
362          }
363    ,
364          {
365
366            "access_type": true,
367            "resource_type": "ns",
368            "operation_name": "add",
369            "dependent_resources": "inventory,ns_l7_latency_config,
                ica_l7_latency_update,af_vserver_policy,ns_config_replicate,
                managed_device,device_backup,upload,ns_device_profile,
                nssdx_device_profile,mps_datacenter,sdx_snmp_config,
                sdx_syslog_config,mail_profile,slack_profile,smtp_server,
                ns_cluster,ns_snmp_config,ns_syslog_config,
                ns_vserver_appflow_config,ns_appflow_param_config,
                advanced_analytics_config,tag"
370          }
371    ,
372          {
373
374            "access_type": true,
375            "resource_type": "haproxyhost",
376            "operation_name": "get",
377            "dependent_resources": "download,traceroute,inventory,
                inventory_status,ping,mps_datacenter,smtp_server,
                haproxy_device_profile,device_backup,tag"
378          }
379    ,
380          {
381
382            "access_type": true,
383            "resource_type": "haproxyhost",
384            "operation_name": "add",
385            "dependent_resources": "inventory,managed_device,mail_profile,
                slack_profile,smtp_server,mps_datacenter,
                haproxy_device_profile,haproxy,device_backup,tag"
386          }
387    ,
388          {
389
```



```
390           "access_type": true,
391           "resource_type": "docker_host",
392           "operation_name": "add",
393           "dependent_resources": "inventory,ns_snmp_config,managed_device
                 ,ns,upload,mail_profile,slack_profile,smtp_server,
                 mps_datacenter,ns_device_profile,docker_nscpx_image"
394          }
395   ,
396        {
397
398           "access_type": true,
399           "resource_type": "docker_host",
400           "operation_name": "get",
401           "dependent_resources": "download,ns_snmp_config,ns_conf,
                 ns_ns_runningconfig,ns_ns_savedconfig,smtp_server,
                 mps_datacenter,ns_device_profile,traceroute,inventory,
                 inventory_status,ping,active_event,ns_ns_license,ns_ns_mode,
                 ns_network_interface"
402          }
403   ,
404        {
405
406           "access_type": true,
407           "resource_type": "perf_reports",
408           "operation_name": "add",
409           "dependent_resources": "mail_profile,slack_profile,smtp_server,
                 perf_custom_dashboard"
410          }
411   ,
412        {
413
414           "access_type": true,
415           "resource_type": "perf_reports",
416           "operation_name": "get",
417           "dependent_resources": "download,smtp_server,
                 perf_report_counters,perf_res_util_report,
                 perf_http_req_tcp_conn_report,perf_lb_ssl_traffic_report,
                 perf_ip_bytes_rxtx_report,perf_ip_pkt_rxtx_report,
                 perf_icmp_pkt_rxtx_report,perf_icmp_bytes_rxtx_report,
                 perf_icmpv6_pkt_rxtx_report,perf_icmpv6_bytes_rxtx_report,
                 perf_ipv6_bytes_rxtx_report,perf_ipv6_pkt_rxtx_report,
                 perf_udp_bytes_rxtx_report,perf_udp_packets_rxtx_report,
                 perf_cmp_bytes_rxtx_report,perf_cmp_tcp_bytes_rxtx_report,
                 perf_cmp_tcp_ratiosaving_report,
                 perf_cmp_decmp_bytes_rxtx_report,
```



```
                perf_cmp_decmp_ratiosaving_report,
                perf_tcp_server_conn_report,
                perf_tcp_surgelen_spareconn_report,perf_http_bytes_rx_report
                ,perf_http_gets_posts_report,
                perf_ssl_transactions_hits_report,
                perf_ssl_client_auth_report,perf_ssl_rsa_dhkey_report,
                perf_ssl_frontend_ciphers_report,
                perf_ssl_backend_ciphers_report,
                perf_wsdevice_cpu_utilization_report,
                perf_wsdevice_send_compression_ratio_report,
                perf_wsdevice_connected_plugins_report,
                perf_wsdevice_data_reduction_report,
                perf_wsdevice_link_utilization_report,
                perf_wsserviceclassstatstable_pass_through_connection_report
                ,perf_wsserviceclassstatstable_service_class_report,
                perf_wsserviceclassstatstable_acceleration_report,
                perf_wslinkstatstable_throughput_report,
                perf_wslinkstatstable_packet_loss_report,
                perf_wsappstatstable_application_report,
                perf_wsqosstatstable_qos_report,
                perf_ssl_cpu_keyexchange_report,perf_ssl_be_rsa_dhkey_report
                ,perf_custom_dashboard,perf_ns_throughput_report,
                perf_network_interface_report"
418          }
419   ,
420        {
421
422          "access_type": true,
423          "resource_type": "perf_threshold",
424          "operation_name": "get",
425          "dependent_resources": "download,perf_reports,
                perf_report_counters,smtp_server,sms_server,sms_profile"
426          }
427   ,
428        {
429
430          "access_type": true,
431          "resource_type": "perf_threshold",
432          "operation_name": "add",
433          "dependent_resources": "mail_profile,slack_profile,smtp_server,
                sms_server,sms_profile"
434          }
435   ,
436        {
437
```



```
438           "access_type": true,
439           "resource_type": "perf_poll_config",
440           "operation_name": "add",
441           "dependent_resources": "mail_profile,slack_profile,smtp_server"
442         }
443   ,
444         {
445
446           "access_type": true,
447           "resource_type": "perf_poll_config",
448           "operation_name": "get",
449           "dependent_resources": "smtp_server,download"
450         }
451   ,
452         {
453
454           "access_type": true,
455           "resource_type": "license_server_info",
456           "operation_name": "get",
457           "dependent_resources": "sms_server,license_proxy_server,
                jazz_license,download,sms_profile,smtp_server,
                user_managed_tp_vserver,managed_vserver,user_managed_vserver
                ,haproxy_frontend,haproxy_backend,license_file,
                device_license_info,license_info,ns_authenticationvserver,
                ns_gslbvserver,ns_vpnvserver,ns_csvserver,ns_crvserver,
                ns_lbvserver,autoselection_preference,license_threshold,
                license_expiry_info"
458         }
459   ,
460         {
461
462           "access_type": true,
463           "resource_type": "license_server_info",
464           "operation_name": "add",
465           "dependent_resources": "sms_server,license_proxy_server,
                jazz_license,sms_profile,mail_profile,slack_profile,
                smtp_server,user_managed_tp_vserver,managed_vserver,upload,
                license_file,license_info,license_threshold,mas_license,
                user_managed_vserver,autoselection_preference,
                license_expiry_info"
466         }
467
468       ],
469       "ui": [
470         {
```



```
471
472           "access_type": true,
473           "name": "ApplicationsDashboard",
474           "display_name": "Dashboard"
475         }
476   ,
477         {
478
479           "access_type": true,
480           "name": "SecurityDashboard",
481           "display_name": "App Security Dashboard"
482         }
483   ,
484         {
485
486           "access_type": true,
487           "name": "Stylebooks",
488           "display_name": "StyleBooks"
489         }
490   ,
491         {
492
493           "access_type": true,
494           "name": "Stylebooks",
495           "display_name": "Configpacks"
496         }
497   ,
498         {
499
500           "access_type": true,
501           "name": "StylebooksSettings",
502           "display_name": "Settings"
503         }
504   ,
505         {
506
507           "access_type": true,
508           "name": "CacheRedirection",
509           "display_name": "Cache Redirection"
510         }
511   ,
512         {
513
514           "access_type": true,
515           "name": "HAProxy",
```



```
          "display_name": "HAProxy"
        }
  ,
      {

        "access_type": true,
        "name": "Servers",
        "display_name": "Servers"
        }
  ,
      {

        "access_type": true,
        "name": "VirtualServers",
        "display_name": "Virtual Servers"
        }
  ,
      {

        "access_type": true,
        "name": "Services",
        "display_name": "Services"
        }
  ,
      {

        "access_type": true,
        "name": "ServiceGroups",
        "display_name": "Service Groups"
        }
  ,
      {

        "access_type": true,
       "name": "Authentication",
        "display_name": "Authentication"
        }
  ,
      {

        "access_type": true,
        "name": "MonitoringAuditing",
        "display_name": "Auditing"
        }
  ,
```



```
561         {
562
563           "access_type": true,
564           "name": "MonitoringSettings",
565           "display_name": "Settings"
566          }
567   ,
568         {
569
570           "access_type": true,
571           "name": "GSLBDomains",
572           "display_name": "Domains"
573          }
574   ,
575         {
576
577           "access_type": true,
578           "name": "GSLBServices",
579           "display_name": "Services"
580          }
581   ,
582         {
583
584           "access_type": true,
585           "name": "GSLBVirtualServer",
586           "display_name": "Virtual Server"
587          }
588   ,
589         {
590
591           "access_type": true,
592           "name": "NetScalerGateway",
593           "display_name": "NetScaler Gateway"
594          }
595   ,
596         {
597
598           "access_type": true,
599           "name": "ContentSwitching",
600           "display_name": "Content Switching"
601          }
602   ,
603         {
604
605           "access_type": true,
```



```
606           "name": "DNSDomainNames",
607           "display_name": "DNS Domain Names"
608         }
609   ,
610       {
611
612           "access_type": true,
613           "name": "NetworkDashboard",
614           "display_name": "Instances Dashboard"
615         }
616   ,
617       {
618
619           "access_type": true,
620           "name": "NetScalerSDWANWOInstances",
621           "display_name": "NetScaler SD-WAN"
622         }
623   ,
624       {
625
626           "access_type": true,
627           "name": "InstanceOperations",
628           "display_name": "Instance Operations"
629         }
630   ,
631       {
632
633           "access_type": true,
634           "name": "NetScalerInstances",
635           "display_name": "NetScaler ADC"
636         }
637   ,
638       {
639
640           "access_type": true,
641           "name": "HAProxyInstances",
642           "display_name": "HAProxy"
643         }
644   ,
645       {
646
647           "access_type": true,
648           "name": "NetScalerCPXDockerHost",
649           "display_name": "Docker Hosts"
650         }
```



```
651  ,
652        {
653
654          "access_type": true,
655          "name": "Reports",
656          "display_name": "Reports"
657         }
658  ,
659        {
660
661          "access_type": true,
662          "name": "Thresholds",
663          "display_name": "Thresholds"
664         }
665  ,
666        {
667
668          "access_type": true,
669          "name": "ReportingSettings",
670          "display_name": "Settings"
671         }
672  ,
673        {
674
675          "access_type": true,
676          "name": "Licenses",
677          "display_name": "License Management"
678         }
679
680      ]
681     }
682
683  }
684
685  <!--NeedCopy-->
```

REST API を使用してアクセスロールを作成する

```
1  URL: https://<MAS_IP>/nitro/v2/config/rba_role
2  HTTPMETHOD: POST
3
4  Payload:
5  {
6
```



```
  "rba_role": {

    "name": "AppOwnerRole",
    "description": "ExampleCompany App Owner Role",
    "policies": [
      "AppOwnerAccessPolicy"
    ]
   }

<!--NeedCopy-->
```

新しい **GSLB StyleBook** をアップロードするための **REST API**

```
URL: https://<MAS_IP>/stylebook/nitro/v2/config/stylebooks
HTTPMETHOD: POST

Payload:
{

    "stylebook": {

      "file_name": "my-own-gslb.yaml",
      "source": "bmFtZTogZ3NsYi1kbnMtZG9tYW...aXRvcm5hbWU=",
      "encoding": "base64"
     }

   }

<!--NeedCopy-->
```

> 注:
>
> StyleBook の名前は、システム上で変更される場合があります。

REST API を使用してグループを作成し、選択したインスタンスと **StyleBook** を割り当てる

```
URL: https://<MAS_IP>/nitro/v2/config/mpsgroup
HTTPMETHOD: POST

Payload:
{

  "mpsgroup": {
```



```
8
9       "id": "",
10      "name": "AppOwnerGroup1",
11      "description": "ExampleCompany App Owner Group",
12      "roles": [
13        "AppOwnerRole"
14      ],
15      "enable_session_timeout": false,
16      "assign_all_devices": false,
17      "ass ign_all_apps": false,
18      "application_names_with_regex": [
19
20      ],
21      "standalone_instances_id": [
22        "72c178da-47df-4426-9acc-cd6316f92506",
23        "c948061e-6240-4062-931c-f6988ef36e3b"
24      ],
25      "application_list": [
26
27      ],
28      "permission": "none",
29      "application_names": [
30
31      ],
32      "authscope_props": [
33        {
34
35          "propname": "configuration_template_id",
36          "propvalues": [
37            "NONE"
38          ]
39        }
40  ,
41        {
42
43          "propname": "dns_domain_entry_id",
44          "propvalues": [
45            "cf6631e5-2f56-4bb1-b0a5-90fabfc0e3e2",
46            "b268905c-522d-47e3-a2ca-3f8d8a754373"
47          ]
48        }
49  ,
50        {
51
52          "propname": "stylebook_id",
```



```
          "propvalues": [
            "gslbbb963abe85936913035e1d4dd14b56f7",
            "moni72fad4494466d102b19c18ac329fa9f3"
          ]
         }

     ],
     "tenant_id": "6d024111-6636-4571-a250-d47b31aba7a8"
    }

 }

<!--NeedCopy-->
```

注:

上記の API ペイロードで使用する DNS ドメイン名、および GSLB StyleBooks の ID を取得するには、通常の Citrix ADM API を使用してエンティティ名に対応する ID を照会できます。たとえば、「app1.acme.com」という DNS ドメインの ID を取得するには、次の Citrix ADM REST API を使用できます。

```
URL: https://<MAS_IP>/nitro/v2/config/dns_domain_entry?filter=name:
    app1.acme.com
HTTPMETHOD: GET

The ID of this domain can be extracted from the following response.
{

  "errorcode": 0,
  "message": "Done",
  "operation": "get",
  "resourceType": "dns_domain_entry",
  "username": "nsroot",
  "tenant_name": "Owner",
  "tenant_id": "568d8e12-1d88-42b2-8943-cbaa04826fd1",
  "resourceName": "",
  "dns_domain_entry": [
    {

      "tenant_id": "568d8e12-1d88-42b2-8943-cbaa04826fd1",
      "name": "app1.acme.com",
      "id": "3e3d85ea-1c21-49b2-97f4-60fccdbae2e0",
      "description": "app1 domain name"
     }

  ]
```



```
 }

<!--NeedCopy-->
```

同様に、名前空間が com.citrix.adc.stylebook、バージョン:1.0、名前:my-own-gslbである StyleBook の StyleBook ID を取得するには、次の API を使用できます。

```
URL: https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks?filter=name:
   my-own-gslb,namespace:com.citrix.adc.stylebooks,version:1.0
HTTPMETHOD: GET
<!--NeedCopy-->
```

レスポンスには、ID 属性を含む StyleBook の詳細が含まれます。

```
{

  "stylebooks": [
    {

      "author": null,
      "builtin": "false",
      "builtins": "{
 "netscaler.nitro.config": "10.5" }
 ",
      "deprecate": "false",
      "description": " This StyleBook is used to configure one or a
         number of Citrix ADCs in different sites into a GSLB setup. It
          is assumed that the SNIP IP on each Citrix ADC to be used by
         this StyleBook as the Site IP is already configured on the
         appliance.",
      "display_name": "HTTP/SSL LoadBalancing StyleBook",
      "filename": "my-own-gslb.yaml",
      "hide": null,
      "id": "gslb5a748d8b7684846cf6c409ad7dea8ccf",
      "imported_by": "",
      "imported_datetime": "2018-05-25 17:20:32.848902",
      "name": "my-own-gslb",
      "namespace": "com.citrix.adc.stylebooks",
      "pkg_id": "gslb5a748d8b7684846cf6c409ad7dea8ccf",
      "primary_keys": "["name"]",
      "private": "false",
      "recompile": "false",
      "schema_version": "1.0",
      "source": "LS0tIApuYW1lOiBsYgpuYW1lc…",
      "system": null,
```



```
        "tags": "",
        "tenant_id": null,
        "user_sb": "false",
        "version": "1.0"
       }
  ,
      {

        …
       }

   ]
  }

<!--NeedCopy-->
```

> 注:
>
> 上記の API は、フィルタに一致する StyleBook のリストを返します。応答から正しい StyleBook を選択して、ID を取得してください。

システムユーザーを作成するための **REST API**

> 注:
>
> この手順はオプションです。

```
URL: https://<MAS_IP>/nitro/v2/config/mpsuser
HTTPMETHOD: POST

Payload:
{

  "mpsuser": {

     "name": "John",
     "password": "welcome",
     "external_authentication": false,
     "enable_session_timeout": false,
     "groups": [
       "AppOwnerGroup1"
     ]
    }

 }

```

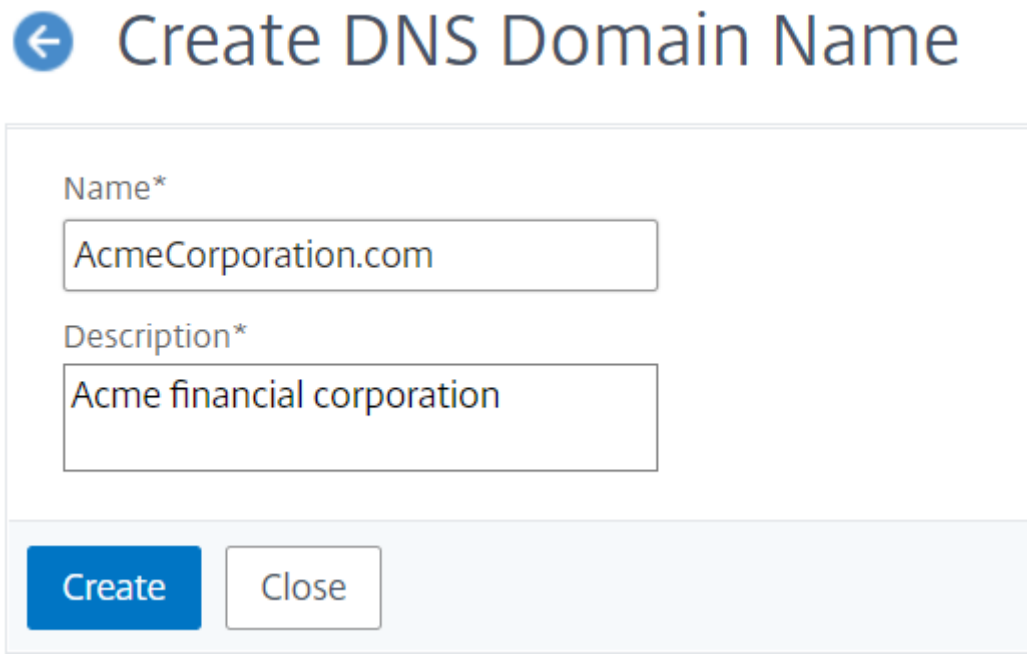


```
<!--NeedCopy-->
```

アプリケーション所有者のワークフロー

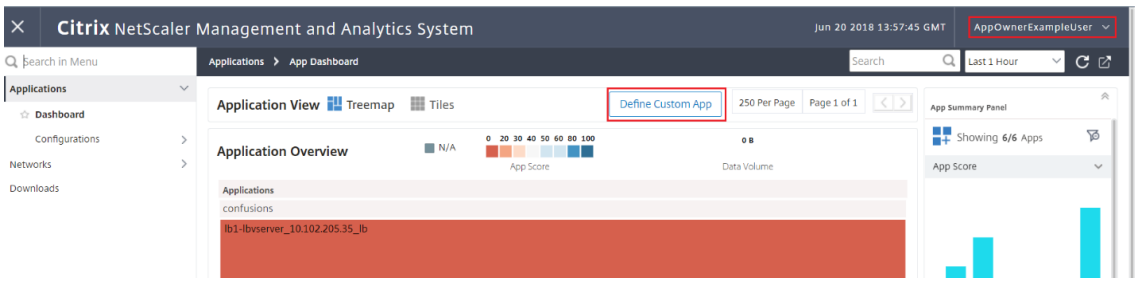
ユーザーは、資格情報を使用してアプリケーションユーザーとしてログオンする必要があります。ユーザーはこのタスクに従って、独自の DNS ドメイン名を作成し、新しい GSLB StyleBook を使用する必要があります。

1. Citrix ADM で、［ネットワーク］>［**DNS** ドメイン名］に移動します。
2. [追加] をクリックして、新しい DNS ドメインを作成します。Citrix ADM で DNS ドメインを作成します。

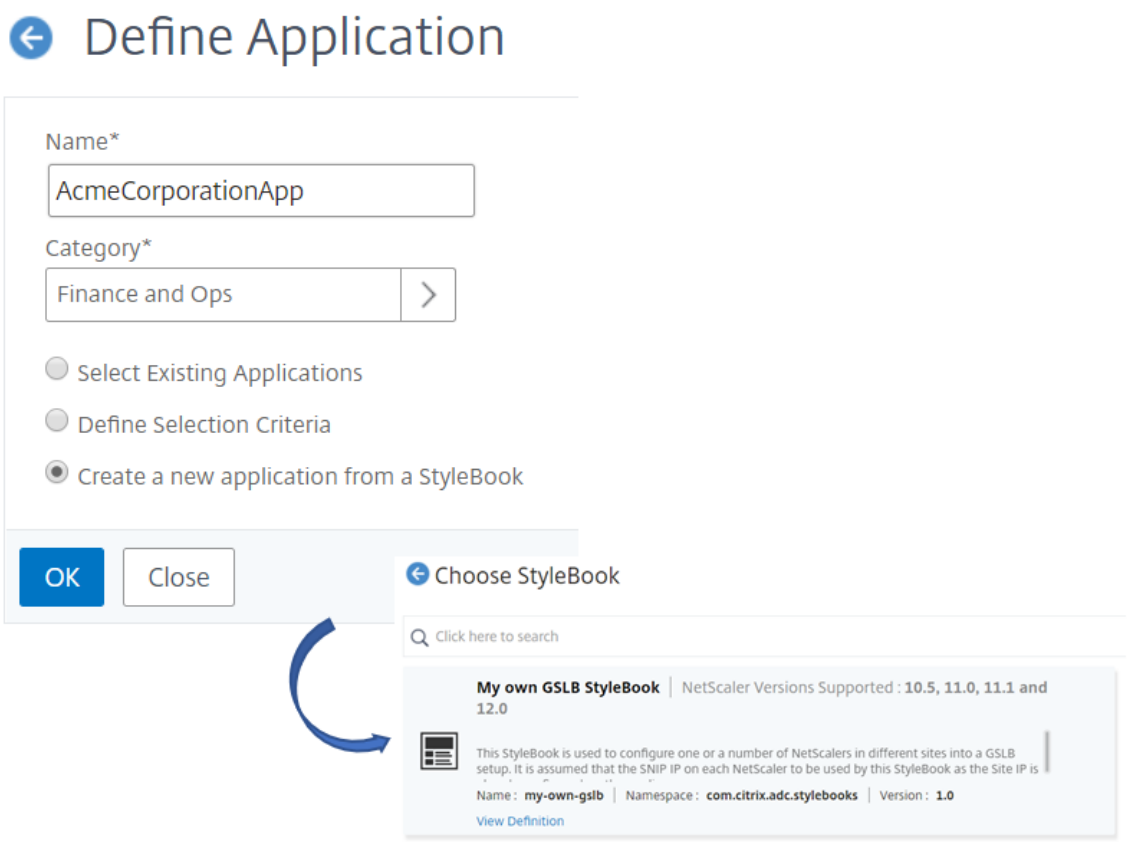


> 注:
>
> 管理者は、これらのドメイン名を作成し、ユーザーグループに割り当てることもできます。

3. [アプリケーション] > [ダッシュボード] に移動し、[カスタムアプリケーションの定義] をクリックします。



4. アプリケーションの名前を入力し、カテゴリを選択します。**StyleBook** から新しいアプリケーションを作成を選択し、「**OK**」をクリックします。[自分の **GSLB StyleBook**] を選択して、選択したインスタンスに設定をデプロイします。



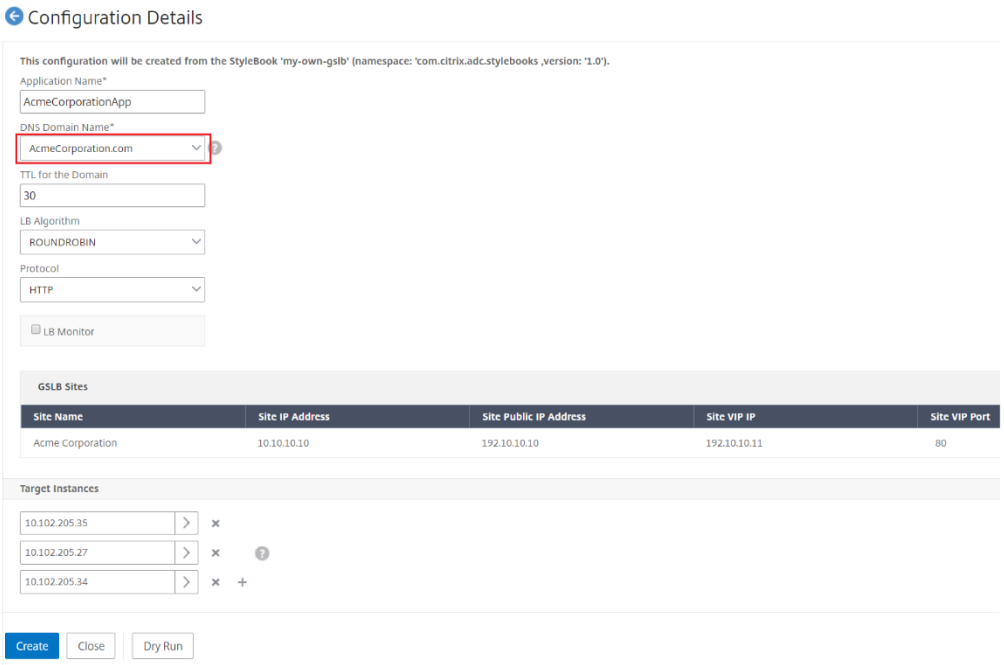
5. StyleBook のすべてのパラメータに必要な値を入力します。

   a) リストからドメイン名を選択します。

   b) 必要に応じて、アプリケーションの GSLB サイトを追加します。

   c) すべての GSLB サイトでターゲット Citrix ADC インスタンスを選択します。

   d) [**Create**] をクリックして、GSLB 設定を作成します。



> 注:
>
> StyleBook パラメータ「DNS ドメイン名」には、Citrix ADM でユーザーに属する DNS ドメインの一覧のみが表示されます。

アプリ所有者のワークフロー用の **Citrix ADM REST API**

Citrix ADM にログオンするための **REST API**

```
URL: http: //<MAS_IP>/nitro/v2/config/login
HTTPMETHOD: POST

Payload:
{

  "login": {

    "username": "<USER_NAME>",
    "password": "<PASSWORD>",
    "session_timeout": 1800
   }

 }

<!--NeedCopy-->
```


DNS ドメイン名を作成する **REST API**

```
URL: https://<MAS_IP>/nitro/v2/config/dns_domain_entry
HTTP METHOD: POST
PAYLOAD: {
 "dns_domain_entry":{
 "name":"app1.acme.com","description":"app1 acme domain"
 }

 }

<!--NeedCopy-->
```

StyleBook を使用してアプリケーションを作成する **REST API**

```
URL: https://<MAS_IP>/nitro/v2/config/application
HTTPMETHOD: POST

Payload:
{

  "params": {

    "action": "app_discovery"
   }
 ,
  "application": {

    "id": "",
    "name": "app1",
    "app_c ategory": "ITOps",
    "stylebook_params": "{
 "name":"my-own-gslb","namespace":"com.citrix.adc.stylebooks","version"
    :"1.0","configpack_payload":{
 "parameters":{
 "name":"app1","domain-name":"app1.acme.com",]"ttl":"30","algorithm":"
    ROUNDROBIN","protocol":"HTTP","sites":[{
 "name":"site1","ipaddress":"6.5.6.77","virtual-ip":"88.6.5.44","
    virtual-port":"80" }
 ] }
 ,"targets":[ {
 "id":"72c178da-47df-4426-9acc-cd6316f92506" }
 , {
 "id":"0e4d0789-bffe-4266-ba1c-09adfc61db4e" }
```

```
 , {
"id":"b5af4455-3f06-4f56-b0cb-3d9f868c1f94" }
] }
 }
"
  }

}

<!--NeedCopy-->
```

上記のペイロードでは:

- 「stylebook_params」には、使用する StyleBook の名前、名前空間、バージョンが含まれています。
- 上記の同等の GUI フォームに示すように、「configpack_payload」には、StyleBook のパラメータが入力されています。Citrix ADM は、ユーザーがアクセスできる DNS ドメイン名のみを、パラメータ「ドメイン名」の値として使用できるようにします。
- 「ターゲット」には、GSLB 構成が展開される NetScaler ID の一覧（GSLB サイトの ADC インスタンス）が含まれます。

NetScaler の管理 IP アドレスを指定して NetScaler ID を取得するには、次の Citrix ADM API を使用できます。

```
URL: https://<MAS_IP>/nitro/v2/config/ns?filter=ip_address:
   192.168.153.162
HTTPMETHOD: GET
<!--NeedCopy-->
```

応答ペイロードには、この NetScaler に関する情報（ID を含む）が含まれます。

```
{

  "errorcode": 0,
  "message": "Done",
  ⋯.."tenant_id": "ec0eb868-0d6b-4729-bfbd-3005dd2694c1",
  "resourceName": "",
  "ns": [
    {

      "manufacturedate": "9/30/2009",
      "is_grace": "false",
      "hostname": "youcef-ns",
      "std_bw_config": "0",
      "gateway_deployment": "false",
      "gateway_ipv6": "",
      "ha_master_state": "Primary",
```



```
        "instance_available": "0",
        "device_finger_print": "",
        "instance_state": "Down",
        "reason": "Device not reachable",
        "name": "",
        "ent_bw_available": "0",
        "description": "",
        "id": "da9ffff2-c100-45f1-a913-c542718338b2",
        "mgmt_ip_address": "192.168.153.162",
        ….
       }

   ]
  }

<!--NeedCopy-->
```

スタイルブックを構築する

ファイル「my-own-gslb.yaml」StyleBook の全内容を以下に示します。このカスタム StyleBook は、そのまま使用することも、必要に応じてカスタマイズして、必要な GSLB 構成を生成することもできます。DNS 名機能を利用するには、この StyleBook の「ドメイン名」という重要なパラメータが StyleBook に存在する必要があります。

```
name: my-own-gslb
namespace: com.citrix.adc.stylebooks
version: "1.0"
display-name: My own GSLB StyleBook
description: This StyleBook is used to configure one or a number of
    NetScalers in different sites into a GSLB setup. It is assumed that
    the SNIP IP on each NetScaler to be used by this StyleBook as the
    Site IP is already configured on the appliance.
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
  -
    namespace: com.citrix.adc.commontypes
    version: "1.0"
    prefix: cmtypes
parameters:
  -
```



```
18      name: name
19      label: Application Name
20      type: string
21      required: true
22      key: true
23
24    -
25      name: domain-name
26      label: DNS Domain Name
27      description: GSLB DNS Domain Name
28      type: string
29      required: true
30      allowed-dynamic-values:
31        source: local
32        resource-type: dns_domain_entry
33
34    -
35      name: ttl
36      label: TTL for the Domain
37      description: Time-To-Live value (number of seconds) for the Domain
38      type: number
39      default: 30
40
41    -
42      name: algorithm
43      label: LB Algorithm
44      description: Global Load Balancing Algorithm
45      type: string
46      default: ROUNDROBIN
47      allowed-values:
48        - ROUNDROBIN
49        - STATICPROXIMITY
50        - SOURCEIPHASH
51
52    -
53      name: protocol
54      label: Protocol
55      description: The protocol of the GSLB VIP
56      type: string
57      default: HTTP
58      allowed-values:
59        - HTTP
60        - FTP
61        - TCP
62        - UDP
```



```
63          - SSL
64          - SSL_BRIDGE
65          - SSL_TCP
66          - NNTP
67          - ANY
68          - SIP_UDP
69          - SIP_TCP
70          - SIP_SSL
71          - RADIUS
72          - RDP
73          - RTSP
74          - MYSQL
75          - MSSQL
76          - ORACLE
77
78      -
79        name: monitor
80        label: LB Monitor
81        description: Monitor to be bound to the GSLB service
82        type: cmtypes::monitor
83
84      -
85        name: sites
86        label: GSLB Sites
87        description: Provide information about the GSLB Sites
88        type: object[]
89        required: true
90        parameters:
91          -
92            name: name
93            label: Site Name
94            type: string
95            required: true
96          -
97            name: ipaddress
98            label: Site IP Address
99            description: The IP Address of this Site. Use a SNIP IP address
                  on the site's appliance.
100           type: ipaddress
101           required: true
102         -
103           name: public-ipaddress
104           label: Site Public IP Address
105           description: The Public IP Address of this Site. It NATs to the
                  Site's IP address
```



```
106         type: ipaddress
107       -
108         name: virtual-ip
109         label: Site VIP IP
110         description: The IP Address for the GSLB Service on this site (
                The VIP on this Site)
111         type: ipaddress
112         required: true
113       -
114         name: virtual-port
115         label: Site VIP Port
116         description: The port number for the GSLB Service (VIP) on this
                site
117         type: tcp-port
118         default: 80
119
120   components:
121     -
122       name: enable-gslb-comp
123       type: ns::nsfeature
124       description: Enables the GSLB feature
125       meta-properties:
126         action: enable
127       properties:
128         feature: ["GSLB", "LB"]
129     -
130       name: gslb-monitor-comp
131       type: cmtypes::monitor
132       condition: $parameters.monitor
133       properties:
134         monitorname: $parameters.name + "-" + $parameters.monitor.
              monitorname + "-gslbmon"
135         type: $parameters.monitor.type
136         destip?: $parameters.monitor.destip
137         destport?: $parameters.monitor.destport
138         httprequest?: $parameters.monitor.httprequest
139         send?: $parameters.monitor.send
140         customheaders?: $parameters.monitor.customheaders
141         respcodes?: $parameters.monitor.respcodes
142         recv?: $parameters.monitor.recv
143         lrtm?: $parameters.monitor.lrtm
144         secure?: $parameters.monitor.secure
145         interval?: $parameters.monitor.interval
146         interval_units?: $parameters.monitor.interval_units
147         resptimeout?: $parameters.monitor.resptimeout
```



```
148         retries?: $parameters.monitor.retries
149         downtime?: $parameters.monitor.downtime
150     -
151       name: gslb-vserver-comp
152       type: ns::gslbvserver
153       description: Creates a GSLB VServer config object
154       properties:
155         name: $parameters.name + "-gslbvserver"
156         servicetype: $parameters.protocol
157         lbmethod: $parameters.algorithm
158       components:
159         -
160           name: gslb-domain-comp
161           type: ns::gslbvserver_domain_binding
162           properties:
163             name: $parent.properties.name
164             domainname: $parameters.domain-name
165             ttl: $parameters.ttl
166     -
167       name: gslb-site-comp
168       type: ns::gslbsite
169       description: Creates a GSLB Site config object
170       repeat: $parameters.sites
171       repeat-item: site
172       properties:
173         sitename: $parameters.name + "-" + $site.name + "-gslbsite"
174         siteipaddress: $site.ipaddress
175         publicip?: $site.public-ipaddress
176       components:
177         -
178           name: gslb-service-comp
179           type: ns::gslbservice
180           description: Creates a GSLB Service
181           properties:
182             servicename: $parameters.name + "-" + $site.name + "-
                  gslbservice"
183             ip: $site.virtual-ip
184             servicetype: $parameters.protocol
185             port: $site.virtual-port
186             sitename: $parent.properties.sitename
187           components:
188             -
189               name: gslb-vserver-service-binding-comp
190               type: ns::gslbvserver_gslbservice_binding
191               description: Creates a Binding between the GSLB vserver and
```



```
                    the GSLB Service
192               properties:
193                 name: $components.gslb-vserver-comp.properties.name
194                 servicename: $parent.properties.servicename
195             -
196               name: gslb-service-monitor-binding-comp
197               type: ns::gslbservice_lbmonitor_binding
198               description: Creates a Binding between the GSLB service and
                      the GSLB monitor
199               condition: $parameters.monitor
200               properties:
201                 servicename: $parent.properties.servicename
202                 monitor_name: $components.gslb-monitor-comp.properties.
                        monitorname
203   <!--NeedCopy-->
```

API を使用して StyleBook から設定を作成する

May 7, 2021

StyleBook を構築したら、Citrix ADM または Citrix ADM API を使用して、その StyleBook を Citrix Application Delivery Management（ADM）にインポートする必要があります。Citrix ADM は、インポート時に StyleBook を検証します。検証が成功すると、StyleBook の Citrix ADM カタログに StyleBook が表示され、構成の作成に使用できます。

StyleBook API を使用して、この StyleBook に基づいて構成を作成できるようになりました。cURL コマンドラインツールや Postman Chrome ブラウザ拡張機能などの任意のツールを使用して、HTTP リクエストを Citrix ADM に送信できます。

例 1

負荷分散仮想サーバーを作成するための StyleBookで作成したlb-vserverStyleBook を考えてみましょう。次のように、REST API を使用して、この StyleBook から設定パックを作成します。

HTTP メソッド: ポスト

URL: `https://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/lb-vserver/configpacks`

リクエストヘッダー:

Content-Type: application/json

Accept: application/json

リクエストボディペイロード**:**

```
{

  "configpack":
  {

    "parameters": {

      "name": "lb1",
      "ip": "10.102.117.31"
     }
 ,
    "targets":
    [
      {

        "id": "deecee30-f478-4446-9741-a85041903410"
       }

    ]
   }

 }

<!--NeedCopy-->
```

この HTTP リクエストでは、ID（例: ”deecee30-f478-4446-9741-a85041903410”）は、負荷分散仮想サーバー lb1 が IP アドレス 10.102.117.31 が作成される Citrix ADC インスタンスのインスタンス ID です。Citrix ADC インスタンスのインスタンス ID は、Citrix ADM から取得されます。

Citrix ADM によって管理されるインスタンスの ID を取得するには、Citrix ADM API を使用します。たとえば、IP アドレスが 192.168.153.160 のインスタンス ID または Citrix ADC インスタンスを取得するには、次の API を使用できます。

HTTP メソッド**:** 取得

URL: `https://<ADM-IP>/nitro/v1/config/ns?filter=ip_address:192.168.153.160`

リクエストヘッダー**:**

Accept: application/json

応答には、JSON ペイロードの ID が含まれています。

期待されるレスポンスヘッダー **(**成功した場合**):**

200 OK

Content-Type: application/json

期待されるレスポンスボディ **(**成功した場合**):**

```
{

  "errorcode": 0,
  "message": "Done",
  "operation": "get",
  "resourceType": "ns",
  "username": "nsroot",
  "tenant_name": "Owner",
  "resourceName": "",
  "ns":
  [
    {

    "is_grace": "false",
    "hostname": "",
    "std_bw_config": "0",
    "gateway_deployment": "false",
    "id": "deecee30-f478-4446-9741-a85041903410",
    }

 ]
 }

<!--NeedCopy-->
```

構成 (構成パック) が正常に作成されると、次の HTTP 応答が表示されます。

期待されるレスポンスヘッダー **(**成功した場合**):**

200 OK

Content-Type: application/json

期待されるレスポンスボディ **(**成功した場合**):**

```
{

  "configpack":
  {

    "config_id": "1460806080"
   }

 }
```



```
10
11  <!--NeedCopy-->
```

ID 1460806080 を使用して一意に識別される最初の構成 (構成パック) を作成しました。この ID を使用して、構成のクエリ、更新、削除を行えます。

例 2

同じ StyleBook を使用して別の構成パックまたは構成パックを作成し、同じまたは異なる Citrix ADC インスタンスで実行できます。この例では、別の構成を作成し、仮想サーバーに異なる名前と IP アドレスを指定します。また、負荷分散の方法として LEASTCONNECTION を指定します。この構成を 2 つの Citrix ADC インスタンスに展開します。

HTTP 要求は次のとおりです。

HTTP メソッド**:** ポスト

URL: `https://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/lb-vserver/configpacks`

リクエストヘッダー**:**

Content-Type: application/json

Accept: application/json

リクエストボディペイロード**:**

```
1  {
2
3    "configpack":
4    {
5
6      "parameters":
7      {
8
9        "name": "lb2",
10       "ip": "10.102.117.32",
11       "lb-alg": "LEASTCONNECTION"
12      }
13   ,
14     "targets"
15     [
16      {
17   "id": "deecee30-f478-4446-9741-a85041903410" }
18   ,
19      {
```



```
20   "id": "debecc60-d589-4557-8632-a74032802412" }
21
22      ]
23     }
24
25   }
26
27  <!--NeedCopy-->
```

この HTTP リクエストでは、IP アドレス 10.102.117.32 の負荷分散仮想サーバー lb2 が、ids “deecee30-f478-4446-9741-a85041903410” と”debecc60-d589-4557-8632-a74032802412” で表される 2 つの Citrix ADC インスタンスに作成されます。

構成パックが正常に作成されると、次の HTTP 応答が受信されます。

期待されるレスポンスヘッダー **(**成功した場合**):**

200 OK

Content-Type: application/json

期待されるレスポンスボディ **(**成功した場合**):**

```
1  {
2
3     "configpack":
4    {
5
6       "config_id": "1657696292"
7     }
8
9   }
10
11  <!--NeedCopy-->
```

この新しい構成パックには、異なる ID 165769629 があります。この ID を使用することで、この構成を更新または削除できます。

例 **3**

基本的な負荷分散の構成を作成するための StyleBookで作成した「basic-lb-config」スタイルブックについて検討してください。次のように、REST API を使用して、この StyleBook から設定パックを作成します。

HTTP メソッド**:** ポスト

URL: `http://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/basic-lb-config/configpacks`

リクエストヘッダー**:**

Content-Type: application/json

Accept: application/json

期待されるレスポンスヘッダー **(**成功した場合**):**

200 OK

Content-Type: application/json

期待されるレスポンスボディ **(**成功した場合**):**

```
{

  "configpack":
  {

    "parameters":
    {

      "name": "myapp",
      "ip": "10.70.122.25",
      "svc-servers": ["192.168.100.11","192.168.100.12"],
       "svc-port": 8080
     }
 ,
    "targets":
    [
     {

      "id": "deecee30-f478-4446-9741-a85041903410"
      }
 ,
     {

      "id": "debecc60-d589-4557-8632-a74032802412"
      }

    ]
   }

 }

<!--NeedCopy-->
```

この HTTP リクエストでは、負荷分散構成は 2 つの Citrix ADC インスタンス上で実行します。これらの Citrix ADC

インスタンスにログオンして、仮想サーバーと 2 つのサービスがバインドされたサービスグループが作成されているかどうかを確認できます。

例 **4**

複合 StyleBook の作成で作成した複合 StyleBook **composite-example** を考えてみましょう。次のように、REST API を使用して、この StyleBook から設定パックを作成します。

HTTP メソッド**:** ポスト

URL: `http://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpacks`

リクエストヘッダー**:**

Content-Type: application/json

Accept: application/json

リクエストボディペイロード**:**

```
{

  "configpack":
  {

    "parameters": {

      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53"]
     }
 ,
    "targets":
    [
     {

      "id": "deecee30-f478-4446-9741-a85041903410"
      }
 ,
     {

      "id": "debecc60-d589-4557-8632-a74032802412"
      }

    ]
   }
```



```
27
28   }
29
30 <!--NeedCopy-->
```

この HTTP リクエストでは、ID で表される 2 つの Citrix ADC インスタンスで構成が作成されます。Citrix ADC インスタンスにログオンすると、「複合例」スタイルブックにインポートされた「basic-lb-config」スタイルブックで作成された構成オブジェクトを表示できます。また、「複合例」StyleBook の一部であったmyapp-monという新しい HTTP モニターも見られます。

構成パックが正常に作成されると、次の HTTP 応答が受信されます。

期待されるレスポンスヘッダー **(**成功した場合**):**

200 OK

Content-Type: application/json

期待されるレスポンスボディ **(**成功した場合**):**

```
1  {
2
3    "configpack": {
4
5      "config_id": "4917276817"
6     }
7
8   }
9
10 <!--NeedCopy-->
```

構成の更新

たとえば、IP アドレス 10.102.29.54 の新しいバックエンドサーバーを負荷分散仮想サーバーmyappに追加して、この構成を更新するには、次のように設定パックを更新するための API を使用します。

HTTP メソッド： PUT

URL: `http://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpacks/4917276817`

リクエストヘッダー**:**

Content-Type: application/json

Accept: application/json

リクエストボディペイロード**:**


```
{

  "configpack": {

    "parameters": {

      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]
   }
 ,
  "targets":
   [
     {

      "id": "deecee30-f478-4446-9741-a85041903410"
      }
 ,
     {

      "id": "debecc60-d589-4557-8632-a74032802412"
      }

   ]
   }

 }

<!--NeedCopy-->
```

構成パックが正常に更新されると、次の HTTP 応答が受信されます。

期待されるレスポンスヘッダー **(**成功した場合**):**

200 OK

Content-Type: application/json

期待されるレスポンスボディ **(**成功した場合**):**

```
{

   "configpack": {

     "config-id": "4917276817"
   }
```



```
7
8   }
9
10  <!--NeedCopy-->
```

構成の削除

この構成を（すべての Citrix ADC インスタンスから）削除するには、次のように API を使用して構成パックを削除します。

構成パックが正常に削除されると、次の HTTP 応答が受信されます。

HTTP メソッド**:** DELETE

URL: `http://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpacks/4917276817`

リクエストヘッダー**:**

Accept: application/json

期待されるレスポンスヘッダー **(**成功した場合**):**

200 OK

Content-Type: application/json

予想される応答ペイロード **(**成功した場合**):**

```
1  {
2
3     "configpack": {
4
5       "config_id": "4917276817"
6     }
7
8   }
9
10  <!--NeedCopy-->
```

Citrix ADC インスタンスにログオンし、この構成パックに含まれるすべての構成オブジェクトが削除されたことを確認できます。

すべてのインスタンスからではなく、特定の Citrix ADC インスタンスから構成を削除する場合は、上記の構成パックの更新操作を使用し、JSON ペイロードの「targets」属性を変更して特定の Citrix ADC インスタンス ID を削除します。

API を使用して証明書とキーファイルをアップロードする設定を作成する

May 7, 2021

StyleBook API を使用して、この StyleBook に基づいて構成を作成します。cURL コマンドラインツールや Postman Chrome ブラウザ拡張機能などの任意のツールを使用して、HTTP リクエストを Citrix ADM に送信できます。

SSL 証明書および証明書キーファイルを Citrix ADM にアップロードするスタイルブックを作成する方法で証明書とキーファイルをアップロードするために作成した StyleBook の例を考えてみましょう。REST API を使用して、この StyleBook から構成パックを次のように作成します。

POST

https://<MAS_IP_Address>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.stylebooks/1.0/lb-mon/configpacks?mode=async

```
Content-Type: application/jsonAccept: application/json {

   "configpack": {

       "parameters": {

           "lb-appname": "lbmon",
           "lb-virtual-ip": "13.1.11.10",
           "lb-virtual-port": "80",
           "lb-service-type": "HTTP",
           "svc-service-type": "HTTP",
           "svc-servers": [
               {

                   "ip": "14.1.1.15",
                   "port": "80" }

      ],
           "certificates": [
               {

                   "cert-name": "server_cert",
                   "cert-file": "server_cert.pem",
                   "ssl-inform": "PEM",
                   "key-name": "server_key",
                   "key-file": "server_key.pem",
                   "cert-password": "secret",
                   "cert-advanced": {
```

```
29
30                          "is-ca-cert": false,
31                          "skip-ca-name": false
32              }
33
34            }
35
36         ],
37              "lb-advanced": {
38
39                  "flush-on-state-down": "ENABLED",
40                  "auth-params": {
41
42                      "authentication": "OFF",
43                      "authentication-http-401": "OFF"
44            }
45  ,
46                  "appflow-log": "ENABLED",
47                  "algorithm": "LEASTCONNECTION"
48          }
49  ,
50              "svcg-advanced": {
51
52                  "svc-client-ip": "DISABLED",
53                  "svc-use-source-ip": "NO",
54                  "svc-use-proxy-port": "NO",
55                  "svc-surge-protection": "OFF",
56                  "svc-client-keepalive": "NO",
57                  "svc-tcp-buffering": "NO",
58                  "svc-compression": "NO",
59                  "svc-state": "ENABLED",
60                  "svc-downstate-flush": "DISABLED",
61                  "svc-enable-health-monitor": "NO"
62          }
63
64       }
65  ,
66          "targets": [
67              {
68
69                  "id": "8c158e7a-0087-423f-91b0-0ccf16de552a"
70          }
71
72       ]
73     }
```



```
74
75   }
76
77  <!--NeedCopy-->
```

この設定パックは、ID 8c158e7a-0087-423F-91b0-0ccf16de552a を使用して一意に識別されます。この ID を使用して、構成のクエリ、更新、削除を行えます。構成パックが正常に更新されると、証明書とキーファイルが Citrix ADM ファイルシステムにアップロードされます。

API を使用して任意のファイルタイプをアップロードする設定を作成する

May 7, 2021

Citrix Application Delivery Management（ADM）API を使用して、選択した Citrix ADC インスタンスにファイルをアップロードする構成パックを作成することもできます。

で任意のタイプのファイルをアップロードするために作成した StyleBook の例を考えてみましょう。StyleBook を作成して Citrix ADM にファイルをアップロードする方法。この例では、構成パックを作成し、Citrix ADM 上の場所ファイルのファイルパスとしてパラメーターlocationfileの値を指定します。
REST API を使用して、この StyleBook から構成パックを次のように作成します。

POST
https://<mas_ip>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.stylebooks.samples/1.0/upload-geolocations/configpacks

```
1  Content-Type: application/json
2  Accept: application/json
3  {
4
5     "configpack":
6     {
7
8        "parameters": {
9
10          "locationfile": "/var/mps/tenants/root/files/ /
                custom_geolocations.csv"
11       }
12   ,
13        "targets": [
14           {
15
16              "id": "5e540839-cd6c-437e-ac53-7d49bc2602b5"
17         }
```



```
18
19      ]
20     }
21
22  }
23
24 <!--NeedCopy-->
```

API を使用してカスタムスタイルブックをインポートする

May 7, 2021

StyleBook API を使用して、カスタム StyleBook を Citrix Application Delivery Management（ADM）にインポートできるようになりました。この StyleBook から設定パックを作成するには、REST API を使用して、cURL コマンドラインツールや Postman Chrome ブラウザ拡張機能などのツールで、次のようにします。たとえば、example-lb という名前の StyleBook をインポートして、Citrix ADC インスタンスでロードバランサー構成を作成できます。

HTTP メソッド: ポスト

URL: `http://<mas-ip>/stylebook/nitro/v1/config/stylebooks`

ヘッダー:

```
1 Content-Type: application/json
2 Accept: application/json
3 <!--NeedCopy-->
```

RequestBody:

```
1  {
2
3          "stylebook":
4    {
5
6       "file_name": "example-lb.yaml",
7       "source": "<base64-contents>",
8       "encoding": "base64"
9     }
10
11  }
12
13 <!--NeedCopy-->
```


ここで、「source」属性の値は、StyleBook ファイルの内容の base64 エンコーディングです。StyleBook ファイルの YAML コンテンツをオンラインツール（https://www.browserling.com/tools/file-to-base64など）に貼り付けて、上記の「source」属性の値として使用できる base64 文字列を取得できます。

この API 呼び出しを使用すると、複数の StyleBook ファイルを含む圧縮された tarball ファイル（.tgz ファイル）を 1 つの API オペレーションでアップロードすることもできます。これを行うには、ファイル名属性を.tgz ファイル名に変更し、ソース属性の値を.tgz ファイルの内容の base64 エンコーディングに変更します。

ツールで API が正常に実行されると、StyleBook が Citrix ADM にインポートされたことを示す次の応答が表示されます。

```
200 OK
<!--NeedCopy-->
```

レスポンス本文**:**

```
{


  "stylebook":
{


    "name": "example-lb",

    "namespace": "com.example.stylebook",

    "version": "1.0"

   }


 }

<!--NeedCopy-->
```

API を使用してカスタムスタイルブックをダウンロードする

May 7, 2021

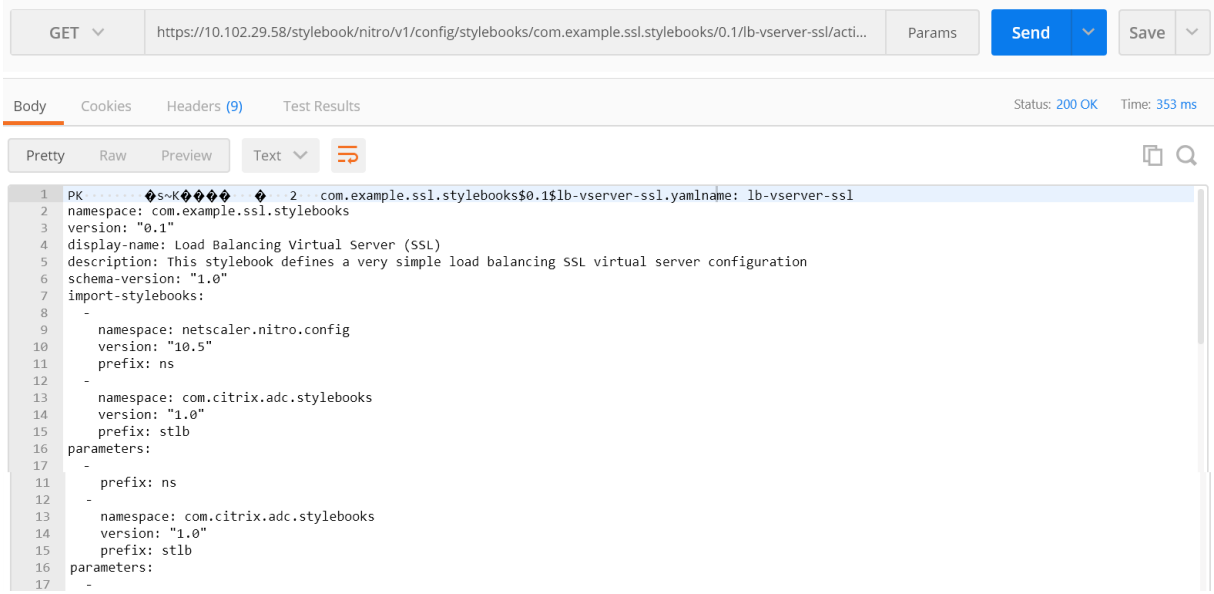
次の StyleBooks REST API を提供することで、カスタム StyleBook をダウンロードできます。

GET `https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<VERSION>/<NAME>/actions/download`

cURL コマンドラインツールなどの任意のツールで API を実行できます。または、IP アドレス、名前、バージョン、名前空間のフィールドを変更した後、Postman chrome ブラウザー拡張機能を使用できます。

GET https://10.102.29.58/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-vserver-ssl/actions/download

.yaml 形式のスタイルブックがダウンロードされます。



API を使用してカスタムスタイルブックを削除する

May 7, 2021

カスタムスタイルブックを削除するには、次の StyleBooks REST API を指定します。

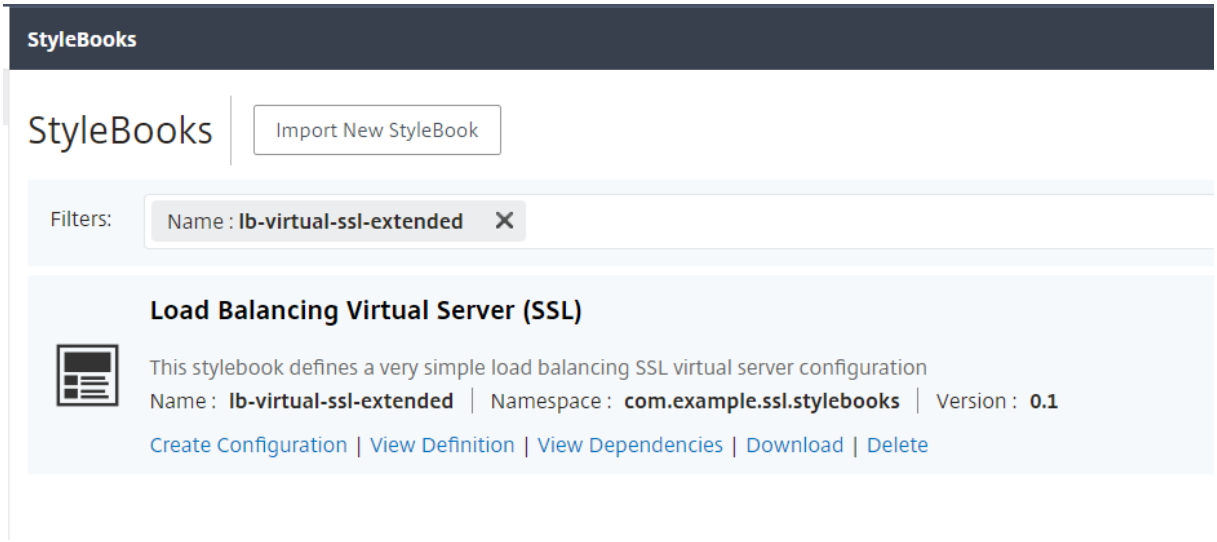
DELETE https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<VERSION>/<NAME>?dependencies=true

URL の依存関係クエリパラメータが指定されていない場合、またはその値が false に設定されている場合、StyleBook の依存関係は削除されません。そして、StyleBook だけが削除されます。

HTTP レスポンスステータスコード 200 を受け取ると、カスタム StyleBook とその依存関係が Citrix Application Delivery Management（ADM）から正常に削除されます。

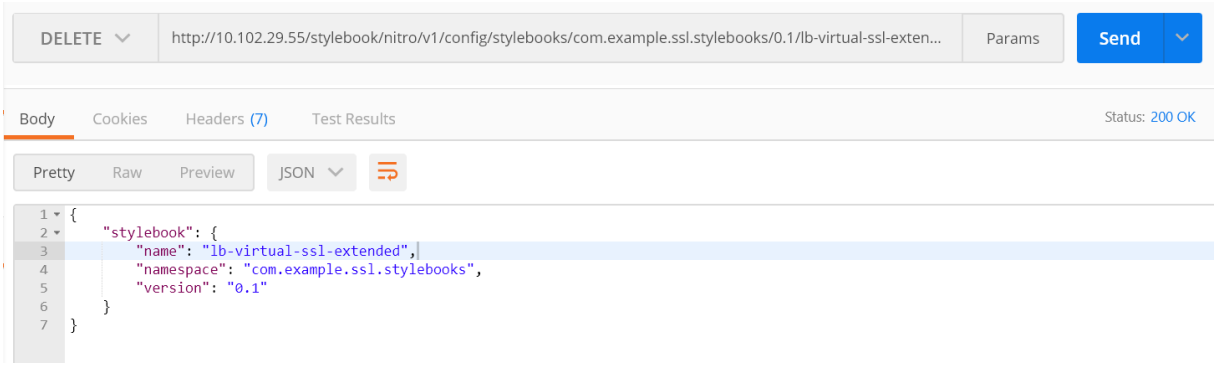
> 注:
>
> MA サービス内の他のスタイルブックが依存しているカスタムスタイルブックは削除できません。

たとえば、Citrix ADM で`lb-virtual-ssl-extended`という名前の StyleBook を作成したと仮定します。後でその StyleBook を削除することにしました。

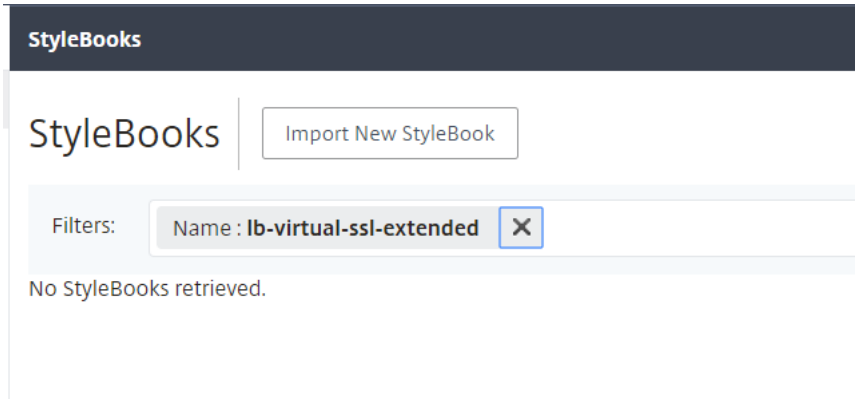


cURL コマンドラインツールなどの任意のツールで API を実行できます。また、IP アドレス、名前、バージョン、名前空間のフィールドを変更した後、Postman chrome ブラウザ拡張機能を使用することができます。

DELETE https://10.102.29.55/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-virtual-ssl-extended?dependencies=false



スタイルブックが Citrix ADM から削除されます。



スタイルブックの文法

May 7, 2021

独自の StyleBook を設計し、Citrix Application Delivery Management（ADM）にインポートし、Citrix ADM GUI または API を使用して構成を作成できます。独自の StyleBook を作成するには、まず、使用できるさまざまな構造および属性の文法と構文について理解しておく必要があります。

このドキュメントでは、StyleBook の作成時に使用できるさまざまな構造および参照について説明します。

次の表で断面名、構成、参照名をクリックして、詳細を表示します。

ヘッダー	StyleBook のインポート
パラメーター	パラメータ-デフォルトソース構成
自動置換	コンポーネント
オプションのプロパティ	ヘルパーコンポーネント
プロパティの既定のソース	ネストされたコンポーネント
条件構成	repeat 構造
繰り返し条件構成	結果
ネストされた繰り返し	親参照
パラメータ参照	置換参照
コンポーネントのリファレンス	操作
変数参照	alarms
Analytics	組み込み関数
式	依存関係の検出
インプレイス補間	

> 注
>
> `repeat-item`、`repeat-index`、または置換関数の引数を定義する際は、ユーザー定義変数`$<var-name>`の名前に次の予約語を使用しないでください。

- StyleBook、パラメータ、置換、コンポーネント、プロパティ、出力、親、自己、操作、分析、アラーム
- repeat-item, repeat-item-0, repeat-item-1, repeat-item-2
- repeat-index, repeat-index-0, repeat-index-1, repeat-index-2
- default
- roles, role, targets, target
- context, parent-context, parent_context

独自の StyleBook を設計する方法の詳細と例については、「独自の StyleBook の作成方法」を参照してください。

ヘッダー

May 7, 2021

StyleBook の先頭の 6 行は、Header セクションです。このセクションでは、StyleBook の ID を定義し、StyleBook の実行内容を記述できます。これは必須セクションです。

次の表は、Header セクションの属性について説明しています。

属性	説明
名前	StyleBook を識別する名前。この属性は必須です。
説明	StyleBook の実行内容を定義する説明。この説明は、Citrix Application Delivery Management（ADM）GUI に表示されます。これはオプションの属性です。
display-name	StyleBook を識別するための任意の名前。この名前は、Citrix ADM GUI に表示されます。これはオプションの属性です。
author	StyleBook を作成した作成者また組織。これはオプションの属性です。
namespace	名前空間は、StyleBook の一意の識別子の一部で、これにより名前の衝突を回避できます。namespace には任意の文字列を指定できますが、StyleBook のセットを作成したまたは所有している会社、部門または部署の名前を使用することをお勧めします。たとえば、次の形式を使用できます。`<company>.<department>.<unit>.stylebooks` これは必須属性です。
version	StyleBook のバージョン番号。バージョン番号は、StyleBook の更新時に変更できます。異なるバージョンの StyleBook を共存させることができます。これは必須属性です。
schema-version	StyleBook スキーマのバージョン。現在のリリースの Citrix ADM では、値「1.0」が使用されます。これは必須属性です。

属性	説明
private	この属性を true に設定すると、Citrix ADM GUI にスタイルブックは表示されません。これは、他の StyleBook の構築ブロックである StyleBook で有用な設定であり、ユーザーが直接使用するものではありません。これはオプションの属性です。デフォルト値は、false です。

例:

```
    name: lb

    description: "This stylebook defines a sample load balancing
       configuration."

    display-name: "Load Balancing StyleBook (HTTP)"

    author: Mike Smith (ACME Infra team)

    namespace: com.example.stylebooks

    schema-version: "1.0"

    version: "0.1"
<!--NeedCopy-->
```

name、namespace、および version の組み合わせにより、システム内で StyleBook が一意に識別されます。Citrix ADM では、名前、名前空間、およびバージョンの同じ組み合わせを持つ 2 つの StyleBook を使用することはできません。ただし、name と version が同じであっても namespace が異なる場合、または namespace と version が同じであっても name が異なる場合は、それらの 2 つの StyleBook を使用できます。

StyleBook のインポート

May 7, 2021

これは StyleBook の第 2 セクションで、現在の StyleBook から参照するほかの StyleBook を宣言できます。このセクションを記述すると、他の StyleBook をインポートして再利用できるため、StyleBook で同じ構成を再作成する必要がなくなります。これは必須セクションです。

現在の StyleBook で参照する StyleBook の名前空間とバージョン番号を宣言する必要があります。いずれかの NITRO 構成オブジェクトを直接使用する場合、StyleBook では、netscaler.nitro.config 名前空間を必ず参照する必要があります。この名前空間には、`lbvserver` サービスやモニターなど、すべての Citrix ADC NITRO タイプが含まれます。Citrix ADC バージョン 10.5 以降の StyleBook がサポートされています。つまり、StyleBook を使用して、リリース 10.5 以降を実行するすべての Citrix ADC インスタンス上で構成を作成および実行できます。

import-stylebooks セクションで使用される **prefix** 属性は、名前空間とバージョンの組み合わせを示すための略語です。たとえば、「ns」プレフィックスを使用して、バージョン 10.5 の名前空間 netscaler.nitro.config を参照できます。StyleBook の以降のセクションでは、StyleBook を名前空間とバージョンで示すたびにこの名前空間とバージョンを使用する代わりに、選択したプレフィックス文字列と、StyleBook を一意に識別する名前を使用できます。

例:

```
      import-stylebooks:
       -
         namespace: netscaler.nitro.config
         version: "10.5"
         prefix: ns
       -
         namespace: com.acme.stylebooks
         version: "0.1"
         prefix: stlb
<!--NeedCopy-->
```

この例では、最初に定義されたプレフィックスは ns と呼ばれ、名前空間 netscaler.nitro.config およびバージョン 10.5 を指します。定義される 2 番目のプレフィックスは`stlb`と呼ばれ、名前空間 com.acme.stylebooks とバージョン 0.1 を参照します。

プレフィックスを定義した後、特定の名前空間とバージョンに属する型または StyleBook を参照するたびに、**<namespace-shorthand>** という表記を使用できます <type-name>。たとえば、**ns lbvserver** は、名前空間 netscaler.nitro.config、バージョン 10.5 で定義されているタイプ`lbvserver`を参照します。

同様に、com.acme.stylebooks 名前空間にあるバージョン「0.1」の StyleBook を示す場合は、**stlb::** という表記を使用できます。

> 注
>
> 慣例により、プレフィックス「ns」は、Citrix ADC NITRO 名前空間を参照するために使用されます。

パラメーター

May 7, 2021

このセクションでは、構成を作成するために必要な StyleBook のすべてのパラメーターを定義します。StyleBook では、このセクションに記述された入力が使用されます。このセクションはオプションですが、ほとんどの StyleBook には必要な場合があります。パラメータセクションを考慮して、StyleBook を使用して Citrix ADC インスタンスで構成を作成するユーザーのフィールドを定義できます。

StyleBook を Citrix ADM にインポートし、それを使用して構成を作成すると、GUI は StyleBook のこのセクションを使用してフォームを表示します。このフォームは、定義されたパラメータ値の入力を受け取ります。

次のセクションでは、このセクションの各パラメータに指定する必要がある属性について説明します。

‘名前’

定義するパラメーターの名前。英数字名を指定できます。

名前はアルファベットで始まる必要があり、さらに多くのアルファベット、数字、ハイフン (-)、またはアンダースコア (_) を含めることができます。

StyleBook を記述するときは、$parameters.<name> という表記を使用して、この「名前」属性を使用して他のセクションのパラメータを参照できます。

必須? はい

‘ラベル’

ADM GUI でこのパラメータの名前として表示される文字列。

必須? いいえ

‘説明’

パラメーターの使用目的について説明するヘルプ文字列。ADM GUI では、このパラメータのヘルプアイコンをクリックすると、このテキストが表示されます。

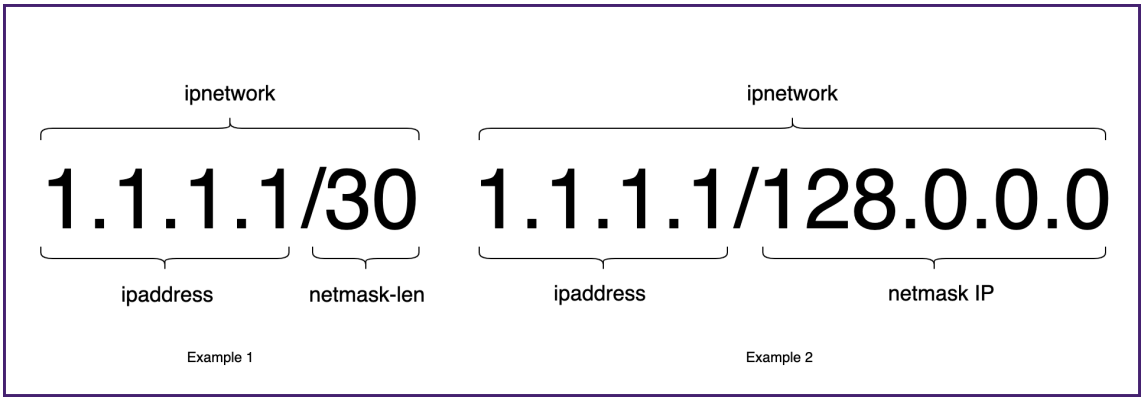
必須? いいえ

‘タイプ’

そのパラメーターで使用できる値のタイプ。パラメータには、
次の組み込み型のいずれかを使用できます。

- `string`: 文字の配列。長さが指定されていない場合、文字列値には、任意の数の文字を使用できます。ただし、min-length 属性と max-length 属性を使用すれば、文字列タイプの長さを制限できます。
- `number`: 整数。min-value 属性と max-value 属性により、このタイプで使用できる最小数と最大数を指定できます。

- **boolean**: 真または偽のどちらでもかまいません。YAML では、すべてのリテラルがブール値と見なされます (たとえば、[はい] または [いいえ])。
- ipaddress: 有効な IPv4 または IPv6 アドレスを表す文字列。
- ipnetwork: それは 2 つの部分を持っています。最初の部分は IP アドレスで、2 番目の部分はネットマスクです。



ネットマスクは、ネットマスク長 (netmask-len) またはネットマスクの IP アドレス (netmask_ip) で表されます。IPv6 アドレスのネットマスク長は、0 ～32 ～128 の整数です。これは、ネットワーク内の IP アドレスのカウントを決定するために使用されます。

- tcp-port: TCP または UDP ポートを表す 0 ～65535 の数値。
- password: 不透明/秘密の文字列値を表します。ADM GUI でこのパラメーターの値を表示すると、アスタリスク (*****) として表示されます。
- certfile: 証明書ファイルを表します。この値を使用すると、ADM GUI を使用して StyleBook 設定を作成するときに、ローカルシステムからファイルを直接アップロードできます。アップロードされた証明書ファイルは、ADM のディレクトリ/var/mps/tenants/\<tenant_path>/ns_ssl_certsに保存されます。

  証明書ファイルは、ADM によって管理される証明書の一覧に追加されます。

- keyfile: 証明書キーファイルを表します。この値を使用すると、ADM GUI を使用して StyleBook 設定を作成するときに、ローカルシステムからファイルを直接アップロードできます。アップロードされた証明書ファイルは、ADM のディレクトリ/var/mps/tenants/\<tenant_path>/ns_ssl_keysに保存されます。

  証明書キーファイルは、ADM によって管理される証明書キーの一覧に追加されます。

- file: ファイルを表します。
- object: この型は、親要素の下にいくつかの関連パラメータをグループ化する場合に使用されます。親パラメータのタイプを「object」として指定します。タイプが「object」のパラメーターにはネストされた「Parameters」セクションを含めることができ、そのセクションに含まれるパラメーターを記述できます。

- another StyleBook: このタイプのパラメータを使用する場合、このパラメータの値は、StyleBook で定義されたパラメータの形式で、その型を示します。

パラメータには、type 型のリストであるを持つこともできます。これを行うには、[] 型の末尾にを追加します。たとえば、type 属性がstring[]の場合、このパラメータは文字列のリストを入力として受け取ります。この StyleBook から構成を作成するときは、このパラメーターに対して 1 つまたは複数の文字列を指定できます。

必須? はい

‘network’

type: ipaddressでは、ADM IPAM ネットワークから IP アドレスを自動割り当てるnetwork属性を指定できます。

ADM は、StyleBook 設定を作成するときに、network 属性から IP アドレスを自動的に割り当てます。

例:

```
      name: virtual-ip
      label: "Load Balancer IP Address"
      type: ipaddress
      network: "network-1"
      required: true
<!--NeedCopy-->
```

この例では、virtual-ipフィールドはnetwork-1から IP アドレスを自動割り当てます。設定が削除されると、IP アドレスはネットワークに解放されます。

‘dynamic-allocation’

dynamic-allocation 属性は、type:ipaddressのパラメータ定義に追加されます。ADM IPAM ネットワークを動的にリストするには、この属性を使用します。この属性は、**true**または**false**を入力として取ることができます。type: ipaddressでは、ADM 内の ADM IPAM dynamic-allocation: **true** ネットワークを動的に一覧表示する属性を指定します。構成パック作成フォームでは、次の操作を実行できます。

1. リストから必要な IPAM ネットワークを選択します。
2. 選択した IPAM ネットワークから割り当てる IP アドレスを指定します。

   IP アドレスが指定されていない場合、ADM は選択した IPAM ネットワークから IP アドレスを自動的に割り当てます。

例:

```
  -
    name: virtual-ip
    label: "Load Balancer IP Address"
```



```
    type: ipaddress
    dynamic-allocation: true
    required: true
<!--NeedCopy-->
```

この例では、virtual-ip フィールドには、ADM 内の ADM IPAM ネットワークが一覧表示されます。リストからネットワークを選択して、ネットワークから IP アドレスを自動割り当てます。設定が削除されると、IP アドレスはネットワークに解放されます。

‘key’

true または false を指定して、このパラメーターが StyleBook のキーパラメーターかどうかを示します。

StyleBook で「キー」パラメーターとして定義できるパラメーターは 1 つだけです。

同じ StyleBook から（
同じまたは異なる ADC インスタンスで）異なる構成を作成する場合、
各構成はこのパラメータに対して異なる/一意の値を持ちます。

デフォルト値は false です。

必須? いいえ

‘required’

true または false を指定して、パラメーターが必須か、任意かを示します。true
に設定した場合、パラメータは必須であり、ユーザーは構成の作成時にこの
パラメータの値を指定する必要があります。

ADM GUI は、このパラメーターに有効な値を指定するようにユーザーを強制します。

デフォルト値は false です。

必須? いいえ

‘allowed-values’

型が「string」に設定されている場合、この属性を使用して、パラメータの有効な値のリストを定義します。

ADM GUI から構成を作成する場合、このリストからパラメータ値を選択するように求められます。このリストは静的であり、ユーザーはリストから値を選択することしかできません。ユーザーがリストに値を追加できるようにするには、[allow-new-values] (#allow-new-values) 属性を使用します。

> 注:
>
> ラジオオプションとしてリスト値を表示する場合は、[layout] (#layout) 属性を設定します。

例 **1**:

```
-
      name: ipaddress
      type: string
      allowed-values:
            -  SOURCEIP
            -  DEST IP
            -  NONE
<!--NeedCopy-->
```

例 **2**:

```
-
      name: TCP Port
      type: tcp-port
      allowed-values:
            -  80
            -  81
            -  8080
<!--NeedCopy-->
```

例 **3**:

tcp-portsのリスト。リストの各要素は、で指定された値のみを持つことができます allowed-values。

```
-
      name: tcpports
      type: tcp-port[]
      allowed-values:
            -  80
            -  81
            -  8080
            -  8081
<!--NeedCopy-->
```

必須? いいえ

‘許可-新しい値’

この属性を使用して、パラメータの動的リストを追加します。ADM GUI から設定を作成または更新する場合、ユーザーはリストに値を追加できます。

ユーザーがパラメータリストに値を追加する場合は、true を指定します。allow-**new**-values属性とallowed-values属性を組み合わせて使用できます。この組み合わせにより、パラメータの推奨値のリストを定義し、新しい値を受け入れることができます。


```
-
      name: port
      type: tcp-port
      allowed-values:
            -  80
            -  81
            -  8080
      allow-new-values: true
<!--NeedCopy-->
```

この例では、構成パックを作成または更新するときに、ユーザーは 80、81、8080 から選択するか、パラメーターportの新しい値を入力できます。

‘default’

任意のパラメーターにデフォルト値を割り当てるには、この属性を使用します。ユーザーが値を指定せずに構成を作成すると、デフォルト値が使用されます。

次の条件が満たされた場合、パラメータは値を取れません。

- パラメータにはデフォルト値はありません。
- ユーザーは、パラメータの値を指定しません。

例 **1**:

```
-
      name: timeout
      type: number
      default: 20
<!--NeedCopy-->
```

例 **2**:

パラメータのデフォルト値をリストするには、次の手順に従います。

```
-
      name: protocols
      type: string[]
      default:
            -  TCP
            -  UDP
            -  IP
<!--NeedCopy-->
```

例 **3**:


```
-
       name: timeout
       type: number
       default: 20
<!--NeedCopy-->
```

例 **4**:

```
-
       name: tcpport
       type: tcp-port
       default: 20
<!--NeedCopy-->
```

必須? いいえ

‘pattern’

この属性を使用して、パラメータの型が「string」の場合に、この
パラメータの有効な値のパターン（正規表現）を定義します。

例:

```
-
       name: appname
       type: string
       pattern: "[a-z]+"
<!--NeedCopy-->
```

必須? いいえ

‘min-value’

この属性を使用して、number またはtcp-portタイプのパラメータの最小値を定義します。

例:

```
-
       name: audio-port
       type: tcp-port
       min-value: 5000
<!--NeedCopy-->
```

数字のmin-valueには負の値を指定できます。ただし、tcp-portのmin-valueは正でなければなりません。

必須? いいえ

‘max-value’

この属性を使用して、number 型または
tcp-portのパラメータの最大値を定義します。

最大値が最小値より大きいことを確認します (定義されている場合)。

例:

```
-
      name: audio-port
      type: tcp-port
      min-value: 5000
      max-value: 15000
<!--NeedCopy-->
```

必須? いいえ

‘min-length’

この属性を使用して、「string」
タイプのパラメータに受け入れられる値の最小長を定義します。

値として定義された文字の最小長は、ゼロ以上であることを確認します。

例:

```
-
      name: appname
      type: string
      min-length: 3
<!--NeedCopy-->
```

必須? いいえ

‘max-length’

種類が「string」のパラメーターに入力できる値の最大文字数を定義するには、
この属性を使用します。

値の最大長が、min-lengthで定義されている文字の長さ以上であることを確認します。

例:


```
-
       name: appname
       type: string
       max-length: 64
<!--NeedCopy-->
```

必須? いいえ

‘min-items’

一覧となっているパラメーターの項目の最小数を定義するには、この属性を使用します。

アイテムの最小数がゼロ以上であることを確認します。

例:

```
-
       name: server-ips
       type: ipaddress[]
       min-items: 2
<!--NeedCopy-->
```

必須? いいえ

‘max-items

リストであるパラメータ内の項目の最大数を定義するには、
この属性を使用します。

アイテムの最大数が、定義されている場合は、アイテムの最小数よりも大きいことを確認してください。

例:

```
-
       name: server-ips
       type: ipaddress[]
       min-items: 2
       max-items: 250
<!--NeedCopy-->
```

必須? いいえ

‘gui’

この属性を使用して、ADM GUI でのパラメータのレイアウトをカスタマイズします。

必須? いいえ

‘columns’

この属性は、gui 属性のサブ属性です。この属性を使用して、ADM GUI でtype: object[]パラメータを表示する列数を定義します。

必須? いいえ

‘updable’

この属性は、gui 属性のサブ属性です。この属性を使用して、構成の作成後にパラメータを更新できるかどうかを指定します。この属性は、文字列、ブール、数値などの単純なパラメータタイプにのみ設定します。

値が**false**に設定されている場合、設定を更新すると、パラメータフィールドはグレー表示されます。

必須? いいえ

‘collapse_pane’

この属性は、gui 属性のサブ属性です。この属性を使用して、このオブジェクトパラメータのレイアウトを定義するペインが折りたたみ可能かどうかを指定します。

値を true に設定すると、ユーザーはこの親パラメーターの下にある子パラメーターを展開したり折りたたんだりできるようになります。

例:

```
gui:

 collapse_pane: true

 columns: 2
<!--NeedCopy-->
```

Parameters セクション全体の例:

```
parameters:

   -

      name: name

      label: Name

      description: Name of the application
```



```
10
11        type: string
12
13        required: true
14
15    -
16
17        name: ip
18
19        label: IP Address
20
21        description: The virtual IP address used for this application
22
23        type: ipaddress
24
25        required: true
26
27    -
28
29        name: svc-servers
30
31        label: Servers
32
33        type: object[]
34
35        required: true
36
37        parameters:
38
39          -
40
41                name: svc-ip
42
43                label: Server IP
44
45                description: The IP address of the server
46
47                type: ipaddress
48
49                required: true
50
51          -
52
53                name: svc-port
54
```



```
                label: Server Port

                description: The TCP port of the server

                type: tcp-port

                default: 80

        -

                name: lb-alg

                label: LoadBalancing Algorithm

                type: string

                allowed-values:

                   - ROUNDROBIN

                   - LEASTCONNECTION

                default: ROUNDROBIN

        -

                name: enable-healthcheck

                label: Enable HealthCheck?

                type: boolean

                default: true
<!--NeedCopy-->
```

次の例では、一覧のすべての属性と、前のセクションで説明した値を定義しています。

```
        -
                name: features-list

                type: string[]

                min-length: 1

                max-length: 3
```



```
9
10                min-items: 1
11
12                max-items: 3
13
14                pattern: "[A-Z]+"
15
16                allowed-values:
17
18                  - SP
19
20                  - LB
21
22                  - CS
23
24                default:
25
26                  - LB
27  <!--NeedCopy-->
```

‘layout’

この属性は、gui 属性のサブ属性です。この属性を使用して、リスト値をラジオボタンとして表示します。StyleBook 定義のパラメータセクションで、layout属性をradioに設定します。これは、[allowed-values](#allowed-values) 属性を持つパラメータに適用されます。構成パックを作成すると、ADM GUI にラジオボタンとしてallowed-valuesリストの値が表示されます。

例:

```
1  -
2      gui:
3          layout: radio
4      allowed-values:
5          - One
6          - Two
7          - Three
8  <!--NeedCopy-->
```

ADM GUI では、1、2、および 3 の値がラジオボタンとして表示されます。

‘dependent-parameters’

この属性は、gui 属性のサブ属性です。別のパラメータで指定された値に基づいて、StyleBook 設定フォームでのパラメータの外観または初期値を動的に制御します。

フォーム上でのパラメーターの動作を制御するソースパラメーターにこの属性を指定します。他のパラメータを制御する複数の条件を含めることができます。たとえば、protocol ソースパラメータには依存パラメータcertificateを指定できます。これは、protocol パラメータ値がSSLである場合にのみ表示されます。

各条件は、次の属性を持つことができます。

- **target-parameter**: この条件が適用されるターゲットパラメータを指定します。
- **matching-values**: アクションをトリガーするソースパラメータの値のリストを指定します。
- **action**: ターゲットパラメータで次のいずれかのアクションを指定します。
  - read-only: パラメーターは読み取り専用になります。
  - show: パラメーターが非表示の場合、フォームに表示されます。
  - hide: パラメーターがフォームから削除されます。
  - set-value: パラメーター値は、value 属性で指定された値に設定されます。
- **value**: アクションがset-valueの場合、ターゲットパラメーターの値。

ユーザー入力がソースパラメーターの指定された値と一致する場合、ターゲットパラメーターの外観または値は、指定されたアクションに従って変化します。

例:

```
-
   name: lb-virtual-port
   label: "Load Balanced App Virtual Port"
   description: "TCP port representing the Load Balanced application"
   type: tcp-port
   gui:
     updatable: false
     dependent-parameters:
           -
             matching-values:
               - 80
             target-parameter: $parameters.lb-service-type
             action: set-value
             allowed-values:
             - HTTP
             - TCP
             - UDP

   default: 80

<!--NeedCopy-->
```

この例では、依存パラメータはパラメータ (lb-virtual-port ソースパラメータ) の下に指定されています。

ソースパラメーターの値がに設定されている場合 80、`lb-service-typeset-value` パラメーターはアクションをトリガーします。その結果、ユーザーは次のいずれかのオプションを選択できます。

- HTTP
- TCP
- UDP

パラメータ-デフォルトソース構成

May 7, 2021

この構造を使用すると、ほかの StyleBook のパラメーター定義を再利用できます。

パラメーターまたはパラメーターグループを複数の StyleBook で繰り返し使用するシナリオについて考えてみます。新しい StyleBook を作成するたびにこれらのパラメーターを再定義することを避けるために、パラメーターを一度定義してから、**parameters-default-sources** 構造を使用して、これらのパラメーターを必要とする StyleBook にその定義をインポートできます。

たとえば、StyleBook の多くで仮想 IP を構成する必要がある場合は、新しく作成する各 StyleBook で仮想 IP に関連する同じパラメーターの定義が必要になることがあります。代わりに、という別の StyleBook を作成できます。たとえば、次の例（`vip-params`）に示すように、関連するすべてのパラメータを定義します。

```
1       -
2
3       name: vip-params
4
5       namespace: com.acme.commontypes
6
7       version: "1.0"
8
9       description: This StyleBook defines a typical virtual IP config.
10
11      private: true
12
13      schema-version: "1.0"
14
15      parameters:
16
17        -
18
19            name: lb-appname
20
21            label: Load Balanced Application Name
22
```



```
23            description: Name of the Load Balanced application
24
25             type: string
26
27             required: true
28
29         -
30
31             name: lb-virtual-ip
32
33             label: Load Balanced App Virtual IP address
34
35             description: Virtual IP address representing the Load
                  Balanced application
36
37             type: ipaddress
38
39             required: true
40
41         -
42
43             name: lb-virtual-port
44
45             label: Load Balanced App Virtual Port
46
47             description: TCP port representing the Load Balanced
                  application
48
49             type: tcp-port
50
51             default: 80
52
53         -
54
55             name: lb-service-type
56
57             label: Load Balanced App Protocol
58
59             description: Protocol used for the Load Balanced application
                  .
60
61             type: string
62
63             default: HTTP
64
```



```
            required: true

            allowed-values:

                - HTTP

                - SSL

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

その後、これらのパラメータを使用する他の StyleBooks を作成できます。以下に、このような StyleBook の例を示します。

```
    -

    name: acme-biz-app

    namespace: com.acme.stylebooks

    version: "1.0"

    description: This stylebook defines the Citrix ADC configuration
       for Biz App

    schema-version: "1.0"

    import-stylebooks:

      -

        namespace: com.acme.commontypes

        prefix: cmtypes

        version: "1.0"

    \*\*parameters-default-sources:\*\*

**          - cmtypes::vip-params**

    parameters:

        -

```



```
31              name: monitorname
32
33              label: Monitor Name
34
35              description: Name of the monitor
36
37              type: string
38
39              required: true
40
41            -
42
43              name: type
44
45              label: Monitor Type
46
47              description: Type of the monitor
48
49              type: string
50
51              required: true
52
53              allowed-values:
54
55                - PING
56
57                - TCP
58
59                - HTTP
60
61                - HTTP-ECV
62
63                - TCP-ECV
64
65                - HTTP-INLINE
66  <!--NeedCopy-->
```

StyleBookacme-biz-appでは、まず、vip-paramsStyleBook の名前空間とバージョンは、「import-stylebooks」セクションを使用してインポートされます。次に、パラメーター **default-sources** 構造が追加され、StyleBook 名 (つまりvip-params) が指定されます。このパラメータは、この StyleBook でvip-params StyleBook のパラメータを直接定義するのと同じ効果があります。

parameters-default-sources は一覧であり、一覧の各項目が StyleBook であると想定されるので、複数の StyleBook のパラメーターを含めることができます。

ほかの StyleBook のパラメーターを含めることができるだけでなく、Parameters セクションを使用して独自のパラメーターを定義することもできます。StyleBook のパラメーターの一覧全体は、ほかの StyleBook のパラメーターとこの StyleBook で定義したパラメーターの組み合わせになります。したがって、式 **$parameters** はこのパラメーターの組み合わせを参照します。

インポートされた StyleBook と現在の StyleBook の両方でパラメータが定義されている場合、現在の StyleBook の定義は、別の StyleBook からインポートされた定義を上書きします。このアプローチは、必要に応じてインポートされたパラメータの一部をカスタマイズし、残りのインポートされたパラメータをそのまま使用することで、効果的に使用できます。

parameters-default-sources 構造は、次に示すようにネストされたパラメーターでも使用できます。

```
parameters:

    -

      name: vip-details

      label: Virtual IP details

      description: Details of the Virtual IP

      type: object

      required: true

      parameters-default-sources:

              - cmtypes::vip-params
<!--NeedCopy-->
```

この方法は、StyleBook`vip-params`のパラメータを、この StyleBook の`vip-details`パラメータの子パラメータとして直接追加することに似ています。

自動置換

May 7, 2021

Substitutions セクションは、StyleBook のほかの部分で StyleBook を読み取りやすくするために使用できる、複雑な式の省略名を定義するために使用されます。また、このセクションは、StyleBook で同じ式または値を複数回使用する場合にも役立ちます（定数値など）。この値に代替名を使用すると、StyleBook に表示されるすべての場所で置換値を更新するのではなく、この値を変更する必要があるときにのみ置換値を更新できます。これはエラーが発生しやすくなります。

置換は、このドキュメントの後の例で示すように、値のマッピングの定義にも使用できます。

一覧の各置換はキーと値で構成されます。値には、単純な値、式、関数、またはマップを指定できます。

次の例では、2 つの置換が定義されています。最初のhttp-portは 8181 の短縮形として使用できます。置換を使用することで、この値を StyleBook のほかの部分で、8181 ではなく **$substitutions.http-port** として参照できるようになります。

置換:

```
http-port: 8181
```

これにより、ポート番号にニーモニック名を指定し、使用回数に関係なく、StyleBook 内の 1 箇所でこのポート番号を定義できます。ポート番号を 8080 に変更する場合は、置換セクションで変更できます。変更内容はニーモニック名http-portが使用されている場所であればどこでも有効になります。次の例は、コンポーネントで置換を使用する方法を示しています。

```
components:

 -

     name: my-lbvserver-comp

     type: ns::lbvserver

     properties:

          name: $parameters.name + "-lb"

          servicetype: HTTP

          ipv46: $parameters.ip

          port: $substitutions.http-port

          lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

置換は複雑な式にすることもできます。次の例は、2 つの置換で式を使用する方法を示しています。

```
substitutions:

  app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS

  app-name: str("acme-") + $parameters.name + str("-app")
<!--NeedCopy-->
```


また、置換式では、次の例に示すように既存の置換式を使用することもできます。

```
substitutions:

  http-port: 8181

  app-name: str("acme-") + $parameters.name + str($substitutions.http-
     port) + str("-app")
<!--NeedCopy-->
```

置換のもう 1 つの便利な機能がマップで、キーを値にマップできます。以下は、マップ置換の例です。

```
substitutions:

    secure-port:

        true: int("443")

        false: int("80")

    secure-protocol:

        true: SSL

        false: HTTP
<!--NeedCopy-->
```

次の例は、マップ secure-port および secure-protocol を使用する方法を示しています。

```
components:

 -

     name: my-lbvserver-comp

     type: ns::lbvserver

     properties:

          name: $parameters.name + "-lb"

          servicetype: $substitutions.secure-protocol[$parameters.is-
             secure]

          ipv46: $parameters.ip
```



```
16
17            port: $substitutions.secure-port[$parameters.is-secure]
18
19            lbmethod: $parameters.lb-alg
20  <!--NeedCopy-->
```

これは、StyleBook のユーザーがパラメータ is-secure にブール値「true」を指定した場合、または Citrix ADM GUI でこのパラメーターに対応するチェックボックスをオンにした場合、このコンポーネントのservicetypeプロパティには値 **SSL** が割り当てられ、ポートプロパティが の値 **443** が割り当てられました。ただし、ユーザーがこのパラメータに「false」を指定するか、Citrix ADM GUI で対応するチェックボックスをオフにすると、servicetypeプロパティには値 **HTTP** が割り当てられ、ポートには値 **80** が割り当てられます。

次の例は、置換を関数として使用する方法を示しています。置換関数は 1 つまたは複数の引数を取ることができます。引数には、文字列、数値、ipaddress、ブール型、その他の型などの単純な型を使用できます。

置換:

form-lb-name(name): $name + “-lb”

この例では、置換関数「form-lb-name」を定義しています。この関数は「name」という名前の string 型の引数を取り、それを使用して name 引数の文字列の末尾に「-lb」を追加した新しい文字列を作成します。この置換関数を使用する式は、次のように記述することができます。

```
$substitutions.form-lb-name("my")
```

my-lbを返します

別の例を考えてみましょう。

置換:

```
cspol-priority(priority): 10100 - 100 * $priority
```

cspol-priority置換は、優先順位と呼ばれる引数を受け取り、それを使用して値を計算する関数です。StyleBook のほかの部分で、この置換を次の例に示すように使用できます。

```
1  components:
2
3    -
4
5      name: cspolicy-binding-comp
6
7      type: ns::csvserver_cspolicy_binding
8
9      condition: not $parameters.is-default
10
11     properties:
12
```



```
13          name: $parameters.csvserver-name
14
15          policyname: $components.cspolicy-comp.properties.policyname
16
17          priority: $substitutions.cspol-priority($parameters.pool.
               priority)
18  <!--NeedCopy-->
```

置換は、キーと値で構成することもできます。値には、単純な値、式、関数、マップ、一覧、またはディクショナリを指定できます。

次に、値がリストであるというslist置換の例を示します。

```
1  substitutions:
2
3    slist:
4
5      - a
6
7      - b
8
9      - c
10 <!--NeedCopy-->
```

置換の値は、以下sdictと呼ばれる置換の例に示すように、キーと値のペアのディクショナリにすることができます。

```
1  substitutions:
2
3    sdict:
4
5      a: 1
6
7      b: 2
8
9      c: 3
10 <!--NeedCopy-->
```

一覧とディクショナリを組み合わせると、もっと複雑な属性を作成できます。たとえば、slistofdictという置換は、キーと値のペアのリストを返します。

```
1    slistofdict:
2
3      -
4
5        a: $parameters.cs1.lb1.port
```



```
6
7       b: $parameters.cs1.lb2.port
8
9     -
10
11      a: $parameters.cs2.lb1.port
12
13      b: $parameters.cs2.lb2.port
14 <!--NeedCopy-->
```

しかし、次の例では、sdictoflist置換はキーと値のペアを返します。ここで、値自体は別のリストです。

```
1   sdictoflist:
2
3     a:
4
5       - 1
6
7       - 2
8
9     b:
10
11      - 3
12
13      - 4
14 <!--NeedCopy-->
```

コンポーネントでは、これらの置換は condition、properties、repeat、repeat-condition 構造で使用できます。

次のコンポーネントの例は、置換を使用してプロパティを指定する方法を示しています。

```
1     properties:
2
3       a: $substitutions.slist
4
5       b: $substitutions.sdict
6
7       c: $substitutions.slistofdict
8
9       d: $substitutions.sdictoflist
10 <!--NeedCopy-->
```

値が一覧またはディクショナリの置換を定義するユースケースは、コンテンツスイッチ仮想サーバーや複数の負荷分散仮想サーバーを構成する場合です。同じ cs 仮想サーバーに関連付けられているすべての lb 仮想サーバーが同じ構成を持つ可能性があるため、置換リストとディクショナリを使用してこの構成を構築すると、各 lb 仮想サーバーに対

してその構成が繰り返されるのを防ぐことができます。

次の例は、cs-lb-monStyleBooks の置換とコンポーネントを示して、コンテンツスイッチング仮想サーバー構成を作成します。cs-lb-monStyleBooks のプロパティを構築している間、複合置換の「lb-properties」は、CS 仮想サーバーに関連付けられた lb 仮想サーバーのプロパティを指定します。「lb-properties」置換は、名前、サービスの種類、仮想 IP アドレス、ポート、サーバーをパラメーターとして取り、値としてキーと値のペアを生成する関数です。cs-poolsコンポーネントでは、この置換の値を各プールの lb-pool パラメータに割り当てます。

```
substitutions:

  cs-port[]:

    true: int("80")

    false: int("443")

  lb-properties(name, servicetype, vip, port, servers):

    lb-appname: $name

    lb-service-type: $servicetype

    lb-virtual-ip: $vip

    lb-virtual-port: $port

    svc-servers: $servers

    svc-service-type: $servicetype

    monitors:

      -

        monitorname: $name

        type: PING

        interval: $parameters.monitor-interval

        interval_units: SEC

        retries: 3

components:
```



```
38
39    -
40
41      name: cs-pools
42
43      type: stlb::cs-lb-mon
44
45      description: | Updates the cs-lb-mon configuration with the
           different pools provided. Each pool with rule result in a dummy
           LB vserver, cs action, cs policy, and csvserver_cspolicy_binding
            configuration.
46
47      condition: $parameters.server-pools
48
49      repeat: $parameters.server-pools
50
51      repeat-item: pool
52
53      repeat-condition: $pool.rule
54
55      repeat-index: ndx
56
57      properties:
58
59        appname: $parameters.appname + "-cs"
60
61        cs-virtual-ip: $parameters.vip
62
63        cs-virtual-port: $substitutions.cs-port($parameters.protocol == "
             HTTP")
64
65        cs-service-type: $parameters.protocol
66
67        pools:
68
69          -
70
71            lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP"
                 , "0.0.0.0", 0, $pool.servers)
72
73            rule: $pool.rule
74
75            priority: $ndx + 1
76  <!--NeedCopy-->
```


置換マップ:

キーを値にマップする置換を作成できます。たとえば、各プロトコル（キー）に使用するデフォルトポート（値）を定義するシナリオを考えてみましょう。このタスクでは、次のように置換マップを記述します。

```
substitutions:

     port:

          HTTP: 80

          DNS: 53

          SSL: 443
<!--NeedCopy-->
```

この例では、HTTP は 80 に、DNS は 53 に、SSL は 443 にマップされます。パラメーターとして与えられた特定のプロトコルのポートを取得するには、次の式を使用します。

$substitutions.port[$parameters.protocol]

この式は、ユーザーが指定したプロトコルに基づいて値を返します。

- キーが HTTP の場合、この式は 80 を返します。
- キーが DNS の場合、この式は 53 を返します。
- キーが SSL の場合、この式は 443 を返します。
- キーがマップ内に存在しない場合、この式はいずれの値も返しません。

コンポーネント

May 7, 2021

StyleBook の components 構造は、StyleBook で最も重要なセクションです。このセクションでは、作成する必要がある構成オブジェクトを定義します。この構造を使用すると、同じ種類の構成オブジェクトを 1 つまたは複数作成できます。

components 構造では、Parameters セクションの入力値を使用して、StyleBook で生成される構成に適応させることができます。このセクションはオプションですが、ほとんどの StyleBook で Components セクションが記述されています。

次の表は、コンポーネントの主要な属性を示しています。

属性	説明
名前	コンポーネントの名前。英数字名を指定できます。名前はアルファベットで始まる必要があり、追加でアルファベット、数字、ハイフン（-）、またはアンダースコア（_）を含めることができます。
説明	StyleBook におけるこのコンポーネントの役割の説明。
種類	このコンポーネントで指定するプロパティはタイプによって決まります。コンポーネントには 2 種類のタイプがあります。組み込み型: このタイプはシステムによって提供され、定義する必要はありません。たとえば、NITRO エンティティタイプ`lbvserver`や`servicegroup`などです。コンポーネントに組み込みの type 属性がある場合、Citrix ADC 上にそのタイプの構成オブジェクトが作成されます。たとえば、コンポーネントが組み込みの種類`lbvserver`を参照する場合、このコンポーネントは構成のターゲットである Citrix ADC インスタンス上に負荷分散仮想サーバーを作成します。複合タイプ: このタイプは、作成して Citrix Application Delivery Management（ADM）にインポートした既存の StyleBook を指します。コンポーネントにコンポジットタイプ属性がある場合、参照先の StyleBook で指定されているすべての構成オブジェクトが、構成のターゲットである Citrix ADC インスタンスに作成されます。これにより、それぞれが最終構成の一部を作成する複数の StyleBook を組み合わせて使用できるようになります。複合スタイルブックについて詳しくは、複合 StyleBook の作成を参照してください。
properties	コンポーネントの type 属性で使用できるサブ属性。コンポーネントに対して有効なプロパティは、そのタイプによって決まります。組み込み型の場合、これらは対応する NITRO オブジェクトのプロパティまたは属性です。コンポーネントのタイプが別の StyleBook である場合（つまり複合タイプの場合）、プロパティはその StyleBook で定義されているパラメーターに対応します。

例:

```
components:

   -

     name: my-lbvserver-comp

     type: ns::lbvserver

     properties:

        name: $parameters.name

        servicetype: HTTP

        ipv46: $parameters.ip

        port: 80

        lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

この例では、my-lbvserver-compというコンポーネントを定義しています。このコンポーネントの型は、nsᵡ lbvserver（組み込み型）です。ここで「ns」は、import-stylebooks セクションで指定した名前空間 netscaler.nitro.config およびバージョン 10.5 を参照する接頭辞であり、lbvserverはこの名前空間内の NITRO リソースです。

このセクションのプロパティには、lbvserverリソースの 4 つの必須属性と 1 つのオプション属性 (lbmethod) が含まれており、これらの属性の値を指定できます。この例では、servicetype およびポートに静的値を指定し、名前、ipv46、lbmethod およびプロパティは入力パラメータから値を取得します。Parameters セクションで定義されているパラメーター名を参照するには、$parameters. という表記を使用します。たとえば、$parameters.ip のように指定します。名前 >

利用可能なすべての Citrix ADC NITRO リソースとその属性/プロパティの詳細については、Citrix ADC NITRO REST API ドキュメントを参照してください。

> 注
>
> NITRO リソースの種類の属性名（コンポーネントのプロパティ）には、小文字を使用する必要があります。そうしないと、StyleBook のインポートに失敗します。

ヘルパーコンポーネント

May 7, 2021

StyleBook のコンポーネントセクションの主な用途は、NITRO 組み込み型または実際の構成オブジェクトを作成する別の StyleBook を使用して設定オブジェクトを生成することです。ヘルパーコンポーネントは、それ自身では構成オブジェクトを構築しません。ヘルパーコンポーネントは、パラメーターオブジェクト、他のコンポーネントのプロパティ、または他のコンポーネントの出力などを入力として、それらを他の形式に変換します。これが後に他のコンポーネントで使用されて、実際の構成オブジェクトが生成されます。ヘルパーコンポーネントには 2 種類あり、オブジェクトタイプとコンポーネントセクションを含まない他の StyleBook です。

次の例は、Citrix ADC インスタンス上で monitor（`lb-mon-comp`）を使用して負荷分散サーバーを作成するために使用される StyleBook のスニペットを示しています。

```
parameters:

  -

    name: appname

    type: string

  -

    name: ips

    type: ipaddress[]

  -

    name: vip

    type: ipaddress

components:

  -

    name: help-comp

    type: cmtypes::server-ip-port-params

    repeat:

```



```
31        repeat-list: $parameters.ips
32
33        repeat-item: server-ip
34
35      properties:
36
37        ip: $server-ip
38
39        port: 80
40
41    -
42
43      name: lb-mon-comp
44
45      type: stlb::lb-mon
46
47      properties:
48
49        lb-appname: $parameters.appname
50
51        lb-virtual-ip: $parameters.vip
52
53        lb-virtual-port: 80
54
55        lb-service-type: HTTP
56
57        svc-service-type: HTTP
58
59        svc-servers: $components.help-comp.properties
60
61  <!--NeedCopy-->
```

パラメーターセクションにはアプリケーションの名前と負荷分散サーバーの IP アドレスを入力することができます。`lb-mon-comp`コンポーネントセクションでは、`lb-mon`StyleBook の`svc-servers`パラメータには、各項目に 2 つのサブパラメータ`ip`とポートがあるオブジェクトのリストが必要です。

ただし、この StyleBook のパラメーターセクションは、$parameters.ips を使ってサーバー IP のみを受け取ります。この StyleBook では、すべてのサーバーがポート 80 で実行されると想定されています。`lb-mon`StyleBook を使用して負荷分散構成を作成するには、$parameters.ips をオブジェクトのリストに変換する必要があります。これは、上記の例では、ヘルパーコンポーネント、help-comp を使用して達成されます。ヘルプコンプコンポーネントの型は`server-ip-port-params`StyleBook です。この StyleBook はコンポーネントを持ちません。結果として、構成オブジェクトを作成しません。help-comp は $parameters.ips の上にリピートリストを作成し、$parameters.ips の各項目に対して、`ip`とポート (静的 80 に設定) で構成されるオブジェクトを構築します。したがって、help-comp は、IP アドレスのリストをオブジェクトのリストに変換し、後

でsvc-serversプロパティを割り当てるためにlb-mon-compで使用することができます。help-comp の結果は、lb-mon-compのsvc-serversプロパティに割り当てられます。

オプションのプロパティ

May 7, 2021

コンポーネントのプロパティは、パラメータ参照などの単純な式またはより複雑な式である式から値を取る場合があります。このプロパティ値の設定は、コンポーネントではオプションです。式から実際の値が返される場合にのみプロパティの値を設定し、値が返されない場合はこのプロパティを設定しなくてもかまいません。

たとえば、設定するプロパティの 1 つが ns lbvserver 型のコンポーネントの lbmethod (負荷分散アルゴリズム) であるとします。以下に示すように、lbmethod プロパティの値は、ユーザーが指定したパラメータ値から取得されます。

```
components

  -

      name: lbvserver_comp

      type: ns::lbvserver

      properties:

        name: $parameters.lb-appname + "-lb"

        servicetype: $parameters.lb-service-type

        ipv46: $parameters.lb-virtual-ip

        port: 80

        lbmethod: $parameters.lb-advanced.algorithm
<!--NeedCopy-->
```

ここで、パラメータ **lb-advanced.algorithm** がオプションのパラメータであることを考えてみましょう。また、オプションであるためにユーザーがこのパラメータの値を指定しない場合、式 **$parameters.lb-advanced.algorithm** は空白の値に評価されます。したがって、lbmethod プロパティに無効な値が渡されます。このような状況を回避するには、次のようにプロパティ名に「?」のサフィックスを付けて、プロパティにオプションであることを示す注釈を付けることができます。

```
components
```



```
2
3     -
4
5       name: lbvserver_comp
6
7       type: ns::lbvserver
8
9       properties:
10
11        name: $parameters.lb-appname + "-lb"
12
13        servicetype: $parameters.lb-service-type
14
15        ipv46: $parameters.lb-virtual-ip
16
17        port: 80
18
19        lbmethod?: $parameters.lb-advanced.algorithm
20  <!--NeedCopy-->
```

「?」を使用すると、右側の式がなしに評価された場合、このプロパティは省略されます。この例では、次のように定義されたコンポーネントと同等になります。

```
1  components
2
3    -
4
5      name: lbvserver_comp
6
7      type: ns::lbvserver
8
9      properties:
10
11       name: $parameters.lb-appname + "-lb"
12
13       servicetype: $parameters.lb-service-type
14
15       ipv46: $parameters.lb-virtual-ip
16
17       port: 80
18 <!--NeedCopy-->
```

lbmethod はオプションなので、省略しても有効なコンポーネントになります。タイプの「ns lbvserver」で定義されている場合、`lbmethod` はデフォルト値を使用する場合があります。

プロパティ-デフォルトソース構成

May 7, 2021

properties-default-sources 構造は parameters-default-sources 構造に似ています。parameters-default-sources 構造では StyleBook で（他の StyleBook から）既存のパラメーターを再利用できますが、properties-default-sources 構造ではユーザーが既存のソースに基づいてコンポーネントのプロパティを指定できます。

コンポーネントのプロパティは、StyleBook のさまざまなセクションに分散される可能性があります。たとえば、オブジェクトのパラメーター、オブジェクトを返す置換、ほかのコンポーネントのプロパティ、またはほかのコンポーネントの出力からプロパティが取得されることがあります。このような場合は、コンポーネントの定義で、StyleBook のほかのセクションで発生するプロパティを再定義する必要があります。明らかに、これは冗長でエラーにつながる可能性があります。この問題に対応するために、properties-default-sources 構造を使用できます。properties-default-sources 構造は、各項目がコンポーネントのプロパティのソースを識別する一覧です。

たとえば、`lbvserver` 構成を作成するコンポーネントについて考えてみましょう。このコンポーネントは、`lbvserver` のプロパティを次のように定義します。

```
parameters:

  -

    name: lb

    type: ns::lbvserver

components:

  -

    name: lb-comp

    type: ns::lbvserver

    properties:

      name: $parameters.lb.name

      ipv46: $parameters.lb.ipv46

      port: $parameters.lb.port

      servicetype: $parameters.lb.servicetype

```



```
27        lbmethod: $parameters.lb.lbmethod
28  <!--NeedCopy-->
```

上記の例では、components セクションで定義されているすべてのプロパティの値は $parameters.lb オブジェクトから取得されていることに注目してください。これらのプロパティは 1 つのソースから取得されますが、StyleBook で再定義されています。さらに、lbvserverの設定に関連する $parameters.lb オブジェクトの新しいサブパラメータが追加された場合、lb-comp コンポーネントを更新して、新しいサブパラメータに対応する新しいプロパティを追加する必要があります。

プロパティの再定義を避け、コンポーネントのすべての関連プロパティを properties セクションで明示的にリストすることなく取得するために、properties-default-sources 構造を使用できます。上の例は、次のように記述することもできます。

```
1  parameters:
2
3    -
4
5      name: lb
6
7      type: ns::lbvserver
8
9  components:
10
11   -
12
13     name: lb-comp
14
15     type: ns::lbvserver
16
17     properties-default-sources:
18
19       - $parameters.lb
20 <!--NeedCopy-->
```

上の例では、properties-default-sources 構造を使用することでコンポーネント定義のサイズが小さくなり、そのためにコンポーネントを簡潔に定義できています。さらに、コンポーネントのプロパティのソースが変更されるたびに、変更内容が自動的に反映されます。たとえば、$parameters.lb オブジェクトに新しいプロパティ、persistencetypeなどが追加されると、persistencetypeプロパティはlbvserverのプロパティであるため、デフォルトでは lb-comp の設定に追加されます。このように、properties-default-sources 構造は、コンポーネントのプロパティのソースに対して行われる変更を気にすることなくコンポーネントを定義できる動的なインターフェイスを提供します。

コンポーネントのプロパティの計算

このセクションでは、コンポーネントで properties-default-sources 構造を使用した場合にプロパティがどのように取得されるかについて説明します。まず、StyleBooks コンパイラーは、その型に基づいてコンポーネントのプロパティのリストを識別します (上記の例では `lbvserver`) 次に、コンパイラーは (コンポーネントの properties-default-sources セクションで) 定義された順序で複数のソースからこれらのプロパティを取得します。プロパティが複数のソースに存在する場合は、最後のソースに出現するプロパティがほかのプロパティより優先されます。最後に、properties-default-sources 構造を使用して取得されたプロパティは、コンポーネントの properties セクションで上書きすることができます。コンポーネントセクションの定義には、少なくともプロパティー default-sources セクションまたはプロパティセクションがあることに注意してください。両方のセクションを持つこともできます。

ネストされたコンポーネント

May 7, 2021

コンポーネントを別のコンポーネント内にネストした場合、ネストされたコンポーネントは、親コンポーネントによって作成される構成オブジェクトまたはコンテキストを参照してその構成オブジェクトを作成できます。ネストされたコンポーネントは、親コンポーネントでオブジェクトが作成されるたびに、1 つまたは複数のオブジェクトを作成できます。コンポーネントを別のコンポーネント内にネストしても、作成される構成オブジェクト間に関係は生じません。ネストを使用すると、親コンポーネントの既存のコンテキスト内で構成オブジェクトを作成するコンポーネントのタスクが容易になります。

例:

```
components:

 -

  name: my-lbvserver-comp

  type: ns::lbvserver

   properties:

      name: $parameters.name + "-lb"

      servicetype: HTTP

      ipv46: $parameters.ip

      port: 80
```



```
18
19        lbmethod: $parameters.lb-alg
20
21        components:
22
23          -
24
25           name: my-svcg-comp
26
27           type: ns::servicegroup
28
29           properties:
30
31              name: $parameters.name + "-svcgrp"
32
33              servicetype: HTTP
34
35           components:
36
37              -
38
39                name: lbvserver-svg-binding-comp
40
41                type: ns::lbvserver_servicegroup_binding
42
43                properties:
44
45                  name: $parent.parent.properties.name
46
47                  servicegroupname: $parent.properties.name
48
49                    -
50
51                      name: members-svcg-comp
52
53                      type: ns::servicegroup_servicegroupmember_binding
54
55                      repeat:
56
57                        repeat-list: $parameters.svc-servers
58
59                        repeat-item: srv
60
61                      properties:
62
```



```
63                          ip: $srv
64
65                          port: str($parameters.svc-port)
66
67                          servicegroupname: $parent.properties.name
68  <!--NeedCopy-->
```

この例では、複数レベルのネストが使用されています。my-lbvserver-compコンポーネントには、my-svcg-compという子コンポーネントがあります。また、my-svcg-compコンポーネントには 2 つの子コンポーネントがあります。my-svcg-compコンポーネントは、組み込みの NITRO リソースタイプ”servicegroup“の属性に値を指定することにより、Citrix ADC インスタンス上にサービスグループ構成オブジェクトを作成するために使用されます。my-svcgコンポーネントの最初の子コンポーネントであるlbvserver-svg-binding-compは、親コンポーネントによって作成されたサービスグループを、親の親コンポーネントによって作成された負荷分散仮想サーバー (lbvserver) にバインドするために使用されます。$parent 表記（親参照とも呼ばれる）は、親コンポーネントのエンティティを参照するために使用されます。2 番目の子コンポーネントmembers-svcg-compは、親コンポーネントによって作成されたサービスグループにサービスのリストをバインドするために使用されます。バインドは、StyleBook の repeat 構造を使用して、パラメータsvc-serversに指定されたサービスのリストを反復処理することで実現されます。repeat 構造については、repeat 構造を参照してください。

同じ構成オブジェクトを、コンポーネントのネストを使用せずに作成することもできます。詳細と例については、「基本的な負荷分散の構成を作成するための StyleBook」を参照してください。

条件構成

May 7, 2021

condition 構造を使用すると、コンポーネントを条件付きにすることができます。condition 構造の値は、true または false に評価されるブール式です。条件が true になる場合、このコンポーネントを使用して構成オブジェクトが作成されます。条件が false になる場合、このコンポーネントはスキップされ、構成オブジェクトの作成には使用されません。多くの場合、ブール式はパラメーター値に基づきます。

例:

```
1  components:
2
3        -
4
5          name: servicegroup-comp
6
7          type: ns::servicegroup
8
9          condition: $parameters.svc-server-ips
```



```
10
11          properties:
12
13                name: $parameters.name + "-svcgrp"
14
15                servicetype: HTTP
16  <!--NeedCopy-->
```

この例では、ユーザーがオプションのパラメータsvc-server-ipsに値を指定した場合、コンポーネントservicegroup-compは StyleBook エンジンによって処理されます。条件が false の場合、つまり、ユーザーがこのパラメータに値を指定しない場合、このパラメータに NULL 値が割り当てられ、false と評価された場合、StyleBook エンジンはこのコンポーネントの存在を無視し、servicegroupは作成されません。

ブール式は、StyleBook でサポートされる任意の有効な式に基づいて設定できます（たとえば、別のコンポーネントが存在するかどうかや、パラメーターに特定の値が指定されているかどうかなど）。

次の例では、条件が true に評価された場合に、NITRO タイプ ns::systemfile の構成オブジェクトを作成します。

例:

```
1       components
2
3            -
4
5              name: pem_key_files
6
7              type: ns::systemfile
8
9              condition: "$components.der-certificate-files-comp or
                  $components.pem-certificate-files-comp"
10
11             properties:
12
13                    filecontent: $certificate.keyfile.contents
14
15                    fileencoding: "BASE64"
16
17                    filelocation: "/nsconfig/ssl"
18
19                    filename: $certificate.keyfile.filename
20  <!--NeedCopy-->
```

この例では、条件は複雑な「or」式です。StyleBook 内のほかの 2 つのコンポーネントが処理された（スキップされなかった）ことでコンポーネント間に依存関係が作成された場合にのみ、StyleBook によってこの構成オブジェクトが作成されるようにしています。

repeat 構造

May 7, 2021

コンポーネントの **repeat** 構造を使用して、同じタイプの複数の構成オブジェクトを作成できます。

次の例では、**members-svcg-comp** コンポーネントは、親コンポーネントが作成したサービスグループにサービス一覧をバインドするために使用されます。各サーバーをサービスグループにバインドする設定オブジェクトを作成するには、**repeat** 構造を使用して、パラメータ **svc-servers** に指定されているサービスのリストを反復処理します。反復処理中、コンポーネントはサービスグループ内の各サービスに対して **servicegroup_servicegroupmember_binding** 型の **NITRO** オブジェクト (repeat-item**** 構造体では ****srv** と呼ばれます) を作成し、各 NITRO オブジェクトの **ip** 属性を対応するサービスの IP アドレス。

例:

```
components:
  -
      name: my-lbvserver-comp
      type: ns::lbvserver
      properties:
           name: $parameters.name + "-lb"
           servicetype: HTTP
           ipv46: $parameters.ip
           port: 80
           lbmethod: $parameters.lb-alg
           components:
                -
                   name: my-svcg-comp
                   type: ns::servicegroup
                   properties:
                        name: $parameters.name + "-svcgrp"
                        servicetype: HTTP
                   components:
                         -
                         name: lbvserver-svg-binding-comp
                         type: ns::lbvserver\servicegroup\binding
                         properties:
                               name: $parent.parent.properties.name
                               servicegroupname: $parent.properties.
                                   name
                         -
                         name: members-svcg-comp
                         type: ns::servicegroup\servicegroupmember\
                            binding
                         repeat:
```



```
29                              repeat-list: $parameters.svc-servers
30                              repeat-item: srv
31                            properties:
32                                  ip: $srv
33                                  port: $parameters.svc-port
34                                  servicegroupname: $parent.properties.
                                        name
35  <!--NeedCopy-->
```

リ ピートはそれ自体でオブジェクトであり、リピートリストと リピートアイテムはリピートオブジェクトの属性です。

- repeat-list は、コンポーネントが反復する一覧を識別する必須の属性です。
- repeat-item はオプションで、反復処理中の現在の項目にフレンドリ名を付けるために使用されます。

指定しない場合、**$ repeat-item** という式を使用して現在の項目にアクセスできます。上の例の最後のコンポーネントは、次のように記述することもできます。

```
1             -
2
3             name: members-svcg-comp
4
5             type: ns::servicegroup_servicegroupmember_binding
6
7             repeat:
8
9               repeat-list: $parameters.svc-servers
10
11            properties:
12
13                  ip: $repeat-item
14
15                  port: $parameters.svc-port
16
17                  servicegroupname: $parent.properties.name
18  <!--NeedCopy-->
```

リストを反復処理する現在のアイテムを参照できるだけでなく、**repeat-index** を使用してリスト内のアイテムの現在のインデックスを参照することもできます。次の例では、**repeat-index** を使用して、現在のインデックスに基づいてポート番号を計算します。

```
1               name: services
2
3               type: ns::service
4
```



```
5               repeat:
6
7                  repeat-list: $parameters.app-services
8
9                  repeat-item: srv
10
11              properties:
12
13                  ip: $parameters.app-ip
14
15                  port: $parameters.base-port + repeat-index
16
17                  servicegroupname: $parent.properties.name
18 <!--NeedCopy-->
```

repeat-item 構造と同様に、別の変数名を割り当てて、反復の現在のインデックスを参照できます。前の例は次の例と同等です。

```
1       -
2
3               name: services
4
5               type: ns::service
6
7               repeat:
8
9                  repeat-list: $parameters.app-services
10
11                 repeat-item: srv
12
13                 repeat-index: idx
14
15              properties:
16
17                  ip: $parameters.app-ip
18
19                  port: $parameters.base-port + $idx
20
21                  servicegroupname: $parent.properties.name
22 <!--NeedCopy-->
```


繰り返し条件構成

May 7, 2021

repeat-condition 構造は repeat 構造の反復処理ごとに評価され、その結果によって、構成オブジェクトをその反復処理で作成するか次の反復処理に進むかが決定されます。次の例は、repeat-condition 構造の使用方法を示しています。

例:

```
components

   -

      name: der-key-files-comp

      type: ns::systemfile

      repeat:

      repeat-list: $parameters.certificates

      repeat-item: certificate

        repeat-condition: $certificate.ssl-inform == DER

        properties:

         filecontent: base64($certificate.keyfile.contents)

         fileencoding: BASE64

         filelocation: /nsconfig/ssl

         filename: $certificate.keyfile.file
<!--NeedCopy-->
```

この例では、der-key-files-comp コンポーネントはユーザーが指定したすべての証明書を繰り返し処理しますが、DER エンコーディングを使用して証明書に対応する設定オブジェクトのみが構築されます。反復処理ごとに repeat-condition 式が評価され、証明書のエンコーディングのタイプが DER かどうかがテストされます。タイプが DER でない場合、現在の反復処理では構成オブジェクトは作成されず、反復処理は一覧の次の証明書に進みます。

ネストされた繰り返し

May 7, 2021

repeat 構造をネストにして使用することで、コンポーネントの定義に応じて各コンポーネントに複数の repeat 構造を含めることができます。2 レベルのネストになった repeat 構造を考えます。外側のリスト（最初の repeat-list）の要素ごとに、内側のリスト（2 番目の repeat-list）の要素すべてに対して repeat リストを作成できます。StyleBook コンパイラでは、ネストになった repeat は最大で 3 つまでサポートされます。各 repeat レベルには、repeat-item 属性および repeat-index 属性を関連付けます。repeat-item 属性と repeat-index 属性はともにオプションです。また、repeat ごとに repeat-condition を指定することもできます。

例:

```
parameters:

  -

      name: vips

      type: ipaddress[]

  -

      name: vip-ports

      type: tcp-port[]

components:

  -

      name: lbvservers-comp

      type: ns::lbvserver

      repeat:

         repeat-list: $parameters.vips

         repeat-item: ip

         repeat:

              repeat-list: $parameters.vip-ports
```



```
32
33                repeat-item: port
34
35        properties:
36
37           name: str("lb-") + str($ip) + '-' + str($port)
38
39           servicetype: HTTP
40
41           ipv46: $ip
42
43           port: $port
44  <!--NeedCopy-->
```

この例では、$parameters.vipsの各項目について、$parameters.vip-portsのすべての項目を反復処理します。したがって、$parameters.vipsで指定されたそれぞれのipaddressについて、$parameters.vip-ports で指定されたすべてのポートのlbvserver設定オブジェクトを作成します。プロパティセクションでは、IP アドレスとポートの組み合わせのプレフィックスとして「lb」を持つオブジェクトの名前を定義します。したがって、反復ごとに、$ip + $portは IP アドレスとポート番号の一意の組み合わせを定義します。

repeat-item属性が指定されていない場合、コンパイラーはそのデフォルト値を生成します。repeat-item のデフォルト値は、各繰り返しレベルごとにぞれぞれ$repeat-item、$repeat-item-1、$repeat-item-2です。同様に、repeat-index 属性が指定されていない場合、コンパイラーはそのデフォルト値を生成します。repeat-index のデフォルト値は、repeat レベルごとにそれぞれ $repeat-index、$repeat-index-1、$repeat-index-2 となります。

以下の例では、ネストになった repeat オブジェクトで repeat-item 属性および repeat-index 属性を指定していない場合の命名規則を示します。

例:

```
1  components:
2
3  -
4
5       name: lbvservers-comp
6
7       type: ns::lbvserver
8
9       repeat:
10
11          repeat-list: $parameters.vips
12
13          repeat:
14
```



```
15              repeat-list: $parameters.vip-ports
16
17      properties:
18
19          name: str("lb-") + str($repeat-item) + '-' + str($repeat-item
                -1)
20
21          servicetype: HTTP
22
23          ipv46: $repeat-item
24
25          port: $repeat-item-1
26  <!--NeedCopy-->
```

結果

May 7, 2021

Outputs セクションでは、StyleBook によってすべての構成オブジェクトが正常に作成された後にユーザーに公開する情報を指定します。StyleBook の Outputs セクションは、必要に応じて記述します。StyleBook で必ずしも出力を返す必要はありません。ただし、内部コンポーネントを出力として返すと、この StyleBook をインポートするすべての StyleBook の柔軟性が向上します。このことは、複合 StyleBook の作成時にわかります。

次の表は、Outputs セクションで使用する属性を示しています。

属性	説明	固定
名前	公開する構成オブジェクトに対応する出力の名前。	はい
説明	出力について説明するテキスト文字列。	いいえ
value	この属性では、StyleBook によって返される値の抽出方法を指定します。	はい

例:

```
1  outputs:
2
3   -
```



```
4
5     name: lbvserver
6
7     description: LBVServer component
8
9     value: $components.my-lbvserver-comp
10
11   -
12
13    name: svc-grp
14
15      description: ServiceGroup name
16
17      value: $components.my-svcg.properties.name
18  <!--NeedCopy-->
```

この例では、**lbvserver** コンポーネントと **StyleBook**servicegroup によって作成される名前を公開します。**lbvserver** という出力の値はコンポーネント **my-lbvserver-comp** です。同様に、**svc-grp** と呼ばれる出力の値は、コンポーネント **my-svcg** によって作成されたservicegroupの名前です。

パラメータ参照

May 7, 2021

コンポーネント構成では、$parameters.<parametername>記法を使用して、パラメータセクションで定義されているパラメータを参照します。<parametername> それ自体にパラメータが含まれている場合（型がオブジェクトの場合）、$parameters.<parametername>.<sub-parametername>表記法を使用する必要があります。

例:

```
1  parameters:
2
3    -
4
5      name: name
6
7      label: Name
8
9      type: string
10
11     required: true
12
```



```
13      -
14
15       name: vip
16
17       label: Virtual IP and Port
18
19       type: object
20
21       required: true
22
23       parameters:
24
25         -
26
27           name: ip
28
29           label: Virtual IP
30
31           description: The Virtual IP Address
32
33           type: ipaddress
34
35           required: true
36
37             -
38
39               name: port
40
41               label: The Virtual Port
42
43               description: The TCP port for the Virtual IP
44
45               type: tcp-port
46
47               default: 80
48
49 components:
50
51   -
52
53     name: my-lbvserver-comp
54
55     type: ns::lbvserver
56
57     properties:
```



```
58
59          name: $parameters.name
60
61          servicetype: HTTP
62
63          ipv46: $parameters.vip.ip
64
65          port: $parameters.vip.port
66  <!--NeedCopy-->
```

親参照

May 7, 2021

ネストされたコンポーネントを使用している場合は、$parent 表記を使用して親コンポーネントを参照できます。親コンポーネントで repeat 構造を使用して複数の構成オブジェクトを作成し、反復処理ごとに子コンポーネントでほかの構成オブジェクトを作成する場合、$parent 表記は常に親コンポーネントの現在の反復処理を参照します。たとえば、$parent.properties.name は、親が現在の反復処理で作成する構成オブジェクトの name プロパティを参照します。

例:

```
1  components:
2
3   -
4
5     name: my-lbvserver-comp
6
7     type: ns::lbvserver
8
9     properties:
10
11      name: $parameters.name + "-lb"
12
13      servicetype: HTTP
14
15      ipv46: $parameters.ip
16
17      port: 80
18
19      lbmethod: $parameters.lb-alg
20
21      components:
```



```
22
23          -
24
25            name: my-svcg-comp
26
27            type: ns::servicegroup
28
29            properties:
30
31              name: $parameters.name + "-svcgrp"
32
33              servicetype: HTTP
34
35              components:
36
37               -
38
39                 name: lbvserver-svg-binding-comp
40
41                 type: ns::lbvserver_servicegroup_binding
42
43                 properties:
44
45                    name: $parent.parent.properties.name
46
47                    servicegroupname: $parent.properties.name
48
49                      -
50
51                        name: members-svcg-comp
52
53                        type: ns::servicegroup_servicegroupmember_binding
54
55                        repeat: $parameters.svc-servers
56
57                        repeat-item: srv
58
59                        properties:
60
61                          ip: $srv
62
63                          port: str($parameters.svc-port)
64
65                          servicegroupname: $parent.properties.name
66  <!--NeedCopy-->
```


また、最上位のコンポーネントまで、親の親のプロパティにアクセスして、コンポーネントの階層を上方に移動することもできます。たとえば、**lbvserver-svg-binding-comp** コンポーネントのプロパティ名は、**$parent.parent** 表記を使用して、親の親 **my-lbvserver-comp** コンポーネントのプロパティ名から値を取ります。

コンポーネントのリファレンス

May 7, 2021

コンポーネント構成では、$components.<componentname>表記を使用して StyleBook の最上位コンポーネントを参照します。最上位コンポーネント内にネストされたコンポーネントがある場合、使用される表記は、それらを参照する$components.<componentname>.components.<component-name>になります。

例:

```
components:

 -

     name: my-lbvserver-comp

     type: ns::lbvserver

     properties:

        name: $parameters.name + "-lb"

        servicetype: HTTP

        ipv46: $parameters.ip

        port: 80

        lbmethod: $parameters.lb-alg

  -

     name: my-svcg-comp

     type: ns::servicegroup

     properties:
```



```
28
29          name: $parameters.name + "-svcgrp"
30
31          servicetype: HTTP
32
33    -
34
35        name: members-svcg-comp
36
37        type: ns::servicegroup_servicegroupmember_binding
38
39        repeat: $parameters.svc-servers
40
41        repeat-item: srv
42
43        properties:
44
45          ip: $srv
46
47          port: str($parameters.svc-port)
48
49          servicegroupname: $components.my-svcg-comp.properties.name
50
51    -
52
53        name: lbvserver-svg-binding-comp
54
55        type: ns::lbvserver_servicegroup_binding
56
57        properties:
58
59            name: $components.my-lbvserver-comp.properties.name
60
61            servicegroupname: $components.my-svcg-comp.properties.name
62  <!--NeedCopy-->
```

この例では、**my-svcg-comp** コンポーネントと **my-lbvserver-comp** コンポーネントを作成してから、最後のコンポーネントである **lbvserver-svg-binding-comp** を作成する必要があります。この最後のコンポーネントには、これらのコンポーネントへの参照が含まれるからです。これらの参照は、`$components.<componentname>`で示されるコンポーネント参照を使用して提供されます。

置換参照

May 7, 2021

コンポーネントセクションまたはオペレーションセクションでは、**$substitutions.<substitution-name>** 表記を使用して、置換セクションで定義されている置換を参照します。たとえば、**$substitutions.http-port** のように指定します。

置換がマップの場合、マップ内の要素を**$substitutions.<substitutions-name>[<map-key>]**として参照できます。たとえば、**$substitutions.protocol-map[$parameters.port]**のようになります。

変数参照

May 7, 2021

コンポーネントの repeat 構造と repeat-item 構造を使用して複数の構成オブジェクトを作成するときに、repeat-item 構造に変数名を割り当てることができます。この変数は、$<varname>記法を使用して、そのコンポーネントのプロパティまたは子コンポーネントで参照できます。コンポーネントで repeat-item 構造を省略して repeat 構造を使用する場合は、$repeat-item というデフォルトの変数を使用して反復処理項目にアクセスできます。

例:

```
components:

  -

    name: server-members-comp

    type: ns::server

    condition: $parameters.svc-server-domain-names

    repeat: $parameters.svc-server-domain-names

    repeat-item: server-name

    properties:

      name: $server-name + "-server"

      domain: $server-name

    components:
```



```
22
23        -
24
25           name: service-members-comp
26
27           type: ns::service
28
29           properties:
30
31             name: $server-name + "-service"
32
33             servername: $parent.properties.name
34
35             servicetype: $parameters.svc-service-type
36
37             port: $parameters.svc-server-port
38  <!--NeedCopy-->
```

上の例では、repeat-item 構造に変数名 server-name が割り当てられています。この変数名は、同じコンポーネントのプロパティと子コンポーネント$<varname>で参照されます。

操作

May 7, 2021

Operations は、StyleBook のオプションのセクションです。このセクションでは、Citrix Application Delivery Management（ADM）分析を構成して、トラフィックトランザクションのすべてまたは一部の AppFlow レコードを収集できます。StyleBook を使用して Citrix ADC インスタンス上に作成された仮想サーバーは、これらのトラフィックトランザクションを処理します。このセクションでは、仮想サーバーで特定のトラフィック条件が満たされたときにアラームをトリガーするように Citrix ADM を構成することもできます。

StyleBook を使用して Citrix ADM を構成して、次のようなさまざまな Citrix ADM Insight からトラフィック統計を収集できます。

- Web Insight
- Security Insight
- HDX Insight
- Citrix ADC Gateway Insight。

サポートされる仮想サーバは、ロードバランシング、コンテンツスイッチング、および VPN 仮想サーバです。

負荷分散またはコンテンツスイッチング仮想サーバーでの分析のために、Web Insight と Security Insight の両方を有効にします。ただし、VPN 仮想サーバーの場合は、HDX Insight と Citrix ADC Gateway Insight の両方を有効にする必要があります。

StyleBooks を介して Citrix ADC インスタンス上で有効化された Citrix ADM インサイトは、IPFIX プロトコル（AppFlow）を使用して、インスタンスから Citrix ADC にデータを送信します。

また、Web Insight を有効にすると、負荷分散およびコンテンツスイッチング仮想サーバーで「クライアント側測定」が有効になります。この機能を有効にすると、ADM は HTML インジェクションを通じて HTML ページのロード時間とレンダリング時間メトリックをキャプチャします。管理者は、これらのメトリックスを使用して、L7 レイテンシーの問題を特定できます。

例 **1**:

次の例は、StyleBook にオペレーションセクションを記述して、VPN 仮想サーバーで HDX Insight と Citrix ADC Gateway Insight の両方を有効にする方法を示しています。

```
name: simple-vpn-ops

namespace: com.example.stylebooks

schema-version: "1.0"

version: "0.1"

description: Test StyleBook to enable hdxinsight and gatewayinsight on
    a VPN vserver

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    version: "10.5"

    prefix: ns

components:

  -

    name: vpnvserver-comp

    type: ns::vpnvserver

    properties:

      name: str("vpn-") + str($current-target.ip)

```



```
      servicetype: SSL

      ipv46: 1.1.21.37

      port: 443

operations:

    analytics:

      -

        name: comp-ops

        properties:

          target: $components.vpnvserver-comp

          filter: "true"

          insights:

            -

              type: hdxinsight
            -
              type: gatewayinsight

outputs:

  -

    name: myvpns

    value: $components.vpnvserver-comp
<!--NeedCopy-->
```

例 **2**:

次の例では、負荷分散仮想サーバーで Web Insight と Security Insight の両方を有効にするために、StyleBook に操作セクションを記述する方法を示します。

```
name: simple-vpn-ops
namespace: com.example.stylebooks
schema-version: "1.0"
```



```
version: "0.1"
description: Test StyleBook to enable hdxinsight and gatewayinsight on
    a VPN vserver
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
components:
    -
        name: vpnvserver-comp
        type: ns::vpnvserver
        properties:
            name: str("vpn-") + str($current-target.ip)
            servicetype: SSL
            ipv46: 1.1.21.37
            port: 443
operations:
    analytics:
        -
            name: comp-ops
            properties:
                target: $components.vpnvserver-comp
                filter: "true"
                insights:
                  -
                 type: hdxinsight
                  -
                 type: gatewayinsight
outputs:
  -
    name: myvpns
    value: $components.vpnvserver-comp
<!--NeedCopy-->
```

Analytics

May 7, 2021

オペレーションセクションの [分析] サブセクションは、コンポーネントセクションに似た構造になっています。分析セクションの各要素は、StyleBook によって作成された 1 つ以上の仮想サーバーの Citrix Application Delivery Management（ADM）分析機能を構成するために使用されます。

analytics セクションの要素には次の属性があります。

属性	説明	固定
名前	分析要素の名前。	はい
説明	この要素の内容を説明するテキスト文字列。	いいえ
condition	ブール式。この条件が false に評価された場合、分析要素全体がスキップされます。	いいえ
リピート	リストを反復します。	いいえ
repeat-condition	ブール式。式が false に評価されると、現在の反復がスキップされます。	いいえ
repeat-item	現在の反復の項目の名前。	いいえ
repeat-index	現在の反復の指数値の名前。	いいえ
properties	分析のプロパティの一覧。	はい
target	一覧のいずれかのプロパティ。ターゲット式は、分析を収集する Citrix ADC で構成された仮想サーバーの名前です。	はい
filter	一覧のいずれかのプロパティ。この属性の値は、分析を収集する仮想サーバー上の要求をフィルタリングするために使用される Citrix ADC の詳細ポリシー式です。デフォルトでは、分析データは仮想サーバーを通過するすべてのトラフィックで収集されます。	いいえ

例:

```
operations:

  analytics:

    -

```



```
    name: lbvserver-ops-comp

    properties:

    target: $components-basic-lb-comp.outputs.lbvserver-name

    filter: HTTP.REQ.URL.CONTAINS("catalog")

    insights:
          -
            type: webinsight
<!--NeedCopy-->
```

分析セクションの各属性は、Citrix ADM Analytics 機能に対して、ターゲットプロパティによって識別される仮想サーバー上の AppFlow レコードを収集するように Citrix ADC インスタンスを構成するように指示するために使用されます。

alarms

May 7, 2021

オペレーションセクションの「アラーム」サブセクションには、Analytics サブセクションと同じ構造と属性があります。唯一異なるのは properties 属性です。properties 属性以外のすべての属性のリストについては、Analyticsを参照してください。

アラームサブセクションでは、次のプロパティを使用できます。

属性	説明	固定
target	アラームが構成されている Citrix ADC で構成された仮想サーバーの名前に評価される式。	はい
email-profile	Citrix Application Delivery Management（ADM）分析機能で定義され、アラームがトリガーされたときに通知する電子メールアドレスのリストを含む電子メールプロファイルの名前。	いいえ（email-profileまたはsms-profileを定義する必要があります）

属性	説明	固定
sms-profile	Citrix ADM Analytics 機能で定義され、アラームがトリガーされたときに通知する電話番号のリストを含む SMS プロファイルの名前。	いいえ（email-profileまたはsms-profileを定義する必要があります）
rules	target プロパティで定義した仮想サーバーに対するアラームをトリガーする条件を定義する規則の一覧。	はい
metric	rules の属性。Citrix ADC 仮想サーバーに関して追跡するメトリックの名前。	はい
operator	rules の属性。測定基準と値の比較に使用する演算子。有効な演算子は、greaterthanおよびlessthanです。	はい
value	rules の属性。演算子を使用して測定基準と比較するしきい値。測定基準値がこのしきい値を超えると、関連するアラームがトリガーされます。	はい
period-unit	rules の属性。アラームの規則条件が満たされている場合にユーザーに通知する頻度。この属性には、日、時間、または週の値を含めることができます。つまり、ルールが満たされると、アラームは期間単位に 1 回 (たとえば 1 日に 1 回) 送信されます。	はい

次の表に、Citrix ADC 仮想サーバーに関して追跡されるメトリックのリストを示します。

カウンター	説明	詳細な説明	Citrix ADM 計算
VPN 仮想サーバーの場合:			

カウンター	説明	詳細な説明	Citrix ADM 計算
total_requests	VPN セッションの合計起動数	ユーザーが指定した期間内に、この VPN 仮想サーバーで起動されたアクティブなセッションの合計数。	新しいセッションの起動ごとに増分される、単調増加カウンター
app_count	VPN アプリケーションの起動数	ユーザーが指定した期間内に、この VPN 仮想サーバーで起動された一意の VPN アプリケーションの合計数。	新しいアプリケーションの起動ごとの単調増加カウンター
app_launch_duration	VPN アプリケーションの起動時間	アプリケーションの起動にかかった平均時間（ミリ秒単位）	この VPN 仮想サーバーで起動された、すべての VPN アプリケーションの起動時間から算出された平均値
その他の仮想サーバ (CS、LB、Auth、GSLB)			
total_requests	要求数	アプライアンスの最後の再起動と、仮想サーバーの作成の、いずれか最近行われた方以降の、この仮想サーバーのクライアント要求数。	この仮想サーバーに対する新しい要求ごとに増分される、単調増加カウンター。
total_bytes	バイト	指定した時間間隔で仮想サーバーから Citrix ADM に転送された合計バイト数。	この仮想サーバーの処理した合計バイト数が考慮された、単調増加カウンター。
application_response_time	応答時間	仮想サーバーの平均応答時間。	アプライアンスの最後のリブート以降（または仮想サーバーの作成以降）以降、この仮想サーバーが受信したすべての要求の応答時間の平均値（最後の方）。

StyleBook の alarms セクションの例:


```
operations:
alarms:
 -
  name:lbvserver_alarm
  properties:
  target: $outputs.lbvserver
  email-profile: $parameters.emailprofile
  sms-profile: "NetScalerSMS"
     rules:
      -
        metric: "total_requests"
        operator: "greaterthan"
        value: 25
        period-unit: weekly
        -
          metric: "total_bytes"
          operator: "lessthan"
          value: 1024
          period-unit: day

<!--NeedCopy-->
```

式

May 7, 2021

StyleBook の最も強力な機能の 1 つは、式の使用です。さまざまなシナリオで StyleBook の式を使用して動的な値を計算できます。次の例は、パラメータ値をリテラル文字列と連結する式です。

例:

```
$parameters.appname + "-mon"
```

この式は、appnameという名前のパラメータを取得し、文字列-monと連結します。

次の種類の式がサポートされています。

算術式

- 加算 (+)
- 減算 (-)
- 乗算 (*)

- 除算 (/)
- モジュロ (%)

例:

- 2 つの数字の加算：$parameters.a + $parameters.b
- 2 つの数字の乗算：$parameters.a * 10
- ある数を別の数で除算した後の余りを見つける：

`15%10` 結果 5

文字列式

- 2 つの文字列を連結する (+)

例:

Concatenate two strings: str(“app-“) + $parameters.appname

式の一覧表示

2 つのリスト（+）をマージします

例:

- Concatenate two lists: $parameters.external-servers + $parameters.internal-servers
- `$parameters.ports-1`が [80, 81] であり、`$parameters.port-2`が [81, 82] であるならば、`$parameters.ports-1 + $parameters.ports-2`がリスト [80, 81, 81, 82] として表示されます。

関係式

- **==** : 2 つのオペランドが等しいかどうかをテストし、それらが等しい場合は true を返し、それ以外の場合は false を返します。
- **!** =: 2 つのオペランドが異なるかどうかをテストし、それらが異なっている場合は true を返し、それ以外の場合は false を返します。
- **>** : 最初のオペランドが 2 番目のオペランドより大きい場合は true を返し、それ以外の場合は false を返します。
- **>=** : 最初のオペランドが 2 番目のオペランド以上の場合は true を返し、それ以外の場合は false を返します。
- **<** : 最初のオペランドが 2 番目のオペランドより小さい場合は true を返し、それ以外の場合は false を返します。
- **<=** : 最初のオペランドが 2 番目のオペランド以下の場合は true を返し、それ以外の場合は false を返します。

例:

- 等価演算子の使用: `$parameters.name = = "abcd"`
- 不等式演算子の使用: `$parameters.name != "default"`
- 他の関係演算子の例

```
- 10 > 9
- 10 >= 10
- 0 < 9
- 10 <= 9
- 10 == 10
- 10 != 1
```

論理式-ブール値

- **AND:** 論理「**and**」演算子。両方のオペランドが true の場合、結果は true となり、それ以外の場合は false となります。
- **or**: 論理 'or' 演算子。いずれかのオペランドが true の場合、結果は true となり、それ以外の場合は false となります。
- **NOT**: 単項演算子。オペランドが真の場合、結果は偽になり、逆になります。
- **in**: 最初の引数が第 2 引数の部分文字列かどうかをテストします
- **in**: 項目がリストの一部であるかどうかをテストします

> 注
>
> 文字列は（int () 組み込み関数を使用して）数字に変換され、数字は（str () 組み込み関数を使用して）文字列に変換される式を型キャストすることができます。同様に、`tcp-port`を数字にキャストすることができます (int () 組み込み関数を使用して)、IP アドレスは（str () 組み込み関数を使用して）文字列にキャストすることができます。
>
> 演算子の前と後に区切り文字を使用します。区切り記号は次のように使えます。
>
> - 演算子の前: `space`、`tab`、`comma`、`(`、`)`、`[`、`]`
> - 演算子の後: `space`、`tab`、`(`、`[`
>
> 次に例を示します:
>
> - `abc + def`
> - `100 % 10`

- `10 > 9`
- `$item in $parameters.some-list`

逐語的な文字列式

文字列内の特殊文字がリテラル形式を取る必要がある場合は、逐語的な文字列を使用できます。これらの文字列には、エスケープ文字、バックスラッシュ、引用符、括弧、空白、角かっこなどを含めることができます。逐語文字列では、特殊文字の通常の解釈はスキップされます。文字列内のすべての文字は、リテラル形式で保持されます。

StyleBooks では、逐語的な文字列を使用して、Citrix ADC ポリシー式をリテラル形式で含めることができます。通常、ポリシー式には特殊文字が含まれています。逐語的な文字列を使用しない場合、文字列を部分文字列に分割して特殊文字をエスケープする必要があります。

逐語的な文字列を作成するには、次のように特殊文字間の文字列をカプセル化します。

```
~{
 string }
 ~
<!--NeedCopy-->
```

StyleBook 式では、逐語的な文字列を使用できます。

> 注:
>
> このシーケンスは逐語的な文字列の終わりを示すため、入力文字列には一連の文字} ~を使用しないでください。

例:

```
 ~{
 HTTP.REQ.COOKIE.VALUE("jsessionid") ALT HTTP.REQ.URL.BEFORE_STR("=").
    AFTER_STR(";jsessionid=") ALT HTTP.REQ.URL.AFTER_STR(";jsessionid="
    ) }
 ~
<!--NeedCopy-->
```

複数の逐語文字列を連結する

逐語文字列を通常の文字列または補間で連結できます。そうすると、StyleBook は逐語文字列のみの解釈をスキップします。連結する文字列の間には、プラス (+) 演算子を使用します。

例:

```
value: "~{
 "id": " }
```



```
 ~ + %{
 $atom.key }
 % + ~{
 ", "value": " }
 ~ + %{
 $atom.value }
 % + ~{
 " }
 ~"
<!--NeedCopy-->
```

この例では、%{ $atom.key } %と%{ $atom.value } %が解釈されます。そして、残りの部分については解釈がスキップされます。

ターゲットエクスプレッション

StyleBook 定義では、$current-target式を使用して現在のターゲットの ADC インスタンスを参照できます。ターゲット ADC インスタンスの IP アドレスを具体的に参照するには、次の式を使用します。

```
$current-target.ip
<!--NeedCopy-->
```

例:

```
components:
 -
  name: lb-comp
  type: ns::lbvserver
  properties:
    name: $current-target.ip + "-lbvserver"
<!--NeedCopy-->
```

この例では、lbvserverの名前はターゲット ADC インスタンスの IP アドレスを使用します。

式の種類の検証

StyleBook エンジンでは、コンパイル時により強力な型チェックが可能になりました。つまり、StyleBook の作成時に使用される式は、設定パックの作成時ではなく、StyleBook 自体のインポート時に検証されます。

パラメータ、置換、コンポーネント、コンポーネントのプロパティ、コンポーネントの出力、ユーザー定義変数 (repeat-item、repeat-index、置換関数への引数) などへの参照はすべて、その存在と型について検証されます。

タイプチェックの例:

次の例では、lbvserverStyleBook のポートプロパティの予想されるタイプはtcp-portです。Citrix Application Delivery Management（ADM）では、タイプの検証はコンパイル時（インポート時）に行われます。コンパイラは、文字列とtcp-portが互換性がない型であることを検出するため、StyleBook コンパイラはエラーを表示し、StyleBook のインポートまたは移行に失敗します。

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: str("80")
      servicetype: HTTP
<!--NeedCopy-->
```

この StyleBook を正常にコンパイルするには、コンパイラで以下を数値として宣言します。

```
port: 80
```

無効な式のフラグ付けの例:

以前のリリースでは、無効な式がプロパティ名に割り当てられている場合、コンパイラは無効な式を検出せず、StyleBook を Citrix ADM にインポートすることができました。これで、この StyleBook が Citrix ADM にインポートされると、コンパイラはこのような無効な式を識別し、フラグを付けます。その結果、StyleBook は Citrix ADM へのインポートに失敗します。

この例では、lb-sg-binding-compコンポーネントの name プロパティに割り当てられる式は $components.lbvserver-comp.properties.lbvservernameです。ただし、コンポーネントlbvserver-compにはlbvservernameと呼ばれるプロパティはありません。以前の Citrix ADM リリースでは、コンパイラはこの式を許可し、正常にインポートされていました。実際の失敗はこの StyleBook を用いて構成パックを作成するときに起こります。ただし、インポート中にこの種のエラーが特定され、StyleBook は Citrix ADM にインポートされません。このようなエラーを手動で修正し、StyleBooks をインポートします。

```
Components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
    name: sg-comp
    type: ns::servicegroup
```



```
    properties:
      servicegroupname: mysg
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.lbvservername
      servicegroupname: $components.sg-comp.properties.servicegroupname
<!--NeedCopy-->
```

インデックスの一覧

一覧のアイテムは直接インデックスすることでアクセスできます。

式	説明
`$components.test-lbs[0]`	`thetest-lbs` コンポーネントの最初の項目を参照します
`$components.test-lbs[0].properties.p1`	test-lbs コンポーネントの最初のアイテムのプロパティ p1 を参照します。
`$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname`	`servicegroups`コンポーネントの 2 番目の項目のプロパティ`servicegroupname`を参照します。これは、`lbcomps`コンポーネントの最初の項目からの出力です。

インプレイス補間

May 7, 2021

StyleBook 式を使用して文字列の一部を置き換えることができるようになりました。これらの文字列式が StyleBook コンパイラによって評価されると、StyleBook 式を使用する文字列の一部が式の値に置き換えられます。文字列に StyleBook 式を含めるには、次の表記法を使用します。

```
"...%{
 ... }
 %..."
```



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

「%{」と「}%」で囲まれた文字は、StyleBook 式を形成します。こうした式は、「インプレース補間」と呼ばれます。

たとえば、`lb-%{ $parameters.appname } %-svc`文字列は StyleBook 式のインプレース補間を含む文字列式です。文字列式の値は、補間式の値によって異なります。**$parameters.appname** に「app1」が割り当てられていることを考えてみましょう。次に、文字列式は **lb-app1-svc** と評価されます。この機能を使用することで、値を文字列式に直接入力するのではなく、ユーザー定義値に応じて決めることができます。

インプレース補間の実用的な使用例としては、StyleBook のポリシー式のパラメーター化があります。HTTP URL に特定の語句（この例では「jpeg」）が含まれているかどうかをチェックするポリシー式を記述するシナリオを考えます。

この場合、記述するポリシー式は「HTTP.REQ.URL.CONTAINS(\“jpeg\”)」となります。

さて、HTTP URL でオブジェクトをパラメータ化したい場合は、StyleBook に文字列パラメータを追加することができます（`$parameters.url-object`など）。ポリシー式は、このパラメータに基づいて記述されます。この目的を達成するには、文字列連結を使用します。式は次のようになります。

```
str("HTTP.REQ.URL.CONTAINS(\\"" + $parameters.url-object + "\\")")
<!--NeedCopy-->
```

`$parameter.url-object`に「csv」が割り当てられている場合、上記の式は”HTTP.REQ.URL.CONTAINS(\“csv\”)” と評価されます。しかし、こうした式は読みにくいものです。インプレース補間を使用することで、こうしたパラメーター化を読みやすくわかりやすいものにすることができます。

インプレース補間を使用した式は次のようになります。

```
str("HTTP.REQ.URL.CONTAINS(%{
 quotewrap($parameters.url-object) }
 %)")
<!--NeedCopy-->
```

上記の式では、インプレース補間を使用して $parameters.url-object の値の前後に内部引用を追加しています。この式の結果は上記と同じですが、より直感的で実際の結果に近いように見えます。

補間式内で使用できる型

補間の内部で値を生成する式を使用できます: ブール、数値、`tcp-port`、`ipaddress`、および文字列。生成された値は、補間式が結果に置き換えられるときに自動で文字列へ変換されます。

文字列式には補間を含めないことも、1 個以上の補間を含めることもできます。順次補間で、文字列式の各部分を異なる StyleBook 式に置き換えることができます。たとえば、文字列 lb-%{$parameters.appname}%-%{$parameters.vip}% では、$parameters.appname が「app1」、$parameters.vip が「1.1.1.1」の場合、lb-app1-1.1.1.1 が返されます。

文字列式は、ネストされた補間もサポートします。つまり、補間式を別の補間式の内側に入れ子にして、ある式の値を別の式の入力にすることができます。

たとえば、文字列「% {lb-% {$ パラメータ.port + 1}%」を考えてみましょう。

内部文字列 “%**{$** パラメータ**.port + 1}%”** は、$ パラメータ.port が 80 の場合、”lb-81” を返します。ここでは、この式は、別の補間式の中にネストされています。

以下の表に、さまざまな種類の補間を例と対応する結果とともに示します。例で使用されているパラメータの値は次のとおりです。

- $parameters.appname: “lb1”
- $parameters.vip: “1.1.1.1”
- $parameters.n1: 1
- $parameters.n2: 3

単純な補間

式	結果
`lb-%{ $parameters.appname } %-def`	`lb-lb1-def`

自動型変換

式	結果
lb-%{1}%	lb-1
lb-%{$parameters.vip}%	lb-1.1.1.1
lb-%{true}%	lb-True

順次補間

式	結果
%{$parameters.appname}%-%{str($parameters.appname)}%	lb1-lb1
lb-%{1}%-%{2}%	lb-1-2

入れ子補間

式	結果
%{ abc-%{ $parameters.n1 + 1 } % } %	abc-2
str("%{ abc-%{ $parameters.n1 } % } %-%{ $parameters.n2 } %")	bc-1-3

quotewrap による補間

式	結果
str("%{ quotewrap(abcd)} %")	\"abcd\
str("%{ quotewrap(https://)} %+HTTP.REQ.HOSTNAME+HTTP.REQ.URL")	<https://"+HTTP.REQ.HOST NAME+HTTP.REQ.URL

補間式のエスケープ文字列

文字「% {」または「}%」が文字列の一部である場合、StyleBook コンパイラがこれらを補間タグとして評価しないように、エスケープ文字として”\” を指定する必要があります。

例:

```
str("%{ \\%\\{ + str($parameters.vip)+ \ } \\% } %")returns "%{ 1.1.1.1 } %
"if $parameters.vip is 1.1.1.1
```

以下の表に、その他の式と結果を示します。

カテゴリ	式	結果
補間のエスケープ	str("%{ str($parameters.n1)+ \ } \\% } %")	1 } %
	lb-%{ str($parameters.n1)+ \ } \\% } %	lb-1 } %
	"%{ str($parameters.n1)+ \\"\\ } \\\%\\"} %"	1 } %

組み込み関数

May 7, 2021

StyleBooks の式では、組み込み関数を使用できます。

たとえば、組み込み関数str()を使用して、数値を文字列に変換できます。


```
str($parameters.order)
```

または、組み込み関数**int**()を使用して、文字列を整数に変換することもできます。

```
int($parameters.priority)
```

以下は、StyleBook の式でサポートされる組み込み関数とその使用例の一覧です。

str()

str()関数は、入力引数を文字列値に変換します。

許可される引数の種類は次のとおりです。

- string
- number
- TCP-port
- **boolean**
- IP address

例:

- "set-"+ str(10)関数は"set-10"を返します。
- str(10)関数は10を返します。
- str(1.1.1.1)関数は1.1.1.1を返します。
- str(T rue)関数は"T rue"を返します。
- str(ADM)関数は"mas"を返します。

int()

この**int**()関数は、文字列、数値、IP アドレス、またはtcpportを引数として取り、整数を返します。

例:

- **int**("10")関数は10を返します。
- **int**(10)関数は10を返します。
- **int**(ip('0.0.4.1'))関数は1025を返します。

bool()

bool()関数は、引数として任意の型を取ります。引数の値が**false**、空の場合、または存在しない場合、この関数は**false**を返します。

それ以外の場合は、**true**を返します。

例:

- bool(**true**)関数は**true**を返します。

- `bool(false)`関数は`false`を返します。
- `bool($parameters.a)`関数は、`$parameters.a`が`false`、空、または存在しない場合に`false`を返します。

len()

`len()`関数は、引数として文字列またはリストを受け取り、文字列内の文字数またはリスト内の項目数を返します。

例 **1**:

次のように置換を定義した場合、

```
items: ["123", "abc", "xyz"]
```

`len($substitutions.items)`関数は 3を返します

例 **2**:

`len("Citrix ADM")`関数は10を返します。

例 **3**:

`$parameters.vips`に値`['1.1.1.1', '1.1.1.2', '1.1.1.3']`がある場合、`len($parameters.vips)`関数は3を返します。

min()

`min()`関数は、リストまたは一連の数値または`tcp-ports`を引数として受け取り、最小の項目を返します。

一連の番号**/tcp** ポートを使用する例:

- `min(80, 100, 1000)`関数は80を返します。
- `min(-20, 100, 400)`関数は-20を返します。
- `min(-80, -20, -10)`関数は-80を返します。
- `min(0, 100, -400)`関数は-400を返します。

番号**/tcp-**ポートのリストを持つ例:

- サポート`$parameters.ports`は、`tcp-ports` のリストであり、次の値を持ちます: `[80, 81, 8080]`.

  `min($parameters.ports)`関数は80を返します。

max()

`max()`関数は、引数として、リストまたは一連の数値または`tcp-ports`のいずれかを取って、最大の項目を返します。

一連の番号**/tcp** ポートを使用する例:

- `max(80, 100, 1000)`関数は`1000`を返します。
- `max(-20, 100, 400)`関数は`400`を返します。
- `max(-80, -20, -10)`関数は`-10`を返します。
- `max(0, 100, -400)`関数は`100`を返します。

番号**/tcp-**ポートのリストを持つ例:

- サポート`$parameters.ports`は`tcp-ports`のリストであり、次の値があります: `[80, 81, 8080]`。

  `max($parameters.ports)`関数は`8080`を返します。

bin()

`bin()`関数は、引数として数値を取り、バイナリ形式で数値を表す文字列を返します。

式の例:

`bin(100)`関数は`0b1100100`を返します。

oct()

`oct()`関数は、引数として数値を取り、8 進形式で数値を表す文字列を返します。

式の例:

`oct(100)`関数は`0144`を返します。

hex()

`hex()`関数は、引数として数値を取り、16 進数形式で数値を表す小文字の文字列を返します。

式の例:

`hex(100)`関数は`0x64`を返します。

lower()

`lower()`関数は、引数として文字列を受け取り、小文字で同じ文字列を返します。

例:

`lower("ADM")`関数は`adm`を返します。

upper()

`upper()`関数は、引数として文字列を受け取り、大文字で同じ文字列を返します。

例:

upper("Citrix ADM")関数はCITRIX ADMを返します。

sum()

このsum()関数は、数値のリストまたはtcpportsを引数として取り、リスト内の数値の合計を返します。

例 **1**:

置換を次のように定義した場合:
置換:

```
list-of-numbers = [11, 22, 55]
```

sum($substitutions.list-of-numbers)関数は88を返します。

例 **2**:

$parameters.portsが[80, 81, 82]の場合、sum($parameters.ports)関数は243を返します。

pow()

pow()関数は、引数として 2 つの数字を取り、2 番目の 1 の累乗に上げられた最初の引数を表す数値を返します。

例:

pow(3,2)関数は9を返します。

ip()

ip()関数は、引数として整数、文字列、または IP アドレスを受け取り、入力値に基づいて IP アドレスを返します。

例:

- ip 関数で IP アドレスを指定します。

  ip(3.1.1.1)関数は3.1.1.1を返します。

- ip 関数に文字列を指定します。

  ip('2.1.1.1')関数は 2.1.1.1を返します

- ip 関数に整数を指定します。

  - ip(12)関数は0.0.0.12を返します。
  - ip 関数で文字列として整数を指定すると、入力と同等の IP アドレスを返します。

    ip('1025')関数は0.0.4.1を返します。

  この関数は、整数の加算および減算操作もサポートし、結果の IP アドレスを返します。

  - 追記: ip(1025)+ ip(12)関数は0.0.4.13を返します。

- 減算: `ip('1025')- ip(12)`関数は`0.0.3.245`を返します。
- 加算と減算を組み合わせる: `ip('1.1.1.1')+ ip('1.1.1.1')- ip(2)` は`2.2.2.0`を返します。

ip_network ()

`ip_network`関数は、引数として IP アドレスとネットマスク長を取り、IP ネットワーク表記を返します。

Example-1:

`ip_network(1.1.1.1, 28)`関数は`1.1.1.1/28`を返します。

Example-2:

ネットワーク`1.1.1.1/30`について考えてみましょう。`ip_network($parameters.ipaddr, 30)`関数は`1.1.1.1`を返します。

Example-3:

ネットワーク`23.1.12.76/24`について考えてみましょう。`ip_network(23.1.12.76, $parameters.netmask-len)`関数は`24`を返します。

network_ip ()

`network_ip()` この関数は、指定された IP ネットワークの最初の IP アドレスを返します。

例:

`network_ip(1.1.1.1/28)`関数は`1.1.1.0`を返します。この例では、`1.1.1.0` は指定されたネットワーク内の最初の IP アドレスです。

subnets()

`subnets()`関数は、指定された IP ネットワークとネットマスク長からのサブネットのリストを返します。

例:

`subnets(1.1.1.1/28, 30)`関数は、指定された IP ネットワークとネットマスク長からサブネットリストを返します。出力は次のようになります。

`[1.1.1.0/30', '1.1.1.4/30', '1.1.1.8/30', '1.1.1.12/30']`

netmask_ip ()

`netmask_ip()`関数は、指定された IP ネットワークのネットマスク IP アドレスを返します。

例:

netmask_ip(1.1.1.1/28)関数は255.255.255.0を返します。指定されたIPネットワークで、255.255.255.0はネットマスクのIPアドレスです。

broadcast_ip ()

broadcast_ip()関数は、指定されたIPネットワークのブロードキャストIPアドレスを返します。

例:

broadcast_ip(1.1.1.1/28)関数は1.1.1.15を返します。指定されたネットワークで、1.1.1.1はブロードキャストIPアドレスです。

cidr ()

cidr()関数は、指定されたIPネットワークのCIDR表記を返します。

例:

cidr(1.1.1.1/28) 関数は、1.1.1.0/28を返します。指定されたネットワークでは、1.1.1.0/28はCIDR表記です。

is_cidr ()

is_cidr()関数は、ipnetworkを入力として受け入れます。そして、指定された値がIPネットワークのCIDR表記と一致した場合にTrueが返されます。

Example-1:

指定された値が指定されたネットワークのCIDR表記であるため、is_cidr(1.1.1.0/24)関数はTrueを返します。

Example-2:

指定されたネットワークのCIDR表記が指定された値と異なるため、is_cidr(1.1.1.1/28)関数はFalseを返します。

is_in_network ()

is_in_network()関数は、ipnetworkおよびipaddressの値を受け入れます。そして、指定された値がIPネットワークのCIDR表記と一致した場合にTrueが返されます。

Example-1:

1.1.1.121アドレスが1.1.1.1/24ネットワークの一部であるため、is_in_network(1.1.1.1/24, 1.1.1.121)関数はTrueを返します。

Example-2:

2.1.1.1アドレスが1.1.1.1/28ネットワークの一部ではないため、is_in_network(1.1.1.1/28, 2.1.1.1)関数はFasleを返します。

base64.encode()

base64.encode() この関数は、文字列引数を受け取り、base64 でエンコードされた文字列を返します。

例:

base64.encode("abcd")関数はYWJjZA==を返します。

base64.decode()

base64.decode関数は、base64 でエンコードされた文字列を引数として取り、デコードされた文字列を返します。

例:

base64.decode("YWJjZA==")関数はabcdを返します。

exists()

exists()関数は、任意の型の引数を受け取り、ブール値を返します。入力に値がある場合戻り値はTrueです。戻り値は、入力引数が値を持たない場合 (つまり、値がない場合)False です。

$parameters.monitor はオプションのパラメータであるとします。構成パックの作成時にこのパラメータに値を指定すると、($parameters.monitor)関数はTrueを返します。

それ以外の場合は、Falseを返します。

filter()

filter()関数は 2 つの引数を取ります。

引数 1: 1 つの引数を受け取ってブーリアン型の値を返す置換関数です。

引数 2: 一覧です。

この関数は、最初の引数の置換関数に渡されたときに各要素がTrueに評価される元のリストのサブセットを返します。

例:

置換関数を次のように定義したとします。

Substitutions:

```
x(a): $a != 81
```


この関数は、入力値が81と等しくない場合に True を返します。それ以外の場合は、`False`を返します。

`$parameters.ports`を`[81, 80, 81, 89]`と想定します。

`filter($substitutions.x, $parameters.ports)`は、リストからすべての81のオカレンスを削除して`[80, 89]`を返します。

if-then-else()

`if``-then-`**`else`**`()`関数は 3 つの引数を取ります。

引数 1: ブール式

引数 2: 任意の式

引数 3: 任意の式（オプション）

引数 1 の式が`True`と評価された場合、関数は引数 2 として指定された式の値を返します。

それ以外の場合は、引数 3 が指定されている場合、この関数は引数 3 の式の値を返します。

引数 3 が指定されていない場合、関数は`no`を返します。

例 **1**:

`$parameters.servicetype`が値`HTTP`を持っている場合、**`if`**`-then-`**`else`**`($parameters.servicetype == HTTP, 80, 443)`関数は`80`を返します。それ以外の場合、関数は`443`を返します。

例 **2**:

`if``-then-`**`else`**`($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport)` 関数は、`$parameters.servicetype`が`HTTP`値を持っている場合、`$parameters.hport`の値を返します。

それ以外の場合、関数は`$parameters.sport`の値を返します。

例 **3**:

`$parameters.servicetype`が値`HTTP`を持っている場合、**`if`**`-then-`**`else`**`($parameters.servicetype == HTTP, 80)`は`80`を返します。

それ以外の場合、関数は値を返しません。

join()

`join()`関数は、次の 2 つの引数を取ります。

引数 1: 数値、`tcp-ports`、文字列、または IP アドレスのリスト

引数 2: 区切り文字列（オプション）

この関数は、引数 1 として指定されたリストの要素を文字列に結合します。各要素は、引数 2 として提供される区切り文字列で区切られています。引数 2 を指定しない場合、リスト内の要素は 1 つの文字列として結合されます。

例:

- `$parameters.ports`は`[81, 82, 83]`です。
  - デリミタ引数付き:

    `join($parameters.ports, '-')`関数は`81-82-83`を返します。
  - デリミタ引数なし:

    `join($parameters.ports)`関数は`818283`を返します。

split()

`split()`関数は、指定された区切り文字に応じて、複数のリストに入力文字列を分割します。セパレータを指定しなかったり、空白 (`''`) を指定した場合、この関数はスペースをセパレータとみなし、文字列をリストに分割します。

例:

- `split('Example_string_split', 's')`関数は`['Example_','tring_','plit']`を返します。
- `split('Example string split')`関数は`['Example','string','split']`を返します。
- `split('Example string split', '')`関数は`['Example','string','split']`を返します。
- `split('Example string')`関数は`['Example','string']`を返します。

  この関数は、連続空間を 1 つのスペースとみなします。

map()

`map()`関数は 2 つの引数を取ります。

引数 1: 任意の関数

引数 2: 要素の一覧

この関数は、リスト内の各要素は、引数 2 の対応する要素に`map()`関数（引数 1）を適用した結果であるリストを返します。

引数 1 で許可される関数は次のとおりです。

- 1 つの引数を取る組み込み関数:

  `base64.encode`, `base64.decode`, `bin`, `bool`, `exists`, `hex`, **`int`**, `ip`, `len`, `lower`, `upper`, `oct`, `quotewrap`, `str`, `trim`, `upper`, `url.encode`, `url.decode`

- 1 つ以上の引数を受け取る置換関数。

例:

Suppose $parameters.nums is `[81, 82, 83]`.

- Map using a built-in function, str

  `map(str, $parameters.nums)`関数は `["81", "82", "83"]`を返します

  map 関数の結果は文字列の一覧であり、文字列の各要素は、入力した一覧 ($parameters.nums) の対応する要素に str 関数を適用して処理されています。

- 置換関数を使用した map
  - Substitutions:

    ```
    add-10(port): $port + 10
    ```

  - 式:

    `map($substitutions.add-10, $parameters.nums)`関数は、数値のリストを返します。`[ 91, 92, 93 ]`

このマップ関数の結果は、数字のリストであり、各要素は、入力リスト(`$parameters.nums`)内の対応する要素に置換関数`$substitutions.add-10`を適用することによって計算されます。

quotewrap()

`quotewrap()`関数は、引数として文字列を受け取り、入力値の前後に二重引用符を追加した後に文字列を返します。

例:

`quotewrap("ADM")`関数は `"mas"`を返します

replace()

`replace()`関数は、次の 3 つの引数を取ります。

引数 1: 文字列

引数 2: 文字列またはリスト

引数 3: 文字列（オプション）

この関数は、引数 1 の中にある引数 2 のすべてのアイテムを引数 3 で置き換えます。

引数 3 が指定されていない場合、引数 2 のすべての出現は引数 1 から削除されます (つまり、空の文字列に置き換えられます)。

文字列の一部を、別の文字列の一部で置き換えます。

- `replace('abcdef', 'def', 'xyz')`関数は`abcxyz`を返します。

  `def`のすべてのオカレンスは`xyz`に置き換えられます。

- `replace('abcdefabc', 'def')`は`abcabc`を返します。

  3 番目の引数がないので、結果の文字列から`def`が削除されます。

置換する文字リストを文字列で指定します。

```
$parameters.spl_chars = ['@', '##', '!', '%']
```

このリストには、入力文字列で置換する必要がある値が含まれています。

`replace('An##example@to%replace!characters', $parameters.spl_chars, '_')`関 数は`An_example_to_replace_characters`を返します。

出力文字列には、`$parameters.spl_chars` リストで指定された文字の代わりにアンダースコア (_) が表示されます。

trim()

`trim()`関数は、入力文字列から先頭と末尾の空白を取り除いた文字列を返します。

例:

`trim('abc ')`関数は`abc`を返します。

truncate()

`truncate()`関数は、次の 2 つの引数を取ります。

引数 1: 文字列

引数 2: 数字

この関数は、引数 1 の入力文字列を、引数 2 で指定された長さに切り捨てた文字列を返します。

例:

`truncate('Citrix ADM', 6)`は`Citrix`を返します。

distinct()

`distinct()`関数は、リスト入力から一意の項目を抽出します。

例:
`$parameters.input_list`が`['ADM', 'ADC', 'VPX', 'ADC', 'ADM', 'CPX']`の 場 合、`distinct($parameters.input_list)`関数は`['ADM', 'ADC', 'VPX', 'CPX']`を返します。

url.encode ()

`url.encode()`関数は、RFC 3986 に従って ASCII 文字セットを使用して文字が変換される文字列を返します。

例:

`url.encode("a/b/c")`関数は`a%2Fb%2Fc`を返します。

url.decode ()

`url.decode()`関数は、URL エンコードされた引数が RFC 3986 に従って通常の文字列にデコードされる文字列を返します。

例:

`url.decode("a%2Fb%2Fc")`関数は`a/b/c`を返します。

is-ipv4()

`is-ipv4()`関数は、引数として IP アドレスを受け取り、IP アドレスが IPv4 形式の場合はブール値`True`を返します。

`is-ipv4(10.10.10.10)`関数は `True`を返します

is-ipv6()

`is-ipv6()`関数は、引数として IP アドレスを受け取り、IP アドレスが IPv6 形式の場合はブール値`True`を返します。

`is-ipv6(2001:DB8::)`関数は `True`を返します

startsWwith ()

`startswith()`関数は、文字列が指定されたプレフィックスで始まるかどうかを決定します。この関数には、2 つの必須文字列引数が必要です。

```
startswith(str, sub_str)
```

この関数は、文字列（`str`）が部分文字列（`sub_str`）で始まるときに`True`を返します。

例:

- `startswith('Citrix', 'Ci')`関数は`True`を返します。
- `startswith('Citrix', 'iC')`関数は `False`を返します
- `startswith('Citrix', 'Ab')`関数は `False`を返します

endswith ()

endswith()関数は、文字列が指定された接尾辞で終わるかどうかを決定します。この関数には、2 つの必須文字列引数が必要です。

```
endswith(str, sub_str)
```

この関数は、文字列（str ）が部分文字列（sub_str）で終わるときにTrueを返します。

例:

- endswith('Citrix', 'ix')関数はTrueを返します。
- endswith('Citrix', 'Ix')関数はFalseを返します。
- endswith('Citrix', 'ab')関数はFalseを返します。

() を含む

contains()関数は、文字列に指定された部分文字列が含まれているかどうかを判定します。この関数には、2 つの必須文字列引数が必要です。

```
contains(str, sub_str)
```

この関数は、部分文字列（sub_str）が文字列（str）内の任意の場所に含まれている場合にTrueを返します。

例:

- contains('Citrix', 'tri')関数はTrueを返します。
- contains('Citrix', 'Ci')関数はTrueを返します。
- contains('Citrix', 'ti')関数は Falseを返します

部分文字列 ()

substring() 関数を使用して、文字列から部分文字列を抽出します。

```
substring(str, start_index, end_index)
```

この関数には、2 つの必須引数と 1 つのオプションの整数引数が必要です。

- str (必須)
- start_index (必須)
- end_index （オプション）

この関数は、指定されたインデックス位置の間にある文字列 (str) から部分文字列を返します。終了インデックス位置を指定しない場合、関数は開始インデックスから文字列の末尾までの部分文字列を抽出します。

> 注:
>
> end_indexを指定すると、そのend_index位置の文字は部分文字列から除外されます。

例:

- `substring('Citrix', 2)`関数は `trix`を返します
- `substring('Citrix', 10)`関数は (") を返します

  この例では、無効な`start_index`位置があるため、関数は空白の文字列を返します。
- `substring('Citrix', 2, 4)`関数は `tr`を返します

  この例では、関数は 2 ～4 つのインデックス位置の間の文字を抽出します。
- `substring('Citrix', -3)`関数は `rix`を返します

  文字列の末尾にある文字を抽出する場合は、`start_index` 引数に負の値を指定します。

  この例では、関数は、文字列の最後の 3 文字を含む部分文字列を抽出します。

依存関係の検出

May 7, 2021

StyleBook のコンポーネントでは、同じ StyleBook に含まれる別のコンポーネントのプロパティまたはセクションを参照できます。コンポーネントはそれ自体が完全なブロックであり、実行する必要があるのと同じ順序で書き込まれない場合があります。StyleBook コンパイラは、コンポーネントが書き込まれる順序をチェックし、論理的な順序で実行されます。

例:

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: mylb

      ipv46: 10.102.190.15

      port: 80

      servicetype: HTTP

-
    name: lb-sg-binding-comp
```



```
21
22      type: ns::lbvserver_servicegroup_binding
23
24      condition: $parameters.create-binding
25
26      properties:
27
28        name: $components.lbvserver-comp.properties.name
29
30        servicegroupname: $components.sg-comp.properties.servicegroupname
31
32  -
33      name: sg-comp
34
35      type: ns::servicegroup
36
37      properties:
38
39        servicegroupname: mysg
40
41        servicetype: HTTP
42  <!--NeedCopy-->
```

上記の例では、定義された 3 つのコンポーネントがあります- **lbvserver-comp**、**lb-sg-binding-comp**、および **sg-comp**。この StyleBook を実行すると、`lbvserver-comp`が最初に作成されます。`lb-sg-binding-comp`は`lbvserver-comp`プロパティを参照しますが、StyleBook で定義されている 2 番目のコンポーネントですが、次に作成することはできません。これは、`lb-sg-binding-comp`がまだ作成されていない`sg-comp`にも依存しているためです。その結果、コンパイラーはコンポーネントの順序を変更して、コンポーネントが作成されるまでにコンポーネントの依存関係が解決され、この順序が変更されたコンポーネントのリストを実行します。上記の StyleBook の実行順序は `lbvserver-comp`、`sg-comp`、`lb-sg-binding-comp`です。

したがって、StyleBook の作成者がコンポーネントの正確な順序を気にする必要はありません。コンポーネントはどのような順序で記載しても構いません。コンパイラにより、コンポーネント間の参照関係に基づいて適切なコンポーネントの実行順序が計算されます。これは、置換セクションと出力セクションにも適用されます。

循環依存関係

コンポーネントは別のコンポーネントを参照する場合があるため、依存関係のサイクルが StyleBook の定義に導入される可能性があります。たとえば、コンポーネント A がコンポーネント B で定義されているプロパティを参照しており、さらにコンポーネント B がコンポーネント A で定義されているプロパティを参照している場合などです。こうした依存関係は、循環依存関係と呼ばれます。循環依存関係を自動で解決することはできません。StyleBook の作成者は、StyleBook の定義を手動で修正して、このような循環依存を排除します。コンパイラは循環依存関係を特定することができ、循環依存関係が存在する場合にはレポートします。

以下の例に、コンポーネントの循環依存関係を示します。

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: $components.lb-sg-binding-comp.properties.name

      ipv46: 10.102.190.15

      port: 80

      servicetype: HTTP

  -

    name: lb-sg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    condition: $parameters.create-binding

    properties:

      name: mylb

      servicegroupname: $components.sg-comp.properties.servicegroupname

  -

    name: sg-comp

    type: ns::servicegroup

    properties:

      servicegroupname: mysg

      servicetype: $components.lbvserver-comp.properties.servicetype
```



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

上記の例では、**lbvserver-comp**、**lb-sg-binding-comp**、および **sg-comp** の 3 つのコンポーネントがあります。lbvserver-comp コンポーネントは lb-sg-binding-comp、lb-sg-binding コンポーネントに依存します。そして、これらのコンポーネントはsg-compに依存します。sg-compコンポーネントはlbvserver-compに依存します。このように、これらのコンポーネント間で依存関係の循環が生じており、この循環は自動で解決できません。その結果、この StyleBook を実行することはできません。StyleBook コンパイラはこれを検出し、StyleBook が Citrix ADM にインポートされないようにします。

インスタンス管理

May 7, 2021

インスタンスは、Citrix Application Delivery Management（ADM）を使用して管理、監視、トラブルシューティングを行うことができる Citrix Application Delivery Controller（ADC）アプライアンスです。Citrix ADM にインスタンスを追加して監視します。インスタンスは、Citrix ADM の設定時またはそれ以降でも追加できます。Citrix ADM にインスタンスを追加すると、継続的にポーリングされ、後で問題の解決やレポートデータとして使用できる情報を収集します。

インスタンスは、静的グループまたはプライベート IP ブロックとしてグループ化できます。インスタンスの静的グループは、設定ジョブなどの特定のタスクを実行する場合に便利です。プライベート IP ブロックは、地理的な場所に基づいてインスタンスをグループ化します。

インスタンスを追加する

インスタンスは、Citrix ADM サーバーの初回セットアップ時に追加することも、後で追加することもできます。インスタンスを追加するには、各 Citrix ADC インスタンスのホスト名または IP アドレス、または IP アドレスの範囲を指定する必要があります。

Citrix ADM にインスタンスを追加する方法については、「Citrix ADM へのインスタンスの追加」を参照してください。

Citrix ADM サーバーにインスタンスを追加すると、サーバーはインスタンスをトラップ先として暗黙的に追加し、インスタンスのインベントリを収集します。詳しくは、「[Citrix ADM によるインスタンスの検出方法。]」を参照してください。(http://docs.citrix.com/en-us/netscaler-mas/12-1/overview/how-mas-discovers-instances.html)

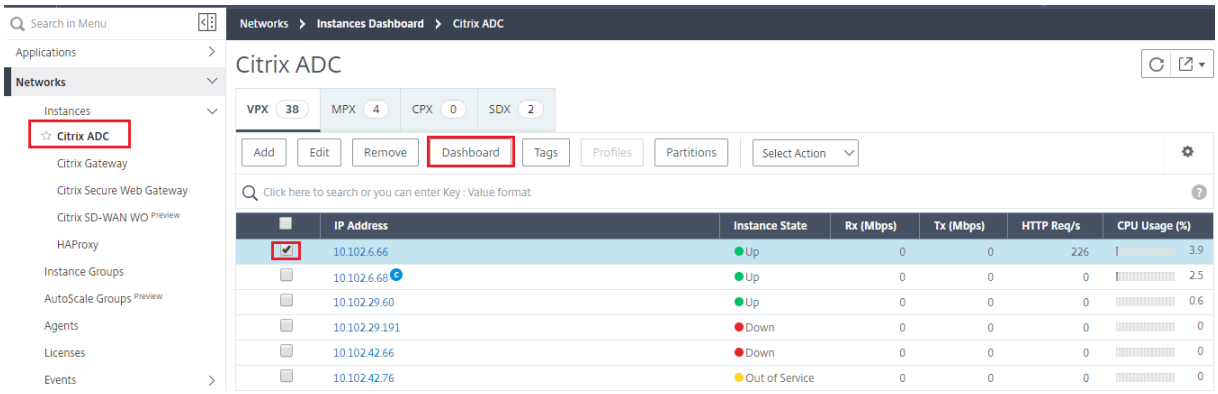
インスタンスを追加したら、[ネットワーク] > [ダッシュボード] の順に選択し、[すべてのインスタンス**]** をクリックしてインスタンスを削除できます。[Instances] ページで、削除するインスタンスを選択し、[**Remove**] をクリックします。

インスタンスダッシュボードの使用方法

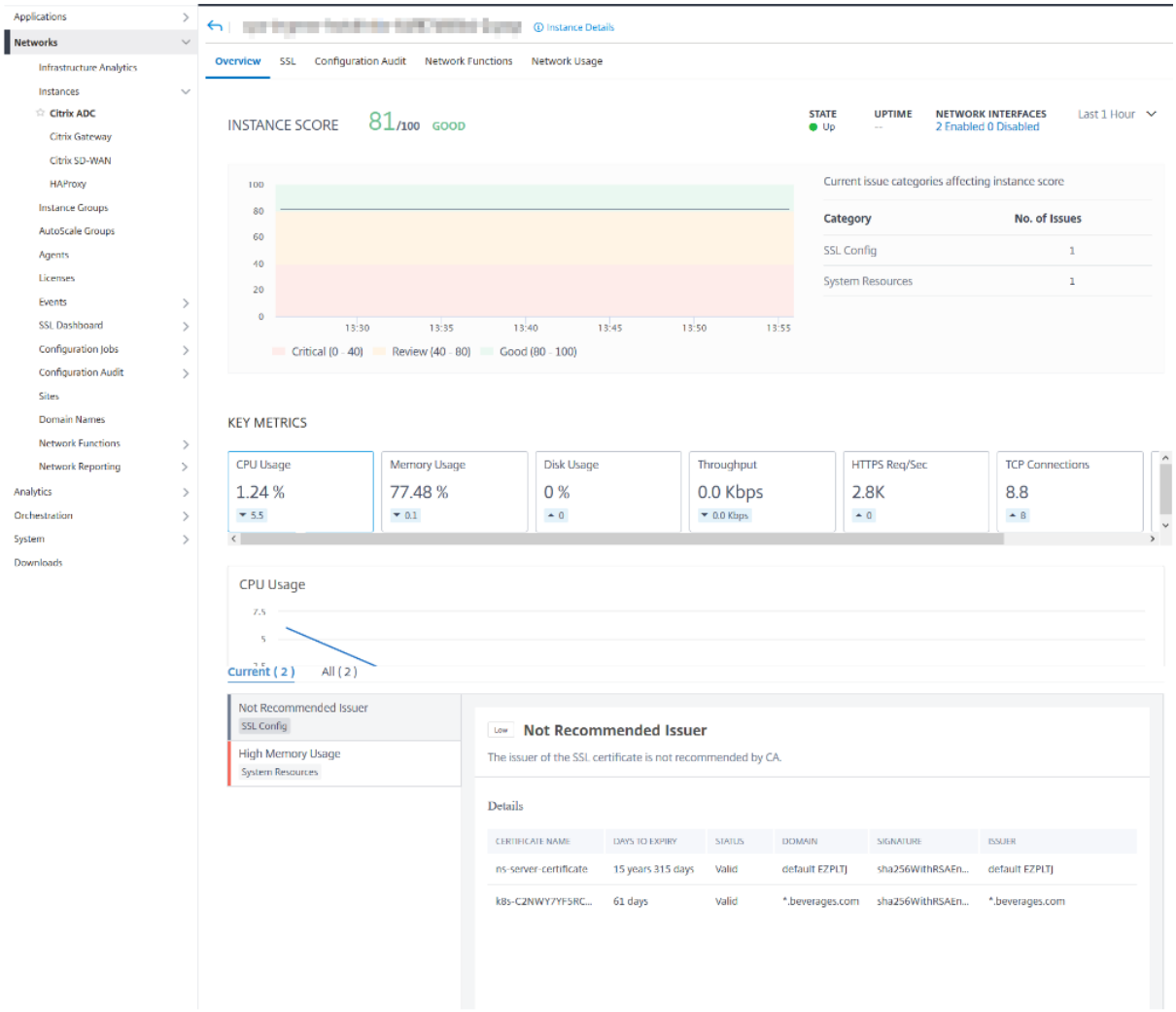
Citrix ADM インスタンスごとのダッシュボードには、選択したインスタンスのデータが表形式およびグラフィック形式で表示されます。ポーリングプロセス中にインスタンスから収集されたデータがダッシュボードに表示されます。

デフォルトでは、1 分ごとに、マネージインスタンスがデータ収集のためにポーリングされます。NITRO 呼び出しを使用して、状態、HTTP リクエスト/秒、CPU 使用率、メモリ使用量、スループットなどの統計情報を継続的に収集します。管理者は、収集したデータをすべて 1 つのページに表示し、インスタンス内の問題を特定し、すぐに修正するためのアクションを実行できます。

特定のインスタンスのダッシュボードを表示するには、[ネットワーク] > [インスタンス] > [**Citrix ADC**] の順に移動します。[Citrix ADC] ページで、インスタンスタイプを選択し、表示するインスタンスを選択し、[ダッシュボード] をクリックします。



次の図は、インスタンス単位のダッシュボードに表示されるさまざまなデータの概要を示しています。



- 概要。概要タブには、選択したインスタンスの CPU とメモリの使用量が表示されます。インスタンスによって生成されたイベントとスループットデータを表示することもできます。IP アドレス、ハードウェアと LOM バージョン、プロファイルの詳細、シリアル番号、連絡先など、インスタンス固有の情報もここに表示されます。さらに下にスクロールすると、選択したインスタンスで使用できるライセンスされた機能と、そのインスタンスで設定されたモードが表示されます。詳しくは、「インスタンスの詳細」を参照してください。
- **SSL** ダッシュボード。インスタンスごとのダッシュボードの [SSL] タブを使用して、選択したインスタンスの SSL 証明書、SSL 仮想サーバー、および SSL プロトコルの詳細を表示または監視できます。グラフの「数字」をクリックすると、詳細が表示されます。
- 構成監査。[configuration audit] タブを使用して、選択したインスタンスで発生したすべての設定変更を表示できます。ダッシュボード上の **Citrix ADC** 構成保存ステータスおよび **CitrixADC** 構成ドリフトグラフには、保存されていない構成に対する構成変更に関する詳細な詳細情報が表示されます。
- ネットワーク機能。ネットワーク機能ダッシュボードを使用して、選択した Citrix ADC インスタンスに構成されているエンティティの状態を監視できます。クライアント接続、スループット、サーバー接続などのデータを表示する仮想サーバーのグラフを表示できます。

- ネットワークの使用状況。選択したインスタンスのネットワークパフォーマンスデータは、[ネットワーク使用状況] タブで確認できます。1 時間、1 日、1 週間、または 1 か月分のレポートを表示できます。タイムラインスライダ機能を使用して、生成されるネットワークレポートの持続時間をカスタマイズできます。デフォルトでは、8 つのレポートのみが表示されますが、画面の右下隅にある「プラス」アイコンをクリックすると、別のパフォーマンスレポートを追加できます。

グローバルに分散したサイトを監視する方法

May 7, 2021

ネットワーク管理者は、さまざまな地域に展開されたネットワークインスタンスを必要に応じて監視および管理する必要があります。ただし、地理的に分散したデータセンターでネットワークインスタンスを管理する場合、ネットワークの要件を評価することは容易ではありません。

Citrix Application Delivery Management（Citrix ADM）のジオマップでは、サイトをグラフィカルに表示し、ネットワーク監視エクスペリエンスを地域別に分類できます。また、ネットワークインスタンスの分布を場所ごとに表示し、ネットワークの問題を監視することもできます。

以下のセクションでは、Citrix ADM でデータセンターを監視する方法について説明します。

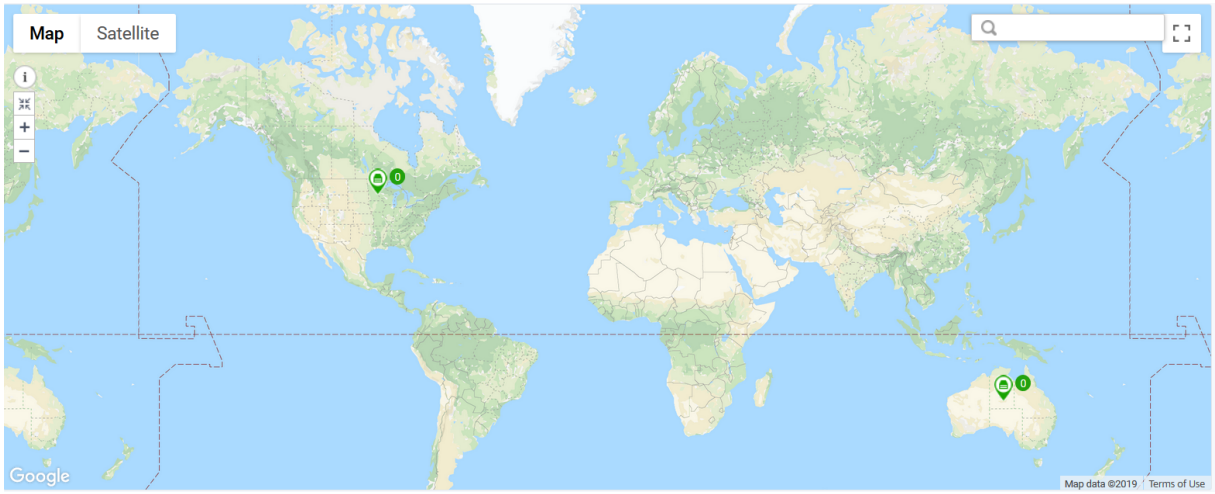
Citrix ADM でグローバルに分散したサイトの監視

Citrix ADM サイトは、特定の地理的場所にある Citrix アプリケーション Delivery Controller（Citrix ADC）インスタンスの論理的なグループです。たとえば、あるサイトが Amazon Web Services（AWS）に割り当てられ、別のサイトが Azure™ に割り当てられる場合があります。テナントの敷地内に別のサイトがホストされています。Citrix ADM は、すべてのサイトに接続されているすべての Citrix ADC インスタンスを管理および監視します。Citrix ADM を使用して、syslog、AppFlow、SNMP、および管理対象インスタンスから発信されるそのようなデータを監視および収集できます。

Citrix ADM ジオマップでは、サイトをグラフィカルに表現できます。また、Geomaps はネットワークモニタリング体験を地理別に分解します。ジオマップを使用すると、場所ごとにネットワークインスタンスの分布を視覚化し、すべてのネットワーク問題を監視できます。メニューの [ネットワーク] をクリックすると、インスタンスダッシュボードが表示され、ワールドマップ上に作成されたサイトが視覚的に表示されます。

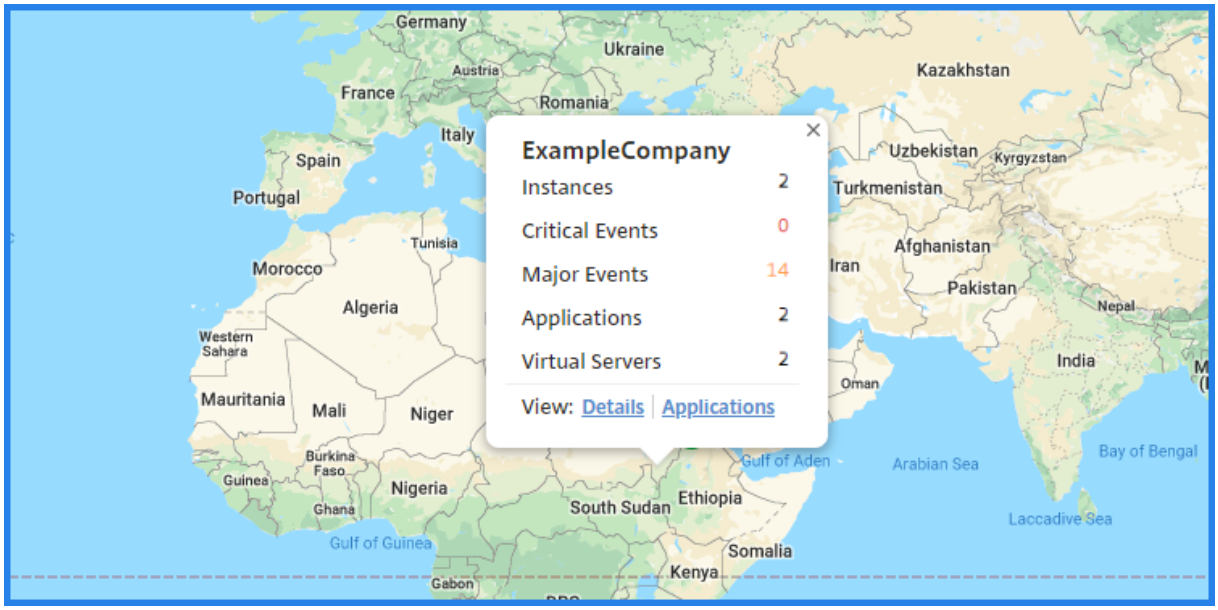
使用例

大手モバイルキャリア会社、ExampleCompany は、リソースとアプリケーションをホスティングするためにプライベートサービスプロバイダーに依存していました。同社はすでに 2 つのサイトを持っていました。1 つは米国のミネアポリス、もう 1 つはオーストラリアのアリススプリングスにあります。この画像では、2 つのマーカーが 2 つの既存のサイトを表していることがわかります。



マーカーには、サイト上の次のコンポーネントの数も表示されます。

- インスタンス: 使用可能なインスタンスの数を示します。
- アプリケーション: ホストされているアプリケーションの数を示します。
- 仮想サーバー: 使用可能な仮想サーバーの数を示します。
- **Critical Events**: インスタンスで発生したクリティカルイベントの数を示します。
- メジャーイベント: インスタンスで発生したメジャーイベントの数を示します。

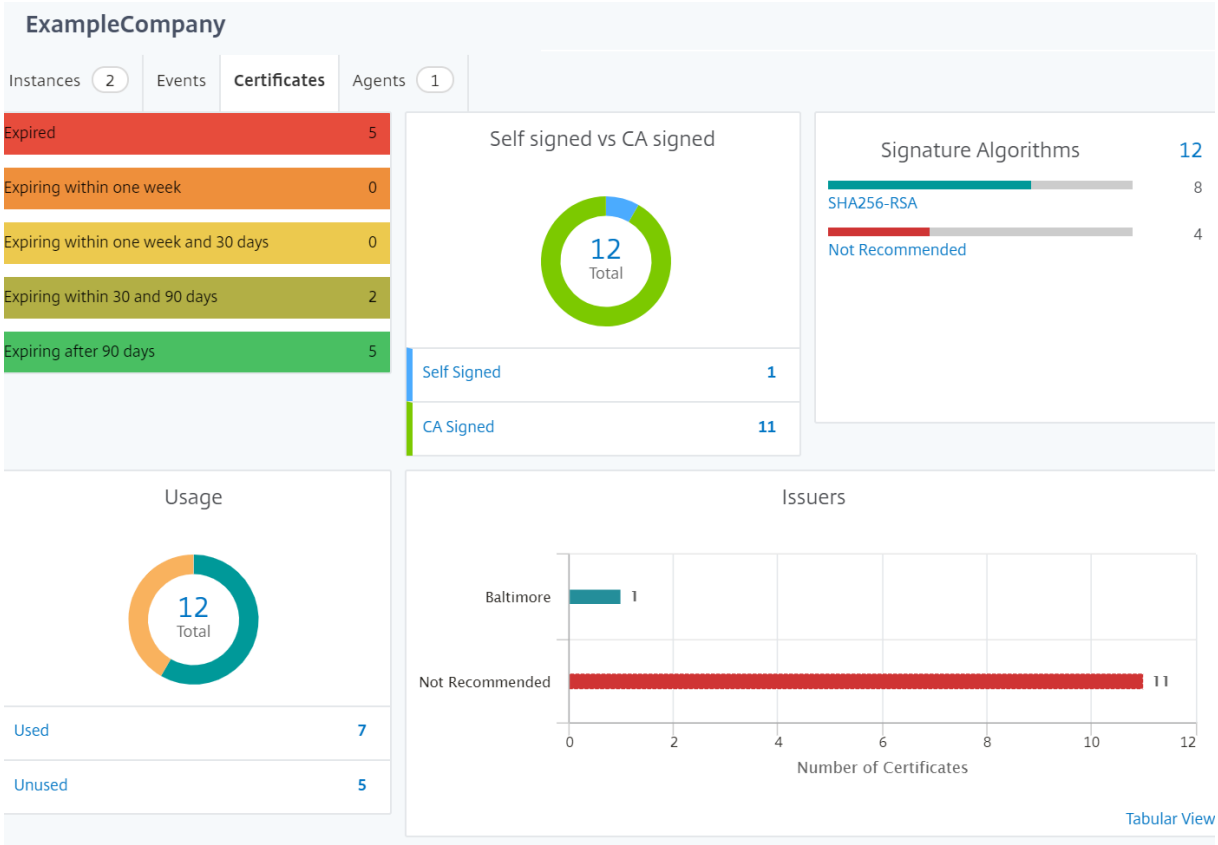


[アプリケーション] をクリックして、各サイトで作成されたすべてのカスタムアプリケーションを表示します。

[詳細] をクリックして、各サイトに追加された Citrix ADC インスタンスの一覧を表示します。タブをクリックして、詳細情報を表示します。

- [**Instances**] タブ: このタブで次の項目を表示します。
  - 各ネットワークインスタンスの IP アドレス

  - Citrix ADC インスタンスのタイプ
  - クリティカルイベントの数
  - Citrix ADC インスタンスで発生した重要なイベントとすべてのイベント。
- [**Events**] タブ: インスタンスで発生した重要なイベントと重要なイベントのリストを表示します。
- [証明書] タブ: このタブで次の項目を表示します。
  - すべてのインスタンスの証明書のリスト
  - 有効期限のステータス
  - 重要な情報と、使用中の多くの証明書による上位 10 のインスタンス。
- [**Agents**] タブ: インスタンスがバインドされているエージェントのリストを表示します。



ジオマップの設定

例 Company は、インドのバンガロールに 3 番目のサイトを作成することにしました。同社は、重要度の低い社内 IT アプリケーションの一部をバンガロールオフィスにオフロードすることで、クラウドをテストしたいと考えていました。同社は、AWS クラウドコンピューティングサービスを利用することに決めました。

管理者として、まずサイトを作成し、次に Citrix ADC インスタンスを Citrix ADM に追加する必要があります。また、インスタンスをサイトに追加し、エージェントを追加し、エージェントをサイトにバインドする必要があります。Citrix ADM は、Citrix ADC インスタンスとエージェントが属するサイトを認識します。

Citrix ADC インスタンスの追加について詳しくは、インスタンスの追加を参照してください。

サイトを作成するには、次の手順に従います。

Citrix ADM でインスタンスを追加する前にサイトを作成します。位置情報を提供することで、サイトを正確に見つけることができます。

1. Citrix ADM で、［ネットワーク］>［サイト］に移動し、［追加］をクリックします。
2. [サイトの作成] ページで、次の情報を更新し、[作成] をクリックします。
   a) サイトタイプ。[データセンター] を選択します。

   > 注**:**
   >
   > このサイトは、プライマリデータセンターとしても支店としても機能します。適宜選択してください。

   a) タイプ。リストから AWS をクラウドプロバイダーとして選択します。

   > 注**:**
   >
   > [既存の **VPC** をサイトとして使用する] チェックボックスをオンにします。

   b) サイト名。サイトの名前を入力します。
   c) 検索場所。都市の名前を入力します。[位置を取得] をクリックして、サイトに正確に配置します。[都市]、[郵便番号]、[地域]、[国]、[緯度]、および [経度] フィールドは自動的に入力されます。

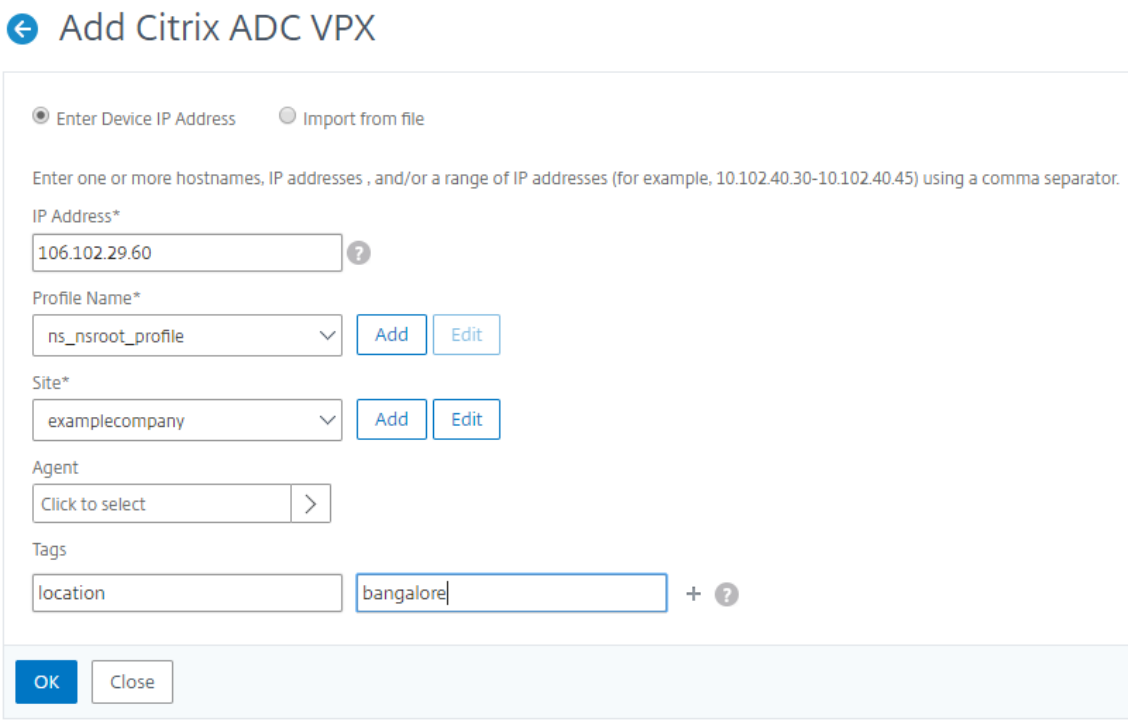
   ![サイトの作成] (/en-us/citrix-application-delivery-management-service/media/nmaservice-global-datacenters-4.png)

   d) バンガロールにサイトを作成するには、**[**作成**]** をクリックします。

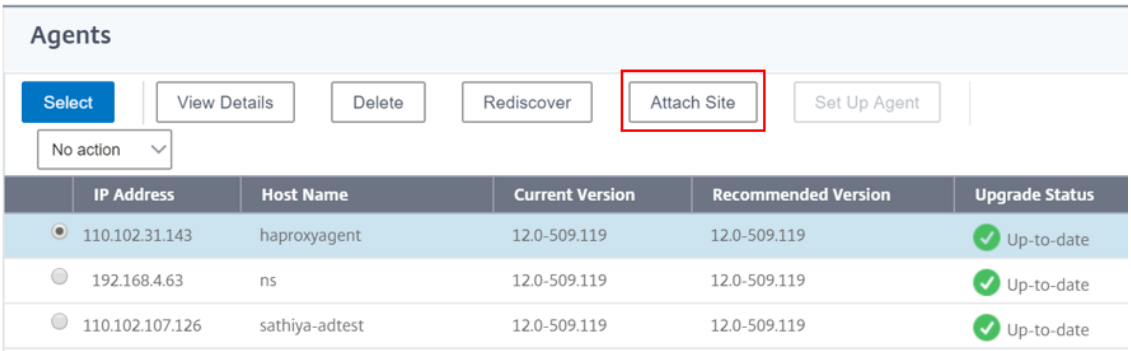
インスタンスを追加してサイトを選択するには**:**

サイトを作成したら、Citrix ADM でインスタンスを追加する必要があります。以前に作成したサイトを選択するか、サイトを作成してインスタンスを関連付けることもできます。

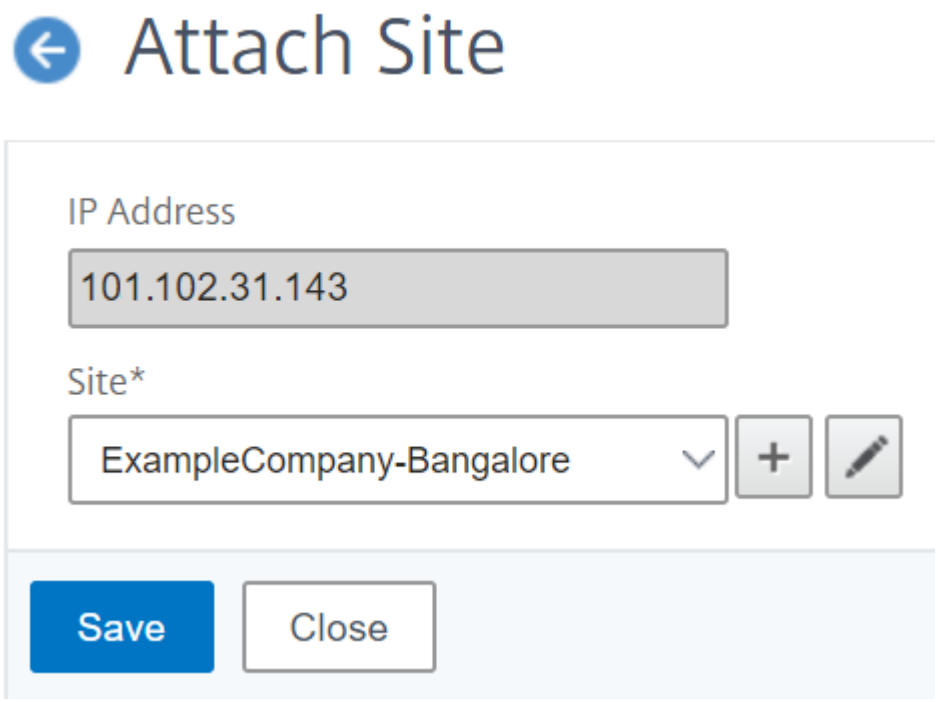
1. Citrix ADM で、［ネットワーク］>［インスタンス］**>**［**Citrix ADC**］に移動します。
2. **VPX** を選択し、［追加］をクリックします。
3. ［**Citrix ADC VPX** の追加］ページで、IP アドレスを入力し、リストからプロファイルを選択します。
4. リストからサイトを選択します。[サイト] フィールドの横にある [追加] ボタンをクリックしてサイトを作成するか、[編集] ボタンをクリックして既定のサイトの詳細を変更できます。
5. 右矢印をクリックし、表示されるリストからエージェントを選択します。



6. エージェントを選択したら、エージェントをサイトに関連付ける必要があります。この手順では、エージェントをサイトにバインドできます。エージェントを選択し、[サイトの接続] をクリックします。



a) リストからサイトを選択し、[保存] をクリックします。



7. オプションで、タグのキーと値フィールドを入力できます。
8. [**OK**] をクリックします。

エージェントをサイトに接続するには、[ネットワーク] > [エージェント] を選択します。

Citrix ADM エージェントをサイトに関連付けるには:

1. Citrix ADM で、[ネットワーク] > [エージェント] に移動します。
2. エージェントを選択し、[サイトの接続] をクリックします。
3. サイトを関連付けて、[保存] をクリックします。

Citrix ADM は、バンガロールサイトに追加された Citrix ADC インスタンスと、他の 2 つのサイトのインスタンスも監視を開始します。

このダッシュボードのレポートをエクスポートするには、次の手順に従います。

このページのレポートをエクスポートするには、このページの右上にある [**Export**] アイコンをクリックします。[エクスポート] ページでは、次のいずれかの操作を実行できます。

1. [今すぐエクスポート] タブを選択します。レポートを PDF、JPEG、PNG、または CSV 形式で表示して保存します。
2. [スケジュールエクスポート] タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、電子メールまたは余裕期間メッセージでレポートを送信するには。

> 注
>
> - [毎週の繰り返し] を選択した場合は、レポートをスケジュールする平日を選択してください。
> - [毎月の繰り返し] を選択した場合は、レポートをスケジュールするすべての日をカンマで区切って入力します。

タグを作成してインスタンスに割り当てる方法

May 7, 2021

Citrix Application Delivery Management（ADM）では、Citrix ADC インスタンスをタグに関連付けることができるようになりました。タグは、インスタンスに割り当てることができるキーワードまたは単語のことです。タグは、インスタンスに関するいくつかの追加情報を追加します。タグは、インスタンスを記述するのに役立つメタデータと考えることができます。タグを使用すると、これらの特定のキーワードに基づいてインスタンスを分類および検索できます。1 つのインスタンスに複数のタグを割り当てることもできます。

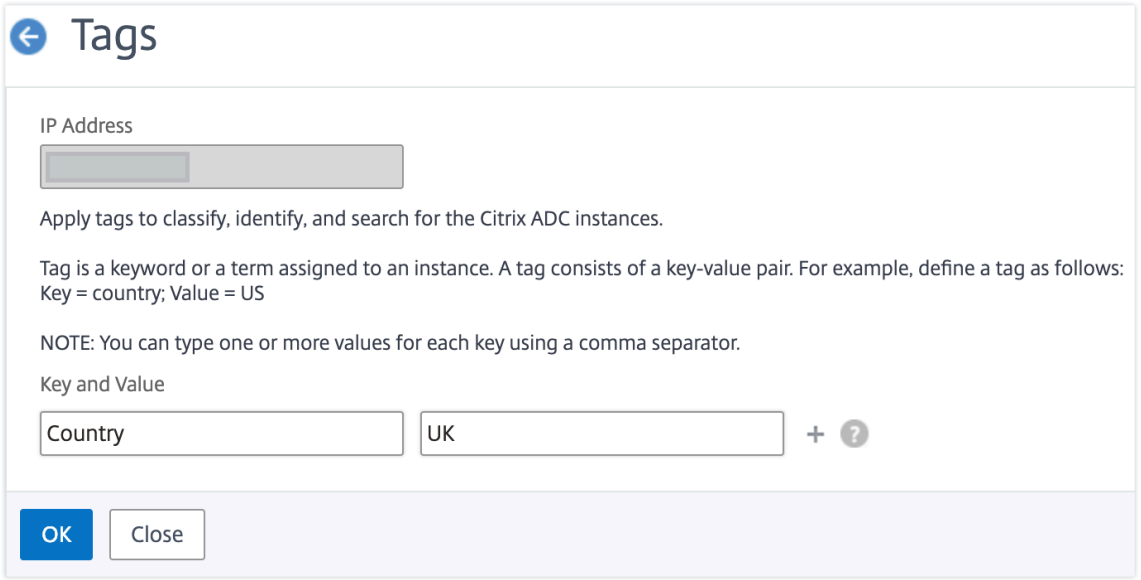
以下のユースケースは、インスタンスのタグ付けがインスタンスのモニタリングにどのように役立つかを理解するのに役立ちます。

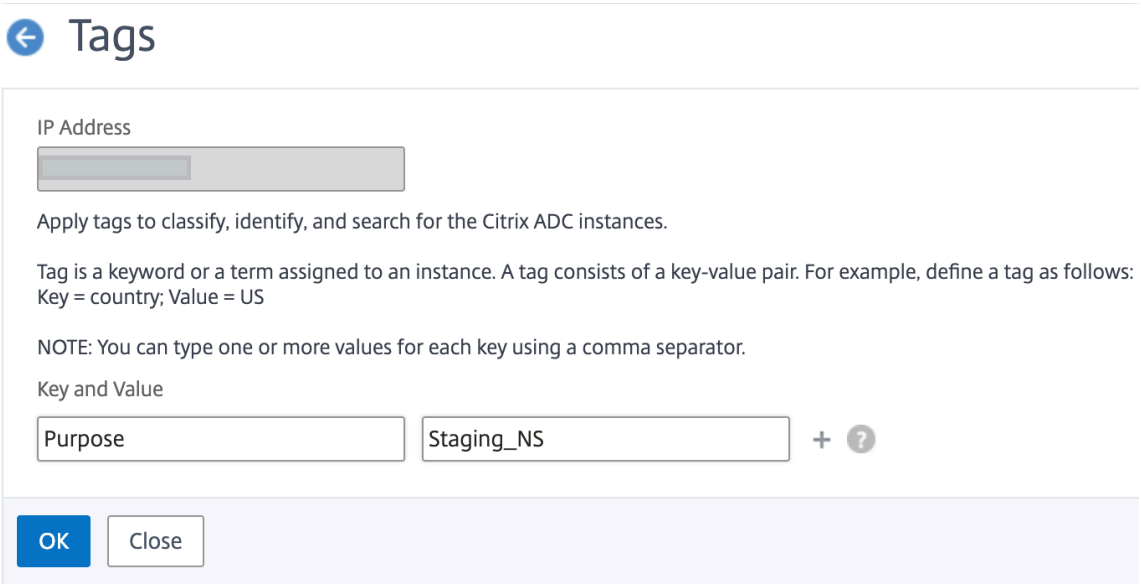
- ユースケース **1**: タグを作成して、英国にあるすべてのインスタンスを識別できます。ここでは、キーを「国」、値を「UK」としてタグを作成することができます。このタグは、英国にあるすべてのインスタンスを検索および監視するのに役立ちます。
- ユースケース **2**: ステージング環境にあるインスタンスを検索する場合。ここでは、キーを「目的」、値を「staging_NS」としてタグを作成できます。このタグは、ステージング環境で使用されているすべてのインスタンスを、クライアント要求が実行されているインスタンスから分離するのに役立ちます。
- ユースケース **3**: 英国の Swindon エリアにあり、David T（David T）が所有する Citrix ADC インスタンスのリストを調べる状況を考えてみましょう。これらすべての要件に対応するタグを作成し、これらの条件を満たすすべてのインスタンスに割り当てることができます。

Citrix ADC VPX インスタンスにタグを割り当てるには:

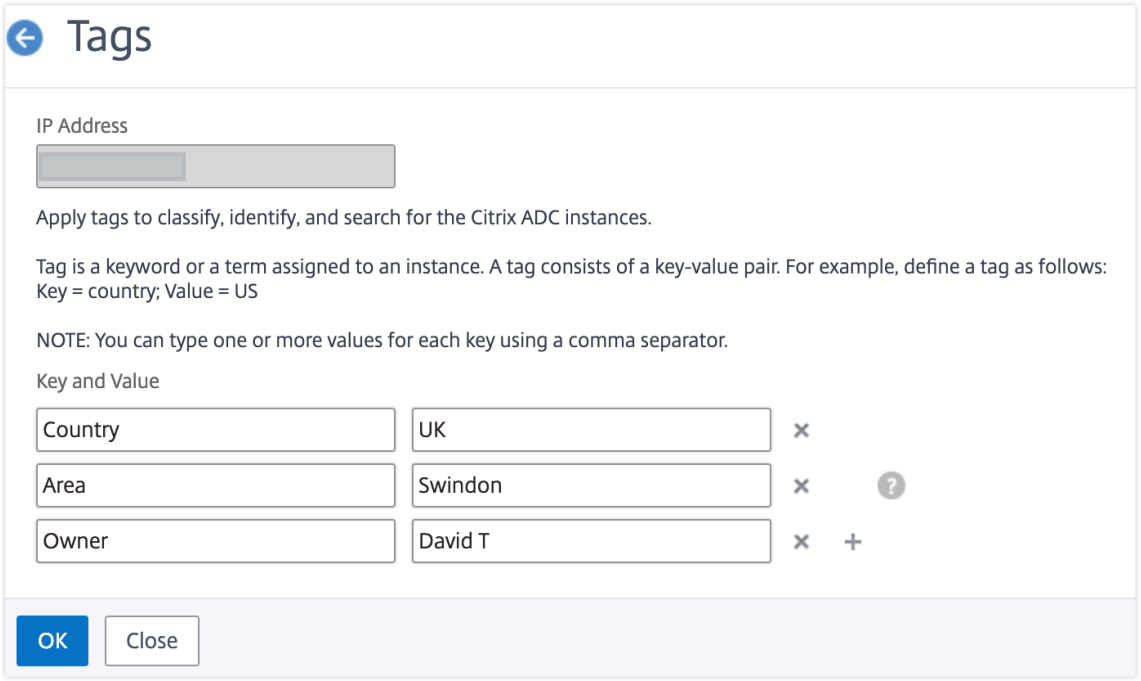
1. Citrix ADM で、［ネットワーク］>［インスタンス］**>**［**Citrix ADC**］に移動します。
2. [**VPX**] タブを選択します。
3. 必要な VPX インスタンスを選択します。
4. [タグ] をクリックします。表示される [タグ] ウィンドウでは、作成したすべてのキーワードに値を割り当てることによって、独自の「キーと値」のペアを作成できます。

   たとえば、次の画像は、作成されたいくつかのキーワードとその値を示しています。独自のキーワードを追加し、各キーワードに値を入力できます。



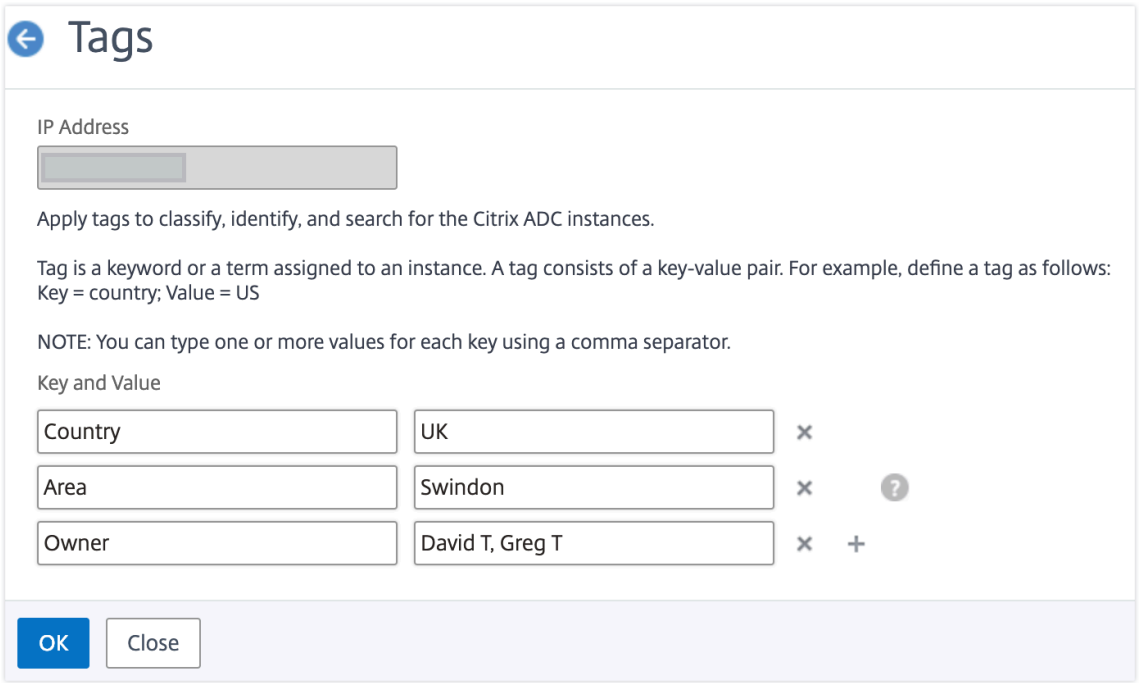


「+」をクリックして複数のタグを追加することもできます。複数の意味のあるタグを追加すると、インスタンスを効率的に検索できます。



キーワードに複数の値を追加するには、カンマで区切ります。

たとえば、別の同僚である Greg T に管理者ロールを割り当てているとします。この名前は、カンマで区切って追加できます。複数の名前を追加すると、いずれかの名前または両方の名前で検索できます。Citrix ADM は、カンマで区切られた値を 2 つの異なる値に認識します。



タグに基づいてインスタンスを検索する方法の詳細については、「タグとプロパティの値を使用してインスタンスを検索する方法」を参照してください。

5. [**OK**] をクリックします。

> 注:
>
> 後で新しいタグを追加したり、既存のタグを削除したりできます。作成するタグの数に制限はありません。

タグとプロパティの値を使用してインスタンスを検索する方法

May 7, 2021

Citrix Application Delivery Management（ADM）が多くの Citrix ADC インスタンスを管理している場合があります。管理者は、特定のパラメータに基づいてインスタンスインベントリを検索できる柔軟性が必要な場合があります。Citrix ADM では、検索フィールドで定義したパラメーターに基づいて、Citrix ADC インスタンスのサブセットを検索する機能が強化されました。タグとプロパティの 2 つの基準に基づいてインスタンスを検索できます。

- タグ。タグとは、Citrix ADC インスタンスに関する追加の説明を追加するために、ユーザーが Citrix ADC インスタンスに割り当てることができる用語またはキーワードです。これで、Citrix ADC インスタンスをタグに関連付けることができます。これらのタグは、Citrix ADC インスタンスの識別と検索をより良くするために使用できます。
- **[** プロパティ**]**: Citrix ADM で追加された各 Citrix ADC インスタンスには、そのインスタンスに関連付けられたデフォルトのパラメータまたはプロパティがいくつかあります。たとえば、各インスタンスには独自のホスト名、IP アドレス、バージョン、ホスト ID、ハードウェアモデル ID などがあります。これらのプロパティの値を指定して、インスタンスを検索できます。

たとえば、バージョン 12.0 で UP 状態の Citrix ADC インスタンスのリストを調べたい場合を考えてみましょう。ここでは、インスタンスのバージョンと状態は、デフォルトのプロパティによって定義されます。

インスタンスの 12.0 バージョンおよび UP 状態に加えて、所有しているインスタンスを検索することもできます。「所有者」タグを作成し、そのタグに値「David T」を割り当てることができます。タグの作成と割り当て方法の詳細については、「タグを作成してインスタンスに割り当てる方法」を参照してください。

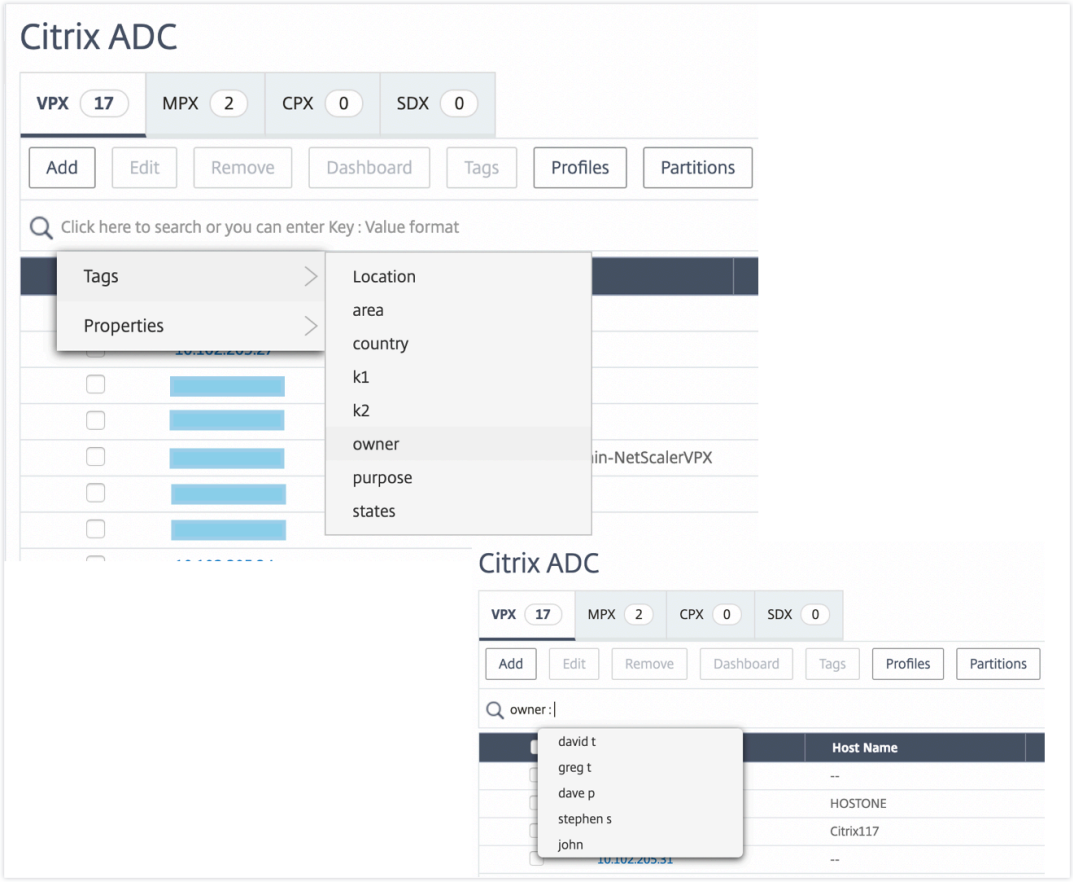
タグとプロパティの組み合わせを使用して、独自の検索条件を作成できます。

Citrix ADC VPX インスタンスを検索するには

1. Citrix ADM で、[ネットワーク] > [インスタンス] **>** [**Citrix ADC**] に移動します。
2. [**VPX**] タブを選択します。
3. 検索フィールドをクリックします。検索式は、タグまたはプロパティを使用するか、両方を組み合わせて作成できます。

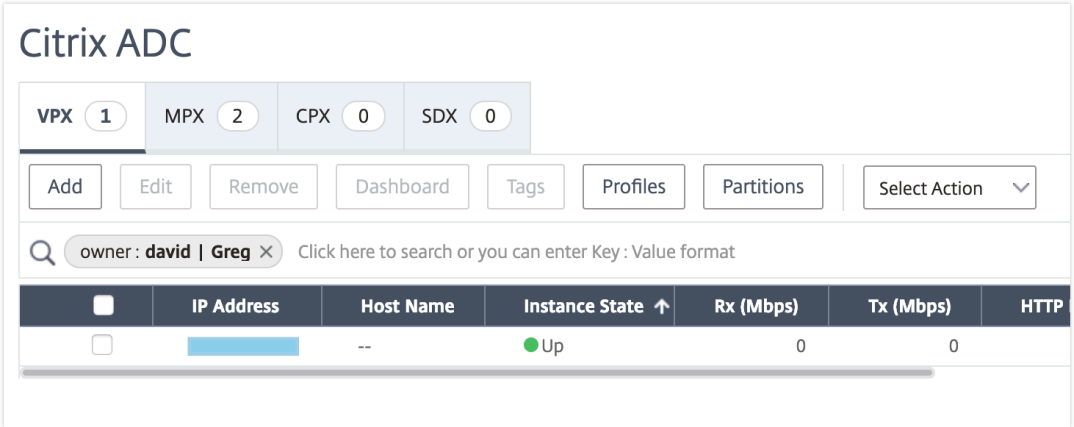
   次の例は、検索式を効率的に使用してインスタンスを検索する方法を示しています。

a) [タグ] オプションを選択し、[所有者] を選択します。「デビッド T」を選択します。

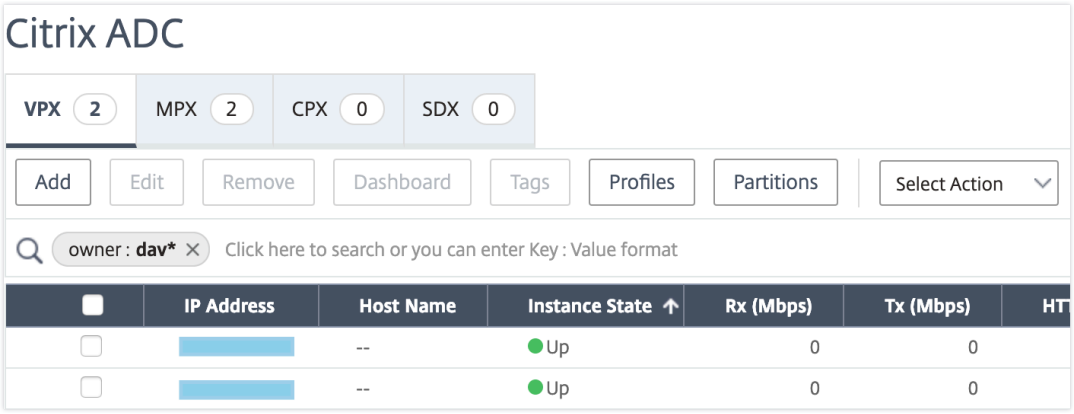


Citrix ADM では、検索式で正規表現とワイルドカード文字がサポートされています。

a) 正規表現を使用して、検索条件をさらに拡張できます。たとえば、David または Stephen が所有するインスタンスを検索したいとします。このような場合は、値を「|」式で区切って値を入力できます。



b) ワイルドカード文字を使用して、1 つ以上の文字を置換または表すこともできます。たとえば、Dav* と入力すると、「David」と「Dave P」が所有するすべてのインスタンスを検索できます。



> 注:
>
> 正規表現とワイルドカード文字とその使用方法について詳しくは、検索バーの「情報」アイコンをクリックします。

Citrix ADC インスタンスの管理パーティションの管理

May 7, 2021

Citrix ADC（Citrix ADC）インスタンスで管理者パーティションを構成して、組織内の異なるグループに同じ Citrix ADC インスタンス上の異なるパーティションを割り当てることができます。ネットワーク管理者を割り当てて、複数の Citrix ADC インスタンス上の複数のパーティションを管理できます。

Citrix Application Delivery Management ADM（Citrix ADM）では、管理者が所有するすべてのパーティションを単一のコンソールからシームレスに管理できます。これらのパーティションは、他のパーティション構成を中断することなく管理できます。

複数のユーザーが異なる管理パーティションを管理できるようにするには、グループを作成し、それらのグループにユーザーとパーティションを割り当てる必要があります。グループまたはユーザーの作成の詳細については、ユーザーの作成およびグループの作成を参照してください。

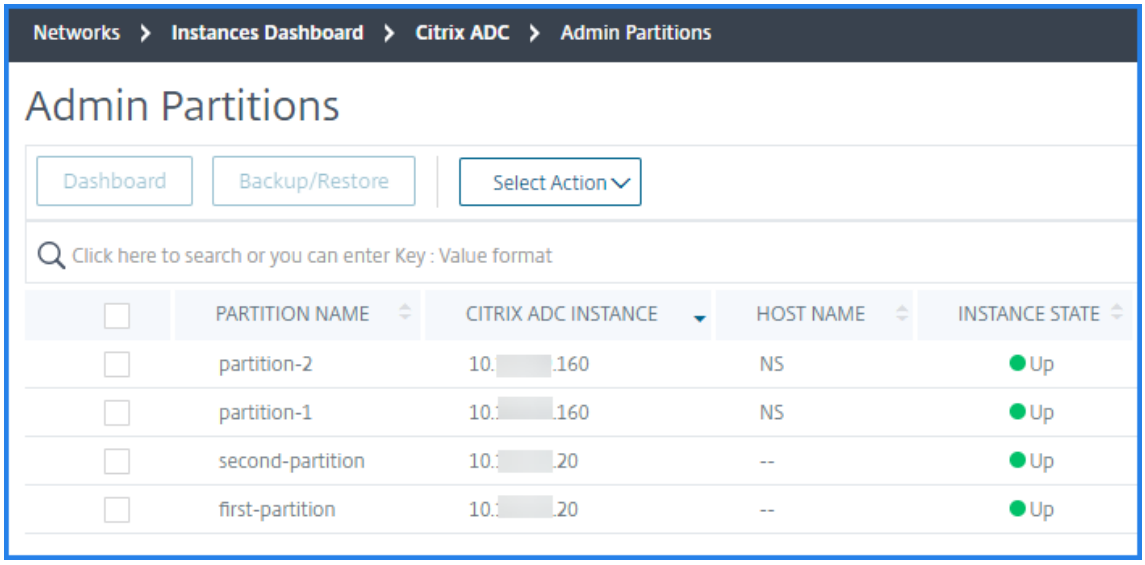
ユーザーは、そのユーザーが属するグループ内のパーティションのみを表示および管理できます。Citrix ADC インスタンスを検出すると、その Citrix ADC インスタンスに構成されている管理パーティションが自動的にシステムに追加されます。各管理パーティションは、Citrix ADM ではインスタンスと見なされます。

管理パーティションの表示

Citrix ADC VPX インスタンスが 2 つあり、各インスタンスには 2 つの管理パーティションが構成されているとします。たとえば、Citrix ADC インスタンス 10.xx.xx.160 にはパーティション 1 とパーティション 2 があり、10.xx.xx.20 インスタンスには最初のパーティションと 2 番目のパーティションがあります。

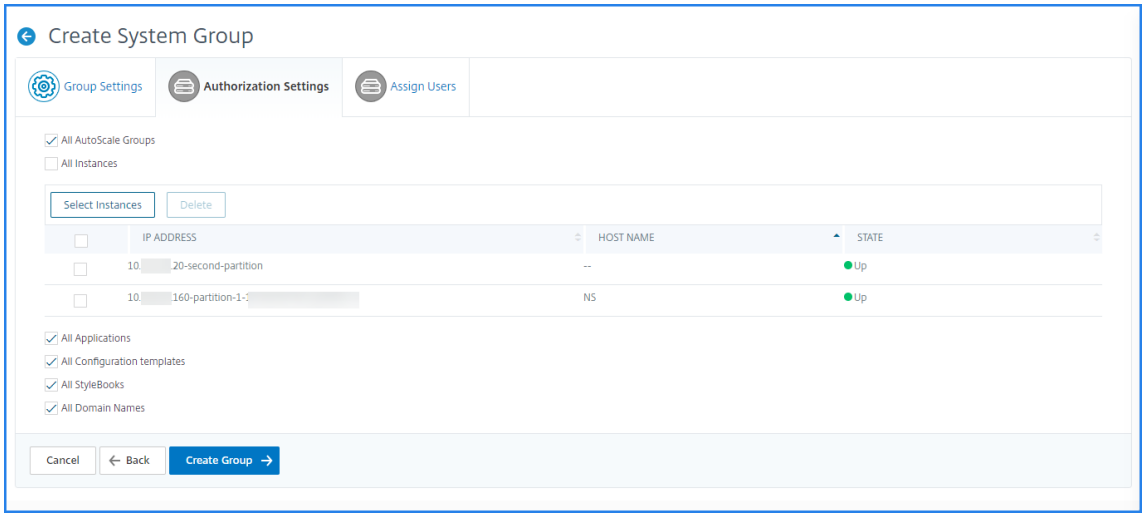
管理パーティションを表示するには、次の手順を実行します。

1. [ネットワーク] > [インスタンス] > [**Citrix ADC**] に移動します。
2. [**VPX**] タブで、[パーティション] をクリックします。

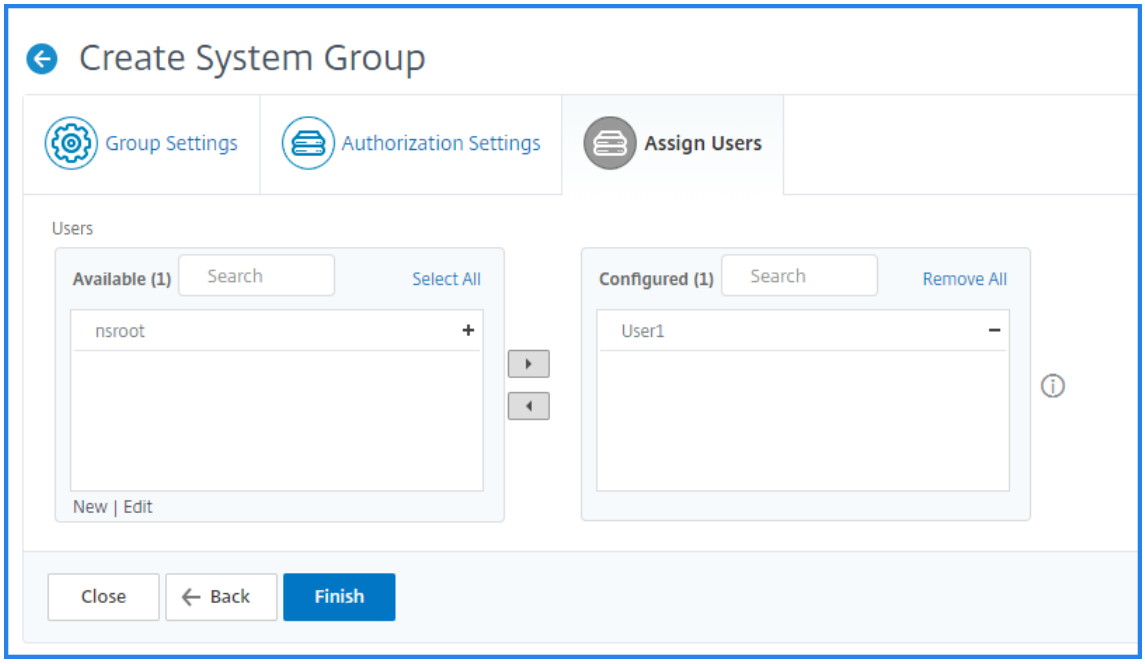


たとえば、次の条件でグループを作成するとします。

- [承認設定] タブで、「10.xx.xx.20-sond パーティション」および「10.xx.xx.160-partition-1」インスタンスが選択されます。



- 「User1」がグループに割り当てられます。



User1 は、グループに追加されたパーティションのみを表示および管理できます。ただし、グループに追加されないパーティションは、同じインスタンスに属しているにもかかわらず、ユーザーに制限されます。

この例では、10.xx.xx.20-最初のパーティションと 10.xx.xx.160-partition-2 が制限されています。インスタンスは、ユーザーが割り当てられているグループに追加されないためです。

管理者パーティション 10.xx.xx.20-first パーティションおよび 10.xx.xx.160-partition-2 を別のユーザで管理する場合は、次の条件でグループを作成します。

- [認証設定] タブで、10.xx.xx.20 の最初のパーティションと 10.xx.xx.160-パーティション 2 インスタンスを選択します。
- 必要なユーザーをグループに割り当てます。

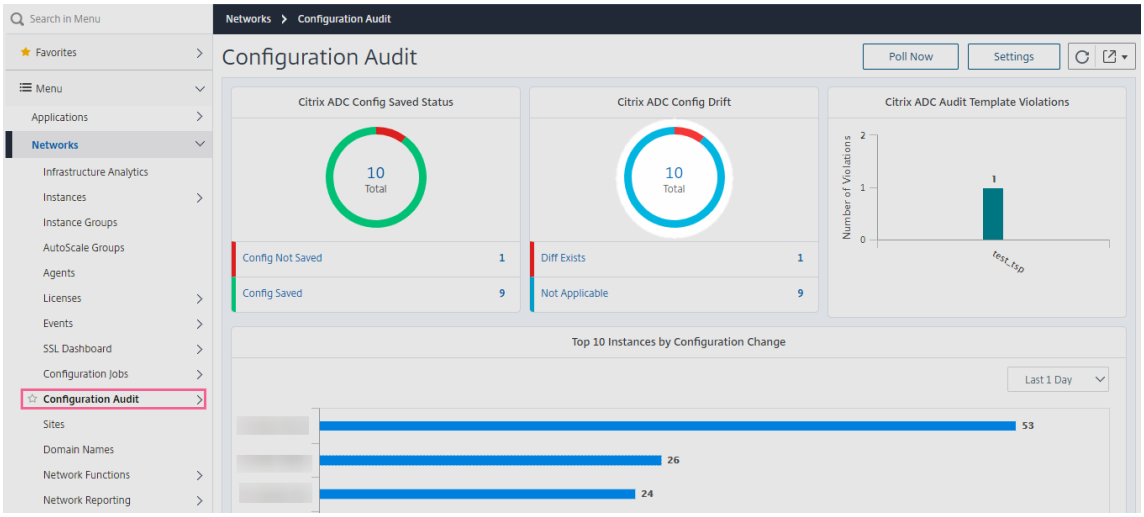
このグループにより、割り当てられたユーザーは、選択した管理パーティションを表示および管理できます。

リビジョン履歴の違いを表示する

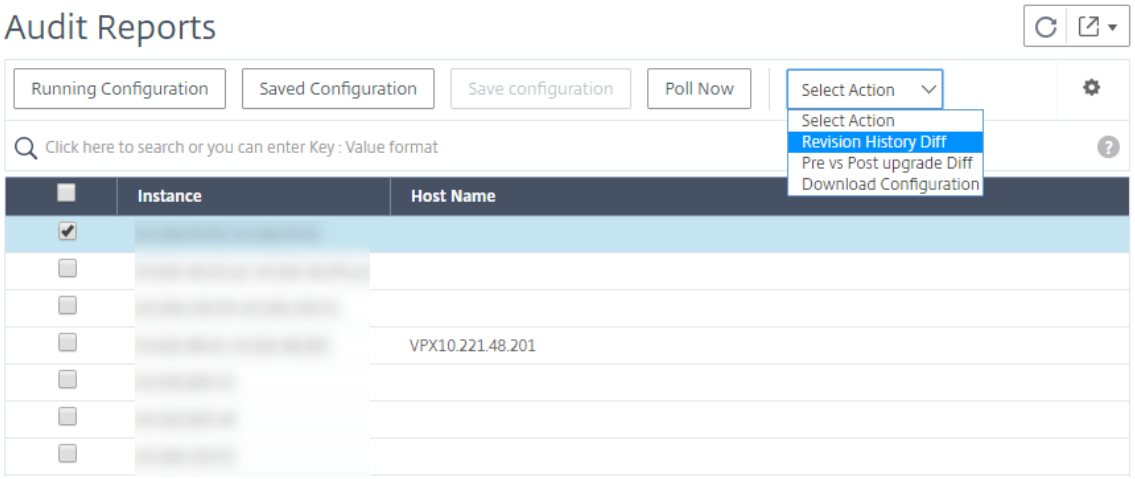
管理パーティションのリビジョン履歴の違いにより、パーティション化された Citrix ADC インスタンスの 5 つの最新の構成ファイルの違いを確認できます。構成ファイルを相互に（構成リビジョン 1 と構成リビジョン-2 の例）、または Configuration Revision を使用して現在実行または保存された構成と比較できます。構成の違いとともに、修正構成も示されています。すべての修正コマンドをローカルフォルダにエクスポートし、設定を修正できます。

改訂履歴の差異を表示する手順は、次のとおりです。

1. [ネットワーク**] > [**構成監査] に移動します。構成監査ダッシュボードには、さまざまなレポートが表示されます。ドーナツグラフの中央に表示されている数字をクリックします。

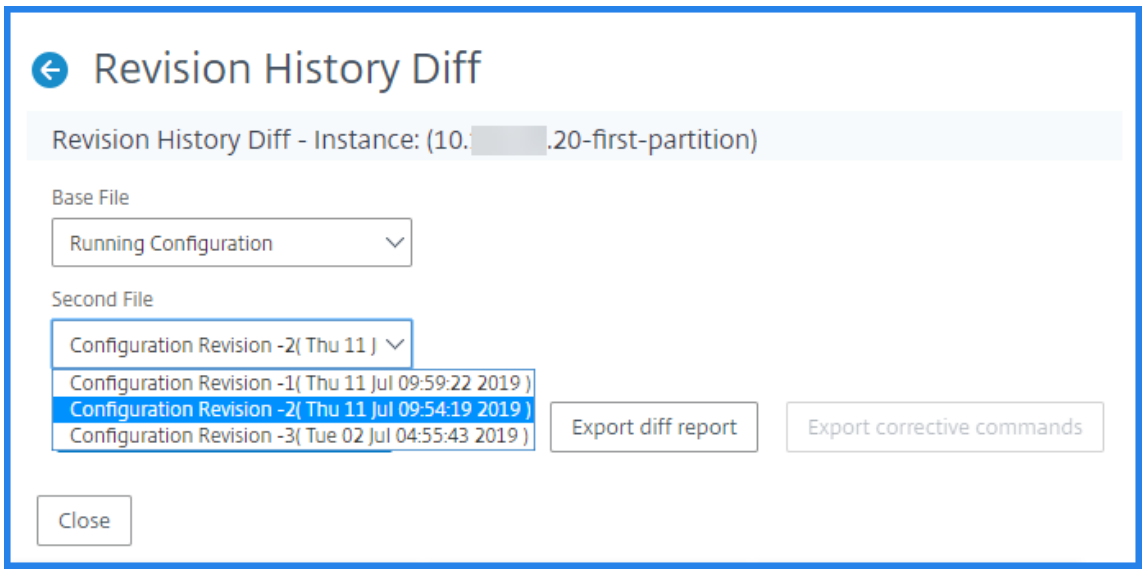


2. パーティション分割された Citrix ADC インスタンスを選択します。
3. [アクション] ボックスで、[リビジョン履歴の相違] をクリックします。

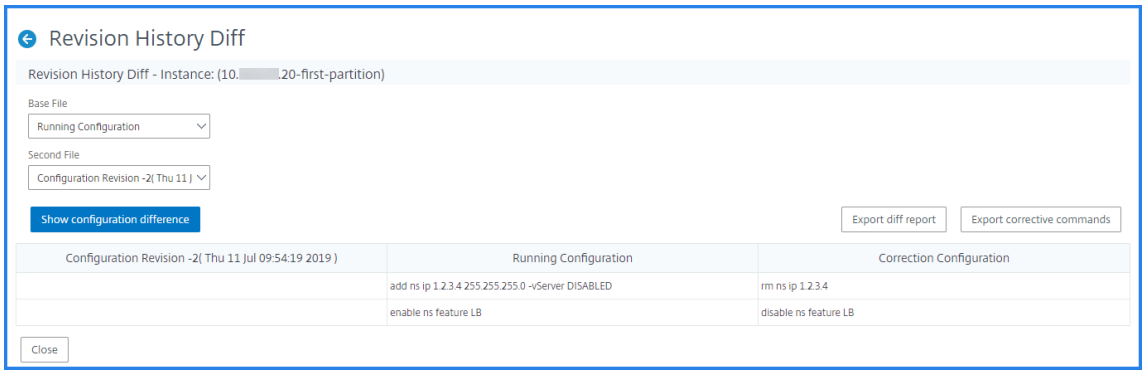


4. [リビジョン履歴の差分] ページで、比較するファイルを選択します。たとえば、保存された構成と構成 Revision-2 を比較し、[構成の違いを表示] をクリックします。

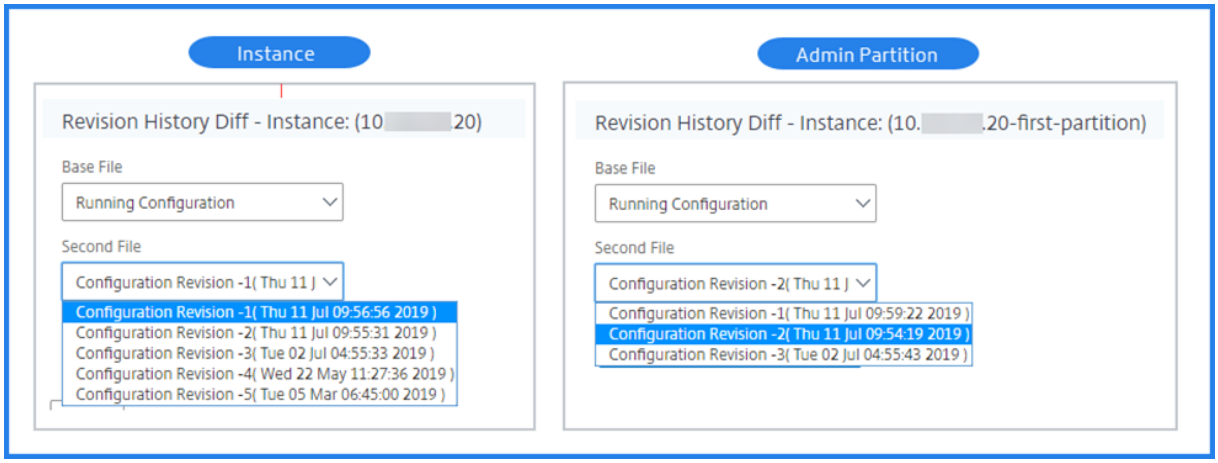
   次に、選択したパーティション化された Citrix ADC インスタンスの 5 つの最新の構成ファイルの違いを確認できます。次に、3 つの設定が保存されている admin パーティションの例を示します。



修正構成コマンドを表示し、これらの修正コマンドをローカルフォルダにエクスポートすることもできます。これらの修正コマンドは、構成を目的の状態（比較に使用される構成ファイル）にするために、ベースファイルで実行する必要があるコマンドです。



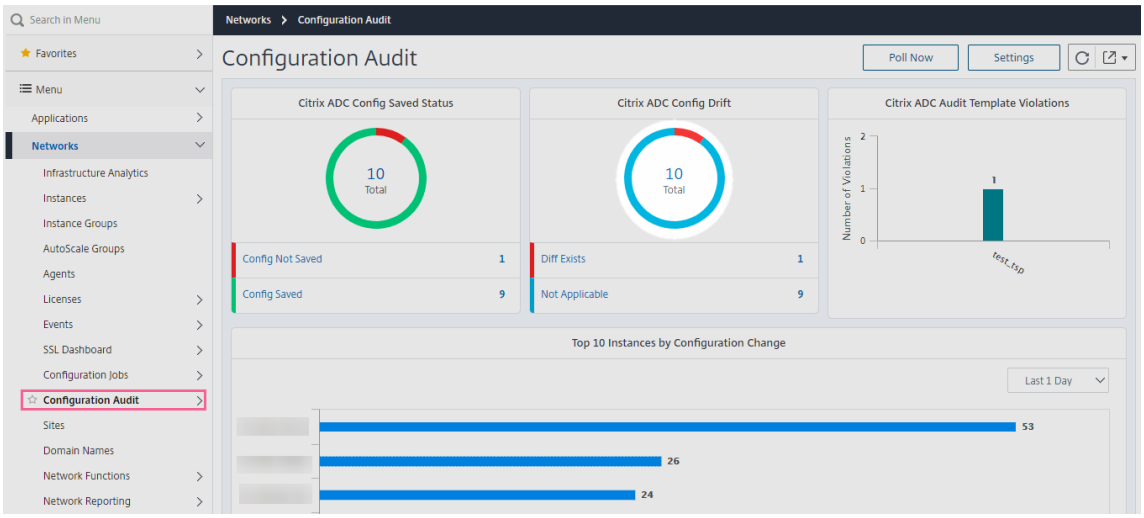
管理パーティションとインスタンスに保存された設定は異なります。次の例では、10.xx.xx.20 インスタンスに 5 つの保存済み設定があり、このインスタンスの管理パーティションには 3 つの異なる保存済み設定があります。



テンプレートと実行の違いを表示する

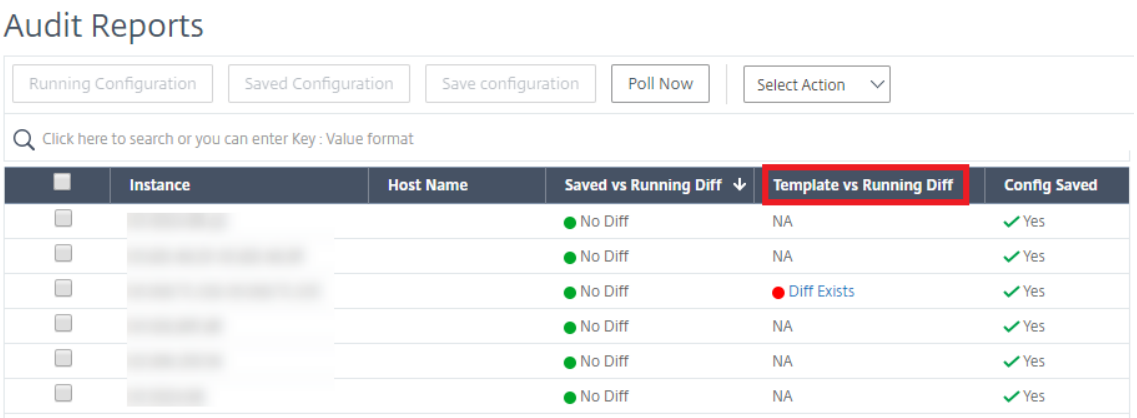
パーティションの監査テンプレートを使用すると、カスタム構成テンプレートを作成し、それをパーティションインスタンスに関連付けることができます。監査テンプレートを使用したインスタンスの実行構成のバリエーションは、[監査レポート] ページの [テンプレートと実行時の差分] 列に表示されます。構成の違いとともに、修正構成も示されています。また、すべての修正コマンドをローカルフォルダにエクスポートして、設定を修正することもできます。

1. [ネットワーク**] > [**構成監査] に移動します。構成監査ダッシュボードには、さまざまなレポートが表示されます。ドーナツグラフの中央に表示されている数字をクリックします。



2. 「監査レポート」ページで、「テンプレートと実行中の差分」列の下にある「相違が存在する」ハイパーリンクをクリックします。

   監査テンプレートと実行構成に違いがある場合、その違いはハイパーリンクとして表示されます。ハイパーリンクをクリックすると、相違点が表示されます（存在する場合）。構成の違いとともに、修正構成も示されています。また、すべての修正コマンドをローカルフォルダにエクスポートして、設定を修正することもできます。



このダッシュボードのレポートをエクスポートするには、次の手順に従います。

このページのレポートをエクスポートするには、このページの右上にある エクスポートアイコンをクリックします。[エクスポート] ページでは、次のいずれかの操作を実行できます。

1. [今すぐエクスポート] タブを選択します。レポートを PDF、JPEG、PNG、または CSV 形式で表示して保存します。
2. [スケジュールエクスポート] タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、電子メールまたは余裕期間メッセージでレポートを送信するには。

> 注
>
> - [毎週の繰り返し] を選択した場合は、レポートをスケジュールする平日を選択してください。
> - [毎月の繰り返し] を選択した場合は、レポートをスケジュールするすべての日をカンマで区切って入力します。

Citrix ADC インスタンスのバックアップと復元

May 7, 2021

Citrix ADC（Citrix ADC）インスタンスの現在の状態をバックアップし、後でバックアップしたファイルを使用して、Citrix ADC インスタンスを同じ状態に復元できます。インスタンスをアップグレードする前に、または予防的な理由により、常にインスタンスをバックアップする必要があります。安定したシステムのバックアップを使用すると、不安定になった場合に、安定した状態に復元できます。Citrix ADC インスタンスでバックアップおよびリストアを実行する方法は複数あります。GUI、CLI を使用して Citrix ADC 構成を手動でバックアップおよび復元できます。または、Citrix Application Delivery Management（Citrix ADM）を使用して自動バックアップと手動リストアを実行できます。Citrix ADM は、NITRO コールとセキュアシェル（SSH）プロトコルとセキュアコピー（SCP）プロトコルを使用して、管理対象 Citrix ADC インスタンスの現在の状態をバックアップします。

Citrix ADM は完全なバックアップを作成し、次の Citrix ADC インスタンスタイプを復元します。

- Citrix ADC SDX
- Citrix ADC VPX
- Citrix ADC MPX
- Citrix ADC BLX

詳しくは、「[ADC インスタンスのバックアップと復元]」を参照してください。(https://docs.citrix.com/en-us/citrix-adc/13/system/basic-operations/backup-restore-citrix-adc-appliance.html)

> 注
>
> - Citrix ADM では、Citrix ADC クラスターでバックアップと復元操作を実行できません。
> - あるインスタンスから取られたバックアップファイルを、異なるインスタンスを復元するために使用することはできません。

バックアップファイルは、圧縮された TAR ファイルとして次のディレクトリに保存されます。


```
/var/mps/tenants/root/tenants/<specify-the-tenant-name>/device_backup/

<!--NeedCopy-->
```

ディスク領域が使用できないことによる問題を回避するために、このディレクトリには最大 50 個のバックアップファイルを保存できます。

Citrix ADC インスタンスをバックアップおよび復元するには、まず Citrix ADM でバックアップ設定を構成する必要があります。設定を構成したら、単一の Citrix ADC インスタンスまたは複数のインスタンスを選択し、これらのインスタンスで構成ファイルのバックアップを作成できます。必要に応じて、これらのバックアップファイルを使用して Citrix ADC インスタンスを復元することもできます。

Citrix ADCitrix ADM を使用して、選択した **Citrix ADC** インスタンスのバックアップを作成する

選択した Citrix ADC インスタンスまたは複数のインスタンスをバックアップする場合は、次のタスクを実行します。

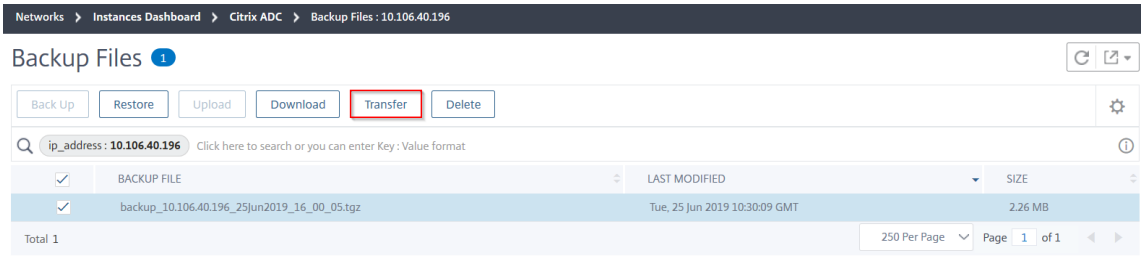
1. Citrix ADM で、[ネットワーク] > [インスタンス] に移動します。[インスタンス] で、画面に表示するインスタンスのタイプ（VPX など）を選択します。
2. バックアップするインスタンスを選択します。
   - MPX、VPX、BLX インスタンスの場合は、［アクションの選択］リストから［バックアップ/復元］を選択します。
   - SDX インスタンスの場合は、[バックアップ**/**復元] をクリックします。
3. ［**Backup Files**］ページで［**Back Up**］をクリックします。
4. セキュリティを強化するために、バックアップファイルを暗号化するかどうかを指定します。パスワードを入力するか、[Instance Backup Settings] ページで以前に指定したグローバルパスワードを使用できます。
5. ［続行］をクリックします。

バックアップファイルを外部システムに転送する

予防措置として、バックアップファイルのコピーを別のシステムに転送できます。構成を復元する場合は、まずバックアップファイルを Citrix ADM サーバーにアップロードしてから、復元操作を実行する必要があります。

Citrix ADM バックアップファイルを転送するには：

1. [ネットワーク] > [インスタンス] > [**Citrix ADC**] に移動し、インスタンスタイプを選択します。たとえば、VPX です。
2. インスタンスを選択し、**[**アクションの選択**]** リストから [バックアップ**/**復元] を選択します。
3. バックアップファイルを選択し、[転送] をクリックします。



[バックアップファイルの転送] ページが表示されます。次のパラメータを指定します。

a) サーバ：バックアップファイルを転送するシステムの IP アドレス。

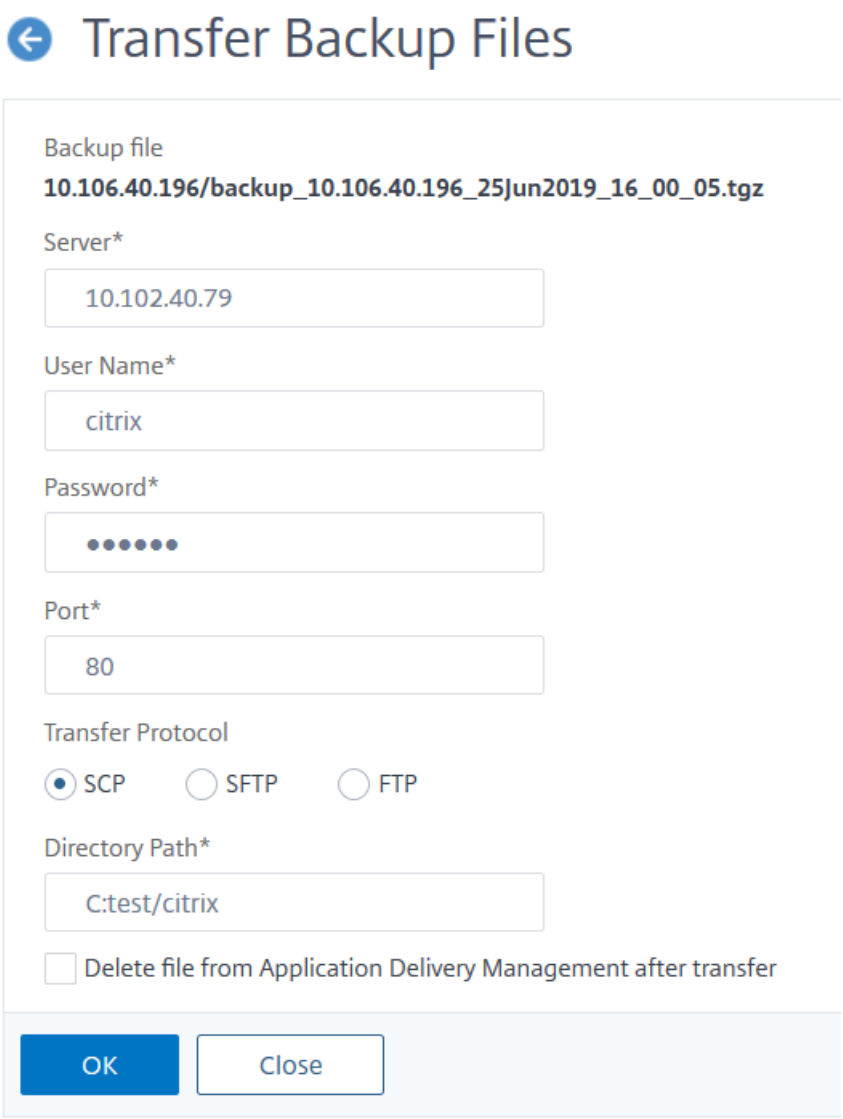
b) **[User name** and **password]**：バックアップされたファイルがコピーされる新しいシステムのユーザー資格情報。

c) **Port**： ファイルの転送先となるシステムのポート番号。

d) 転送プロトコル：バックアップファイルの転送に使用されるプロトコル。バックアップファイルを転送するには、SCP、SFTP、または FTP プロトコルを選択できます。

e) ディレクトリパス：バックアップファイルが新しいシステム上で転送される場所。

f) [**OK**] をクリックします。



Citrix ADM を使用して **Citrix ADC** インスタンスを復元する

> 注：高可用性ペアに Citrix ADC インスタンス
>
> がある場合は、次の点に注意する必要があります。
>
> - バックアップファイルの作成元と同じインスタンスを復元します。たとえば、HA ペアのプライマリ・インスタンスからバックアップが作成されたシナリオを考えてみましょう。リストア・プロセス中に、プライマリ・インスタンスでなくなった場合でも、同じインスタンスをリストアしていることを確認します。
> - プライマリ ADC インスタンスで復元プロセスを開始すると、プライマリインスタンスにアクセスできず、セカンダリインスタンスは **STAY**SECTARY に変更されます。プライマリインスタンスで復元プロセスが完了すると、セカンダリ ADC インスタンスは **STAY** SECTARY モードから ENABE **NA** BD モードに変わり、再び HA ペアの一部になります。リストア・プロセスが完了するまで、プライマリ・インスタンス

> のダウンタイムが発生する可能性があります。

以前に作成したバックアップファイルを使用して Citrix ADC インスタンスを復元するには、次のタスクを実行します。

1. [ネットワーク] > [インスタンス] に移動し、復元するインスタンスを選択し、[**View Backup**] をクリックします。
2. [バックアップファイル] ページで、復元する設定を含むバックアップファイルを選択し、[復元] をクリックします。

Citrix ADM を使用して **Citrix ADC SDX** アプライアンスを復元する

Citrix ADM では、Citrix ADC SDX アプライアンスのバックアップには次のものが含まれます。

- アプライアンスでホストされている Citrix ADC インスタンス
- SVM SSL 証明書とキー
- Instance の削除設定（XML 形式）
- Instance のバックアップ設定（XML 形式）
- SSL 証明書ポーリング設定（XML 形式）
- SVM データベースファイル
- SDX 上に存在するデバイスの Citrix ADC 構成ファイル
- Citrix ADC ビルドイメージ
- Citrix ADC XVA イメージの場合、これらのイメージは次の場所に保存されます。
  `/var/mps/sdx_images/`
- SDX 単一バンドルイメージ（SVM+XS）
- サードパーティのインスタンスイメージ（プロビジョニングされている場合）

Citrix ADC SDX アプライアンスをバックアップファイルで使用可能な構成に復元する必要があります。アプライアンスの復元中に、現在の構成全体は削除されます。

別の Citrix ADC SDX アプライアンスのバックアップを使用して Citrix ADC SDX アプライアンスをリストアする場合は、復元プロセスを開始する前に、ライセンスを追加し、バックアップファイル内の設定と一致するようにアプライアンスの管理サービスのネットワーク設定を構成してください。

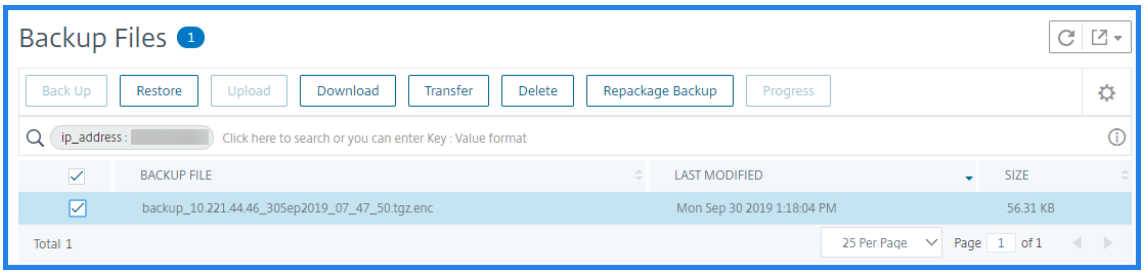
バックアップされた Citrix ADC SDX プラットフォームバリアントが、復元しようとしているものと同じであることを確認します。異なるプラットフォームのバリアントでは復元できません。

> 注:
>
> SDX RMA アプライアンスを復元する前に、バックアップされたバージョンが RMA バージョンと同じかそれ以上であることを確認してください。

バックアップしたファイルから SDX アプライアンスを復元するには:

1. Citrix ADM GUI で、［ネットワーク］**>**［インスタンス］**>**［**Citrix ADC**］に移動します。
2. [バックアップ**/**復元] をクリックします。

3. 復元する同じインスタンスのバックアップファイルを選択します。
4. [バックアップを再パッケージ] をクリックします。



SDX アプライアンスをバックアップすると、XVA ファイルとイメージは別々に保存され、ネットワーク帯域幅とディスク容量が節約されます。したがって、SDX アプライアンスを復元する前に、バックアップファイルを再パッケージ化する必要があります。

バックアップファイルを再パッケージ化すると、SDX アプライアンスを復元するために、すべてのバックアップファイルが一緒に含まれます。再パッケージされたバックアップファイルは、SDX アプライアンスの正常なリストアを保証します。

5. 再パッケージするバックアップファイルを選択し、[**Restore**] をクリックします。

このダッシュボードのレポートをエクスポートする

このページのレポートをエクスポートするには、このページの右上にある エクスポートアイコンをクリックします。[エクスポート] ページでは、次のいずれかの操作を実行できます。

1. [今すぐエクスポート] タブを選択します。レポートを PDF、JPEG、PNG、または CSV 形式で表示して保存します。
2. [スケジュールエクスポート] タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、電子メールまたは余裕期間メッセージでレポートを送信するには。

> 注
>
> - [毎週の繰り返し] を選択した場合は、レポートをスケジュールする平日を選択してください。
> - [毎月の繰り返し] を選択した場合は、レポートをスケジュールするすべての日をカンマで区切って入力します。

セカンダリ **Citrix ADC** インスタンスへのフェイルオーバーを強制する

May 7, 2021

たとえば、プライマリ Citrix Application Delivery Controller（Citrix ADC）インスタンスを交換またはアップグレードする必要がある場合など、フェイルオーバーを強制的に実行できます。プライマリインスタンス、セカンダリ

インスタンスのいずれからでもフェールオーバーを強制できます。プライマリインスタンスでフェールオーバーを強制した場合、プライマリがセカンダリとなり、セカンダリがプライマリとなります。強制フェールオーバーを実行できるのは、セカンダリインスタンスが UP の状態であることをプライマリインスタンスが判別できるときのみです。

強制フェールオーバーは継承されたり、同期されたりしません。強制フェールオーバー後の同期の状態を確認するには、インスタンスの状態を表示してください。

次の状況では、強制フェールオーバーを実行できません。

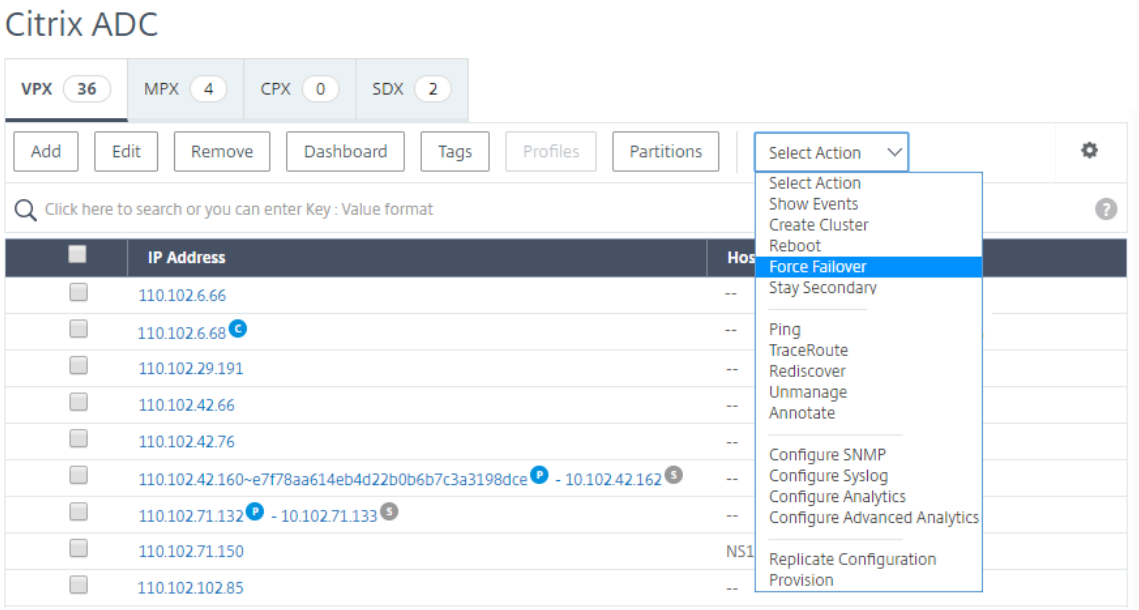
- スタンドアロンシステムにフェールオーバーを強制する。
- セカンダリインスタンスが無効または非アクティブである。セカンダリインスタンスが非アクティブの場合、状態が UP になるまで待ってからフェールオーバーを強制してください。
- セカンダリを維持するようにセカンダリインスタンスが構成されている。

force failover コマンドを実行したときに潜在的な問題が検出されると、Citrix ADC インスタンスで警告メッセージが表示されます。メッセージには警告の要因に関する情報が含まれており、手順を進める前に確認が求められます。

プライマリインスタンスまたはセカンダリインスタンスでフェールオーバーを強制できます。

Citrix ADCCitrix ADM を使用してセカンダリ **Citrix ADC** インスタンスにフェイルオーバーを強制するには:

1. Citrix ADM で、[ネットワーク] > [インスタンス] に移動します。[**VPX**] タブに移動し、インスタンスを選択します。
2. 選択したインスタンスの種類にリストされているインスタンスから、HA セットアップを構成するインスタンスを選択します。
3. [操作] ボックスで、[強制フェイルオーバー] を選択します。
4. [**Yes**] をクリックして強制フェールオーバーアクションを確定します。



セカンダリ **Citrix ADC** インスタンスを強制的にセカンダリとして保持する

May 7, 2021

高可用性 (HA) セットアップでは、プライマリノードの状態に関係なく、セカンダリノードを強制的にセカンダリ状態にすることができます。

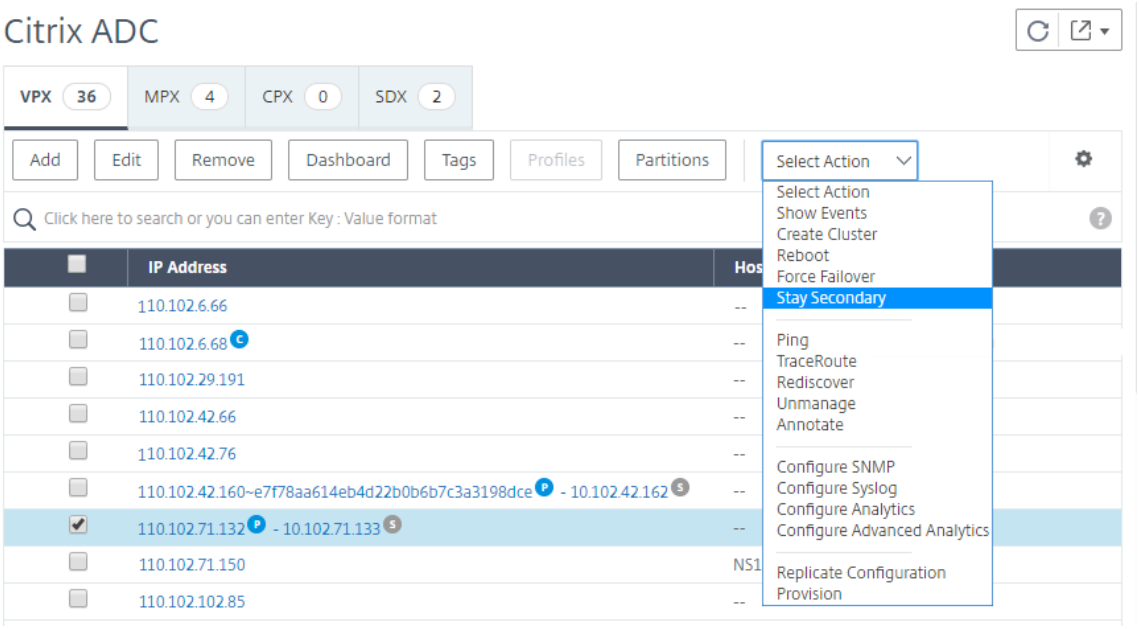
たとえば、プライマリノードをアップグレードする必要があり、アップグレード処理に数秒かかるとします。アップグレード中、プライマリノードが数秒間停止することがありますが、セカンダリノードを引き継ぎたくないため、プライマリノードで障害が検出された場合でも、セカンダリノードのままにします。

セカンダリノードを強制的にセカンダリのままにすると、プライマリノードがダウンしてもセカンダリのままになります。HA ペアの一方のノードのステータスをセカンダリのまま強制的に維持すると、そのノードは、HA 状態マシン遷移には参加しません。ノードのステータスは、STAYSECONDARY として表示されます。

> 注
>
> システムをセカンダリのまま強制的に維持する場合、その強制を実施するプロセスは、伝播も同期もされません。コマンドを実行するノードのみが対象となります。

Citrix ADM を使用してセカンダリ **Citrix ADC** インスタンスをセカンダリとして保持するように構成するには:

1. Citrix ADM で、[ネットワーク] > [インスタンス] の順に選択し、インスタンスタイプ（VPX）でインスタンスを選択します。
2. 選択したインスタンスの種類にリストされているインスタンスから、HA セットアップを構成するインスタンスを選択します。
3. [操作] ボックスで、[セカンダリに維持する] を選択します。
4. [はい] をクリックして、[セカンダリに保存] アクションの実行を確定します。



インスタンスグループの作成

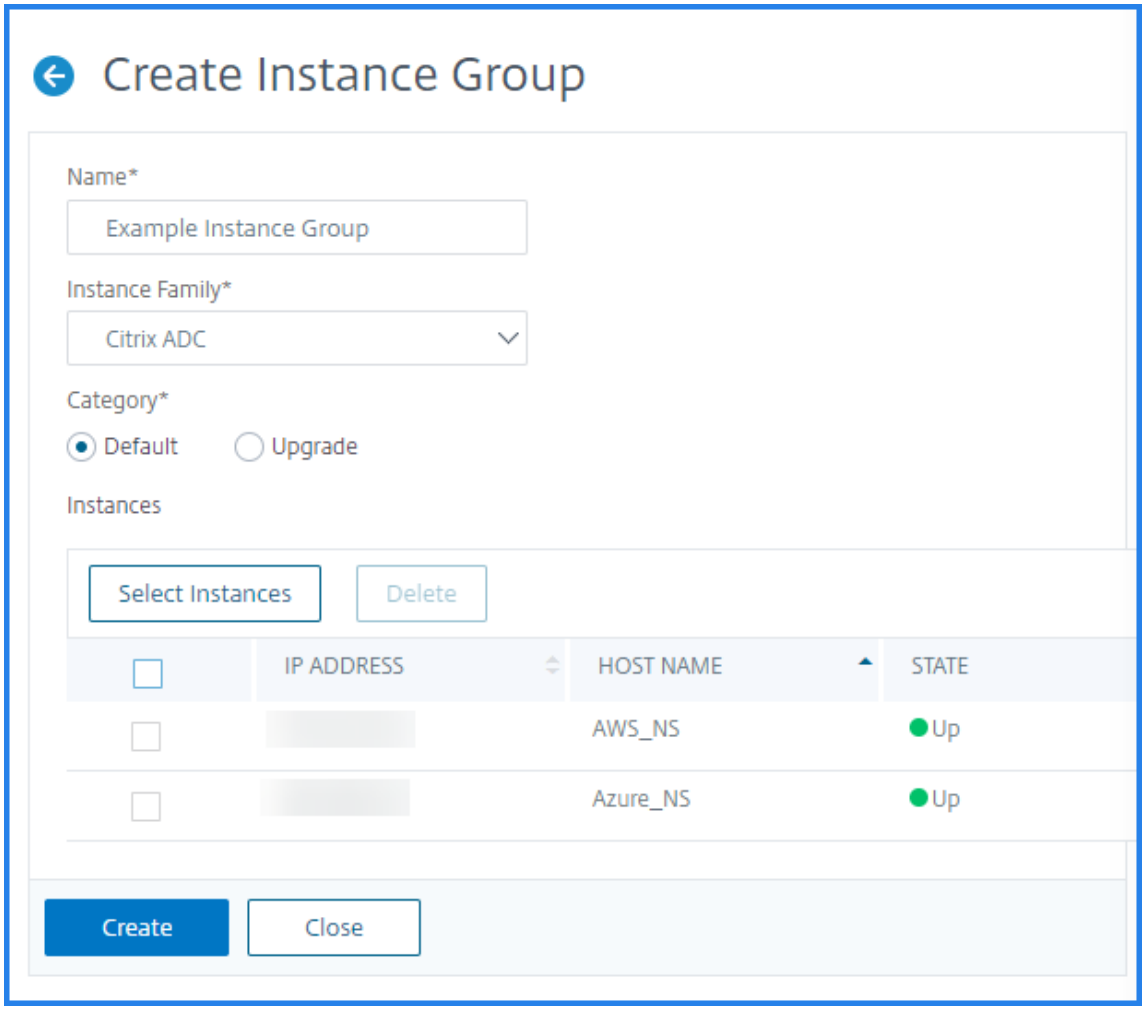
May 7, 2021

インスタンスグループを作成するには、まずすべての Citrix ADC インスタンスを Citrix ADM に追加する必要があります。インスタンスを正常に追加したら、インスタンスファミリーに基づいてインスタンスグループを作成します。インスタンスのグループを作成すると、グループ化されたインスタンスを一度にアップグレード、バックアップ、または復元できます。

Citrix ADM を使用してインスタンスグループを作成するには

1. Citrix ADM で、［ネットワーク］>［インスタンスグループ］の順に選択し、［追加］をクリックします。
2. インスタンスグループの名前を指定し、［インスタンスファミリー］リストから［**Citrix ADC**］を選択します。
3. [カテゴリ] で、[既定] オプションを選択します。
4. [インスタンスを選択**]** をクリックします。[**Select Instances**] ページで、グループ化するインスタンスを選択し、[**Select**] をクリックします。

   テーブルには、選択したインスタンスとその詳細が一覧表示されます。グループからインスタンスを削除する場合は、テーブルからインスタンスを選択し、[**Delete**] をクリックします。
5. ［作成］をクリックします。



ADM を使用して SDX 上の ADC VPX インスタンスのプロビジョニング

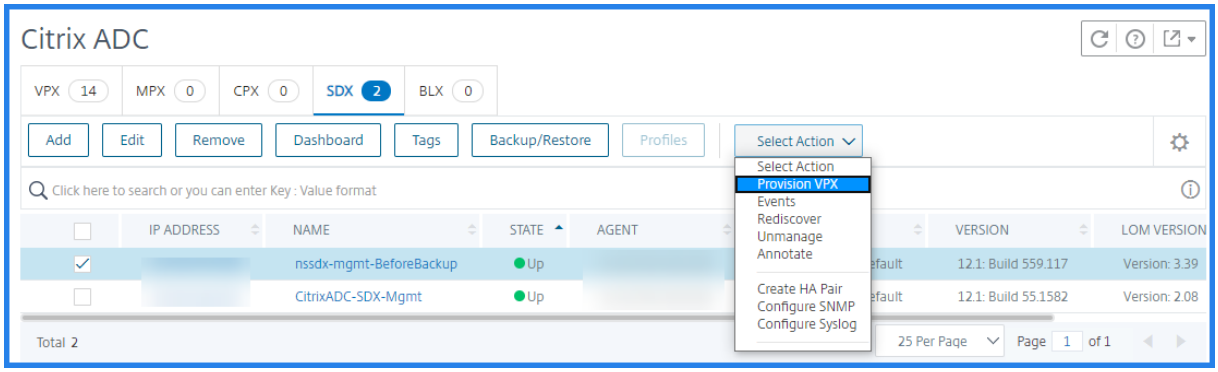
May 7, 2021

Citrix ADM を使用して、SDX アプライアンス上に 1 つ以上の ADC VPX インスタンスをプロビジョニングできます。デプロイできるインスタンスの数は、購入したライセンスによって異なります。追加されたインスタンスの数がライセンスで指定された数と同じである場合、ADM サービスでは、より多くの Citrix ADC インスタンスをプロビジョニングすることはできません。

開始する前に、VPX インスタンスをプロビジョニングする ADM に SDX インスタンスを追加してください。

VPX インスタンスをプロビジョニングするには、次の手順を実行します。

1. [ネットワーク**] > [**インスタンス**] > [Citrix ADC**] に移動します。
2.「**SDX** 」タブで、VPX インスタンスをプロビジョニングする SDX インスタンスを選択します。
3.「アクションの選択」で、「**VPX** のプロビジョニング」を選択します。

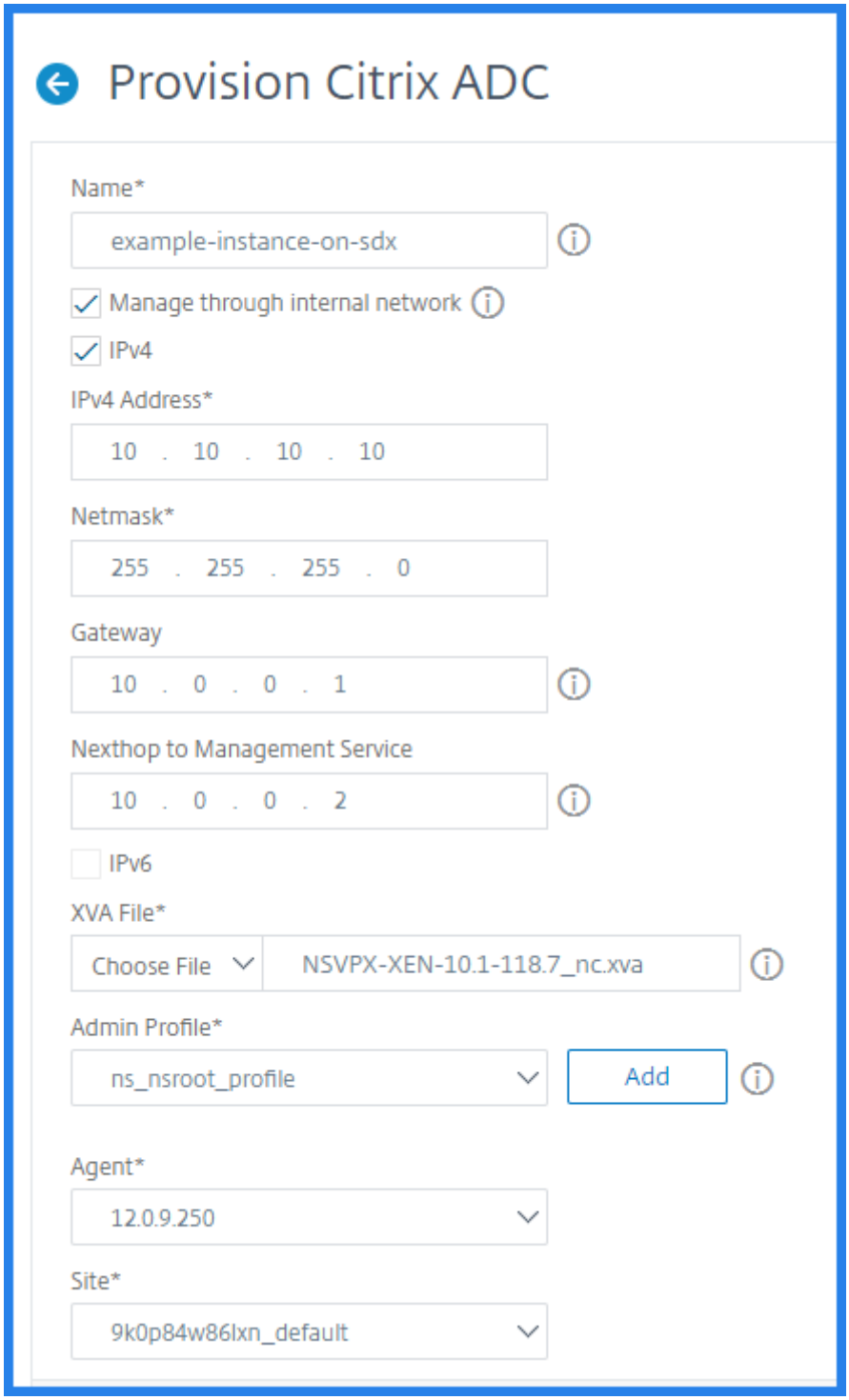


ステップ **1-VPX** インスタンスを追加する

ADM サービスは、次の情報を使用して、SDX アプライアンスの VPX インスタンスを構成します。

- 名前 - ADC インスタンスに名前を指定します。
- SDX と VPX 間の通信ネットワークを確立します。これを行うには、リストから必要なオプションを選択します。
  - 内部ネットワークを介して管理 -このオプションは、ADM と VPX インスタンス間の通信のための内部ネットワークを確立します。
  - **IP** アドレス -Citrix VPX インスタンスを管理するために、**IPv4** または **IPv6** アドレス、またはその両方を選択できます。VPX インスタンスは、1 つの管理 IP（Citrix ADC IP とも呼ばれます）のみを持つことができます。Citrix ADC IP アドレスを削除することはできません。

    選択したオプションで、IP アドレスのネットマスク、デフォルトゲートウェイ、およびネクストホップを ADM サービスに割り当てます。
- **XVA** ファイル -VPX インスタンスをプロビジョニングする XVA ファイルを選択します。XVA ファイルを選択するには、次のいずれかのオプションを使用します。
  - ローカル-ローカルマシンから XVA ファイルを選択します。
  - アプライアンス -ADM ファイルブラウザから XVA ファイルを選択します。
- 管理者プロファイル -このプロファイルは、VPX インスタンスをプロビジョニングするためのアクセスを提供します。このプロファイルを使用すると、ADM はインスタンスから設定データを取得します。プロファイルを追加する必要がある場合は、[追加] をクリックします。
- **Agent**： インスタンスを関連付けるエージェントを選択します。
- **[** サイト**]:** インスタンスを追加するサイトを選択します。



ステップ **2-**ライセンスの割り当て

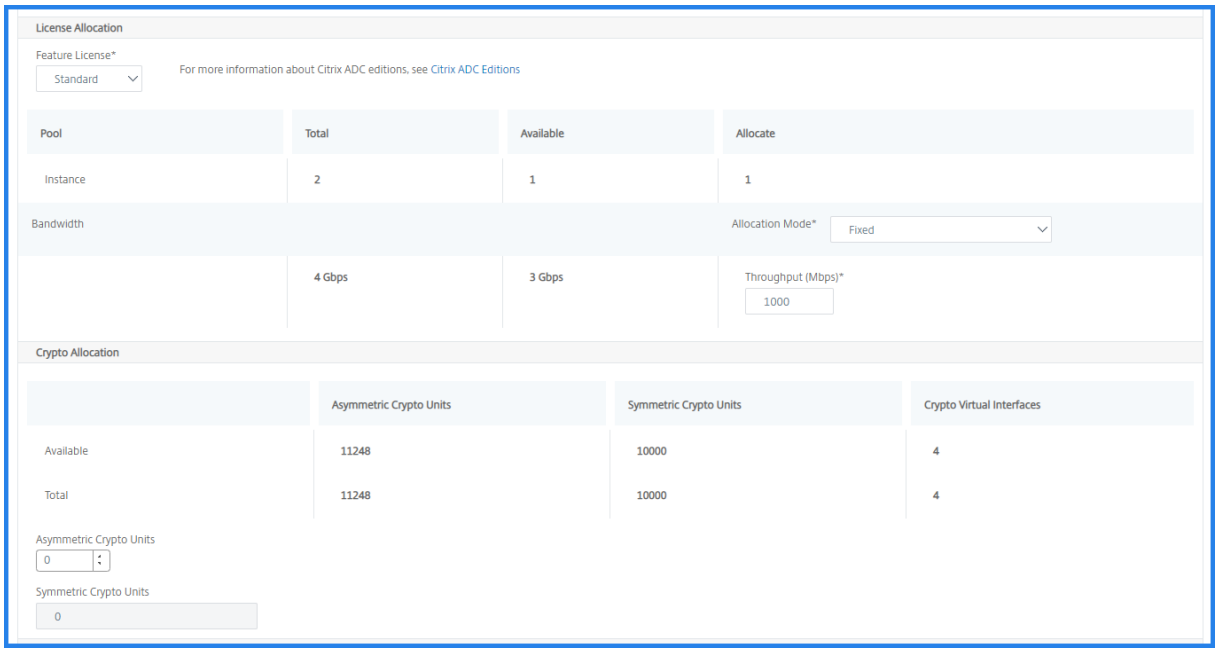
［ライセンスの割り当て］セクションで、VPX ライセンスを指定します。スタンダード、アドバンスト、プレミアムライセンスを使用できます。

- 割り当てモード：帯域幅プールに対して [固定] または [バースト可能] モードを選択できます。

  バースト可能モードを選択した場合、固定帯域幅に達したときに追加の帯域幅を使用できます。

- スループット -インスタンスに合計スループット（Mbps）を割り当てます。

> 注：
>
> SDX アプライアンス上の Citrix Secure Web Gateway（SWG）インスタンスについては、別途ライセンス（Secure Web Gateway 用 SDX 2 インスタンスアドオンパック）を購入してください。このインスタンスパックは、SDX プラットフォームライセンスまたは SDX インスタンスパックとは異なります。
>
> 詳細については、「SDX アプライアンスへの Citrix Secure Web Gateway インスタンスの展開」を参照してください。



SDX 12.0 57.19 バージョンから、暗号容量を管理するインターフェイスが変更されました。詳しくは、「暗号容量の管理」を参照してください。

ステップ **3-**リソースを割り当てる

「リソース割り当て」セクションで、リソースを VPX インスタンスに割り当てて、トラフィックを維持します。

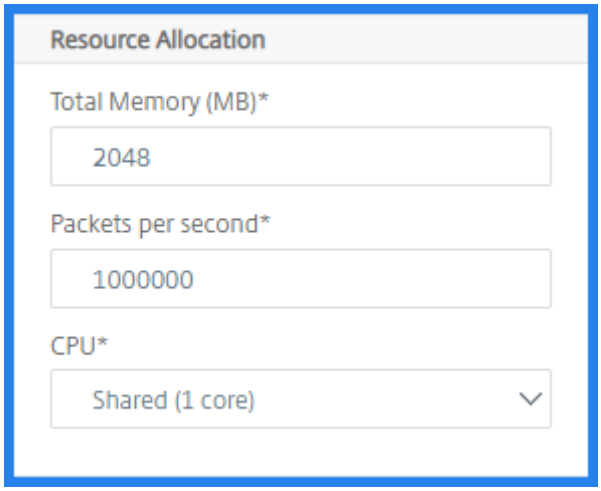
- 合計メモリ（**MB**） -インスタンスに合計メモリを割り当てます。最小値は 2048 MB です。
- [パケット**/**秒]-1 秒あたりに送信するパケット数を指定します。
- **CPU** -インスタンスに対する CPU コアの数を指定します。共有 CPU コアまたは専用の CPU コアを使用できます。

  インスタンスに対して共有コアを選択すると、リソース不足時に他のインスタンスは共有コアを使用できます。

パフォーマンスの低下を避けるため、CPU コアが再割り当てされたインスタンスを再起動します。

SDX 25000xx プラットフォームを使用している場合は、インスタンスには最大 16 コアを割り当てることができます。また、SDX 2500xxx プラットフォームを使用している場合は、インスタンスには最大 11 個のコアを割り当てることができます。

> 注:
>
> インスタンスの場合、構成する最大スループットは 180 Gbps です。



次の表に、サポートされている VPX、シングルバングルイメージのバージョン、およびインスタンスに割り当て可能なコア数を示します。

プラットフォーム名	総コア数	VPX プロビジョニングで使用可能なコアの合計	1 つのインスタンスに割り当て可能な最大コア数
SDX 8015、SDX 8400、SDX 8600	4	3	3
SDX 8900	8	7	7
SDX 11500、SDX 13500、SDX 14500、SDX 16500、SDX 18500、SDX 20500	12	10	5
SDX 11515、SDX 11520、SDX 11530、SDX 11540、SDX 11540、SDX 11542	12	10	5
SDX 17500、SDX 19500、SDX 21500	12	10	5

プラットフォーム名	総コア数	VPX プロビジョニングで使用可能なコアの合計	1 つのインスタンスに割り当て可能な最大コア数
SDX 17550、SDX 19550、SDX 20550、SDX 21550	12	10	5
SDX 14020、SDX 14030、SDX 14040、SDX 14060、SDX 14080、SDX 14100	12	10	5
SDX 22040、SDX 22060、SDX 22080、SDX 22100、SDX 22120	16	14	7
SDX 24100 と SDX 24150	16	14	7
SDX 14020 40G、SDX 14030 40G、SDX 14040 40G、SDX 14060 40G、SDX 14060 40G、SDX 14080 40G、SDX 14100 40G	12	10	10
SDX 14020 FIPS、SDX 14030 FIPS、SDX 14040 FIPS、SDX 14060 FIPS、SDX 14080 FIPS、SDX 14100。FIPS	12	10	5
SDX 14040 40S、SDX 14060 40S、SDX 14080 40S、SDX 14100 40S	12	10	5
SDX 25100A、25160A、25200A	20	18	9

プラットフォーム名	総コア数	VPX プロビジョニングで使用可能なコアの合計	1 つのインスタンスに割り当て可能な最大コア数
SDX 25100-40G、25160-40G、25200-40G	20	18	16 (バージョンが 11.1-51.x 以上の場合); 9 (バージョンが 11.1-50.x 以下の場合、11.0 および 10.5 のすべてのバージョン)
SDX 26100, 26160, 26200, 26250	28	26	13
15000-50G	16	14	7

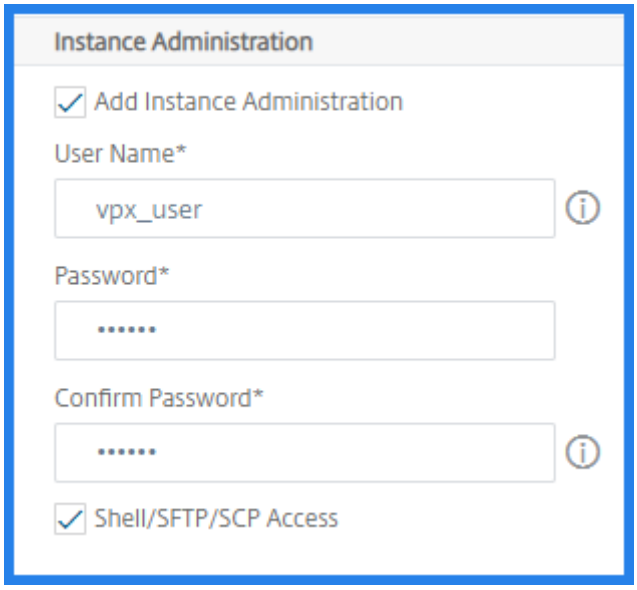
> 注:
>
> SDX 26xxx プラットフォームでは、VPX インスタンスに最大 26 個の CPU コアを割り当てることができます。暗号化ユニットがインスタンスに割り当てられている場合、コアの最大数は、暗号ユニットとデータインターフェイスの数によって異なります。
>
> たとえば、24000 暗号ユニットをインスタンスに割り当てると、24 CPU コアと最大 2 つのデータインターフェイスをインスタンスに割り当てることができます。SDX アプライアンスは、データインターフェイスと暗号ユニットを PCI デバイスと見なします。26000 暗号ユニットでは、データインターフェイスを追加するスペースがないため、VPX インスタンスのプロビジョニングが失敗します。

ステップ **4-**インスタンス管理を追加する

VPX インスタンスの管理ユーザーを作成できます。これを行うには、[インスタンス管理**] **** セクションの **[**** インスタンス管理を追加] を選択します。

次の詳細を指定します。

- ユーザー名: Citrix ADC インスタンス管理者のユーザー名。このユーザはスーパーユーザアクセスできますが、VLAN およびインターフェイスを設定するためのネットワークコマンドへのアクセス権がありません。
- パスワード: ユーザー名のパスワードを指定します。
- シェル**/SFTP/SCP** アクセス: Citrix ADC インスタンス管理者に許可されたアクセス。このオプションはデフォルトで選択されています。



手順 **5-**ネットワーク設定を指定する

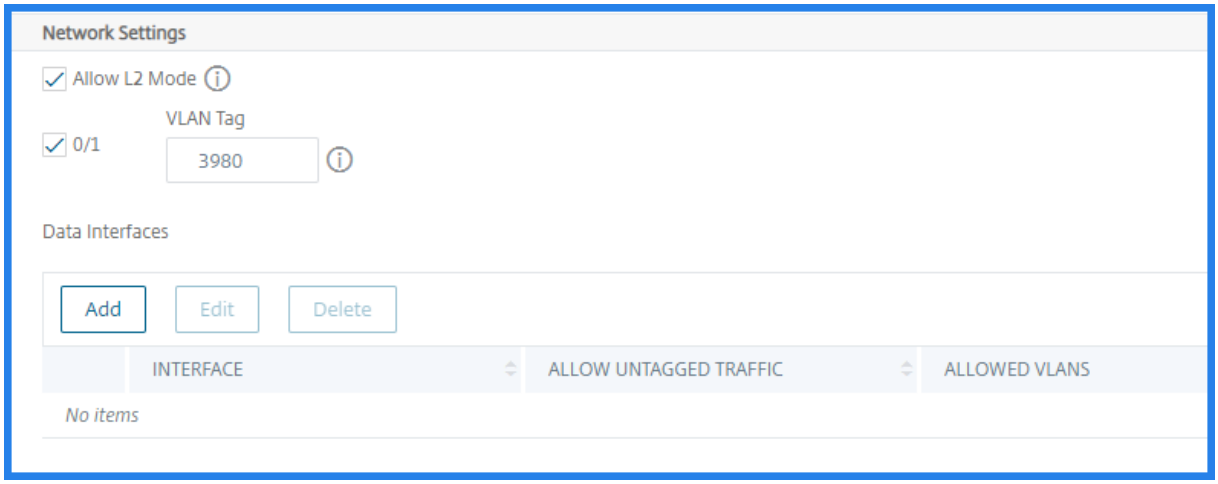
インスタンスに必要なネットワーク設定を選択します。

- ネットワーク設定で **L2** モードを許可する -Citrix ADC インスタンスで L2 モードを許可できます。[ネットワーク設定] で [L2 モードを許可する] を選択します。インスタンスにログオンし、L2 モードを有効にする前に。詳しくは、「Citrix ADC インスタンスでの L2 モードの許可」を参照してください。

  > 注
  >
  > インスタンスの L2 モードを無効にする場合は、インスタンスにログオンし、そのインスタンスから L2 モードを無効にする必要があります。そうしないと、インスタンスの再起動後に他のすべての Citrix ADC モードが無効になる可能性があります。

- **0/1** - **VLAN** タグで、管理インターフェイスの VLAN ID を指定します。
- **0/2** - **VLAN** タグで、管理インターフェイスの VLAN ID を指定します。

デフォルトでは、インターフェイス **0/1** および **0/2** が選択されます。

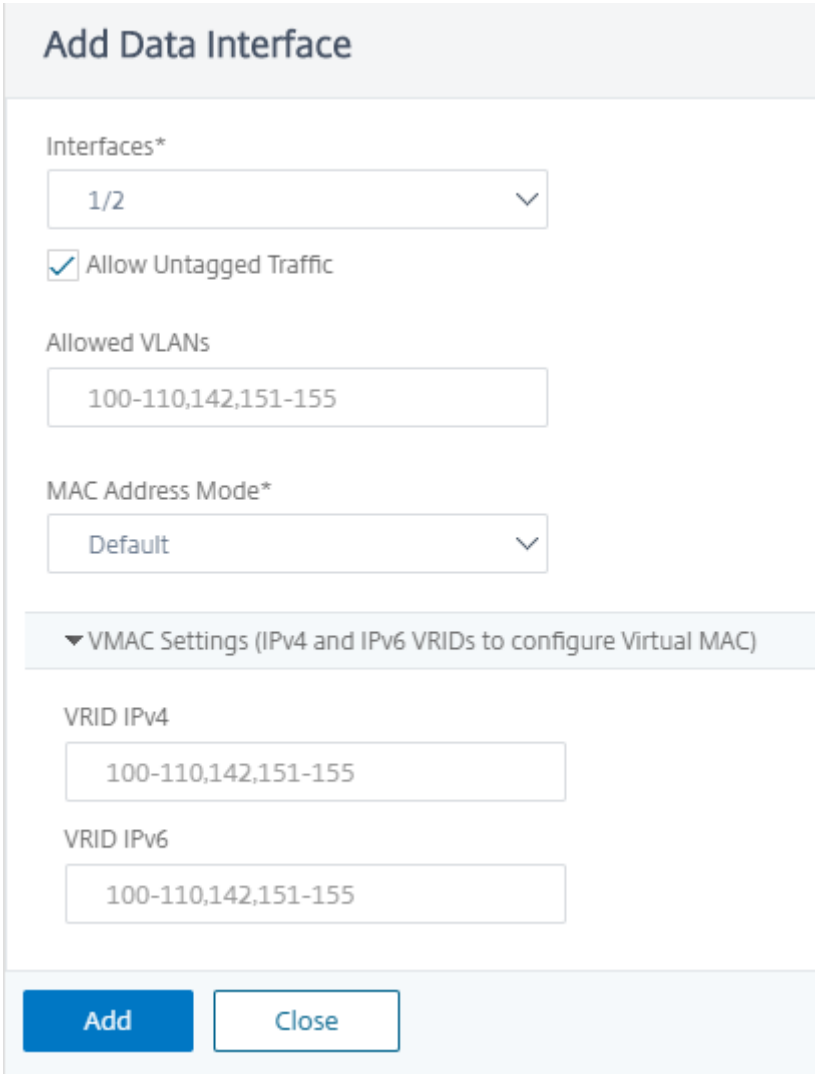


「データ・インタフェース」で、「追加」をクリックしてデータ・インタフェースを追加し、次を指定します。

- [インタフェース]-リストからインターフェイスを選択します。

  > 注:
  >
  > インスタンスに追加するインターフェイスのインターフェイス ID は、SDX アプライアンスでの物理インターフェイスの番号付けに対応しているとは限りません。
  >
  > たとえば、インスタンス 1 に関連付ける最初のインターフェイスは SDX インターフェイス 1/4 で、そのインスタンスのインターフェイス設定を表示すると、インターフェイス 1/1 として表示されます。このインターフェイスは、instance-1 に関連付けた最初のインターフェイスであることを示します。

- 許可された **VLAN**： Citrix ADC インスタンスに関連付けることができる VLAN ID のリストを指定します。
- **MAC** アドレスモード -インスタンスに MAC アドレスを割り当てます。次のいずれかのオプションを選択します:
  - デフォルト -Citrix Workspace によって MAC アドレスが割り当てられます。
  - [カスタム]: 生成された MAC アドレスを上書きする MAC アドレスを指定するには、このモードを選択します。
  - **Generated** -前に設定したベース MAC アドレスを使用して MAC アドレスを生成します。ベース MAC アドレスの設定については、「インターフェイスへの MAC アドレスの割り当て」を参照してください。
- **VMAC** 設定（仮想 **MAC** を設定するための **IPv4** および **IPv6 VRID**）
  - **VRID IPV4** -VMAC を識別する IPv4 VRID。可能な値:1 ～255 詳しくは、「インターフェイスでの VMAC の設定」を参照してください。
  - VRID IPV6-VMAC を識別する IPv6 VRID。可能な値:1 ～255 詳しくは、「インターフェイスでの VMAC の設定」を参照してください。



［追加］をクリックします。

ステップ **6-**管理 **VLAN** 設定を指定する

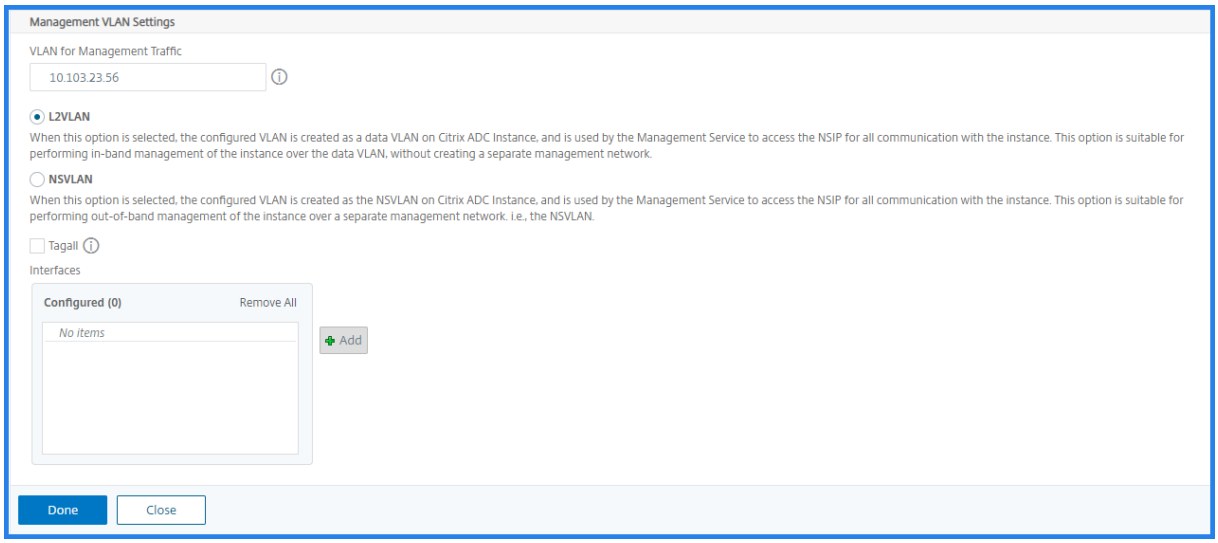
VPX インスタンスの管理サービスと管理アドレス（NSIP）は同じサブネットワークにあり、通信は管理インタフェースを介して実行されます。

管理サービスとインスタンスが異なるサブネットワークにある場合は、VPX インスタンスのプロビジョニング中に VLAN ID を指定します。したがって、インスタンスは、アクティブなときにネットワーク経由で到達可能です。

VPX インスタンスのプロビジョニング中に、選択したインターフェイスからのみ NSIP にアクセスできるようにする必要がある場合は、［**NSVLAN**］を選択します。また、NSIP は他のインターフェイスを介してアクセスできなくなります。

- HA ハートビートは、NSVLAN の一部であるインターフェイスだけで送信されます。
- NSVLAN は、VPX XVA ビルド9.3–53.4以降からのみ構成できます。

> 重要
>
> - VPX インスタンスをプロビジョニングした後は、この設定を変更できません。
> - **NSVLAN** が選択されていない場合、**VPX** インスタンス上で**clear config full**コマンドを実行すると、**VLAN** 構成が削除されます。

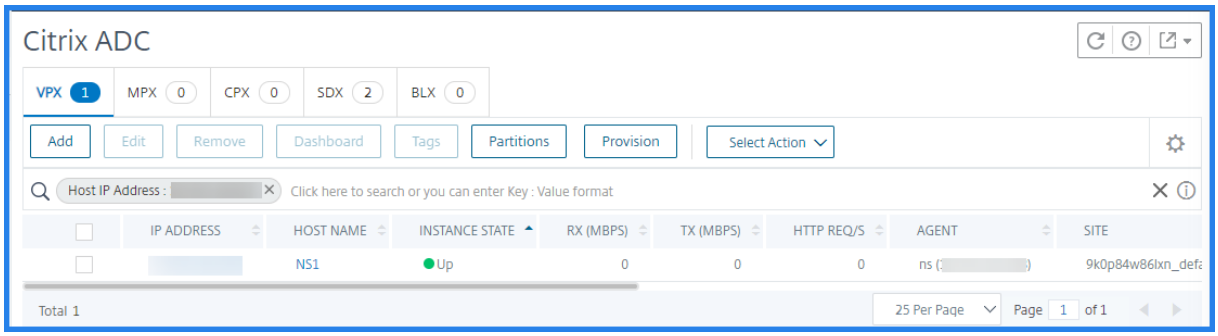


「完了」をクリックして、VPX インスタンスをプロビジョニングします。

プロビジョニングされた **VPX** インスタンスの表示

新しくプロビジョニングされたインスタンスを表示するには、次の手順を実行します。

1. [ネットワーク**] > [**インスタンス**] > [Citrix ADC**] に移動します。
2. [**VPX**] タブで、[ホスト **IP** アドレス] プロパティでインスタンスを検索し、そのインスタンスに SDX インスタンスの IP を指定します。



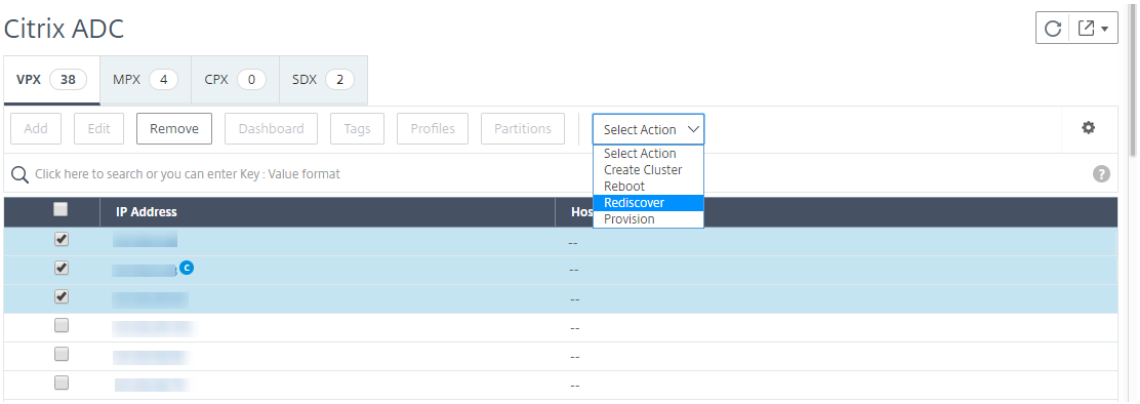
複数の **Citrix ADC VPX** インスタンスの再検出

May 7, 2021

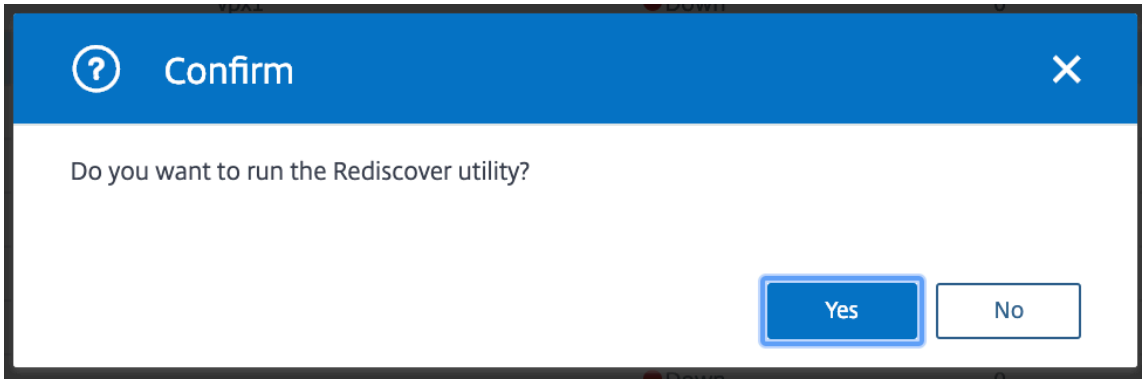
Citrix Application Delivery Manegement（Citrix ADM）の設定で、複数の Citrix Application Delivery Controller（Citrix ADC）VPX インスタンスを再検出できるようになりました。以前は、単一の Citrix ADC VPX インスタンスのみを再検出できました。これらのインスタンスの最新の状態と構成を表示する場合は、複数の Citrix ADC VPX インスタンスを再検出できます。Citrix ADM サーバーは、すべての Citrix ADC VPX インスタンスを再検出し、Citrix ADC インスタンスが到達可能かどうかを確認します。

複数の **Citrix ADC VPX** インスタンスを再検出するには:

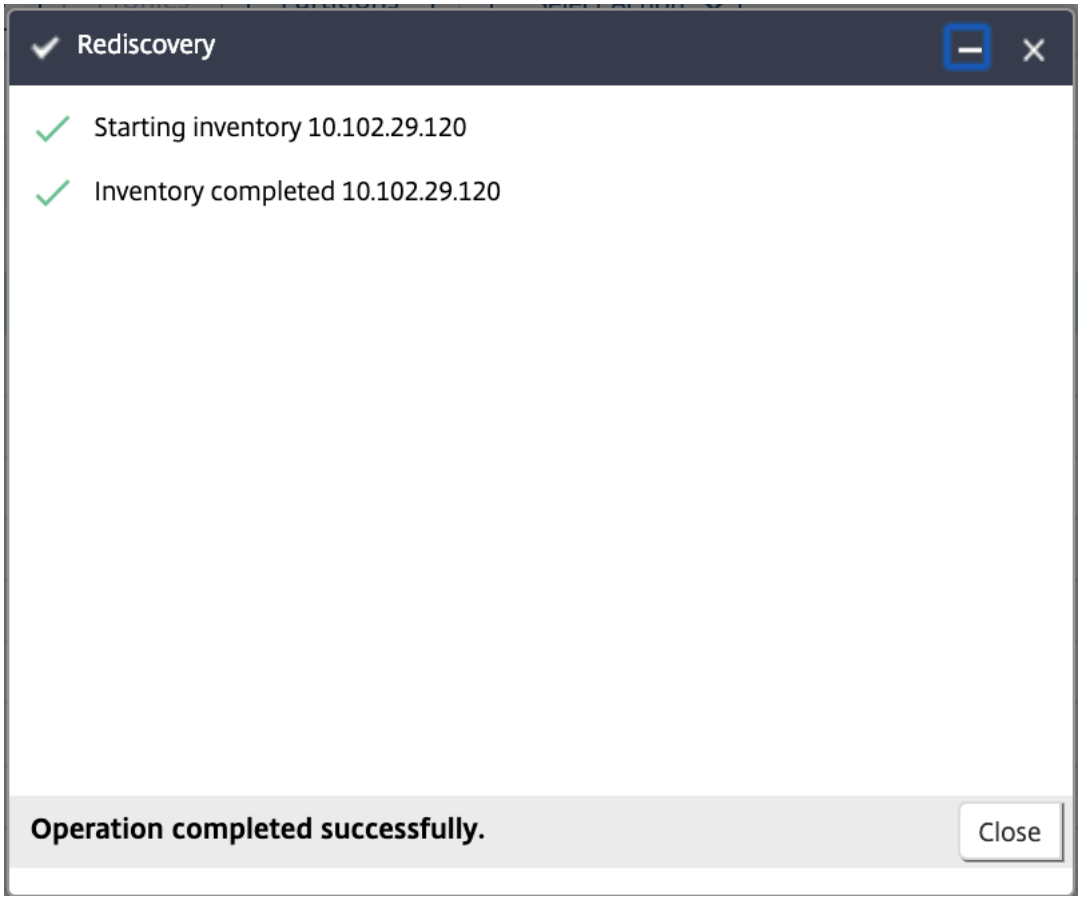
1. [ネットワーク] > [インスタンス] **>** [**Citrix ADC**] > [**VPX**] の順に選択し、再検出するインスタンスを選択します。
2. [操作] ボックスで、[再検出] をクリックします。



3. 再検出ユーティリティを実行するための確認メッセージが表示されたら、[はい] をクリックします。



各 Citrix ADC VPX インスタンスの再検出の進行状況が画面に表示されます。



ポーリングの概要

May 7, 2021

ポーリングは、Citrix Application Delivery Management（ADM）が Citrix ADC インスタンスから特定の情報を収集するプロセスです。世界中の組織に複数の Citrix ADC インスタンスを構成している可能性があります。Citrix ADM を使用してインスタンスを監視するには、すべての管理対象 Citrix ADM C インスタンスから、CPU 使用率、メモリ使用率、SSL 証明書、ライセンスされた機能、ライセンスタイプなどの特定の情報を収集する必要があります。ADM と管理対象インスタンスの間で発生するさまざまな種類のポーリングを次に示します。

- インスタンスのポーリング
- インベントリのポーリング
- パフォーマンス・データの収集
- インスタンスのバックアップポーリング
- 構成監査ポーリング
- SSL 証明書のポーリング

- エンティティのポーリング

Citrix ADM は、NITRO 呼び出し、セキュアシェル（SSH)、セキュアコピー（SCP）などのプロトコルを使用して、Citrix ADC インスタンスからの情報をポーリングします。

Citrix ADM が管理対象インスタンスおよびエンティティをポーリングする方法

デフォルトでは、Citrix ADM は定期的に自動的にポーリングします。また、Citrix ADM では、いくつかの種類のポーリングに対してポーリング間隔を構成し、必要に応じて手動でポーリングすることもできます。

次の表に、ポーリングのタイプ、ポーリング間隔、使用されるプロトコルなどの詳細を示します。

ポーリングタイプ	ポーリング間隔	ポーリングされた情報	使用されるプロトコル	ポーリング間隔の設定
インスタンスのポーリング	5 分ごと（デフォルト）	状態、1 秒あたりの HTTP 要求、CPU 使用率、メモリ使用率、スループットなどの統計情報。	NITRO 呼び出し	いいえ
インベントリのポーリング	60 分ごと（デフォルト）	ビルドバージョン、システム情報、ライセンスされた機能、モードなどのインベントリの詳細。	NITRO 呼び出しと SSH	いいえ
パフォーマンス・データの収集	5 分ごと（デフォルト）	ネットワークレポート情報	NITRO 呼び出し	いいえ
インスタンスのバックアップポーリング	12 時間ごと (デフォルト)	管理されている ADC インスタンスの現在の状態のバックアップファイル	NITRO 呼び出し、SSH、および SCP。	はい。[ネットワーク] > [インスタンス] > [**Citrix ADC**] に移動します。インスタンスを選択し、[**Select Action**] リストから [バックアップ/復元] をクリックします。

ポーリングタイプ	ポーリング間隔	ポーリングされた情報	使用されるプロトコル	ポーリング間隔の設定
構成監査ポーリング	10 時間ごと (デフォルト)	ADC インスタンスで発生する設定変更（構成実行と構成保存など）	SSH、SCP、および NITRO 呼び出し	はい。[ネットワーク] > [構成監査] に移動します。[構成監査] ページで、[設定] をクリックし、[構成監査ポーリング] のポーリング間隔を構成します。
				構成監査を手動でポーリングし、インスタンスのすべての構成監査を直ちに Citrix ADM に追加できます。これを行うには、[ネットワーク] > [構成の監査] に移動し、[今すぐポーリング] をクリックします。[**Poll Now**] ページでは、ネットワーク内のすべてのインスタンスまたは選択したインスタンスをポーリングできます。
SSL 証明書のポーリング	24 時間ごと（デフォルト）	Citrix ADC インスタンスにインストールされている SSL 証明書。	NITRO 呼び出しおよび SCP	はい。[ネットワーク] > [**SSL** ダッシュボード] に移動します。[SSL ダッシュボード] ページで、[設定] をクリックしてポーリング間隔を設定します。

ポーリングタイプ	ポーリング間隔	ポーリングされた情報	使用されるプロトコル	ポーリング間隔の設定
				SSL 証明書を手動でポーリングし、インスタンスのすべての証明書を直ちに Citrix ADM に追加できます。これを行うには、[ネットワーク] > [**SSL** ダッシュボード] に移動し、[今すぐポーリング] をクリックします。[**Poll Now**] ページでは、ネットワーク内のすべてのインスタンスまたは選択したインスタンスをポーリングできます。
エンティティのポーリング	60 分ごと（デフォルト）	インスタンスに設定されているすべてのエンティティ。エンティティは、ADC インスタンスにアタッチされたポリシー、仮想サーバー、サービス、またはアクションのいずれかです。エンティティのポーリングを有効にするには、ADM 機能の有効化または無効化を参照してください。	NITRO 呼び出し	はい。ただし、10 分未満に設定することはできません。設定するには、[ネットワーク**] > [**ネットワーク機能] に移動します。[ネットワーク機能] ページで、[設定] をクリックしてポーリング間隔を構成します。

ポーリングタイプ	ポーリング間隔	ポーリングされた情報	使用されるプロトコル	ポーリング間隔の設定
				エンティティを手動でポーリングし、インスタンスのすべてのエンティティを直ちに Citrix ADM に追加できます。これを行うには、[ネットワーク] > [ネットワーク機能] に移動し、[今すぐポーリングする] をクリックします。[**Poll Now**] ページでは、ネットワーク内のすべてのインスタンスまたは選択したインスタンスをポーリングできます。

> 注:
>
> ポーリングに加えて、管理対象 ADC インスタンスによって生成されたイベントは、インスタンスに送信された SNMP トラップを介して Citrix ADM によって受信されます。たとえば、システム障害や構成の変更が発生したときにイベントが生成されます。
>
> インスタンスのバックアップ中に、SSL ファイル、CA 証明書ファイル、ADC テンプレート、データベース情報などが Citrix ADM にダウンロードされます。構成監査中は、ns.conf ファイルがダウンロードされてファイルシステムに格納されます。管理対象の Citrix ADC インスタンスから収集されたすべての情報は、データベース内に内部的に保存されます。

インスタンスをポーリングするさまざまな方法

Citrix ADM が管理対象インスタンスに対して実行するポーリング方法は次のとおりです。

- インスタンスのグローバルポーリング
- インスタンスの手動ポーリング
- エンティティの手動ポーリング

インスタンスのグローバルポーリング

Citrix ADM は、ユーザーが設定した間隔に応じて、ネットワーク内のすべての管理対象インスタンスを自動的にポーリングします。デフォルトのポーリング間隔は 60 分ですが、[ネットワーク] > [ネットワーク機能] > [設定] の順に選択して、要件に応じて間隔を設定できます。

インスタンスの手動ポーリング

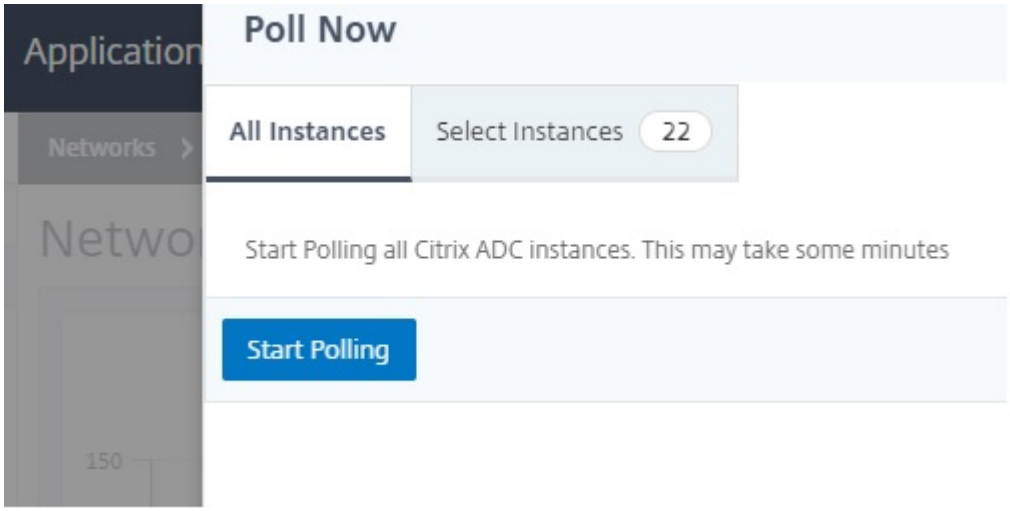
Citrix ADM が多くのエンティティを管理している場合、ポーリングサイクルにレポートの生成に時間がかかり、画面が空白になったり、システムに以前のデータが表示される場合があります。

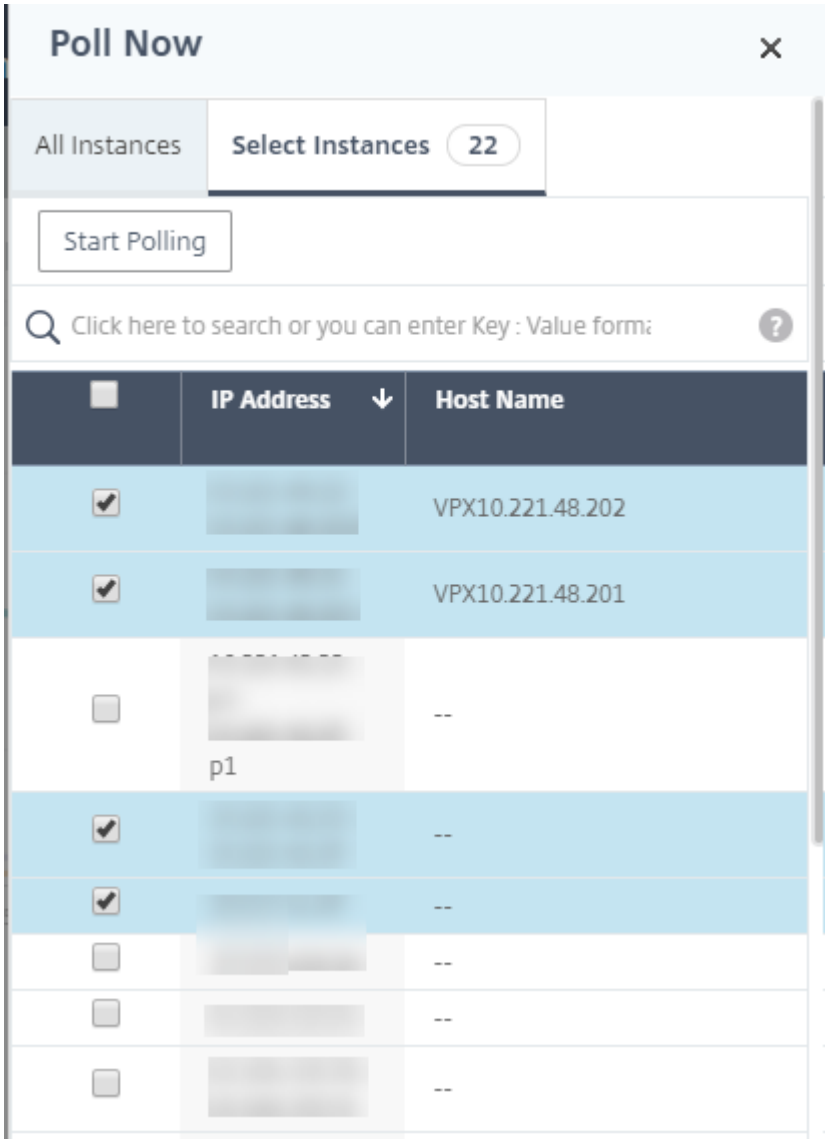
Citrix ADM では、自動ポーリングが行われない最小ポーリング間隔があります。新しい Citrix ADC インスタンスを追加した場合、またはエンティティが更新された場合、次のポーリングが行われるまで、Citrix ADM は新しいインスタンスまたはエンティティに対して行われた更新を認識しません。また、さらに操作を行うために仮想 IP アドレスの一覧をすぐに取得する方法はありません。最短のポーリング間隔期間が経過するまで待つ必要があります。手動でポーリングして新しく追加されたインスタンスを検出することはできますが、これにより Citrix ADC ネットワーク全体がポーリングされ、ネットワークに大きな負荷が生じます。Citrix ADM では、ネットワーク全体をポーリングする代わりに、特定の時点で選択したインスタンスおよびエンティティのみをポーリングできるようになりました。

Citrix ADM は、管理対象インスタンスを自動的にポーリングして、1 日に設定された時刻に情報を収集します。選択されたポーリングにより、選択したインスタンスにバインドされたエンティティの最新のステータスを Citrix ADM で表示するために必要な更新時間が短縮されます。

Citrix ADM で特定のインスタンスをポーリングするには:

1. Citrix ADM で、［ネットワーク］>［ネットワーク機能］に移動します。
2. [ネットワーク機能] ページの右上隅にある [今すぐポーリングする] をクリックします。
3. [**Poll Now**] ポップアップページには、ネットワーク内のすべての Citrix ADC インスタンスをポーリングするか、選択したインスタンスをポーリングするかを選択できます。
   a) [**All Instances**] タブ-[ポーリング開始] をクリックして、すべてのインスタンスをポーリングします。
   b) **[** インスタンスを選択] タブ-リストからインスタンスを選択します。
4. [ポーリングの開始] をクリックします。





Citrix ADM は手動ポーリングを開始し、すべてのエンティティを追加します。

エンティティの手動ポーリング

Citrix ADM では、インスタンスにバインドされているいくつかの選択されたエンティティのみをポーリングすることもできます。たとえば、このオプションを使用して、インスタンス内の特定のエンティティの最新のステータスを知ることができます。この場合、更新された 1 つのエンティティのステータスを知るために、インスタンス全体をポーリングする必要はありません。エンティティを選択してポーリングすると、Citrix ADM はそのエンティティのみをポーリングし、Citrix ADM GUI でステータスを更新します。

仮想サーバがダウンしている例を考えてみましょう。次の自動ポーリングが行われる前に、その仮想サーバのステータスが [**UP**] に変更されている可能性があります。仮想サーバの変更されたステータスを表示するには、その仮想サーバだけをポーリングして、正しいステータスが GUI にすぐに表示されるようにします。

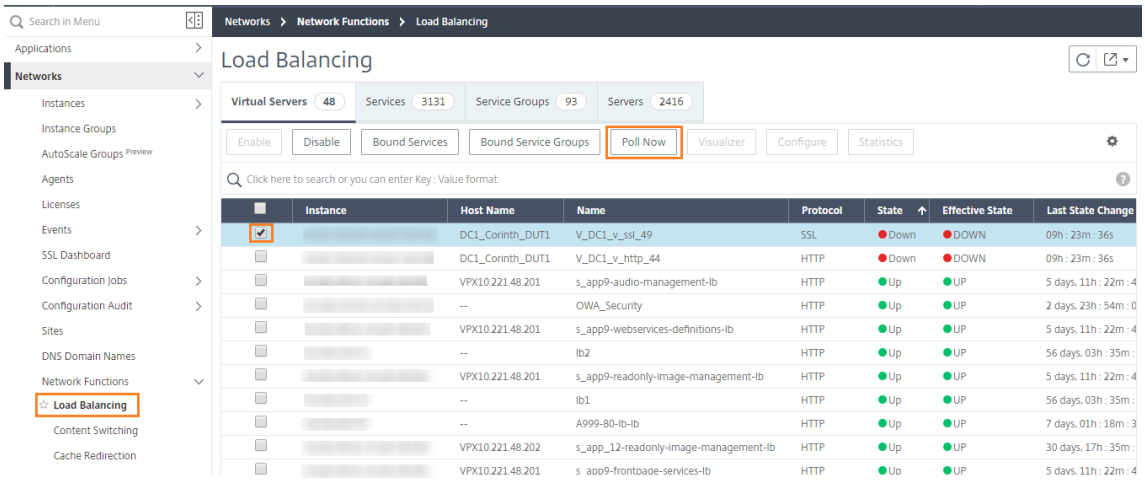
次のエンティティのステータス、サービス、サービスグループ、負荷分散仮想サーバー、キャッシュ削減仮想サーバー、コンテンツスイッチング仮想サーバー、認証仮想サーバー、VPN 仮想サーバー、GSLB 仮想サーバー、アプリケーションサーバーの更新をポーリングできるようになりました。

> 注:
>
> 仮想サーバをポーリングする場合、その仮想サーバだけがポーリングされます。サービス、サービスグループ、サーバなどの関連エンティティはポーリングされません。関連するすべてのエンティティをポーリングする必要がある場合は、エンティティを手動でポーリングするか、インスタンスをポーリングする必要があります。

Citrix ADM の特定のエンティティをポーリングするには:

たとえば、このタスクは、ロードバランシング仮想サーバーのポーリングに役立ちます。同様に、他のネットワーク機能エンティティもポーリングできます。

1. Citrix ADM で、[ネットワーク] > [ネットワーク機能] > [負荷分散] > [仮想サーバー] に移動します。
2. 状態が [ダウン] と表示されている仮想サーバーを選択し、[今すぐポーリング] をクリックします。仮想サーバのステータスが [**UP**] に変わります。



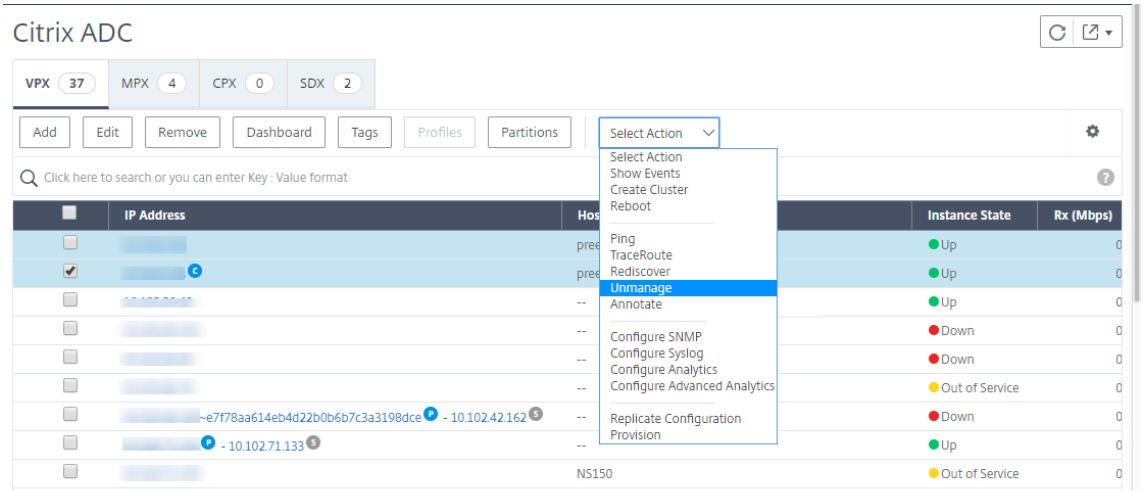
インスタンスの管理解除

May 7, 2021

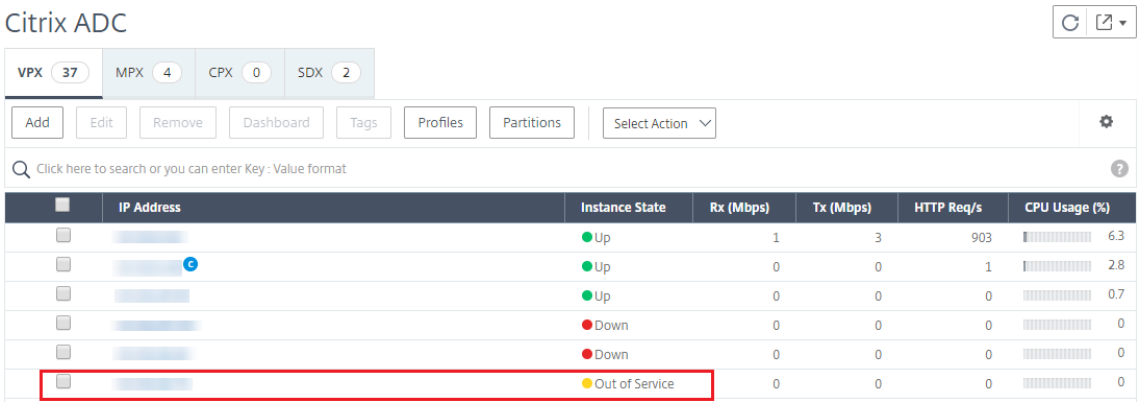
Citrix Application Delivery Management（Citrix ADM）とネットワーク内のインスタンス間の情報交換を停止する場合は、インスタンスの管理を解除できます。

インスタンスの管理を解除するには、次の手順に従います。

1. [ネットワーク] > [インスタンス] > [**Citrix ADC**] に移動します。
2. ADC インスタンスタブ（VPX など）を選択します。
3. インスタンスのリストで、インスタンスを右クリックして [**Unmane**] を選択するか、[インスタンス] を選択して [**Action**] リストから [**Unmane**] を選択します。



選択したインスタンスのステータスが [**Out of Service**] に変わります。



インスタンスは Citrix ADM によって管理されなくなり、Citrix ADM とデータを交換できなくなります。

インスタンスへのルートをトレースする

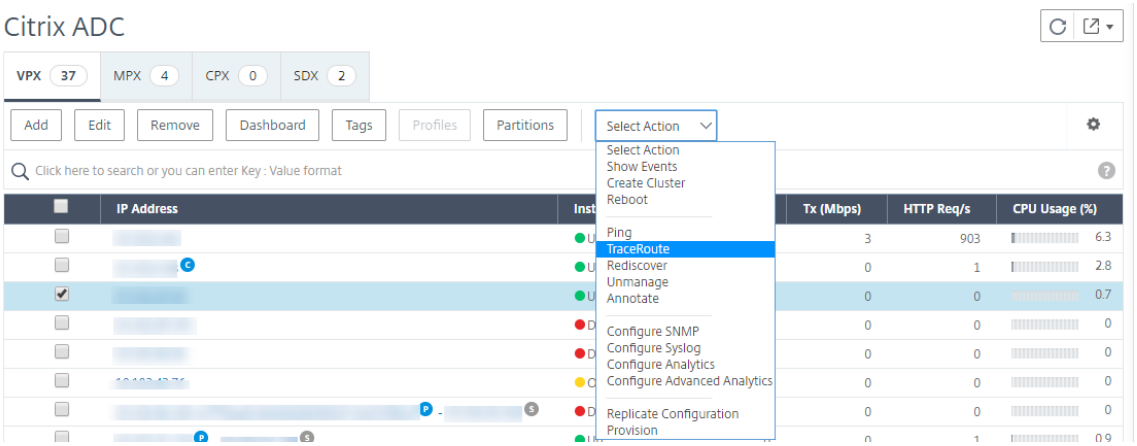
May 7, 2021

Citrix ADM（Citrix Application Delivery Management ADM）からインスタンスへのパケットのルートを追跡することで、インスタンスに到達するために必要なホップ数などの情報を確認できます。traceroute は、送信元から宛先へのパケットのパスをトレースします。これには、ルート内の各エンティティのホスト名と IP アドレスと共に、ネットワークホップの一覧が表示されます。

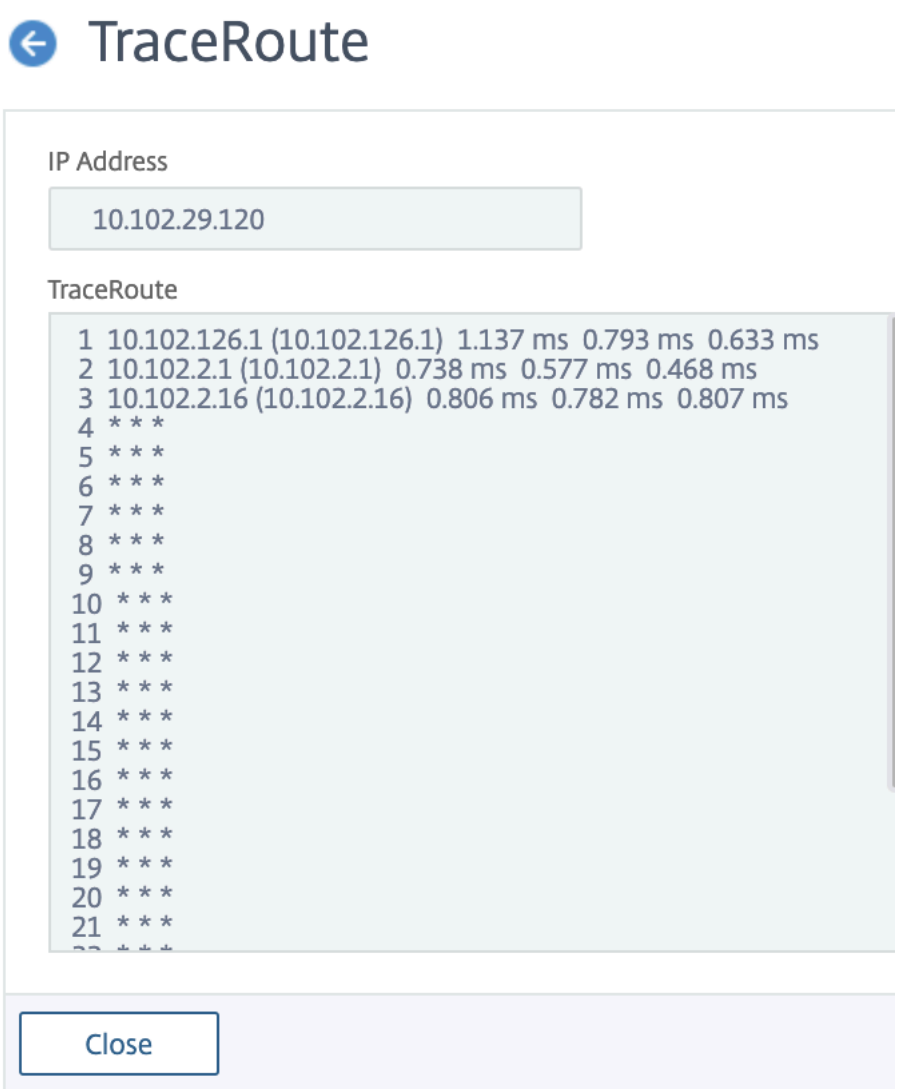
また、Traceroute では、あるホップから別のホップへパケットが移動するのにかかる時間が記録されます。パケットの転送に中断がある場合、traceroute は問題の発生場所を示します。

インスタンスのルートをトレースするには:

1. [ネットワーク] > [インスタンス] > [**Citrix ADC**] に移動します。
2. ADC インスタンスタブ（VPX など）を選択します。
3. インスタンスのリストで、インスタンスを右クリックして **TraceRoute** を選択するか、インスタンスを選択し、[アクション] リストから [**TraceRoute**] をクリックします。



[TraceRoute] メッセージボックスに、インスタンスへのルート、および各ホップでかかった時間（ミリ秒単位）が表示されます。



Citrix ADC MPX または VPX ルートパスワードを変更する方法

May 7, 2021

セキュリティ上の理由やパスワードローテーションポリシーの遵守のために、Citrix ADC アプライアンスの root パスワードを変更する必要がある場合があります。

このドキュメントでは、Citrix ADM Cloud を介して管理される Citrix ADC MPX および VPX アプライアンスのルートパスワードを変更するために必要な手順について説明します。

ADC パスワードを変更する場合は、その ADC に関連付けられている ADM 管理プロファイルを変更する必要があります。ADM 管理者プロファイルは、REST API、SSH、SCP、または ADC アプライアンスとの SNMP ベースの通信の ADC 認証情報を保持します。Citrix ADM は、管理者プロファイルを使用して、Citrix ADC MPX および VPX アプライアンスを管理します。

構成ジョブ機能を使用したパスワードの変更

Citrix ADM 構成ジョブ機能を使用すると、個々のインスタンスにアクセスすることなく、繰り返しパスワード変更プロセスを簡素化し、変更を Citrix ADC アプライアンスに適用できます。

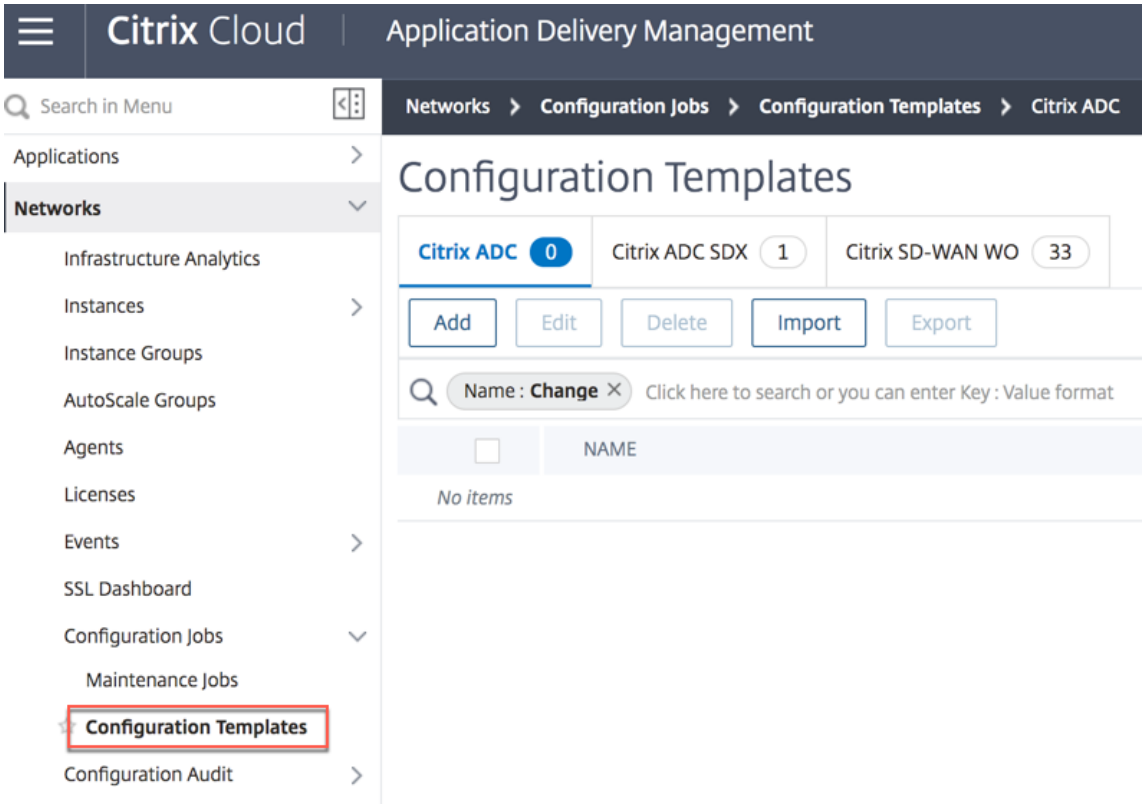
パスワードを変更するには、次の手順に従います。

- 手順 1. 構成テンプレートを作成します。
- 手順 2. 構成ジョブを作成します。
- 手順 3. 管理者プロファイルを作成し、修正します。

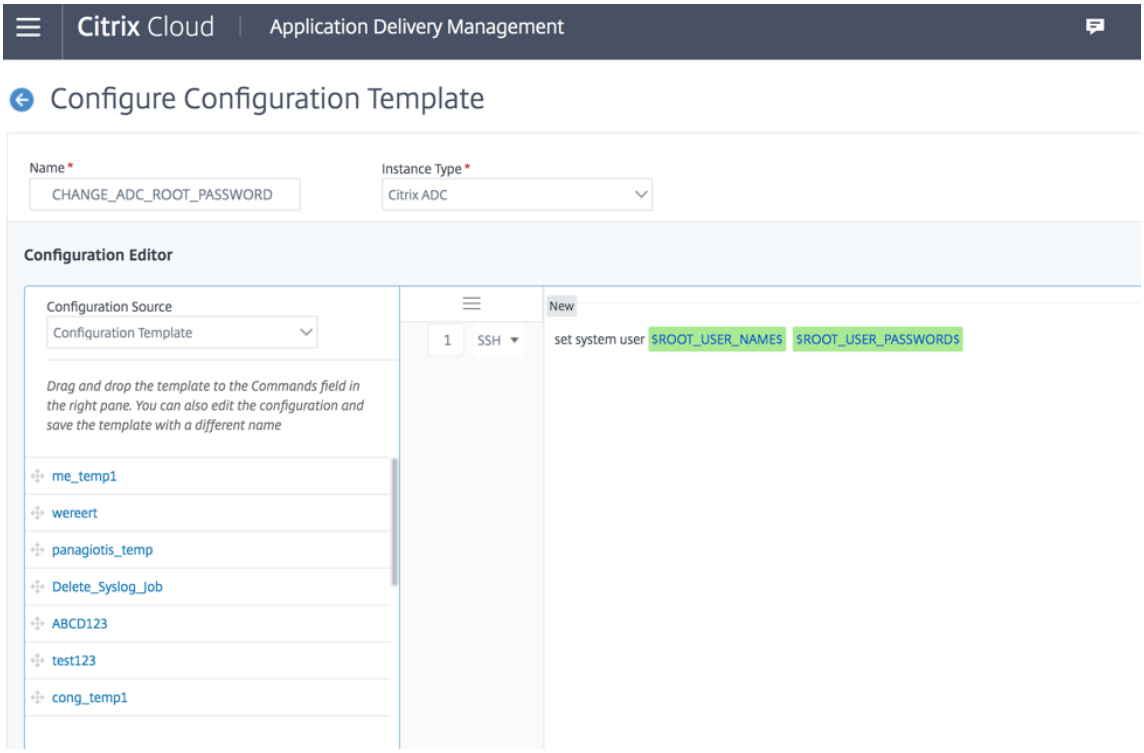
> 注：ADC アプライアンスが他のツールによって管理されている場合は、それらのツールの認証情報も変更する必要があります。

構成テンプレートの作成

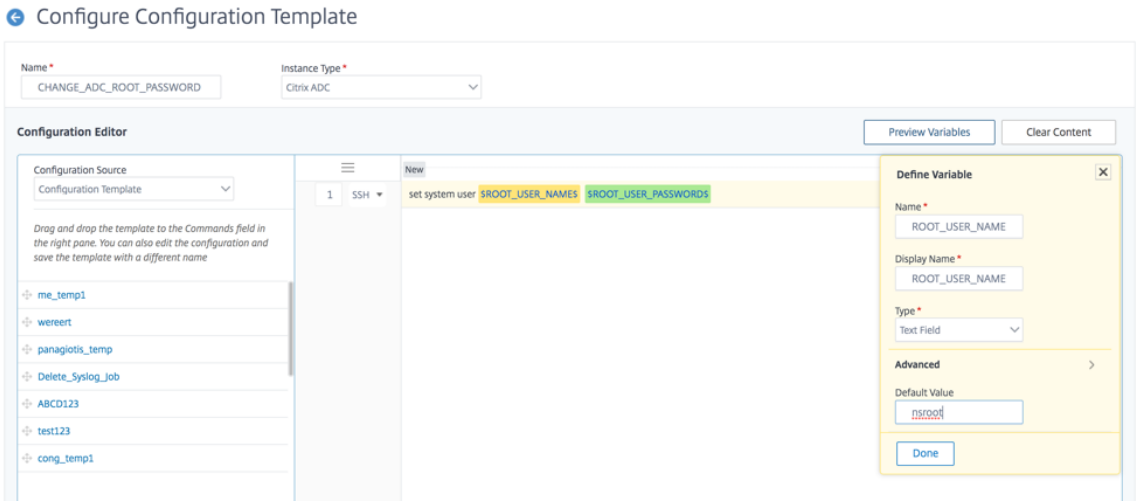
1. ADM GUI から、[ネットワーク] **>** [構成ジョブ] **>** [構成テンプレート] に移動します。



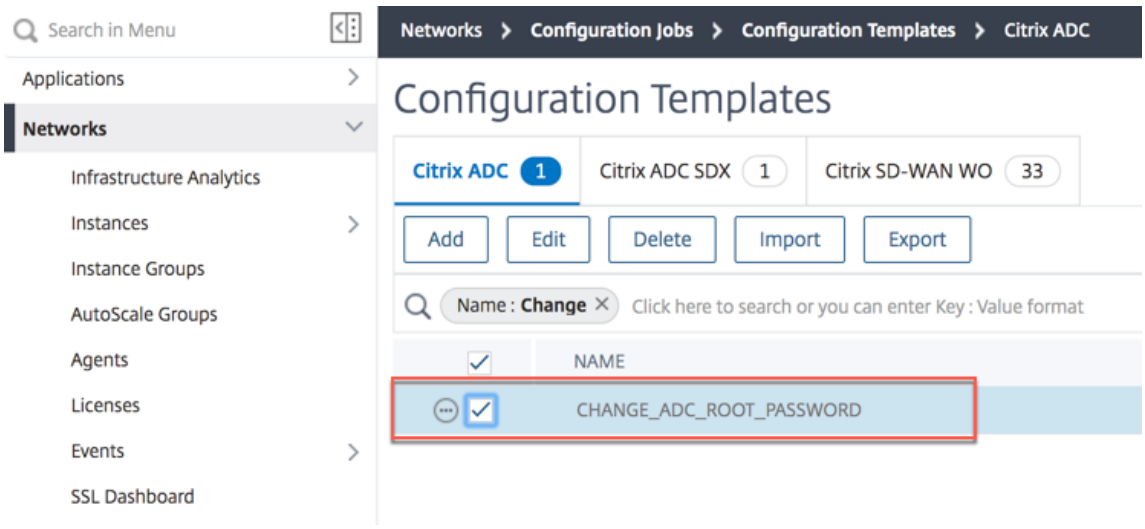
2. [追加] を選択します。SSH コマンドを入力して、`set system user $ROOT_USER_NAME$ $ROOT_USER_PASSWORD$`で設定テンプレートを作成します。



3. $ROOT_USER_NAME$ 変数を選択し、[タイプ] として **[**テキストフィールド] を選択します。
4. 必要に応じて、root ユーザー名のデフォルト値を指定します。変数設定を保存するには、[完了] を選択します。

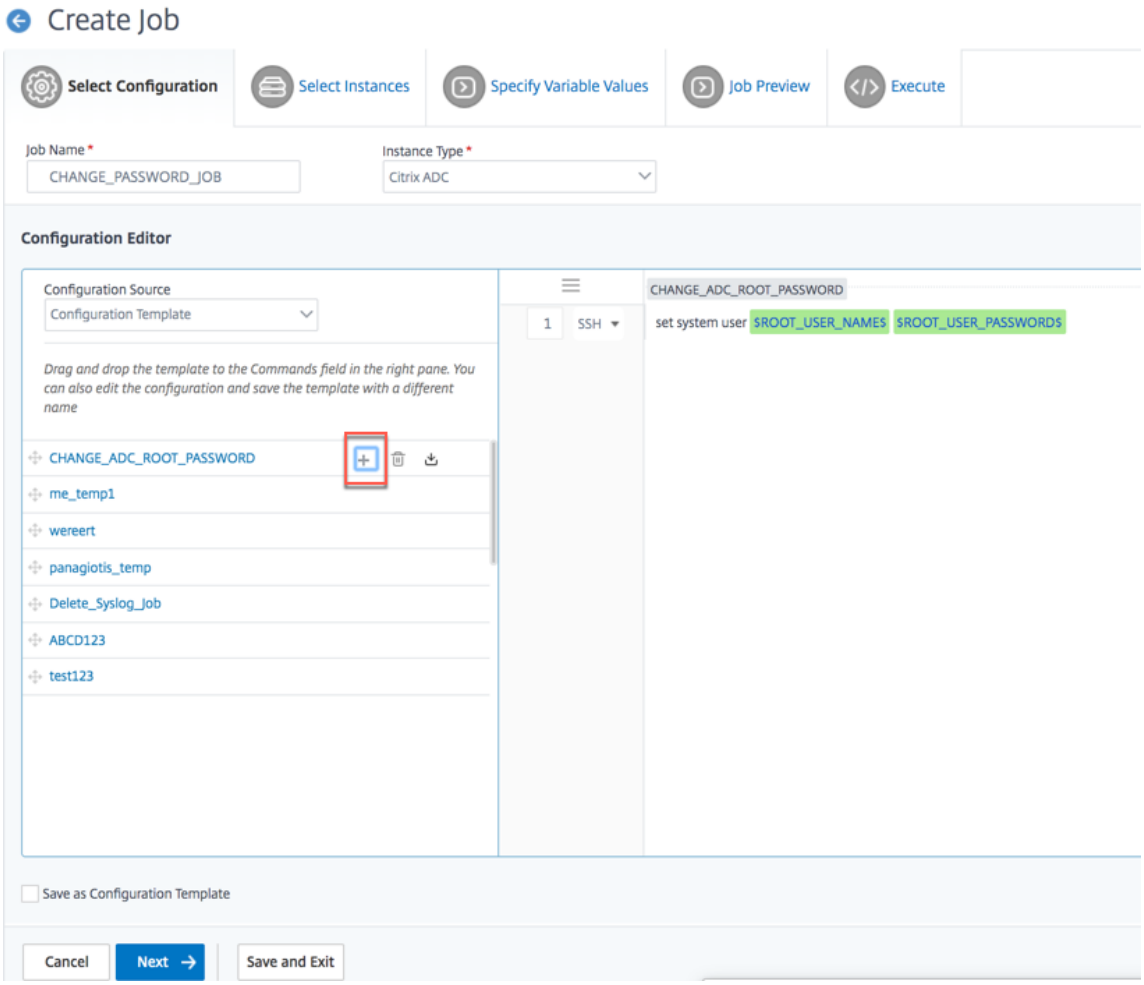


5. $ROOT_USER_PASSWORD$ 変数を選択し、「タイプ」として「パスワードフィールド」を選択します。変数設定を保存するには、[完了] を選択します。
6. 「**OK**」を選択して、構成テンプレートを保存します。
7. 新しい構成テンプレートが [構成テンプレート] の下に表示されます。

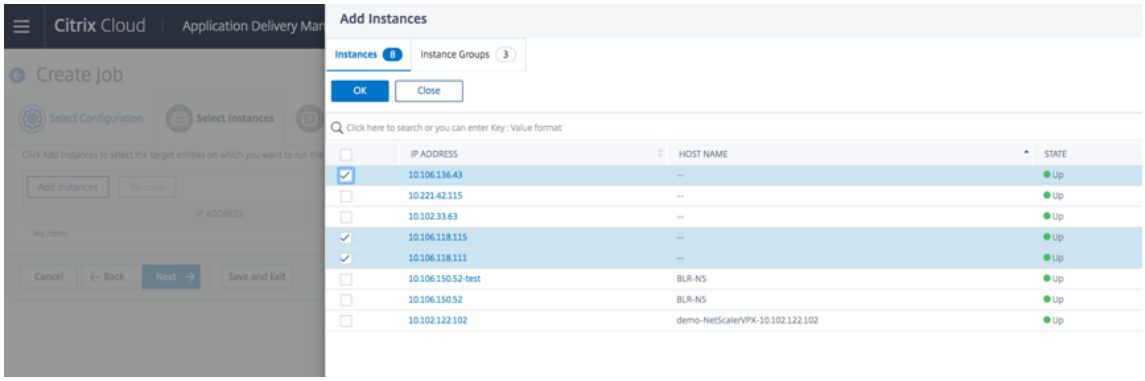


構成ジョブの作成

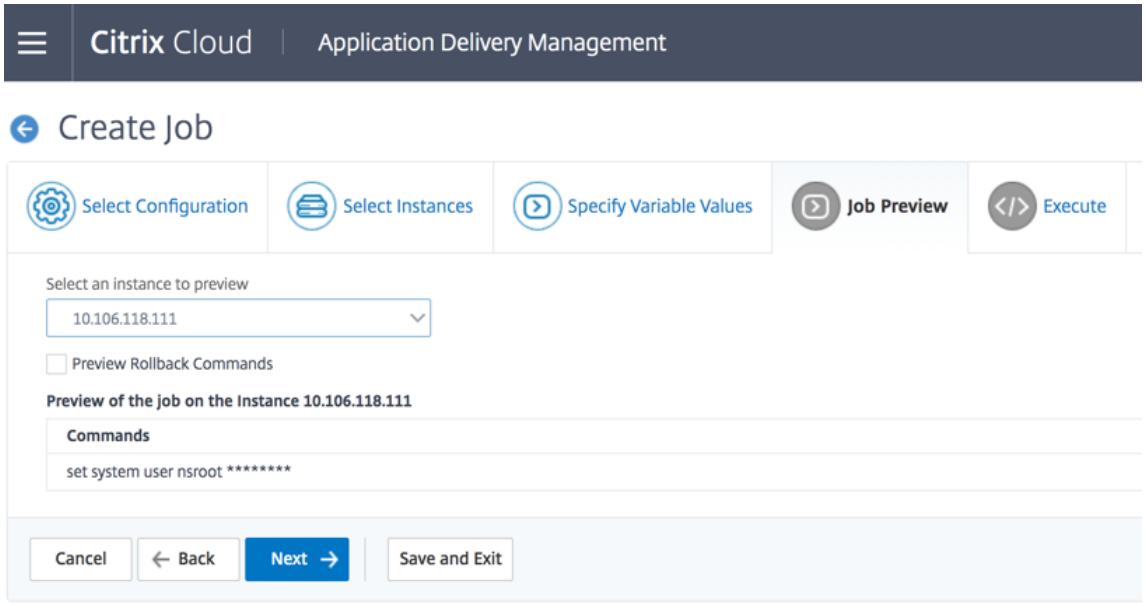
1. ADM GUI から、[ネットワーク**] > [**構成ジョブ] に移動します。
2. [**Create Job**] を選択し、新しい構成テンプレートの「+」アイコンをクリックします。[次へ] をクリックします。



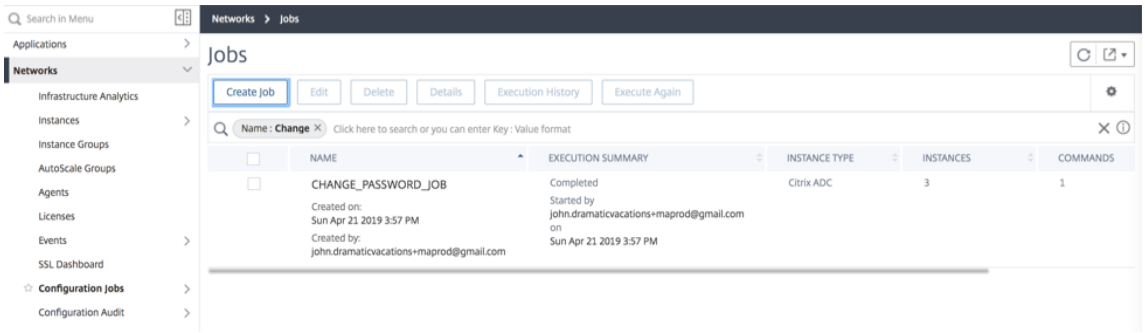
3. パスワードを変更する必要がある ADC インスタンス 1 つまたは複数のインスタンスを選択します。



4. **[** インスタンスの選択] ペインで、インスタンスを選択し、[次へ] をクリックします。
5. [変数値の指定] ペインでユーザー名とパスワードの値を指定し、[次へ] をクリックします。
6. [**Job Preview**] で、ADM が ADC インスタンスで実行する実際の CLI コマンドを確認します。プレビューが正常に表示される場合は、[次へ] をクリックします。



7. [**Execute**] ペインでは、ジョブをすぐに実行するか、後でスケジュールするかを選択できます。選択したすべてのインスタンスでジョブを並列実行するか、連続して実行するかを選択することもできます。実行の詳細を指定したら、[完了] を選択します。
8. 構成ジョブは、実行が成功したか失敗したかを示します。

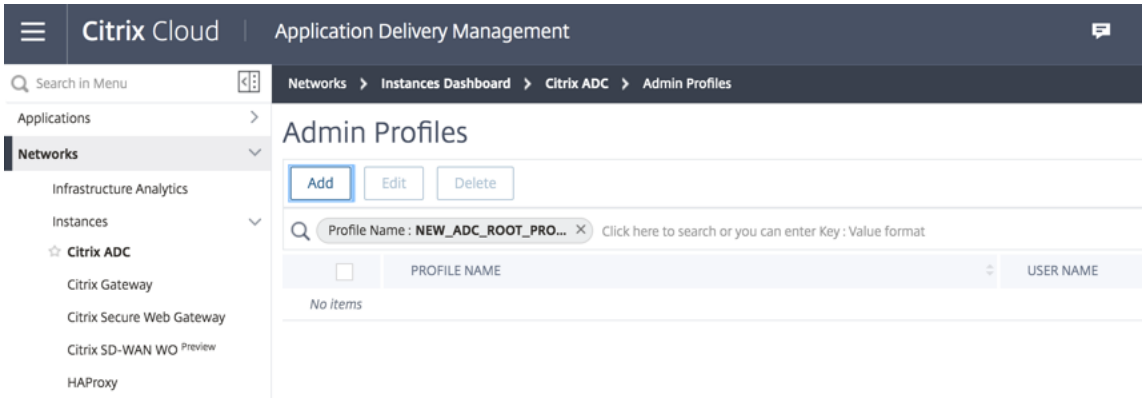


9. ジョブを選択し、[詳細] をクリックします。実行の詳細には、個々のインスタンスレベルでのステータスが表示されます。

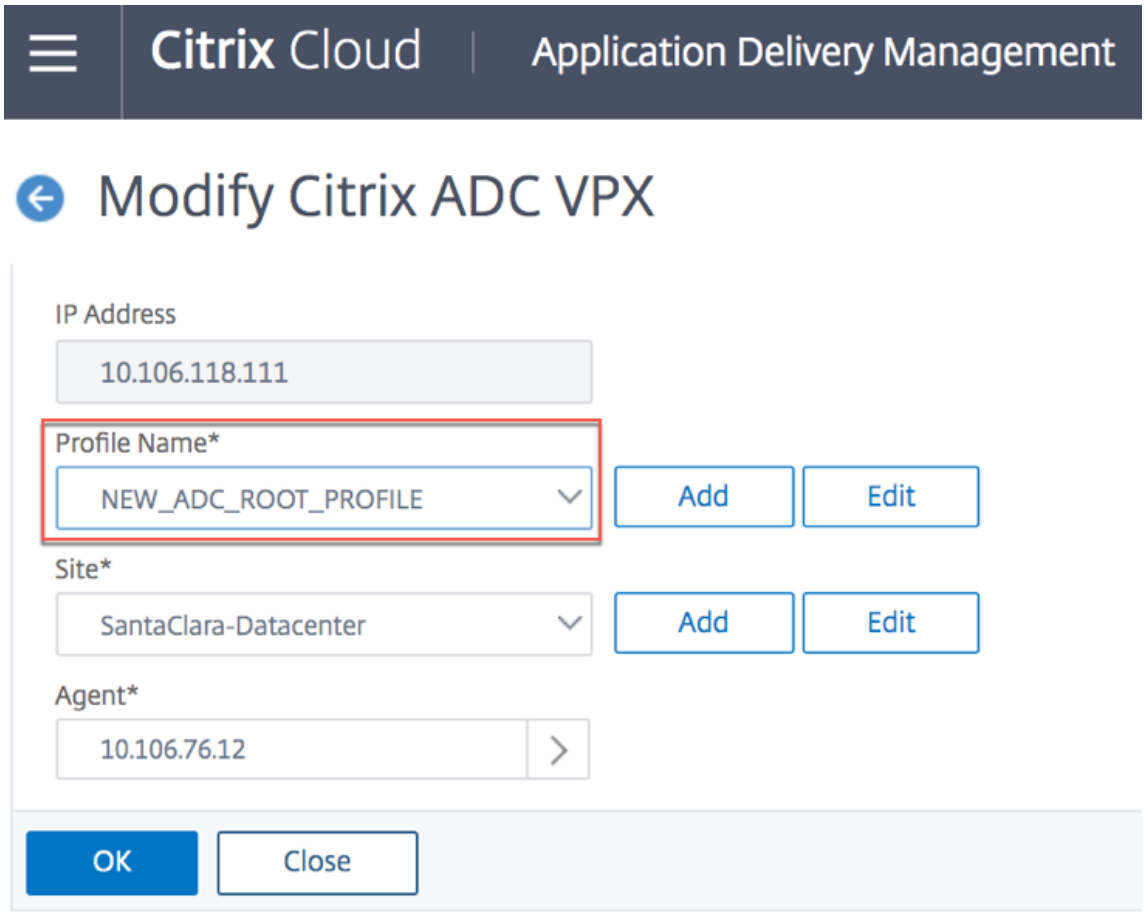
管理者プロファイルの変更

ADC パスワードを変更したら、インスタンスの管理プロファイルを追加および変更する必要があります。次の手順を実行します:

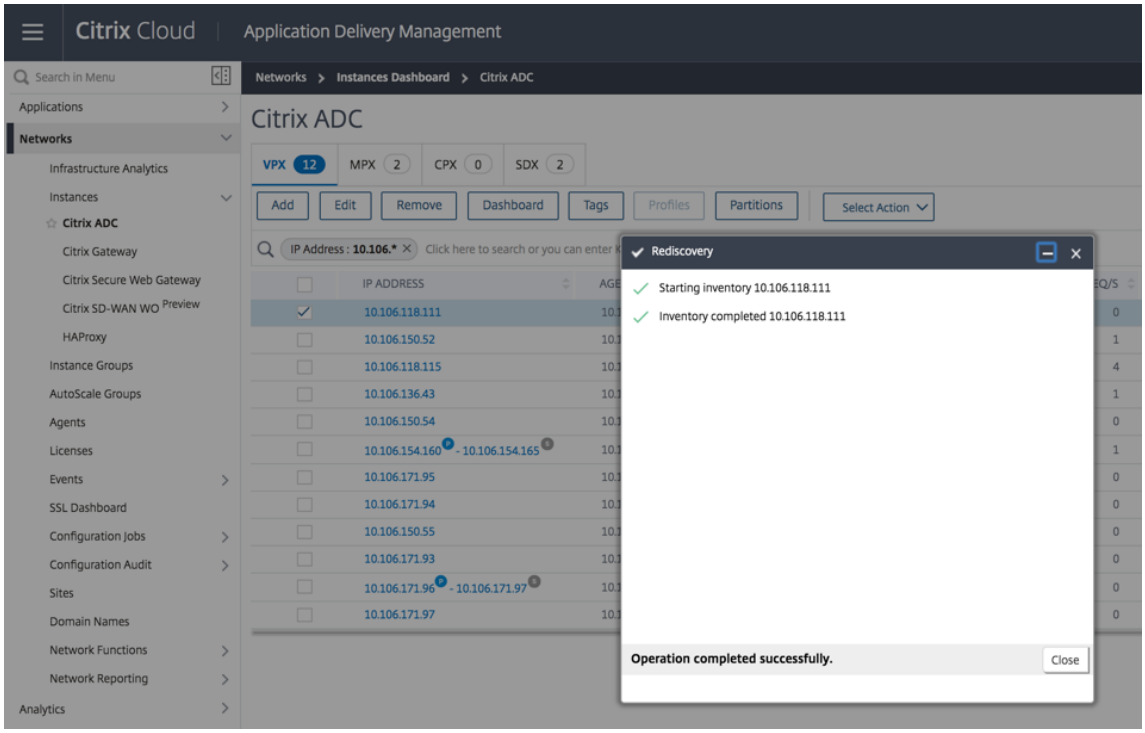
1. [ネットワーク**] > [**インスタンス**] > [Citrix ADC**] に移動します。
2. [プロファイル] をクリックして、すべての管理者プロファイルを表示します。
3. [追加] を選択して、管理者プロファイルを作成し、新しい Citrix ADC 資格情報を入力します。



4. 新しく作成したプロファイルが [管理者プロファイル] の下に表示されます。
5. ［ネットワーク］**>**［インスタンス］**>**［**Citrix ADC**］の順に選択します。パスワードが変更された Citrix ADC インスタンスを選択し、［編集］を選択します。
6. 新しく作成したプロファイル名を選択し、「**OK**」をクリックします。



7. インスタンスを再度選択して右クリックし、[**Rediscover**] を選択します。



パスワードが正常に変更されました。

SDX アプライアンスのパスワードの変更については、「Citrix ADC SDX ルートパスワードを変更する方法」を参照してください。

Citrix ADC SDX ルートパスワードを変更する方法

May 7, 2021

セキュリティ上の理由やパスワードローテーションポリシーの遵守のために、Citrix ADC アプライアンスの root パスワードを変更する必要がある場合があります。

このドキュメントでは、Citrix ADM クラウドで管理される Citrix ADC SDX アプライアンスのルートパスワードを変更するために必要な手順について説明します。

ADC パスワードを変更する場合は、その ADC に関連付けられている ADM 管理プロファイルを変更する必要があります。ADM 管理者プロファイルは、REST API、SSH、SCP、または ADC アプライアンスとの SNMP ベースの通信の ADC 認証情報を保持します。Citrix ADM は、管理者プロファイルを使用して、Citrix ADC SDX アプライアンスを管理します。

パスワードの変更

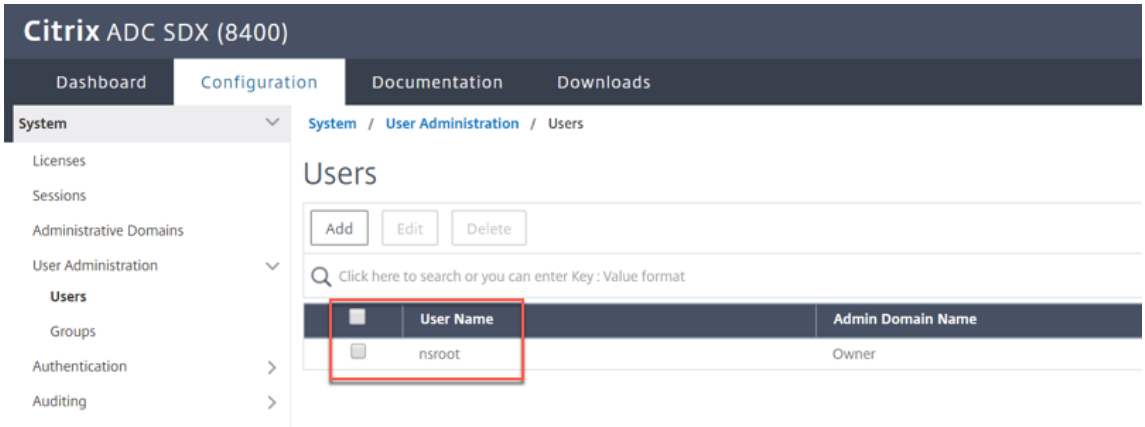
パスワードを変更するには、次の手順に従います。

- 手順 1. SDX 管理サービスの GUI から SDX パスワードを変更します。
- 手順 2. SDX に関連付けられている ADM 管理プロファイルを変更します。

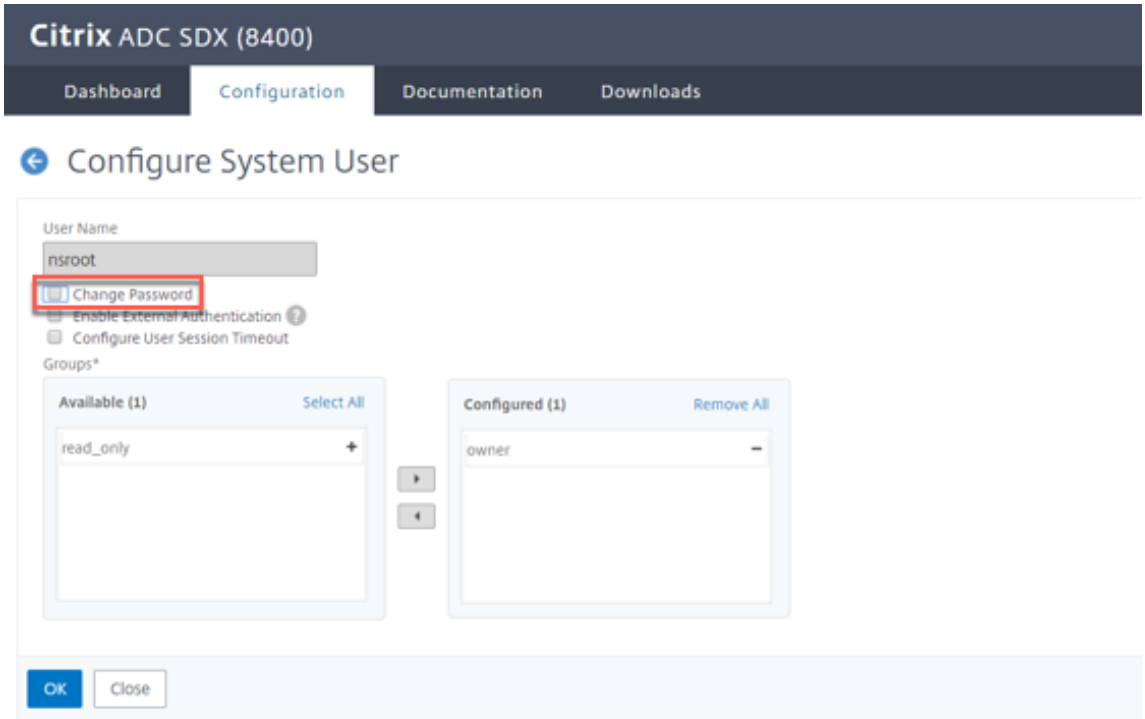
> 注:SDX アプライアンスが他のツールによって管理されている場合は、それらのツールの認証情報も変更する必要があります。

SDX 管理サービスの **GUI** から **SDX** パスワードを変更する

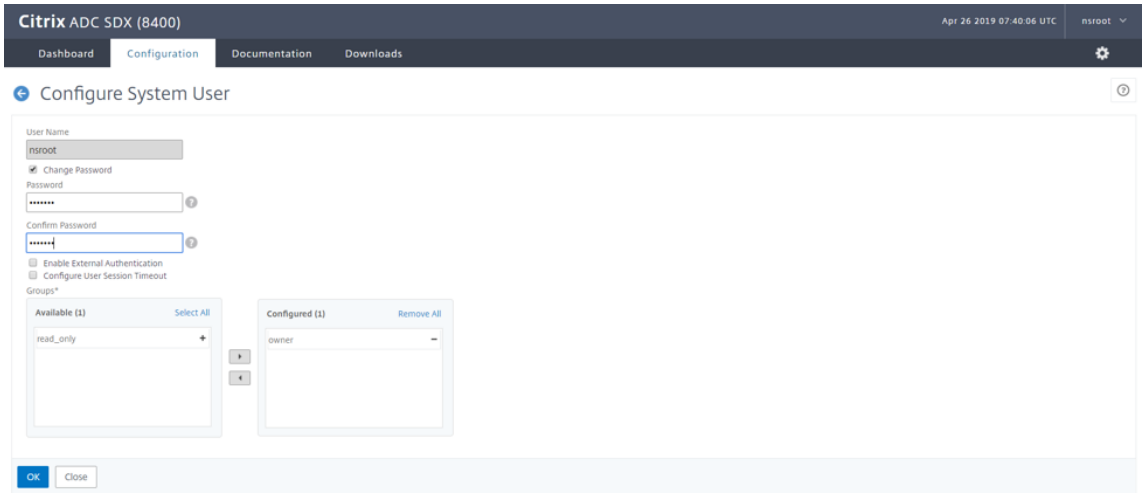
1. SDX 管理サービスから、「システム」**>**「ユーザー管理」**>**「ユーザー」に移動します。
2. パスワードを変更するユーザー名を選択し、[**Edit**] をクリックします。



3. [パスワードの変更] を選択します。



4. 新しいパスワードを入力し、「**OK**」をクリックします。

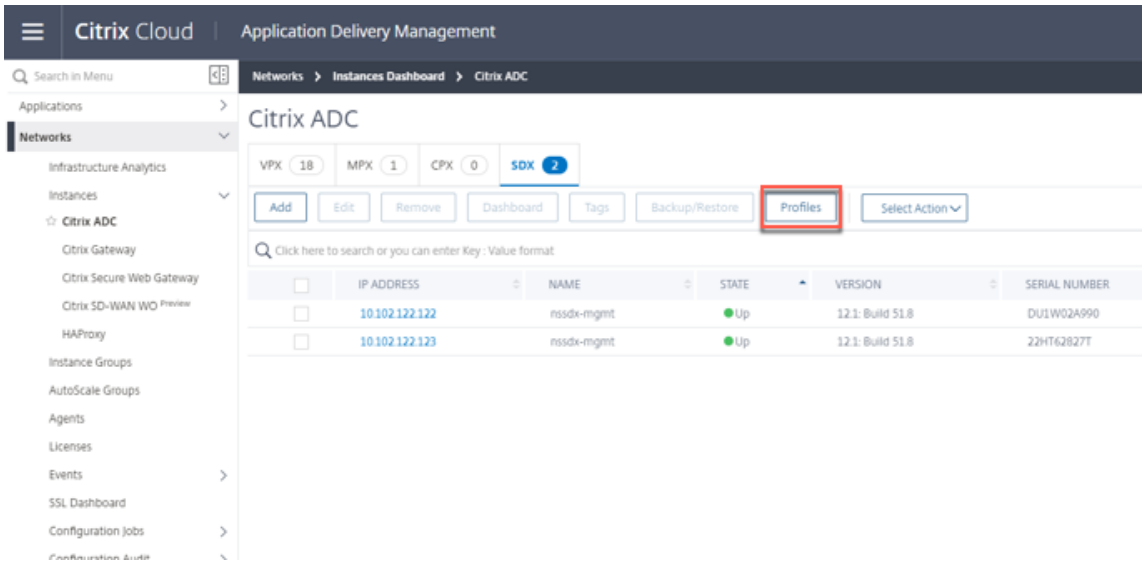


5. SDX パスワードが変更されました

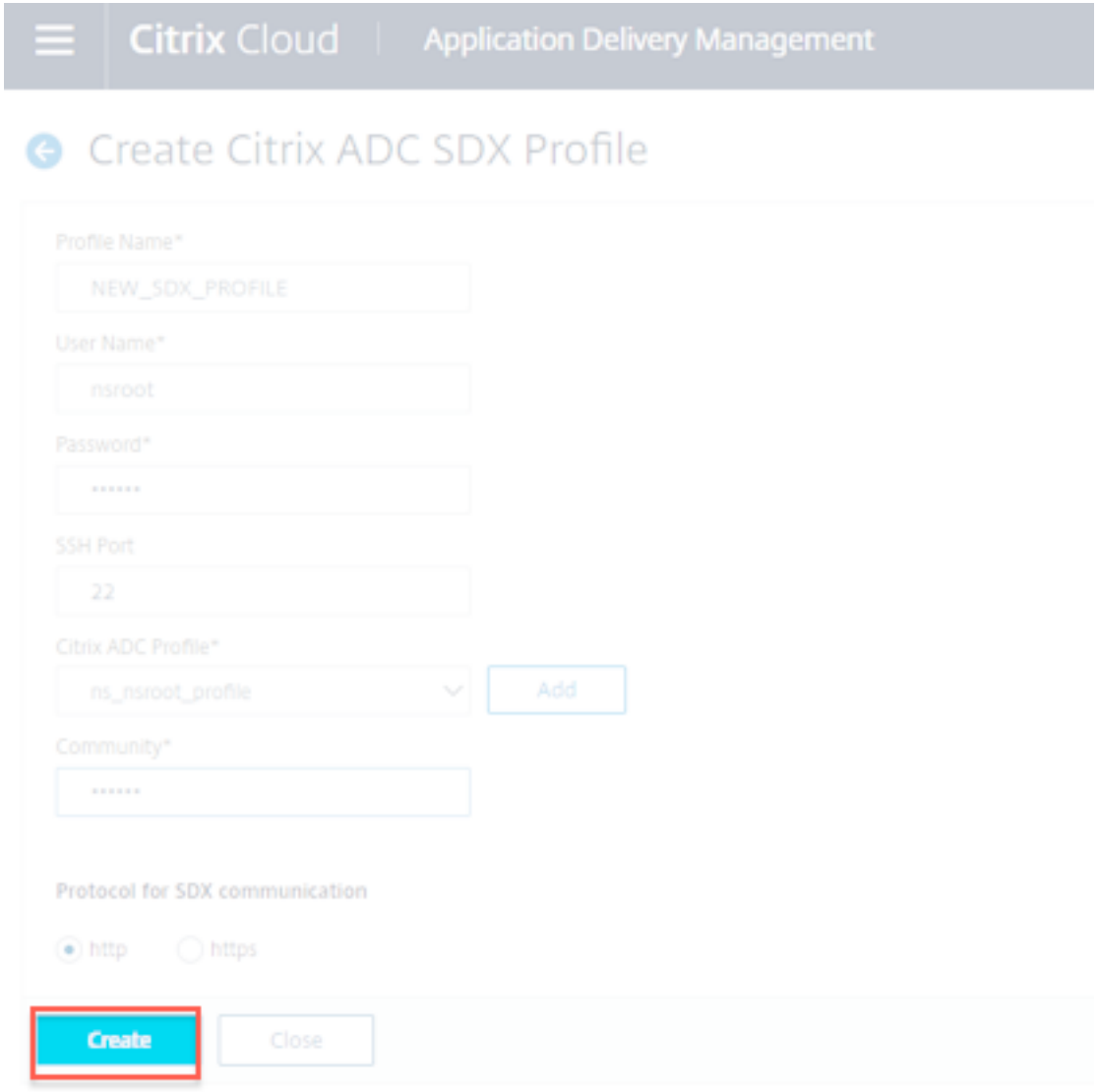
ADM 管理者プロファイルの変更

SDX パスワードを変更したら、インスタンスの管理プロファイルを変更する必要があります。次の手順を実行します:

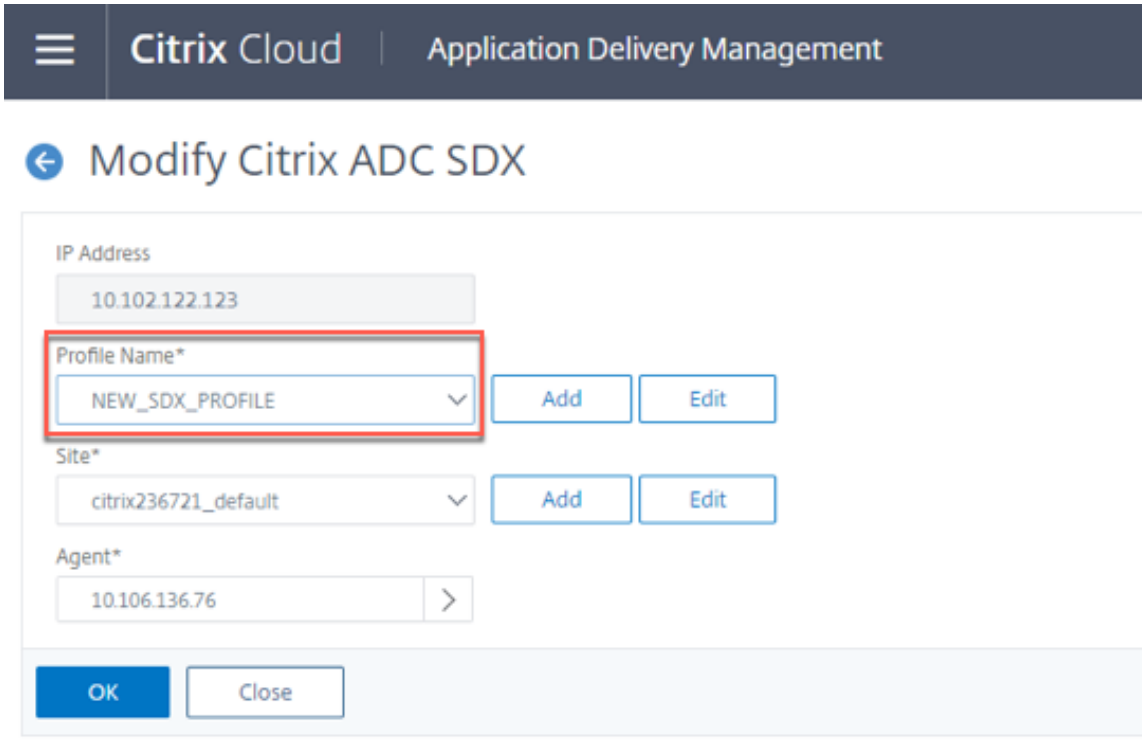
1. ネットワーク **>** インスタンスダッシュボード **> Citrix ADC > SDX** の順に移動します。
2. [プロファイル] を選択して、すべての管理者プロファイルを表示します。



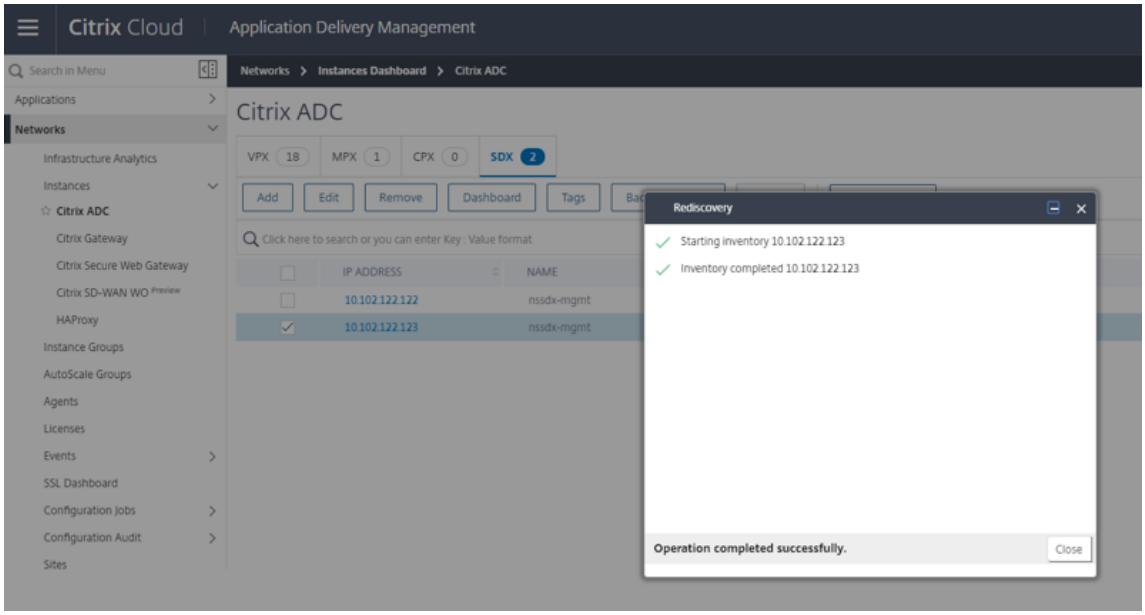
3. [追加] を選択して、管理者プロファイルを作成します。
4. 新しい Citrix ADC 資格情報を入力し、［作成］をクリックします。



5. 新しく作成したプロファイルが [管理者プロファイル] の下に表示されます。
6. **[** ネットワーク**] > [**インスタンス**] > [Citrix ADC] > [SDX**] の順に選択します。パスワードが変更されたインスタンスを選択し、[**Edit**] を選択します。
7. 新しく作成したプロファイル名を選択し、「**OK**」をクリックします。



8. インスタンスを再度選択して右クリックし、[**Rediscover**] をクリックします。



パスワードが正常に変更されました。

SDX アプライアンスのパスワードの変更については、「Citrix ADC MPX または VPX ルートパスワードを変更する方法」を参照してください。

イベント

May 7, 2021

Citrix ADM（Citrix ADC）インスタンスの IP アドレスが Citrix Application Delivery Management（Citrix ADM）に追加されると、Citrix ADM は NITRO 呼び出しを送信し、インスタンスがトラップまたはイベントを受信するためのトラップ先として暗黙的に追加します。

イベントは、管理対象 Citrix ADC インスタンスでのイベントまたはエラーの発生を表します。たとえば、システム障害や構成の変更が発生した場合、イベントが生成され、Citrix ADM サーバーに記録されます。Citrix ADM で受信したイベントは［イベントの概要］ページ（[ネットワーク］>［イベント]）に表示され、［イベントメッセージ］ページ（[ネットワーク］>［イベント］>［イベントメッセージ]）にすべてのアクティブなイベントが表示されます。

また、Citrix ADM は、インスタンスで生成されたイベントをチェックして、異なる重大度のアラームを形成し、メッセージとして表示します。一部のイベントには、即時対応が必要な場合があります。たとえば、システム障害は「Critical」イベントの重大度に分類でき、すぐに解決できます。

特定のイベントを監視するように規則を構成できます。ルールを使用すると、Citrix ADC インフラストラクチャ全体で生成されたさまざまなイベントを容易に監視できます。

特定の条件で規則を構成し、規則にアクションを割り当てることで、一連のイベントにフィルターを適用できます。生成されたイベントがルール内のフィルタ条件を満たすと、そのルールに関連付けられたアクションが実行されます。フィルタを作成できる条件は、重大度、Citrix ADC インスタンス、カテゴリ、障害オブジェクト、構成コマンド、メッセージです。

また、イベントについて、そのイベントが解決されるまで特定の間隔で通知を複数回表示するように設定することもできます。追加の対策として、特定の件名、ユーザーメッセージを使用してメールをカスタマイズし、添付ファイルをアップロードすることもできます。

イベントダッシュボードの使用

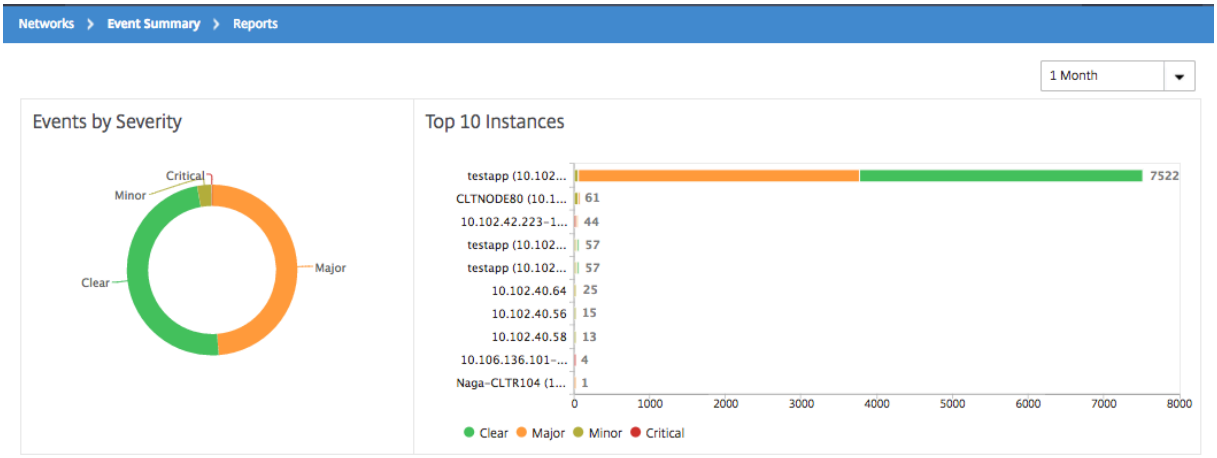
May 7, 2021

ネットワーク管理者は、Citrix Application Delivery Controller（Citrix ADC）インスタンスの構成変更、ログイン条件、ハードウェア障害、しきい値違反、エンティティの状態の変更などの詳細と、特定のインスタンスでのイベントとその重要度を表示できます。Citrix ADM（Citrix Application Delivery Management ADM）のイベントダッシュボードを使用して、すべての Citrix ADC インスタンスで重要なイベントの重要度の詳細について生成されたレポートを表示できます。

イベント・ダッシュボードで詳細を表示するには、次の手順に従います。

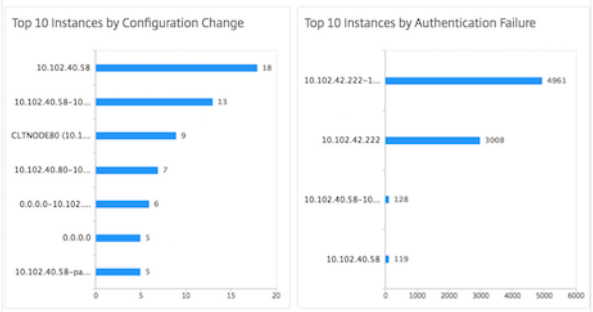
[ネットワーク] > [イベント] > [レポート] に移動します。

ダッシュボードの［Top 10 Devices］グラフには、各インスタンスで生成されたイベントの数に基づき、上位 10 個のインスタンスが表示されます。グラフのインスタンスをクリックすると、イベントの重大度の詳細を表示できます。

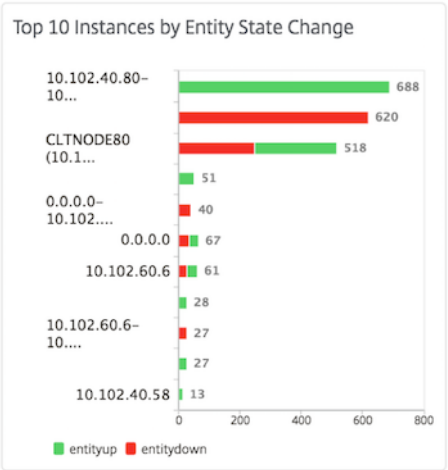


詳細を表示するには、Citrix ADC インスタンスタイプ（［ネットワーク］>［イベント］>［レポート］**>**［**Citrix ADC/Citrix ADC SDX/Citrix ADC SD-WAN WO**］）に移動して、次の項目を表示します。

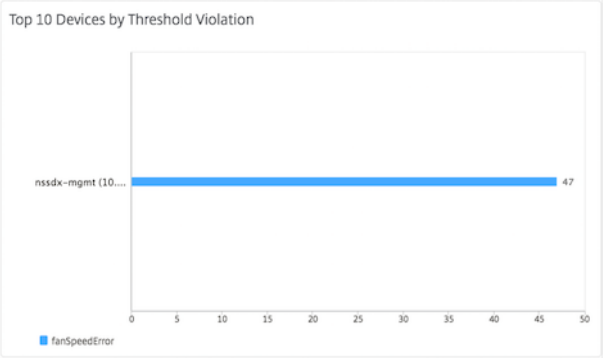
- ハードウェアエラー件数上位 10 デバイス
- 構成変更件数上位 10 デバイス
- 認証エラー件数上位 10 デバイス



- エンティティの状態変更件数上位 10 デバイス



- しきい値の超過件数上位 10 デバイス



このダッシュボードのレポートをエクスポートするには、次の手順に従います。

このページのレポートをエクスポートするには、このページの右上にある エクスポートアイコンをクリックします。[エクスポート] ページでは、次のいずれかの操作を実行できます。

1. [今すぐエクスポート] タブを選択します。レポートを PDF、JPEG、PNG、または CSV 形式で表示して保存します。
2. [スケジュールエクスポート] タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、電子メールまたは余裕期間メッセージでレポートを送信するには。

> 注
>
> - [毎週の繰り返し] を選択した場合は、レポートをスケジュールする平日を選択してください。
> - [毎月の繰り返し] を選択した場合は、レポートをスケジュールするすべての日をカンマで区切って入力します。

イベントのイベント期間を設定する

May 7, 2021

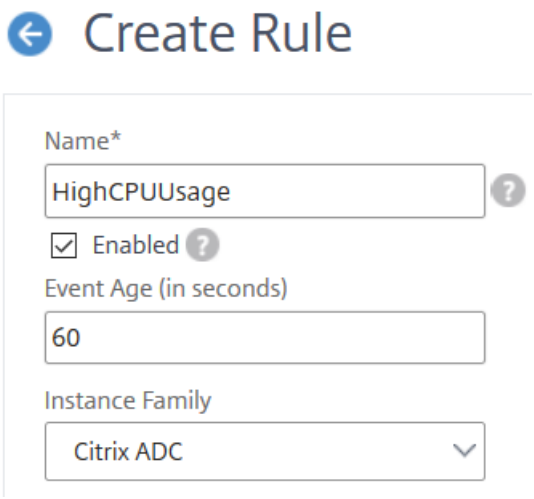
イベントの経過時間オプションを設定して、時間間隔（秒単位）を指定できます。Citrix ADM は、設定された期間までアプライアンスを監視し、イベントの経過時間が設定された期間を超えた場合にのみイベントを生成します。

> 注:
>
> イベント経過時間の最小値は 60 秒です。[**Event Age**] フィールドを空白のままにすると、イベントが発生した直後にイベントルールが適用されます。

たとえば、さまざまな ADC アプライアンスを管理し、仮想サーバーのいずれかが 60 秒以上ダウンしたときに電子メールで通知を受け取ることを考えます。必要なフィルタを使用してイベントルールを作成し、ルールのイベント経過時間を 60 秒に設定できます。その後、仮想サーバーが 60 秒以上ダウンしたままになるたびに、エンティティ名、ステータスの変更、時刻などの詳細が記載された電子メール通知を受信します。

Citrix ADM でイベントの経過期間を設定するには:

1. Citrix ADM で、［ネットワーク］>［イベント］>［ルール］の順に選択し、［追加］をクリックします。
2. ［**Create Rule**］ページで規則パラメーターを設定します。
3. イベント期間を秒数で指定します。



イベントフィルタをスケジュールする

May 7, 2021

ルールのフィルタを作成した後、生成されたイベントがフィルタ条件を満たすたびに Citrix Application Delivery Management（Citrix ADM）から通知を送信しないようにするには、毎日、毎週、毎月などの特定の時間間隔でのみトリガーされるようにフィルタをスケジュールできます。

たとえば、インスタンスの複数のアプリケーションを対象に、異なるタイミングでシステムメンテナンスのスケジュールを指定している場合、それらのインスタンスによって複数のアラームが生成される可能性があります。

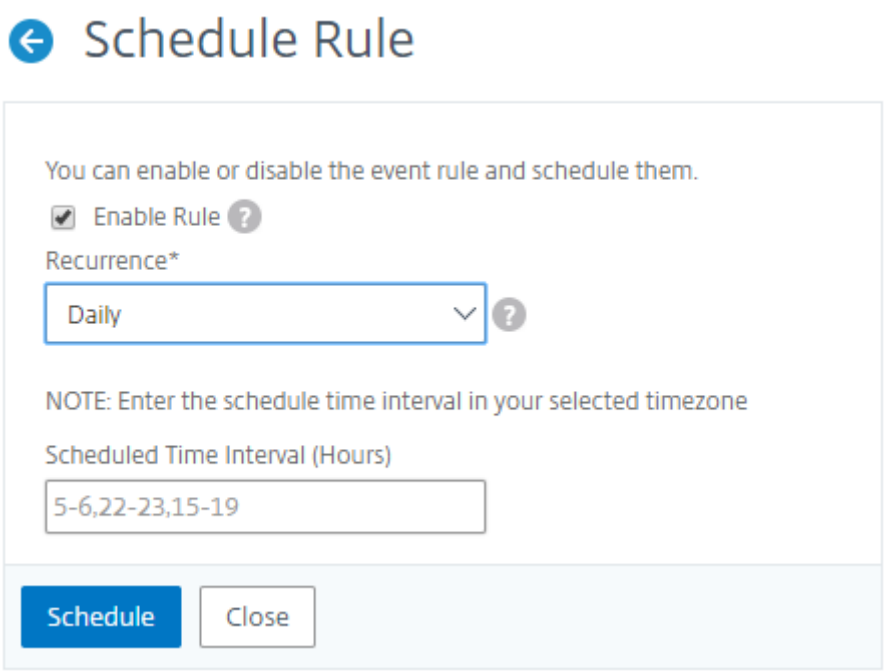
これらのアラームのフィルタを構成し、これらのフィルタで電子メール通知を有効にした場合、Citrix ADM がこれらのトラップを受信すると、サーバーは多数の電子メール通知を送信します。このようなサーバーによるメール通知の送信を特定期間に限定するには、フィルターにスケジュールを指定します。

Citrix ADM を使用してフィルタをスケジュールするには:

1. Citrix ADM で、［ネットワーク］>［イベント］>［ルール］に移動します。
2. スケジュールを指定するフィルターの対象となっている規則を選択し、［**View Schedule**］をクリックします。
3. ［**Scheduled Rule**］ページの［**Schedule**］をクリックして、次のパラメーターを指定します。
    - [ルールを有効にする] — スケジュールされたイベントルールを有効にするには、このチェックボックスをオンにします。

- **Recurrence** - 規則に適用するスケジュールの間隔です。
- [スケジュールされた時間間隔 **(**時間**)**]: 規則をスケジュールする時間 (24 時間形式を使用)。

4. [**Schedule**] をクリックします。



イベントに対して繰り返し電子メール通知を設定する

May 7, 2021

すべての重要なイベントに対処し、重要な電子メール通知が失われないようにするには、選択した条件を満たすイベントルールについて、電子メール通知を繰り返し送信することができます。たとえば、ディスク障害に関連するインスタンスに対してイベントルールを作成し、問題が解決するまで通知を受け取るには、それらのイベントに関する電子メール通知を繰り返し受信するように選択できます。

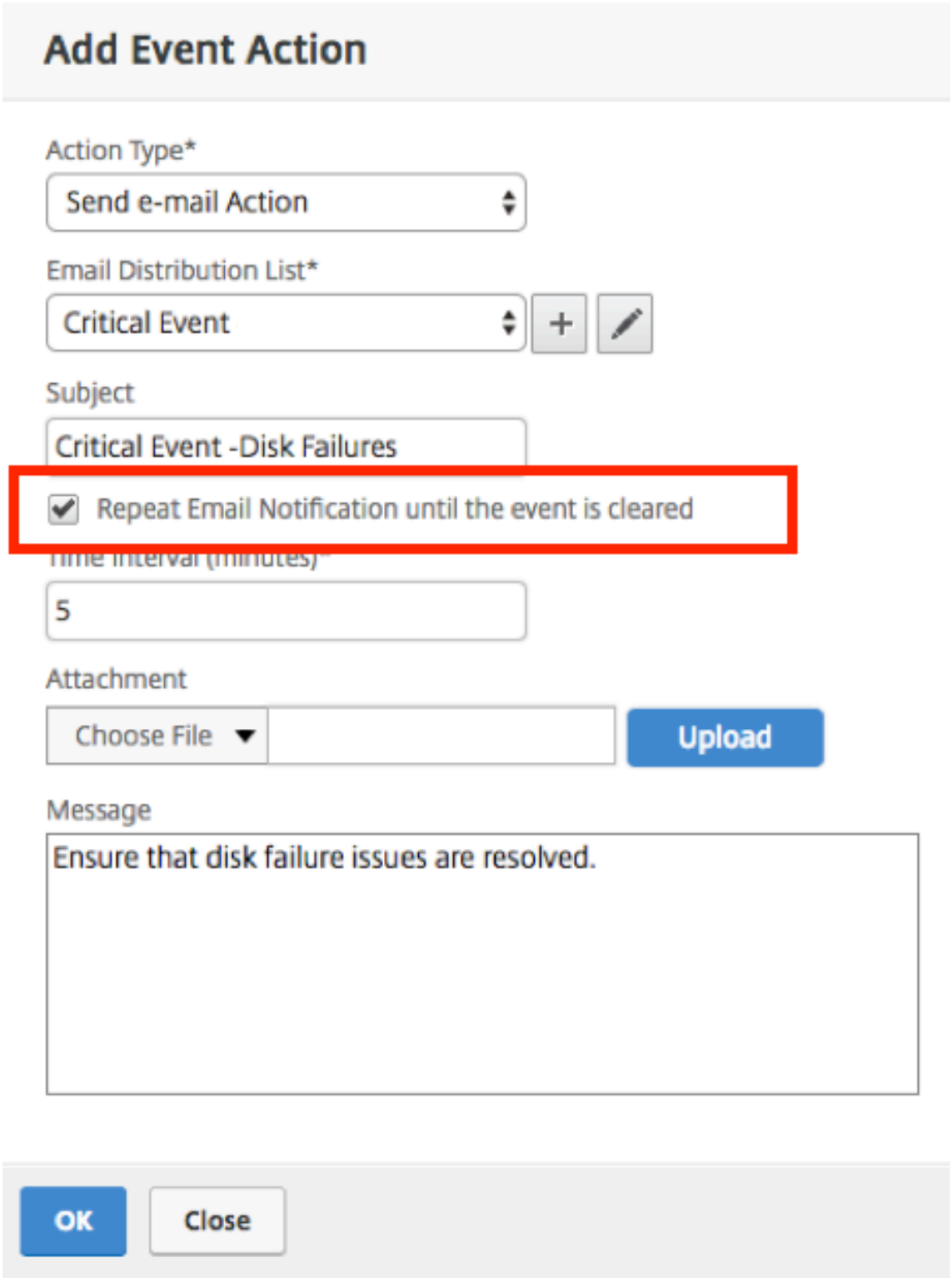
これらのメール通知は、受信者が通知を見たことを確認するか、イベント規則が解除されるまで、定義された間隔で繰り返し送信されます。

> 注
>
> イベントを自動的にクリアできるのは、同等の「クリア」トラップが設定され、Citrix ADC インスタンスから送信される場合のみです。
>
> イベントを手動でクリアするには、次の操作を行います。
>
> - [ネットワーク] **>** [イベント] **>** [イベントの概要] に移動し、[カテゴリ] を選択し、カテゴリでイベント

> を選択して [クリア] をクリックします。
> - または、[ネットワーク] **> [**イベント**] > [**イベントメッセージ] に移動します。インスタンスタイプを選択し、次のグリッドからイベントを選択し、[**Clear**] をクリックします。

Citrix ADM から繰り返し電子メール通知を設定するには:

1. Citrix ADM で、［ネットワーク］>［イベント］>［ルール］の順に選択し、［追加］をクリックしてルールを作成します。
2. ［**Create Rule**］ページで規則パラメーターを設定します。
3. [イベントルールのアクション] で、[アクションを追加] をクリックします。次に、[アクション ****** タイプ**]** ドロップダウンリストから **[**電子メールアクションの送信 **] を選択し、[電子メール配布リスト] を選択します。
4. 構成した規則と受信イベントが適合したときに、カスタマイズした件名とユーザーメッセージを追加し、添付ファイルをメールにアップロードすることもできます。
5. ［**Repeat Email Notification until the event is cleared**］チェックボックスをオンにします。



イベントを抑制する

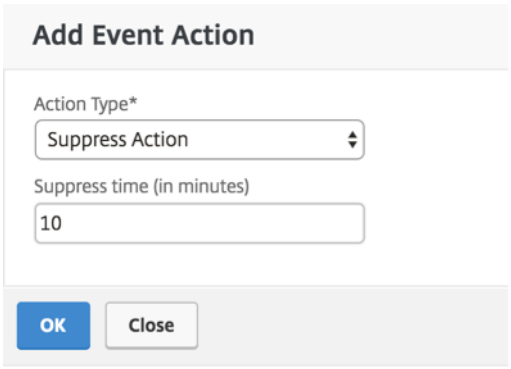
May 7, 2021

[**Suppress Action]** イベントアクションを選択すると、イベントを抑制またはドロップする期間を分単位で設定できます。最短で 1 分間イベントを非表示にできます。

> 注:
>
> 抑制時間を 0 分に設定することもできます。これは無限時間を意味します。期間を指定しない場合、Citrix ADM は抑制時間をゼロとみなし、期限切れになることはありません。

Citrix ADM を使用してイベントを抑制するには:

1. Citrix ADM で、［ネットワーク］>［イベント］>［ルール］に移動します。
2. **[** ルールの作成] ページまたは [規則の設定] ページに移動します。規則を作成するために必要なすべてのパラメーターを指定します。
3. ［**Event Rule Actions**］の［**Add Action**］をクリックして、イベントの通知アクションを割り当てます。
4. **[** イベントアクションの追加**]** ページで、**[** アクションの種類**]** ドロップダウンメニューから **[**アクションの抑制**]** を選択し、イベントを抑制する必要がある期間を分単位で指定します。
5. ［**OK**］をクリックします。



イベントルールの作成

May 7, 2021

特定のイベントを監視するように規則を構成できます。ルールを使用すると、インフラストラクチャ全体で生成されたイベントを容易にフィルタリングできます。

特定の条件で規則を構成し、規則にアクションを割り当てることで、一連のイベントにフィルターを適用できます。生成されたイベントがルール内のフィルタ条件を満たすと、そのルールに関連付けられたアクションが実行されます。

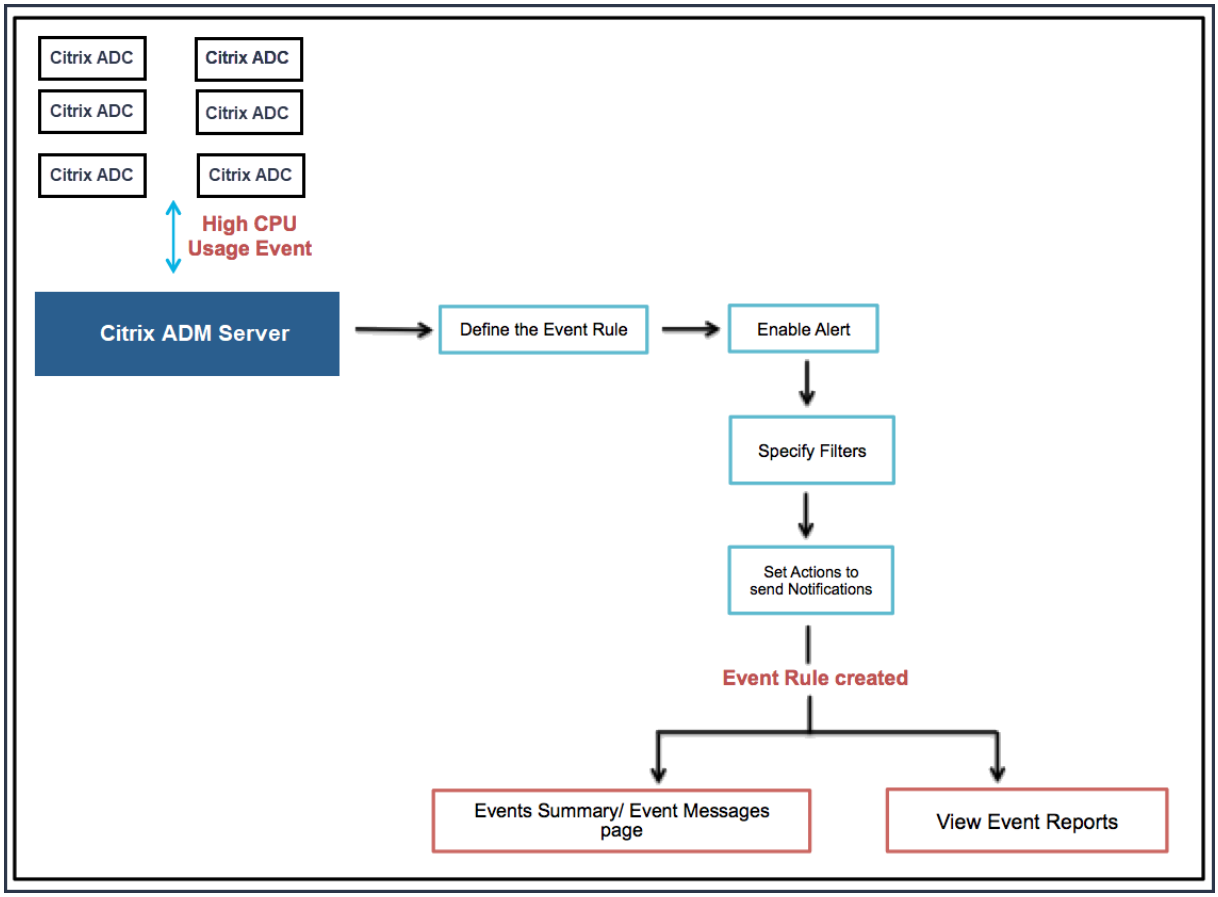
フィルターを作成できる条件は、重大度、Citrix Application Delivery Controller（Citrix ADC）インスタンス、カテゴリ、障害オブジェクト、構成コマンド、メッセージです。

次のアクションをイベントに割り当てられます。

- 電子メール送信アクション：フィルタ条件に一致するイベントについて電子メールを送信します。
- トラップ送信アクション：外部トラップ宛先に SNMP トラップを送信または転送します。
- コマンドアクションの実行: 着信イベントが設定されたルールを満たしたときにコマンドを実行します。
- **[** ジョブアクションの実行]: 指定したフィルタ条件に一致するイベントに対してジョブを実行します。
- 抑制処理: 特定の期間のイベントのドロップを抑制します。
- **Slack** 通知を送信: 設定済みの Slack チャンネルで、フィルタ条件に一致するイベントに関する通知を送信します。
- **PagerDuty** 通知の送信：フィルタ条件に一致するイベントの PagerDuty 構成に基づいてイベント通知を送信します。
- **ServiceNow** 通知の送信: フィルタ条件に一致するイベントの ServiceNow インシデントを自動生成します。

詳しくは、「イベントルールアクションの追加」を参照してください。

イベントが解決されるまで指定した間隔で通知が再送信されるように設定することもできます。また、特定の件名、ユーザーメッセージ、および添付ファイルを使用して電子メールをカスタマイズすることもできます。



たとえば、管理者として、ADC インスタンスの「高い CPU 使用率」イベントを監視し、停止につながる可能性があります。通知を受信するには、次のいずれかのアクションを実行できます。

- インスタンスを監視するルールを作成します。また、そのようなイベントが発生したときに通知を受け取るアクションをルールに追加します。
- 特定の間隔でインスタンスを監視するルールをスケジュールします。したがって、そのようなイベントがその間隔内に発生すると、通知を受け取ります。

イベント規則の構成では以下の作業を行います。

1. 規則を定義する
2. 規則の検出対象イベントの重要度を選択する
3. イベントのカテゴリを指定する
4. ルールを適用する Citrix ADC インスタンスの指定
5. 障害オブジェクトの選択
6. 詳細フィルタの指定
7. 規則でイベントが検出された場合に実行するアクションを指定する

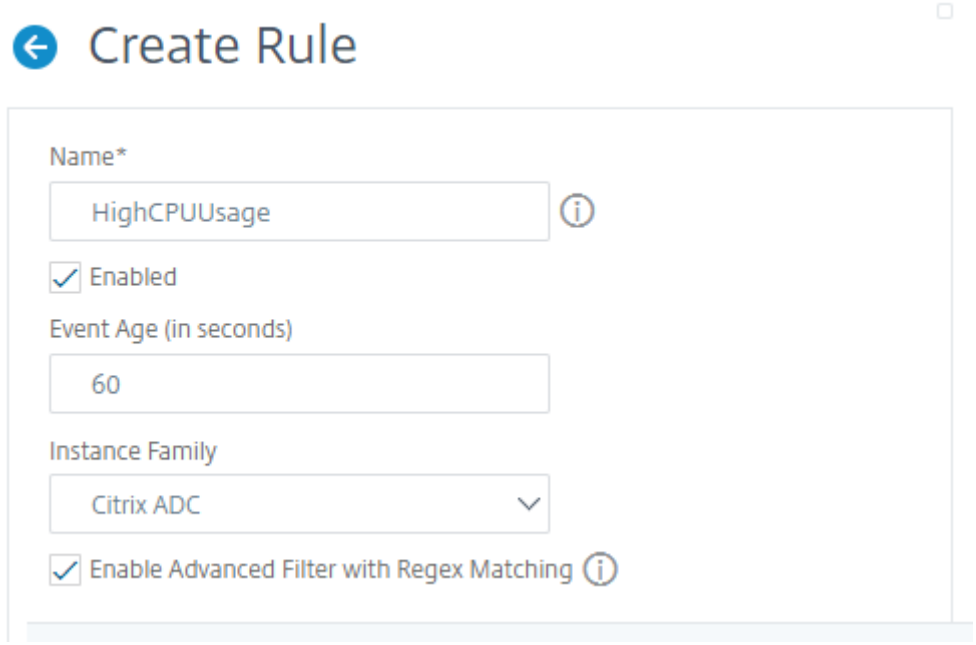
ステップ **1-**イベントルールを定義する

[ネットワーク] > [イベント] > [ルール] に移動し、[追加] をクリックします。ルールを有効にする場合は、[ルールを有効にする] チェックボックスをオンにします。

[イベントの経過時間] オプションを設定して、Citrix ADM がイベントルールを更新するまでの時間間隔（秒単位）を指定できます。

> 注:
>
> イベント経過時間の最小値は 60 秒です。[**Event Age**] フィールドを空白のままにすると、イベントが発生した直後にイベントルールが適用されます。

上記の例に基づいて、Citrix ADC インスタンスで 60 秒以上の「高い CPU 使用率」イベントが発生するたびに、メールで通知を受け取ることができます。イベントの経過時間を 60 秒に設定することで、Citrix ADC インスタンスで 60 秒以上の「高い CPU 使用率」イベントが発生するたびに、イベントの詳細が記載された電子メール通知を受け取ることができます。



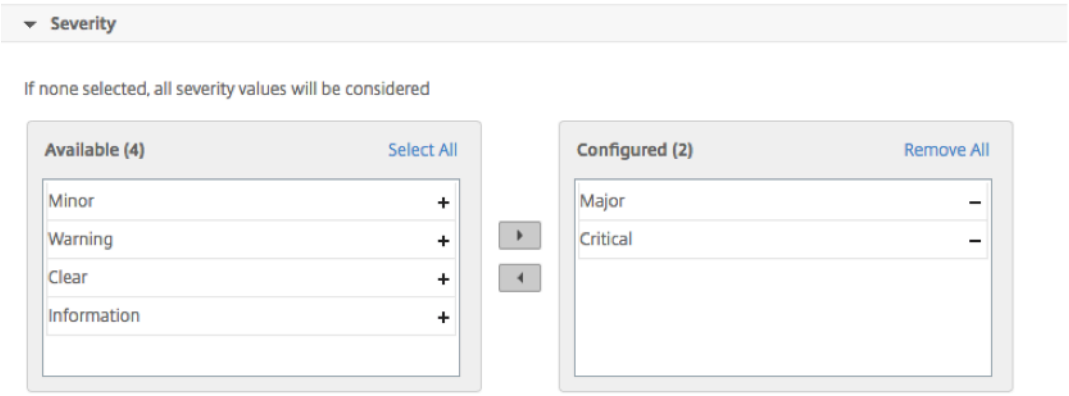
また、インスタンスファミリーでイベントルールをフィルタリングして、Citrix ADM がイベントを受信する Citrix ADC インスタンスを追跡することもできます。

アスタリスク（*）パターンマッチング以外の正規表現を含める場合は、「正規表現マッチングで高度なフィルタを有効にする」を選択します。

ステップ **2-**イベントの重要度を選択する

デフォルトの重要度設定を使用したイベント規則を作成できます。[重要度] には、イベントルールを追加するイベントの現在の重大度を指定します。

重要度レベルは、Critical、Major、Minor、Warning、Clear、Information で定義できます。

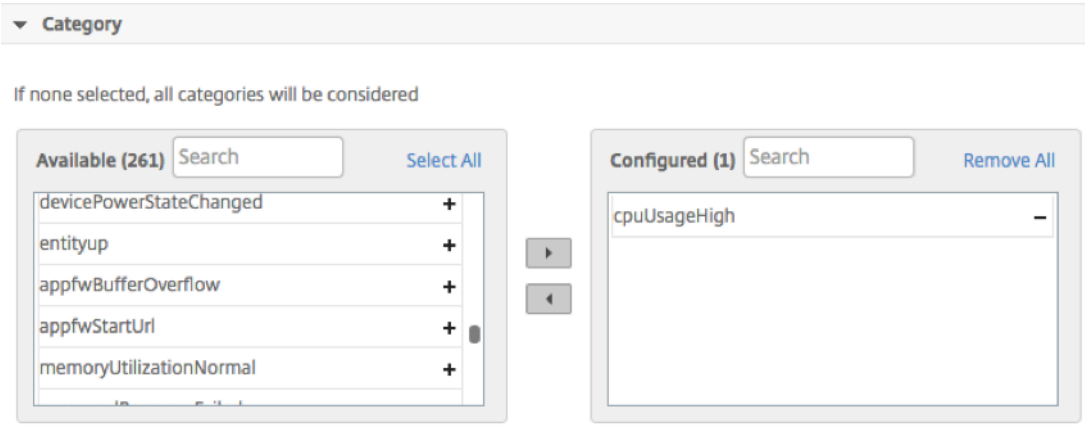


> 注
>
> 汎用イベントとアドバンス固有のイベントの両方について、重大度を設定できます。Citrix ADM で管理されている Citrix ADC インスタンスのイベントの重要度を変更するには、［ネットワーク］>［イベント］>［イベント設定］に移動します。イベントの重大度を設定する カテゴリを選択し、[Configure Sever **ity**] をクリックします。新しい重大度レベルを割り当てて、[**OK**] をクリックします。

ステップ **3-**イベントカテゴリの指定

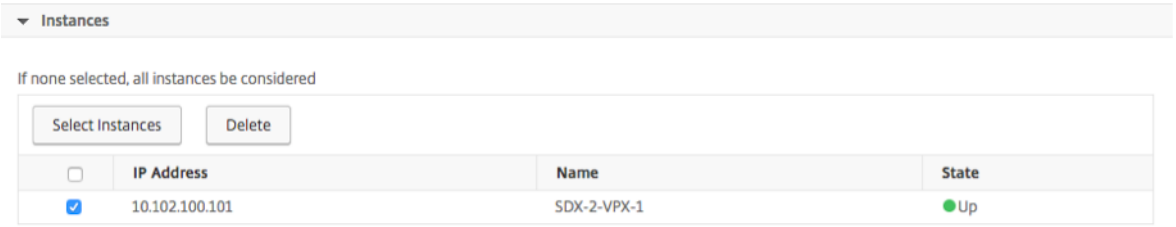
Citrix ADC インスタンスによって生成されるイベントのカテゴリを指定できます。すべてのカテゴリは、Citrix ADC インスタンスに作成されます。これらのカテゴリは、イベントルールの定義に使用できる Citrix ADM にマッピングされます。考慮するカテゴリを選択し、「使用可能」(Available) テーブルから「構成済み」(構成済み) テーブルに移動します。

上記の例では、表示されたテーブルからイベントカテゴリとして「cpuusageHigh」を選択する必要があります。



ステップ **4-Citrix ADC** インスタンスの指定

イベントルールを定義する Citrix ADC インスタンスの IP アドレスを選択します。[インスタンス] セクションで、[インスタンスを選択] をクリックします。[**Select Instances]** ページで、インスタンスを選択し、[**Select**] をクリックします。



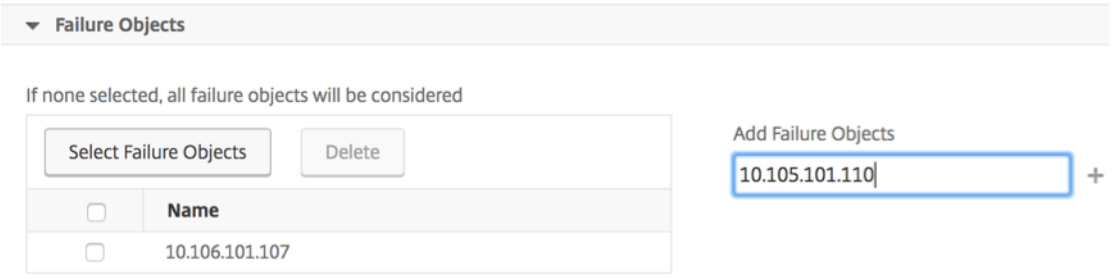
ステップ **5-**障害オブジェクトの選択

表示されたリストから障害オブジェクトを選択するか、イベントが生成された障害オブジェクトを追加できます。正規表現を指定して、失敗オブジェクトを追加することもできます。指定された正規表現に応じて、失敗オブジェクトは自動的にリストに追加されます。エラーオブジェクトは、イベント生成の対象となるエンティティのインスタンスまたはカウンターです。

> 重要
>
> ：正規表現を使用して失敗オブジェクトを一覧表示するには、「手順 **1**で正規表現マッチングで高度なフィルタを有効にする」を選択します。

障害オブジェクトは、イベントの処理方法に影響し、通知されたとおりに正確な問題を反映します。このフィルターを使用すると、障害オブジェクトの問題をすばやく追跡し、問題の原因を特定できます。たとえば、ユーザーがログインの問題がある場合、ここでの failure オブジェクトは、`nsroot`のようなユーザー名またはパスワードです。

このリストには、すべてのしきい値関連のイベントではカウンター名、すべてのエンティティ関連のイベントではエンティティ名、証明書関連のイベントでは証明書名などが含まれます。

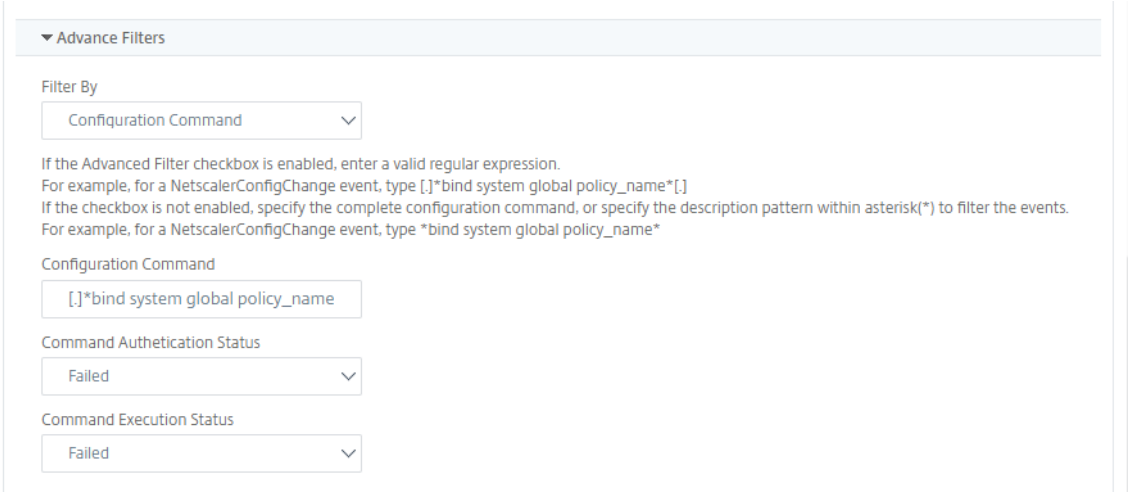


ステップ **6-**高度なフィルタを指定する

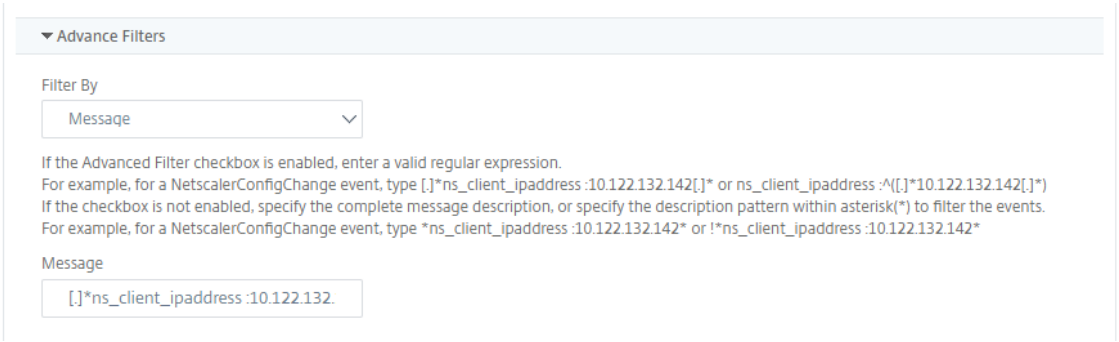
イベント規則は以下の基準によりフィルタリングできます。

- 構成コマンド -完全な構成コマンドを指定することも、正規表現を指定してイベントをフィルタリングすることもできます。

さらに、コマンドの認証ステータスと、またはその実行ステータスによって、イベントルールをフィルタリングできます。たとえば、NetscalerConfigChange eventの場合は、[.]*bind system global policy_name[.]*と入力します。



- メッセージ-メッセージの完全な説明を指定することも、正規表現を指定してイベントをフィルタリングすることもできます。
  たとえば、NetscalerConfigChangeイベントの場合は、[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :^([.]*10.122.132.142[.]*)と入力します。



> 重要
>
> : アスタリスク (*) パターンマッチング以外の正規表現を使用して構成コマンドおよびメッセージをフィルタリングするには、手順 1で **Enable Advanced Filter with Regex Matching** を選択します。

ステップ **7-**イベントルールアクションを追加する

イベント規則アクションを追加して、イベントに対する通知アクションを割り当てることができます。これらの通知は、イベントが上記で設定した定義されたフィルター条件を満たす場合に送信または実行されます。追加できるイベントアクションは以下のとおりです。

- 電子メール送信アクション

- Send Trap Action
- Run Command Action
- ジョブアクションの実行
- Suppress Action
- Slack 通知を送信
- PagerDuty 通知を送信
- サービス通知の送信

電子メールイベントルールのアクションを設定するには

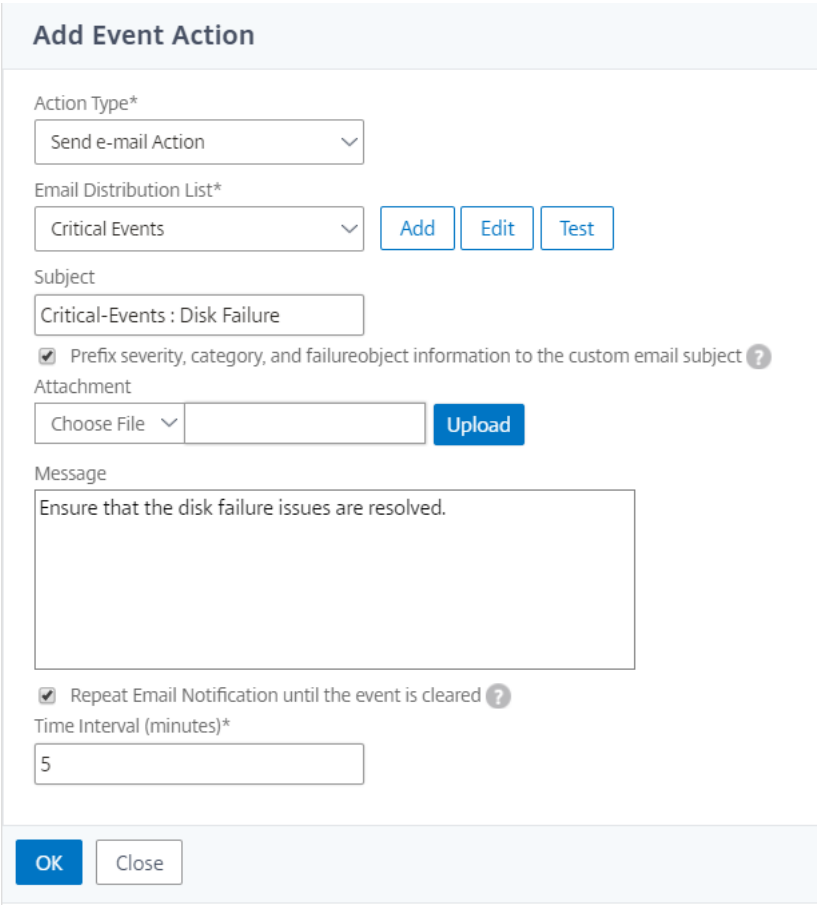
[**Send email Action**] を選択すると、イベントが定義されたフィルタ条件を満たすと、電子メールがトリガーされます。メールサーバーまたはメールプロファイルの詳細を指定して電子メール配布リストを作成するか、以前に作成した電子メール配布リストを選択できます。

Citrix ADM では多数の仮想サーバーを構成しているため、毎日多数の電子メールを受信することがあります。電子メールには、イベントの重大度、イベントのカテゴリ、および失敗オブジェクトに関する情報を提供するデフォルトの件名行があります。ただし、件名には、これらのイベントが発生した仮想サーバーの名前に関する情報は含まれません。これで、影響を受けるエンティティの名前、つまり失敗オブジェクトの名前などの追加情報を含めるオプションが追加されました。

また、カスタマイズされた件名行とユーザーメッセージを追加し、受信イベントが設定されたルールと一致したときに電子メールに添付ファイルをアップロードすることもできます。

イベント通知の電子メールを送信するときに、テスト電子メールを送信して、構成済みの設定をテストすることができます。「テスト」ボタンで、電子メールサーバー、関連付けられた分散リストなどの設定を行った後、テスト電子メールを送信できるようになりました。この機能により、設定が正常に動作することが保証されます。

また、[イベントがクリアされるまで電子メール通知を繰り返す**]** チェックボックスをオンにして、選択した条件を満たすイベントルールに対して **E** メール通知を繰り返し送信することで、重要なイベントがすべて処理され、重要な電子メール通知が失われないようにすることもできます。たとえば、ディスク障害に関連するインスタンスに対してイベントルールを作成し、問題が解決するまで通知を受け取るには、それらのイベントに関する電子メール通知を繰り返し受信するように選択できます。



トラップイベントルールアクションを設定するには

[**Send Trap Action**] イベントアクションタイプを選択すると、SNMP トラップは外部トラップ宛先に送信または転送されます。トラップ同報リスト（またはトラップ宛先およびトラッププロファイルの詳細）を定義することにより、イベントが定義されたフィルタ基準を満たしたときに、トラップメッセージが特定のトラップリスナーに送信されます。

[コマンドを実行**]** アクションを設定するには

［コマンドアクションの実行］イベントアクションを選択すると、特定のフィルタ条件に一致するイベントに対して Citrix ADM で実行できるコマンドまたはスクリプトを作成できます。

[コマンドアクションの実行] スクリプトには、次のパラメータを設定することもできます。

パラメーター	説明
$source	このパラメーターは、受信したイベントのソース IP アドレスに相当します。

$category	このパラメーターは、フィルターのカテゴリで定義されているトラップのタイプに対応します
$entity	このパラメーターは、イベント生成の対象となるエンティティのインスタンスまたはカウンターに相当します。このパラメーターには、しきい値関連のイベントではカウンター名、エンティティ関連のイベントではエンティティ名、すべての証明書関連のイベントでは証明書名が含まれます。
$severity	このパラメーターは、イベントの重要度に相当します。
$failureobj	エラーオブジェクトはイベントの処理方法に影響を与え、通知されたとおりの問題がエラーオブジェクトに反映されるようにします。このオブジェクトを使用すると、単にイベントをありのままレポートするのではなく、問題を素早く突き止めてエラーの原因を特定することができます。

> 注
>
> コマンドの実行中、これらのパラメータは実際の値に置き換えられます。

たとえば、負荷分散仮想サーバーのステータスが「ダウン」の場合に、run command アクションを設定するとします。管理者は、別の仮想サーバーを追加することで、迅速な回避策を提供することを検討できます。Citrix ADM では、次の操作を実行できます。

- スクリプト (.sh) ファイルを記述します。

  次に、サンプルスクリプト (.sh) ファイルを示します。

```
#!/bin/sh
source=$1
failureobj=$2
payload='{
"params":{
"warning":"YES" }
,"lbvserver":{
"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","
   port":"80","td":"","m":"IP","state":"ENABLED","rhistate":"
   PASSIVE","appflowlog":"ENABLED","
bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":"" }
 }
'
```



```
12  url="http://$source/nitro/v1/config/lbvserver"
13  curl --insecure -basic -u nsroot:nsroot -H "Content-type:
        application/json" -X POST -d $payload $url
14
15  <!--NeedCopy-->
```

- .sh ファイルを Citrix ADM エージェント上の任意の永続的な場所に保存します。たとえば、/varなどです。
- ルールの条件が満たされたときに実行する Citrix ADM 内の.sh ファイルの場所を指定します。

新しい仮想サーバーを作成するための「コマンドの実行」アクションを設定するには、次の手順で行います。

1. 規則を定義する
2. イベントの重要度を選択します。
3. イベントカテゴリ エンティティの選択
4. 仮想サーバーが構成されているインスタンスを選択します。
5. 仮想サーバの障害オブジェクトを選択または作成します。
6. [イベントルールアクション] で、[アクションの追加] をクリックし、[アクションの ** 種類] リストから [コマンドアクションの実行 **] を選択します。
7. [コマンド実行リスト] で、[追加] をクリックします。

   [コマンド配布リストの作成] ページが表示されます。

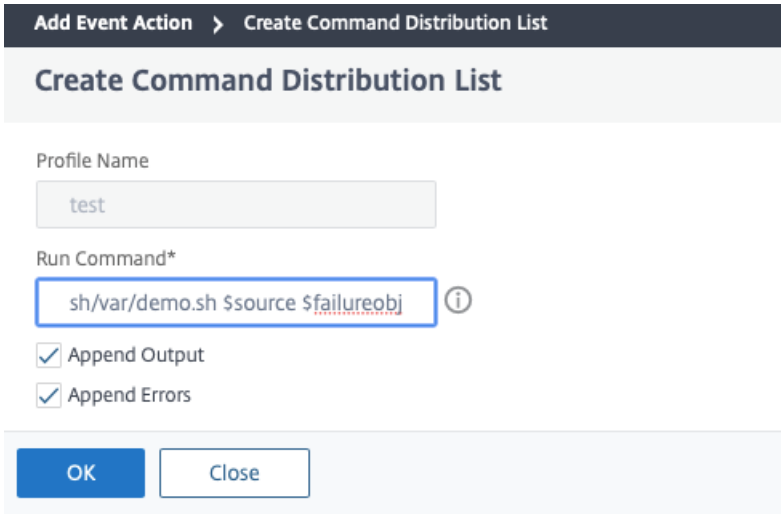
   a)「プロファイル名」で、任意の名前を指定します。

   b) [コマンドの実行] で、スクリプトを実行する Citrix ADM エージェントの場所を指定します。例: /sh/var/demo.sh $source $failureobj。

   c)「出力を追加」と「エラーを追加」を選択します。

   > 注
   >
   > コマンドスクリプトの実行時に生成された 出力と エラー（存在する場合）を **Citrix ADM** サーバーのログファイルに保存する場合は、[**Append** Output] オプションと [Append Errors] オプションを有効にできます。これらのオプションを有効にしないと、Citrix ADM はコマンドスクリプトの実行中に生成されたすべての出力とエラーを破棄します。

   d) [作成] をクリックします。
8. [イベントアクションの追加] ページで、[**OK**] をクリックします。

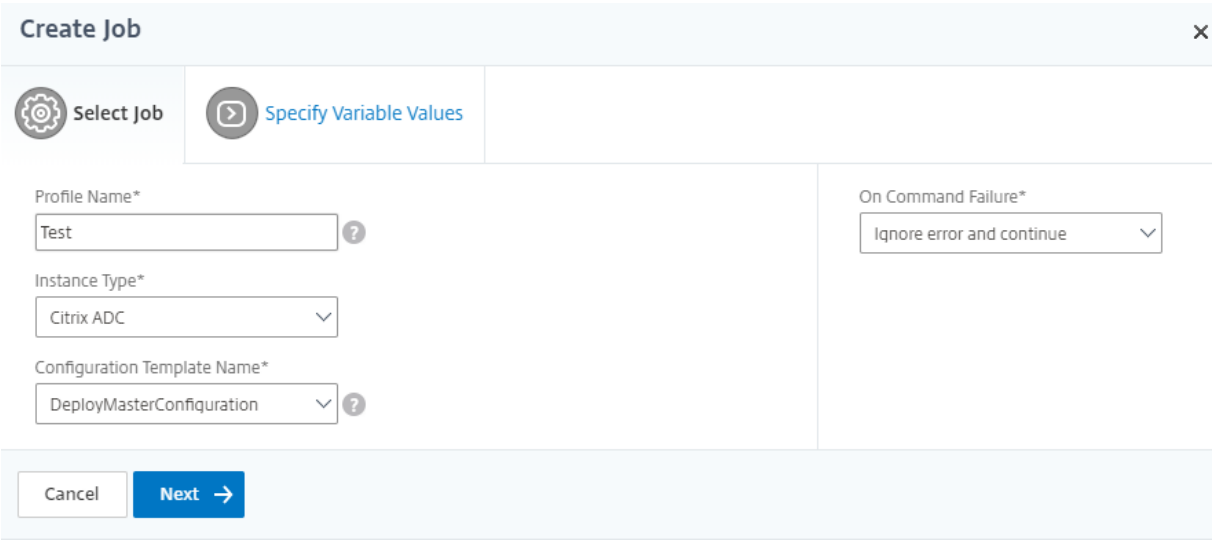


> 注
>
> コマンドスクリプトの実行時に生成された 出力と エラー（存在する場合）を **Citrix ADM** サーバーのログファイルに保存する場合は、［**Append** Output］オプションと［Append Errors］オプションを有効にできます。これらのオプションを有効にしないと、Citrix ADM はコマンドスクリプトの実行中に生成されたすべての出力とエラーを破棄します。

[ジョブの実行**]** アクションを設定するには

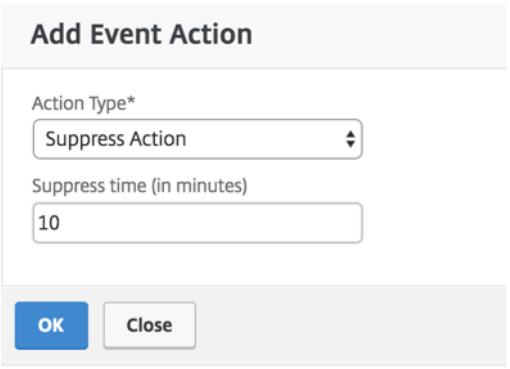
構成ジョブを使用してプロファイルを作成すると、指定したフィルター条件に一致するイベントとアラームについて、Citrix ADC、Citrix ADC SDX、および Citrix SD-WAN WO インスタンスの組み込みジョブまたはカスタムジョブとしてジョブが実行されます。

1. [イベントルールアクション] で、[アクションの追加] をクリックし、[****** アクションの種類**]** リストから **[**ジョブアクションの実行 ******] を選択します。
2. イベントが定義済みのフィルタ基準を満たすときに実行するジョブを含むプロファイルを作成します。
3. ジョブの作成時に、プロファイル名、インスタンスタイプ、設定テンプレート、ジョブのコマンドが失敗した場合に実行するアクションを指定します。
4. 選択したインスタンスタイプと選択した設定テンプレートに基づいて、変数の値を指定し、[**Finish**] をクリックしてジョブを作成します。



抑制アクションを設定するには

[**Suppress Action]** イベントアクションを選択すると、イベントを抑制またはドロップする期間を分単位で設定できます。最短で 1 分間イベントを非表示にできます。



Citrix ADM から **Slack** 通知を設定するには

Citrix ADM GUI でプロファイル名と Webhook URL を指定して、必要な Slack チャネルを構成します。イベント通知はこのチャンネルに送信されます。複数の Slack チャンネルを設定して、これらの通知を受け取ることができます。

1. Citrix ADM で、［ネットワーク］>［イベント］>［ルール］の順に選択し、［追加］をクリックしてルールを作成します。
2. **[** ルールの作成] ページで、重大度やカテゴリなどのルールパラメータを設定します。監視するインスタンスおよび障害オブジェクトを選択します。
3. [イベントルールの操作] で、[アクションの追加] をクリックします。次に、[アクションタイプ] リストから [**Slack** 通知を送信] を選択し、[**Slack** プロファイルリスト**]** を選択します。

4. Slack プロファイルリスト欄の横にある「追加」をクリックして、**Slack** プロファイルリストを追加することもできます。
5. プロファイルリストを作成するには、次のパラメータを入力します。
   a) プロファイル名。Citrix ADM で構成するプロファイルリストの名前を入力します。
   b) チャネル名。イベント通知の送信先となる Slack チャンネルの名前を入力します。
   c) **Webhook URL**。以前に入力したチャンネルの Webhook URL を入力します。受信ウェブフックは、外部ソースからのメッセージを Slack に投稿する簡単な方法です。URL は内部的にチャンネル名にリンクされ、イベント通知はすべてこの URL に送信され、指定された Slack チャンネルに投稿されます。ウェブフックの例は次のとおりです。https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK
6. [**Create**] をクリックし、[**Add Event Action**] ウィンドウで [**OK**] をクリックします。

> 注:
>
> [アカウント] > [通知] > [Slack プロフィール] の順に選択して、**Slack** プロファイルを追加することもできます。[追加] をクリックし、前のセクションの説明に従ってプロファイルを作成します。

作成した Slack プロファイルのステータスを確認できます。

これで、適切なフィルターが設定され、適切なイベント規則アクションが定義されたイベント規則が作成されました。

Citrix ADM から **PagerDuty** 通知を設定するには

Citrix ADM オプションとして PagerDuty プロファイルを追加して、PagerDuty 構成に基づいてインシデント通知を監視できます。PagerDuty では、電子メール、SMS、プッシュ通知、および登録番号への電話による通知を設定できます。

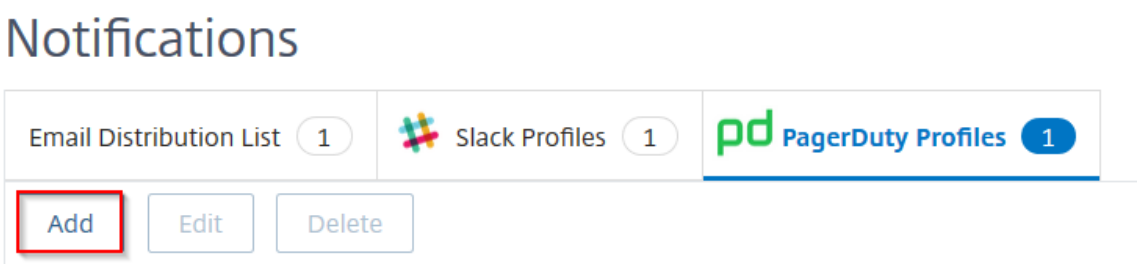
Citrix ADM で PagerDuty プロファイルを追加する前に、PagerDuty で必要な構成が完了していることを確認します。詳しくは、「ページデューティのドキュメント」を参照してください。

PagerDuty プロファイルをオプションの 1 つとして選択して、次の機能に関する通知を受け取ることができます。

- イベント — Citrix ADC インスタンスに対して生成されるイベントのリスト。
- **[Licenses]**: 現在アクティブで、期限切れが近づいているなどのライセンスのリスト。
- **SSL** 証明書 — Citrix ADC インスタンスに追加される SSL 証明書のリスト。

ADM で **PagerDuty** プロファイルを追加するには:

1. 管理者の資格情報を使用して Citrix ADM にログオンします。
2. アカウント > 通知 > **PagerDuty** プロファイルに移動します。
3. [追加] をクリックしてプロファイルを作成します。



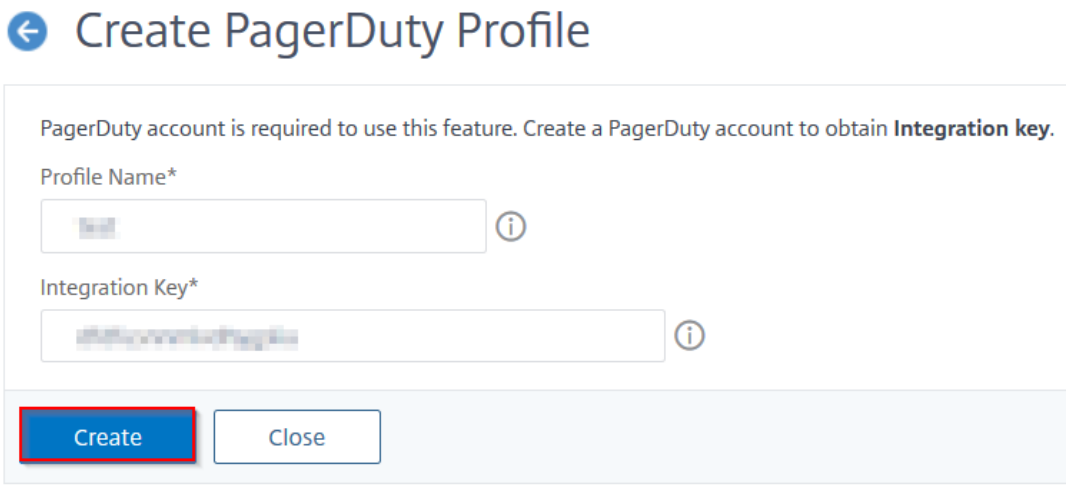
4. 「ページデューティプロファイルの作成」ページで、次の操作を行います。

   a) 任意のプロファイル名を入力します。

   b) 統合キーを入力します。

      統合キーは、PagerDuty ポータルから入手できます。

   c) ［作成］をクリックします。



ユースケース:

次のようなシナリオを考えてみましょう。

- あなたの PagerDuty プロファイルに通知を送信したいです。
- では、PagerDuty で通知を受信するためのオプションとして電話が設定されています。
- では、Citrix ADC イベントに関する電話通知を受信できます。

を構成するには、次の手順に従います。

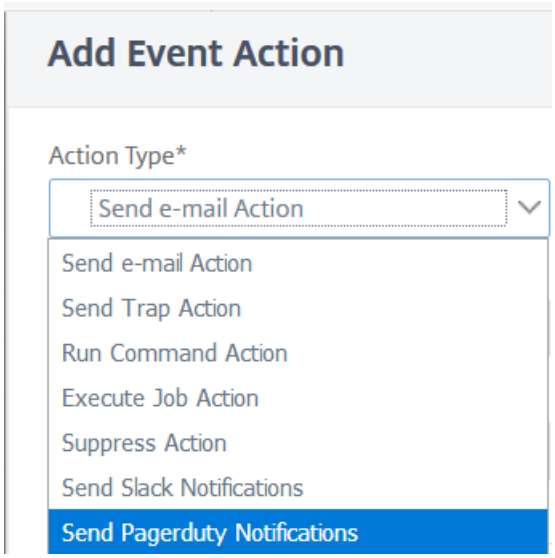
a) 「イベント」>「ルール」にナビゲートします。

b) **[** ルールの作成] ページで、他のすべてのパラメータを設定してルールを作成します。

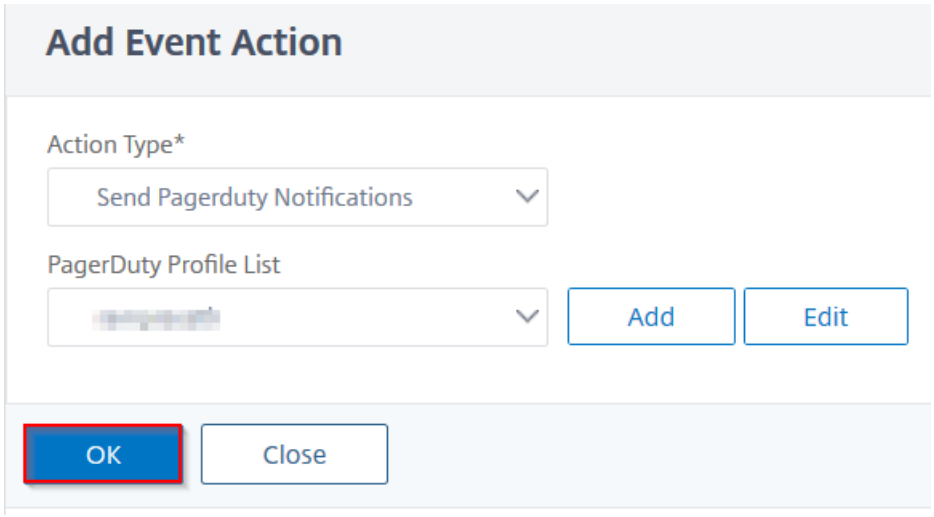
c) [ルールのアクションの作成] で、[アクションの追加] をクリックします。

「イベント・アクションの追加」ページが表示されます。

i. [アクションタイプ] で、[**PagerDuty** 通知を送信] を選択します。



ii. PagerDuty プロファイルを選択し、[**OK**] をクリックします。



構成が完了すると、Citrix ADC インスタンスに対して新しいイベントが生成されるたびに、電話が送信されます。電話から、次のことを決定できます。

- イベントを承認する
- 解決済みとしてマークする
- 他のチームメンバーへのエスカレーション

Citrix ADM から **ServiceNow** インシデントを自動生成するには

Citrix ADM GUI で ServiceNow プロファイルを選択して、Citrix ADM イベントの ServiceNow インシデントを自動生成できます。イベントルールを構成するには、Citrix **ADM** で **ServiceNow** プロファイルを選択する必要があります。

ServiceNow インシデントを自動生成するようにイベントルールを構成する前に、Citrix ADM サービスと ServiceNow インスタンスを統合します。詳しくは、「サービス用の ITSM アダプタの構成 Now」を参照してください。

イベントルールを設定するには、**[**イベント**] > [**** ルール] に移動します。**

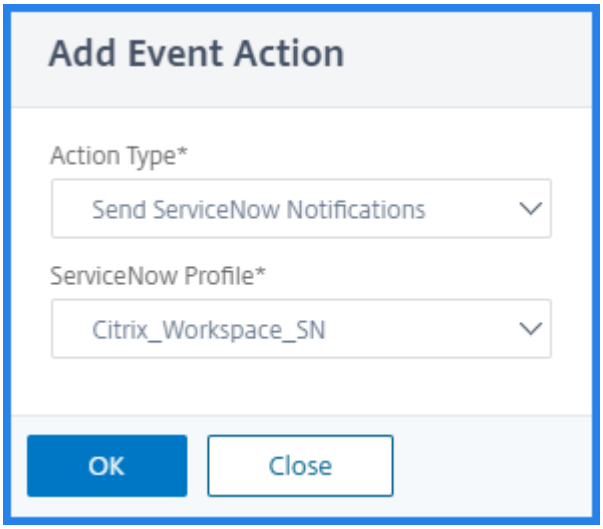
1. **[** ルールの作成] ページで、他のすべてのパラメータを設定してルールを作成します。
2. [ルールのアクションの作成] で、[アクションの追加] をクリックします。

   「イベント・アクションの追加」ページが表示されます。

   a) [アクションの種類] で、[**ServiceNow** 通知の送信] を選択します。

   b)「サービス」の「プロファイル」で、リストから「**Citrix_Workspace_SN** 」プロファイルを選択します。

   c) [**OK**] をクリックします。



Citrix ADC インスタンスで発生するイベントの報告された重大度を変更する

May 7, 2021

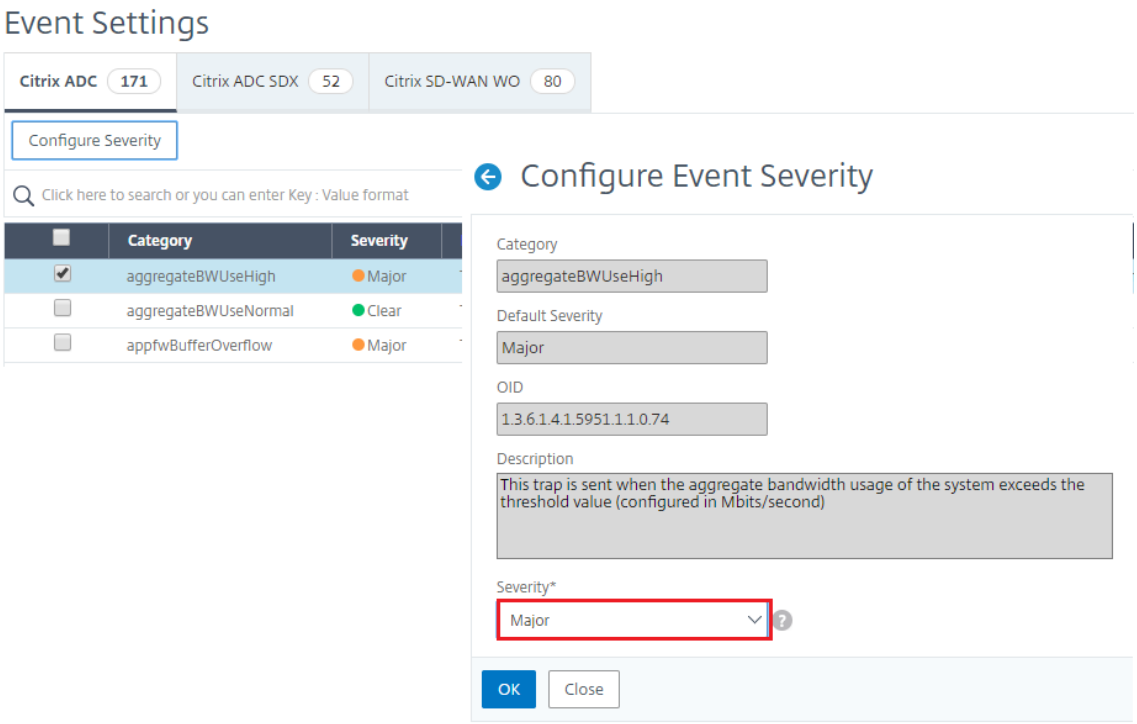
すべてのデバイスで生成されたイベントのレポートを管理できます。これにより、インスタンス上の特定のイベントに関するイベントの詳細を表示し、イベントの重大度に基づいてレポートを表示できます。また、デフォルトの重要度設定を使用するイベントルールを作成したり、重大度設定を変更したりできます。汎用イベントとエンタープライズ固有のイベント双方に対して、重要度を構成できます。

重要度レベルは、Critical、Major、Minor、Warning、Clear で定義できます。

イベントの重大度を変更するには、次の手順に従います。

1. [ネットワーク] > [イベント] > [イベント設定**]** に移動します。

2. 変更する Citrix ADC インスタンスタイプのタブをクリックします。次に、リストからカテゴリを選択し、[重要度の設定] をクリックします。
3. [**Configure Event Severity**] でボックスの一覧から重要度レベルを選択します。
4. [**OK**] をクリックします。

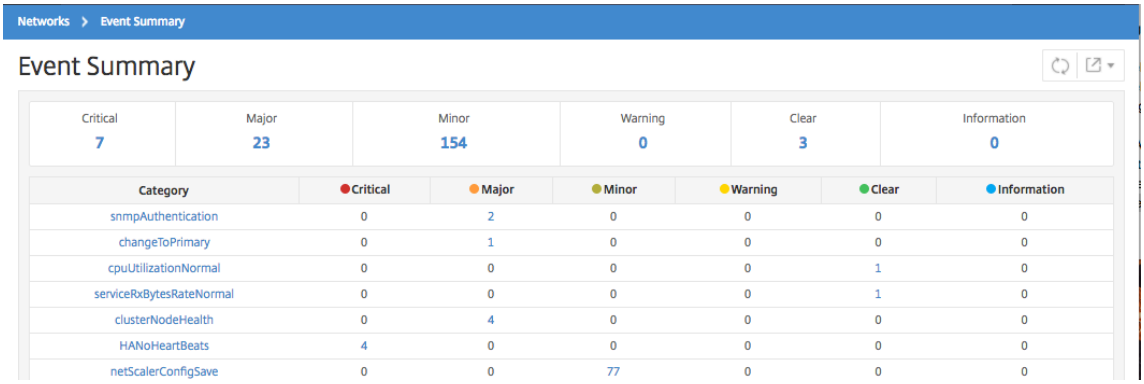


イベントの概要の表示

May 7, 2021

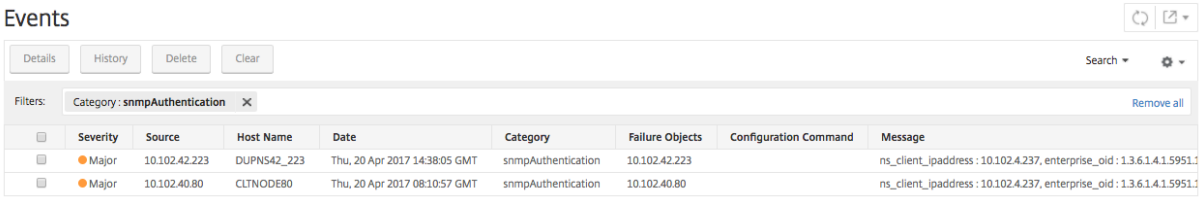
[イベントの概要] ページを表示して、Citrix Application Delivery Management（Citrix ADM）で受信したイベントとトラップを監視できるようになりました。[ネットワーク] > [イベント] に移動します。[Events Summary] ページには、以下の情報が表形式で表示されます。

- **Citrix ADM** が受信したすべてのイベントの概要。イベントはカテゴリ別にリストされ、重要度（クリティカル、メジャー、マイナー、警告、クリア、情報）の異なる列に表示されます。たとえば、Citrix ADC（Citrix ADC）インスタンスがダウンし、Citrix ADM への情報の送信を停止すると、クリティカルイベントが発生します。イベント中は、インスタンスがダウンした理由、インスタンスがダウンしていた時間などを説明する通知が管理者に送信されます。その後、イベントは [イベントの概要] ページに記録されます。このページでは、概要を表示したり、イベントの詳細にアクセスしたりできます。



- 各カテゴリに対して受信されたトラップの数。重要度で分類された受信済みのトラップの数。デフォルトでは、Citrix ADC インスタンスから Citrix ADM に送信される各トラップには重大度が割り当てられていますが、ネットワーク管理者は Citrix ADM GUI で重要度を指定できます。

カテゴリタイプまたはトラップをクリックすると、[**Events**] ページが表示され、[Category] や [Severity] などのフィルタが事前に選択されます。このページには、Citrix ADC インスタンスの IP アドレスとホスト名、トラップを受信した日付、カテゴリ、障害オブジェクト、構成コマンドの実行、メッセージ通知など、イベントに関する詳細情報が表示されます。



Citrix ADM でイベントを表示する日数は、1～40 の間で構成できます。たとえば、[30 日] を選択すると、30 日間のイベントが Citrix ADM に表示され、30 日後にイベントがクリアされます。このイベント設定を構成するには、[**設定] > [**データレンタルポリシー**]** に移動します。詳しくは、「データ保持ポリシー」を参照してください。

このダッシュボードのレポートをエクスポートするには、次の手順に従います。

このページのレポートをエクスポートするには、このページの右上にある エクスポートアイコンをクリックします。[エクスポート] ページでは、次のいずれかの操作を実行できます。

1. [今すぐエクスポート] タブを選択します。レポートを PDF、JPEG、PNG、または CSV 形式で表示して保存します。
2. [スケジュールエクスポート] タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、電子メールまたは余裕期間メッセージでレポートを送信するには。

> 注
>
> - [毎週の繰り返し] を選択した場合は、レポートをスケジュールする平日を選択してください。
> - [毎月の繰り返し] を選択した場合は、レポートをスケジュールするすべての日をカンマで区切って入力します。

イベントの重大度と **SNMP** トラップの詳細を表示します

May 7, 2021

Citrix Application Delivery Management（Citrix ADM）でイベントとその設定を作成すると、[イベントの概要] ページでイベントをすぐに表示できます。同様に、インフラストラクチャダッシュボードで、Citrix ADCitrix ADM サーバーに追加されたすべての Citrix Application Delivery Controller（Citrix ADC）インスタンスの正常性、稼働時間、モデル、およびバージョンを詳細に表示および監視できます。

Infrastructure ダッシュボードでは、無関係な値をマスクして、重要度、正常性、稼働時間、モデル、Citrix ADC インスタンスのバージョンなどの情報をより簡単に表示および監視できるようになりました。

たとえば、重大度が Critical のイベントはほとんど発生しません。しかしながら、ネットワーク上でこれらの重大イベントが実際に発生した場合は、そのイベントが発生した場所と時間をさらに調査、トラブルシューティング、監視できます。Critical 以外のすべての重要度レベルを選択すると、グラフに重大イベントの発生のみが表示されます。また、グラフをクリックすると、[**Severity bared events**] ページが表示されます。このページには、選択した期間におけるクリティカルイベントの発生時期に関するすべての詳細（インスタンスのソース、日付、カテゴリ、およびクリティカルイベント発生時に送信されたメッセージ通知）を確認できます。

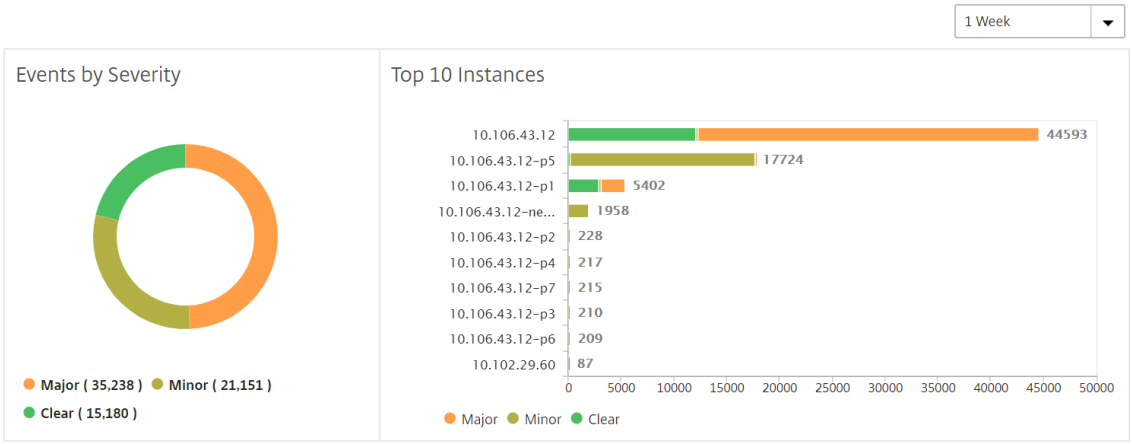
同様に、ダッシュボードで Citrix ADC VPX インスタンスの状態を確認できます。インスタンスが稼働していた時間をマスクし、インスタンスが稼働停止していた時間のみを表示できます。グラフをクリックすると、そのインスタンスのページが表示され、アウトオブサービスフィルタがすでに適用されており、ホスト名、1 秒あたりに受信した HTTP リクエストの数、CPU 使用率などの詳細が表示されます。インスタンスを選択し、詳細についてはインスタンスのダッシュボードを表示することもできます。

Citrix ADM で特定のイベントを重要度別に選択するには：

1. 管理者の資格情報を使用して Citrix ADM にログオンします。
2. [ネットワーク] > [ダッシュボード] に移動します。

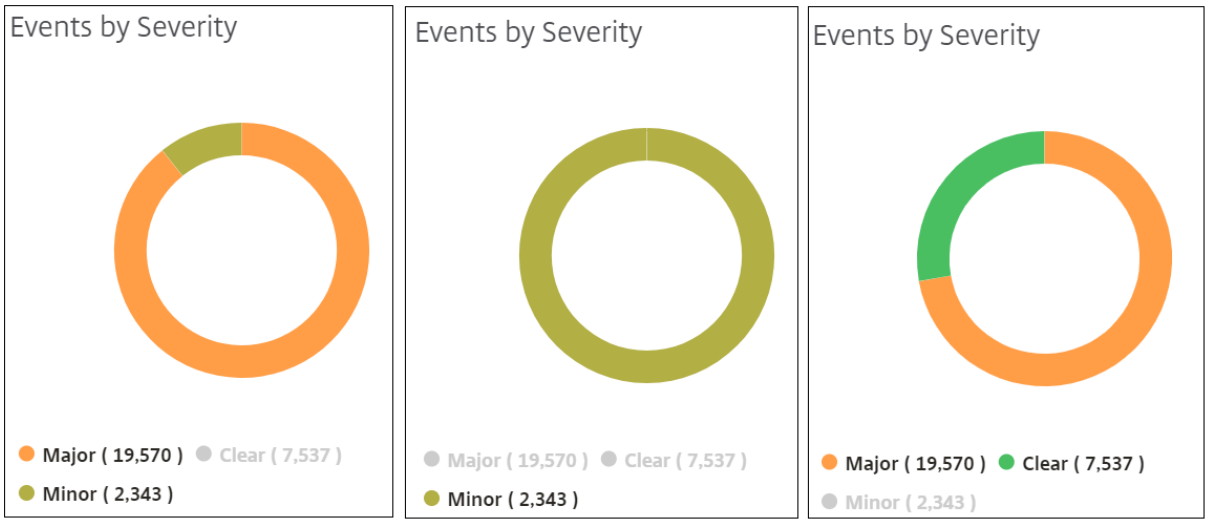
   または

   [ネットワーク] > [イベント] > [レポート] に移動します。
3. ページの右上隅にあるボックスの一覧から、イベントを重要度別に表示する期間を選択します。



4. [重大度別イベント] ドーナツグラフには、すべてのイベントが重要度別に視覚的に表示されます。異なる種類のイベントは異なる色が付いたセクションとして表され、各セクションの長さは、その種類の重要度の合計イベント数に対応しています。
5. ドーナツグラフの各セクションをクリックすると、対応する「重大度ベースのイベント」ページが表示されます。このページには、選択した期間における選択した重要度に関する次の詳細が表示されます。
   - インスタンスのソース
   - イベントの日付
   - Citrix ADC インスタンスによって生成されるイベントのカテゴリ
   - 送信されたメッセージ通知

> 注
>
> ドーナツグラフの下には、グラフに表示されている重大度の一覧が表示されます。デフォルトでは、ドーナツグラフには、すべての重要度タイプのすべてのイベントが表示されます。そのため、一覧内のすべての重要度タイプが強調表示されます。重大度タイプを切り替えて、選択した重大度をより簡単に表示および監視できます。

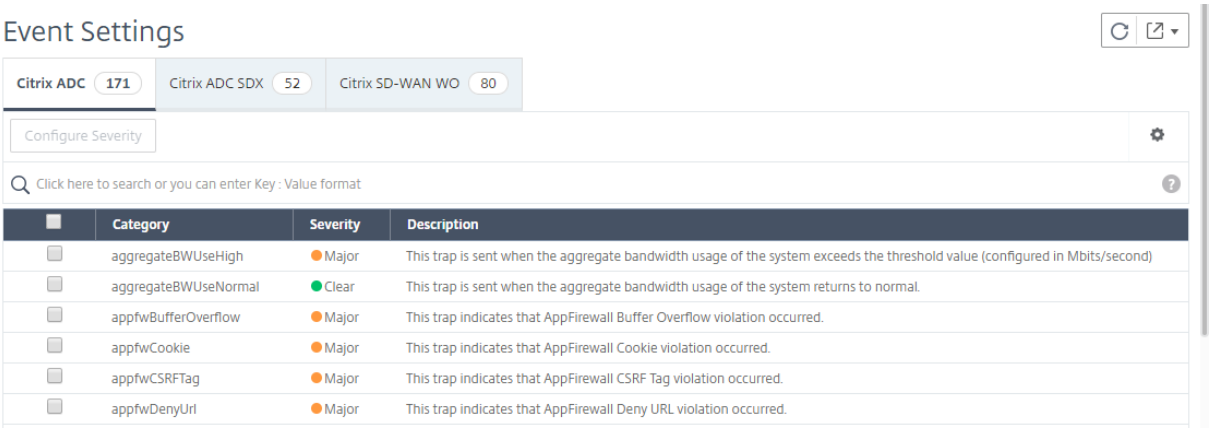


Citrix ADM で **Citrix ADC SNMP** トラップの詳細を表示するには:

［イベント設定］ページで、管理対象の Citrix ADC インスタンスから受信した各 SNMP トラップの詳細を、Citrix ADM で表示できるようになりました。[ネットワーク] > [イベント] > [イベント設定] に移動します。インスタンスから受信した特定のトラップについては、タブ形式で次の詳細を表示できます。

- **Category** : イベントが属するインスタンスのカテゴリを指定します。
- 重大度：イベントの重大度は、色とその重大度タイプで示されます。
- 説明**:** イベントに関連付けられたメッセージを指定します。

たとえば、トラップカテゴリが **monresptimeOutbeLowthResh** のイベントの場合、トラップの説明は、「このトラップは、モニタプローブの応答タイムアウトが正常に戻ったときに、設定されたしきい値より小さくなったときに送信されます。」



syslog メッセージの表示とエクスポート

May 7, 2021

サーバー上で受信されたすべての syslog メッセージのエクスポートをスケジュールすることで、Citrix ADCitrix Application Delivery Management（Citrix ADM）にログインせずに syslog メッセージを表示できます。Citrix アプリケーション Delivery Controller（Citrix ADC）インスタンスで生成された syslog メッセージを、PDF、CSV、PNG、および JPEG 形式でエクスポートできます。また、これらのレポートのエクスポートを指定された電子メールアドレスにさまざまな間隔でスケジュールできます。

> 注
>
> Citrix ADM での syslog サーバーの構成および syslog メッセージの表示の詳細については、「Citrix ADM 監査情報を表示する方法」を参照してください。

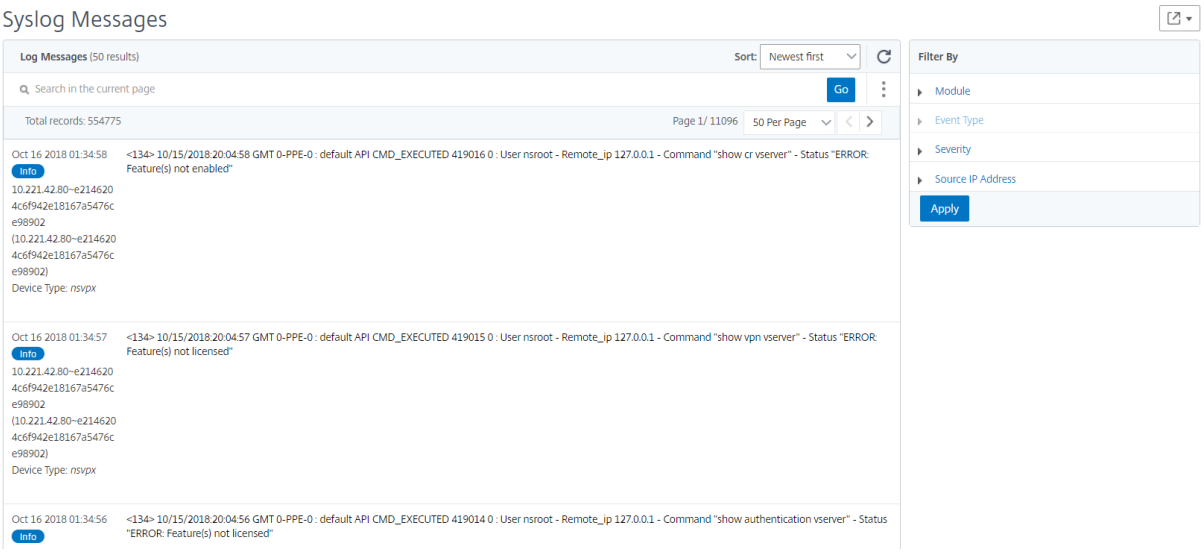
syslog メッセージを表示する

管理対象 Citrix ADC インスタンスで生成されたすべての syslog メッセージを表示できます。メッセージを表示するには、Syslog メッセージを Citrix ADM サーバーにリダイレクトするようにインスタンスを構成する必要がありま

す。Syslog メッセージは、データベースの中央に格納され、監査目的で Syslog ビューアで使用できます。このログ情報を組み合わせて、収集されたデータから分析用のレポートを生成できます。

Syslog を構成して、さまざまな種類のイベントをログ記録することもできます。

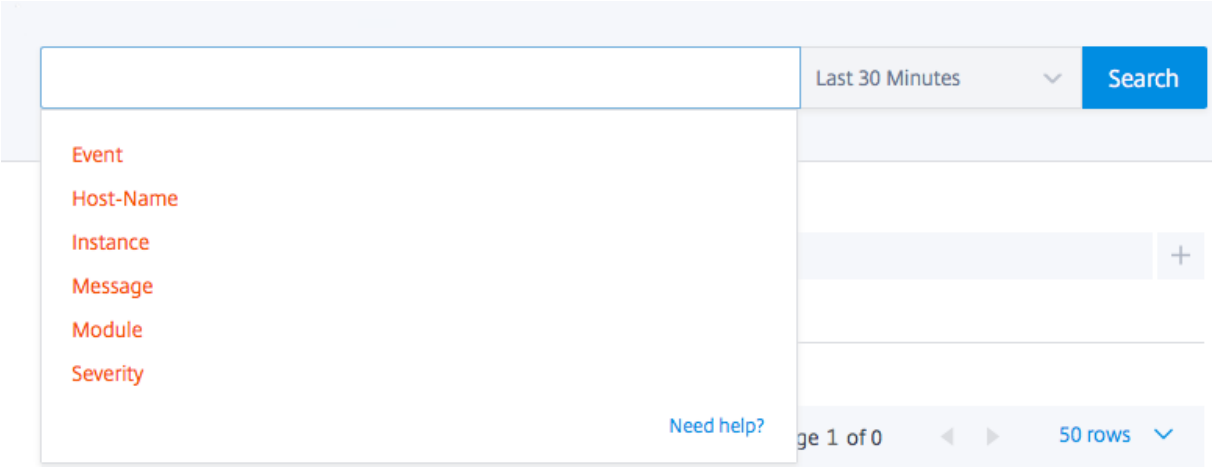
Syslog ビューアを表示するには、[ネットワーク] > [イベント] > [**Syslog** メッセージ] に移動します。システムログメッセージを表示するには、適切なフィルタを選択します。



syslog メッセージの検索

フィルタを使用して、syslog メッセージと監査ログメッセージを検索し、結果を絞り込み、探しているものをリアルタイムで見つけることができます。

ADM ソフトウェアに存在するすべての ADC インスタンスの syslog メッセージを検索するには、ADM GUI から **[**ネットワーク**] > [**イベント**] > [Syslog** メッセージ**]** に移動します。新しいフィルタカテゴリは、インスタンス、モジュール、イベント、重大度、およびメッセージです。



ADM ソフトウェアに存在するすべての ADM システム監査ログメッセージを検索するには、ADM GUI から **[**アカウ

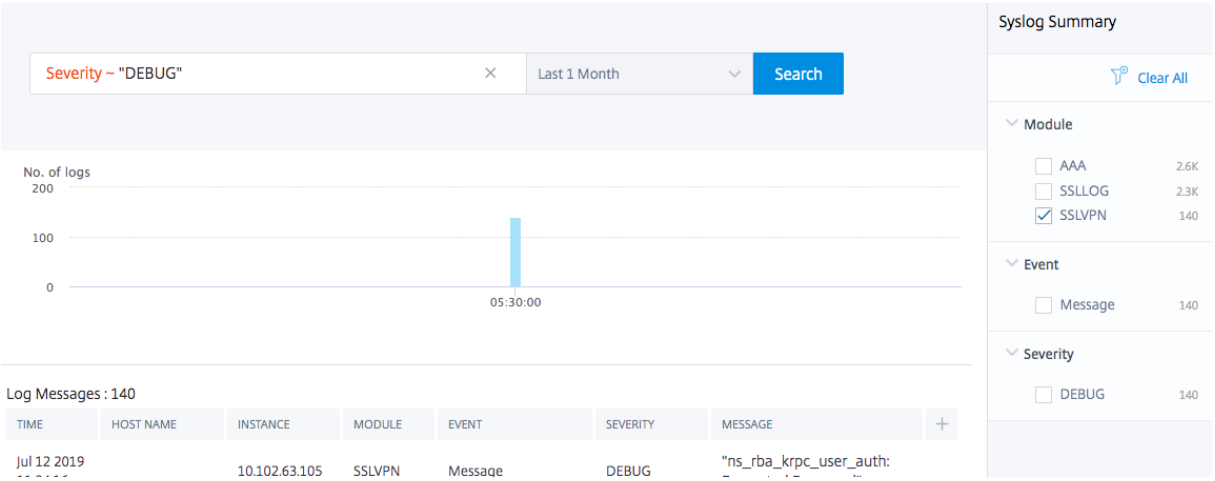
ント**] > [**監査ログメッセージ] に移動します。新しいフィルタカテゴリは、インスタンス、モジュール、イベント、重大度、およびメッセージです。

ADM に存在するすべてのアプリケーションの監査ログメッセージを検索するには、ADM GUI から、[ネットワーク] > [ネットワーク機能**] > [**監査] に移動します。

ADM 上の特定のアプリケーションの監査ログメッセージを検索するには、ADM GUI から [アプリケーション**] > [**ダッシュボード] に移動し、監査ログメッセージを検索する仮想サーバーを選択します。次に、[監査ログ] タブをクリックします。

フィルタカテゴリを選択した後、そのカテゴリが検索語と等しいか、含まれているかを指定します。

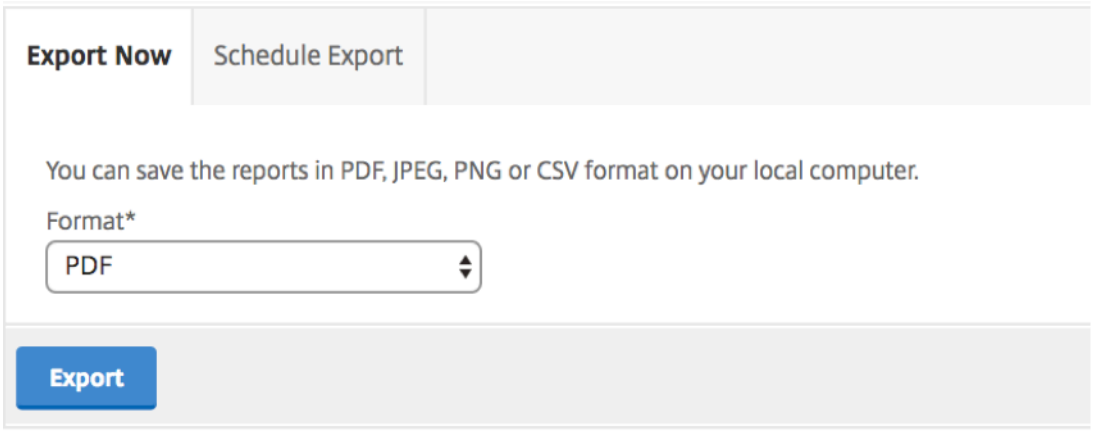
次に、検索語を追加します。一部のカテゴリでは、あらかじめ入力された検索語の一覧が表示されます。デフォルトでは、検索時間は 1 日です。下向き矢印をクリックすると、時刻と日付の範囲を変更できます。[**Syslog** の概要**]** ペインまたは **[**** 監査ログの概要 ******] ペインからオプションを選択して、検索をさらに絞り込むことができます。



syslog メッセージのエクスポート

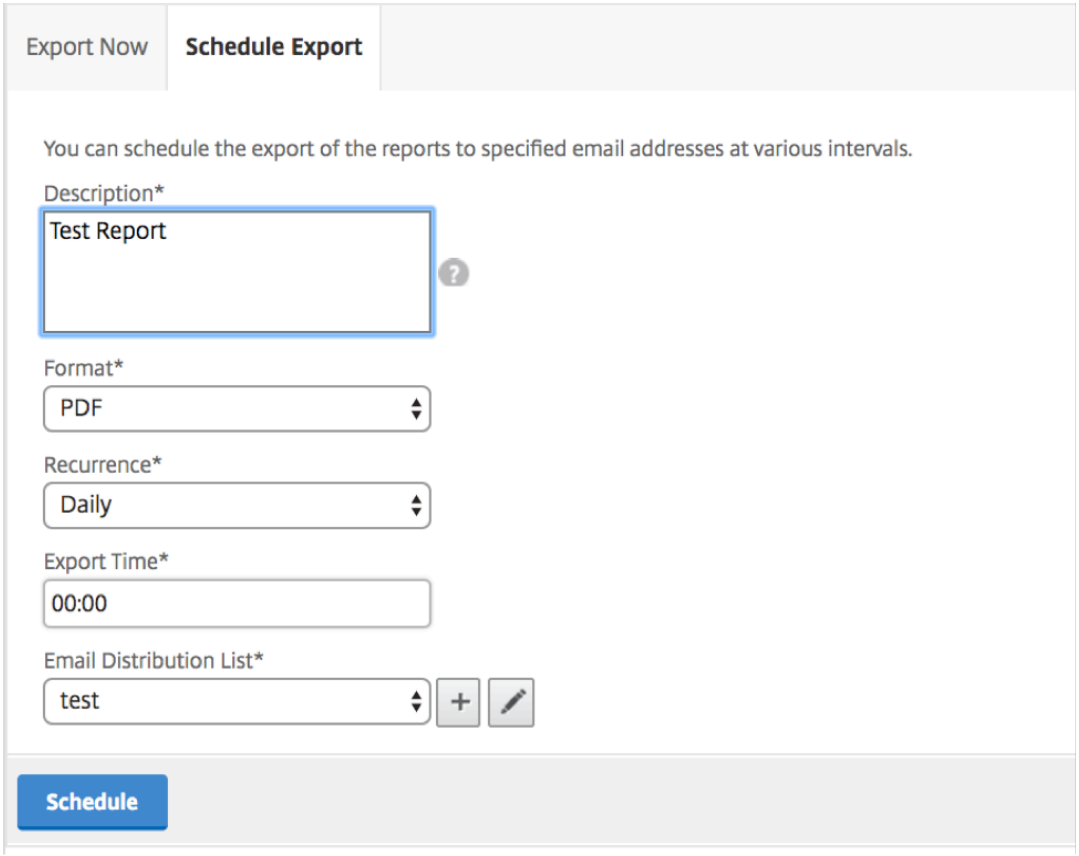
Citrix ADM を使用して **syslog** メッセージレポートをエクスポートするには:

1. [ネットワーク] > [イベント] > [**Syslog** メッセージ] に移動します。
2. 右側のペインで、[Syslog Messages] ページの右上隅にある [エクスポート] ボタンをクリックします。
3. [今すぐエクスポート] で、必要な形式を選択し、[エクスポート] をクリックします。



Citrix ADM を使用して **syslog** メッセージレポートのエクスポートをスケジュールするには:

1. [ネットワーク] > [イベント] > [**Syslog** メッセージ] に移動します。
2. [**Syslog** メッセージ] ページの右ペインで、[エクスポート] をクリックします。
3. [レポートのスケジュール] タブで、次のパラメータを設定します。
    - 説明: レポートをエクスポートする理由を説明するメッセージ。
    - フォーマット: レポートをエクスポートするフォーマット。
    - 繰り返し: レポートをエクスポートする間隔。
    - エクスポート時間: レポートをエクスポートする時間。現地時間帯の時間を 24 時間形式で入力します。
    - 電子メール配布リスト: 電子メールでレポートを受信する受信者のリスト。表示されたリストから電子メール配布リストを選択します。電子メールは、レポートが生成されスケジュールの時間基準が満たされると送信されます。電子メール配布リストを作成する場合は、[**+**] をクリックし、メールサーバーとメールプロファイルの詳細を指定します。



syslog メッセージの抑制

May 7, 2021

Syslog サーバーとして構成されている場合、Citrix Application Delivery Management（ADM）は、構成済みの Citrix ADC（Citrix ADC）インスタンスからすべての syslog メッセージを受信します。見たくないメッセージが多数あるかもしれません。たとえば、すべての情報レベルのメッセージを表示することに興味がない場合があります。必要のない一部の syslog メッセージを破棄できるようになりました。いくつかのフィルタを設定することで、ADM に送信される syslog メッセージの一部を抑制できます。Citrix ADM は、条件に一致するすべてのメッセージをドロップします。これらのドロップされたメッセージは Citrix ADM GUI には表示されません。また、これらのメッセージはお客様の Citrix ADM データベースにも保存されません。

いくつかのフィルタを設定することで、ADM に送信されるロギングされた syslog メッセージの一部を抑制できます。syslog メッセージを非表示にするために使用できる 2 つのフィルターは、重要度とファシリティです。特定の Citrix ADC インスタンスまたは複数のインスタンスからのメッセージを抑制することもできます。また、Citrix ADM でメッセージを検索および非表示にするテキストパターンを指定することもできます。Citrix ADM は、条件に一致するすべてのメッセージをドロップします。これらのドロップされたメッセージは Citrix ADM GUI には表示されません。また、これらのメッセージは顧客データベースにも保存されません。それにより、ストレージサーバー上

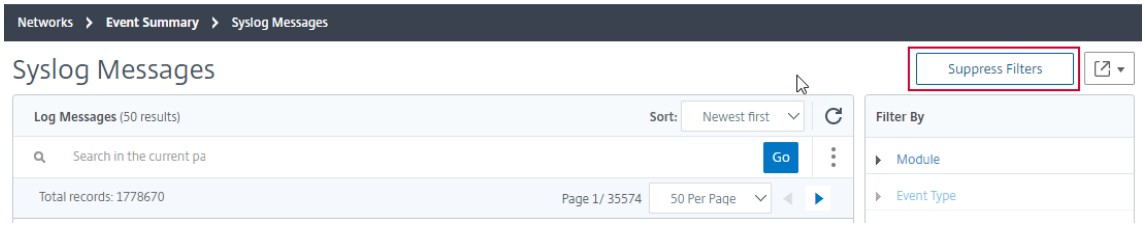
のかなりの領域が節約されます。

syslog メッセージを非表示にするためのいくつかのユースケースを次に示します。

- 情報レベルのすべてのメッセージを無視する場合は、レベル 6（情報）を非表示にします。
- ファイアウォールのエラー条件のみを記録する場合は、レベル 3（エラー）以外のすべてのレベルを非表示にします。

フィルタの作成による **syslog** メッセージの抑制

1. Citrix ADM で、［ネットワーク］>［イベント］>［**Syslog** メッセージ］に移動します。
2. [フィルタを非表示] をクリックします。

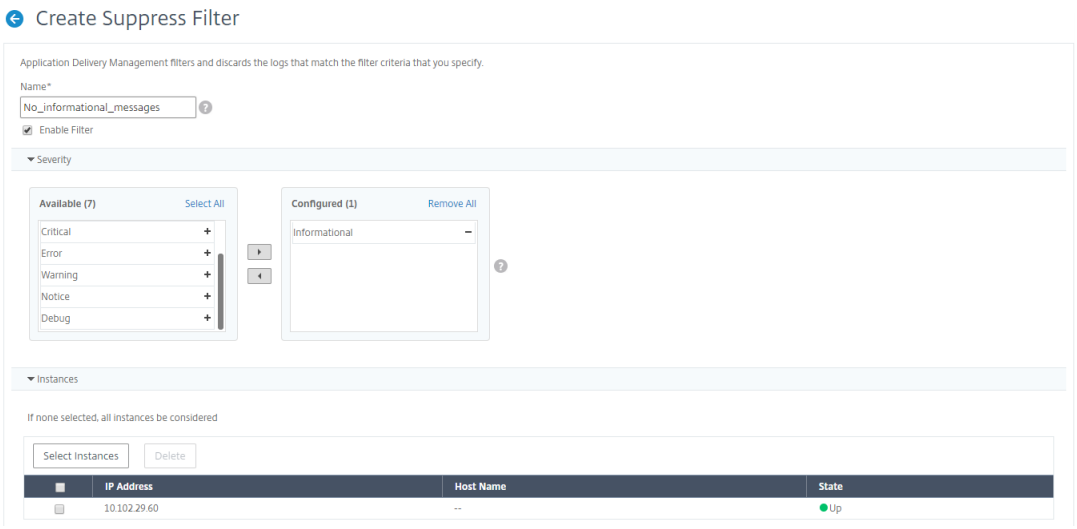


3. [フィルタの抑制] ページで、[追加] をクリックします。
4.「抑制フィルタの作成」ページで、次の情報を更新します。
   a) [名前]: フィルタの名前を入力します。

      > 注:
      >
      > 異なるユーザーが複数の Citrix ADC インスタンスに対して異なるアクセス権を持っている場合は、インスタンスごとに異なるフィルタを作成する必要があります。これは、ユーザーがすべてのインスタンスにアクセスできるフィルタのみを表示できるためです。

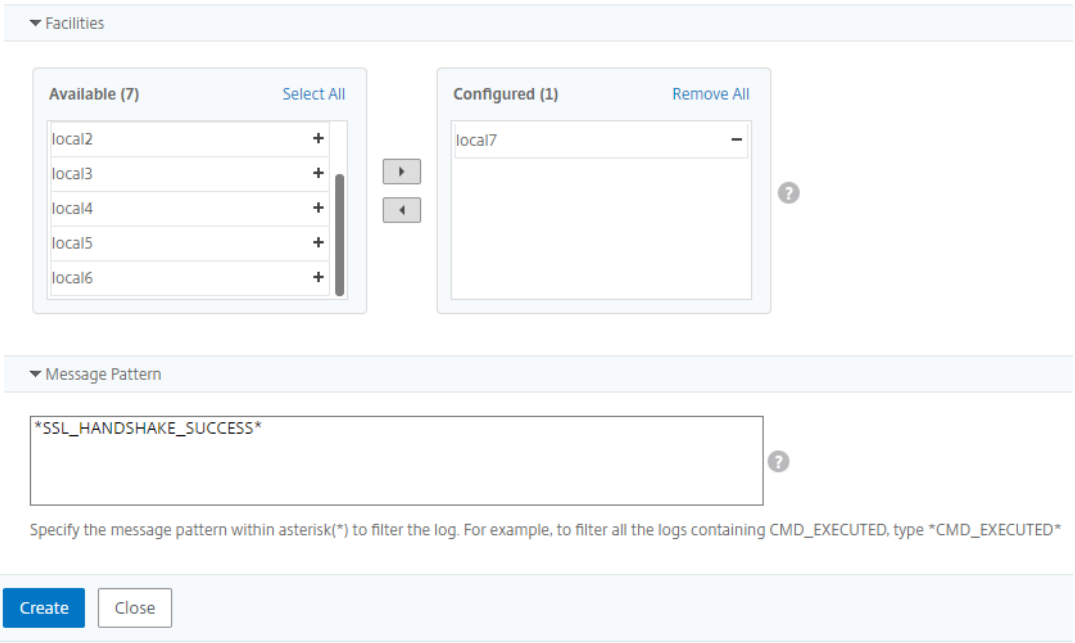
   b) 重大度：メッセージを抑制する必要があるログ・レベルを選択し、追加します。
   たとえば、入ってくる情報メッセージを表示しない場合は、[情報] を選択してこれらのメッセージを非表示にできます。

   c) インスタンス -syslog メッセージが構成されている Citrix ADC インスタンスを選択します。



d) ファシリティ-メッセージを生成するソースに基づいてメッセージを抑制するファシリティを選択します。

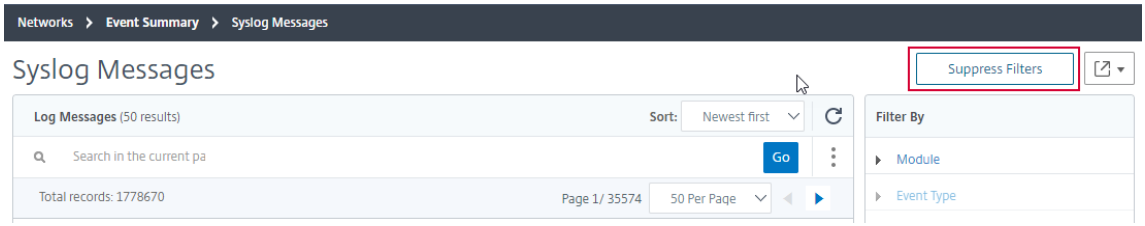
e) メッセージパターン -アスタリスク (*) で囲まれたテキストパターンを入力して、メッセージを非表示にすることもできます。メッセージに対してテキストパターン文字列が検索され、このパターンが含まれているメッセージが非表示になります。



フィルターの無効化

Citrix ADM でメッセージを表示できるようにするには、フィルタを無効にする必要があります。

1. [ネットワーク] > [イベント] > [**Syslog** メッセージ] に移動します。
2. [フィルタを非表示] をクリックします。



3. [フィルタの抑制] ページで、フィルタを選択し、[編集] をクリックします。
4. [フィルタの抑制の構成] ページで、[フィルタを有効にする] チェックボックスをオフにして、フィルタを無効にします。

SSL ダッシュボード

May 7, 2021

Citrix Application Delivery Management（Citrix ADM）は、証明書管理のあらゆる側面を合理化するようになりました。1 つのコンソールから、使われていない、または期限切れが近い証明書のタブは閉じたまま、正しい発行者、キーの強度、および正しいアルゴリズムを確保する自動化されたポリシーを作成することができます。Citrix ADM の SSL ダッシュボードとその機能を使用するには、SSL 証明書とは何か、および Citrix ADM を使用して SSL 証明書を追跡する方法を理解する必要があります。

SSL トランザクションの一部であるセキュアソケットレイヤー (SSL) 証明書は、企業 (ドメイン) または個人を識別するデジタルデータフォーム (X509) です。この証明書には、サーバーとの安全なトランザクションを開始しようとするすべてのクライアントが確認できる公開キーコンポーネントが含まれます。対応する秘密キーは、Citrix ADC アプライアンスに安全に常駐し、非対称キー（または公開キー）の暗号化と復号化を完了するために使用されます。

SSL 証明書およびキーは、次のいずれかの方法で入手できます。

- 承認された証明機関 (CA) から
- Citrix ADC アプライアンスで新しい SSL 証明書とキーを生成する

Citrix ADM では、管理対象のすべての Citrix ADC インスタンスにインストールされた SSL 証明書を一元的に表示できます。SSL ダッシュボードでは、証明書の発行者、キー強度、署名アルゴリズム、期限切れの証明書または未使用の証明書などを追跡するのに役立つグラフを表示できます。また、仮想サーバーで実行されている SSL プロトコルの分布および各サーバーで有効化されているキーも確認できます。

また、証明書の有効期限が近づいたときに通知を設定し、その証明書を使用する Citrix ADC インスタンスに関する情報を含めることもできます。

Citrix ADC インスタンス証明書を CA 証明書にリンクできます。ただし、同じ CA 証明書にリンクする証明書には、同じソースと発行元が同じであることを確認してください。1 つまたは複数の証明書を CA 証明書にリンクしたら、それらのリンクを解除できます。

> 注
>
> また、Venafi Trust Protection Platform サーバーと ADM を使用して、SSL 証明書のライフサイクル全体の管理を自動化することもできます。詳しくは、「SSL 証明書管理の自動化」を参照してください。

SSL ダッシュボードを使用する

May 7, 2021

Citrix Application Delivery Management（Citrix ADM）の SSL 証明書ダッシュボードを使用して、証明書の発行者、キー強度、署名アルゴリズムを追跡するのに役立つグラフを表示できます。SSL 証明書ダッシュボードには、次の項目を示すグラフも表示されます。

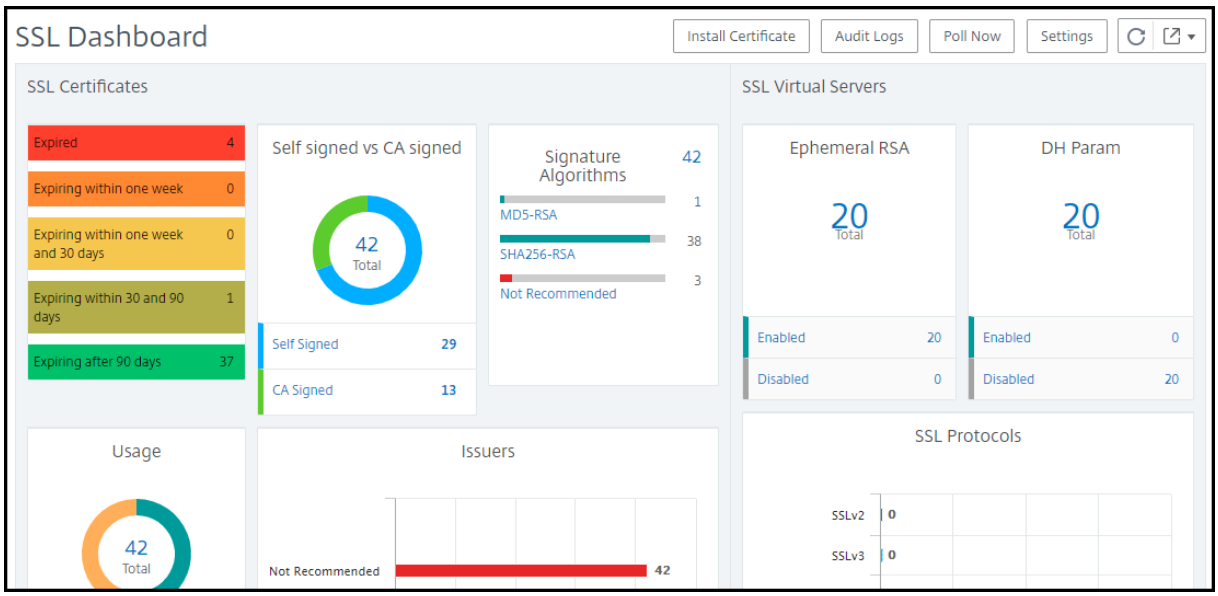
- 証明書が有効期限切れになるまでの日数
- 使用されている証明書および未使用の証明書の数
- 自己署名および CA 署名の証明書の数
- 発行者数
- 署名アルゴリズム
- SSL プロトコル
- 使用中の証明書件数上位 10 インスタンス

SSL 証明書の監視

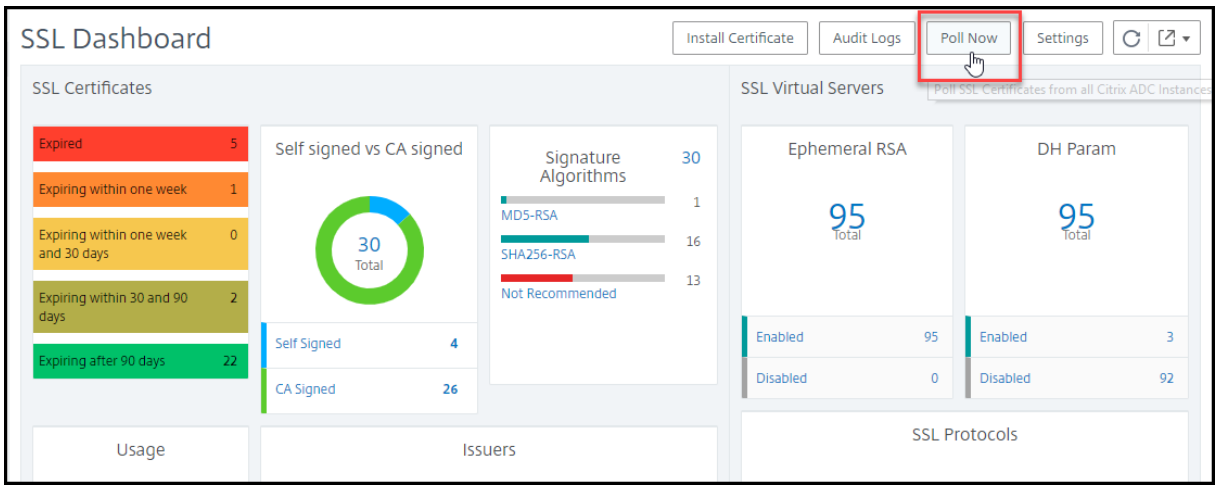
企業で SSL ポリシーを設定している場合は、Citrix ADM SSL ダッシュボードを使用して証明書を監視できます。たとえば、すべての証明書には 2048 ビットの最小キー長があり、信頼できる CA 機関が認証する必要があるなど、特定の SSL 証明書要件が定義されています。

別の例として、新しい証明書をアップロードしたが、それを仮想サーバーにバインドするのを忘れた場合について述べます。SSL ダッシュボードでは、使用中または未使用の SSL 証明書が強調表示されます。[使用法] セクションには、インストールされている証明書の数と、使用されている証明書の数が表示されます。グラフをさらにクリックすると、証明書名、証明書が使用されているインスタンス、有効性、署名アルゴリズムなどを確認できます。

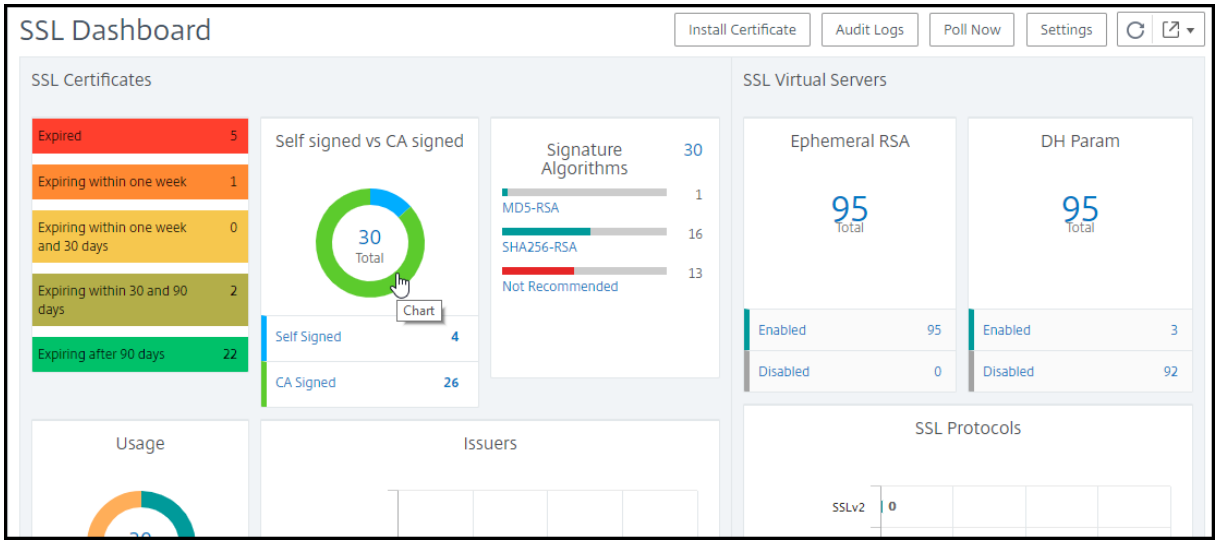
Citrix ADM で SSL 証明書を監視するには、［ネットワーク］>［**SSL** ダッシュボード］に移動します。



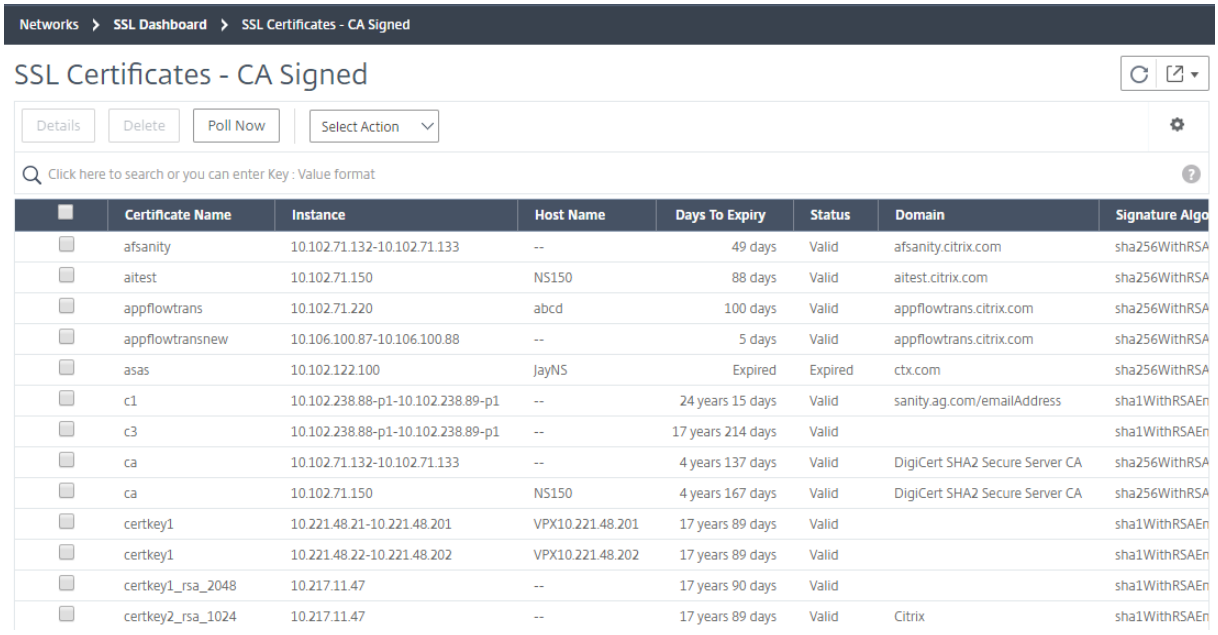
Citrix ADM では、SSL 証明書をポーリングし、インスタンスのすべての SSL 証明書を直ちに Citrix ADM に追加できます。これを行うには、[ネットワーク] > [**SSL** ダッシュボード] に移動し、[今すぐポーリング] をクリックします。[今すぐポーリングする] ページがポップアップし、ネットワーク内のすべての Citrix ADC インスタンスをポーリングするか、選択したインスタンスをポーリングするオプションが表示されます。



Citrix ADM SSL ダッシュボードを使用して、SSL 証明書、SSL 仮想サーバー、SSL プロトコルの詳細を表示または監視できます。「合計」数はリンクになっています。クリックすると、SSL 証明書、SSL 仮想サーバー、または SSL プロトコルに関連する詳細を表示できます。



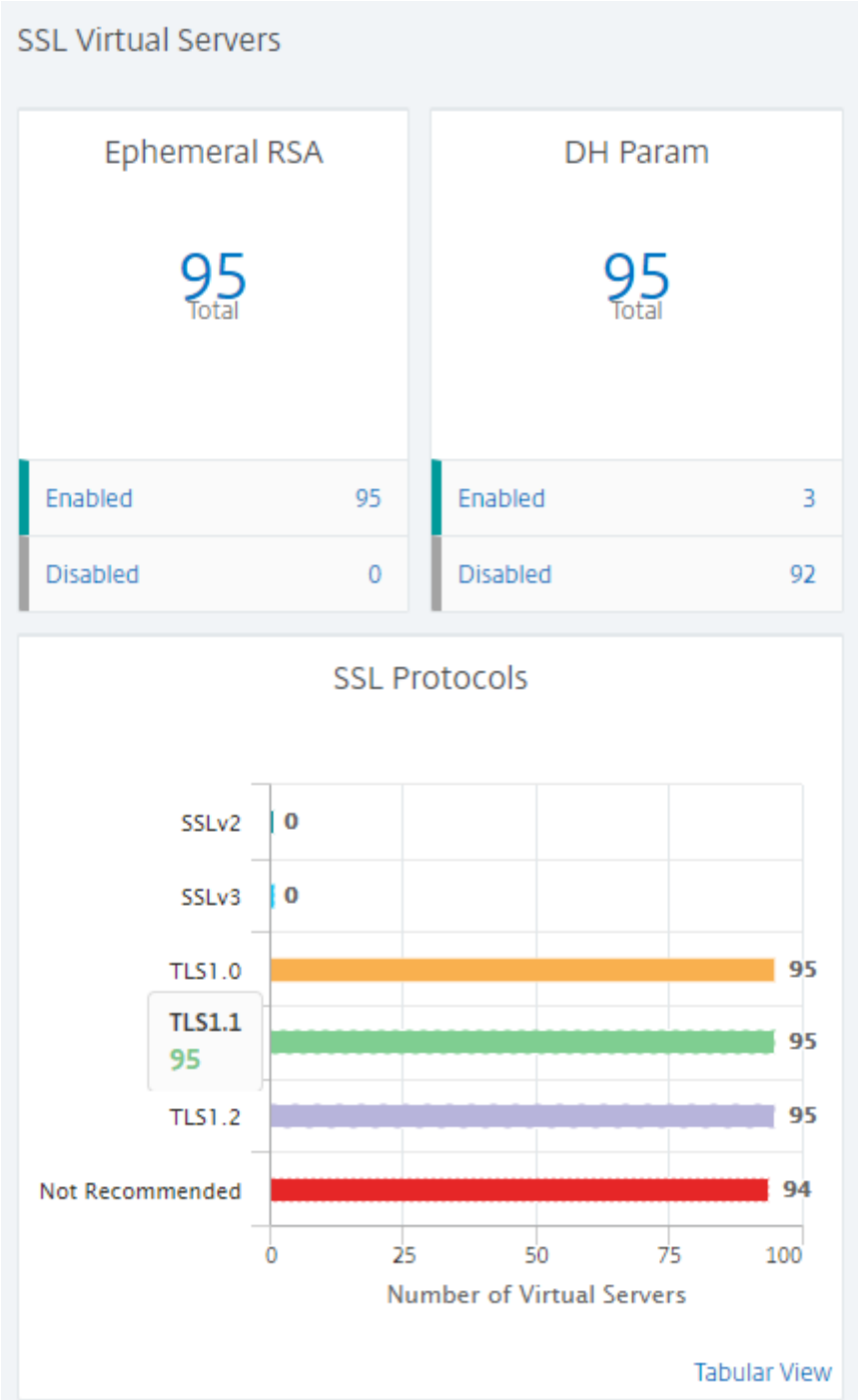
たとえば、ユーザーが「自己署名と CA signed」をクリックすると、新しいウィンドウが開き、Citrix ADC インスタンス上の 30 の SSL 証明書の詳細が表示されます。



Citrix ADM SSL ダッシュボードには、仮想サーバーで実行されている SSL プロトコルの分布も表示されます。管理者は、SSL ポリシーを使用して監視するプロトコルを指定できます。詳しくは、SSL ポリシーを設定するを参照してください。サポートされているプロトコルは、SSLv2、SSLv3、TLS1.0、TLS1.1、および TLS1.2 です、仮想サーバー上で使用されている SSL プロトコルは、棒グラフ形式で表示されます。特定のプロトコルをクリックすると、そのプロトコルを使用する仮想サーバーの一覧が表示されます。

ドーナツチャートは、SSL ダッシュボードで Diffie-Hellman (DH) キーまたは一時的な RSA キーを有効または無効にした後に表示されます。これらのキーにより、1024 ビットの証明書の場合のように、サーバー証明書でエクスポートクライアントがサポートされていない場合でも、エクスポートクライアントとの安全な通信が実現されます。適切なグラフをクリックすると、DH または Ephemeral RSA キーが有効になっている仮想サーバのリストが表示され

ます。

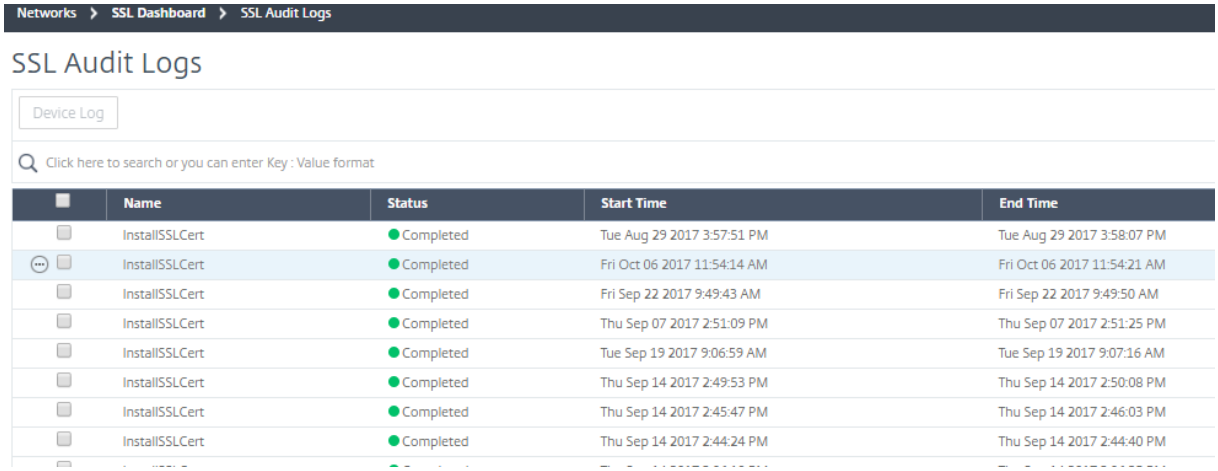


SSL 証明書の監査ログを表示する

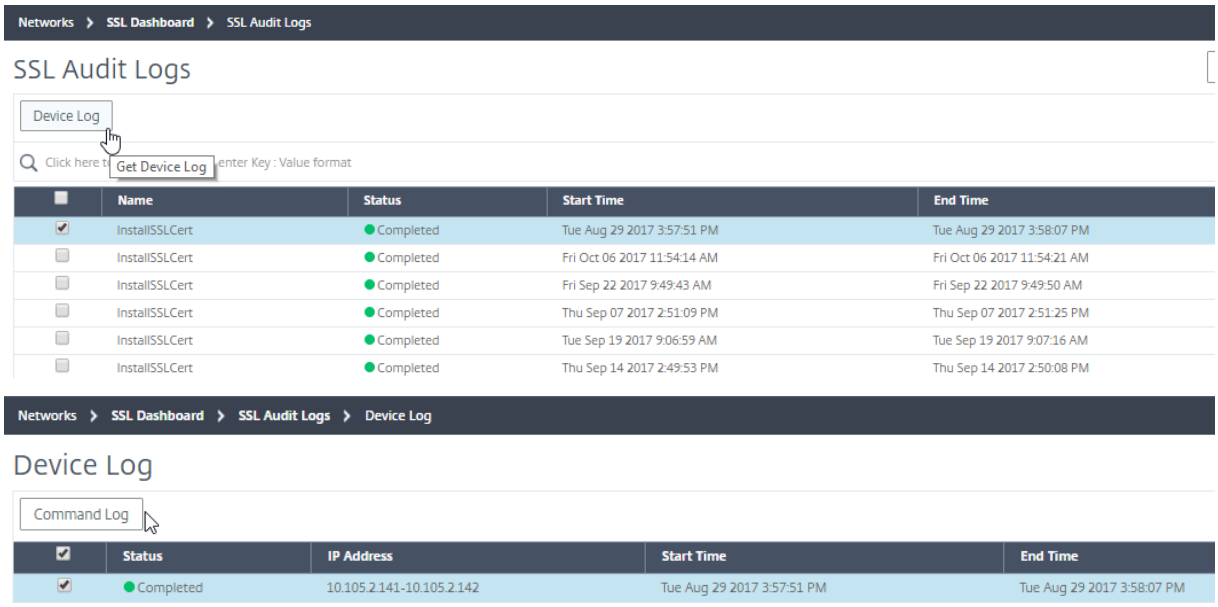
Citrix ADM で SSL 証明書のログの詳細を表示できるようになりました。ログの詳細には、SSL 証明書のインストール、SSL 証明書のリンクとリンク解除、SSL 証明書の更新、SSL 証明書の削除など、Citrix ADM で SSL 証明書を使用して実行された操作が表示されます。監査ログ情報は、複数の所有者を持つアプリケーションで実行された SSL 証

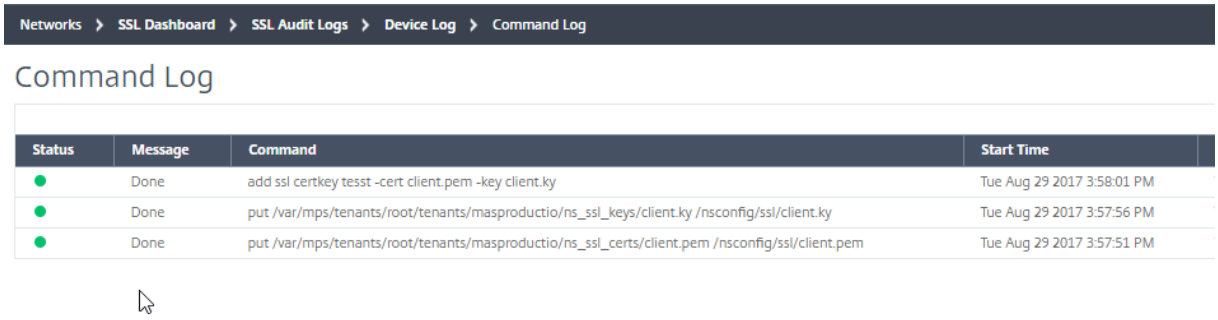
明書の変更を監視するときに役立ちます。

SSL 証明書を使用して Citrix ADM で実行された特定の操作の監査ログを表示するには、［ネットワーク］>［**SSL** ダッシュボード］の順に選択し、［監査ログ］を選択します。



SSL 証明書を使用して実行された特定の操作について、そのステータス、開始時刻、および終了時刻を表示できます。さらに、操作が実行されたインスタンスと、そのインスタンスで実行されたコマンドを表示できます。



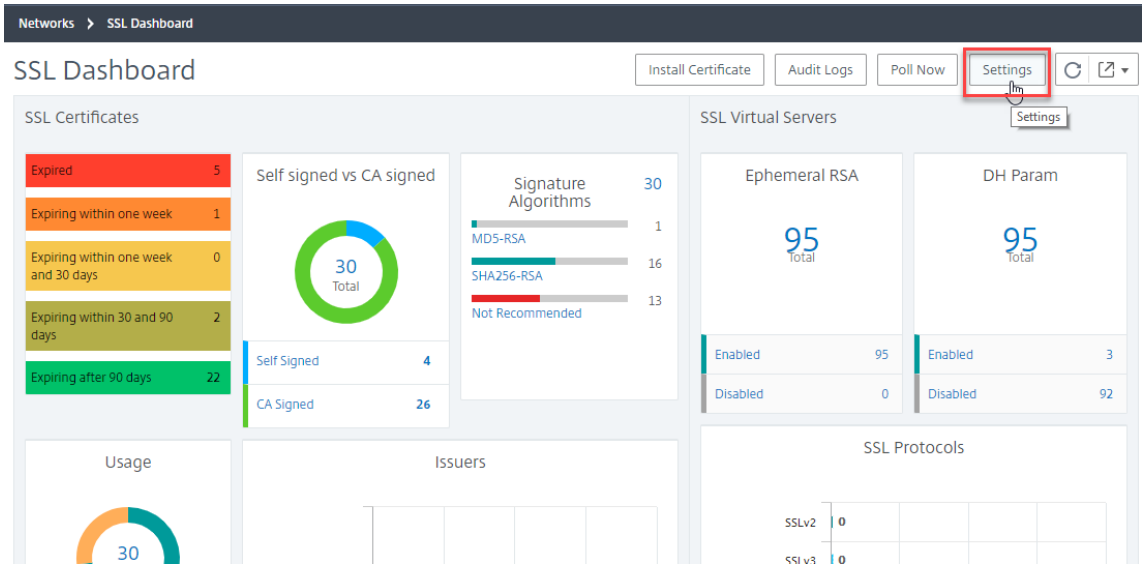


SSL ダッシュボードでデフォルトの **Citrix ADC** 証明書を除外する

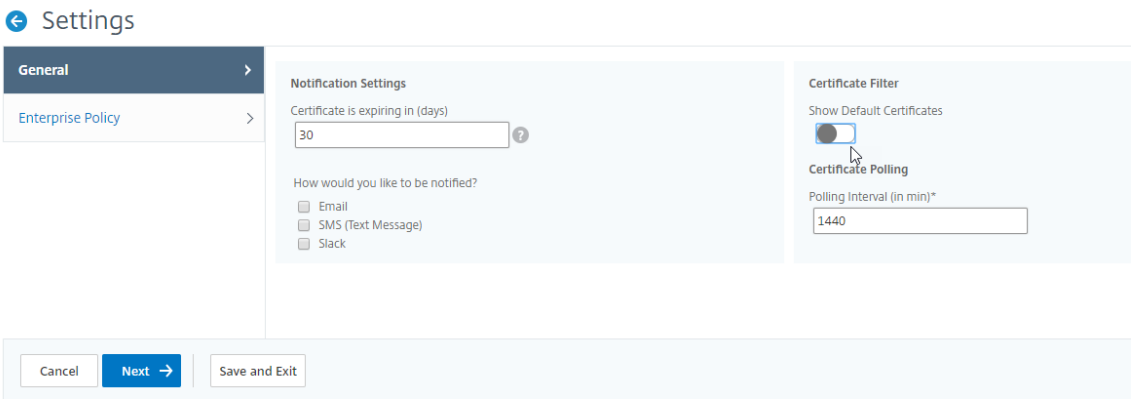
Citrix ADM では、設定に基づいて、SSL ダッシュボードのグラフに表示されるデフォルトの証明書の表示と非表示を切り替えることができます。デフォルトでは、デフォルトの証明書を含むすべての証明書が SSL ダッシュボードに表示されます。

SSL ダッシュボードでデフォルトの証明書を表示または非表示にするには**:**

1. Citrix ADM GUI で［ネットワーク］>［**SSL** ダッシュボード］に移動します。
2. [**SSL** ダッシュボード] ページで、[設定] をクリックします。



3. **[** 設定] ページで、[一般] を選択します。
4. [証明書フィルタ] セクションで、[既定の証明書を表示] を無効にし、[保存して終了] を選択します。



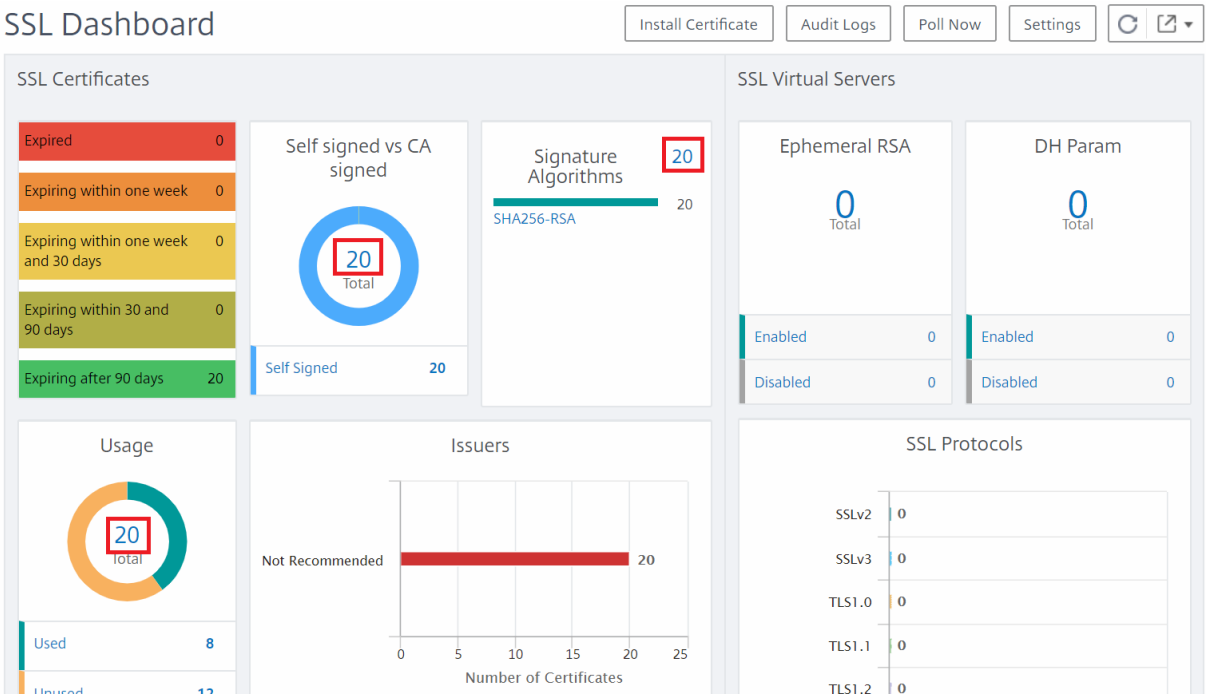
SSL 証明書のダウンロード

SSL 証明書は、インスタンスごとに個別に管理する必要があります。Citrix ADM は、複数のインスタンスに展開されたすべての証明書を表示します。

- 有効期限が切れる証明書を選択し、証明書の更新を自動化できます。
- ポリシーは、許可された証明書と署名機関の種類に基づいて設定および適用できます。
- SSL 証明書をダウンロードして更新し、後でアップロードすることもできます。

SSL 証明書をダウンロードするには、次の手順に従います。

1. Citrix ADM GUI で［ネットワーク］>［**SSL** ダッシュボード］に移動します。
2. [**SSL** ダッシュボード] ページで、グラフ内の SSL 証明書の総数をクリックします。



1. [**SSL** 証明書] ページで、ダウンロードする証明書をクリックします。たとえば、次の 1 週間で有効期限が切れるものをダウンロードするとします。
2. 「アクションの選択」リスト・ボックスから、「ダウンロード」を選択します。
3. 証明書がシステムにダウンロードされます。

このダッシュボードのレポートをエクスポートするには、次の手順に従います。

このページのレポートをエクスポートするには、このページの右上にある エクスポートアイコンをクリックします。[エクスポート] ページでは、次のいずれかの操作を実行できます。

1. [今すぐエクスポート] タブを選択します。レポートを PDF、JPEG、PNG、または CSV 形式で表示して保存します。
2. [スケジュールエクスポート] タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、電子メールまたは余裕期間メッセージでレポートを送信するには。

> 注
>
> - [毎週の繰り返し] を選択した場合は、レポートをスケジュールする平日を選択してください。
> - [毎月の繰り返し] を選択した場合は、レポートをスケジュールするすべての日をカンマで区切って入力します。

SSL 証明書の有効期限の通知を設定する

May 7, 2021

セキュリティ管理者は、証明書の有効期限が近づいたときの通知を構成し、それらの証明書を使用する Citrix ADC インスタンスに関する情報を含めることができます。通知を有効にすることで、SSL 証明書を遅れずに更新できます。

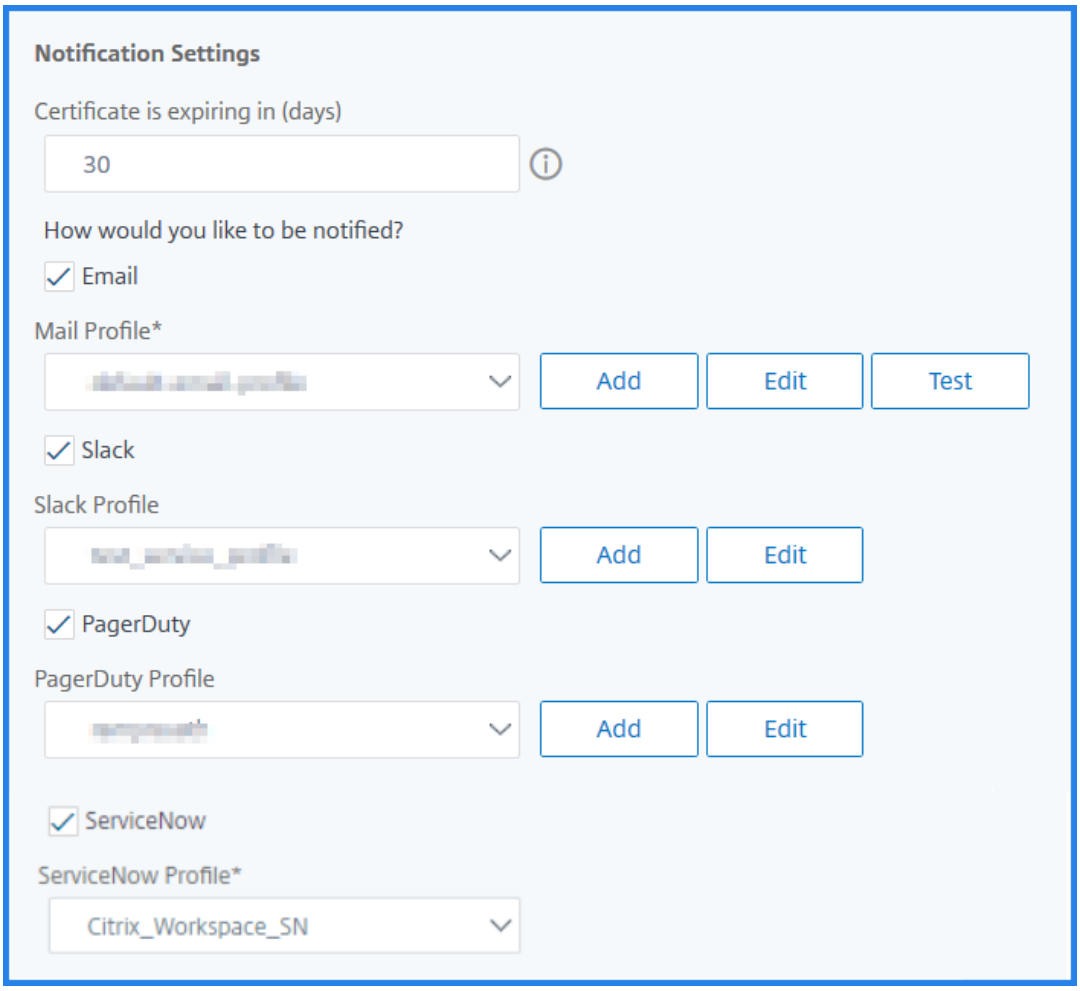
たとえば、証明書が満期になる 30 日前にメール配布リストを送信するようにメール通知を設定できます。

Citrix ADM からの通知を設定するには:

1. Citrix ADM で、［ネットワーク］>［**SSL** ダッシュボード］に移動します。
2. [**SSL** ダッシュボード] ページで、[設定] をクリックします。
3. [設定] ページで、[全般] をクリックします。
4. [通知設定**]** セクションで、有効期限より前の日数で通知を送信するタイミングを指定します。
5. 送信する通知の種類を選択します。メニューから通知タイプと配布リストを選択します。通知の種類を次に示します。
   - **Email** - メールサーバーとプロファイルの詳細を指定します。証明書の有効期限が近づくと、メールがトリガーされます。
   - **slack** slack プロファイルを指定します。証明書の有効期限が近づくと、通知が送信されます。

- **PagerDuty** -PagerDuty プロファイルを指定します。PagerDuty ポータルで構成された通知設定に基づいて、証明書の有効期限が近づくと通知が送信されます。
- **ServiceNow** -証明書の有効期限が近づくと、既定の ServiceNow プロファイルに通知が送信されます。

> 重要:
>
> Citrix Cloud ITSM アダプタが ServiceNow 用に構成され、Citrix ADM サービスと統合されていることを確認します。詳しくは、「Citrix ADM サービスと ServiceNow インスタンスの統合」を参照してください。



6. [保存して終了] をクリックします。

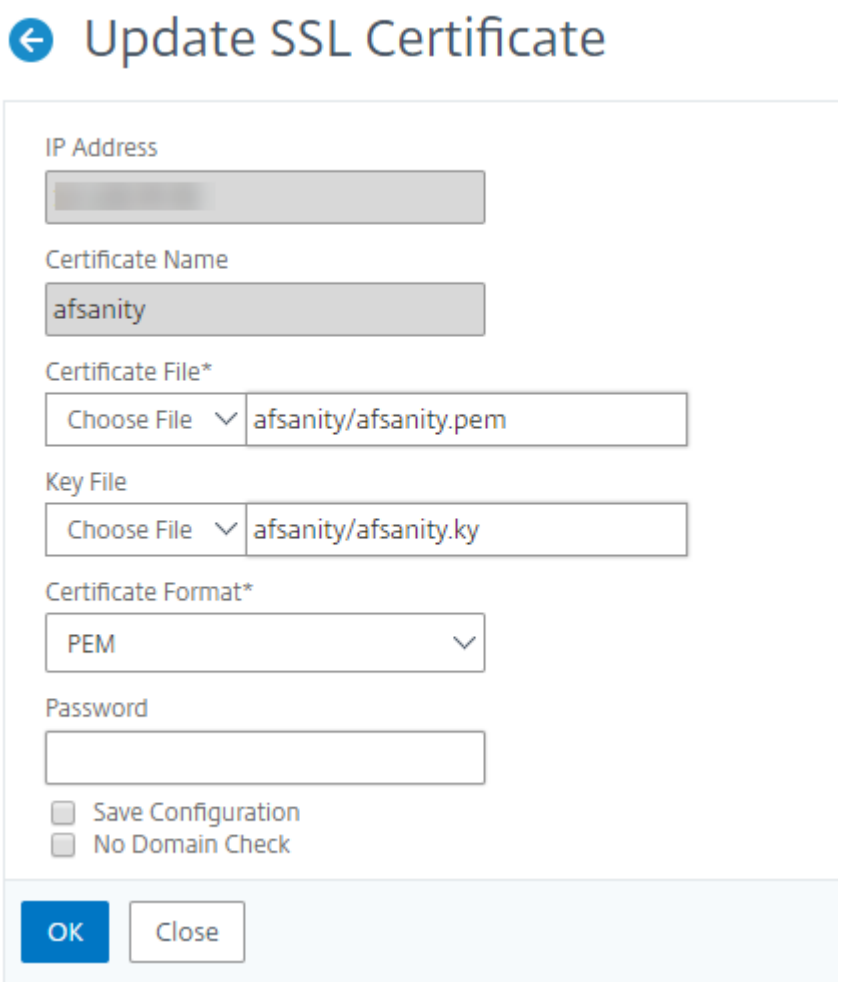
インストールされた証明書を更新する

May 7, 2021

認証局（CA）から更新された証明書を受け取った後、Citrix ADC インスタンスにログオンしなくても、Citrix ADM（Citrix ADM）から既存の証明書を更新できます。

Citrix ADM から **SSL** 証明書、キー、またはその両方を更新するには：

1. Citrix ADM で、［ネットワーク］>［**SSL** ダッシュボード］に移動します。
2. いずれかのグラフをクリックして、SSL 証明書の一覧を表示します。
3. ［**SSL Certificates**］ページで証明書を選択し、［**Update**］をクリックします。または、SSL 証明書をクリックして詳細を表示し、[**SSL** 証明書] ページの右上隅にある [更新] をクリックします。
4. ［**Update SSL Certificate**］ページで、証明書およびキーに必要な変更を加えて、［**OK**］をクリックします。



Citrix ADC インスタンスへの **SSL** 証明書のインストール

May 7, 2021

Citrix ADC インスタンスに SSL 証明書をインストールする前に、証明書が信頼できる CA によって発行されていることを確認してください。また、証明書キーのキー強度が 2,048 ビット以上であり、キーが安全な署名アルゴリズムで署名されていることを確認します。

別の **Citrix ADC** インスタンスから **SSL** 証明書をインストールするには:

選択した Citrix ADC インスタンスから証明書をインポートし、Citrix ADM GUI からターゲットとなる他の Citrix ADC インスタンスに適用することもできます。

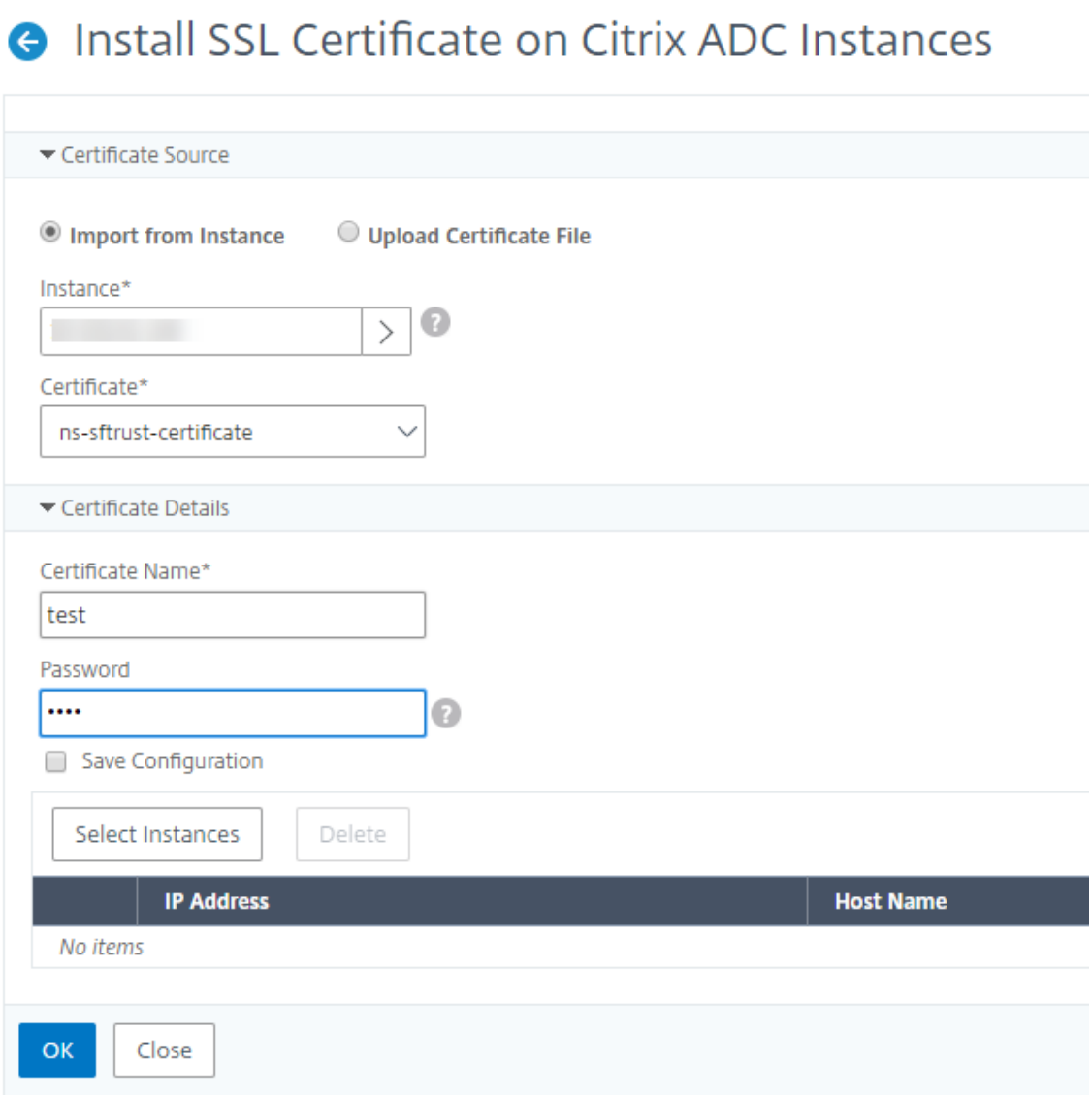
1. [ネットワーク] > [**SSL** ダッシュボード] に移動します。
2. SSL ダッシュボードの右上隅にある [証明書のインストール] をクリックします。
3. [**Citrix ADC** インスタンスへの **SSL** 証明書のインストール] ページで、次のパラメータを指定します。
   a) 証明書ソース

      [インスタンスからインポート] オプションを選択します。

      - 証明書のインポート元のインスタンスを選択します。
      - インスタンスのすべての SSL 証明書ファイルのリストから [Certificate] を選択します。

   b) 証明書詳細

      - 証明書名。証明書キーの名前を指定します。
      - パスワード。秘密キーを暗号化するためのパスワード。このオプションを使用して、暗号化された秘密キーをアップロードできます。
4. [インスタンスの選択] をクリックして、証明書をインストールする Citrix ADC インスタンスを選択します。
5. [**OK**] をクリックします。



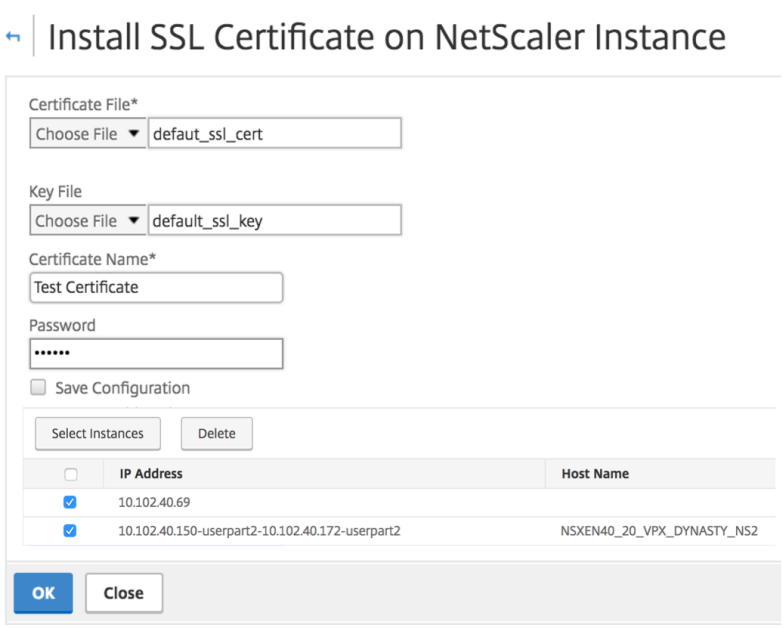
Citrix ADM から **SSL** 証明書をインストールするには:

1. Citrix ADM で、［ネットワーク］>［**SSL** ダッシュボード］に移動します。
2. ダッシュボードの右上隅にある [証明書のインストール] をクリックします。
3. ［**Citrix ADC** インスタンスへの **SSL** 証明書のインストール］ページで、次のパラメータを指定します。
   - 証明書ファイル:［ローカル］（ローカルマシン）または［アプライアンス］（証明書ファイルは Citrix ADM 仮想インスタンス上に存在する必要があります）を選択して、SSL 証明書ファイルをアップロードします。
   - **Key File** - キーファイルをアップロードします。
   - **Certificate Name** - 証明書のキーの名前を指定します。
   - **Password** - 秘密キーを暗号化するためのパスワード。このオプションを使用して、暗号化された秘密

キーをアップロードできます。

- インスタンスの選択 -証明書をインストールする Citrix ADC インスタンスを選択します。

4. 今後使用するために構成を保存するには、[構成を保存] チェックボックスをオンにします。
5. [**OK**] をクリックします。



証明書署名要求 **(CSR)** の作成

May 7, 2021

CSR（Certificate Signing Request：証明書署名要求）は、証明書が使用されるサーバー上で生成される暗号化済みテキストのブロックです。これには、組織名、共通名 (ドメイン名)、地域、国など、証明書に含まれる情報が含まれています。

Citrix ADM を使用して **CSR** を作成するには：

1. Citrix ADM で、[ネットワーク] > [**SSL** ダッシュボード] に移動します。
2. グラフのいずれかをクリックして、インストールされている SSL 証明書のリストを表示し、CSR を作成する証明書を選択し、[Select **Action]** ドロップダウンリストから **[**Create CSR**]** を選択します ** 。
3. [**Create Certificate Signing Request (CSR)**] ページで、CSR の名前を指定します。
4. 次のいずれかを行います：
   - **Upload a key** - [**I have a Key**] オプションを選択します。キーファイルをアップロードするには、[ローカル]（ローカルマシン）または [アプライアンス]（キーファイルは Citrix ADM 仮想インスタンスに存在している必要があります）を選択します。

- キーを作成する -[キーがありません] オプションを選択し、次のパラメータを指定します。

暗号化アルゴリズム	キーの種類。たとえば、RSA などがあります。
キーファイル名	RSA キーが保存されたファイル名。
キーサイズ	キーサイズ（ビット）。
公開指数値	表示されるドロップダウンリストから [**3**] または [**F4**] を選択します。この値は、RSA キーを作成するのに必要な暗号アルゴリズムの一部です。
キーの形式	デフォルトでは PEM が選択されています。SSL 証明書には、PEM が推奨されるキーの形式です。
PEM エンコーディングアルゴリズム	ドロップダウンリストで、生成された RSA キーの暗号化に使用するアルゴリズム（**DES** または **DES3**）を選択します。このアルゴリズムを選択する場合は、PEM パスフレーズを指定する必要があります。
PEM パスフレーズ	[PEM エンコーディングアルゴリズム] を選択した場合は、パスフレーズを入力します。
PEM パスフレーズの確認	PEM パスフレーズを確認します。

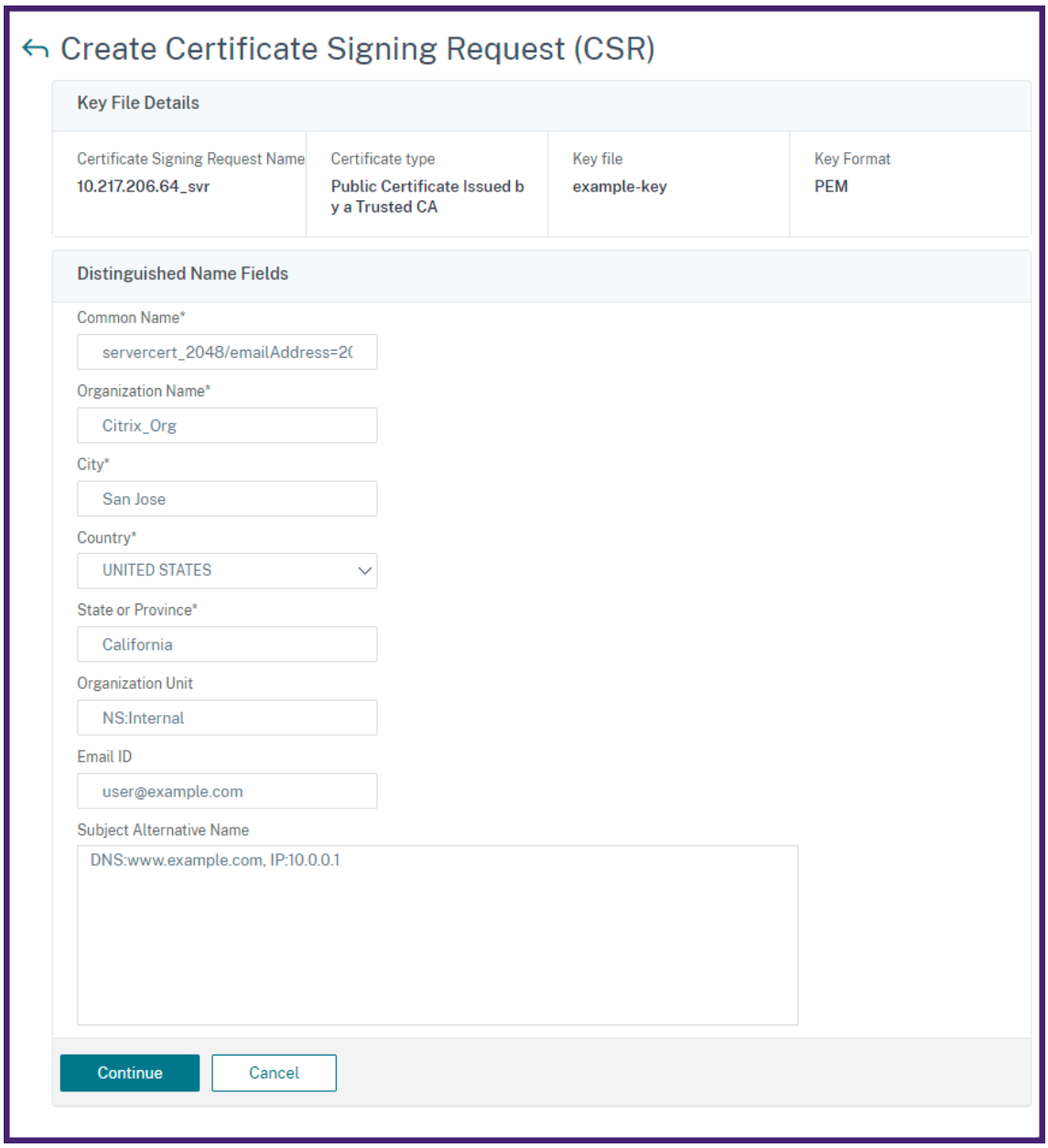
5. ［続行］をクリックします。
6. 次のページで、詳細を入力します。

   大半のフィールドには、選択した証明書のサブジェクトから抽出したデフォルト値が設定されます。サブジェクトには、共通名、組織名、州、国などの詳細が含まれています。

   [サブジェクトの別名] フィールドで、単一の証明書を使用して、ドメイン名や IP アドレスなどの複数の値を指定できます。サブジェクトの別名を使用すると、単一の証明書で複数のドメインを保護できます。

   ドメイン名と IP アドレスを次の形式で指定します。

```
DNS:<Domain name>, IP:<IP address>
<!--NeedCopy-->
```

この例では、`10.0.0.1`と`www.example.com`がセキュリティで保護されています。

フィールドを確認し、[**Continue**] をクリックします。

> 注
>
> ほとんどの CA が電子メールによる証明書の送信を受け付けています。CA は、CSR の送信元の電子メールアドレスに有効な証明書を返します。

SSL 証明書のリンクとリンク解除

May 7, 2021

複数の証明書をまとめて関連付けて、証明書パッケージを作成します。証明書を別の証明書に関連付けるとき、1 番目の証明書の発行者が 2 番目の証明書のドメインと一致しなければなりません。たとえば、証明書 A を証明書 B にリンクする場合、証明書 A の「発行者」は証明書 B の「ドメイン」と一致する必要があります。

Citrix ADM を使用して **SSL** 証明書を別の証明書にリンクするには:

1. Citrix ADM で、［ネットワーク］>［**SSL** ダッシュボード］に移動します。
2. いずれかのグラフをクリックして、SSL 証明書の一覧を表示します。
3. リンクする証明書を選択し、**[** アクションの選択**]** ドロップダウンリストから **[** リンク**]** を選択します。
4. 一致する証明書の一覧から関連付ける対象の証明書を選択して、［**OK**］をクリックします。

   > 注
   >
   > 一致する証明書がない場合は「No certificate found to link.」というメッセージが表示されます。

Citrix ADM を使用して **SSL** 証明書のリンクを解除するには:

1. Citrix ADM で、［ネットワーク］>［**SSL** ダッシュボード］に移動します。
2. いずれかのグラフをクリックして、SSL 証明書の一覧を表示します。
3. リンクされた証明書のいずれかを選択し、**[** アクションの選択**]** ドロップダウンリストから **[** リンク解除**]** を選択します。
4. ［**OK**］をクリックします。

   > 注
   >
   > 選択した証明書が別の証明書に関連付けられていない場合、「Certificate does not have any CA link.」というメッセージが表示されます。

エンタープライズポリシーの構成

May 7, 2021

Citrix ADM（Citrix Application Delivery Management ADM）では、エンタープライズポリシーを構成し、すべての信頼できる CA、セキュリティで保護された署名アルゴリズムを追加し、証明書キーの推奨キー強度を選択できます。Citrix ADC インスタンスにインストールされている証明書のいずれかがエンタープライズポリシーに追加されていない場合、SSL 証明書ダッシュボードには、これらの証明書の発行元が［推奨されていません］と表示されます。

また、証明書のキー強度が、企業のポリシーで推奨されているキー強度と同じでない場合、SSL 証明書のダッシュボードには、これらのキーの強度が［Not Recommended］として表示されます。

Citrix ADM でエンタープライズポリシーを構成するには:

1. Citrix ADM で、［ネットワーク］>［**SSL** ダッシュボード］の順に選択し、［設定］をクリックします。
2. [設定] ページで、[エンタープライズポリシー] アイコンをクリックして、信頼された CA とセキュリティで保護された署名アルゴリズムをすべて追加し、証明書とキーの推奨キー強度を選択します。
   - 推奨されるキー強度 -アルゴリズムのセキュリティとキーのビット数を示します。
   - 推奨される署名アルゴリズム -アプリケーションの署名付きトークンの問題を示します。
   - 推奨信頼された **CA** -デジタル証明書を発行する信頼されたエンティティを示します。[**+**] アイコンをクリックして、エンティティを追加します。
   - 推奨 **SSL** プロトコル -TLS/SSL バージョンを示します。
3. [完了] または [保存して終了] をクリックして、エンタープライズポリシーを保存します。

Citrix ADC インスタンスからの **SSL** 証明書のポーリング

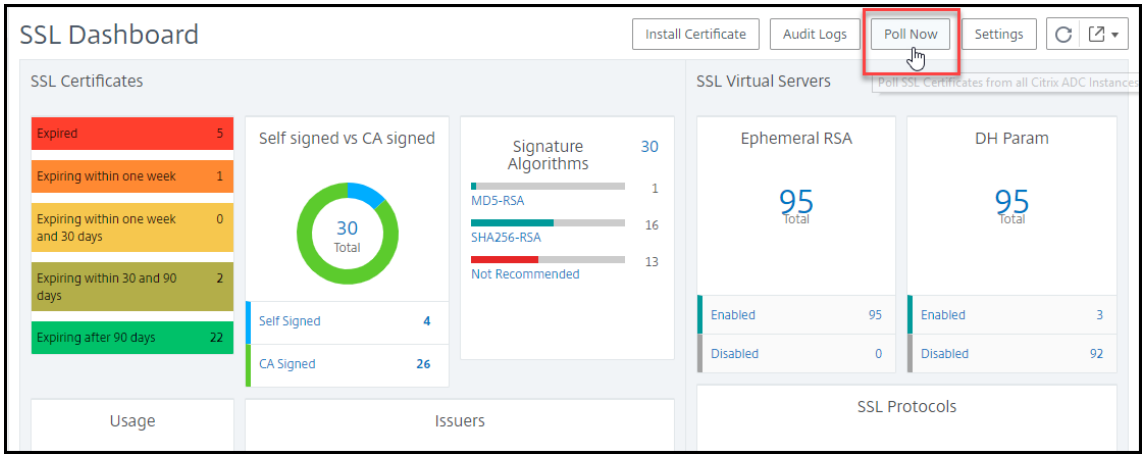
May 7, 2021

Citrix Application Delivery Management（Citrix ADM）は、NITRO 呼び出しとセキュアコピー（SCP）プロトコルを使用して、24 時間に 1 回、SSL 証明書を自動的にポーリングします。SSL 証明書を手動でポーリングして、Citrix ADC インスタンスで新しく追加された SSL 証明書を検出することもできます。すべての Citrix ADC インスタンスの SSL 証明書をポーリングすると、ネットワークに大きな負荷がかかります。

すべての Citrix ADC インスタンスの SSL 証明書をポーリングする代わりに、選択したインスタンスの SSL 証明書のみを手動でポーリングできます。

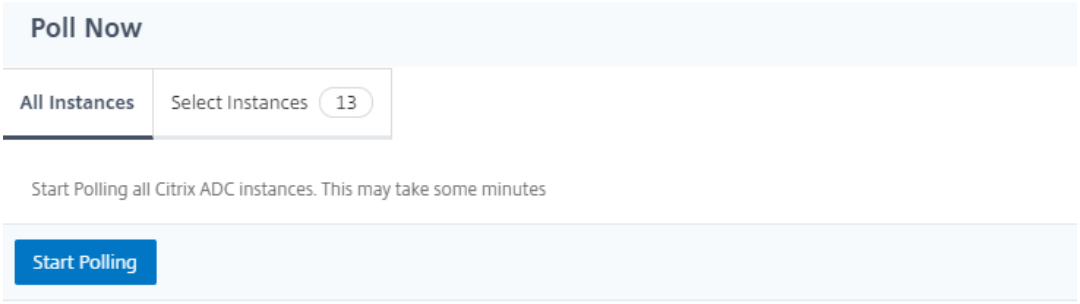
Citrix ADC インスタンスで **SSL** 証明書をポーリングするには:

1. Citrix ADM で、［ネットワーク］>［**SSL** ダッシュボード］に移動します。
2. [**SSL** ダッシュボード] ページの右上隅にある [今すぐポーリングする] をクリックします。

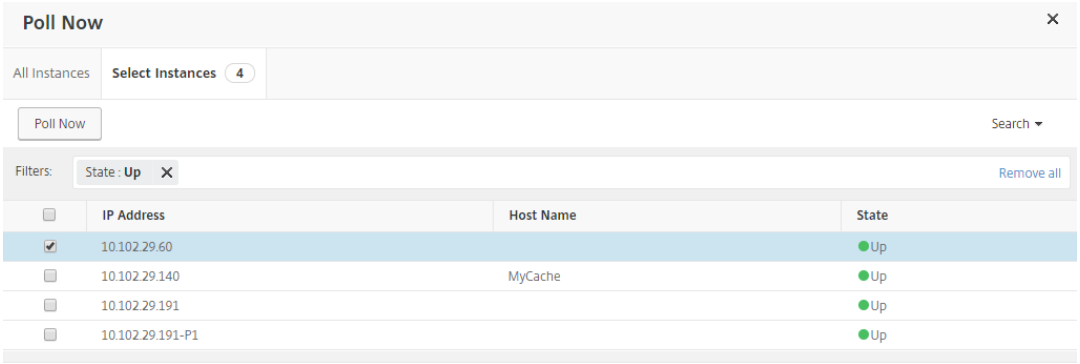


3. [**Poll Now**] ページが表示され、ネットワーク内のすべての Citrix ADC インスタンスをポーリングするか、選択したインスタンスをポーリングするかを選択できます。

   - すべての Citrix ADC インスタンスの SLL 証明書をポーリングするには、[すべてのインスタンス] タブを選択し、[ポーリング開始] をクリックします。



   - 特定のインスタンスをポーリングするには、[Select **Instances**] タブを選択し、リストからインスタンスを選択し、[**Poll Now**] をクリックします。



このダッシュボードのレポートをエクスポートするには、次の手順に従います。

このページのレポートをエクスポートするには、このページの右上にある エクスポートアイコンをクリックします。[エクスポート] ページでは、次のいずれかの操作を実行できます。

1. [今すぐエクスポート] タブを選択します。レポートを PDF、JPEG、PNG、または CSV 形式で表示して保存します。
2. [スケジュールエクスポート] タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、電子メールまたは余裕期間メッセージでレポートを送信するには。

> 注
>
> - [毎週の繰り返し] を選択した場合は、レポートをスケジュールする平日を選択してください。
> - [毎月の繰り返し] を選択した場合は、レポートをスケジュールするすべての日をカンマで区切って入力します。

IP アドレス管理 (IPAM) の構成

May 7, 2021

ADM IPAM は、ADM 管理設定で IP アドレスを自動割り当ておよび解放する機能を提供します。次の IP プロバイダーを使用して定義されたネットワークまたは IP 範囲から IP を割り当てることができます。

- ADM 内蔵 IP アドレス管理プロバイダ。
- Infoblox IPAM ソリューション。詳しくは、「インフォブロックス DDI」を参照してください。

現在、ADM IPAM は次の用途で使用できます。

- **StyleBook**s: 設定を作成するときに、IP を仮想サーバーに自動割り当てます。
- **Kubernetes** 入力: 仮想 IP アドレスを Kubernetes クラスタ内の入力設定に自動的に割り当てます。
- **API** ゲートウェイ: API プロキシに IP アドレスを自動割り当てます。

また、ADM によって管理される各ネットワークまたは IP 範囲で、割り当てられた IP アドレスと使用可能な IP アドレスを追跡することもできます。

外部 IP アドレスプロバイダーの追加

ADM には、IP および IP 範囲を管理するための IP アドレス管理プロバイダーが組み込まれています。ADM に外部 IP アドレスプロバイダーを追加することもできます。

> 重要 開始する前に、外部 IP アドレスプロバイダーで次のアクセス許可が有効になっていることを確認してください。
>
> - プロバイダーに存在するネットワークを照会する機能。
> - 新しいネットワークを登録します。
> - 既存のネットワークの登録を解除します。
> - ネットワーク内の IP アドレスを予約します。
> - ネットワークから IP アドレスを解放します。
> - ネットワークから使用された IP アドレスを取得します。
> - ネットワークから利用可能な IP アドレスを取得します。

ADM に外部 IP プロバイダーソリューションを追加するには、次の手順を実行します。

1. [ネットワーク**] > [IPAM**] に移動します。
2. 「プロバイダ」で、「追加」をクリックします。
3. IP プロバイダーを追加するには、次の詳細を指定します。
    - 名前 -ADM で使用する IP プロバイダー名を指定します。
    - [ベンダー]: リストから IPAM ベンダーを選択します。

- **URL** -ADM 環境で IP アドレスを割り当てる IP アドレス管理ソリューションの URL を指定します。URL を次の形式で指定してください。

```
https://<host name>
<!--NeedCopy-->
```

例: `https://myinfoblox.example.com`

- [ユーザー名]: IPAM ソリューションにログインするためのユーザー名を指定します。
- パスワード -IPAM ソリューションにログインするためのパスワードを指定します。

4. [追加] をクリックします。

ネットワークの追加

ADM 管理設定で IP アドレス管理を使用するネットワークを追加します。

1. [ネットワーク**] > [IPAM**] に移動します。
2. [ネットワーク] で、[追加] をクリックします。
3. 次の詳細を指定します。
   - ネットワーク名 -ADM でネットワークを識別するネットワーク名を指定します。
   - プロバイダ -リストからプロバイダを選択します。

     このリストには、ADM に追加されたプロバイダが表示されます。
   - [ネットワークの種類]-要件に基づいて、リストから [**IP** 範囲] または [**CIDR**] を選択します。
   - ネットワーク値 -ネットワーク値を指定します。

     > 注:
     >
     > ADM IPAM は IPv4 アドレスのみをサポートします。

     [**IP** 範囲] には、次の形式でネットワーク値を指定します。

```
<first-IP-address>-<last-IP-address>
<!--NeedCopy-->
```

例:

```
10.0.0.20-10.0.0.100
<!--NeedCopy-->
```

CIDR の場合は、次の形式でネットワーク値を指定します。

```
<IP-address>/<subnet-mask>
<!--NeedCopy-->
```


例:

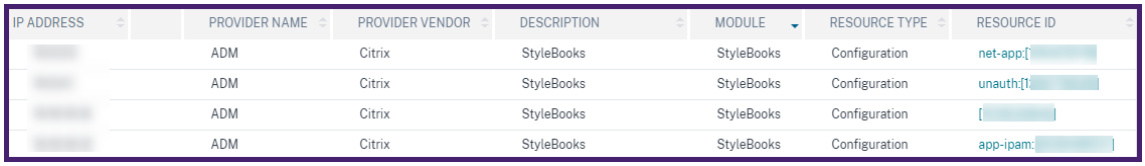
```
10.70.124.0/24
<!--NeedCopy-->
```

4. [作成] をクリックします。

割り当てられた **IP** アドレスの表示

IPAM ネットワークから割り当てられた IP アドレスの詳細を表示するには、次の手順を実行します。

1. [ネットワーク**] > [IPAM**] に移動します。
2. [ネットワーク] タブで、[割り当てられた **IP** をすべて表示] をクリックします。



IP ADDRESS	PROVIDER NAME	PROVIDER VENDOR	DESCRIPTION	MODULE	RESOURCE TYPE	RESOURCE ID
[redacted]	ADM	Citrix	StyleBooks	StyleBooks	Configuration	net-app:[
[redacted]	ADM	Citrix	StyleBooks	StyleBooks	Configuration	unauth:[1
[redacted]	ADM	Citrix	StyleBooks	StyleBooks	Configuration	[
[redacted]	ADM	Citrix	StyleBooks	StyleBooks	Configuration	app-ipam:

このペインには、IP アドレス、プロバイダー名、プロバイダーのベンダー、および説明が表示されます。また、この IP アドレスを予約したリソースの詳細も表示されます。

- **Module**: IP アドレスを予約した ADM モジュールを表示します。たとえば、StyleBooks が IP アドレスを予約した場合、この列には StyleBooks がモジュールとして表示されます。
- リソースタイプ: そのモジュールのリソースタイプを表示します。StyleBooks モジュールでは、設定リソースタイプだけが IPAM ネットワークを使用します。したがって、この列の下に [構成] が表示されます。
- リソース **ID**: リンク付きの正確なリソース ID を表示します。このリンクをクリックして、IP アドレスを使用しているリソースにアクセスします。構成リソースタイプの場合、構成パック ID がリソース ID として表示されます。

> 注**:**
>
> IP アドレスを解放する場合は、解放する IP アドレスを選択し、[割り当てられた **IP** を解放] をクリックします。

構成ジョブ

May 7, 2021

Citrix Application Delivery Management（ADM）構成管理プロセスにより、ネットワーク内の複数の Citrix ADC インスタンス間で、構成変更、システムのアップグレード、およびその他のメンテナンスアクティビティを適切にレプリケーションできます。

Citrix ADM では、これらのすべてのアクティビティを 1 つのタスクとして複数のデバイスで簡単に実行できる構成ジョブを作成できます。構成ジョブとテンプレートは、Citrix ADM 上で最も反復的な管理タスクを単一のタスクに簡素化します。構成ジョブには、1 つまたは複数の管理対象デバイスで実行できる一連の構成コマンドが含まれています。

構成ジョブでは、ローカルストレージから他のアプライアンスに対して、SSH コマンドを使用して構成コマンドを実行したり、SCP を使用してファイルのコピーを実行したりできます。たとえば、HA フェールオーバーや HA アップグレードのスケジュールを設定できます。

Citrix ADM で以下の 4 つのオプションのいずれかを使用して、構成ジョブを作成できます。これらのいずれかを使用して、構成ジョブを実行するためのシステムへのコマンドおよび指示の再利用可能なソースを作成します。

1. 設定テンプレート
2. インスタンス
3. ファイル
4. Record and Play

構成テンプレート**:**

ジョブを作成し、一連の構成コマンドをテンプレートとして保存するときに、構成テンプレートを作成できます。これらのテンプレートは、[Create Jobs] ページで保存すると、[Create Template] ページに自動的に表示されます。

> 注**:**
> [名前の変更] オプションは、既定の構成テンプレートでは無効になっています。ただし、カスタム構成テンプレートの名前は変更できます。

次のいずれかのテンプレートを使用できます。

構成エディタ: 構成エディタを使用して CLI コマンドを入力し、構成をテンプレートとして保存し、ジョブを設定するために使用できます。

作り込みテンプレート: 構成テンプレートのリストから選択できます。これらのテンプレートには CLI コマンドの構文が用意されており、変数の値を指定できます。組み込みテンプレートは、説明とともに下の表に一覧表示されます。組み込みテンプレートオプションを使用して、ジョブにスケジュールを指定できます。ジョブとは、管理対象インスタンスで実行できる一連の構成コマンドのことです。たとえば、組み込みテンプレートオプションを使用して、Syslog サーバーを構成するジョブにスケジュールを指定できます。また、ジョブをすぐに実行するか、後段階で実行するようにジョブをスケジュールすることもできます。

インスタンス**:**

Citrix ADC リリース 11.0 以降を実行している Citrix ADC SDX インスタンスのシングルバンドル・アップグレードを実行できます。シングルバンドルのアップグレードを実行するには、Citrix ADM 組み込みタスクを使用します。実行構成または保存された構成を抽出し、同じタイプの別の Citrix ADC インスタンスでコマンドを実行することによって、Citrix ADC インスタンスをアップグレードすることもできます。このアップグレードにより、一方のインスタンスの設定を他方のインスタンスに複製できます。

ファイル:

ローカルマシンから構成ファイルをアップロードして、ジョブを作成できます。

ファイル使用の利点

- 任意のテキストファイルを使用して、構成コマンドの再利用可能なソースを作成できます。
- 書式設定は一切必要ありません。
- ファイルはローカルマシンに保存できます。

新しいファイルを作成および保存するか、既存のファイルをインポートして、コマンドを実行できます。

録音と再生**:**

Create job を使用して独自の CLI コマンドを入力するか、［記録と再生］ボタンを使用して Citrix ADC セッションからコマンドを取得できます。ジョブを実行すると、選択したインスタンスの ns.conf の変更が記録され、Citrix ADM にコピーされます。

関連トピック

- 構成ジョブで SCP（put）コマンドを使う方法
- 構成ジョブで変数を使用する方法
- 修正コマンドから構成ジョブを作成する方法
- 構成テンプレートを使用して監査テンプレートを作成する方法
- 記録と再生を使用して構成ジョブを作成する方法
- Citrix ADM でマスター構成テンプレートを使用する方法

このダッシュボードのレポートをエクスポートするには、次の手順に従います。

このページのレポートをエクスポートするには、このページの右上にある エクスポートアイコンをクリックします。[エクスポート] ページでは、次のいずれかの操作を実行できます。

1. [今すぐエクスポート] タブを選択します。レポートを PDF、JPEG、PNG、または CSV 形式で表示して保存します。
2. [スケジュールエクスポート] タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、電子メールまたは余裕期間メッセージでレポートを送信するには。

> 注
>
> - [毎週の繰り返し] を選択した場合は、レポートをスケジュールする平日を選択してください。
> - [毎月の繰り返し] を選択した場合は、レポートをスケジュールするすべての日をカンマで区切って入力します。

構成ジョブの作成

May 7, 2021

ジョブとは、1 つまたは複数の管理対象インスタンスに対して作成および実行できる構成コマンドのセットです。

ジョブを作成して、インスタンス間で設定を変更できます。ネットワーク上で複数のインスタンスでの構成の複製を実行し、また Citrix Application Delivery Management（ADM）GUI を使用して設定タスクの記録と再生を実行し、CLI コマンドに変換できます。

Citrix ADM 構成ジョブ機能を使用して、構成ジョブの作成、電子メール通知の送信、および作成されたジョブの実行ログの確認を行うことができます。

Citrix ADM で構成ジョブを作成するには:

1. [ネットワーク] > [構成ジョブ] に移動します。
2. [ジョブの作成] をクリックします。
3. [**Create Job**] ページの [**Select Configuration**] タブで、[Job Name] を指定し、リストから [**Instance Type**] を選択します。
4. [構成ソース] リストで、作成する構成ジョブテンプレートを選択します。選択したテンプレートのコマンドを追加します。
   - コマンドを入力するか、保存されている構成テンプレートから既存のコマンドをインポートできます。
   - 構成ジョブでジョブを作成するときに、構成エディタで異なるタイプの複数のテンプレートを追加することもできます。
   - [**Configuration Source**] リストから別のテンプレートを選択し、テンプレートを構成エディタにドラッグします。テンプレートタイプは、構成テンプレート、組み込みテンプレート、マスター構成、レコードと再生、インスタンスとファイルです。

   > 注
   >
   > マスター構成ジョブの展開テンプレートを初めて追加する場合は、異なる種類のテンプレートを追加すると、ジョブテンプレート全体がマスター構成の種類になります。

   設定エディタでコマンドを再配置したり、並べ替えたりすることもできます。コマンドラインをドラッグアンドドロップすると、コマンドを別の行に移動できます。テキストボックスでコマンドライン番号を変更するだけで、コマンドラインを 1 行から任意のターゲットラインに移動または再配置することもできます。構成ジョブの編集中に、コマンドラインを並べ替えたり、並べ替えたりすることもできます。

   変数を定義して、これらのパラメータに異なる値を割り当てたり、複数のインスタンス間でジョブを実行したりできます。構成ジョブの作成または編集中に定義したすべての変数を、1 つの統合ビューで確認できます。「変数のプレビュー」(Preview Variables) タブをクリックして、設定ジョブの作成または編集中に定義した 1 つの統合ビューで変数をプレビューします。

   構成エディタのすべてのコマンドに対して、ロールバックコマンドをカスタマイズできます。カスタマイズされたコマンドを指定するには、カスタムロールバックオプションを有効にします。

> 重要 カスタムロールバックを有効にするには、[ジョブの作成] ウィザードを完了します。[実行] タブで、[コマンド 失敗時に] リストから [成功したコマンドのロールバック] オプションを選択します。

5. [**Select Instanc** es] タブで、構成監査を実行するインスタンスを選択します。
   a) Citrix ADC の高可用性ペアでは、プライマリノードまたはセカンダリノードに対してローカルに構成ジョブを実行できます。ジョブを実行するノードを選択します。
      - [プライマリノードで実行する]: プライマリノードでのみジョブを実行するには、このオプションを選択します。
      - **[** セカンダリノードで実行]: セカンダリノードでのみジョブを実行するには、このオプションを選択します。

      プライマリノードとセカンダリノードの両方を選択して、同じ構成ジョブを実行することもできます。プライマリノードまたはセカンダリノードを選択しない場合、構成ジョブはプライマリノード上で自動的に実行されます。
   b) [**Add Instances**] をクリックし、リストからインスタンスを選択します。[**OK**] をクリックします。
   c) [次へ] をクリックします。
6. 「変数値の指定」タブには、次の 2 つのオプションがあります。
   a) 入力ファイルをダウンロードして、コマンドで定義した変数の値を入力し、Citrix ADM サーバーにファイルをアップロードします。
   b) すべてのインスタンスに定義した変数に共通の値を入力します。
   c) [次へ] をクリックします。
7. [ジョブプレビュー] タブで、各インスタンスで実行するコマンドを評価および確認します。このタブには、[構成の選択] タブでロールバックコマンドが指定されている場合は、ロールバックコマンドも表示されます。
8. [**Execute**] タブで、ジョブを今すぐ実行するか、後でジョブを実行するようにスケジュールするかを選択します。

   また、[コマンドが失敗した場合] ボックスの一覧から、コマンドが失敗した場合に **Citrix** ADM が実行する必要があるアクションのいずれかを選択します。
   - エラーを無視して続行: Citrix ADM は、失敗したコマンドを無視し、選択したインスタンスに対して残りのコマンドを実行します。

     > 注**:**
     >
     > この操作では、進行中の構成ジョブを中止することはできません。
   - 後続の実行を **Citrix ADM**: 実行中にコマンドが失敗すると、残りのコマンドが停止します。
   - 成功したコマンドのロールバック: 実行中にコマンドが失敗した場合、Citrix ADM は正常に実行されたコマンドをリストアします。

カスタムロールバックが有効な場合、Citrix ADM は、失敗したコマンドに対応するロールバックコマンドを実行します。

9. [完了] をクリックします。

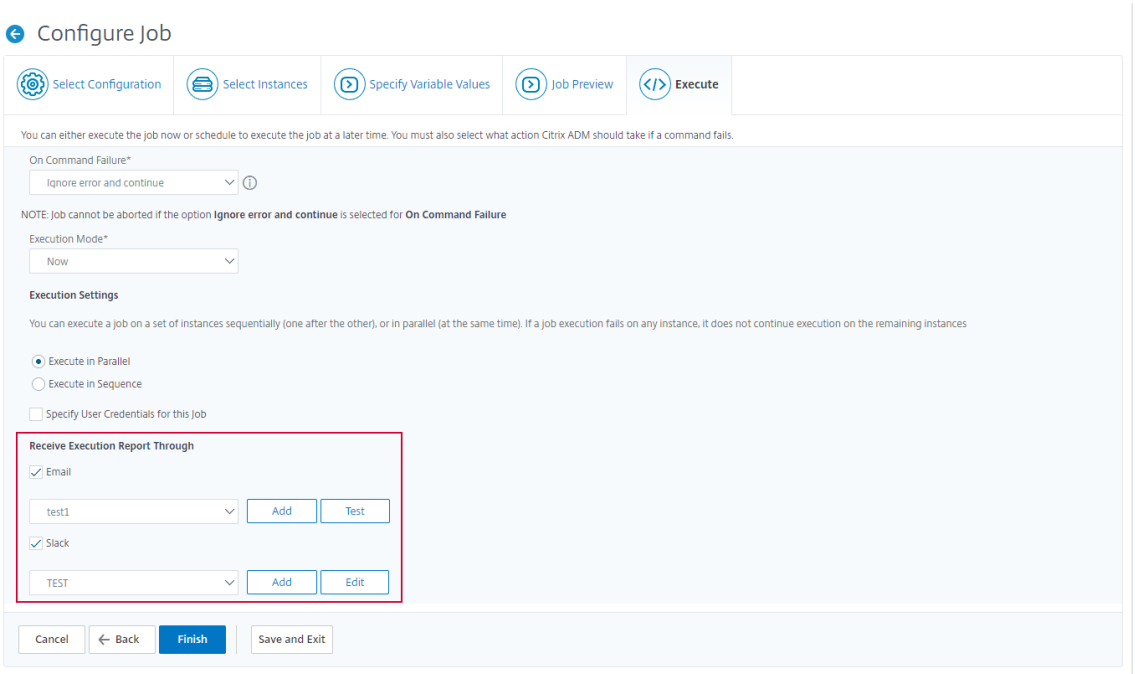
ジョブにメールと **Slack** 通知を送信するには:

ジョブが実行またはスケジュールされるたびに、メールと Slack 通知が送信されるようになりました。通知には、関連する詳細とともに、ジョブの成功または失敗などの詳細が含まれます。

1. [ネットワーク] > [構成ジョブ] に移動します。
2. メールと Slack 通知を有効にするジョブを選択し、[編集] をクリックします。
3. [実行] タブで、[実行レポートの受信方法] ペインに移動します。
   - [**Email**] チェックボックスをオンにして、実行レポートの送信先となる電子メール配布リストを選択します。

     電子メール配布リストを追加する場合は、[追加] をクリックし、電子メールサーバーの詳細を指定します。
   - 「**Slack** 」チェック・ボックスを選択し、実行レポートの送信先となる Slack チャネルを選択します。

     Slack プロファイルを追加する場合は、[追加] をクリックし、必要な Slack チャンネルのプロファイル名 **、チャンネル名、** トークンを指定します。

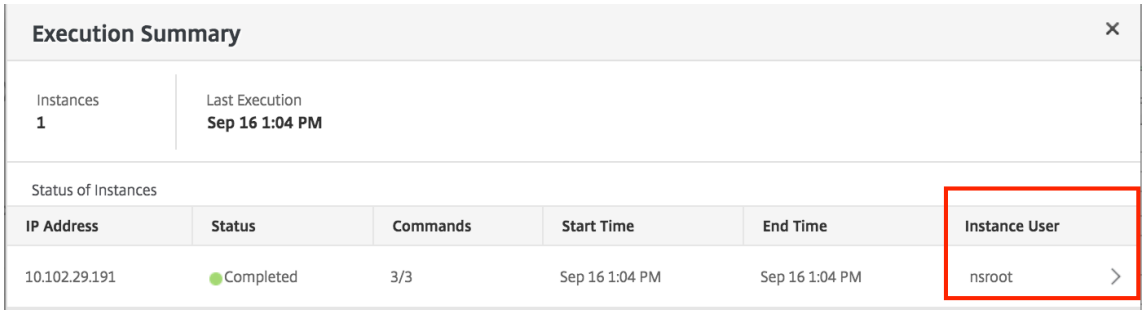


4. [完了] をクリックします。

実行要約の詳細を表示する手順は、次のとおりです。

1. [ネットワーク] > [構成ジョブ] に移動します。

2. 実行サマリーを表示するジョブを選択し、「詳細」をクリックします。
3. 「実行サマリー」をクリックすると、次の項目が表示されます。
    - 実行されたジョブのインスタンスのステータス
    - コマンドはジョブで実行される
    - ジョブの開始時刻と終了時刻、および
    - インスタンスユーザーの名前



レコードアンドプレイを使用して構成ジョブを作成する

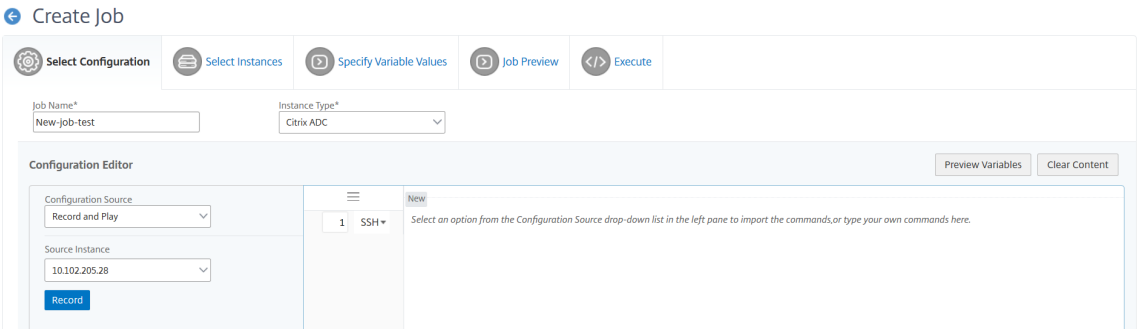
May 7, 2021

Citrix ADC GUI を使用して Citrix ADC インスタンスを構成することに慣れている場合、構成タスクを作成して複数の Citrix ADC インスタンスで実行するための正確な CLI コマンドを呼び出すことが困難な場合があります。

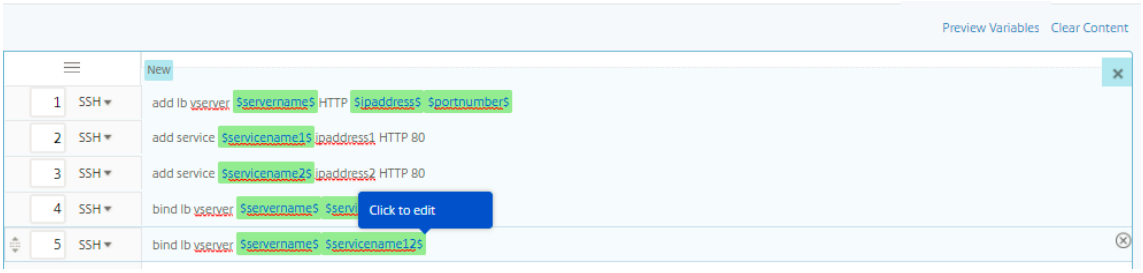
Citrix Application Delivery Management（ADM）を使用すると、Citrix ADC インスタンスの GUI を使用して実行された構成タスクを記録し、CLI コマンドに変換できます。変換された CLI コマンドから構成タスクを作成し、複数のインスタンスでそのタスクを実行できます。

GUI 構成を記録して設定タスクに変換するには、次の手順を実行します。

1. [**Networks**] > [**Configuration Jobs**] の順に選択してから、[**Create Job**] をクリックします。
2. ジョブ名とインスタンスのタイプを指定します。
3. [構成ソース] リストから [記録と再生] を選択し、構成を記録するソースインスタンスを選択します。[**Record**] をクリックします。



4. **Citrix ADC** の **GUI** が開きます。構成タスクに含める機能と設定を構成します。次に、Citrix ADC GUI ウィンドウを閉じ、構成エディターで「停止」をクリックします。左ペインにコマンドがリンクとして表示されます。コマンドを右側のウィンドウ枠にドラッグし、[次へ] をクリックします。



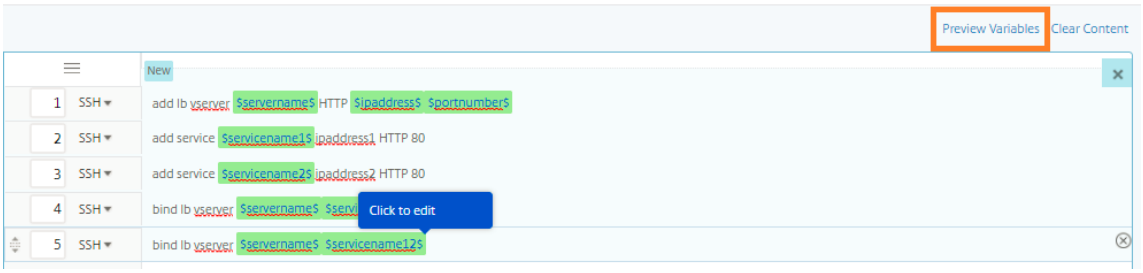
その後、コンフィグレーションエディタでコマンドを並べ替えたり、並べ替えたりすることができます。コマンドラインをドラッグアンドドロップすると、コマンドを別の行に移動できます。テキストボックスでコマンドライン番号を変更するだけで、コマンドラインを 1 行から任意のターゲットラインに移動または再配置することもできます。

5. 構成ジョブの作成または編集中に定義したすべての変数を、1 つの統合ビューで確認できます。

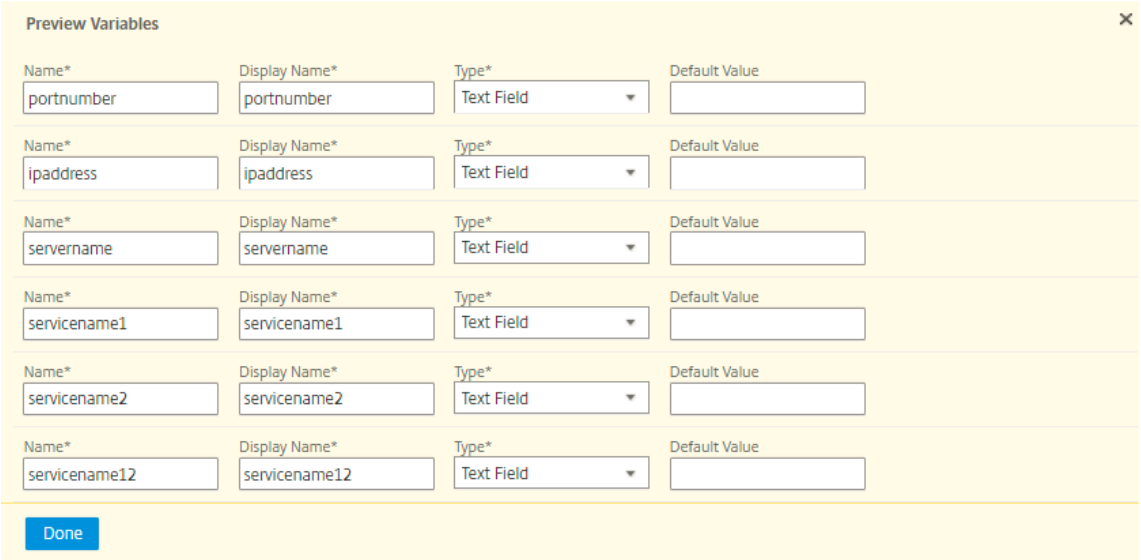
6. 次のいずれかの操作を行って、すべての変数を 1 つの統合ビューに表示します。

   - 構成ジョブの作成中に、[ネットワーク**] > [**構成ジョブ] に移動し、[ジョブの作成] を選択します。[**Create Job**] ページでは、構成ジョブの作成時に追加したすべての変数を確認できます。
   - 構成ジョブの編集中に、[ネットワーク**] > [**構成ジョブ] に移動し、[ジョブ名] を選択して [編集] をクリックします。[ジョブの構成] ページでは、構成ジョブの作成時に追加されたすべての変数を確認できます。

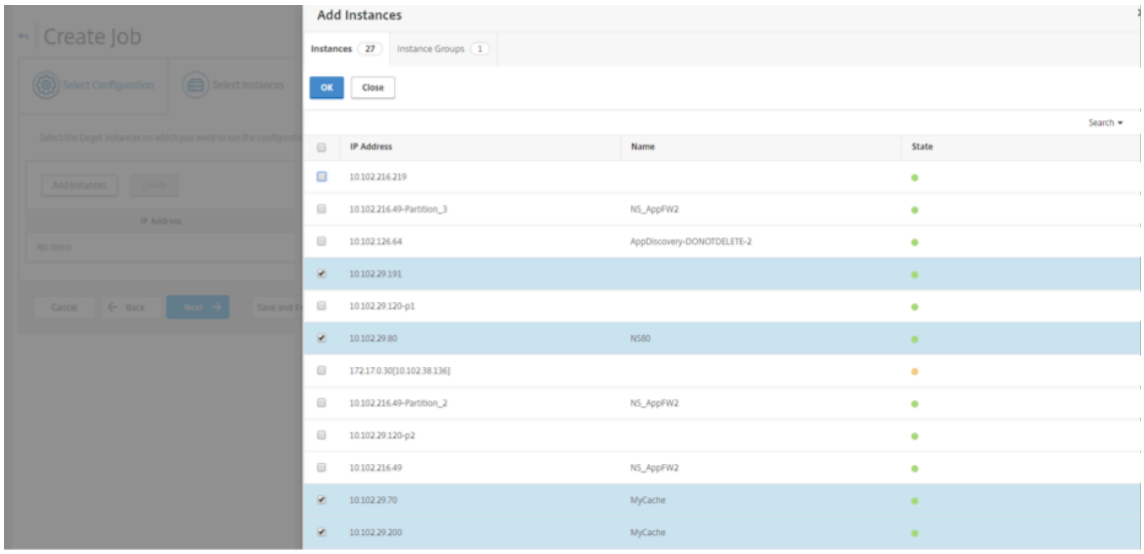
7. 次に、「変数のプレビュー」(Preview Variables) タブをクリックして、設定ジョブの作成または編集中に定義した 1 つの統合ビューで変数をプレビューできます。



8. 新しいポップアップウィンドウが表示され、名前、表示名、タイプ、デフォルト値などの変数のすべてのパラメータが表形式で表示されます。これらのパラメータを編集および修正することもできます。パラメータを編集または変更したら、[完了] ボタンをクリックします。



9. [**Add Instances**] をクリックし、設定ジョブを実行するインスタンスを選択します。[**OK**] をクリックした後、[**Next**] をクリックします。



10. コマンドで変数を指定した場合は、**[Specified Variable Values**] タブで、次のいずれかのオプションを選択して、インスタンスの変数を指定します。

    - 変数値の入力ファイルをアップロード: [入力キーファイルのダウンロード] をクリックして、入力ファイルをダウンロードします。入力ファイルで、コマンドで定義した変数の値を入力し、Citrix ADM サーバーにファイルをアップロードします。
    - すべてのインスタンスの共通変数値: 変数の値を入力します。選択したテンプレートによって、変数は変わります。

変数値を含む入力ファイルは、設定ジョブで (同じファイル名で) 保持されます。設定ジョブの作成または編集中に、以前に使用およびアップロードした入力ファイルを表示および編集できます。

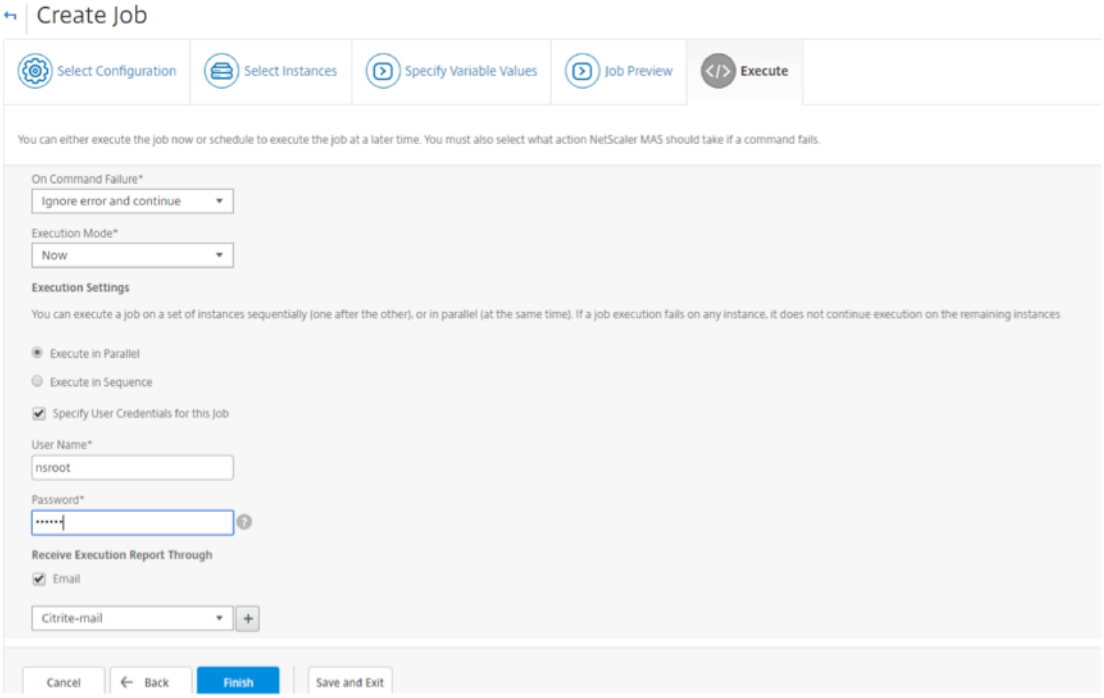
構成ジョブの作成中に実行構成ジョブを表示するには、[ネットワーク] > [構成ジョブ] に移動し、[ジョブの作成] をクリックします。**[** ジョブの作成] ページ。[変数値の指定] タブで、[すべてのインスタンスに共通変数値] オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします（同じファイル名を維持します)。

構成ジョブの編集中にすでに実行されている構成ジョブを表示するには、[ネットワーク] > [構成ジョブ] に移動し、[ジョブ名] を選択して [編集] をクリックします。[ジョブの設定] ページの [変数値の指定] タブで、[すべてのインスタンスに共通変数値] オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします (同じファイル名を使用)。10. [**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。

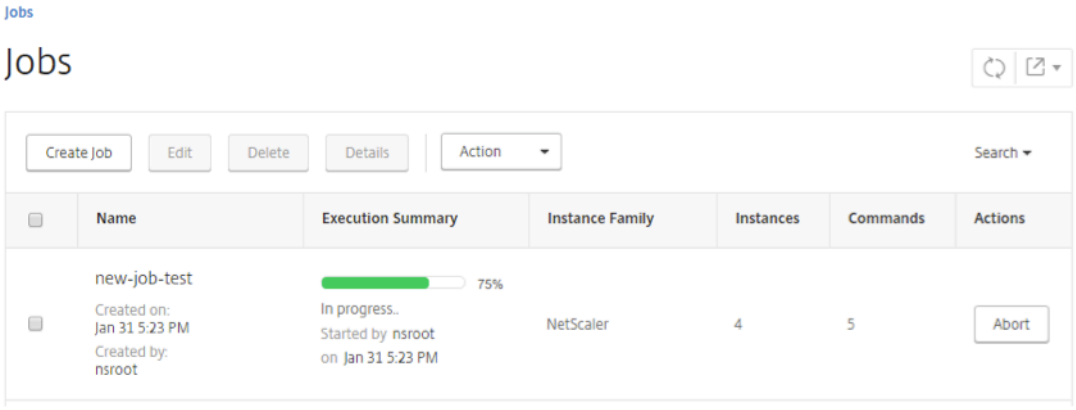
11. [**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。

12. [**Execute**] タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。コマンドが失敗した場合に Citrix ADM が実行する必要があるアクションを選択することもできます。

    また、承認されたユーザーが管理対象インスタンスでジョブを実行できるようにすることもできます。また、ジョブの成功または失敗に関する電子メール通知を他の詳細とともに送信するかどうかを選択できます。



13. [**Jobs**] ページでは、すべてのインスタンスでの設定タスク実行の進行状況を表示できます。



構成ジョブを使用して、1 つのインスタンスから複数のインスタンスに構成を複製する

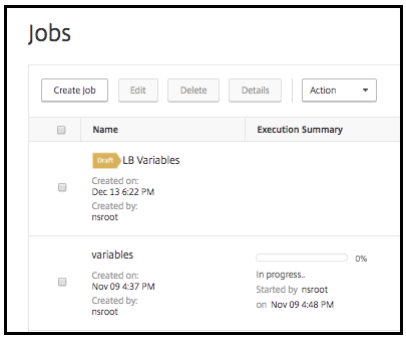
May 7, 2021

展開環境の Citrix ADC インスタンスで、負荷分散と AppFlow の両方を構成している場合があります。ただし、AppFlow 構成のみを他の Citrix ADC インスタンスにレプリケートします。

Citrix Application Delivery Management（ADM）の構成ジョブ機能を使用して、Citrix ADC インスタンスから AppFlow 構成を抽出し、複数のインスタンスにレプリケートできます。

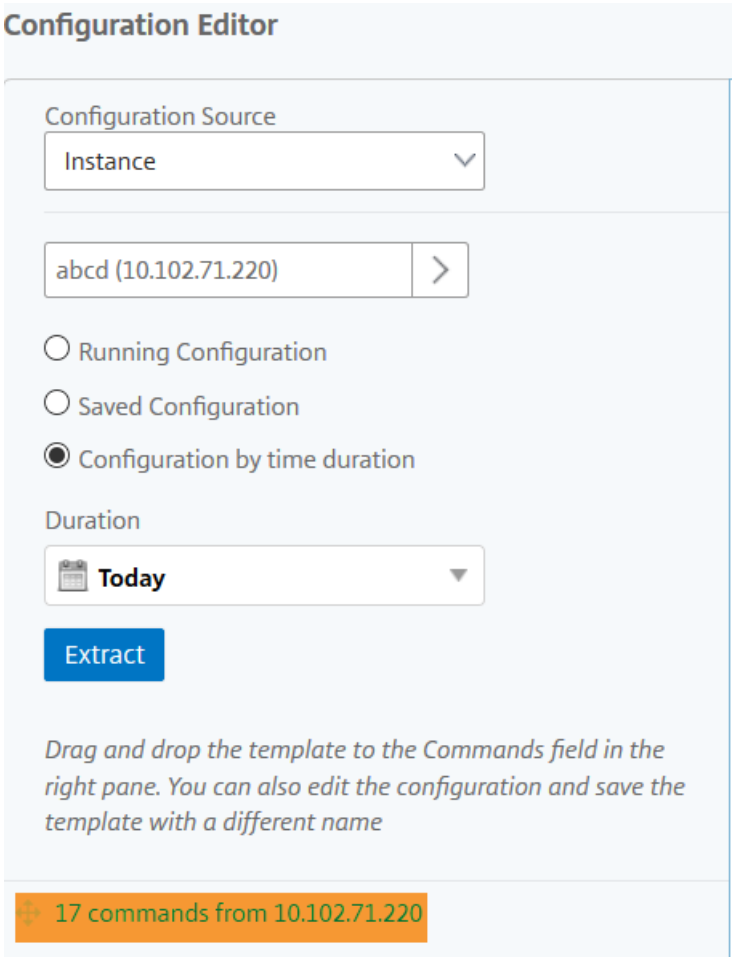
あるインスタンスから他の **Citrix ADC** インスタンスに構成を取得して複製するには：

1. ［**Networks**］>［**Configuration Jobs**］の順に選択してから、［**Create Job**］をクリックします。



2. ジョブ名とインスタンスのタイプを指定します。
3. 「構成ソース」として「インスタンス」を選択し、構成を複製するソース・インスタンスを選択します。抽出する構成のタイプを選択します。[期間による構成] を選択した場合は、この構成を実行した期間を設定し、[抽出] をクリックします。

   選択した期間内にそのインスタンスで実行されるコマンドの数が、次の図で強調表示されているように画面に表示されます。



4. 右ペインの [Commands] フィールドにコマンドをドラッグします。

FEO に関するコマンドのみを保持します。負荷分散に関するコマンド、または他のすべての構成に関するコマンドは手動で削除し、［**Next**］をクリックします。

5. [**Add Instanc** es] をクリックし、FEO 設定を適用するインスタンスを追加します。[**OK**] をクリックし、[次へ] をクリックします。

   コマンドに変数を指定した場合は、［Specify Variable Values］タブで［**Download Input Key File**］をクリックします。ダウンロードしたファイルで、変数の値を指定し、そのファイルを Citrix ADM にアップロードします。

[**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。

［実行］タブで［完了］をクリックして、選択した Citrix ADC インスタンスでジョブを実行します。

構成ジョブでの変数の使用

May 7, 2021

設定ジョブは、1 つまたは複数の管理対象インスタンスで実行できる設定コマンドのセットです。複数のインスタンスで同じ設定を実行する場合、設定で使用されるパラメーターに異なる値を使用することが必要な場合があります。変数を定義して、これらのパラメータに異なる値を割り当てたり、複数のインスタンス間でジョブを実行したりできます。

たとえば、負荷分散仮想サーバーを追加し、2 つのサービスを追加し、それらのサービスをその仮想サーバーにバインドするという、基本的な負荷分散構成を考えてみましょう。ここでは、2 つのインスタンスで同じ構成を使用するが、仮想サーバーとサービスの名前および IP アドレスに異なる値を使用する必要があるとします。これを実現するには、変数を使用して仮想サーバーとサービスの名前および IP アドレスを定義することで、構成ジョブ機能を使用します。

この例では、次のコマンドと変数を使用します。

```
1 add lb vserver \*\*servername\*\* HTTP \*\*ipaddress\*\* \*\*portnumber
      \*\*
2
3 add service \*\*servicename1\*\* \*\*ipaddress1\*\* HTTP 80
4
```



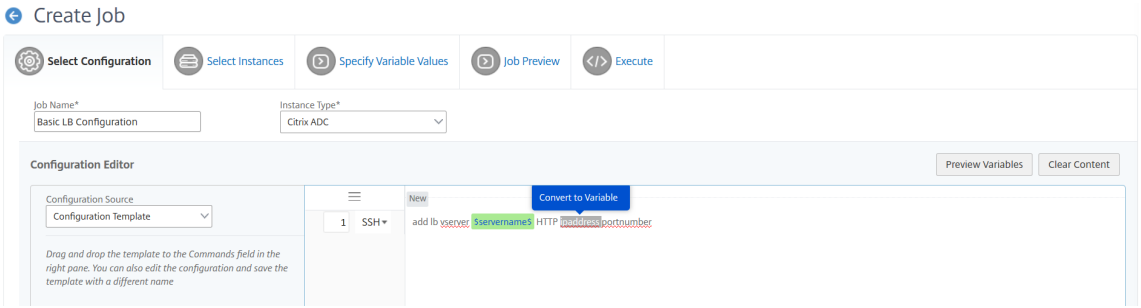
```
add service \*\*servicename2\*\* \*\*ipaddress2\*\* HTTP 80

bind lb vserver \*\*servername\*\* \*\*servicename1\*\*

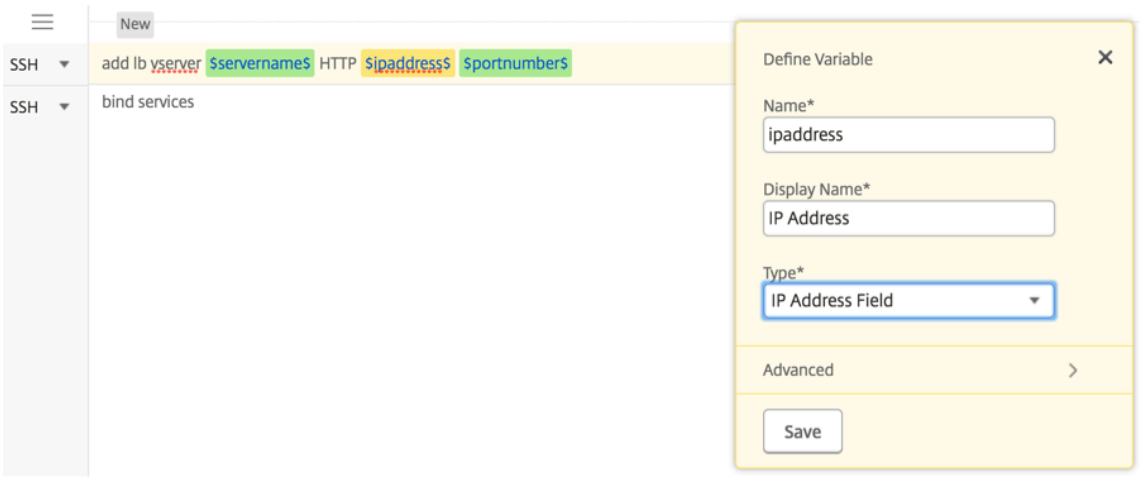
bind lb vserver \*\*servername\*\* \*\*servicename2\*\*
<!--NeedCopy-->
```

Citrix ADM で変数を定義して構成ジョブを作成するには:

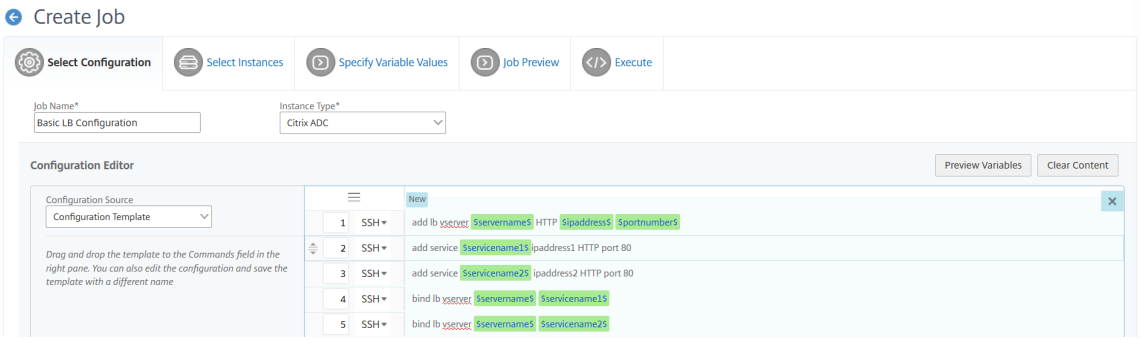
1. [ネットワーク] > [構成ジョブ] に移動します。
2. [ジョブの作成] をクリックします。
3. [**Create Job**] ページで、ジョブの名前、インスタンスタイプ、設定タイプなどのカスタムジョブパラメータを選択します。
4. [Configuration Editor] でコマンドを入力して、負荷分散仮想サーバー、2 つのサービスを追加し、それらのサービスをその仮想サーバーにバインドします。変数に変換する値をダブルクリックして選択し、[変数に変換] をクリックします。たとえば、負荷分散サーバー`ipaddress`の IP アドレスを選択し、次の図に示すように [変数に変換] をクリックします。



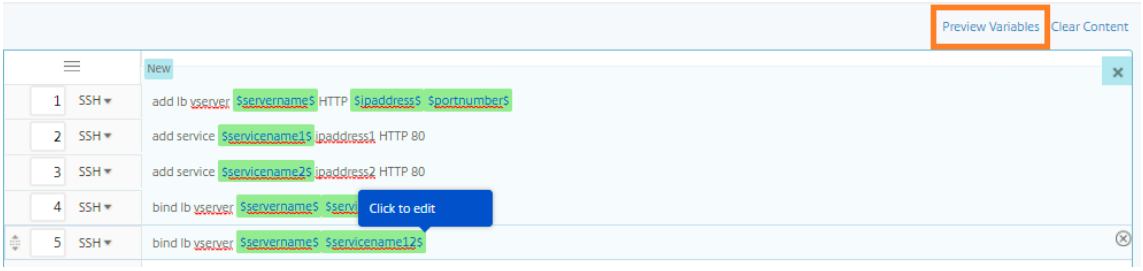
5. 変数の値を囲むドル記号が表示されたら、変数をクリックして、名前、表示名、タイプなどの変数の詳細をさらに指定します。変数のデフォルト値をさらに指定する場合は、「詳細」(**Advanced**) オプションをクリックすることもできます。[保存] をクリックし、[次へ] をクリックします。



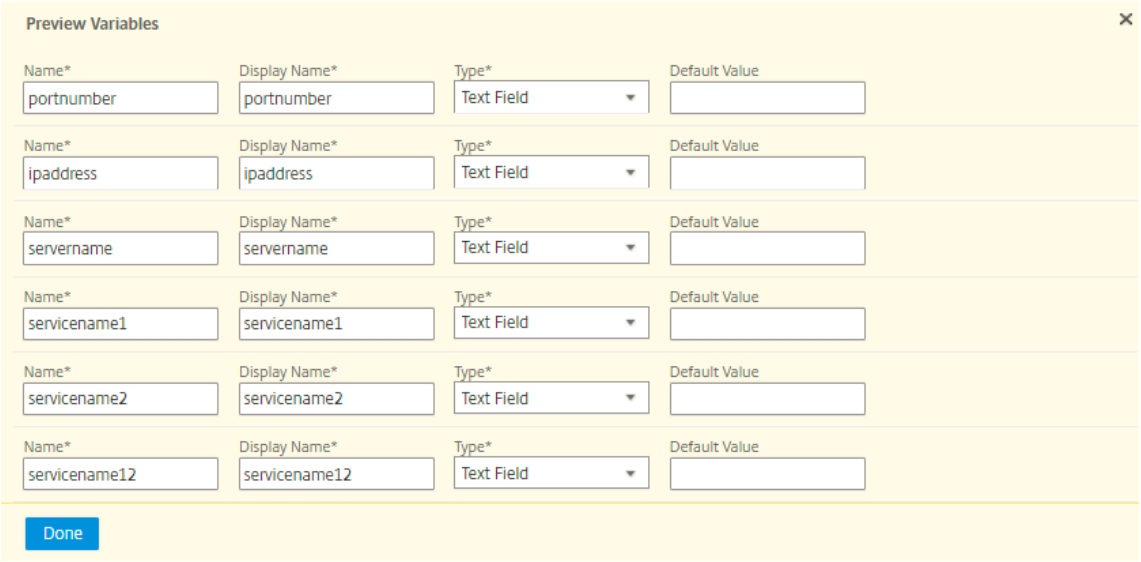
残りのコマンドを入力し、すべての変数を定義します。



6. 構成ジョブの作成または編集中に定義したすべての変数を、1 つの統合ビューで確認できます。
7. 次のいずれかの操作を行って、すべての変数を 1 つの統合ビューに表示します。
   - 構成ジョブの作成中に、[ネットワーク] > [構成ジョブ] に移動し、[ジョブの作成] を選択します。[**Create Job**] ページでは、構成ジョブの作成時に追加したすべての変数を確認できます。
   - 構成ジョブの編集中に、[ネットワーク] > [構成ジョブ] に移動し、[ジョブ名] を選択して [編集] をクリックします。[ジョブの構成] ページでは、構成ジョブの作成時に追加されたすべての変数を確認できます。
8. 次に、「変数のプレビュー」(Preview Variables) タブをクリックして、設定ジョブの作成または編集中に定義した 1 つの統合ビューで変数をプレビューできます。



9. 新しいポップアップウィンドウが表示され、名前、表示名、タイプ、デフォルト値などの変数のすべてのパラメータが表形式で表示されます。これらのパラメータを編集および修正することもできます。パラメータを編集または変更したら、[完了] ボタンをクリックします。



10. その後、コンフィグレーションエディタでコマンドを並べ替えたり、並べ替えたりすることができます。コマンドラインをドラッグアンドドロップすると、コマンドを別の行に移動できます。テキストボックスでコマンドライン番号を変更するだけで、コマンドラインを 1 行から任意のターゲットラインに移動または再配置することもできます。

11. 構成ジョブを実行するインスタンスを選択します。

12. [変数値の指定] タブで、[変数値の入力ファイルをアップロード] オプションを選択し、[入力キーファイルのダウンロード] をクリックします。例では、各インスタンス上のサーバー名、サーバーとサービスの IP アドレス、ポート番号、およびサービス名を指定する必要があります。ファイルを保存し、アップロードします。値が正確に定義されていない場合、システムはエラーをスローする可能性があります。

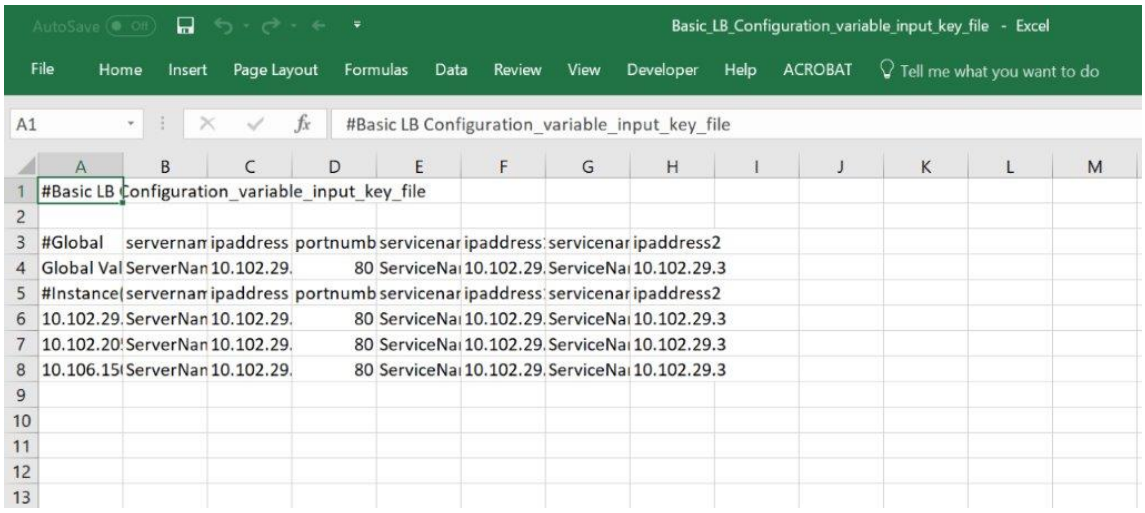
13. 入力キーファイルはローカルシステムにダウンロードされ、以前に選択した各 Citrix ADC インスタンスの変数値を指定し、［アップロード］をクリックして入力キーファイルを Citrix Application Delivery Management（ADM）にアップロードすることで編集できます。［次へ］をクリックします。入力キーファイルがローカルシステムにダウンロードされ、以前に選択した各 Citrix ADC インスタンスの変数値を指定することで編集できます。

    > 注:
    >
    > 入力キーファイルでは、変数は 3 つのレベルで定義されています。
    >
    > ```
    > 1    - グローバルレベル
    > ```
    >
    > - インスタンスグループレベル
    > - インスタンスレベル

    グローバル変数は、すべてのインスタンスに適用される変数値です。インスタンスグループレベルの変数の値は、グループ内で定義されているすべてのインスタンスに適用されます。インスタンスレベルの変数の値は、特定のインスタンスにのみ適用されます。

Citrix ADM は、インスタンスレベルの値を優先します。個々のインスタンスの変数に値が指定されていない場合、Citrix ADM はグループレベルで指定された値を使用します。グループレベルで値が指定されていない場合、Citrix ADM はグローバルレベルで指定された変数値を使用します。3 つのレベルすべてにわたって変数の入力を指定すると、Citrix ADM はインスタンスレベル値をデフォルト値として使用します。

14. [アップロード] をクリックして、入力キーファイルを Citrix ADM にアップロードします。［次へ］をクリックします。



> 重要
>
> Mac から CSV ファイルをアップロードすると、CSV ファイルはコンマではなくセミコロンで保存されます。これにより、入力ファイルをアップロードしてジョブを実行したときに、構成が失敗します。Mac を使用している場合は、テキストエディタを使用して必要な変更を行い、ファイルをアップロードします。

15. また、すべてのインスタンスで共通の変数値を指定し、［アップロード］をクリックして入力キーファイルを Citrix ADM にアップロードすることもできます。

    変数値を含むキー入力ファイルは、設定ジョブで (同じファイル名で) 保持されます。設定ジョブの作成または編集中に、以前に使用およびアップロードした入力ファイルを表示および編集できます。

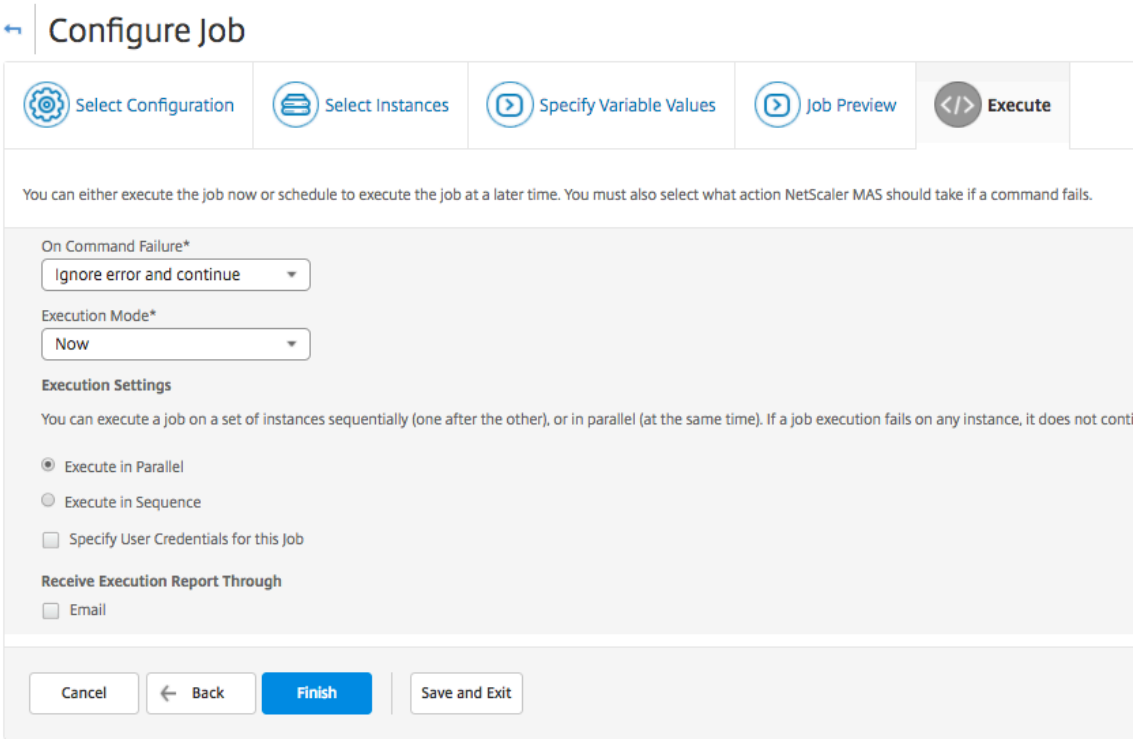
    構成ジョブの作成中に実行構成ジョブを表示するには、[ネットワーク] > [構成ジョブ] に移動し、[ジョブの作成] をクリックします。**[** ジョブの作成] ページ。[変数値の指定] タブで、[すべてのインスタンスに共通変数値] オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします（同じファイル名を維持します)。

    構成ジョブの編集中にすでに実行されている構成ジョブを表示するには、[ネットワーク] > [構成ジョブ] に移動し、[ジョブ名] を選択して [編集] をクリックします。[ジョブの設定] ページの [変数値の指定] タブで、[すべてのインスタンスに共通変数値] オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします（同じファイル名を維持します)。

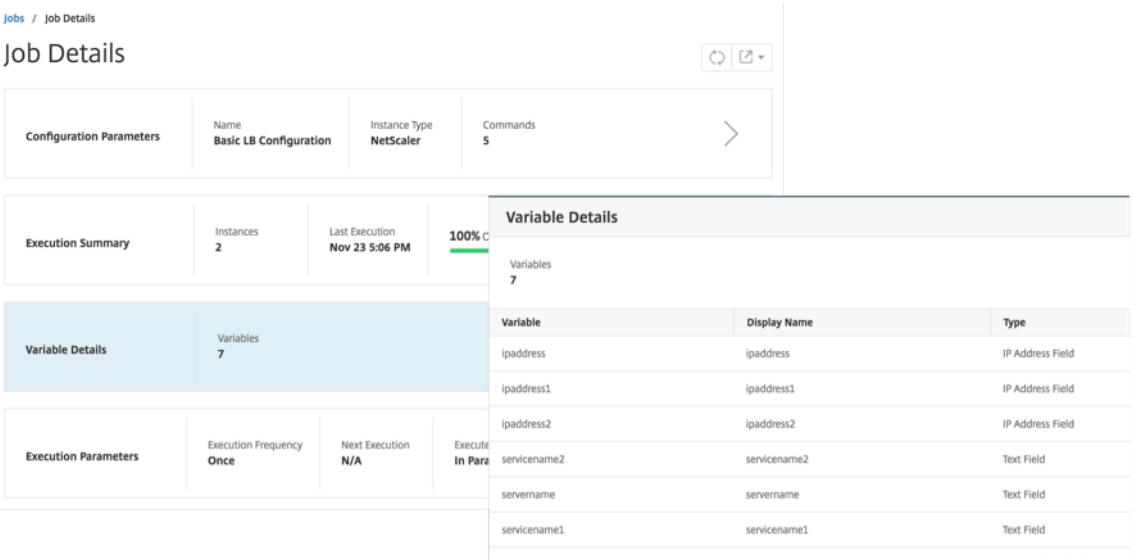
16. [**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および

検証できます。

17. [**Execute**] タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。また、コマンドが失敗した場合に Citrix ADM が実行する必要があるアクションや、ジョブの成功または失敗に関する電子メール通知を他の詳細とともに送信するかどうかを選択することもできます。



ジョブを構成して実行した後、[ネットワーク] > [構成ジョブ] に移動して、設定したジョブを選択すると、ジョブの詳細を確認できます。[詳細] をクリックし、[変数の詳細] をクリックして、ジョブに追加された変数のリストを表示します。



> 注
>
> 手順 **5** で変数に指定した値は、ジョブを保存して終了するとき、または後でジョブを実行するようにスケジュールするときに、Citrix ADM によって保持されます。

修正コマンドからの構成ジョブの作成

May 7, 2021

Citrix Application Delivery Management（ADM）の監査テンプレート機能を使用して、管理対象の Citrix ADC インスタンスの構成変更を監視し、構成エラーのトラブルシューティングを行うことができます。

監査テンプレートを使用して構成変更を監査する場合の一般的なワークフローは、次の手順で構成されます。

1. インスタンスの構成を監査するために、有効/期待される一連の Citrix ADC コマンドを含む監査テンプレートを作成します。
2. 監査テンプレートを実行する Citrix ADC インスタンスを選択して、実行構成と予想される構成の違いがないか確認します。
3. 差分/修正コマンドを理解し、「Create Job」機能を使用して、インスタンスの設定を目的の状態にします。

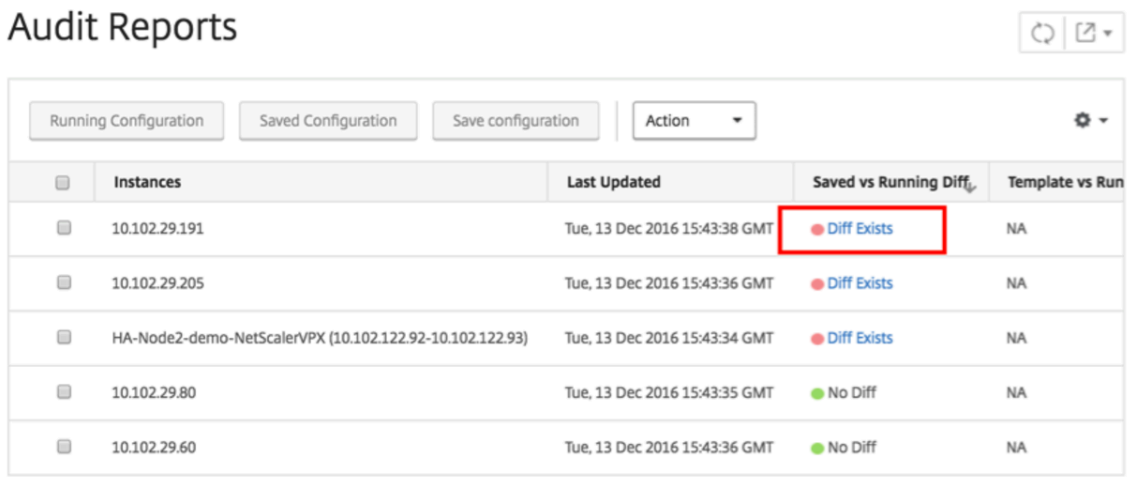
複数の管理者が 5 つの Citrix ADC インスタンスを管理しているシナリオを考えてみましょう。これらの管理者すべてが、既存のインスタンスの構成に、変更が必要になれば更新するとします。スーパー管理者は他の管理者からの変更にかかわらず、特定の重要な構成の設定は触れられずに保持されることを確保したいと考えます。このユースケースでは、スーパー管理者は、Citrix ADC インスタンス上に存在すると予想される構成のテンプレートを作成し、インスタンスに対して実行します。Citrix ADM は監査テンプレート構成と実行構成を比較し、［構成監査］ダッシュボードで不一致を報告します。

一部のインスタンスの構成に変更があった場合は、ADM 修正コマンド機能を使用して、特定の Citrix ADC インスタンスの変更および修正された構成コマンドで構成ジョブを作成できます。

監査テンプレート設定と構成実行の間に相違がある場合は、「監査レポート」(Audit Report) ページに「差分」(**Diff Exist** s) ステータスメッセージが表示されます。「相違の出口」リンクをクリックすると、「構成の差分」ページが表示され、修正コマンドを表示できます。また、これらの修正コマンドを使用して、構成ジョブを作成し、特定の Citrix ADC インスタンスで実行して、必要な構成に戻すこともできます。

Citrix ADM で修正コマンドで構成ジョブを作成するには：

1. [ネットワーク] > [構成監査] に移動します。
2. [構成監査] ページで、2 つのドーナツチャートのいずれかの中をクリックして、[監査レポート] ページにアクセスします。
3. 構成コマンドを修正するインスタンスの [差分] リンク（表の [**Saved vs Running Diff**] 列の下）をクリックします。[**Configuration Diff**] ページが表示され、そのインスタンスの [保存された設定]、[実行設定]、[修正設定] の相違点が一覧表示されます。



4. 「ジョブの作成」をクリックして、「ジョブの作成」ページに移動します。このページには、修正コマンドがあらかじめ入力されています。構成ジョブの作成方法については、「Citrix ADM で構成ジョブを作成する方法」を参照してください。

ある **Citrix ADC** インスタンスから別のインスタンスに実行および保存された構成を複製する

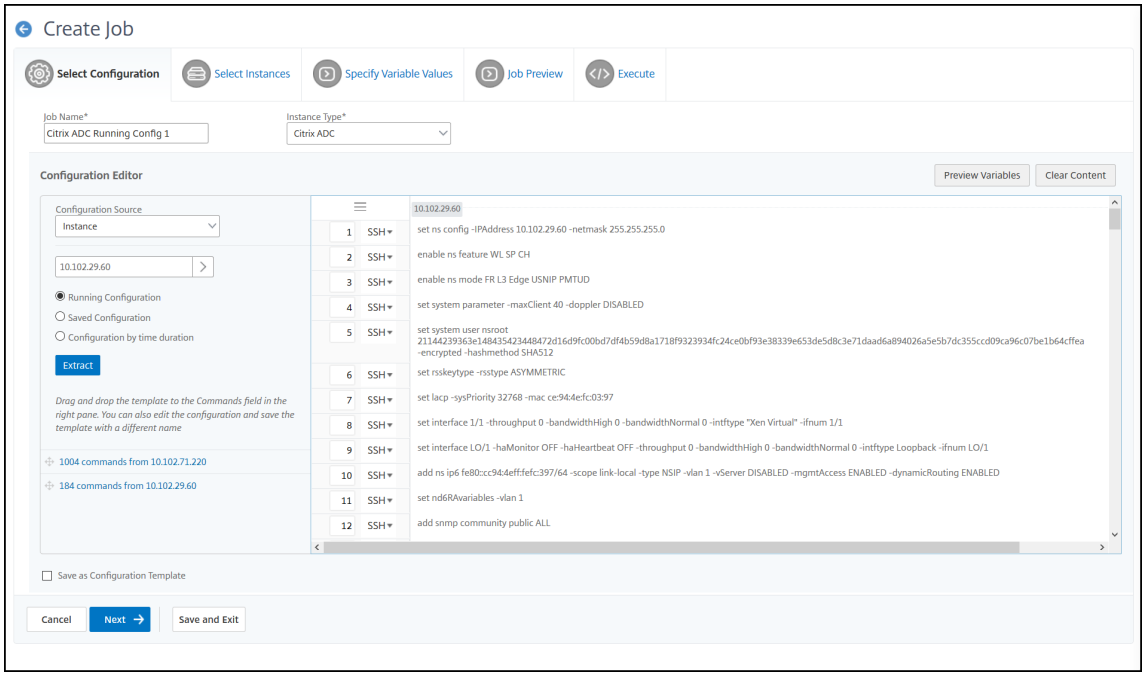
May 7, 2021

Citrix ADC インスタンスの構成を他のインスタンスにレプリケートできるようになりました。Citrix Application Delivery Management（ADM）でジョブを構成する場合は、構成ソースとしてインスタンスを選択し、選択したインスタンスの実行中または保存された構成を選択します。

たとえば、Citrix ADM 実行構成］を選択して［抽出］をクリックすると、選択した Citrix ADC インスタンスに実行構成を検索する要求が送信され、テンプレートとして表示されます。テンプレートは、右側のペインの [**Commands**] フィールドにドラッグできます。コマンド、パラメーター、およびインスタンスを変更できます。

あるインスタンスの実行および保存された構成コマンドを **Citrix ADM** 上の別のインスタンスにレプリケートするには:

1. [ネットワーク] > [構成ジョブ] に移動し、[ジョブの作成] をクリックします。
2. ジョブ名とインスタンスのタイプを指定します。たとえば、ジョブの名前として「構成 *1* を実行する *Citrix ADC* 」、インスタンスタイプを「*Citrix ADC*」と指定します。
3. [構成ソース] として [インスタンス] を選択し、他のインスタンスに構成をレプリケートするソース・インスタンスを選択します。
4. 次の 3 つのオプションが表示されます。
   - [Running Configuration]
   - [Saved Configuration]
   - [Configuration by time duration]
5. 「実行構成」を選択し、「抽出」をクリックします。そのインスタンスで実行されている実行構成の数が表示されます。



6. 右ペインの [Commands] フィールドでコマンドをドラッグします。
7. [Commands] フィールドでコマンドを編集できます。たとえば、抽出されたコマンドが Citrix ADC インスタンスをセットアップする場合などです。これには、パーティションの追加、負荷分散の設定、負荷分散サーバーのサービスへのバインドなどが含まれます。コマンドを編集して、パーティションなしで新しい Citrix ADC インスタンスをセットアップすることもできます。したがって、パーティションを削除するには、パーティションの作成に関連するコマンドを手動で削除し、[次へ] をクリックします。
8. [**Add Instanc** es] をクリックし、実行中の構成コマンドを適用するインスタンスを追加します。[**OK**] をクリックし、[次へ] をクリックします。

9. コマンドで変数を指定した場合は、[変数値の指定] タブで [入力キーファイルのダウンロード] をクリックします。ダウンロードしたファイルで、変数の値を指定し、そのファイルを Citrix ADM にアップロードします。
10. [**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。
11. [**Execute**] タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。また、コマンドが失敗した場合に Citrix ADM が実行する必要があるアクションや、ジョブの成功または失敗に関する電子メール通知を他の詳細とともに送信するかどうかを選択することもできます。

実行構成ジョブを再利用する

May 7, 2021

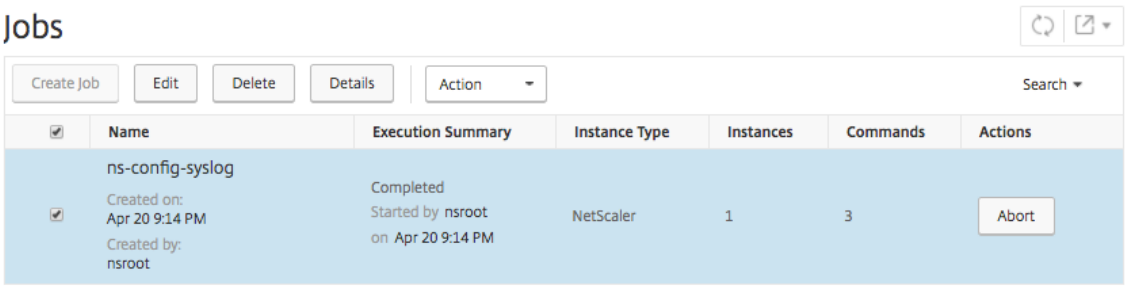
設定ジョブを使用すると、1 つ以上の管理対象インスタンスで実行できる設定コマンドのセットを作成できます。また、保存した構成ジョブのコマンド、パラメーター、構成ソース、インスタンスを変更してから、そのジョブの同様のセットを実行することもできます。この機能は、同じ一連のコマンドを別のインスタンスで実行する必要がある場合や、ジョブでエラーが発生してそれ以降の実行を停止する場合に便利です。

Citrix Application Delivery Management（ADM）には、完了したジョブを再度実行する機能があります。この機能を使用すると、完全に実行されたジョブは、ジョブ名を変更せずに再度実行できます。

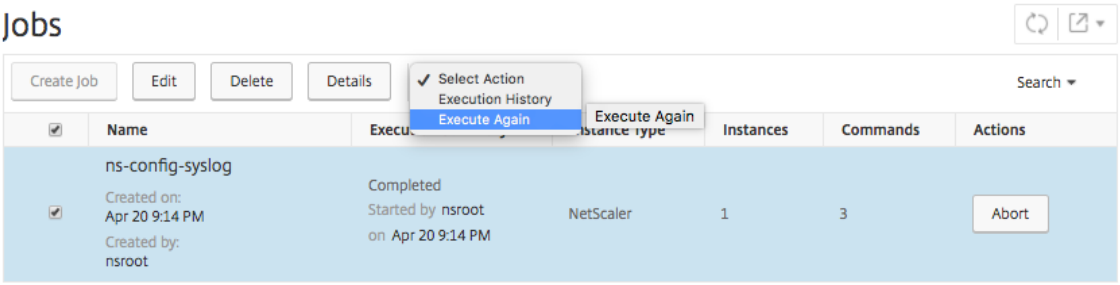
> 注:
>
> 実行モードが「今」のときに実行されるジョブのみを再実行できます。

完了したジョブを編集するには、次の手順に従います。

1. ADM ホームページから、[ネットワーク] > [構成ジョブ] に移動します。
2. 「ジョブ」ページで、「実行サマリー」が「完了」と表示されるジョブを選択し、「編集」をクリックします。スケジュール指定された構成ジョブも編集できます。
3. [**Configure Job**] ページで、[Job Name] と [Instance Type] が編集できないことを確認できます。構成ソースをはじめとするその他のフィールドの変更、インスタンスの追加、変数値の編集、実行設定の指定を行うことができます。
4. [完了] をクリックして、構成ジョブを再度実行します。



> 注
>
> ジョブを選択し、もう一度 [**Execute**] をクリックすると、ソース、インスタンス、コマンドを変更せずにジョブを実行することもできます。このオプションは、同じインスタンスで同じコマンドセットを実行する必要がある場合に便利です。場合によっては、ジョブがサーバー側から一時的なエラーが発生し、ジョブを再度実行する必要がある場合があります。



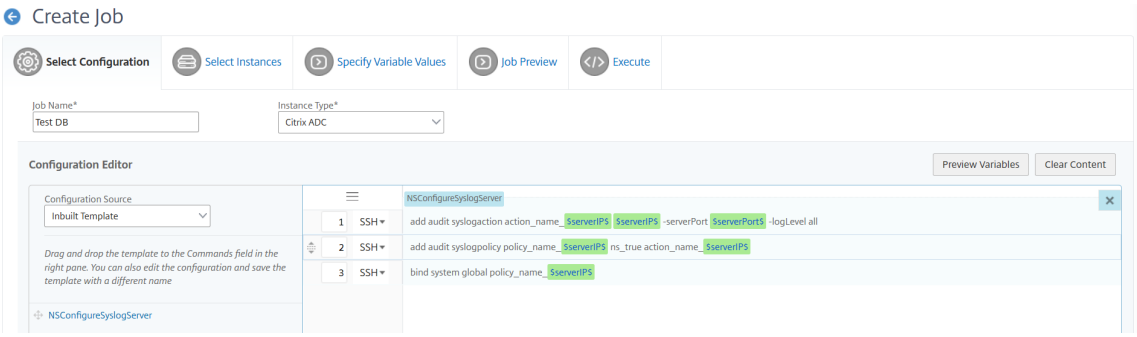
組み込みテンプレートを使用して作成されたジョブをスケジュールする

May 7, 2021

組み込みテンプレートオプションを使用して、ジョブにスケジュールを指定できます。ジョブとは、管理対象インスタンスで実行できる一連の構成コマンドのことです。たとえば、組み込みテンプレートオプションを使用して、Syslog サーバーを構成するジョブにスケジュールを指定できます。また、ジョブをすぐに実行するか、後段階で実行するようにジョブをスケジュールすることもできます。

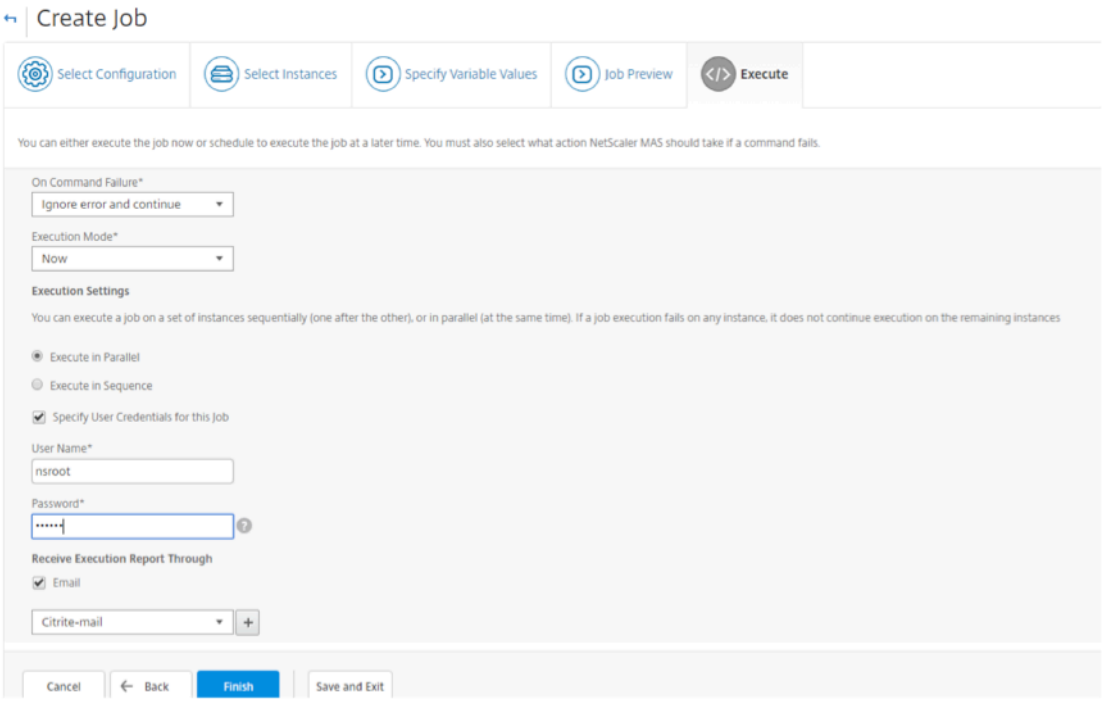
Citrix ADM 組み込みテンプレートを使用してジョブをスケジュールするには:

1. Citrix Application Delivery Management（ADM）で、[ネットワーク] > [構成ジョブ] の順に選択し、[ジョブの作成] をクリックします。
2. [**Create Job**] ページの [**Select Configuration**] タブで、[**Job Name**] を指定し、ドロップダウンリストから [**Instance Type**] を選択します。
3. 「構成ソース」ドロップダウンリストから「作り込みテンプレート」を選択します。*nsConfigureSysLogServer* コマンドを右側のウィンドウ枠にドラッグし、[次へ] をクリックします。



4. [インスタンスの選択] タブで、[インスタンスの追加] をクリックし、ジョブを実行するインスタンスを選択し、[**OK**] をクリックします。
5. ［次へ］をクリックします。［**Specify Variable Values**］タブで次のいずれかのオプションを選択してインスタンスの変数を指定します。
    - 入力ファイルから変数値：入力ファイルをダウンロードして、コマンドで定義した変数の値を入力し、ファイルを Citrix ADM サーバーにアップロードします。
    - **Common variable values for all instances** - Syslog サーバーの IP アドレスとポートを指定します。
6. [**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。
7. ［次へ］をクリックします。
8. [実行] タブで、次の条件を設定します。
    - コマンド失敗の場合 -コマンドが失敗した場合、エラーを無視してジョブの実行を続行するか、ジョブのさらなる実行を停止するかを選択できます。ドロップダウンリストから、実行するアクションを選択します。
    - 実行モード -ジョブを今すぐ実行することも、後でジョブを実行するようにスケジュールすることもできます。後でジョブをスケジュールする場合は、そのジョブの実行頻度設定を指定する必要があります。ジョブに定めるスケジュールをボックスの一覧から選択します。
9. 「実行設定」(**Execution Settings**) で必要なメソッドを選択して、一連のインスタンスに対してジョブを順次または並列で実行することもできます。いずれかのインスタンスでジョブの実行にエラーが発生した場合、残っているインスタンスに続行することはありません。

    また、承認されたユーザーが管理対象インスタンスでジョブを実行できるようにすることもできます。また、ジョブの成功または失敗に関する電子メール通知を他の詳細とともに送信するかどうかを選択できます。
10. ［完了］をクリックします。



メンテナンス・ジョブを使用した **Citrix ADC SDX** インスタンスのアップグレード

May 7, 2021

Citrix ADC リリース 11.0 以降を実行している Citrix ADC SDX インスタンスのシングルバンドル・アップグレードを実行できます。シングルバンドルアップグレードを実行するには、Citrix Application Delivery Management（ADM）の組み込みタスクを使用します。この組み込みタスクを使用すると、Citrix ADC SDX 管理サービス、XenServer ハイパーバイザー、および Citrix Hypervisor 用のサプリメンタルパックと修正プログラムをアップグレードできます。

Citrix ADM を使用して **Citrix ADC SDX** インスタンスをアップグレードするには:

1. Citrix ADM で、［ネットワーク］>［構成ジョブ］>［メンテナンスジョブ］に移動します。
2. [ジョブの作成] をクリックします。［ジョブの作成］ページで、［**Citrix ADC SDX** 組み込みのアップグレード］タスクを選択して、Citrix ADC SDX インスタンスをアップグレードします。[続行] をクリックします。
3. ［**Citrix ADC** アプライアンスのアップグレード］ページの［インスタンスの選択］タブで、ジョブ名を指定し、［インスタンスの追加］をクリックします。
4. アップグレードするターゲットインスタンスまたはインスタンスグループを選択します。
5. Citrix ADC インスタンスまたはインスタンスグループを追加したら、［次へ］をクリックして、選択したインスタンスでアップグレード前の検証を開始します。画面には、各 Citrix ADC インスタンスの事前検証の進行状況が報告されます。
6. ［アップグレード **Citrix ADC** アプライアンスの変更］ページで、［アップグレード］タブを選択します。［ソフトウェアイメージ］ドロップダウンメニューから、［ローカル］（ローカルマシン）または［アプライアン

ス］（ビルドファイルは Citrix ADM 上に存在する必要があります）を選択します。

7. また、検証前のアップグレードエラーが発生しているインスタンスがあるかどうかを確認することもできます。これらのエラーは、メッセージの形式で表示されます。メッセージでは、ディスクスペース、ハードディスクドライブ、およびユーザーのカスタマイズに関するエラーが示されます。事前検証アップグレードチェックに失敗したインスタンスの使用を続行しない場合は、そのインスタンスを削除できます。インスタンスを削除するには、インスタンスを選択し、[**Delete**] をクリックします。
8. [タスクのスケジュール] タブでは、アップグレードプロセスを今すぐ実行したり、後でスケジュールしたりできる実行の詳細を設定することもできます。また、Citrix ADC SDX インスタンスのバックアップ、電子メールによる実行レポートの受信、高可用性ノードの 2 段階アップグレードの実行を選択することもできます。

HA のノードの 2 段階アップグレードでは、アップグレードをすぐに実行するか、ノードを次々に更新する時間をスケジュールするかを選択できます。ノードの同期と伝播は、両方のノードが正常にアップグレードされるまで無効になります。

Citrix SD-WAN WANOP インスタンスの構成ジョブの作成

May 7, 2021

ジョブとは、管理対象インスタンスに対して作成およびスケジュール設定できる構成コマンドのセットです。Citrix SD-WAN WANOP インスタンスの場合、次のオプションを使用してジョブを作成できます。

- 構成テンプレート：構成エディタを使用して CLI コマンドを入力し、構成をテンプレートとして保存し、ジョブを設定するために使用できます。

- 作り込みテンプレート：構成テンプレートのリストから選択できます。これらのテンプレートには CLI コマンドの構文が用意されており、変数の値を指定できます。作り付けのテンプレートとその説明を次の表に示します。
- ファイル: ローカルマシンから設定ファイルをアップロードし、ジョブを作成できます。

ジョブを作成したら、ジョブをすぐに実行するか、後で実行するようにジョブをスケジュールするかを選択できます。また実行頻度も設定できます。

作り込みテンプレート	説明
EnableCloudBridgeWANOpt	Citrix SD-WAN WANOP アプライアンスを通過するトラフィックを有効にします。
DisableCloudBridgeWANOpt	Citrix SD-WAN WANOP アプライアンスを経由するトラフィックを無効にします。
RestartCloudBridgeWANOpt	Citrix SD-WAN WANOP アプライアンスを再起動します。
RestoreConfig	Citrix SD-WAN WANOP アプライアンスの構成を復元します。
AddLink	リンクを作成または定義すると、SD-WAN WANOP アプライアンスはリンクの輻輳や損失を防ぎ、トラフィックシェーピングを実行できます。リンク上で送信または受信された最大帯域幅を定義でき、LAN 側または WAN 側のトラフィックを指定することもできます。
ConfigureBandwidth	帯域幅の制限と他の帯域幅管理の設定を設定します。
AddUser	特権を割り当てる新しいユーザーを追加します。
AddUserAdvancedPlatform	AddUser テンプレートでは使用できない、特権割り当てを有効にする新しいユーザーを追加します。
AddService-class	1 つ以上のサービスクラスフィルタを使用して SD-WAN WANOP アプライアンスのサービスクラスを作成し、有効にします。
SetApplication	アプリケーション分類子の定義を設定します。
AddorRemoveVideoCachingPorts	ビデオソースがデータを送受信するポート番号を追加または削除します。デフォルトポートは 80 です。
RemoveVideoCachingSource	1 つまたは複数のビデオキャッシュソースを削除します。ビデオソースの IP アドレスまたはドメイン名を指定します。
RemoveAllVideoCaching	すべての利用可能なビデオキャッシュソースを削除します。

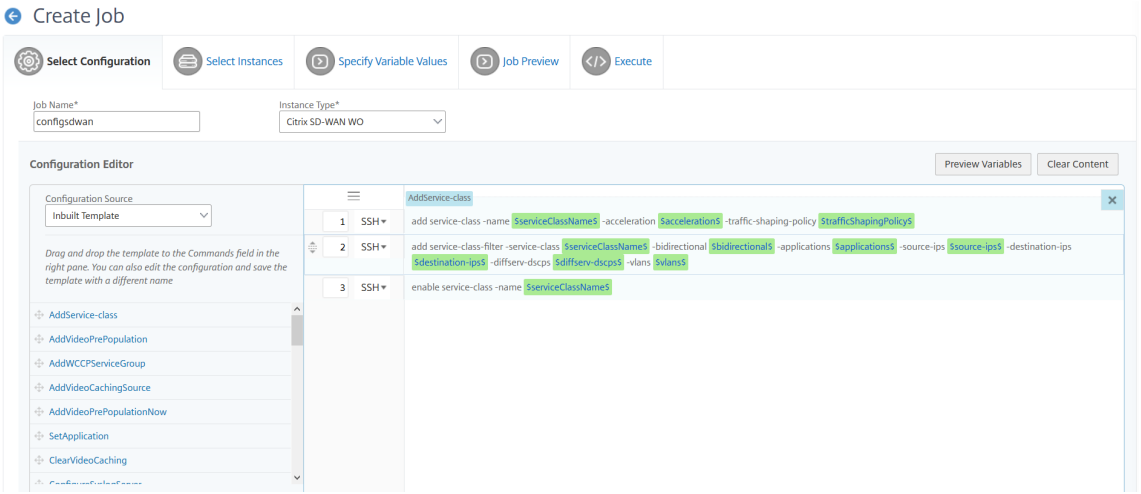
作り込みテンプレート	説明
VideoCachingState	Citrix SD-WAN WANOP アプライアンスのビデオキャッシュ機能を有効または無効にします。
ClearVideoCaching	ビデオキャッシュまたはビデオキャッシュ統計情報のいずれかをクリアします。
SetVideoCaching	キャッシュされるオブジェクトの最大サイズを設定します。この制限より大きなオブジェクトはキャッシュされません。デフォルトでは、キャッシュされるオブジェクトサイズは最大 100MB です。
AddVideoCachingSource	ビデオソースの IP アドレスまたはドメイン名を追加します。そのソースのビデオキャッシュを有効または無効にするオプションが含まれています。
ConfigureRemoteLicenseServer	集中ライセンスサーバーを構成します。ライセンスサーバーのモデル、IP アドレス、およびポート番号を指定します。
ConfigureLocalLicenseServer	ライセンスサーバーの場所をローカルに設定します。
InstallCACert	Citrix SD-WAN WANOP アプライアンスに CA 証明書をインストールします。証明書名、ファイル名、およびキーストアのパスワードを指定します。
InstallCombinedCerKey	統合された SSL 証明書とキーのペアファイルをインストールします。
InstallSeperateCertKey	SSL 証明書とキーを別のファイルとしてインストールします。
EnableWCCP	WCCP 展開モードを有効にします。
AddWCCPServiceGroup	Citrix SD-WAN WANOP アプライアンスの新しい WCCP サービスグループ定義を追加します。
DisableWCCP	WCCP 展開モードを無効にします。
AddTrafficShapingPolicy	Citrix SD-WAN アプライアンスのトラフィックシェーピングポリシーを作成します。このポリシーはネットワーク帯域幅を制御します。
SetTrafficShapingPolicy	Citrix SD-WAN WANOP アプライアンスのトラフィックシェーピングポリシーを変更します。このポリシーはネットワーク帯域幅を制御します。

作り込みテンプレート	説明
AddVideoPrePopulation	事前のビデオのダウンロードとキャッシュを有効にする、ビデオの事前設定エントリを作成します。いつビデオをキャッシュするかも指定できます。
UpdateVideoPrePopulation	いつビデオをキャッシュするかを指定する、ビデオの事前設定エントリを変更します。
AddVideoPrePopulationNow	ビデオを即座にダウンロードしてキャッシュを有効にする、ビデオ事前設定を構成します。1 つ以上の URL から動画をダウンロードしてキャッシュする方法を制御できます。
VideoPrePopulationState	ビデオの事前設定を変更、開始、更新、および削除します。
ConfigureSyslogServer	syslog サーバーの IP アドレスとポート番号を設定します。
ConfigureAlert	アラートレベルを構成します。

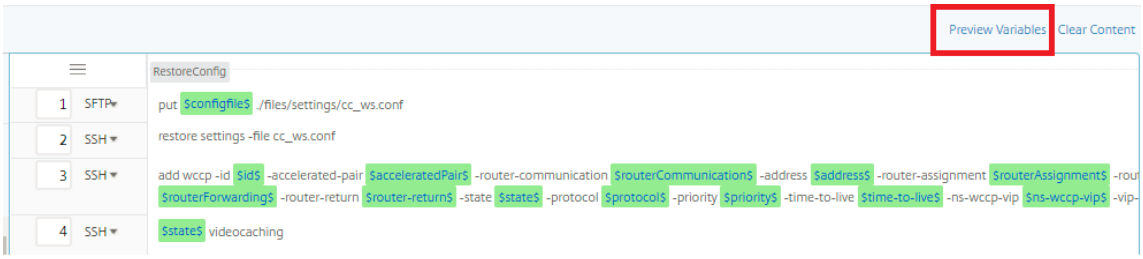
Citrix SD-WAN WANOP インスタンスの構成ジョブを作成するには:

1. Citrix ADM で、［ネットワーク］>［構成ジョブ］の順に選択し、［ジョブの作成］をクリックします。
2. [ジョブの作成] ページの [構成の選択] タブで、[ジョブ名] を指定します。
3. ［インスタンスタイプ］フィールドで ［**Citrix SD-WAN WO**］を選択します。
4. [構成ソース] ドロップダウンリストで、ジョブを作成するオプションを選択します。

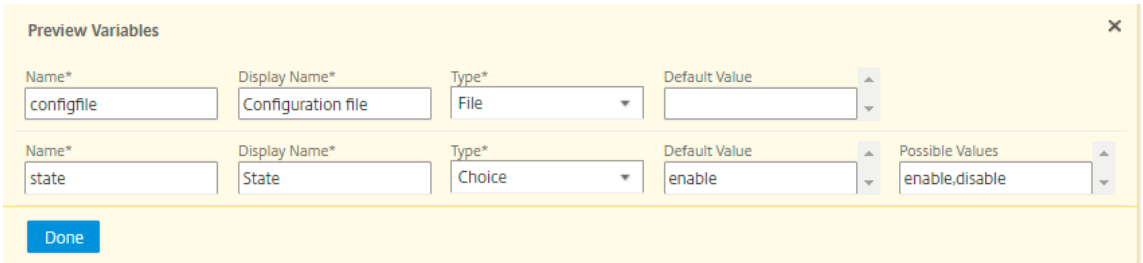
> 注
>
> [構成テンプレートとして保存] を選択し、名前を指定して構成をテンプレートとして保存し、再利用します。



5. 構成ジョブの作成または編集中に定義したすべての変数を、1 つの統合ビューで確認できます。
6. 次のいずれかの操作を行って、すべての変数を 1 つの統合ビューに表示します。
   - 構成ジョブの作成中に、[ネットワーク] > [構成ジョブ] に移動し、[ジョブの作成] を選択します。[**Create Job**] ページでは、構成ジョブの作成時に追加したすべての変数を確認できます。
   - 構成ジョブの編集中に、[ネットワーク] > [構成ジョブ] に移動し、[ジョブ名] を選択して [編集] をクリックします。[ジョブの構成] ページでは、構成ジョブの作成時に追加されたすべての変数を確認できます。
7. 次に、「変数のプレビュー」(Preview Variables) タブをクリックして、設定ジョブの作成または編集中に定義した 1 つの統合ビューで変数をプレビューできます。



8. 新しいポップアップウィンドウが表示され、名前、表示名、タイプ、デフォルト値などの変数のすべてのパラメータが表形式で表示されます。これらのパラメータを編集および修正することもできます。パラメータを編集または変更したら、[完了] ボタンをクリックします。

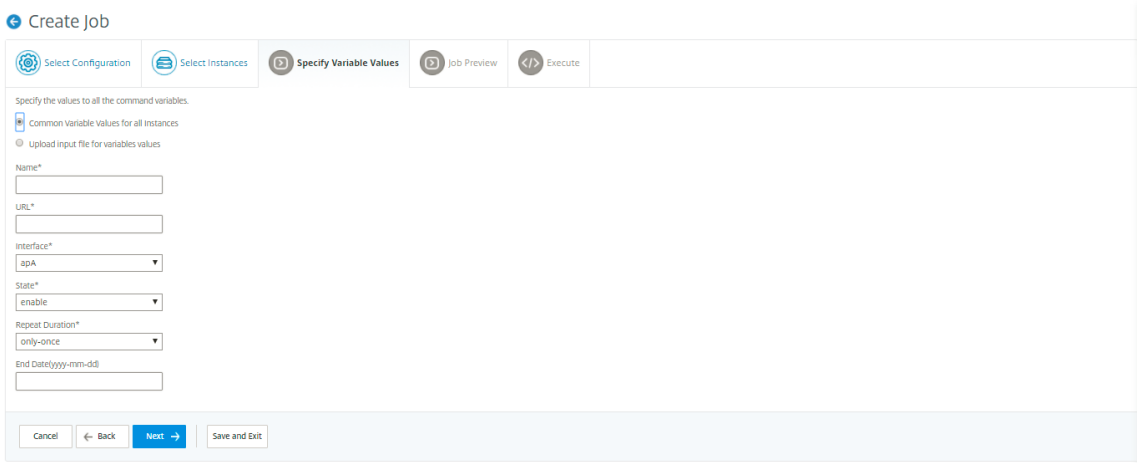


9. [次へ] をクリックし、[インスタンスの選択] タブで **[**インスタンスの追加**]** をクリックします。ジョブを実行

するインスタンスを選択し、「**OK**」をクリックします。

10. [次へ] をクリックし、[変数値の指定] タブで、次のいずれかのオプションを選択して、インスタンスの変数を指定します。

    - 変数値の入力ファイルをアップロード**:** [入力キーファイルのダウンロード] をクリックして、入力ファイルをダウンロードします。入力ファイルで、コマンドで定義した変数の値を入力し、Citrix ADM サーバーにファイルをアップロードします。
    - すべてのインスタンスの共通変数値: 変数の値を入力します。選択したテンプレートによって、変数は変わります。



    変数値を含む入力ファイルは、設定ジョブで (同じファイル名で) 保持されます。設定ジョブの作成または編集中に、以前に使用およびアップロードした入力ファイルを表示および編集できます。

    構成ジョブの作成中に実行構成ジョブを表示するには、[ネットワーク] > [構成ジョブ] に移動し、[ジョブの作成] をクリックします。**[** ジョブの作成] ページ。[変数値の指定] タブで、[すべてのインスタンスに共通変数値] オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします（同じファイル名を維持します)。

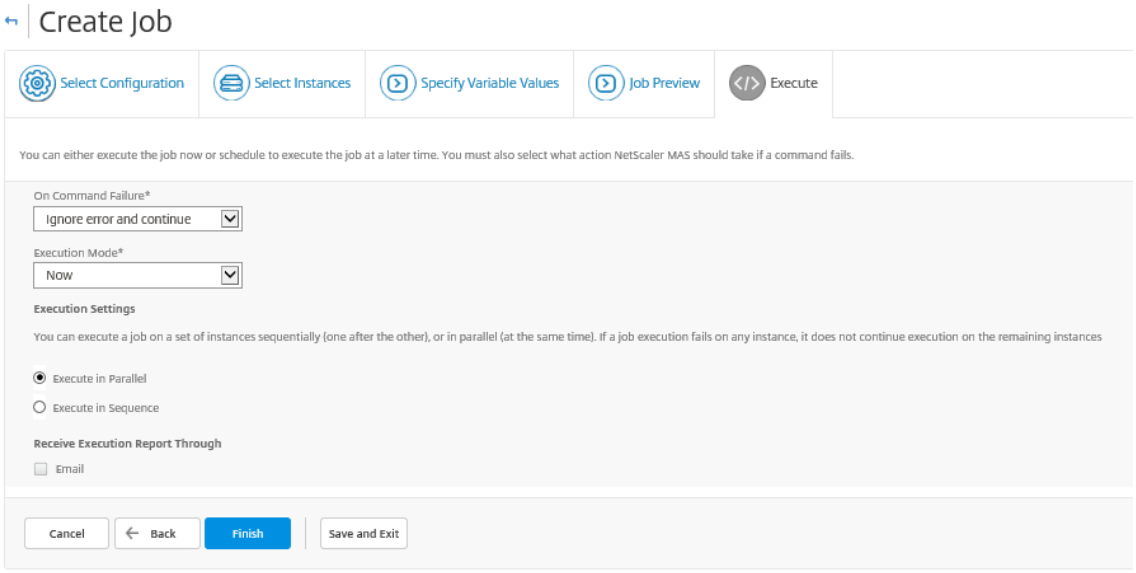
    構成ジョブの編集中にすでに実行されている構成ジョブを表示するには、[ネットワーク] > [構成ジョブ] に移動し、[ジョブ名] を選択して [編集] をクリックします。[ジョブの設定] ページの [変数値の指定] タブで、[すべてのインスタンスに共通変数値] オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします（同じファイル名を使用)。

11. [次へ] をクリックし、[ジョブプレビュー] タブで、ジョブとして実行するコマンドを評価および確認できます。

12. [次へ] をクリックし、[実行] タブで、次の条件を設定します。

    - コマンド失敗の場合: コマンドが失敗した場合の対処方法: エラーを無視してジョブを続行するか、ジョブの実行を停止します。ボックスの一覧からアクションを選択します。

- 実行モード: ジョブをすぐに実行するか、後で実行をスケジュールします。後で実行するようにスケジュールを指定する場合、ジョブの実行頻度の設定を指定する必要があります。「実行頻度」ドロップダウン・リストから、ジョブが従うスケジュールを選択します。



13. 「実行設定」で、ジョブを順番に実行するか（次々に）実行するか、並行して（同時に）実行するかを選択します。
14. ジョブ実行レポートを受信者のリストに電子メールで送信するには、**[**実行レポートの受信方法] セクションの [電子メール送信] チェックボックスをオンにします。表示されるボックスの一覧から電子メール配布リストを選択します。電子メール配布リストを作成するには、[**+**] アイコンをクリックし、受信者の電子メールアドレスと電子メールサーバーの詳細を入力します。
15. ［完了］をクリックします。

マスター構成テンプレートの使用

May 7, 2021

マスター構成テンプレートを使用すると、複数の Citrix ADC インスタンスにマスター構成を作成して展開できます。

管理者は、構成を変更し、ライセンス、証明書、およびその他のファイルを Citrix ADC インスタンスに保存することができます。新しい構成をマスター構成テンプレート（.conf ファイル）として保存できます。

Citrix ADC インスタンスからマスター構成テンプレートを保存するには、次のいずれかの操作を行います。

- コマンドプロンプトに対して、s **ave ns config** と入力します。設定は、インスタンスのフラッシュメモリに /nsconfig/ns.conf ファイルに保存されます。
- Citrix ADC インスタンスの GUI から、［診断］>［構成の表示］に移動します。保存したい構成の種類を選択します。たとえば、Citrix ADC インスタンスの保存された構成を保存する場合は、［保存された構成］を選択

します。「テキストをファイルに保存」リンクをクリックして、「ns.conf」ファイルをローカルマシンに保存します。

ジョブの作成時に「DeployMasterConfiguration」構成テンプレートを使用してマスター構成テンプレートを展開する場合、コマンドを追加したり、既存のコマンドを変更したり、入力ファイルに異なる変数値を指定したりすることで、特定の Citrix ADC インスタンスごとにカスタマイズできます。。

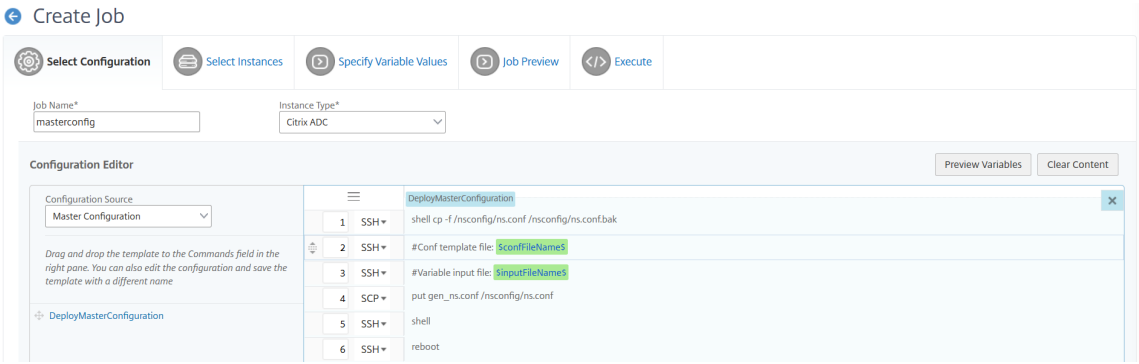
たとえば、管理者は、ns.conf ファイルに加えて Citrix ADC インスタンスに証明書キーをアップロードし、マスター構成も展開できます。

> 重要
>
> Citrix ADC CPX インスタンス、クラスタ内に構成された Citrix ADC インスタンス、またはパーティション化された Citrix ADC インスタンスでは、DeployMasterConfiguration テンプレートを使用して構成ジョブを実行することはできません。

Citrix ADM でマスター構成構成構成テンプレートを使用して構成ジョブを作成するには:

1. Citrix Application Delivery Management（ADM）で、[ネットワーク] > [構成ジョブ] の順に選択し、[ジョブの作成] をクリックします。
2. [**Create Job**] ページの [**Select Configuration**] タブで、[**Job Name**] を指定し、ドロップダウンリストから [**Instance Type**] を選択します。
3. 「構成ソース」ドロップダウンリストから「マスター構成」を選択します。DeployMasterConfiguration テンプレートのコマンドを右側のペインにドラッグします。右側のペインでは、コマンドを追加、変更、削除することもできます。[次へ] をクリックします。

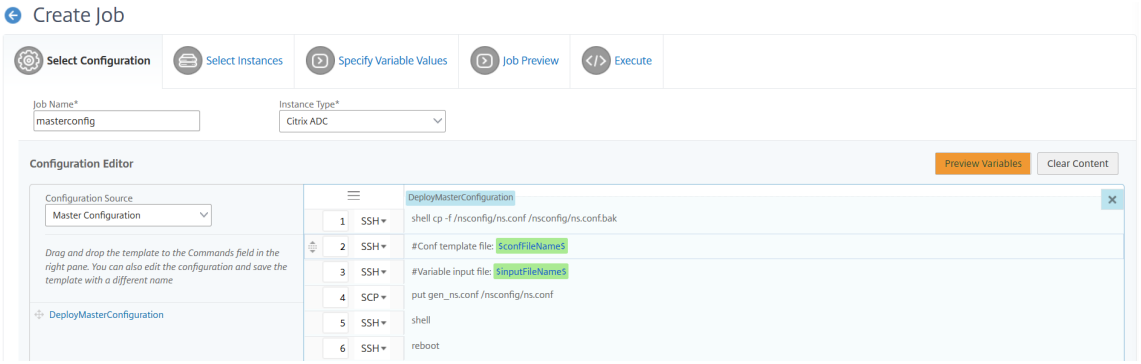
   > 注
   >
   > p **ut** コマンドを追加して、入力ファイルをテンプレートに追加できます。この例では、設定テンプレートファイルと変数入力ファイルに加えて、証明書とキーファイルをアップロードする必要があります。

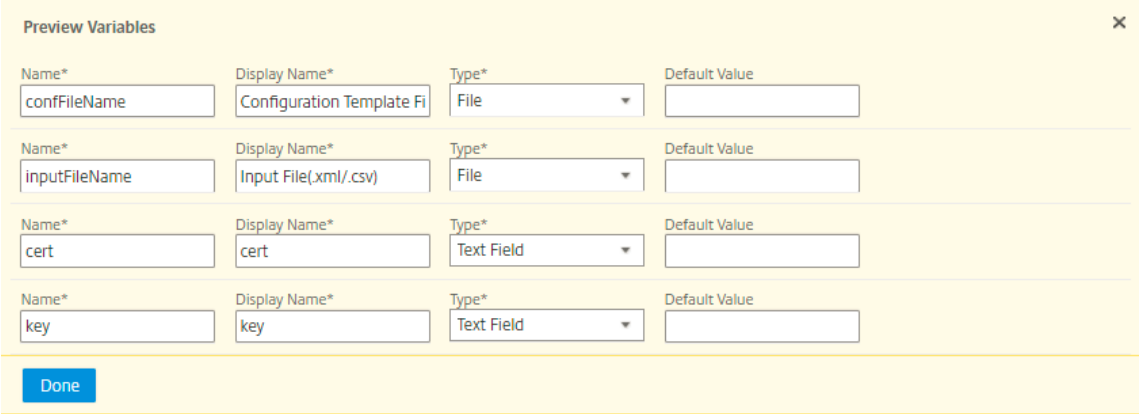
4. 構成ジョブの作成または編集中に定義したすべての変数を、1 つの統合ビューで確認できます。
5. 次のいずれかの操作を行って、すべての変数を 1 つの統合ビューに表示します。
   - 構成ジョブの作成中に、[ネットワーク**] > [**構成ジョブ] に移動し、[ジョブの作成] を選択します。[**Create Job**] ページでは、構成ジョブの作成時に追加したすべての変数を確認できます。

- 構成ジョブの編集中に、[ネットワーク**] > [**構成ジョブ] に移動し、[ジョブ名] を選択して [編集] をクリックします。[ジョブの構成] ページでは、構成ジョブの作成時に追加されたすべての変数を確認できます。

6. 次に、「変数のプレビュー」(Preview Variables) タブをクリックして、設定ジョブの作成または編集中に定義した 1 つの統合ビューで変数をプレビューできます。



7. 新しいポップアップウィンドウが表示され、名前、表示名、タイプ、デフォルト値などの変数のすべてのパラメータが表形式で表示されます。これらのパラメータを編集および修正することもできます。パラメータを編集または変更したら、[完了] ボタンをクリックします。



8. 構成ジョブを実行するインスタンスを選択し、[**Next**] をクリックします。
9. [変数値の指定] タブで、次のファイルをアップロードします。

   - 構成テンプレートファイル（**.conf**）-Citrix ADC インスタンスから抽出した.conf ファイルをアップロードします。
   - 入力ファイルのアップロード **(.xml/csv)** -コマンドで定義した変数の値を含む入力ファイルをアップロードします。

   ここでは、サンプルの xml ファイルが用意されています。xml ファイルに、使用している ADC インスタンスに対応する詳細が含まれていることを確認します。

```
1 <?xml version="1.0" encoding="UTF-8" ?>
2
```



```
<properties>

<!--

Provide inputs for all the parameters defined in the master config
    file.

-  global. This tag contains all the common parameters and value.

-  devicegroup. This tag contains all the instance group specific
   parameters and values.

If the same parameters are defined in global and instance tags,
   the instance specific parameters value will take precedence
   over the instance group. The instance group specific parameters
    value will take precedence over global parameters in the
   execution.

-  name. This attribute represents the name of the instance group.

-  device. This tag contains all the instance specific parameters
   and value.

If the same parameters are defined in global and instance tags,
   the instance specific parameters value will take precedence in
   the execution.

-  name. This attribute represents the IP Address of the instance.
    Host name is not supported for the attibute.

HA pair should be represented as <primaryip>-<secondaryip>.
   Example 10.102.2.1-10.102.2.2

In the template file, the parameter name must be specified within
   the dollar sign,Example: $NSIP$, $CC_Trap_Dest$ and parameters
   names are case sensitive.
-->

<global>

</global>
<devicegroup name="BLR_DEVS">
</devicegroup>
<device name="10.106.101.209">
<param name="IP" value="10.106.101.209"/>
```



```
</device>

<!-- HA PAIR-->
<!--<device name="10.102.43.154-10.102.43.155">
<param name="NSIP" value="10.102.43.154"/>
<param name="HostName" value="NS43HA"/>
<param name="LBSERVER" value="haserver43http"/>
<param name="SNMPTrapDest" value="10.102.43.130"/>
</device>-->
</properties>

<!--NeedCopy-->
```

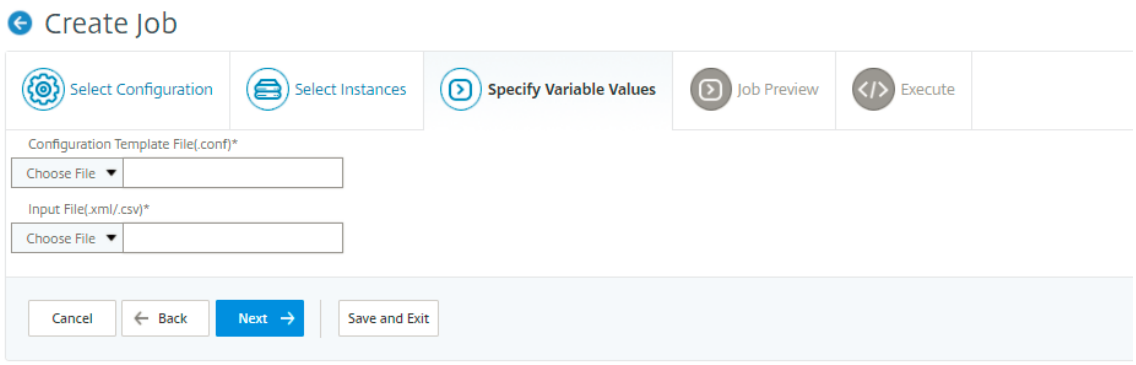
ここでは、サンプルの csv ファイルが用意されています。

```
#job-s_variable_input_key_file ,,,,
,,,,
#Global,NSIP,HostName,LBSERVER,SNMPTrapDest
Global Values,,,,
#InstanceGroup,NSIP,HostName,LBSERVER,SNMPTrapDest
example_doc,,,,
#Instance(s),NSIP,HostName,LBSERVER,SNMPTrapDest
10.xx.xx.xx,,,,
<!--NeedCopy-->
```

同じファイルが Microsoft Excel に表示されます。

#job-s_variable_input_key_file				
#Global	NSIP	HostName	*LBSERVER*	SNMPTrapDest
Global Values				
#InstanceGroup	NSIP	HostName	LBSERVER	SNMPTrapDest
example_doc				
#Instance(s)	NSIP	HostName	LBSERVER	SNMPTrapDest

10. ［次へ］をクリックします。

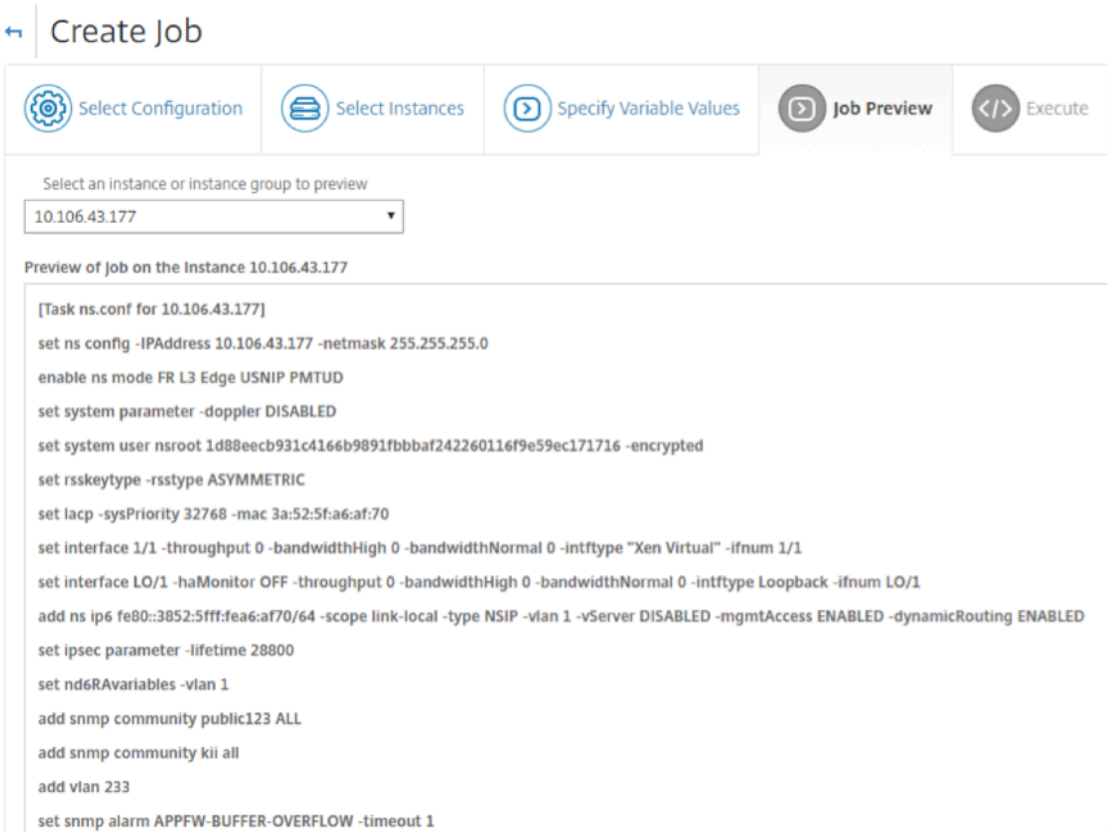


変数値を含む入力ファイルは、設定ジョブで (同じファイル名で) 保持されます。設定ジョブの作成または編集中に、以前に使用およびアップロードした入力ファイルを表示および編集できます。

構成ジョブの作成中に実行構成ジョブを表示するには、[ネットワーク] > [構成ジョブ] に移動し、[ジョブの作成] をクリックします。**[** ジョブの作成] ページ。[変数値の指定] タブで、[すべてのインスタンスに共通変数値] オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします（同じファイル名を維持します)。

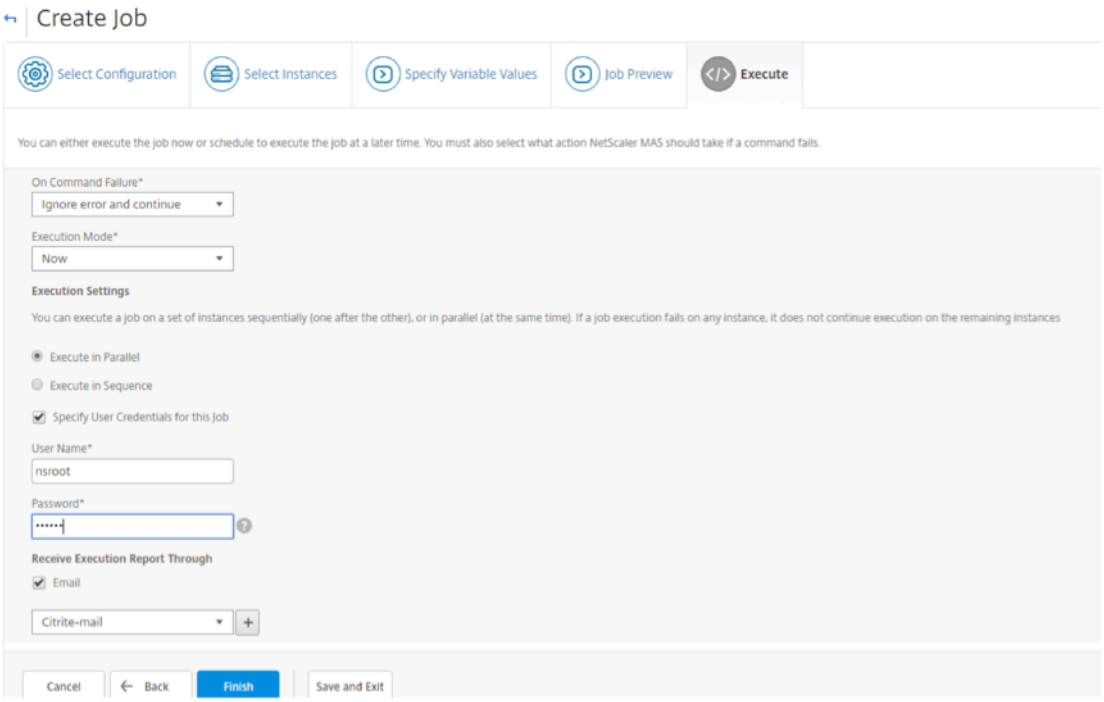
構成ジョブの編集中にすでに実行されている構成ジョブを表示するには、[ネットワーク] > [構成ジョブ] に移動し、[ジョブ名] を選択して [編集] をクリックします。[ジョブの設定] ページの [変数値の指定] タブで、[すべてのインスタンスに共通変数値] オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、ファイルを編集してアップロードします（同じファイル名を維持します)。

11. [**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価して確認し、[**Next**] をクリックします。

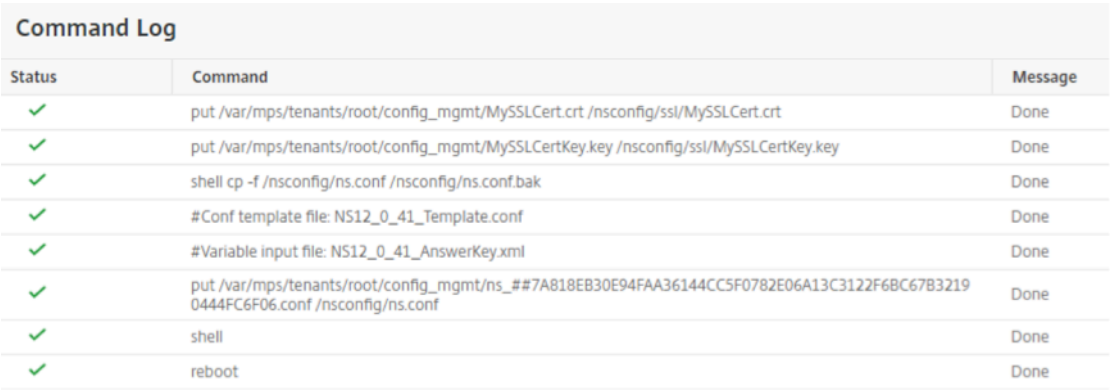


12. [**Execute**] タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。コマンドが失敗した場合に Citrix ADM が実行する必要があるアクションを選択することもできます。

    また、承認されたユーザーが管理対象インスタンスでジョブを実行できるようにすることもできます。また、ジョブの成功または失敗に関する電子メール通知を他の詳細とともに送信するかどうかを選択できます。



ジョブの実行後、[ネットワーク] > [構成ジョブ] に移動して、設定したばかりのジョブを選択すると、ジョブの詳細を確認できます。[詳細] をクリックし、[実行の概要] をクリックして、ジョブの詳細を確認します。インスタンスをクリックして **Command Logs** を表示して、ジョブで実行されたコマンドを確認します。



Command Log

Status	Command	Message
✓	put /var/mps/tenants/root/config_mgmt/MySSLCert.crt /nsconfig/ssl/MySSLCert.crt	Done
✓	put /var/mps/tenants/root/config_mgmt/MySSLCertKey.key /nsconfig/ssl/MySSLCertKey.key	Done
✓	shell cp -f /nsconfig/ns.conf /nsconfig/ns.conf.bak	Done
✓	#Conf template file: NS12_0_41_Template.conf	Done
✓	#Variable input file: NS12_0_41_AnswerKey.xml	Done
✓	put /var/mps/tenants/root/config_mgmt/ns_##7A818EB30E94FAA36144CC5F0782E06A13C3122F6BC67B32190444FC6F06.conf /nsconfig/ns.conf	Done
✓	shell	Done
✓	reboot	Done

ジョブを使用して **Citrix ADC** インスタンスをアップグレードする

May 7, 2021

Citrix Application Delivery Management（ADM）では、1 つ以上の Citrix ADC インスタンスをアップグレードできます。インスタンスをアップグレードする前に、ライセンスフレームワークとライセンスのタイプを知っておく必要があります。

前提条件

ADC インスタンスをアップグレードする前に、アップグレードするインスタンスに対して事前検証チェックを実行します。

1. カスタマイズをチェックする -カスタマイズをバックアップし、インスタンスから削除します。インスタンスのアップグレード後に、バックアップしたカスタマイズを再適用できます。
2. ディスクハードウェアの問題の確認 -ハードウェアの問題があれば解決します。

ADC の高可用性ペア

ADC 高可用性ペアをアップグレードする場合は、次の点に注意してください。

- セカンダリノードが最初にアップグレードされます。
- ノードの同期と伝播は、両方のノードが正常にアップグレードされるまで無効になります。
- 高可用性ペアのアップグレードが成功すると、実行履歴にエラーメッセージが表示されます。このメッセージは、高可用性ペアのノードが異なるビルドまたはバージョン上にある場合に表示されます。このメッセージは、1 次ノードと 2 次ノード間の同期が無効になっていることを示します。

ADC 高可用性ペアは、次の 2 つの段階でアップグレードできます。

1. アップグレードジョブを作成し、いずれかのノードで直ちに実行するか、後でスケジュールします。
2. 後で残りのノードで実行するようにアップグレードジョブをスケジュールします。最初のノードのアップグレード後に、必ずこのジョブをスケジュールしてください。

ADC クラスタ

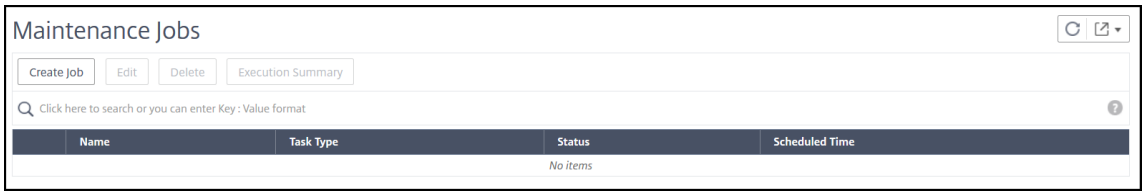
ADC クラスタをアップグレードすると、アップグレード前の検証段階で、ADM は指定されたインスタンスのみを検証します。したがって、確認し、クラスターノード上の次の問題を解決します。

- カスタマイズ
- ディスク使用率
- ハードウェアの問題

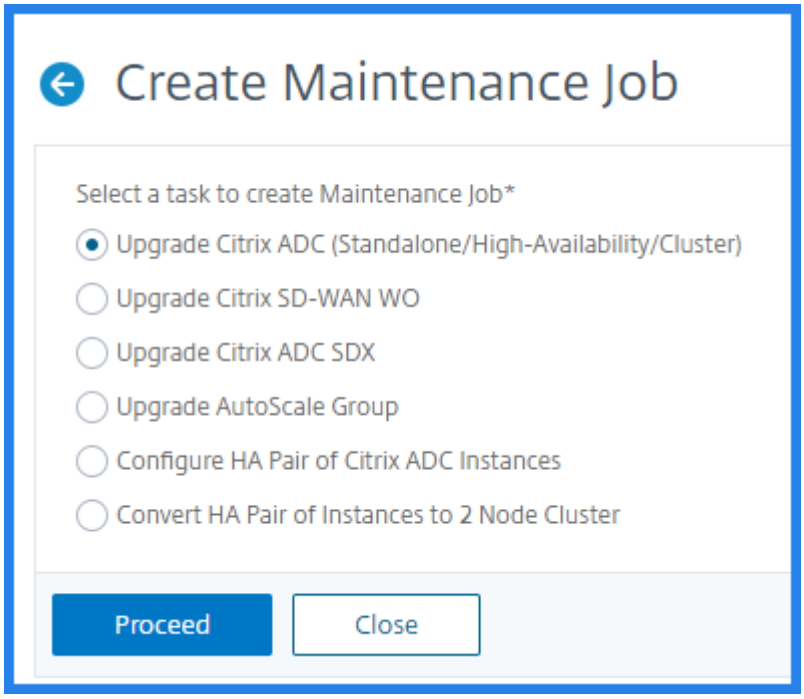
ADC アップグレード・ジョブの作成

ADC アップグレードジョブを作成するには、次の手順を実行します。

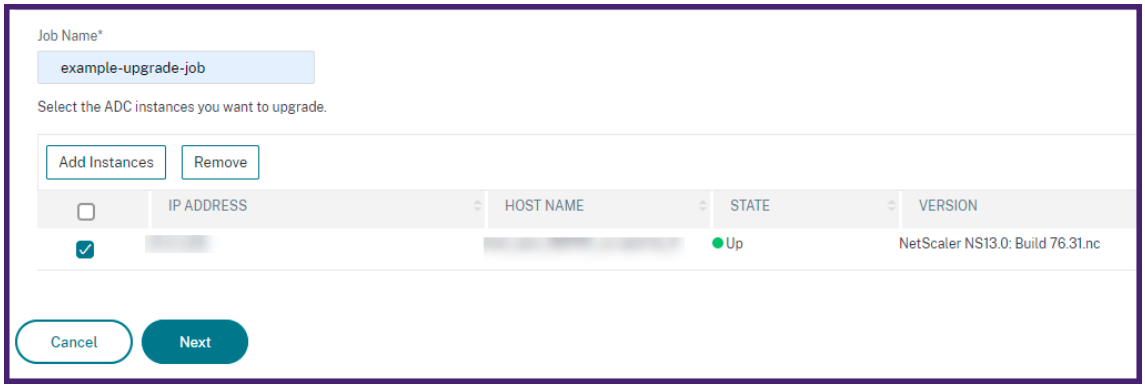
1. ネットワーク **>** 構成ジョブ **>** メンテナンスジョブに移動します。



2. ［保守ジョブの作成］で ［**Citrix ADC**（スタンドアロン/高可用性/クラスター）のアップグレード］を選択し、［続行］をクリックします。



3. **[** インスタンスの選択**]** で、[ジョブ名**]** に選択した名前を入力します。
4. [**Add Instances**] をクリックして、アップグレードする ADC インスタンスを追加します。
   - ADC 高可用性ペアをアップグレードするには、プライマリノードまたはセカンダリノードの IP アドレスを指定します。
   - クラスターをアップグレードするには、クラスターの IP アドレスを指定します。



5. [**Next**] をクリックして、選択したインスタンスでアップグレード前の検証を開始します。

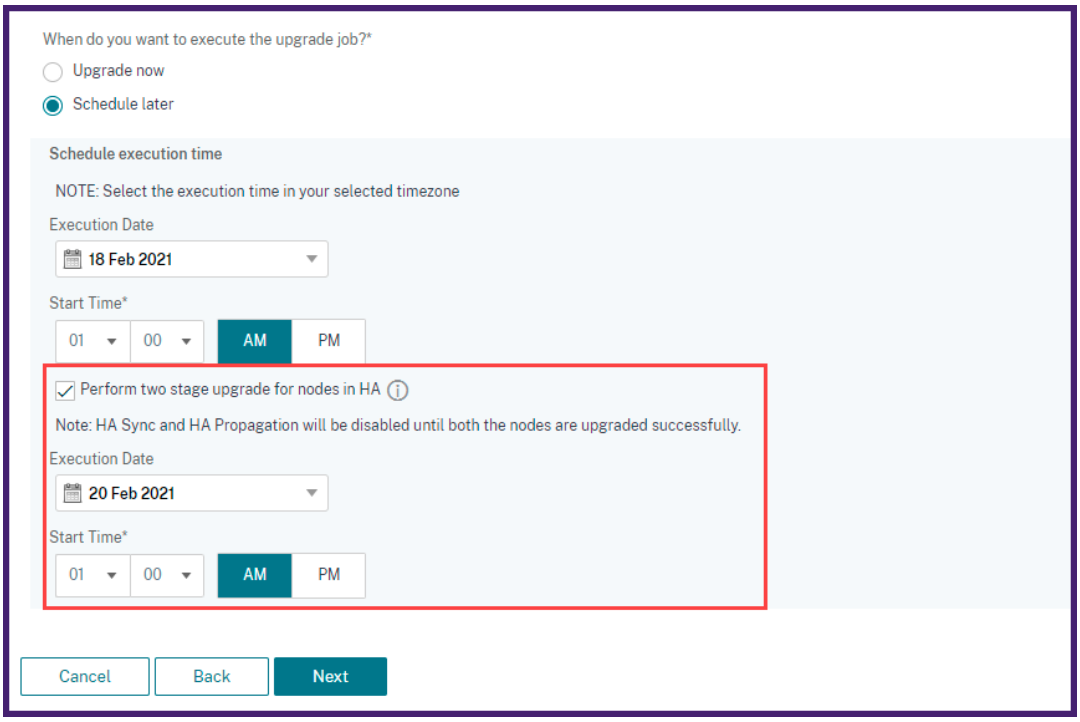
   [アップグレード前の検証] タブには、失敗したインスタンスが表示されます。失敗したインスタンスを削除して、[次へ] をクリックします。

> 重要:
>
> クラスター IP アドレスを指定した場合、ADM は、他のクラスターノードではなく、指定されたインスタンスでのみアップグレード前の検証を行います。

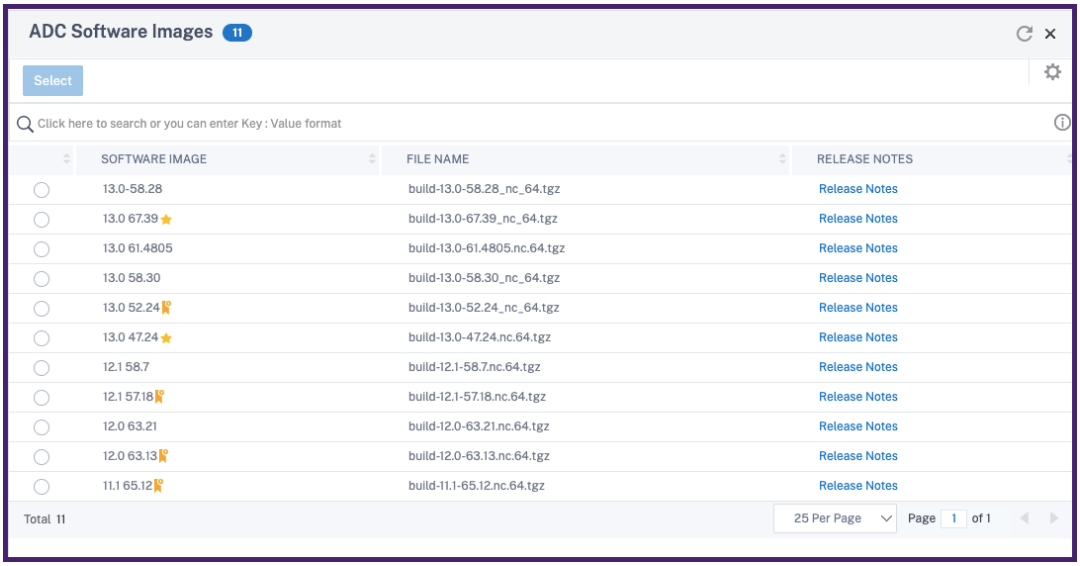
6. 必要に応じて、[カスタムスクリプト] で、インスタンスのアップグレードの前後に実行するスクリプトを指定します。詳しくは、「カスタムスクリプトを使用する」を参照してください。
7. 「タスクのスケジュール」で、次のいずれかのオプションを選択します。
   - 今すぐアップグレード: アップグレードジョブはすぐに実行されます。
   - [後でスケジュール]: このアップグレードジョブを後で実行するには、このオプションを選択します。インスタンスをアップグレードする場合は、[実行日] と **[開始時刻]** を指定します。

     ADC 高可用性ペアを 2 段階でアップグレードする場合は、[高可用性のノードに対して **2** 段階アップグレードを実行する] を選択します。

     高可用性ペアの別のインスタンスをアップグレードする場合は、[**Execution Date]** と **[Start Time]** を指定します。



     詳しくは、「ADC の高可用性ペア」を参照してください。
8. 「ジョブの作成」で、次の詳細を指定します。
   - **ADC** ソフトウェアイメージを選択: リストから ADC イメージを選択します。このオプションでは、Citrix ダウンロード Web サイトで使用可能なすべての ADC イメージが一覧表示されます。



ADC ソフトウェアイメージには、優先ビルドに星形のアイコンが表示されます。そして、ほとんどのダウンロードビルドにはブックマークアイコンが付いています。

- **ADC** ソフトウェアイメージのアップロード: ローカルコンピュータまたは ADC アプライアンスからイメージをアップロードできます。ADC アプライアンスを選択すると、/var/mps/mps_imagesに存在するインスタンスファイルが ADM GUI に表示されます。ADM GUI からイメージを選択します。

アップグレードジョブをスケジュールする場合、インスタンスにイメージをアップロードするタイミングを指定できます。

- 今すぐアップロード: 画像をすぐにアップロードするには、このオプションを選択します。ただし、アップグレードジョブは、スケジュールされた時刻に実行されます。
- **[** 実行時にアップロード**]:** アップグレードジョブの実行時にイメージをアップロードするには、このオプションを選択します。

その他のアップグレードオプションの詳細については、ADC アップグレード・オプションを参照してください。

9. [ジョブの作成] をクリックします。

アップグレードジョブは、**[**ネットワーク**] > [**構成ジョブ**] > [**メンテナンスジョブ] に表示されます。既存のジョブを編集するときに、必須フィールドにすでに入力されている場合は、任意のタブに切り替えることができます。たとえば、[構成の選択] タブが表示されている場合は、[ジョブプレビュー] タブに切り替えることができます。

ADC ディスク領域をクリーンアップする

ADC インスタンスのアップグレード中にディスク容量不足の問題が発生した場合は、ADM GUI 自体からディスク領域をクリーンアップします。

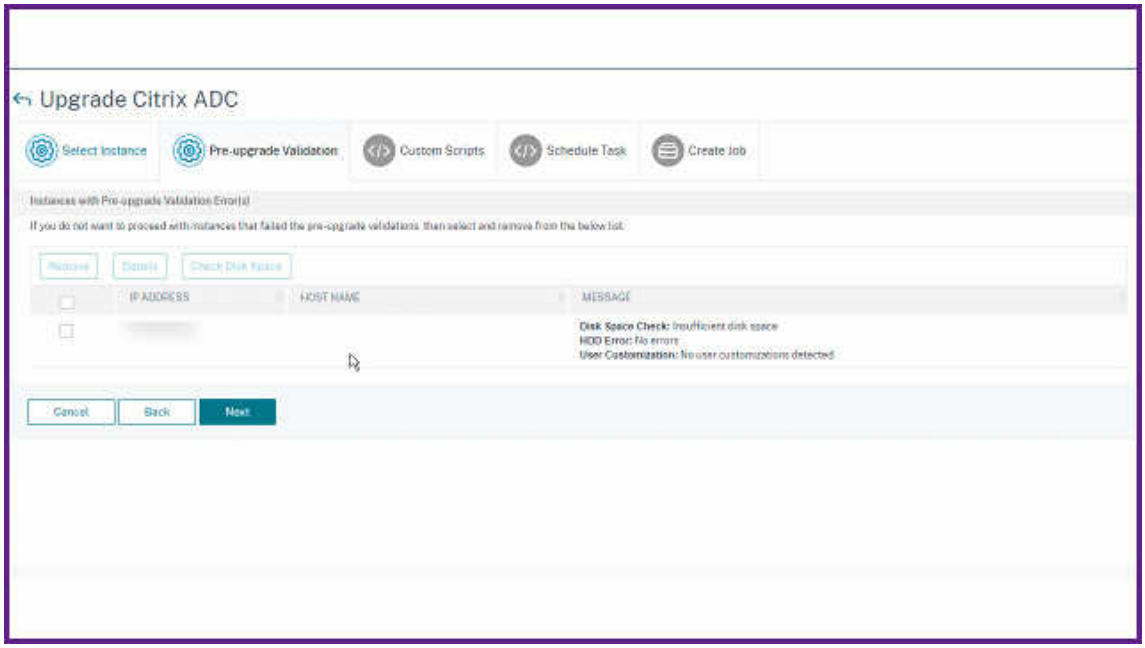
1. [アップグレード前の検証] タブで、ディスク領域の問題があるインスタンスを選択します。

2. [ディスク領域の確認] を選択します。

   このペインには、容量の少ないインスタンスのディスクが表示されます。また、ディスク上で使用され、使用可能なメモリの量も表示されます。

3. [**Check Disk Space**] ペインで、クリーンアップが必要なインスタンスを選択します。

4. [ディスククリーンアップ] をクリックします。



5. 消去するファイルを選択します。

6. [削除] をクリックします

カスタムスクリプトを使用する

ADC アップグレードジョブの作成を実行する間、カスタムスクリプトを指定できます。カスタムスクリプトは、ADC インスタンスのアップグレードの前後に変更をチェックするために使用されます。例:

- アップグレード前とアップグレード後のインスタンスのバージョン。
- アップグレード前後のインターフェイス、高可用性ノード、仮想サーバ、およびサービスのステータス。
- 仮想サーバーとサービスの統計。
- ダイナミックルート。

次のステージで実行するカスタムスクリプトを指定します。

- アップグレード前: インスタンスをアップグレードする前に、指定されたスクリプトが実行されます。
- アップグレード前のフェールオーバー後（**HA** に適用可能）: このステージは、高可用性配置にのみ適用されます。指定されたスクリプトは、ノードのアップグレード後、フェールオーバーの前に実行されます。

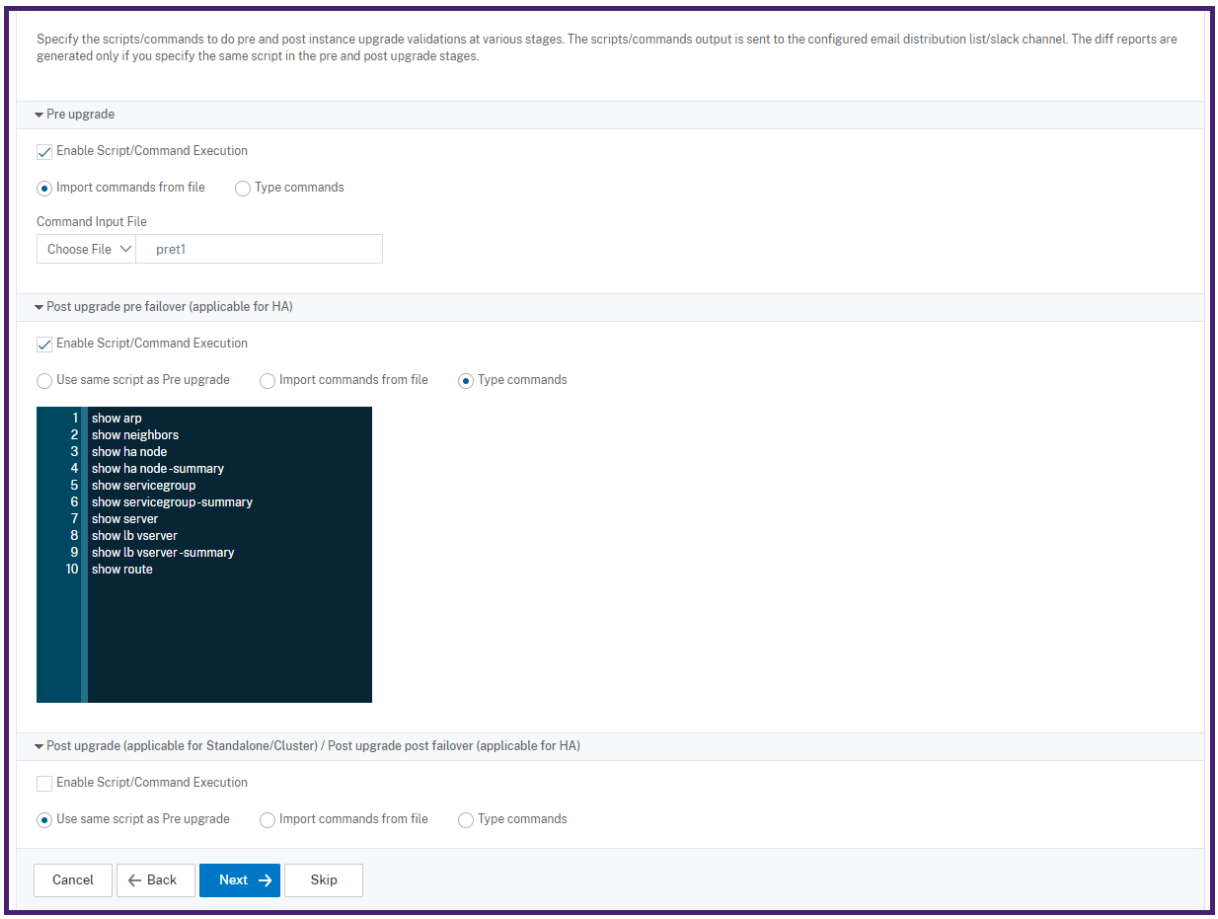
- アップグレード後（スタンドアロンに適用）/フェールオーバー後のアップグレード後（**HA** に適用可能）：指定されたスクリプトは、スタンドアロンデプロイでインスタンスをアップグレードした後に実行されます。高可用性展開では、スクリプトはノードとフェイルオーバーをアップグレードした後に実行されます。

> 注
>
> - 必要な段階で、スクリプトまたはコマンドの実行を有効にしてください。そうしないと、指定されたスクリプトは実行されません。
> - 相違レポートが生成されるのは、アップグレード前およびアップグレード後の段階で同じスクリプトを指定した場合だけです。したがって、アップグレード後の段階で [アップグレード前のスクリプトと同じスクリプトを使用] を選択してください。ADC アップグレード・ジョブの統合差分レポートのダウンロードを参照してください。

ADM GUI では、スクリプトファイルをインポートしたり、コマンドを直接入力したりできます。

- ファイルからコマンドをインポートする: ローカルコンピュータからコマンド入力ファイルを選択します。
- コマンドの入力：**GUI** 上でコマンドを直接入力します。

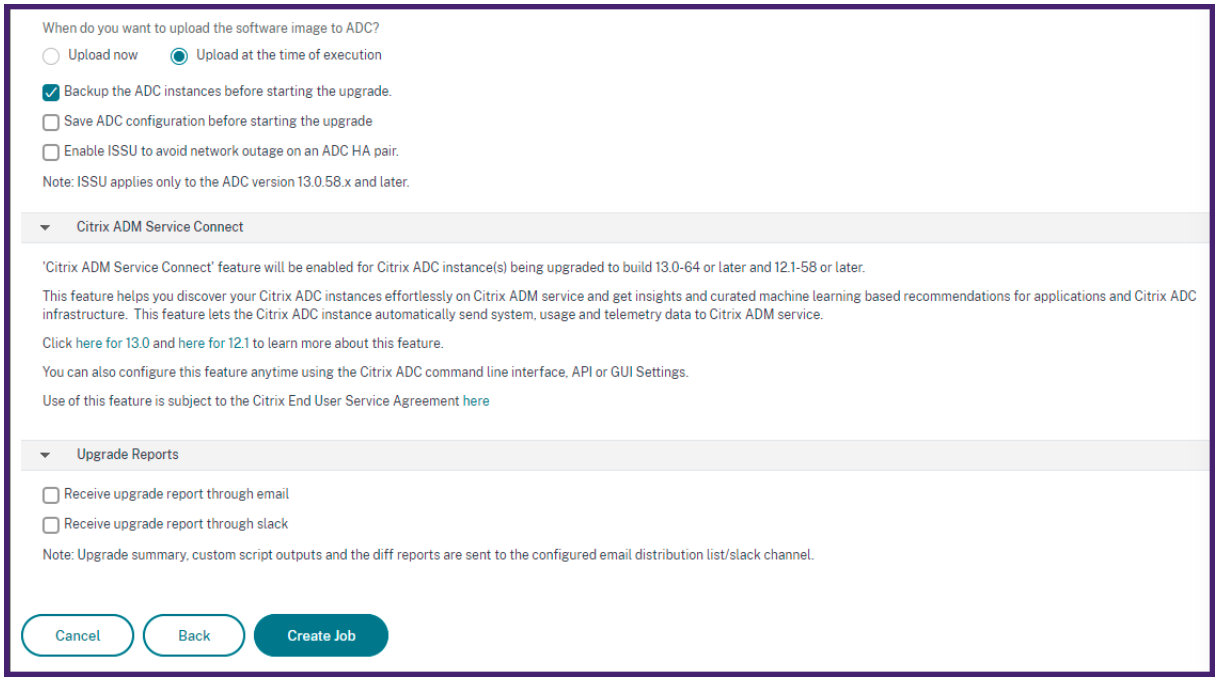
アップグレード後のステージでは、アップグレード前のステージで指定したスクリプトと同じスクリプトを使用できます。



ADC アップグレード・オプション

ADC アップグレードジョブの作成を実行する間、[**Create Job**] タブで次のオプションを選択できます。

- アップグレードの成功時に **Citrix ADC** からソフトウェアイメージをクリーンアップ-インスタンスのアップグレード後に ADC インスタンスでアップロードされたイメージをクリアするには、このオプションを選択します。
- アップグレードを開始する前に、**ADC** インスタンスをバックアップしてください。: 選択した ADC インスタンスのバックアップを作成します。
- アップグレード後に高可用性ノードのプライマリおよびセカンダリステータスを維持する: 各ノードのアップグレード後にアップグレードジョブでフェールオーバーを開始する場合は、このオプションを選択します。このようにして、アップグレードジョブはノードのプライマリとセカンダリのステータスを維持します。
- アップグレード開始前に **ADC** 設定を保存**-ADC** インスタンスをアップグレードする前に、実行中の ADC 設定を保存します。
- **ISSU** を有効にして、**ADC HA** ペアでのネットワーク停止を回避する -ISSU は、ADC 高可用性ペアでのダウンタイムなしのアップグレードを保証します。このオプションは、アップグレード中に既存の接続を使用する移行機能を提供します。そのため、ダウンタイムなしで ADC 高可用性ペアをアップグレードできます。ISSU 移行タイムアウトを分単位で指定します。
- 実行レポートを電子メールで受信する-実行レポートを電子メールで送信します。電子メール同報リストを追加するには、電子メール配布リストの作成を参照してください。
- **slack** による実行レポートの受信-実行レポートを slack で送信します。Slack プロファイルを追加するには、「Slack プロファイルの作成」を参照してください。



ADC アップグレード・ジョブの統合差分レポートのダウンロード

Citrix ADM では、ADC アップグレードジョブの差分レポートをダウンロードできます。これを行うには、アップグレードジョブにカスタムスクリプトが必要です。差分レポートには、アップグレード前スクリプトとアップグレード後のスクリプトの出力の違いが含まれます。このレポートを使用すると、アップグレード後に ADC インスタンスで発生した変更を確認できます。

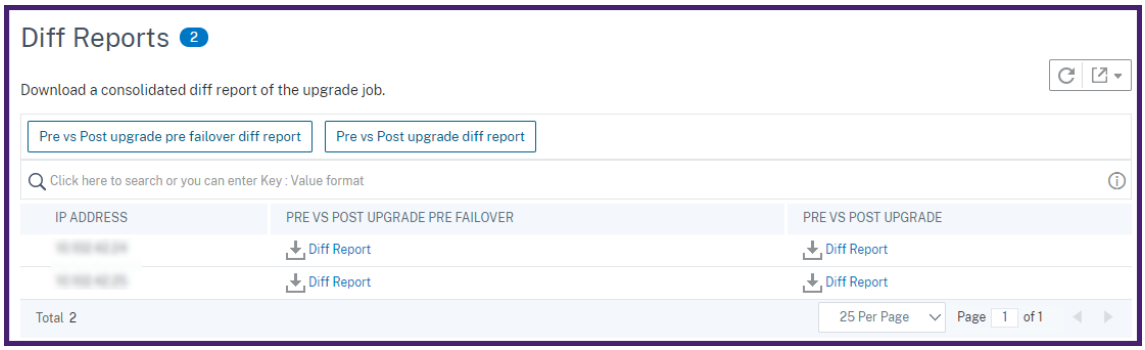
> 注:
>
> 相違レポートが生成されるのは、アップグレード前およびアップグレード後の段階で同じスクリプトを指定した場合のみです。

アップグレードジョブの相違レポートをダウンロードするには、次の手順を実行します。

1. [ネットワーク] **>** [構成ジョブ] **>** [メンテナンスジョブ] に移動します
2. 差分レポートをダウンロードするアップグレードジョブを選択します。
3. 「相違レポート」をクリックします。
4. 相違レポートで、選択したアップグレードジョブの統合差分レポートをダウンロードします。

   このページでは、次の相違レポートの種類をダウンロードできます。

   - アップグレード前とポストアップグレード前のフェイルオーバー差分レポート
   - アップグレード前とアップグレード後の差分レポート



構成テンプレートを使用した監査テンプレートの作成

May 7, 2021

以前に構成テンプレートとして保存した構成コマンドを使用して、特定の Citrix ADC インスタンスに適用できる監査テンプレートを作成できるようになりました。監査テンプレートの作成中に、以前に保存した設定テンプレートを [**Commands**] フィールドにドラッグし、要件に合わせてテンプレートを編集できます。その後、監査テンプレートを特定の Citrix ADC インスタンスに適用できます。Citrix Application Delivery Management（ADM）は、これらのインスタンスを監査テンプレートと比較し、不一致があれば報告します。このプロセスは、エラーを識別し、直ちに修正するために役立ちます。

ジョブを作成し、一連の構成コマンドをテンプレートとして保存するときに、構成テンプレートを作成できます。これらのテンプレートを [ジョブの作成] ページに保存すると、[テンプレートの作成] ページに自動的に表示されます。

たとえば、負荷分散仮想サーバーを追加し、2 つのサービスを追加し、それらのサービスをその仮想サーバーにバインドするという、基本的な負荷分散構成を考えてみましょう。

この例では、次のコマンドを使用します。

```
add lb vserver **servername** HTTP **ipaddress portnumber**

add service **servicename1 ipaddress1** HTTP 80

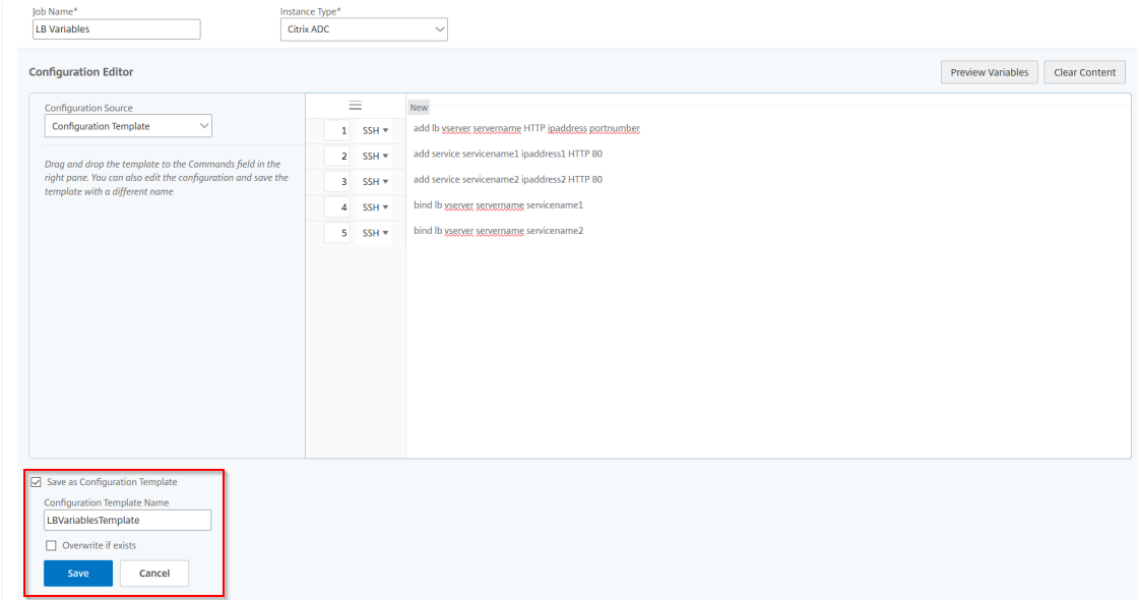
add service **servicename2 ipaddress2** HTTP 80

bind lb vserver **servername servicename1**

bind lb vserver **servername servicename2**
```

Citrix ADM で構成テンプレートを保存するには:

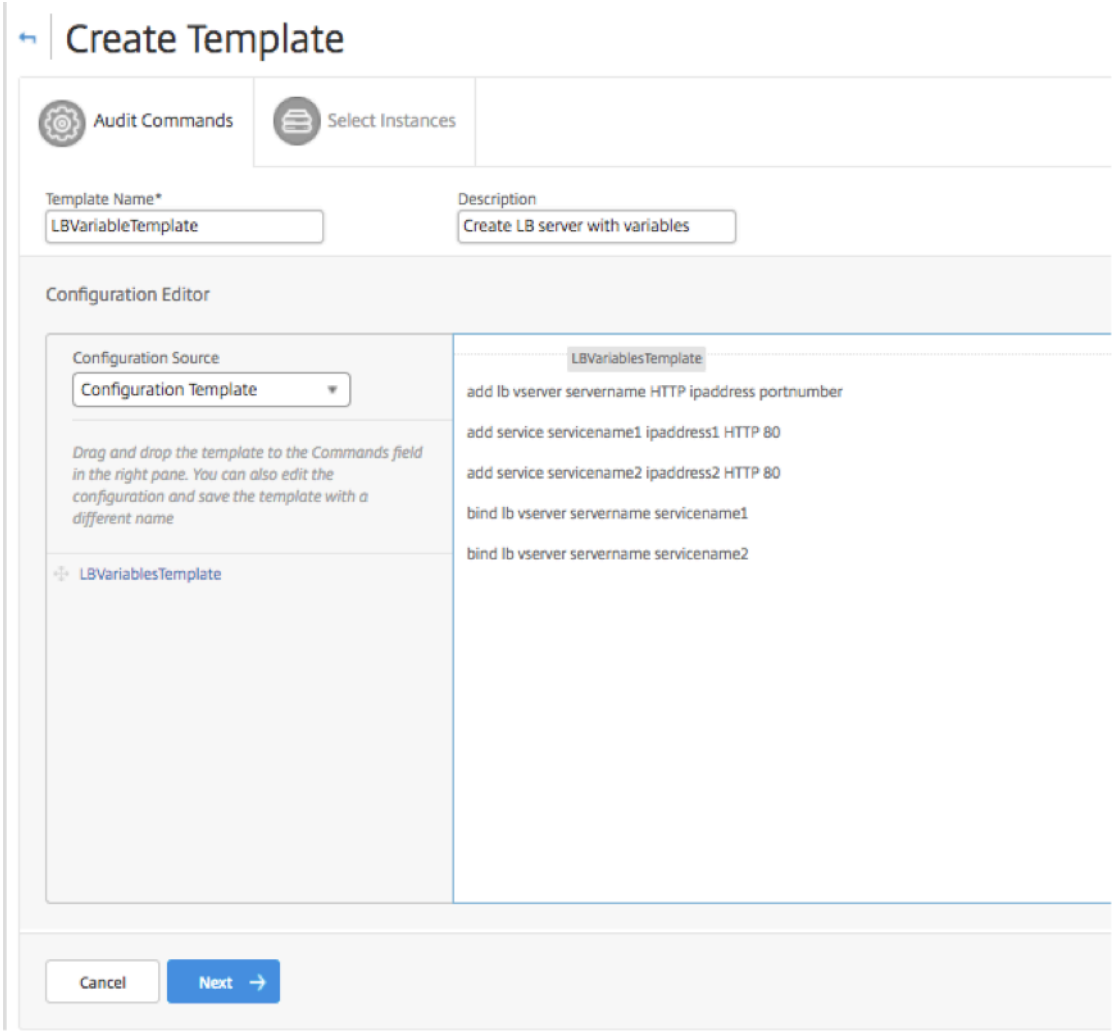
1. [ネットワーク] > [構成ジョブ] に移動し、[ジョブの作成] をクリックします。
2. [**Create Job**] ページで、ジョブ名とインスタンスタイプを指定します。
3. [設定ソース] として **[**設定テンプレート**]** を選択し、**[**コマンド**]** フィールドに、前述の例のようなコマンドを入力します。
4. [構成テンプレートとして保存] チェックボックスをオンにし、テンプレートの名前を指定します。同じ名前が付いた他のテンプレートが存在する場合はそれを上書きすることを選択できます。
5. [保存] をクリックします。



構成テンプレートを使用して **Citrix ADM** で監査テンプレートを作成するには:

1. [ネットワーク] > [構成監査] > [監査テンプレート] に移動し、[追加] をクリックします。

2. [テンプレートの作成] ページで、テンプレート名の名前を指定し、説明を入力します。
3. [構成ソース] ボックスの一覧から [構成テンプレート] を選択し、右側のペインの [コマンド] フィールドにテンプレートをドラッグします。構成を編集し、テンプレートを別の名前で保存することもできます。[次へ] をクリックします。
4. [**Select Instances**] タブで、[**Add** Instances] をクリックし、設定を実行するインスタンスを追加します。[**OK**] をクリックします。
5. [完了] をクリックします。



監査テンプレートは、[Audit Templates] ボックスの一覧に表示され、指定したインスタンスの構成に対して 12 時間ごとに実行されます。

設定ジョブで **SCP (put)** コマンドを使用する

May 7, 2021

Citrix Application Delivery Management（ADM）の構成ジョブ機能を使用して、構成ジョブの作成、電子メール通知の送信、および作成されたジョブの実行ログの確認を行うことができます。ジョブとは、管理対象インスタンスに対して作成および実行できる構成コマンドのセットです。たとえば、デバイスのアップグレードのために構成ジョブを使用できます。

Citrix ADM の構成ジョブでは、Secure Shell（SSH）コマンドを使用してインスタンスを構成し、Secure Copy（SCP）を使用してファイルを安全に転送するように構成ジョブを構成できます。SCP は SSH プロトコルに基づいています。構成ジョブに含めることができる SCP コマンドの 1 つは、「put」コマンドです。構成ジョブで「put」コマンドを使用して、システムのローカルディレクトリに保存されている 1 つ以上のファイルを Citrix ADM にアップロードまたは転送し、次に Citrix ADC インスタンスのディレクトリにアップロードまたは転送できます。

> 注:
>
> ファイルは Citrix ADM にアップロードされ、後で選択した Citrix ADC インスタンスにコピー（PUT）されます。アップロードされたファイルは Citrix ADM に保存され、ジョブが削除されたときにのみ削除されます。これは、後で実行するようにスケジュールされているジョブに必要です。

このコマンドの構文を次に示します。

```
put <local_filename> <remote_path/remote_filename>
<!--NeedCopy-->
```

各項目の意味は次のとおりです。

<local_filename> は、アップロードするローカルファイルの名前です。

<remote_path/ remote_filename> は、リモートディレクトリへのパス、およびファイルがそのディレクトリにコピーされるときにそのファイルに割り当てる名前です。

構成ジョブの作成中に、ローカルファイル名とリモートファイル名のパラメーターを変数に変換できます。これにより、ジョブを実行するたびに、同じ Citrix ADC インスタンスのセットに対して、これらのパラメーターに異なるファイルを割り当てることができます。また、1 つのファイルをジョブ内の複数の位置で使用しており、そのファイルの名前を変更する必要がある場合は、すべての位置でファイル名を変更するのではなく、変数を再定義できます。

put コマンドを使用して、設定ジョブでファイルをアップロードするには、次の手順を実行します。

1. Citrix ADM で、［ネットワーク］>［構成ジョブ］に移動します。
2. [ジョブ] ページで、[ジョブの作成] をクリックします。
3. [ジョブの作成] ページで、[ジョブ名] フィールドにジョブの名前を入力し、[構成エディタ] ペインで [put] コマンドを入力します。

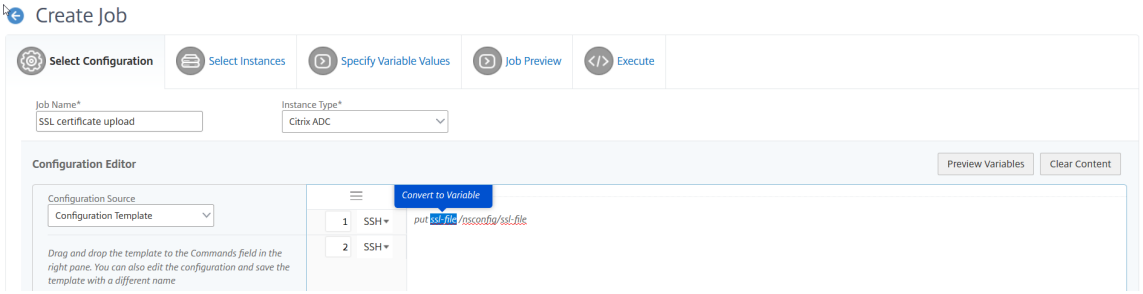
   たとえば、ローカルシステムに保存されている SSL 証明書ファイルを複数の Citrix ADC インスタンスにコピーする構成ジョブを作成する場合は、特定のファイルの名前の代わりに変数を使用する「put」コマンドを追加し、変数の種類を「file」として定義できます。

   ```
   put ssl-file /nsconfig/ssl-file
   <!--NeedCopy-->
   ```


この例の説明を次に示します。

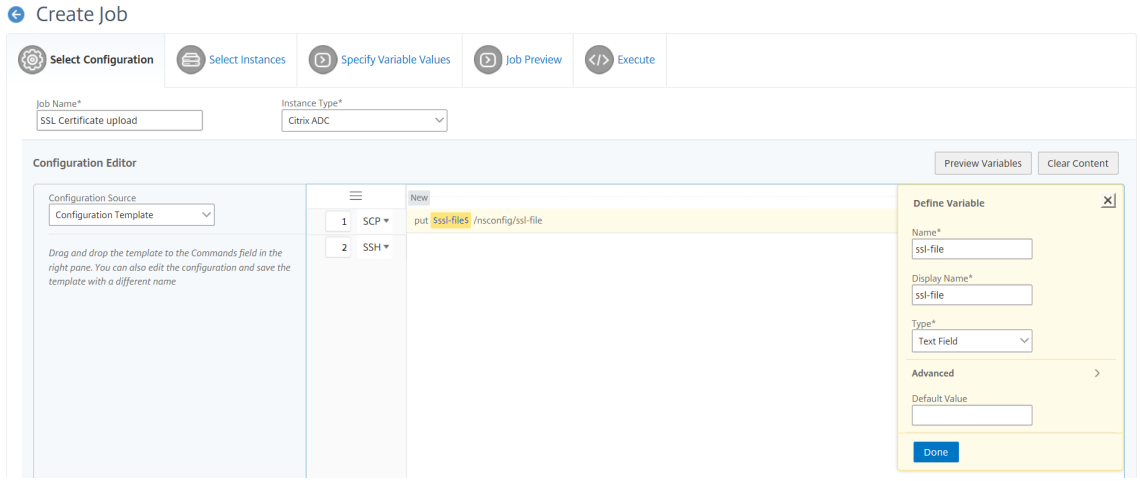
- `ssl-file` -Citrix ADC インスタンスにアップロードする必要があるファイルの名前です。
- `/nsconfig/ssl-file` - タスクの実行後に`ssl-file`が配置されるインスタンス上の宛先フォルダです。

4. 次の図に示すように、入力したコマンドで、変数に変換するファイル名を選択し、[変数に変換] をクリックします。

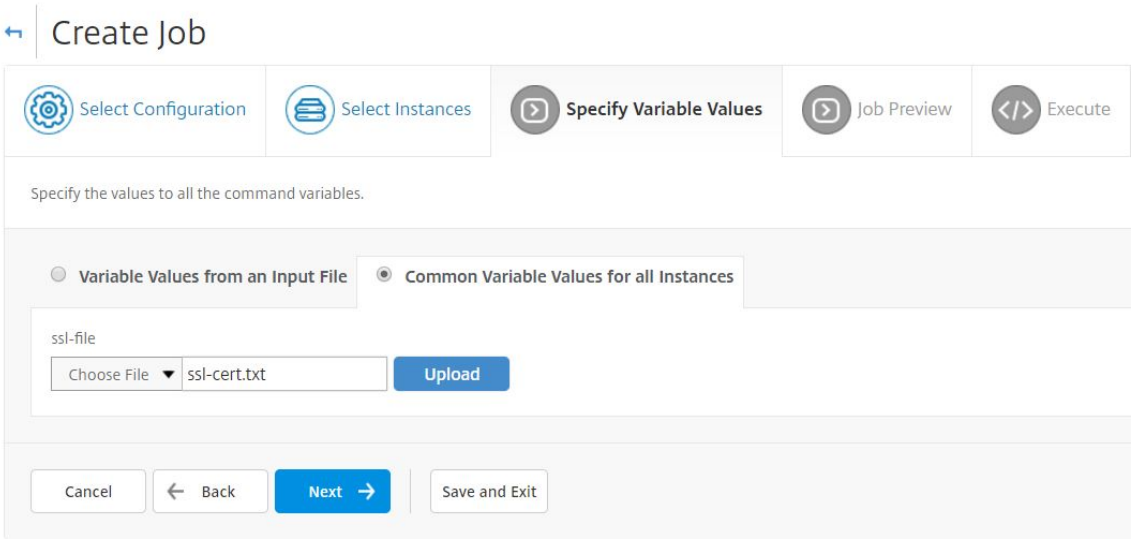


5. ファイル名がドル記号 (変数であることを示す) で囲まれていることを確認し、変数をクリックします。
6. 名前、表示名、タイプなど、変数の詳細を指定します。
7. [タイプ] ドロップダウンリストから [ファイル] を選択します。［保存］をクリックします。

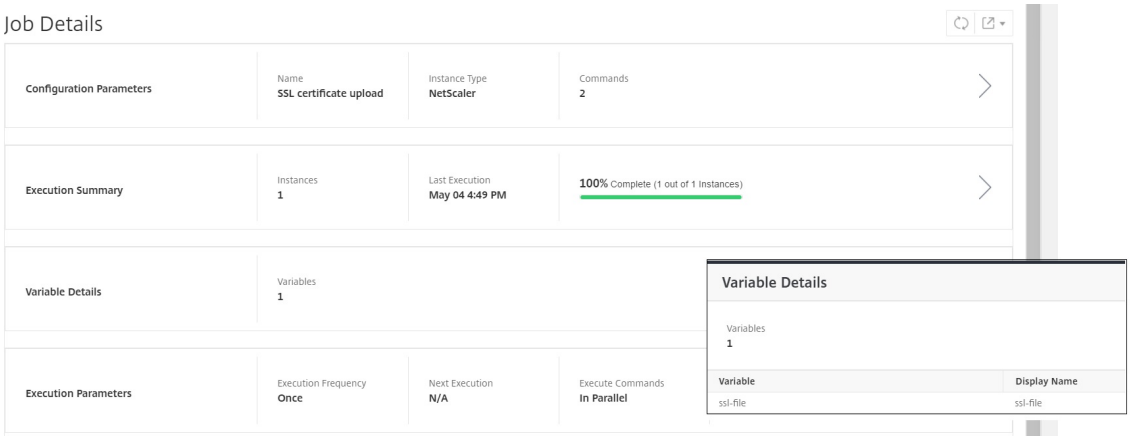
   変数を「ファイル」タイプとして宣言すると、ファイルを Citrix ADM にアップロードできます。



8. ［次へ］をクリックし、ファイルをコピーする Citrix ADC インスタンスを選択します。
9. ［変数値の指定］タブで、［すべてのインスタンスの共通変数値］セクションで、システム上のローカルストレージからファイルを選択し、［アップロード］をクリックしてファイルを Citrix ADM にアップロードし、［次へ］をクリックします。



10. [**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証できます。
11. [**Execute**] タブでは、ジョブを今すぐ実行することも、後で実行するようにスケジュールすることもできます。コマンドが失敗した場合に Citrix ADM が実行する必要があるアクションを選択することもできます。また、ジョブの成功または失敗、およびその他の詳細について通知を受け取るように、メール通知を作成できます。[完了] をクリックします。
12. ジョブの詳細を表示するには、[ネットワーク] > [構成ジョブ] に移動し、設定したジョブを選択します。[詳細] をクリックし、[変数の詳細] をクリックして、ジョブに追加された変数の一覧を表示します。



組み込みテンプレートを使用して構成されたジョブを再スケジュールする

May 7, 2021

Citrix Application Delivery Management（ADM）の組み込みテンプレートを使用して、スケジュールしたジョ

ブを再スケジュールできます。たとえば、コマンドが失敗した場合に Citrix ADM が実行する必要があるアクションを変更できます。エラーを無視して続行するように設定していた場合、その設定を、1 つのコマンドが失敗したらすべての成功したコマンドをロールバックするように変更できます。

Citrix ADM で組み込みテンプレートを使用して構成されたジョブを再スケジュールするには:

1. Citrix ADM で、［ネットワーク］>［構成ジョブ］に移動します。
2. インスタンスを編集、追加、または削除するジョブを選択し、変数値を指定してから、実行アクションと設定を変更します。
3. ［**Finish**］をクリックしてジョブを再スケジュールします。

> 注
>
> ジョブを選択し、もう一度 [**Execute**] をクリックすると、ソース、インスタンス、コマンドを変更せずにジョブを実行することもできます。これは、同じインスタンスで同じコマンドセットを実行する必要がある場合に便利です。場合によっては、ジョブがサーバー側から一時的なエラーが発生し、ジョブを再度実行する必要がある場合があります。

構成ジョブでの構成監査テンプレートの再利用

May 7, 2021

管理者は、ジョブの作成時および設定監査の実行時に、構成コマンドを再利用可能な設定テンプレートのセットとして保存できるようになりました。構成ジョブモジュールで作成および保存された構成テンプレートは、「構成監査」で使用でき、特定の Citrix ADC インスタンスに適用できる監査テンプレートを作成できます。同様に、構成監査モジュールで作成された監査テンプレートは [構成ジョブ] で使用できるため、テンプレートを構成ジョブとして実行できます。テンプレートに加えられた変更は、設定ジョブと構成 **Audi**t モジュールの両方に表示されます。

以前は、構成ジョブテンプレートと構成監査テンプレートを同じ構成のために別々に作成し、別のファイルとして保存する必要がありました。このため、テンプレートの作成時と保守時に同じ作業を繰り返す必要がありました。

Citrix Application Delivery Management（ADM）では、このテンプレートをシステムに保存して、監査テンプレートを構成ジョブでも使用できます。ここでは、監査テンプレートを構成ジョブの作成に使用できます。このようにして、構成ジョブと構成監査の間でテンプレートを相互に使用することができます。

たとえば、負荷分散仮想サーバーを追加し、2 つのサービスを追加し、それらのサービスをその仮想サーバーにバインドするという、基本的な負荷分散構成を考えてみましょう。

この例では、次のコマンドを使用します。

```
add lb vserver servername HTTP ipaddress portnumber

add service servicename1 ipaddress1 HTTP 80

```



```
add service servicename2 ipaddress2 HTTP 80

bind lb vserver servername servicename1

bind lb vserver servername servicename2
<!--NeedCopy-->
```

構成監査でのテンプレートの作成と構成ジョブでのその使用

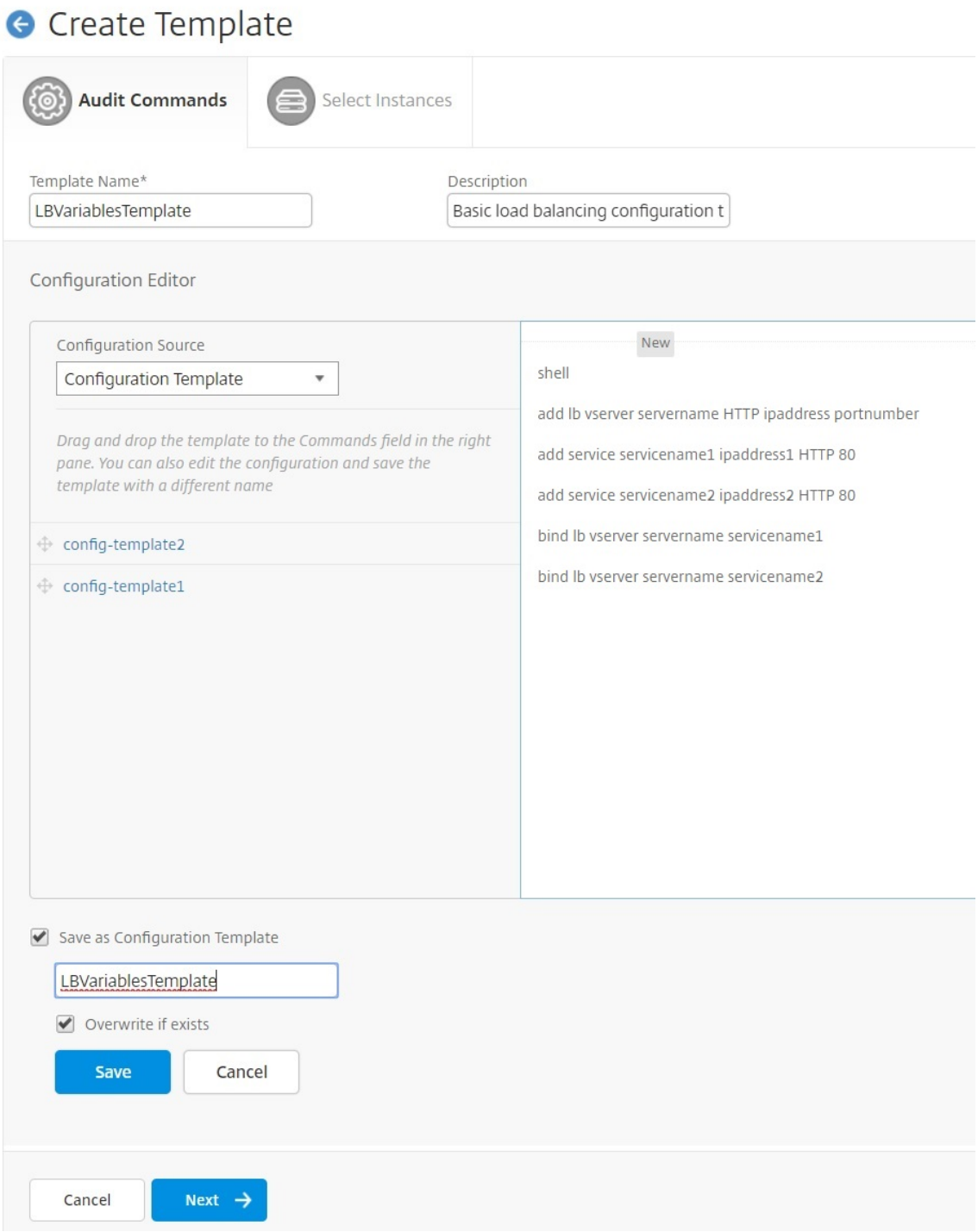
構成監査モジュールにテンプレートを作成し、そのテンプレートを構成ジョブモジュールで再利用するには、次の作業を実行します。

監査テンプレートを作成するには、次の手順に従います。

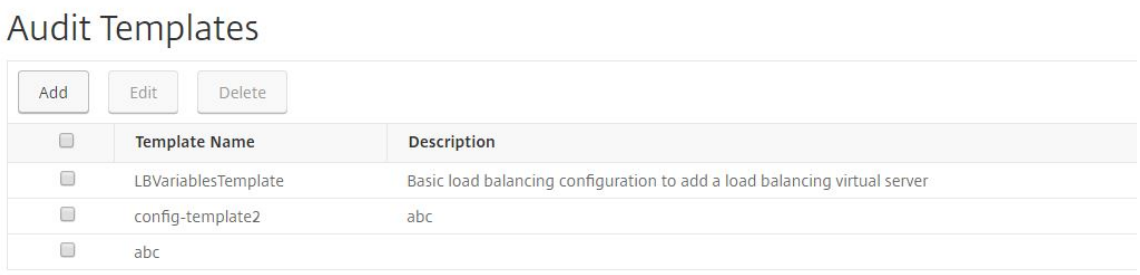
1. Citrix ADM で、[ネットワーク] > [構成監査] > [監査テンプレート] の順に選択し、[追加] をクリックします。
2. **[** テンプレートの作成] ページで、テンプレート名を指定します。[説明] フィールドに、テンプレートの詳細情報を追加することもできます。
3. [**Commands**] ペインで、前の例のようなコマンドを入力します。
4. [構成テンプレートとして保存] チェックボックスをオンにし、テンプレートの名前を指定します。たとえば、このテンプレートに「lbVariableSTemplate」という名前を付けることができます。同じ名前が付いた他のテンプレートが存在する場合はそれを上書きすることを選択できます。

   > **注:**
   >
   > 監査テンプレート名は、構成テンプレート名と同じにすることができます。

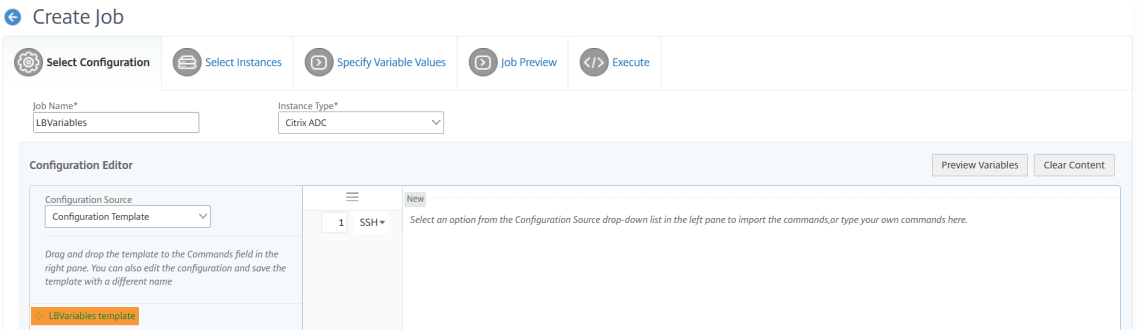
5. [保存] をクリックし、[次へ] をクリックします。



6. ［次へ］をクリックします。
7. ［インスタンスの選択］タブで、これらの構成コマンドを実行する Citrix ADC インスタンスを選択し、［完了］をクリックします。新しいテンプレートが監査テンプレートの一覧に表示されるようになります。

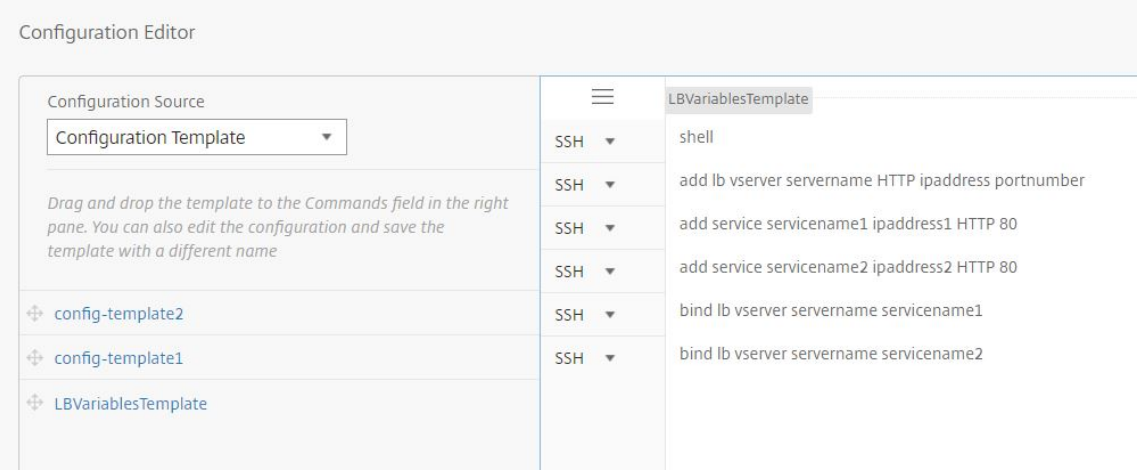


8. これらの構成コマンドを実行するには、[ネットワーク] > [構成ジョブ] に移動し、[ジョブの作成] をクリックします。前に作成した監査テンプレートは、構成テンプレートとして一覧に表示されます。



構成ジョブで監査テンプレートを再利用するには、次の手順に従います。

1. ジョブの名前を入力し、インスタンスタイプを選択し、テンプレートをコマンドペインにドラッグします。



   構成ジョブの作成中に、ローカルファイル名とリモートファイル名のパラメーターを変数に変換できます。これにより、ジョブを実行するたびに、同じ Citrix ADC インスタンスのセットに対して、これらのパラメーターに異なるファイルを割り当てることができます。

2. 入力したコマンドで、変数に変換するファイル名を選択し、[変数に変換] をクリックします。
3. [**Select Inst** ances] タブで、これらのコマンドを実行するインスタンスを選択します。

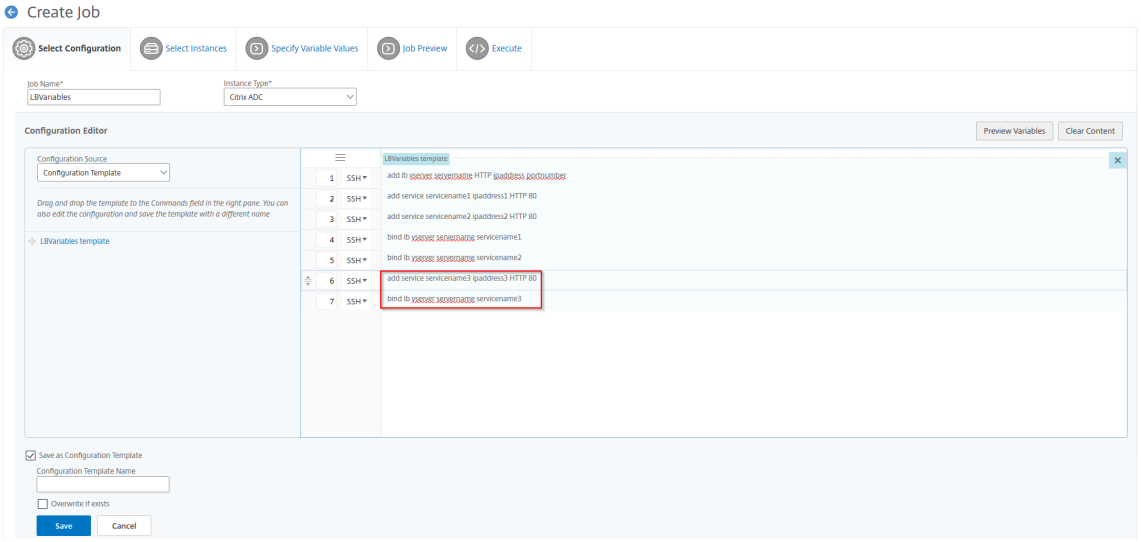
4. コマンドで 変数を指定した場合は、**[Specify Variable Valu** es] タブで、次のいずれかのオプションを選択して、インスタンスの変数を指定します。

   - 入力ファイルから変数値：入力ファイルをダウンロードして、コマンドで定義した変数の値を入力し、ファイルを Citrix ADM サーバーにアップロードします。
   - Common variable values for all instances - Syslog サーバーの IP アドレスとポートを指定します。

5. [**Job Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および検証し、[**Next**] をクリックします。

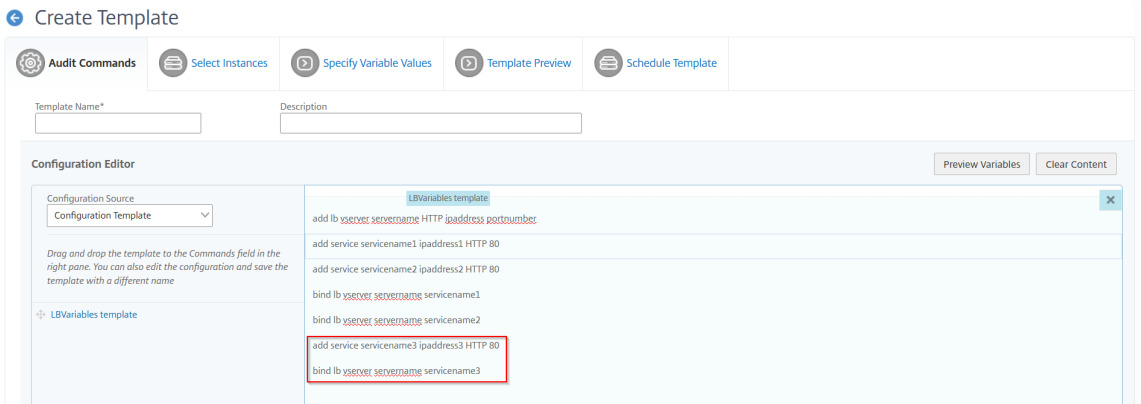
6. [実行] タブで、[完了] をクリックして構成ジョブを実行します。

   この時点で、別のサービスをこの負荷分散サーバーに追加して、そのサービスをそのサーバーにバインドする必要がある場合は、コマンドページでコマンドを編集し、保存することができます。



7.「監査テンプレート」にナビゲートし、「追加」をクリックします。

8.「lbVariablesTemplate」テンプレートをコマンドペインにドラッグします。そのテンプレートが新しいコマンドで更新されたことがわかります。



監査テンプレートは、[Audit Templates] ボックスの一覧に表示され、指定したインスタンスの構成に対して 12 時間ごとに実行されます。これで、テンプレートを作成し、構成ジョブモジュールと構成監査モジュールとの間で再使用できるようになりました。

構成テンプレートのインポートとエクスポート

May 7, 2021

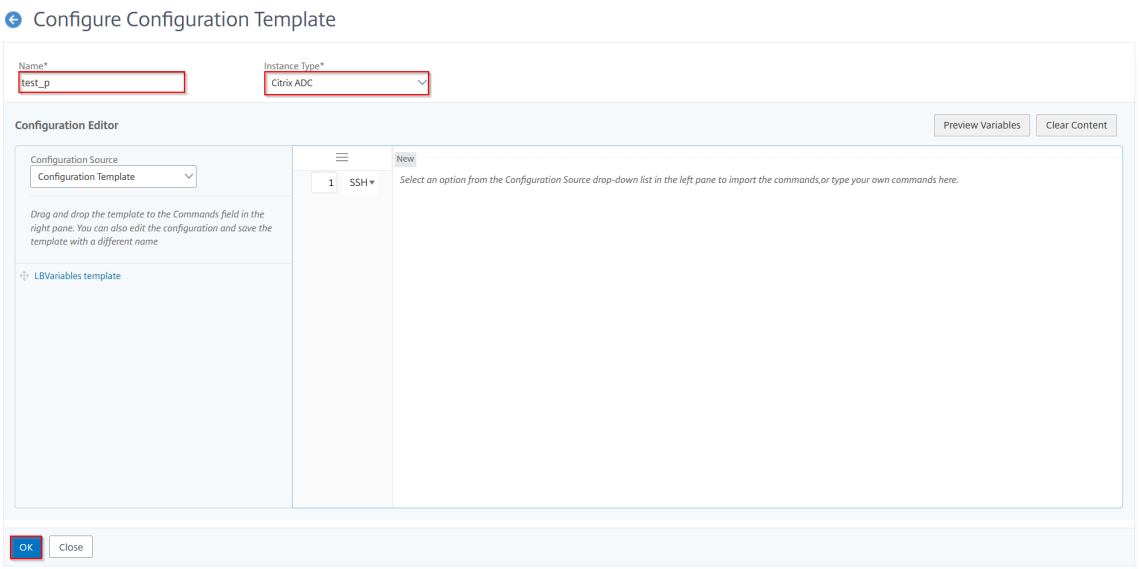
Citrix Application Delivery Management（ADM）アプライアンスから構成テンプレートをエクスポートし、今後いつでも同じまたは他の Citrix ADM アプライアンスにファイルをインポートできます。構成テンプレートデータ（構成コマンド、変数定義、パラメータなど）は失われません。

構成テンプレートを **.json** ファイル形式にエクスポートし、ローカルフォルダに保存できます。構成テンプレートをインポートできます。**json** ファイルを **Citrix** ADM アプライアンスに、同じまたは他の Citrix ADM アプライアンスからエクスポートしたか、手動で作成した可能性があります。

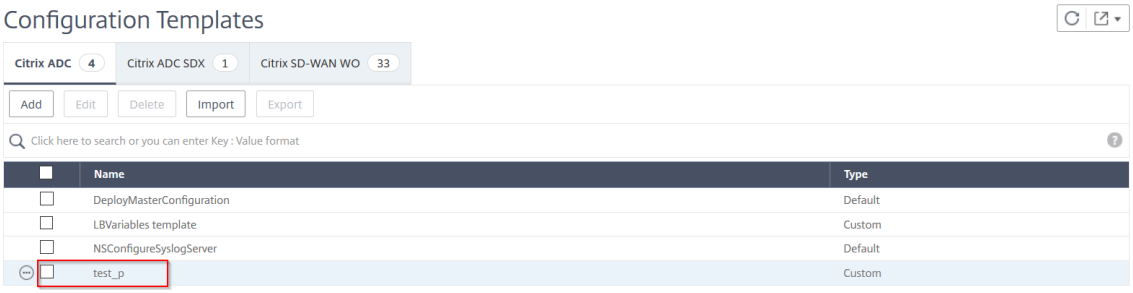
構成テンプレートをエクスポートするには、次の手順に従います。

1. [ネットワーク] > [構成ジョブ] > [構成テンプレート] に移動します。
2. [**Add**] をクリックして、構成テンプレートを作成します。

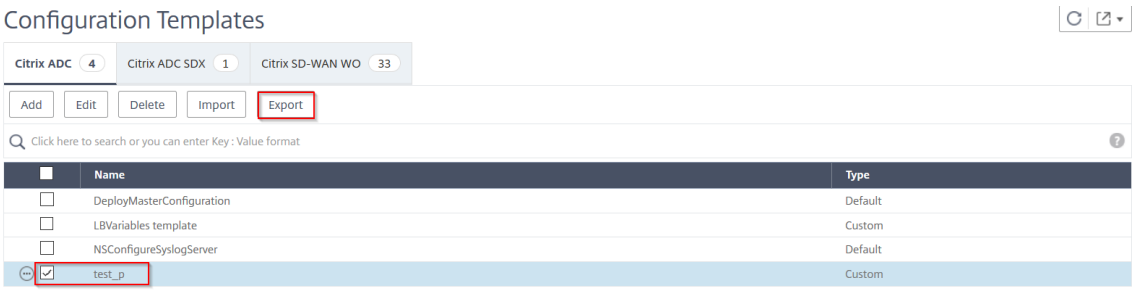
3. [**Create Configuration Template**] ページで、設定テンプレート名を指定し、インスタンスタイプを選択します。[構成エディタ] で、ドロップダウンメニューから [構成テンプレート] として構成ソースを選択します。既存の構成テンプレートを構成エディターにドラッグできます。[**OK**] をクリックします。



4. [ネットワーク] > [構成ジョブ] > [構成テンプレート] に移動して、[構成テンプレート] の一覧で作成されたテンプレートを表示します。



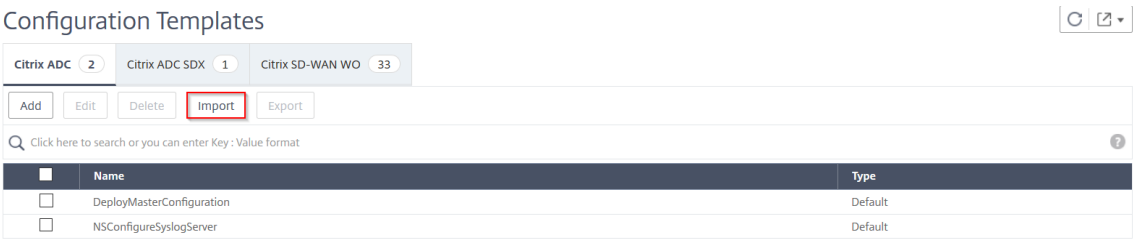
5. 新しく作成した構成テンプレートを選択し、[**Export**] ボタンをクリックします。



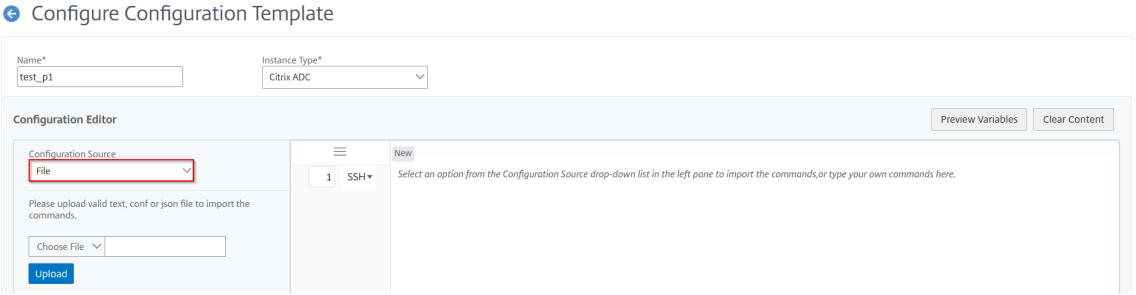
対応する構成テンプレートが **.json** 形式でローカルシステムにダウンロードされます。

構成テンプレートをインポートするには、次の手順に従います。

1. [ネットワーク] > [構成ジョブ] > [構成テンプレート] に移動し、[インポート] ボタンをクリックします。構成テンプレートの.**json** ファイルがあるパスを選択し.**json** ファイルをアップロードします。エクスポート済みの.**json** ファイルをアップロードすることをお勧めします。



2. 構成エディタの **[** ファイル**]** オプションを使用して、構成テンプレートをインポートすることもできます。構成エディタのドロップダウンメニューから **[** ファイル**]** を選択し、**[**ファイル**]** (**.json** ファイル) をローカルシステムからダウンロードし、設定テンプレート**.json** ファイルをアップロードします。



> 注
>
> 構成テンプレートをインポートできるのは、ファイルがに保存されている場合だけです。**json** 形式です。**.json** ファイル以外の構成テンプレートをローカルシステムからインポートすると、エラーが表示され、ファイルのインポートに失敗します。

メンテナンス・ジョブ

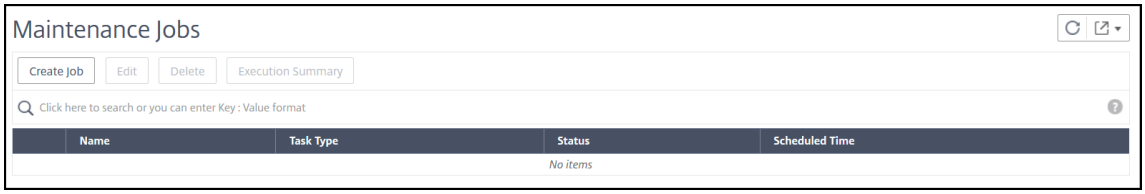
May 7, 2021

Citrix Application Delivery Management（ADM）を使用して、次のメンテナンスタスクを作成できます。その後、特定の日時にメンテナンスタスクをスケジュールできます。

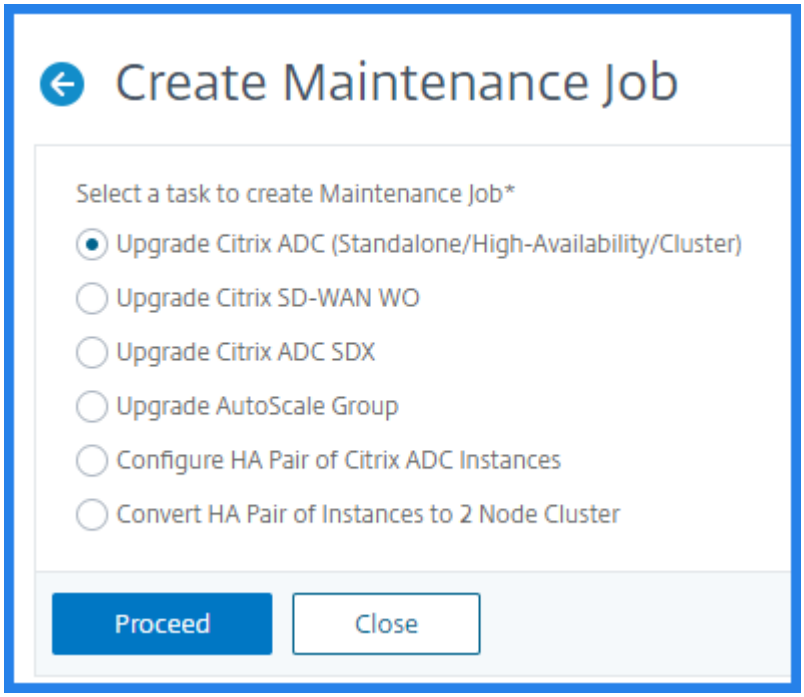
- Citrix ADC インスタンスのアップグレード
- Citrix SD WAN-WO インスタンスのアップグレード
- Citrix ADC SDX インスタンスのアップグレード
- Autoscale グループ内の Citrix ADC インスタンスのアップグレード
- Citrix ADC インスタンスの HA ペアを構成する
- HA インスタンスのペアをクラスターに変換する

Citrix ADC インスタンスのアップグレードをスケジュールする

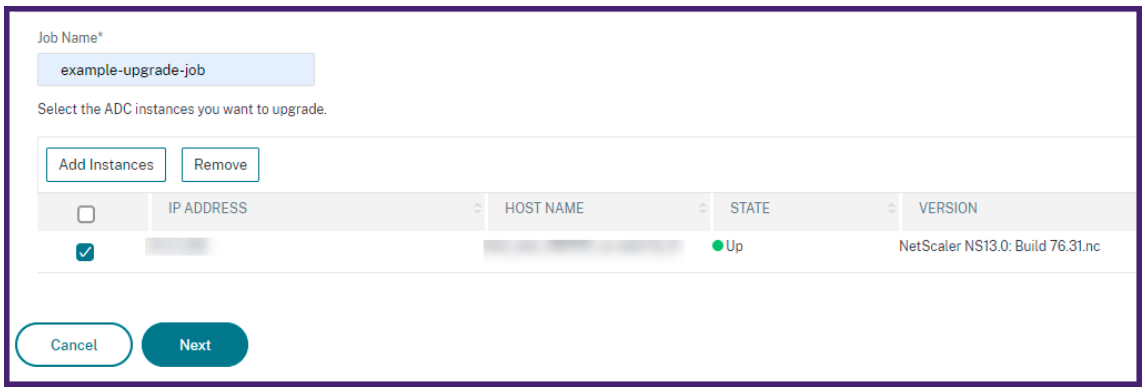
1. Citrix ADM で、[ネットワーク] > [構成ジョブ] **>** [メンテナンスジョブ ******] の順に選択します。**[**** ジョブの作成] ボタンをクリックします。



2. [保守ジョブの作成] で [**Citrix ADC**（スタンドアロン/高可用性/クラスター）のアップグレード] を選択し、[続行] をクリックします。



3. **[** インスタンスの選択**]** で、[ジョブ名**]** に選択した名前を入力します。
4. [**Add Instances**] をクリックして、アップグレードする ADC インスタンスを追加します。
   - HA ペアをアップグレードするには、プライマリノードまたはセカンダリノードの IP アドレスを指定します。ただし、プライマリインスタンスを使用して HA ペアをアップグレードすることをお勧めします。
   - クラスターをアップグレードするには、クラスターの IP アドレスを指定します。



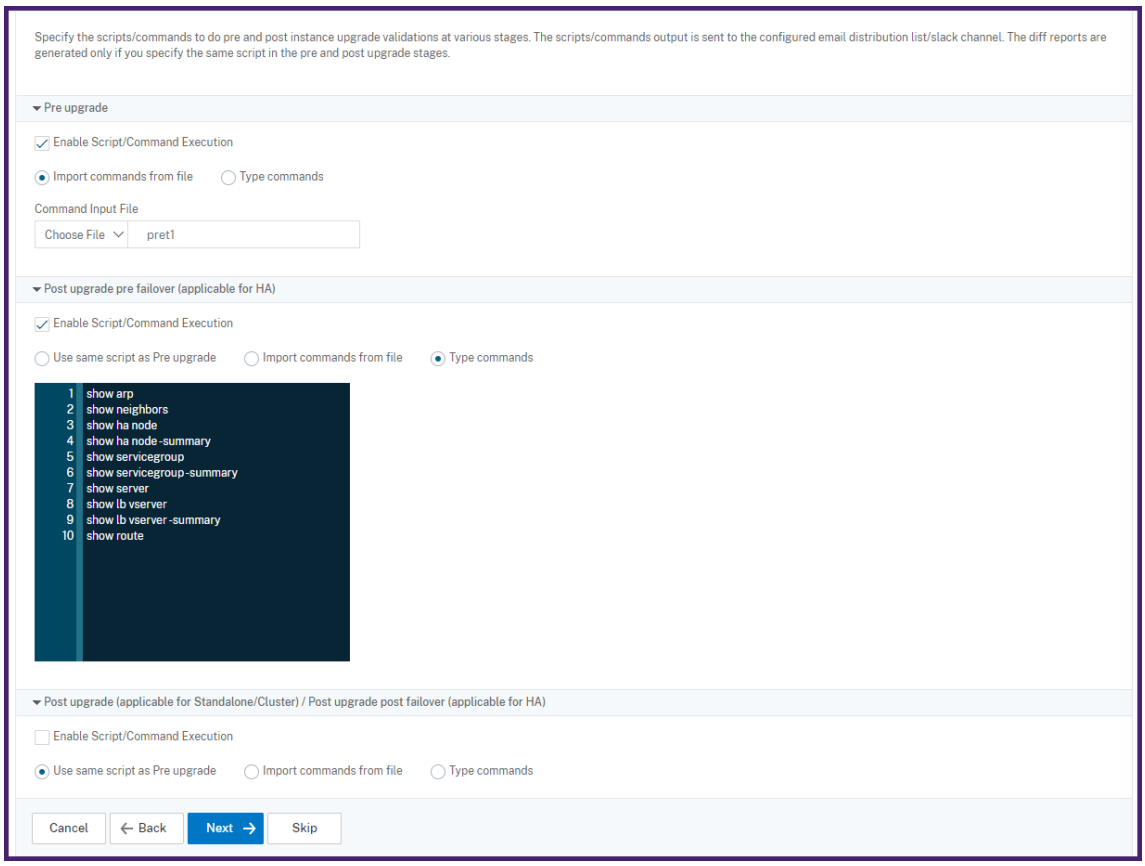
5. [**Next**] をクリックして、選択したインスタンスでアップグレード前の検証を開始します。

   [アップグレード前の検証] タブに、失敗したインスタンスが表示されます。障害が発生したインスタンスを削除し、[**Next**] をクリックします。

   > 重要:
   >
   > クラスター IP アドレスを指定した場合、ADM は、他のクラスターノードではなく、指定されたインスタンスでのみアップグレード前の検証を行います。

6. 必要に応じて、[カスタムスクリプト] で、インスタンスのアップグレードの前後に実行するスクリプトを指定します。次のコマンドを実行するには、次のいずれかの方法を使用します。

   - ファイルからコマンドをインポート -ローカルコンピュータからコマンド入力ファイルを選択します。
   - コマンドを入力 -GUI 上で直接コマンドを入力します。



カスタムスクリプトを使用して、インスタンスのアップグレードの前後に変更を確認できます。例:

- アップグレード前とアップグレード後のインスタンスのバージョン。
- アップグレード前後のインターフェイス、高可用性ノード、仮想サーバ、およびサービスのステータス。
- 仮想サーバーとサービスの統計。
- ダイナミックルート。

7. 「タスクのスケジュール」で、次のいずれかのオプションを選択します。

   - 今すぐアップグレード -アップグレードジョブはすぐに実行されます。
   - [後でスケジュール]: このアップグレードジョブを後で実行する場合は、このオプションを選択します。インスタンスをアップグレードする場合は、[実行日] と [開始時刻] を指定します。

     ADC HA ペアを 2 段階でアップグレードする場合は、[**HA** 内のノードに対して **2** 段階アップグレードを実行する] を選択します。

     HA ペアの別のインスタンスをアップグレードする場合は、[実行日] と [開始時刻] を指定します。

8. 「ジョブの作成」で、次の詳細を指定します。

   a) [ソフトウェアイメージ] リストから、次のいずれかのオプションを選択します。

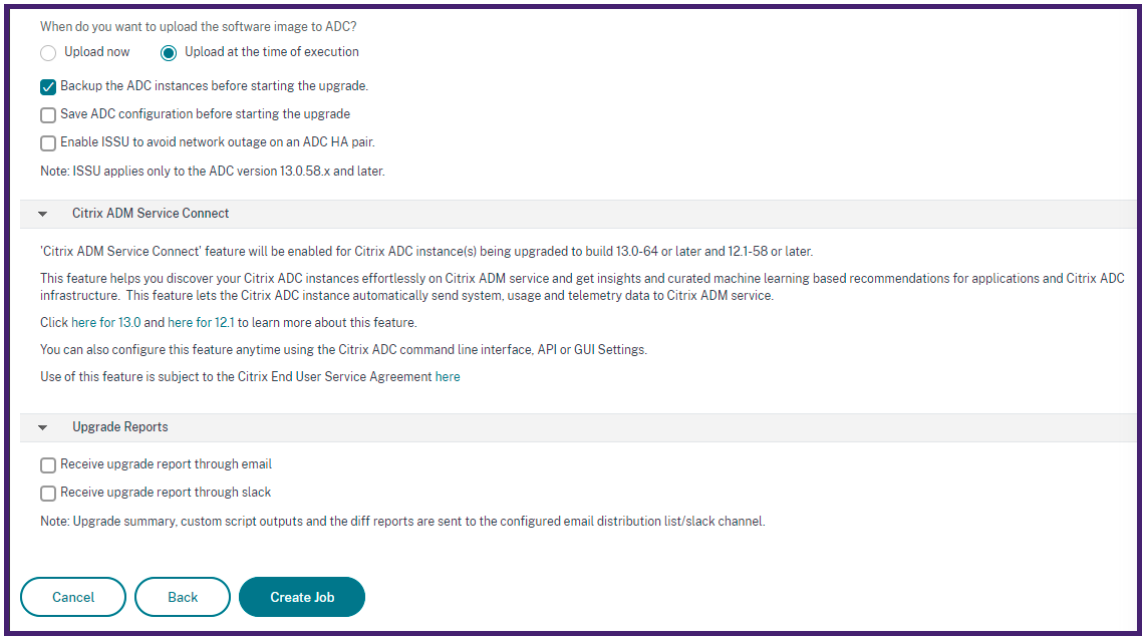
      - [Local]-ローカルマシンからインスタンスアップグレードファイルを選択します。

- アプライアンス -ADM ファイルブラウザからインスタンスアップグレードファイルを選択します。ADM GUI には、/var/mps/mps_imagesに存在するインスタンスファイルが表示されます。

b) イメージをインスタンスにアップロードするタイミングを指定します。

- 今すぐアップロード -画像をすぐにアップロードするには、このオプションを選択します。ただし、アップグレードジョブは、スケジュールされた時刻に実行されます。
- **[** 実行時にアップロード]-アップグレードジョブの実行時にイメージをアップロードするには、このオプションを選択します。

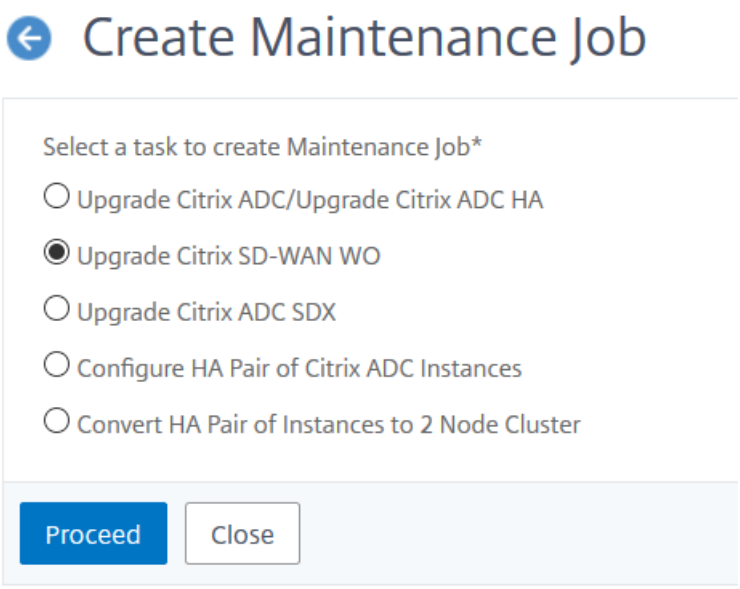
- アップグレードの成功時に **Citrix ADC** からソフトウェアイメージをクリーンアップ-インスタンスのアップグレード後に ADC インスタンスでアップロードされたイメージをクリアするには、このオプションを選択します。
- アップグレードを開始する前に、**ADC** インスタンスをバックアップしてください。：選択した ADC インスタンスのバックアップを作成します。
- **ISSU** を有効にして、**ADC HA** ペアでのネットワーク停止を回避する -ISSU は、ADC 高可用性ペアでのダウンタイムなしのアップグレードを保証します。このオプションは、アップグレード中に既存の接続を使用する移行機能を提供します。したがって、ダウンタイムなしで ADC HA ペアをアップグレードできます。ISSU 移行タイムアウトを分単位で指定します。
- 実行レポートを電子メールで受信する-実行レポートを電子メールで送信します。電子メール同報リストを追加するには、電子メール配布リストの作成を参照してください。
- **slack** による実行レポートの受信-実行レポートを slack で送信します。Slack プロファイルを追加するには、「Slack プロファイルの作成」を参照してください。



9. [ジョブの作成] をクリックします。

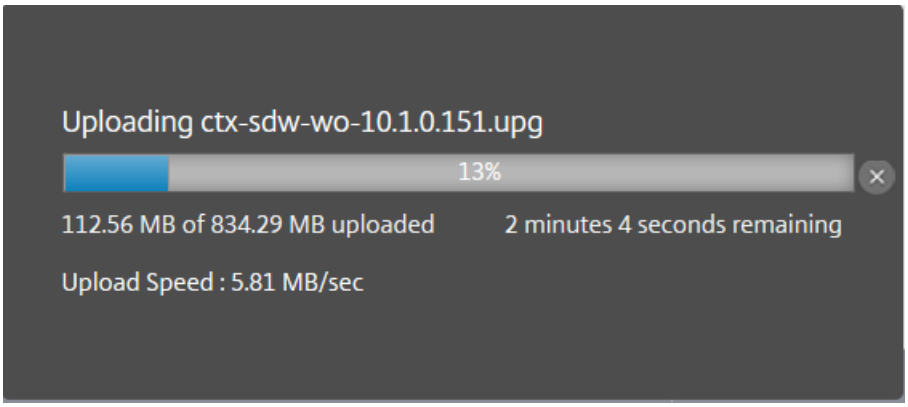
Citrix SD-WAN WO インスタンスのアップグレードのスケジュール設定

1. Citrix ADM で、［ネットワーク］> ［構成ジョブ］**>** ［メンテナンスジョブ ******］の順に選択します。**[**** ジョブの作成] ボタンをクリックします。
2. ［**Citrix SD-WAN WO** のアップグレード］を選択し、［続行］をクリックします。

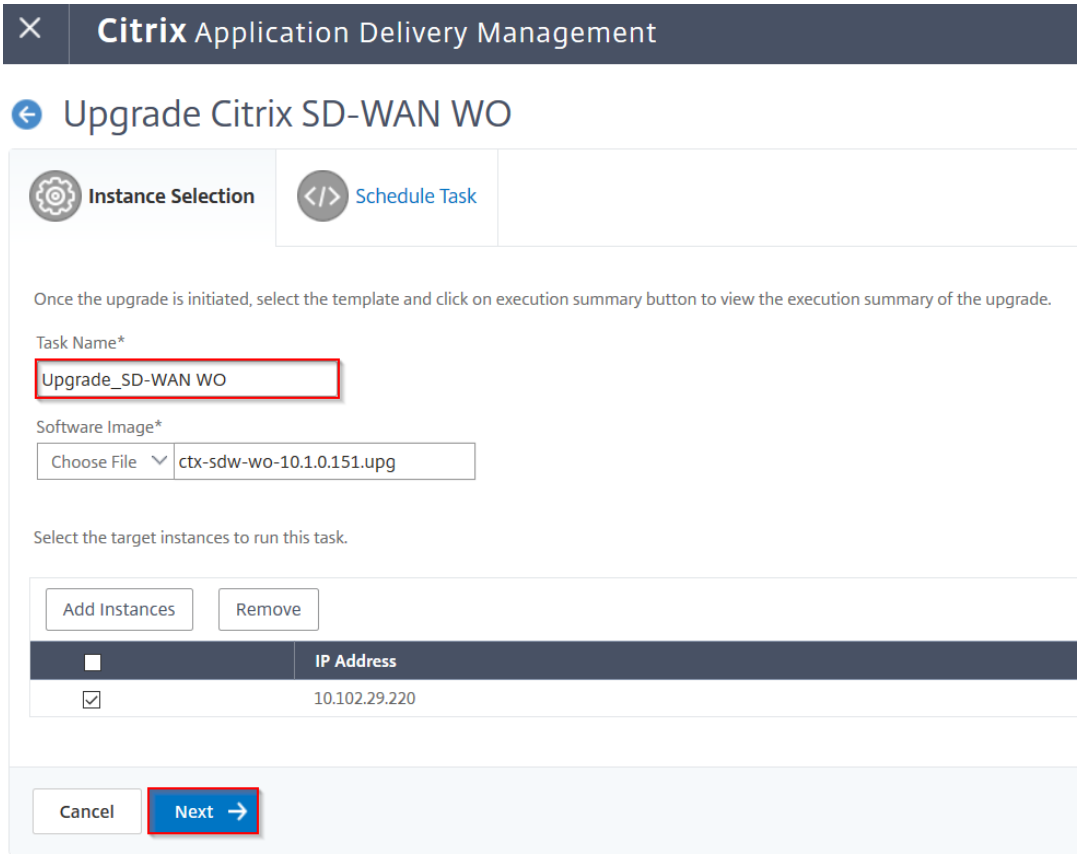


3. ［**Citrix SD-WAN WO** のアップグレード］ページの［インスタンスの選択］タブで、次の操作を行います。
   a) タスク名を追加します。
   b) ［ソフトウェアイメージ］ドロップダウンメニューから、［ローカル］（ローカルマシン）または［アプライアンス］（ビルドファイルが Citrix ADM 仮想アプライアンス上に存在している必要があります）を選択します。

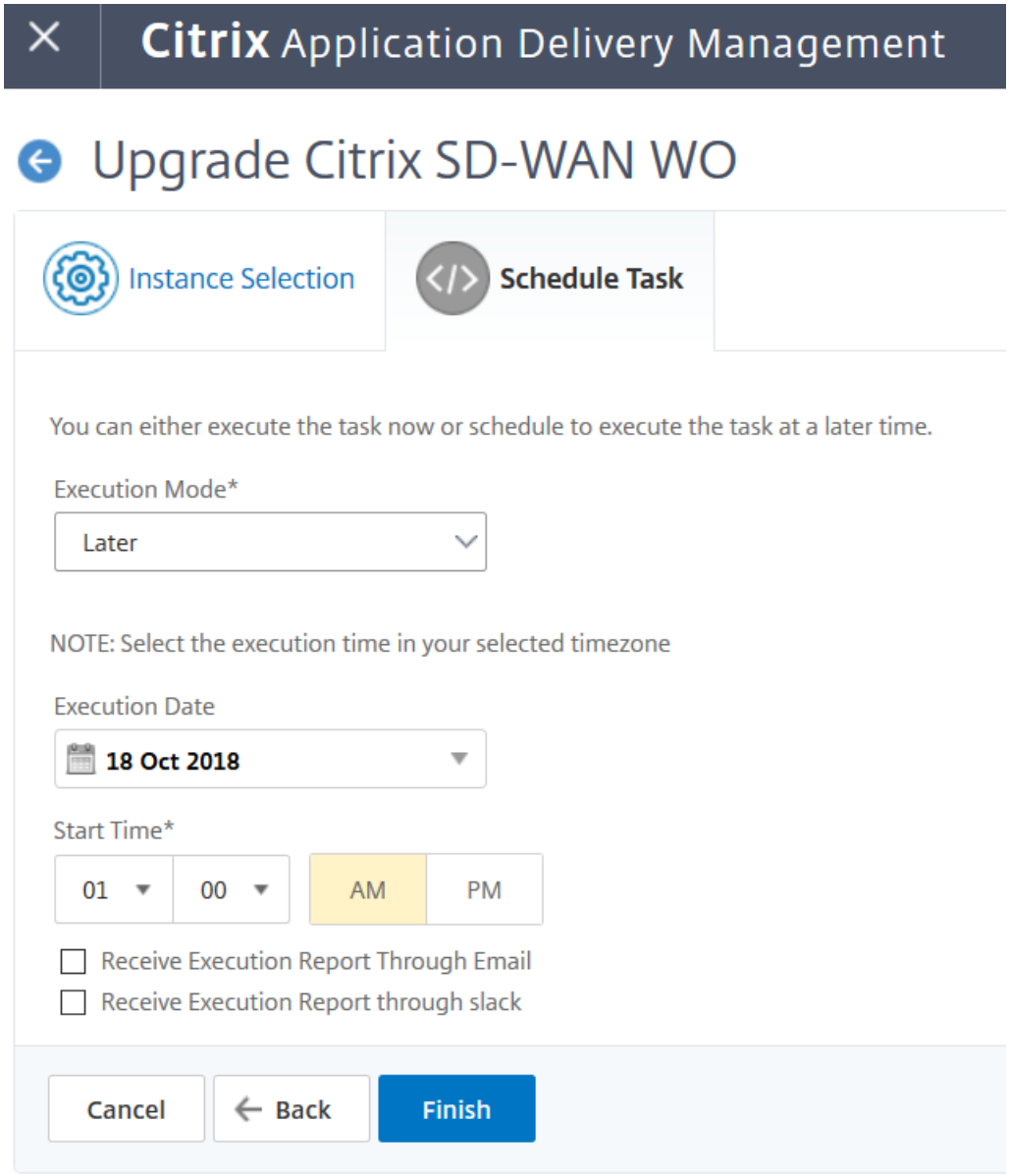
      アップロードプロセスが開始されます。



   c) ［インスタンスの追加］をクリックして、アップグレードプロセスを実行する Citrix SD-WAN WO インスタンスを追加します。
   d) ［次へ］をクリックします。



4. ［タスクのスケジュール設定］タブで、［実行モード］リストから［今すぐ実行］を選択し、Citrix SD-WAN WO インスタンスを今すぐアップグレードし、［完了］をクリックします。
5. Citrix ADC SD-WAN WO インスタンスを後でアップグレードするには、［実行モード］リストから［後で］を選択します。次に、Citrix ADC SD-WAN WO インスタンスをアップグレードするための実行日と開始時刻を選択し、［完了］をクリックします。

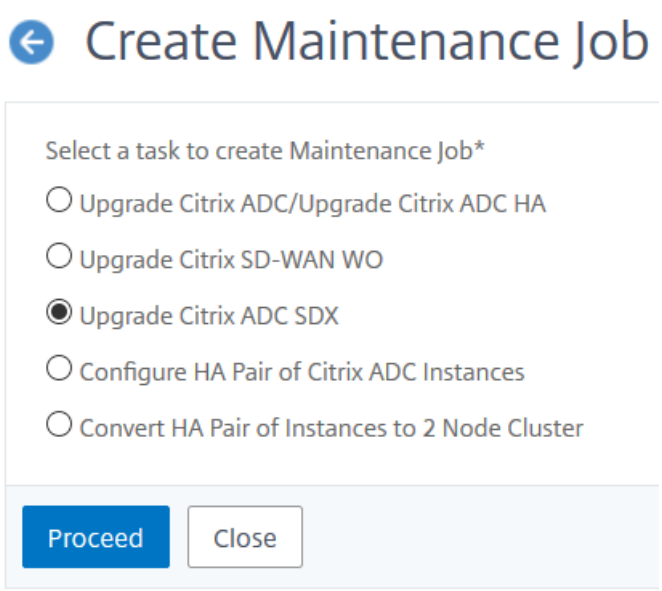


6. 電子メール通知と余裕期間の通知を有効にして、Citrix SD-WAN WO インスタンスのアップグレードの実行レポートを受信することもできます。通知を有効にするには、[電子メールによる実行レポートの受信] チェックボックスおよび **[Slack** による実行レポートの受信] チェックボックスをオンにします。

   電子メール配布リストと slack チャネルを構成する方法の詳細については、「Citrix ADC インスタンスのアップグレードをスケジュールする」の手順 **8** を参照してください。

Citrix ADC SDX インスタンスのアップグレードをスケジュールする

1. Citrix ADM で、［ネットワーク］ **>** ［構成ジョブ］ **>** ［メンテナンスジョブ］に移動します。[ジョブの作成] ボタンをクリックします。
2. ［**Citrix ADC SDX** のアップグレード］を選択し、［続行］をクリックします。

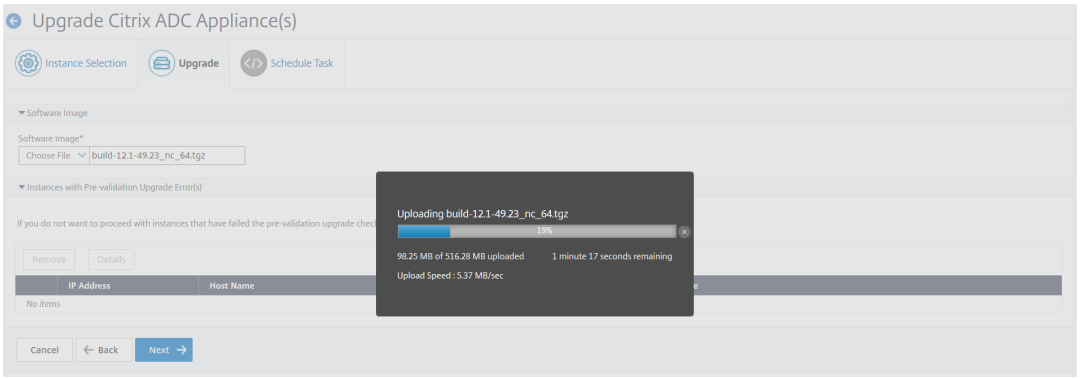


3. [**Citrix ADC SDX** のアップグレード] ページの [インスタンスの選択] タブで、次の操作を行います。

   a) タスク名を追加します。

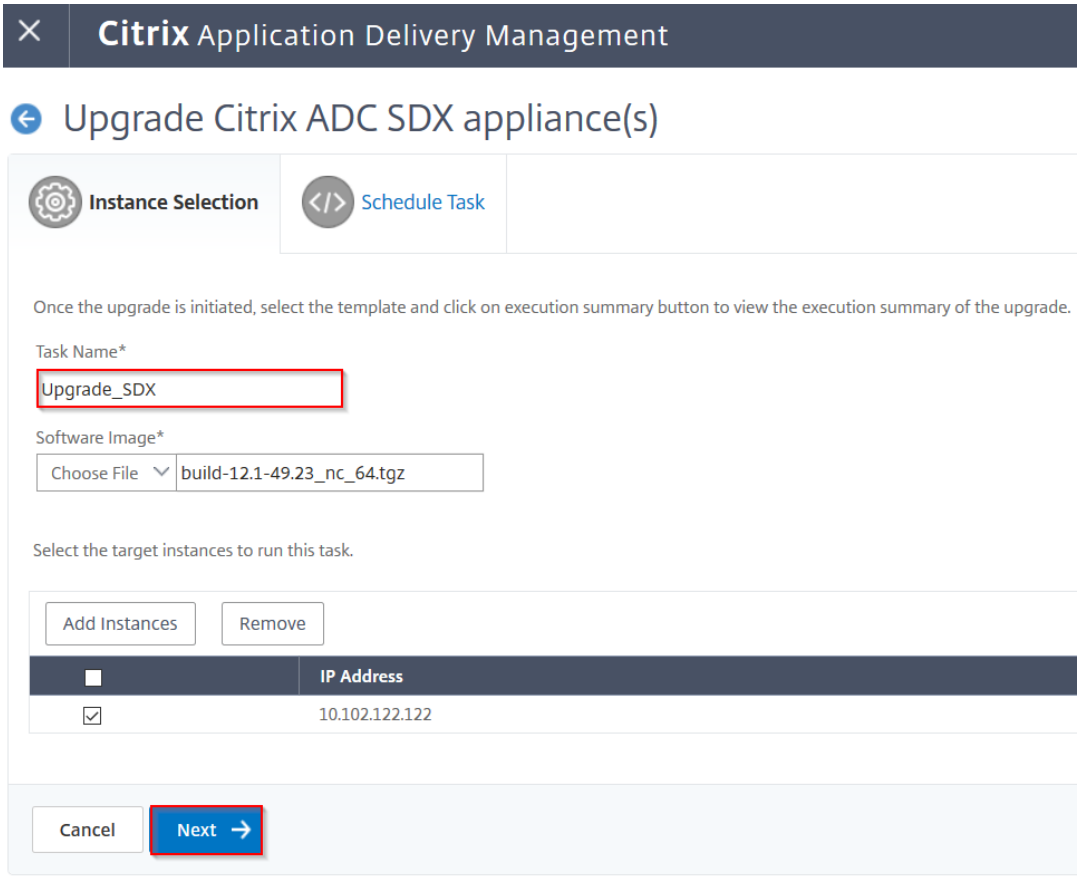
   b) [ソフトウェアイメージ] ドロップダウンメニューから、[ローカル] (ローカルマシン) または [アプライアンス] (ビルドファイルは Citrix ADM 仮想アプライアンス上に存在する必要があります) を選択します。

      アップロードプロセスが開始されます。

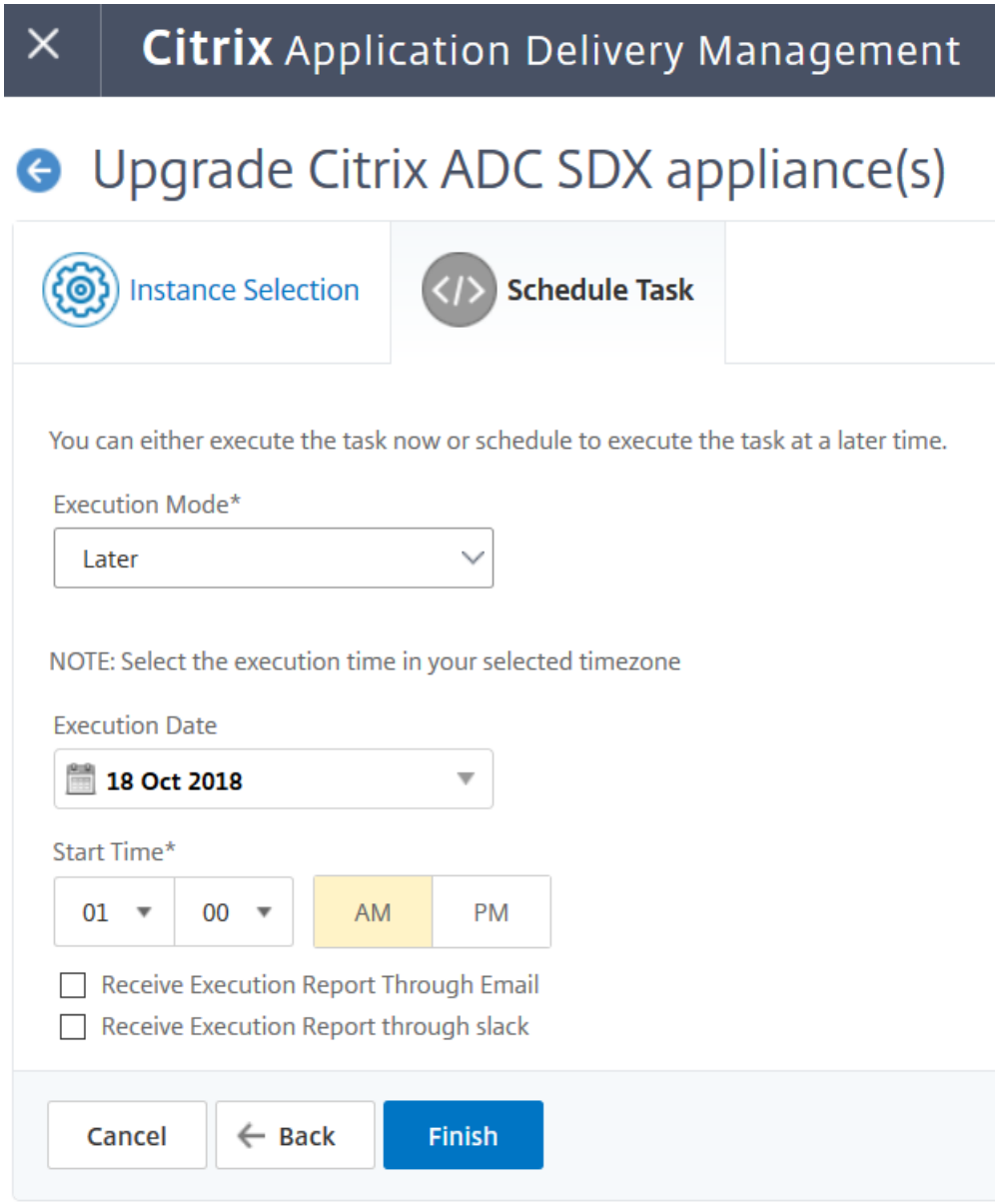


   c) アップグレードプロセスを実行する Citrix ADC SDX インスタンスを追加します。

   d) [次へ] をクリックします。



4. ［タスクのスケジュール設定］タブで、［実行モード］リストから［今すぐ実行］を選択し、Citrix SD-WAN WO インスタンスを今すぐアップグレードし、［完了］をクリックします。
5. Citrix ADC SDX インスタンスを後でアップグレードするには、［実行モード］リストから［後で］を選択します。次に、Citrix ADC SD-WAN WO インスタンスをアップグレードするための実行日と開始時刻を選択し、［完了］をクリックします。



6. また、アップグレード中の Citrix ADC SDX インスタンスの実行レポートを受信するために、電子メールおよび Slack 通知を有効にすることもできます。通知を有効にするには、[電子メールによる実行レポートの受信] チェックボックスおよび **[Slack** による実行レポートの受信] チェックボックスをオンにします。

   電子メール配布リストと slack チャネルを構成する方法の詳細については、「Citrix ADC インスタンスのアップグレードをスケジュールする」の手順 **8** を参照してください。

Autoscale グループのアップグレードをスケジュールする

Autosale グループの一部であるクラウドサービス内のすべてのインスタンスをアップグレードするには、以下の手順を実行します。

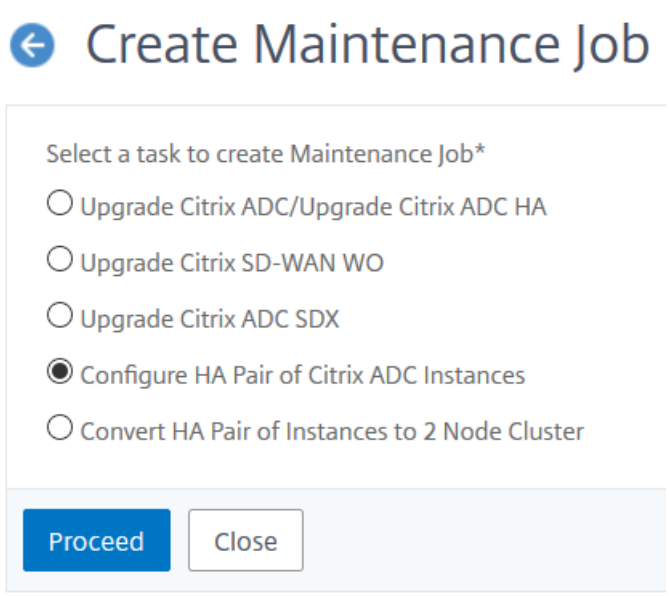
1. Citrix ADM で、[ネットワーク] **>** [構成ジョブ] **>** [メンテナンスジョブ] に移動します。[ジョブの作成] ボタンをクリックします。
2. [**AutoScale** グループをアップグレード] を選択し、[続行] をクリックします。
3. [アップグレード設定] タブで、次の操作を行います。
   a) アップグレードする **Autoscale** グループを選択します。
   b) [イメージ] で、Citrix ADC のバージョンを選択します。このイメージは、Autoscale グループ内の既存のバージョンの Citrix ADC インスタンスです。
   c) **Citrix ADC** イメージで、アップグレードする Citrix ADC バージョンファイルを参照します。

      [**Graceful Upgr**ade] をオンにすると、アップグレードタスクは指定されたドレイン接続期間が終了するまで待機します。
   d) [次へ] をクリックします。
4. [タスクのスケジュール] タブで、次の操作を行います。
   a)「実行モード」(Execution Mode) リストから次のいずれかを選択します。
      - 注：今すぐ Citrix ADC インスタンスを起動するには、すぐにアップグレードします。
      - 後で：後で Citrix ADC インスタンスのアップグレードを開始するには。
   b)「後で」オプションを選択した場合は、アップグレード・タスクを開始するときに「実行日」と「開始時刻」を選択します。

   電子メール通知と Slack 通知を有効にして、アップグレードする Autosale グループの実行レポートを受信することもできます。通知を有効にするには、[電子メールによる実行レポートの受信**]** チェックボックスおよび **[Slack** による実行レポートの受信] チェックボックスをオンにします。
5. [完了] をクリックします。

Citrix ADC インスタンスの **HA** ペアの構成をスケジュールする

1. Citrix ADM で、[ネットワーク] **>** [構成ジョブ] **>** [メンテナンスジョブ] に移動します。[ジョブの作成] ボタンをクリックします。
2. [**Citrix ADC** インスタンスの **HA** ペアの構成] を選択し、[続行] をクリックします。



3. [**Citrix ADC HA** ペア] ページの [インスタンスの選択] タブで、次の操作を行います。

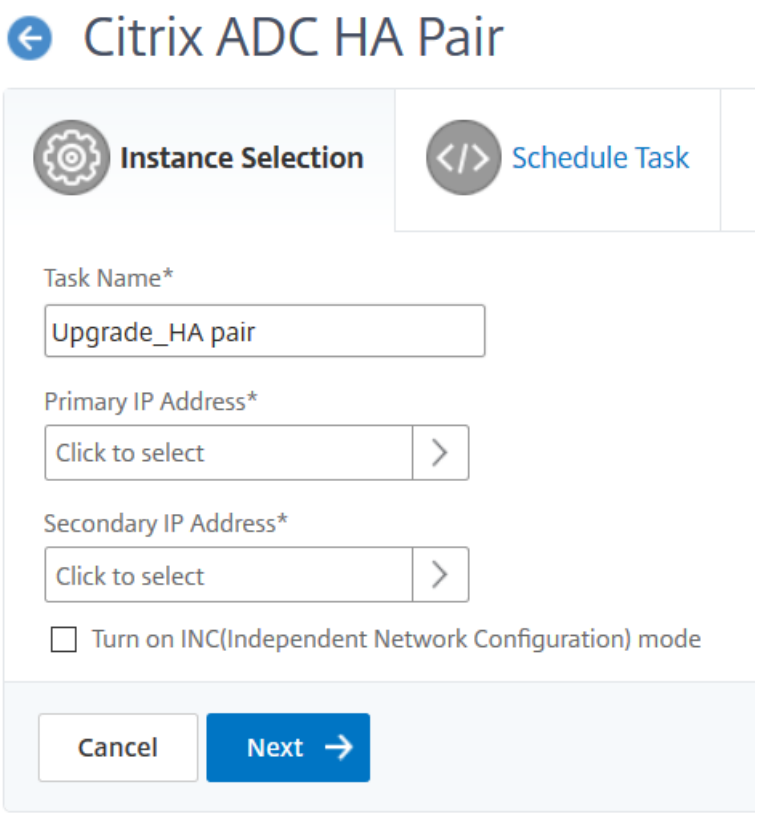
   a) タスク名を追加します。

   b) プライマリ IP アドレスを入力します。

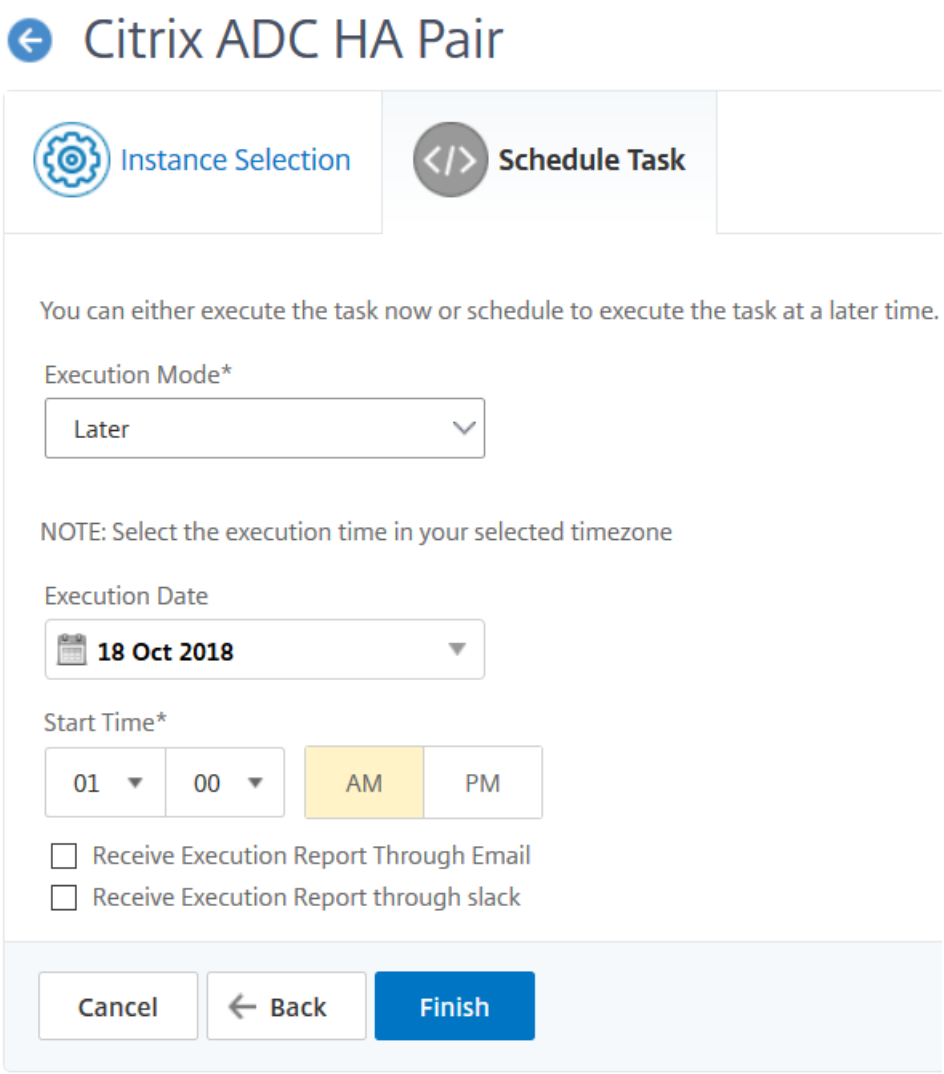
   c) セカンダリ IP アドレスを入力します。

   d) [次へ] をクリックします。

   e) 2 つのサブネットに **HA** ペアインスタンスがある場合は、**[INC (**独立ネットワーク構成**)** モードを有効にする] をクリックして有効にします。



4. ［タスクのスケジュール設定］タブで、［実行モード］リストから［今すぐ実行］を選択し、Citrix SD-WAN WO インスタンスを今すぐアップグレードし、［完了］をクリックします。
5. Citrix ADC HA ペアを後でアップグレードするには、［実行モード］リストから［後で］を選択します。次に、Citrix ADC SD-WAN WO インスタンスをアップグレードするための［実行日］と［開始時刻］を選択し、［完了］をクリックします。

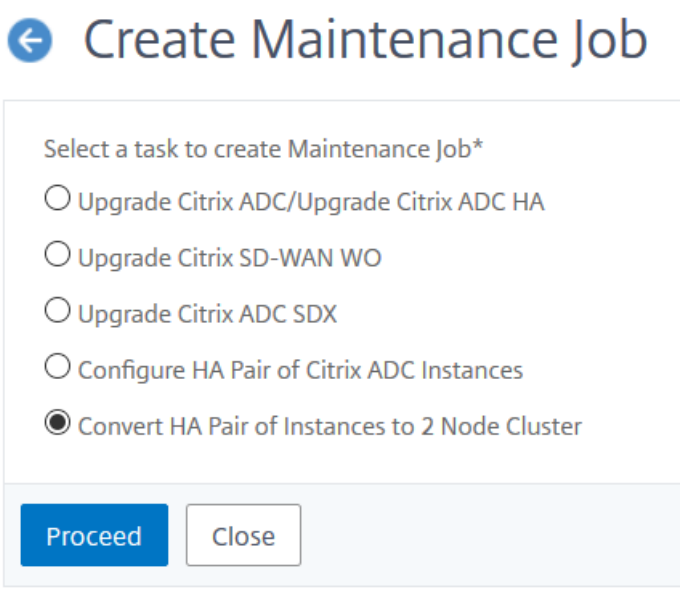


6. また、メール通知と Slack 通知を有効にして、ADC HA ペア作成の実行レポートを受信することもできます。通知を有効にするには、[電子メールによる実行レポートの受信] チェックボックスおよび **[Slack** による実行レポートの受信] チェックボックスをオンにします。

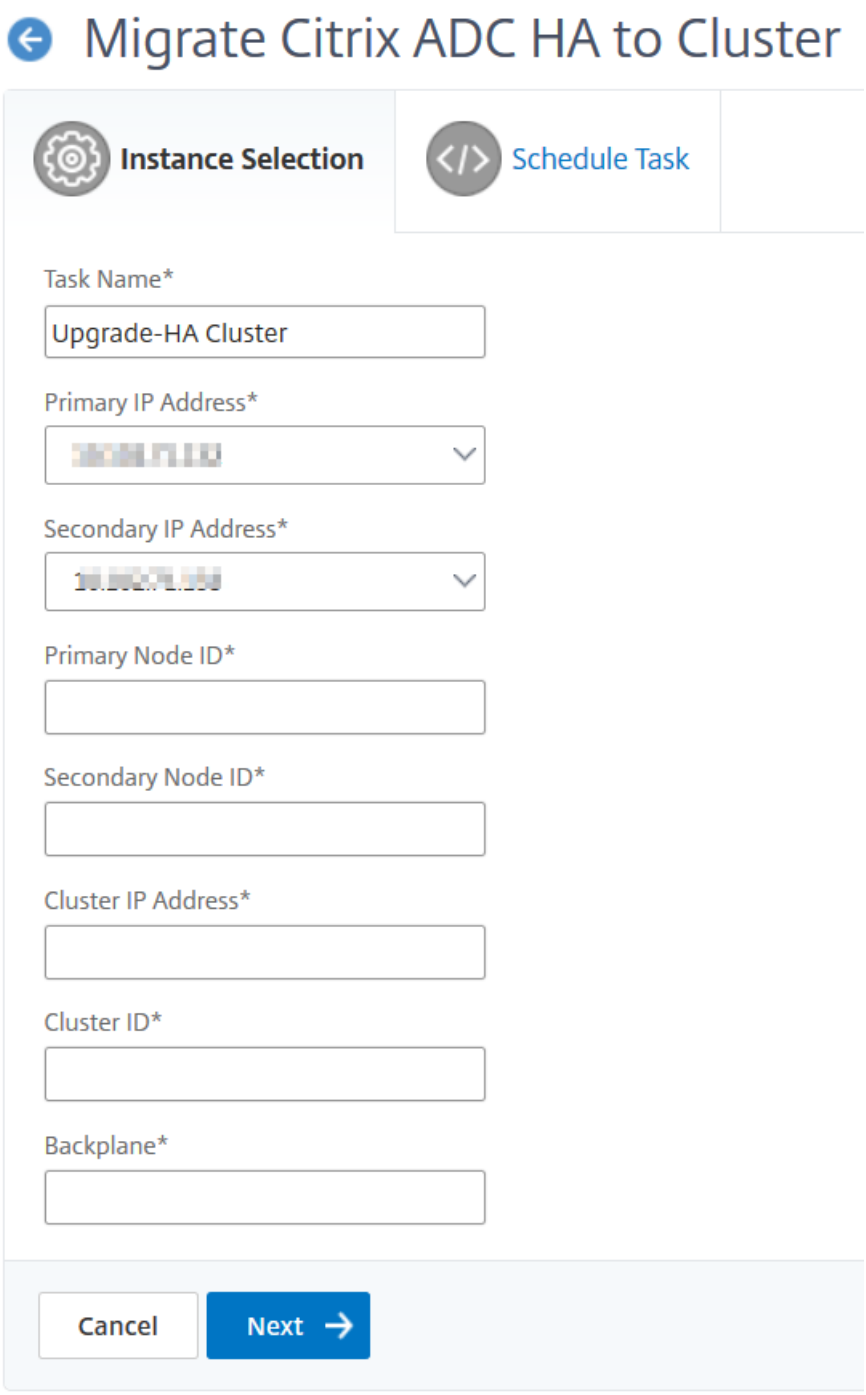
   電子メール配布リストと slack チャネルを構成する方法の詳細については、「Citrix ADC インスタンスのアップグレードをスケジュールする」の手順 **8** を参照してください。

インスタンスの **HA** ペアをクラスターに変換するスケジュールを設定する

1. Citrix ADM で、[ネットワーク] **>** [構成ジョブ] **>** [メンテナンスジョブ] に移動します。[ジョブの作成] ボタンをクリックします。
2. [**HA** インスタンスのペアを **2** ノードクラスタに変換] を選択し、[続行] をクリックします。



3. [**NetScaler HA** をクラスタに移行する] ページの [インスタンスの選択] タブで、タスク名を追加します。プライマリ IP アドレス、セカンダリ IP アドレス、プライマリノード ID、セカンダリノード ID、クラスタ IP アドレス、クラスタ ID、バックプレーンを指定し、[次へ] をクリックします。



4. ［タスクのスケジュール設定］タブで、［実行モード］リストから［今すぐ実行］を選択し、Citrix SD-WAN WO インスタンスを今すぐアップグレードし、［完了］をクリックします。
5. 後でアップグレードするには、[実行モード] リストから [後でアップグレード] を選択します。次に、Citrix ADC SD-WAN WO インスタンスをアップグレードするための［実行日］と［開始時刻］を選択し、［完了］をクリックします。
6. 電子メール通知と余裕期間の通知を有効にして、Citrix ADC SDX インスタンスのアップグレードの実行レポ

ートを受信することもできます。通知を有効にするには、[電子メールによる実行レポートの受信] チェックボックスおよび **[Slack** による実行レポートの受信] チェックボックスをオンにします。

電子メール配布リストと slack チャネルを構成する方法の詳細については、「Citrix ADC インスタンスのアップグレードをスケジュールする」の手順 **8** を参照してください。

構成監査

May 7, 2021

このドキュメントには、以下が含まれます。

- 監査テンプレートの作成
- 監査レポートの表示
- インスタンス間の設定変更の監査
- ネットワーク構成に関する設定アドバイスを取得
- Citrix ADM インスタンスの構成監査をポーリングする方法
- ConfigChange SNMP トラップの構成監査差分を生成

監査テンプレートの作成

May 7, 2021

ネットワークのパフォーマンスを最適化するため、特定の構成を特定のインスタンス上で実行する場合があります。また、管理対象の Citrix ADC インスタンス間の構成変更の監視、構成エラーのトラブルシューティング、および突然のシステムのシャットダウン後に保存されていない構成の回復も必要になります。特定のインスタンスで監査する特定の構成を持つ監査テンプレートを作成できます。Citrix Application Delivery Management（ADM）は、これらのインスタンスを監査テンプレートと比較し、構成に不一致がある場合はレポートします。構成の不一致がある場合、Citrix ADM は構成差分レポートを生成し、トラブルシューティングを行い、不要な構成変更を修正できます。

監査テンプレートの実行を自動化するには、

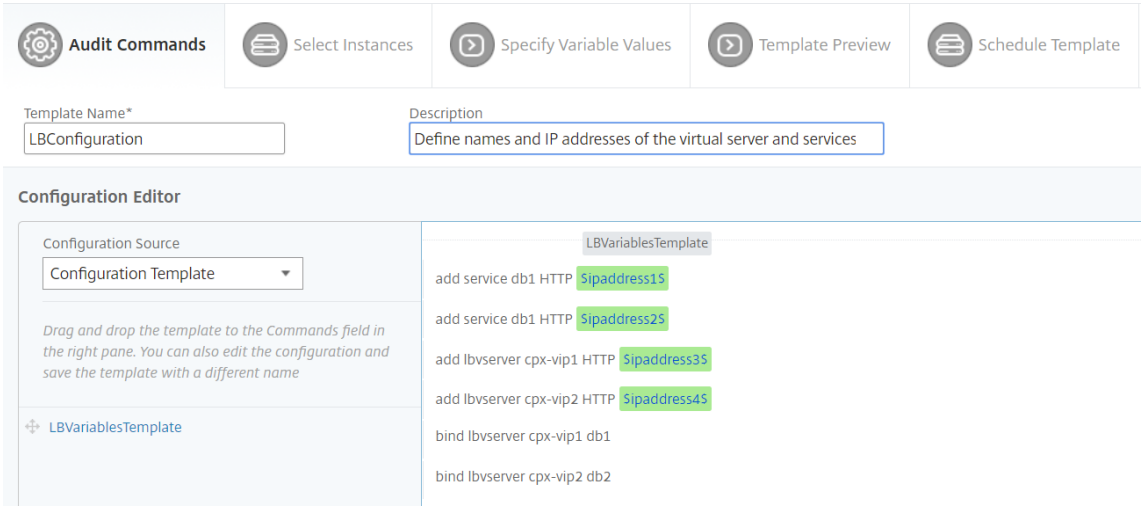
- テンプレートを実行する必要がある時刻をスケジュールする
- Citrix ADM がテンプレートを実行する必要がある頻度の設定。テンプレートは、毎日、週の特定の日、または月の特定の日に実行できます。

また、Citrix ADM によって生成された差分レポートを、構成可能な指定したメールアドレスに送信することもできます。このオプションを使用すると、ユーザーはレポートをメール添付ファイルとして受信できます。ユーザーが Citrix ADM にログオンしてレポートを手動でエクスポートする必要はありません。

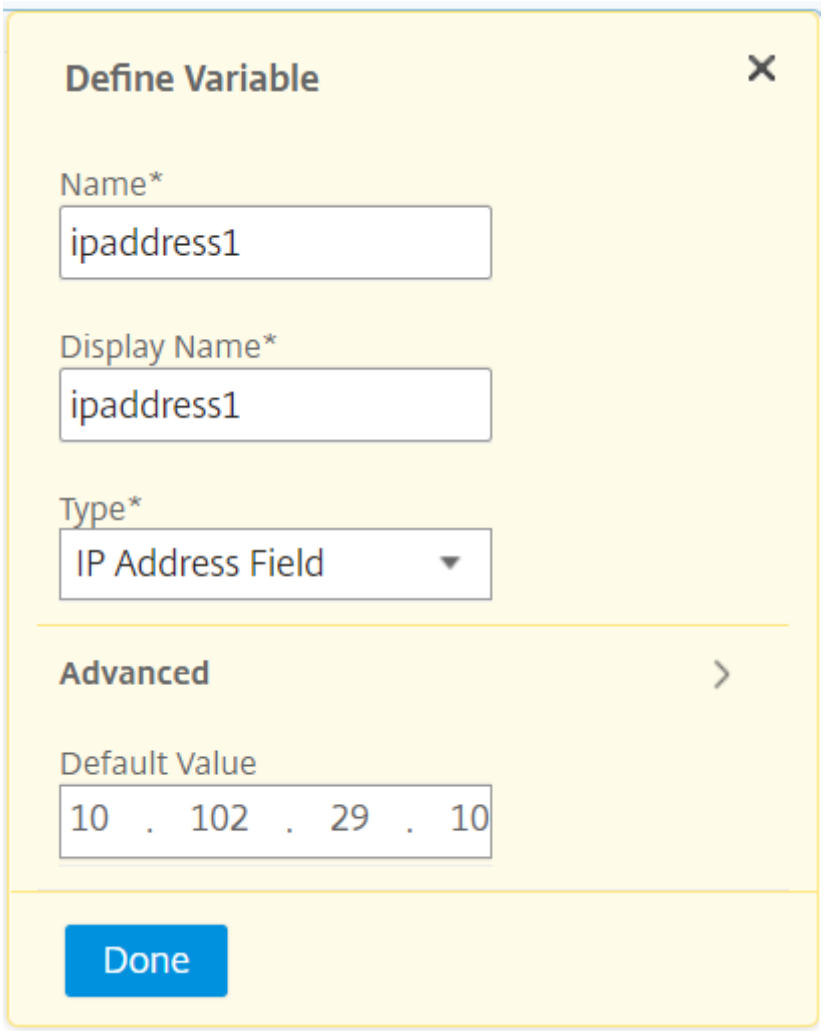
> 注:
> [名前の変更] オプションは、既定の構成テンプレートでは無効になっています。ただし、カスタム構成テンプレートの名前は変更できます。

監査テンプレートを作成するには、次の手順に従います。

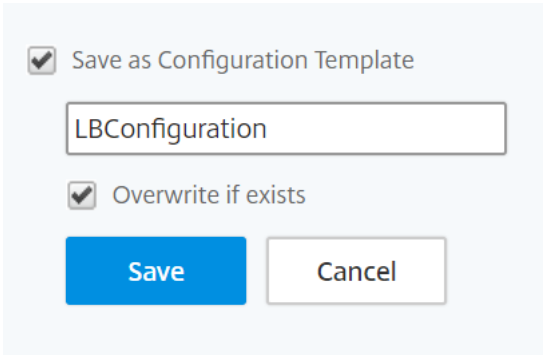
1. [ネットワーク] > [構成監査] > [監査テンプレート] に移動し、[追加] をクリックします。
2. [テンプレートの作成] ページと [監査コマンド] タブで、テンプレート名とその説明を指定します。
3. [構成エディタ] ページで、コマンドを入力し、コマンドを構成テンプレートとして保存します。既存のテンプレートを左ペインからエディタにドラッグすることもできます。
4. 変数に変換する値を選択し、[変数に変換] をクリックします。たとえば、負荷分散サーバー「ipaddress1」の IP アドレスを選択し、[変数に変換] をクリックします。下の図に示すように、変数は「$」で囲まれています。



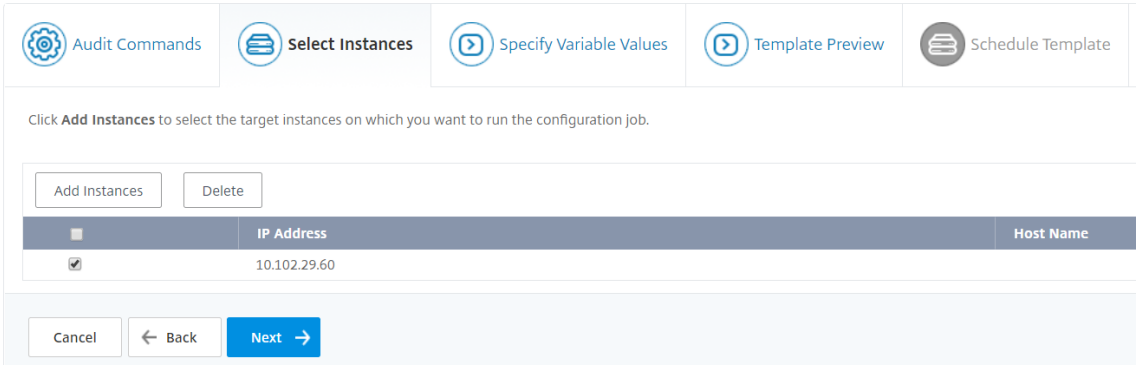
「変数の定義」(Define Variable) ウィンドウで、この変数のプロパティ (名前、表示名、変数のタイプ) を設定します。変数のデフォルト値をさらに指定する場合は、「詳細設定」(**Advanced**) オプションをクリックします。



コマンドを構成テンプレートとして保存することもできます。



5. [保存] をクリックし、[次へ] をクリックします。
6. [**Select Instances**] タブで、設定監査を実行するインスタンスを選択し、[**Next**] をクリックします。

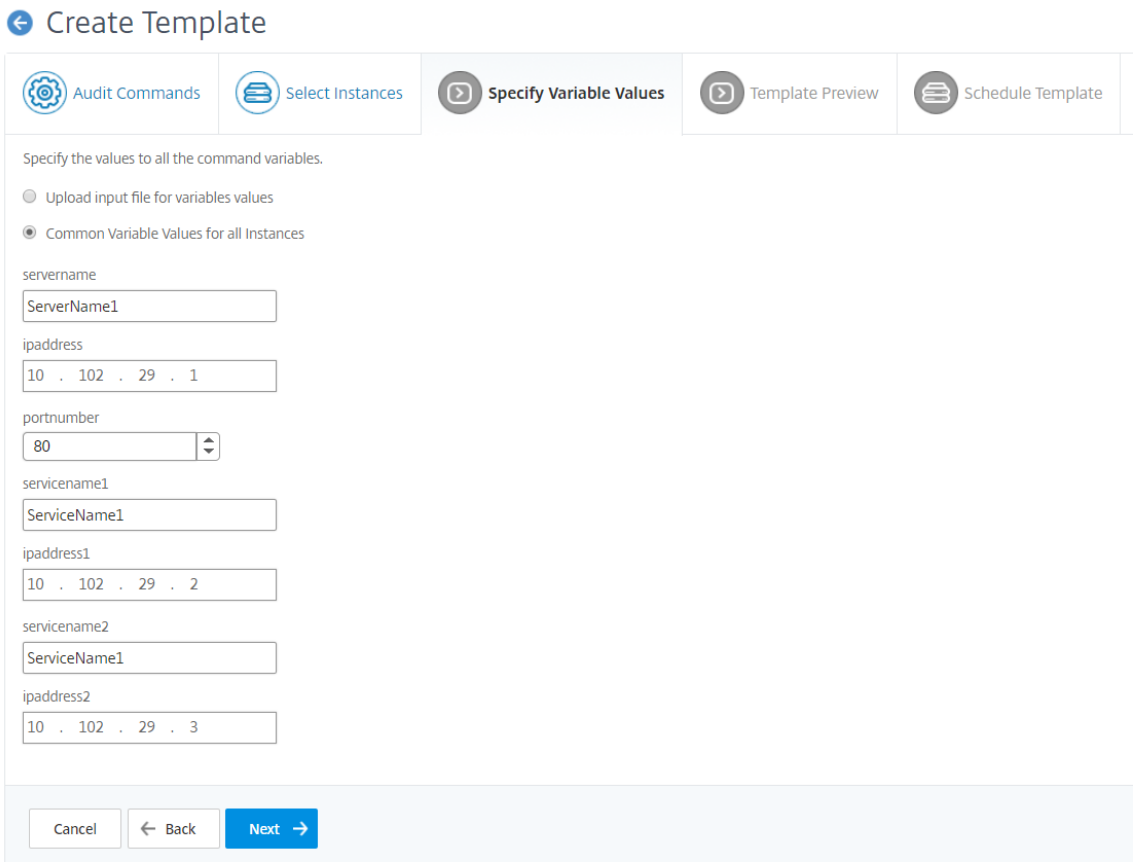


7.「変数値の指定」タブには、次の 2 つのオプションがあります。

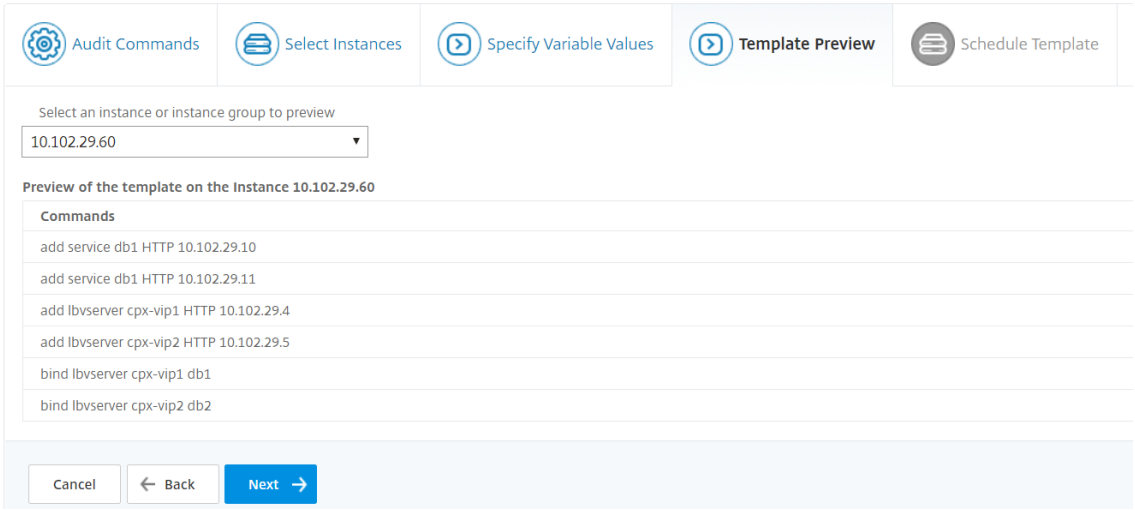
a) 入力ファイルをダウンロードして、コマンドで定義した変数の値を入力し、Citrix ADM サーバーにファイルをアップロードします。

b) すべてのインスタンスに定義した変数に共通の値を入力します。

8.［次へ］をクリックします。



9.［ **Template Preview** ］タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価および確認できます。［次へ］をクリックします。



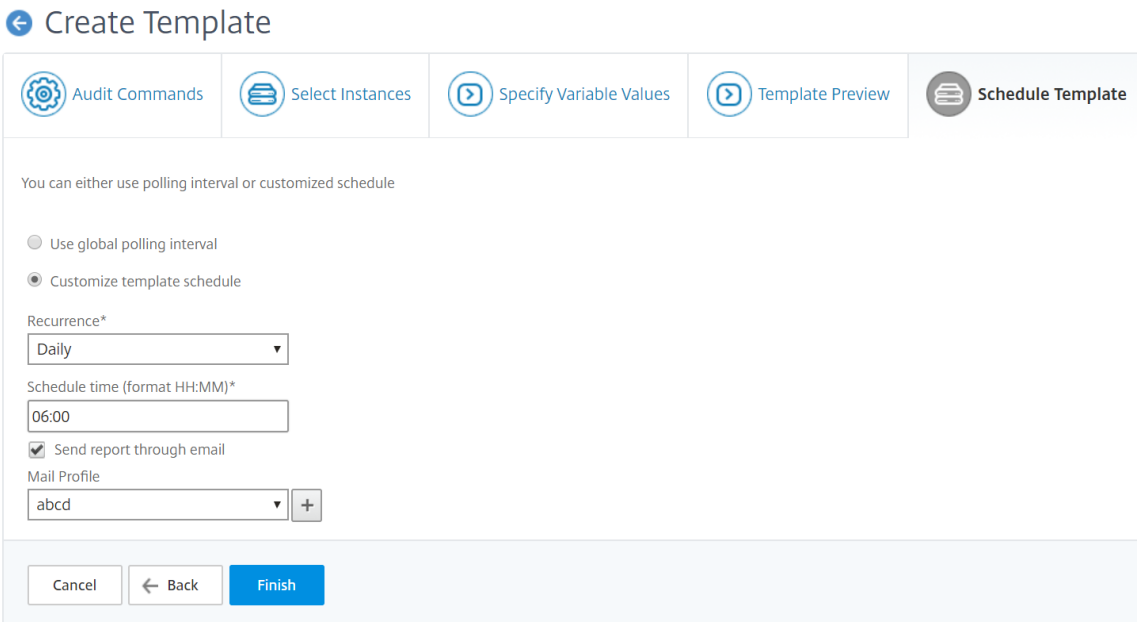
10. [**Schedule Template**] タブには、テンプレートの実行をスケジュールし、差分レポートを送信するようにメールアドレスを設定する次のオプションがあります。

    - グローバルポーリング間隔を使用します。Citrix ADM でグローバルに構成されたインスタンスでテンプレートを一度に実行するには、このオプションを選択します。

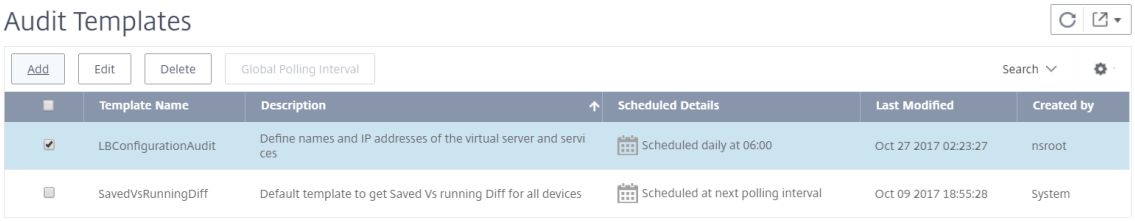
      > 注:
      >
      > Citrix ADM でグローバルポーリング間隔を構成するには、[ネットワーク] > [構成監査] > [監査テンプレート] の順に選択し、[グローバルポーリング間隔] をクリックします。[ポーリング間隔] フィールドに、Citrix ADM がインスタンスをグローバルにポーリングする必要がある分を入力します。

    - テンプレート集計表をカスタマイズします。このオプションを使用して、テンプレートを実行する必要がある時間と頻度を設定します。
    - レポートを電子メールで送信する。このオプションを使用して、差分レポートの送信先となるメールプロファイルをメール添付ファイルとして構成します。

11. [完了] をクリックします。



監査テンプレートは [**Audit Templates**] リストに表示され、指定されたインスタンスの設定に対してスケジュールされた時刻に実行されます。



Citrix ADC インスタンスの構成監査をポーリングする

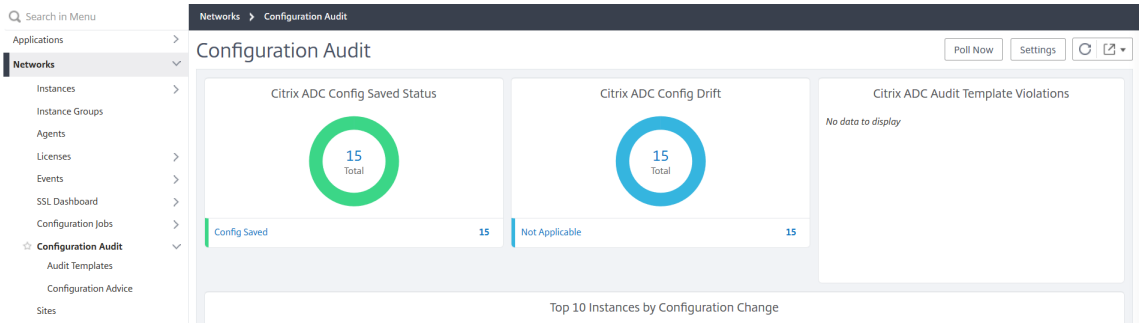
May 7, 2021

Citrix Application Delivery Management（ADM）は、10 時間ごとに構成監査を自動的にポーリングし、Citrix ADC インスタンスで発生する構成の変更を探します。構成監査を手動でポーリングして最近の変更を検出することもできますが、すべての Citrix ADC インスタンスの構成をポーリングすると、ネットワークに大きな負荷がかかります。

Citrix ADC インスタンス構成監査全体をポーリングする代わりに、選択したインスタンスの構成監査のみを手動でポーリングできます。

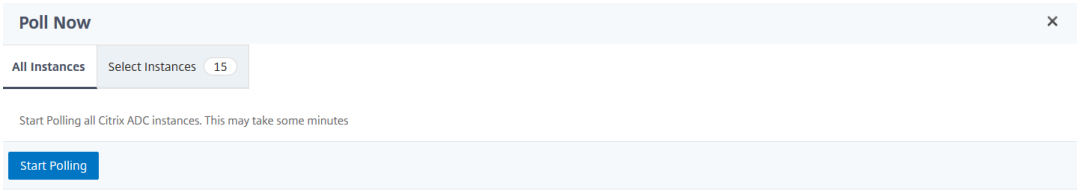
Citrix ADC インスタンスの構成監査をポーリングするには:

1. Citrix ADM で、［ネットワーク］ > ［構成監査］に移動します。
2. [構成の監査] ページの右上隅にある [今すぐポーリングする] をクリックします。

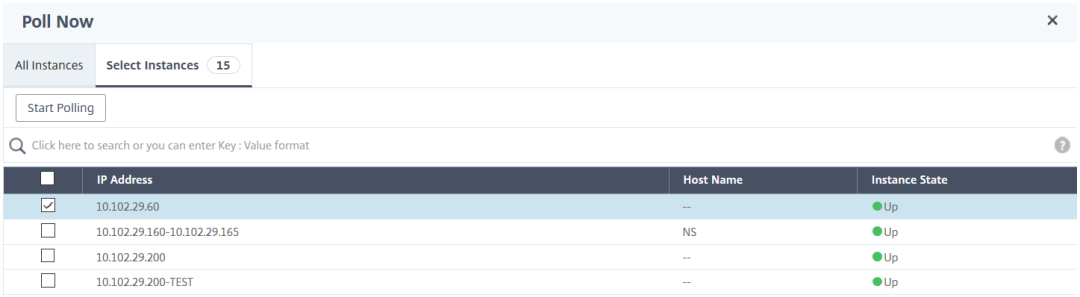


3. [**Poll Now**] ページが表示され、ネットワーク内のすべての Citrix ADC インスタンスをポーリングするか、選択したインスタンスをポーリングするかを選択できます。

   a) すべての Citrix ADC インスタンスをポーリングするには、[すべてのインスタンス] タブを選択し、[ポーリング開始] をクリックします。



   b) 特定のインスタンスをポーリングするには、[Select **Instances**] タブを選択し、リストからインスタンスを選択し、[**Start Polling**] をクリックします。



監査レポートの表示

May 7, 2021

Citrix Application Delivery Management（ADM）では、構成監査セクションで構成監査差分レポートを表示およびダウンロードできます。[Configuration Audit] セクションでは、すべてのインスタンスおよびインスタンスごとにサマリーレポートをエクスポートできます。また、インスタンステンプレートペアごとに詳細な差分レポートをエクスポートすることもできます。

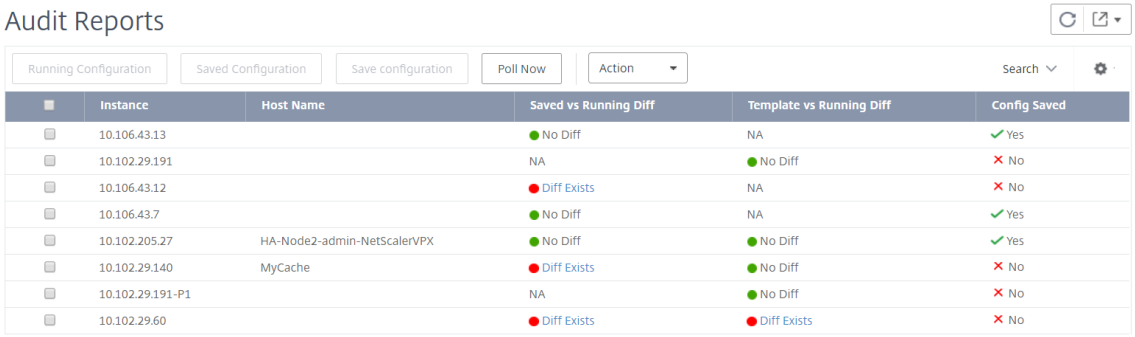
[Audit Templates] リストに表示される監査テンプレートは、指定したインスタンスの設定に対してスケジュールされた時刻に実行されます。[構成監査] ダッシュボードの [**Citrix ADC Config Drift**] グラフには、保存されていない構成に対して保存された構成の変更に関する詳細な情報が表示されます。[**Citrix ADC** 構成ドリフトグラフ]

をクリックすると、［監査レポート］ページに［差分が存在する］と［相違なし］の両方を示すインスタンスのリストが表示されます。Citrix ADM によって表示される差分レポートをダウンロードできます。

Citrix ADM では、差分のレポートの自動エクスポートをメール添付ファイルとしてスケジュールするオプションも用意されています。レポートのエクスポートをスケジュールする方法については、監査テンプレートの作成を参照してください。

構成監査レポートのエクスポート

1. Citrix ADM で、［ネットワーク］>［構成監査］に移動します。
2. ［構成監査］ページで、**Citrix ADC** の構成ドリフトグラフ内をクリックします。
3. 「監査レポート」ページには、相違があるインスタンスが一覧表示されます。このページには、構成実行に違いがないインスタンスのリストも表示されます。

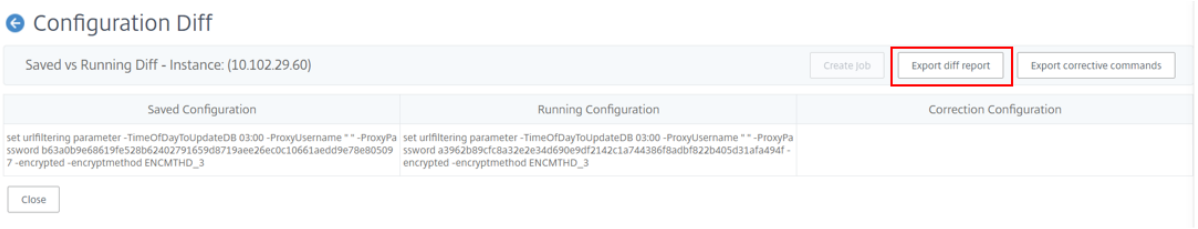


画像では、一部のインスタンスでは差分が 保存済みと実行差分にのみ存在し、一部のインスタンスでは差分がテンプレートと実行差分にのみ存在することがわかります。場合によっては、保存された差分と実行差分とテンプレートと実行差分の両方に違いがあります。

保存された対実行中の差分**:**

インスタンスに保存された設定と、そのインスタンスで現在実行中の設定との相違のレポートを表示できます。たとえば、[保存された差分と実行中の差分] の下のインスタンスの **[**相違が存在する**]** をクリックします。

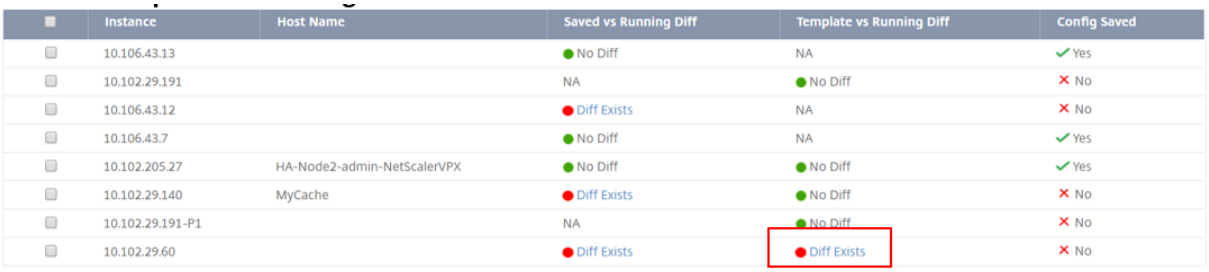
ここでは、そのインスタンスの構成実行差分に対する、保存された構成のレポートを確認できます。



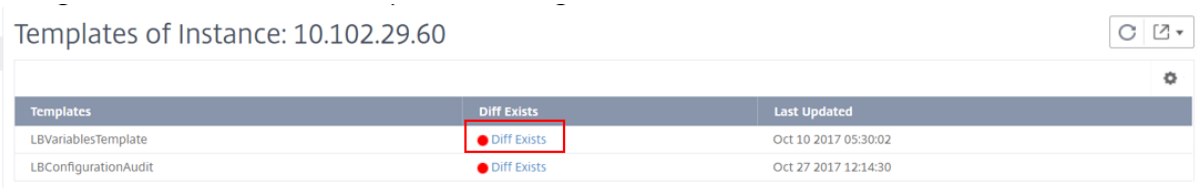
[差分レポートのエクスポート] をクリックして、差分レポートの.csv ファイルをダウンロードします。[修正コマンドのエクスポート] をクリックして、コマンドを.txt ファイルにエクスポートすることもできます。その後、関連する Citrix ADC インスタンス上で構成ジョブからコマンドを実行して、そのインスタンスの構成を修正できます。

テンプレートと実行差分**:**

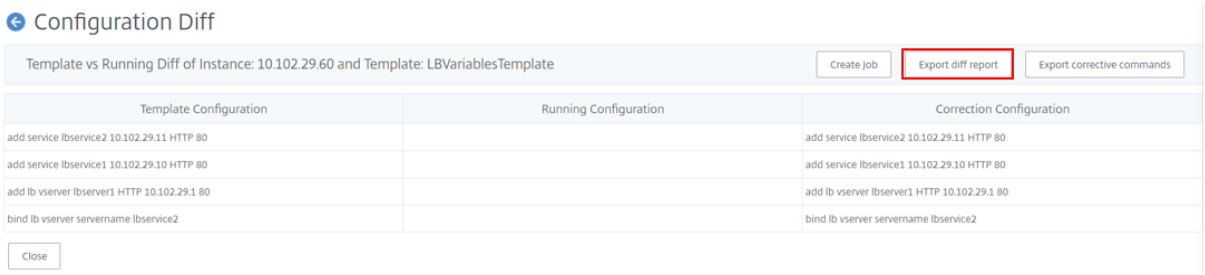
テンプレートと実行差分には、デフォルトのテンプレートである 保存済みと実行差分以外のすべてのテンプレートが含まれます。テンプレートと構成実行の間に存在する違いを表示できます。たとえば、「テンプレート」と「実行中差分」のインスタンスの 1 つに対して「差分」をクリックします。



これで、2 つのテンプレートに差分が表示され、Citrix ADC インスタンスの構成がテンプレートが探しているものとは異なる構成になっていることがわかります。



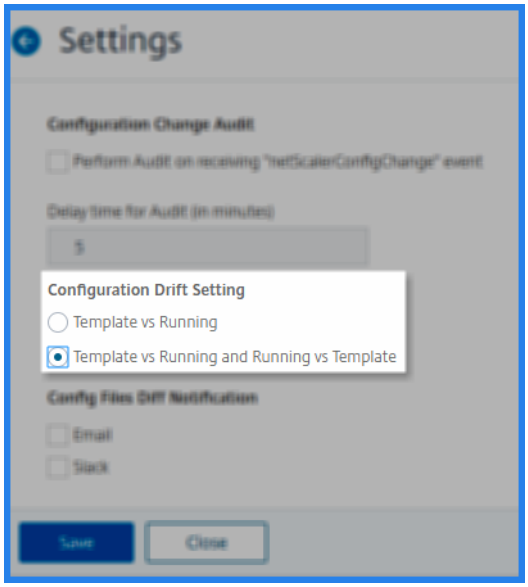
もう一度 [相違が存在する] をクリックします。次の図は、テンプレートが検索する設定と、そのようなコマンドが設定されていないか、削除されていないため、ブランクの構成実行を示しています。また、修正設定や、設定を修正するために実行するコマンドも表示されます。



また、テンプレートと実行と実行とテンプレートのドリフト設定を使用して、両方の方法で設定を比較することもできます。

- 監査テンプレート設定と、インスタンスの実行設定を比較します。
- インスタンスの構成実行と監査テンプレートを比較します。

デフォルトでは、[テンプレート] と [実行中のドリフト] の設定が選択されています。ドリフト設定を変更するには、ADM GUI から、[構成監査] ページで [設定] を選択します。



[差分レポートのエクスポート] をクリックして、差分レポートの.csv ファイルをダウンロードします。[修正コマンドのエクスポート] をクリックして、コマンドを.txt ファイルにエクスポートすることもできます。その後、CLI でコマンドを実行して、そのインスタンスの設定を修正できます。

次の図は、システムにダウンロードされる.csv diff ファイルの例を示しています。

#Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate		
Template Configuration	Running Configuration	Correction Configuration
add service lbservice2 10.102.29.11 HTTP 80		add service lbservice2 10.102.29.11 HTTP 80
add service lbservice1 10.102.29.10 HTTP 80		add service lbservice1 10.102.29.10 HTTP 80
add lb vserver lbserver1 HTTP 10.102.29.1 80		add lb vserver lbserver1 HTTP 10.102.29.1 80
bind lb vserver servername lbservice2		bind lb vserver servername lbservice2

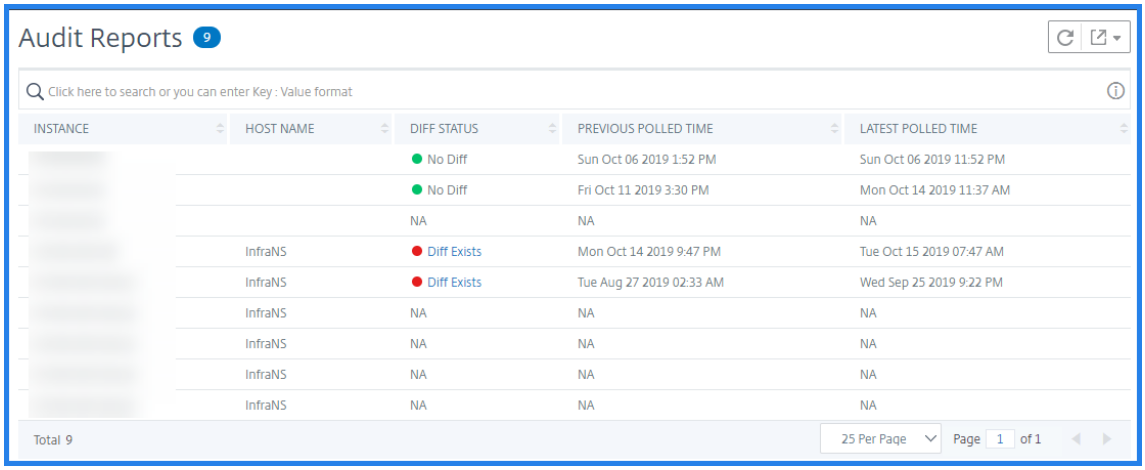
ファイルステータス監査レポートの表示

Citrix ADC ファイルの状態グラフを使用して、`nsconfig` フォルダ内のファイルが追加、変更、または削除されているかどうかを監視できます。たとえば、ADC インスタンスでライセンス・ファイルが更新された場合、このファイルが最後に更新された日時を確認し、適切なアクションを実行できます。

Citrix ADC インスタンスのファイルステータス監査レポートをエクスポートするには:

1. Citrix ADM で、［ネットワーク］>［構成監査］に移動します。
2. ［構成監査］ページで、［**Citrix ADC** ファイルステータス］グラフ内をクリックします。

   「監査レポート」ページには、「差分」ステータスのインスタンスが一覧表示されます。



差分ステータスは、前回のポーリング時刻から最新のポーリング時刻 ** までの間隔について計算されます。相違ステータスは ** 、次のいずれかになります。

- 差分 **exist** s-このステータスは、[前回のポーリング時間] 以降に、インスタンスの nsconfigフォルダ内でファイルが変更されたことを示します。ファイルの変更内容を表示するには、「相違が存在する」をクリックします。

  ![差分がnsconfigフォルダに存在する] (/en-us/citrix-application-delivery-management-service/media/config-audit-file-status-diff.png)

- 相違なし -このステータスは、前回のポーリング時刻以降、nsconfig フォルダ内のファイルが変更されていないことを示します。

- **NA** -このステータスは、ファイルのステータスの監視対象外であることを示します。このステータスは、Citrix ADM がインスタンスをポーリングしない場合に表示されます。たとえば、インスタンスが新しく追加された場合、またはインスタンスの状態が非アクティブの場合、インスタンスのポーリングは行われません。

このダッシュボードのレポートをエクスポートする

このページのレポートをエクスポートするには、このページの右上にある エクスポートアイコンをクリックします。[エクスポート] ページでは、次のいずれかの操作を実行できます。

1. [今すぐエクスポート] タブを選択します。レポートを PDF、JPEG、PNG、または CSV 形式で表示して保存します。
2. [スケジュールエクスポート] タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、電子メールまたは余裕メッセージでレポートを送信する。

> 注
>
> - [毎週の繰り返し] を選択した場合は、レポートをスケジュールする平日を選択してください。
> - [毎月の繰り返し] を選択した場合は、レポートをスケジュールするすべての日をカンマで区切って入力

> します。

構成変更 **SNMP** トラップの構成監査差分を生成

May 7, 2021

ネットワーク内の Citrix ADC インスタンスの構成が変更されると、構成ファイルが更新されます。インスタンスは、ConfigChange SNMP トラップを Citrix Application Delivery Management（ADM）に送信します。インスタンスが ConfigChange SNMP トラップを送信するときに、そのインスタンスに対して Citrix ADM で構成監査を実行するように設定できます。

監査テンプレート設定と構成実行の間に相違がある場合は、「監査レポート」(Audit Report) ページに「差分」(Diff Exist s) ステータスメッセージが表示されます。「相違の出口」リンクをクリックすると、「構成の差分」ページが表示され、修正コマンドを表示できます。これらの修正コマンドを使用して、構成ジョブを作成し、特定の Citrix ADC インスタンスで実行できます。設定ジョブを実行すると、インスタンスは目的の設定に戻ります。修正コマンドから構成ジョブを作成する方法について詳しくは、Citrix ADM で修正コマンドから構成ジョブを作成する方法を参照してください。

ConfigChange SNMP トラップの受信時に構成監査テンプレートを実行するには、次の手順に従います。

Citrix ADM では、Citrix ADM で構成監査テンプレートを実行するオプションを有効にできます。

1. Citrix ADM で、［ネットワーク］>［構成監査］に移動します。
2. [構成の監査] ページで [設定] をクリックします。
3.「構成変更の監査設定」セクションの編集アイコンをクリックします。
4. ［**NetScalerConfigChange** イベントを受信したときに構成監査を行う］チェックボックスをオンにします。

   > 注**:**
   >
   > これはすべてのインスタンスのグローバル設定です。Citrix ADM は、今後 NetScalerConfigChange SNMP トラップを受信するすべてのインスタンスに対して構成監査を実行します。

5. [監査テンプレートの実行時間 **(**分**)**] フィールドに、分を入力します。Citrix ADM は、そのインスタンスによって ConfigChange SNMP トラップを受信すると、この時間が経過すると、Citrix ADC インスタンス上で構成監査テンプレートを実行します。

インスタンス間の設定変更の監査

May 7, 2021

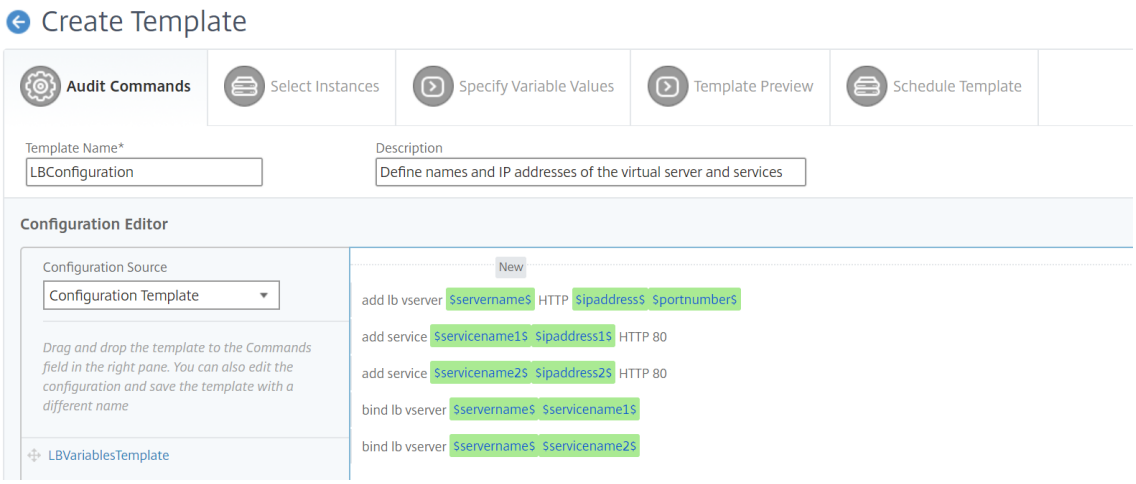
ネットワークのパフォーマンスを最適化するため、特定の構成を特定のインスタンス上で実行する場合があります。また、管理対象の Citrix ADC インスタンス間の構成変更の監視、構成エラーのトラブルシューティング、および突然

のシステムのシャットダウン後に保存されていない構成の回復も必要になります。特定のインスタンスで実行する特定の設定を使用して、監査テンプレートを作成できます。Citrix Application Delivery Management（ADM）は、これらのインスタンスを監査テンプレートと比較し、構成に不一致がある場合はレポートします。この比較により、エラーのトラブルシューティングと修正を行うことができます。

テンプレートを実行する必要がある時間をスケジュールすることで、監査テンプレートの実行を自動化できます。Citrix ADM がテンプレートを実行する必要がある頻度を設定することもできます。テンプレートは、毎日、週の特定の日、または月の特定の日に実行できます。Citrix ADM によって生成された差分レポートを、構成可能な指定された電子メールアドレスに送信することもできます。このオプションを選択すると、ユーザーはレポートをメール添付ファイルとして受信します。ユーザーが Citrix ADM にログオンしてレポートを手動で確認する必要はありません。

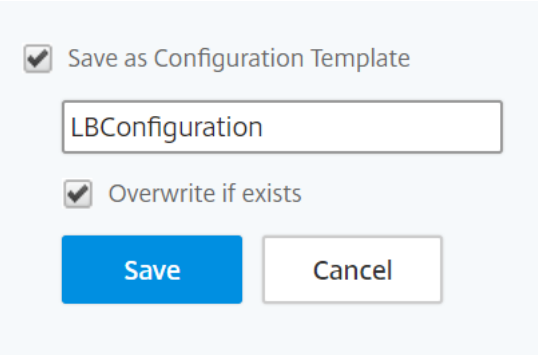
監査テンプレートを作成するには、次の手順に従います。

1. [ネットワーク] > [構成監査] > [監査テンプレート] に移動し、[追加] をクリックします。
2. [テンプレートの作成] ページと [監査コマンド] タブで、テンプレート名とその説明を指定します。
3. 構成エディタでコマンドを入力し、構成テンプレートとしてコマンドを保存します。エディタの左ペインから既存のテンプレートをドラッグすることもできます。
4. 変数に変換する値を選択し、[変数に変換] をクリックします。たとえば、次の図に示すように、負荷分散サーバー`ipaddress`の IP アドレスを選択し、[変数に変換] をクリックします。

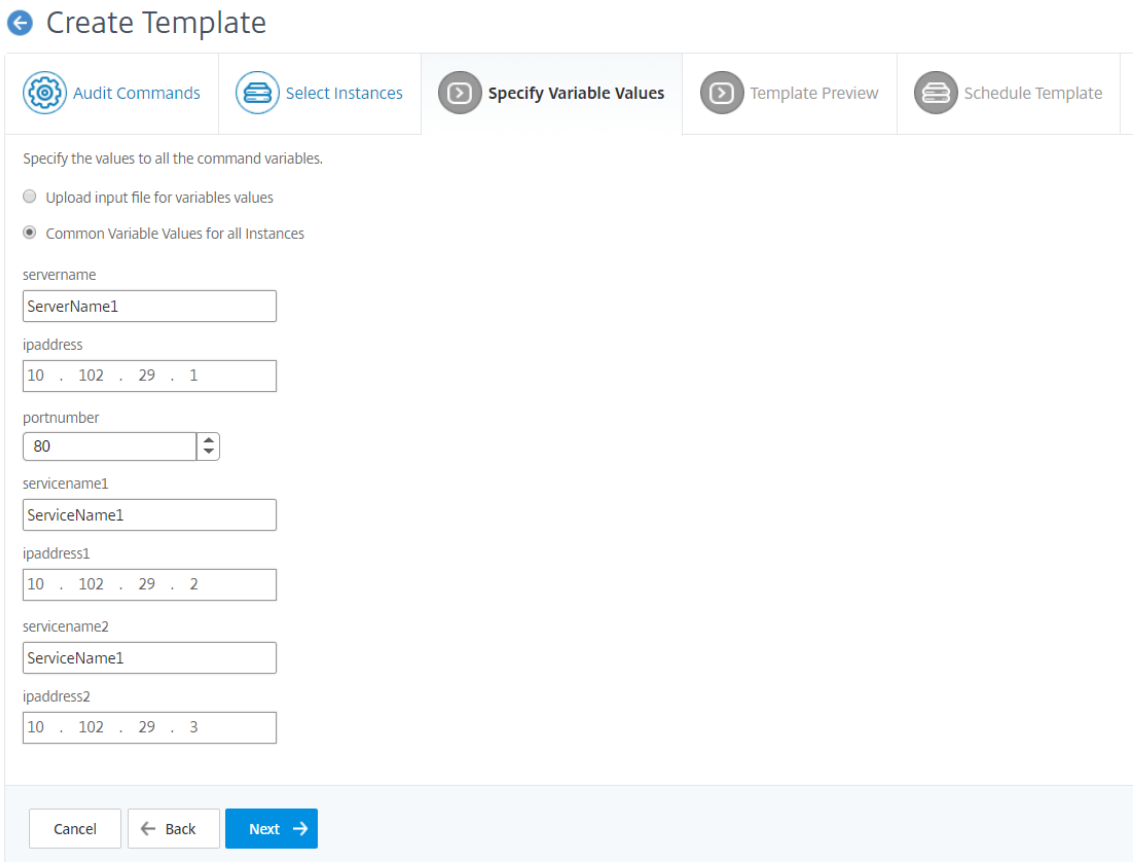


変数のデフォルト値をさらに指定する場合は、「詳細設定」(**Advanced**) オプションをクリックします。

コマンドを構成テンプレートとして保存することもできます。



5. [保存] をクリックし、[次へ] をクリックします。
6. [**Select Instanc** es] タブで、設定監査を実行するインスタンスを選択します。
7. 「変数値の指定」タブには、次の 2 つのオプションがあります。
   a) 入力ファイルをダウンロードして、コマンドで定義した変数の値を入力し、Citrix ADM サーバーにファイルをアップロードします。
   b) すべてのインスタンスに定義した変数に共通の値を入力します。
8. [次へ] をクリックします。



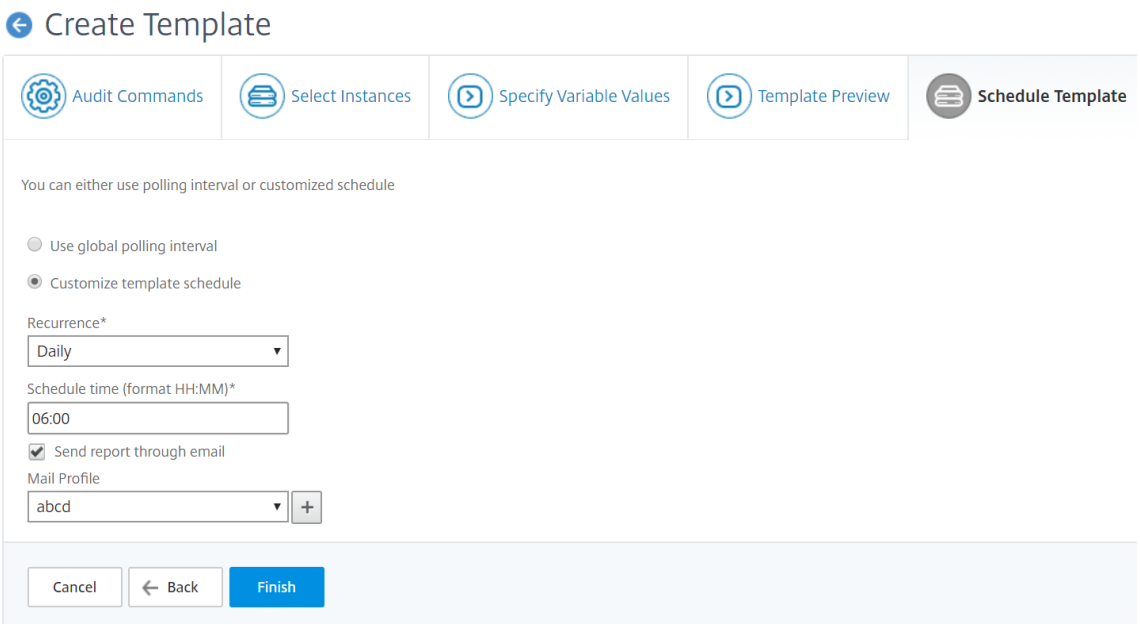
9. [**Template Preview**] タブでは、各インスタンスまたはインスタンスグループで実行するコマンドを評価

および確認できます。［次へ］をクリックします。

10. [**Schedule Template**] タブには、テンプレートの実行を自動化する 3 つのオプションと、差分レポートを送信するためのメールアドレスがあります。

    - グローバルポーリング間隔を使用します。Citrix ADM でグローバルに構成されたインスタンスで一度にテンプレートを実行するには、このオプションを選択します。
    - テンプレート集計表をカスタマイズします。このオプションを使用して、テンプレートを実行する必要がある時刻と頻度を設定します。
    - 電子メールでレポートを送信します。このオプションを使用して、差分レポートの送信先となるメールプロファイルをメール添付ファイルとして構成します。

11. ［完了］をクリックします。

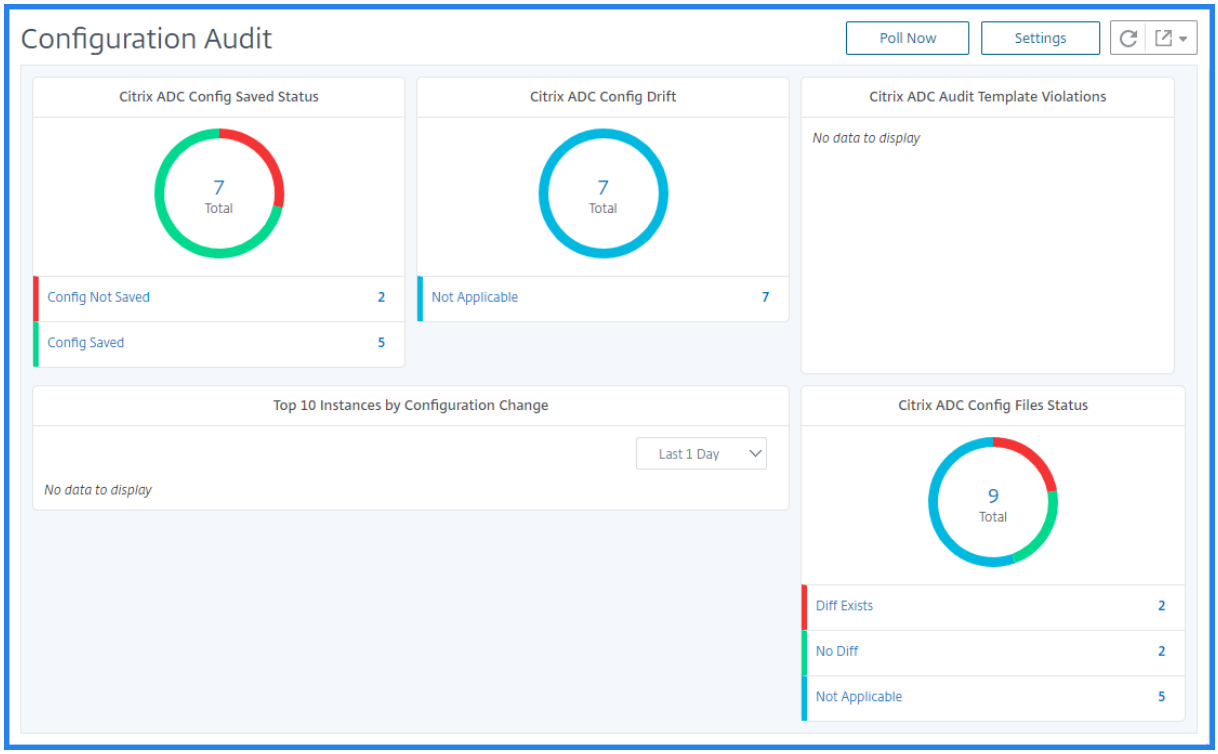


監査テンプレートが [Audit Templates] リストに表示され、指定したインスタンスの設定に対してスケジュールされた時刻に実行されます。

設定変更の詳細の表示

「構成監査」ダッシュボードを使用して、次のような構成変更に関する高度な詳細を表示することもできます。

- 構成変更による上位 10 個のインスタンス
- 保存済みおよび未保存の構成の数
- `nsconfig` フォルダ内で追加、削除、または変更されたファイル

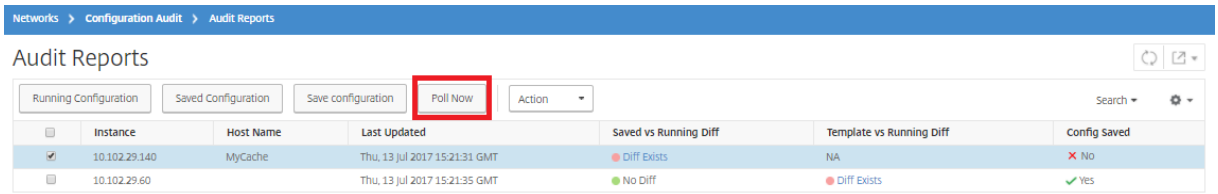


また、Citrix ADM では、構成監査を手動でポーリングし、インスタンスのすべての構成監査を直ちに Citrix ADM に追加します。これを行うには、［ネットワーク］>［構成監査］の順に選択し、［今すぐポーリング］をクリックします。ポップアップページの［今すぐポーリング］には、ネットワーク内のすべての Citrix ADC インスタンスをポーリングするか、選択したインスタンスをポーリングするオプションがあります。

特定のインスタンスに対して監査を強制することもできます。これを行うには、次のグラフのいずれかをクリックします。

- **Citrix ADC** 構成保存ステータス
- **Citrix ADC** コンフィグドリフト

[**Audit Reports**] ページで、インスタンスを選択し、[**Action**] リストで [**Poll Now**] を選択します。

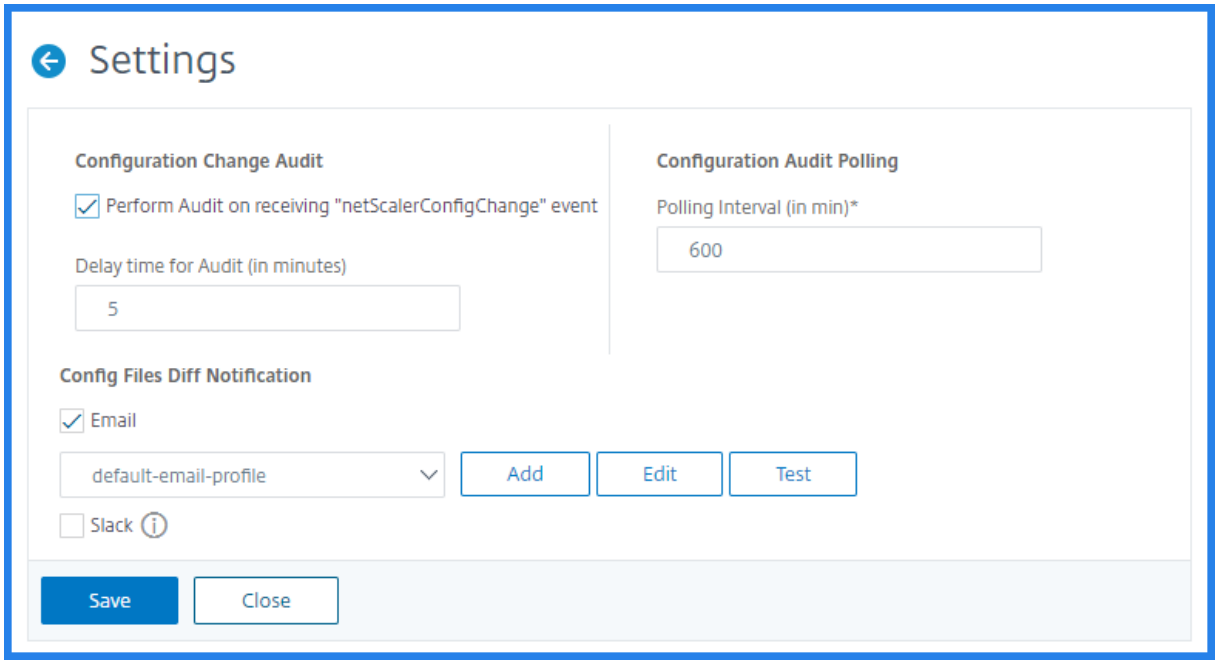


Citrix ADC 構成ファイルのステータスグラフには、`nsconfig` フォルダー内に存在する Citrix ADC ファイルのステータスが表示されます。Citrix ADM は、`nsconfig` フォルダー内のファイルの変更を記録して比較し、相違点を表示します。ファイルステータス監査レポートの表示を参照してください。

構成監査通知の設定

1. [ネットワーク] > [構成監査] に移動します。
2. [構成の監査] ページで、[設定] をクリックします。
3. **[** 設定] ページで、次の操作を行います。
   a) [**NetScalerConfigChange** イベントの受信時に監査を実行する] チェックボックスをオンにして、通知設定を有効にします。
   b) [監査] の [遅延時間] を設定します。
4. [構成監査ポーリング] で、[ポーリング間隔] を設定します。

   Citrix ADM は、指定されたポーリング間隔で構成監査イベントをポーリングします。
5. 「構成ファイル相違通知」で、通知を受信するプラットフォームを選択します。
   - 電子メール -電子メール配布リストを選択します。[追加] をクリックして、通知を受信する電子メール配布リストを追加します。
   - **Slack** -リストから Slack チャンネルを選択します。[追加] をクリックして、通知を受信するチャンネルを追加します。



ネットワーク構成に関する設定アドバイスを取得

May 7, 2021

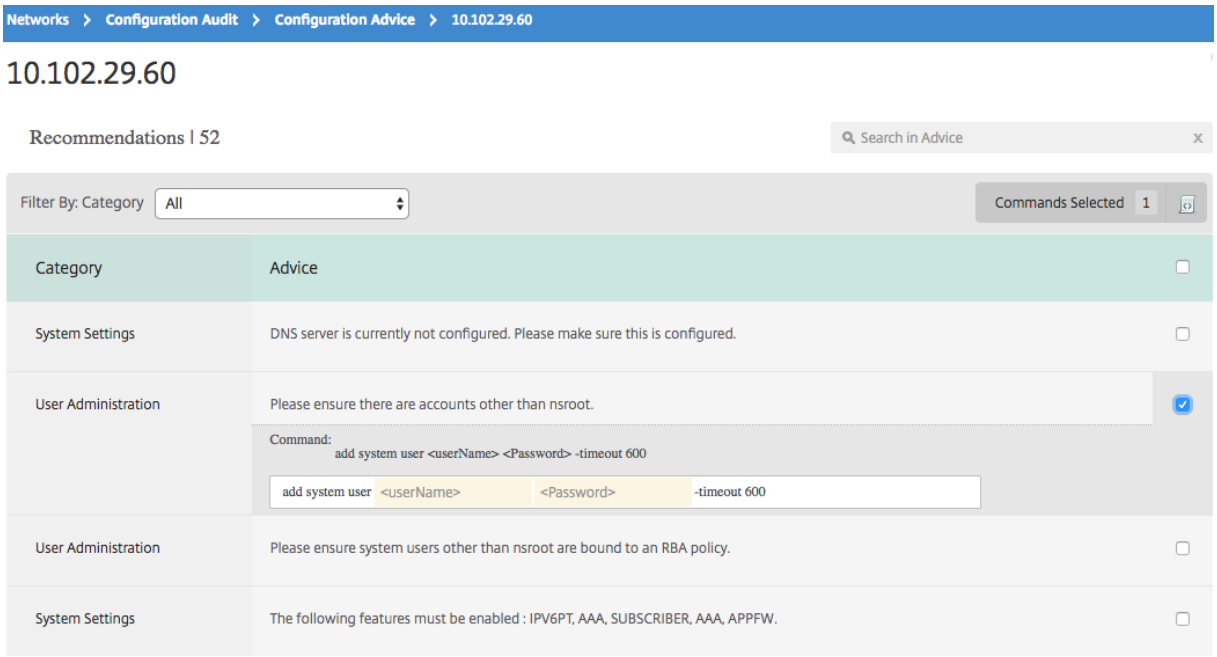
アプリケーションのパフォーマンスを最適化できるように、Citrix ADC インスタンスを最適な構成でセットアップします。ただし、一部の構成は標準構成ではない可能性があり、アプリケーションのパフォーマンスに影響します。

アプリケーションのパフォーマンスを最適化するために、Citrix Application Delivery Management（ADM）は Citrix ADC インスタンスの構成を分析し、推奨事項を提供します。Citrix ADM から推奨される構成を適用できます。

Citrix ADC インスタンスを分析するには:

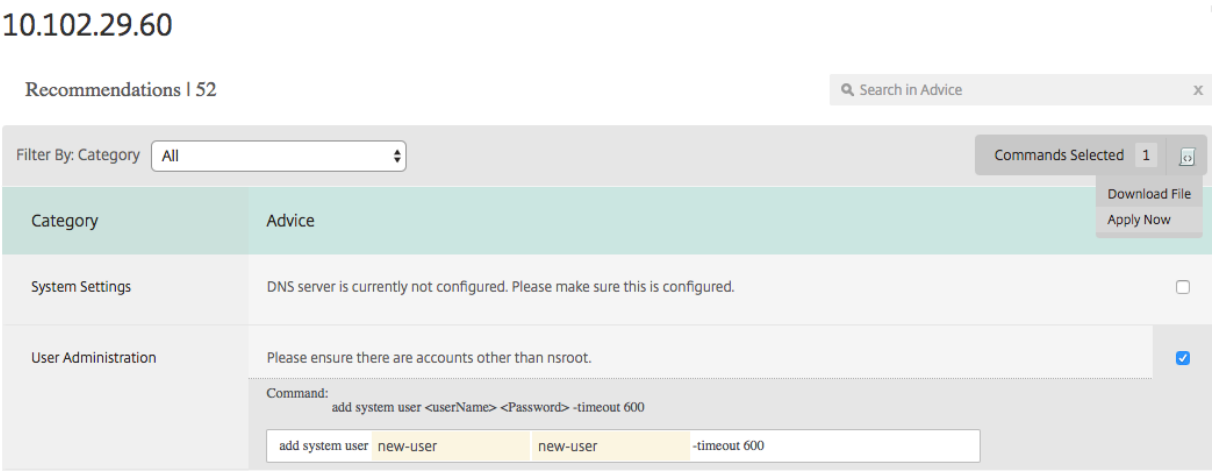
1. [ネットワーク] > [構成監査] > [構成アドバイス] に移動します。
2. 次のいずれかを行います:
   - [**Upload Configuration** File] をクリックし、ネットワークインスタンスの設定ファイルをアップロードします。
   - ［デバイスの選択］をクリックし、分析する Citrix ADC インスタンスを選択します。

Citrix ADM は、インスタンスの構成を分析し、次の図に示すように、推奨される構成のリストを提供します。構成のアドバイスの隣にあるチェックボックスをオンにすると、修正コマンドが表示されます。

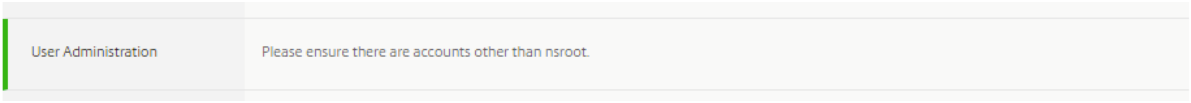


構成を更新する場合は、修正コマンドで変数の値を指定し、次の図に示すように [**Apply Now**] をクリックします。

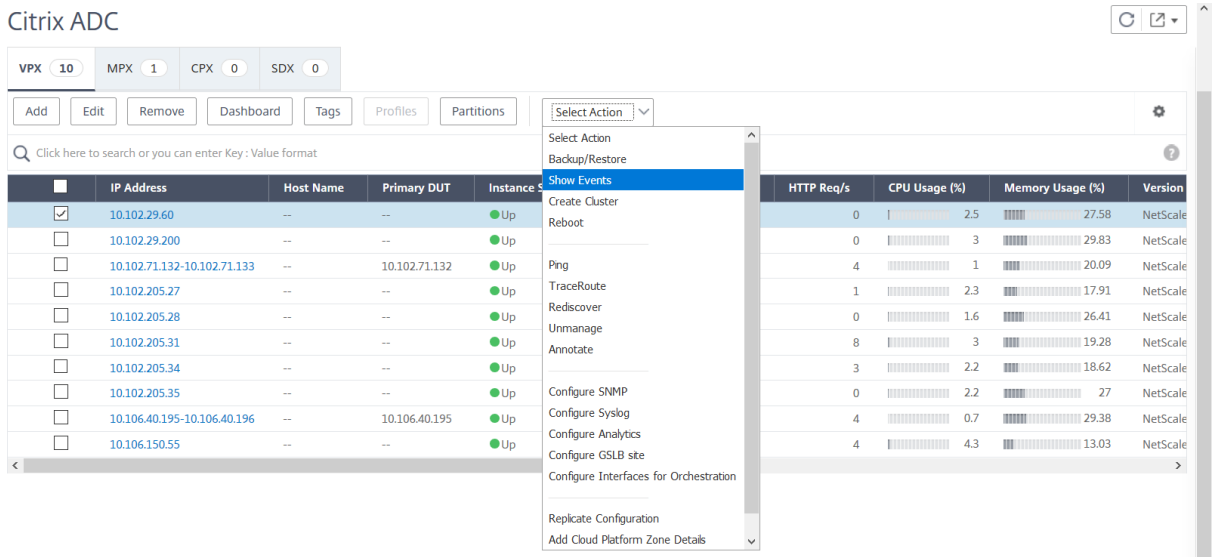
> 注:
>
> ここに記載されているコマンドは、推奨事項に過ぎません。読み取りおよび書き込みアクセス権を持つユーザーは、この機能を使用して任意のコマンドを編集できる場合があります。コマンドを編集してはならないと考えられるユーザーには、限定された特権アクセスを許可してください。



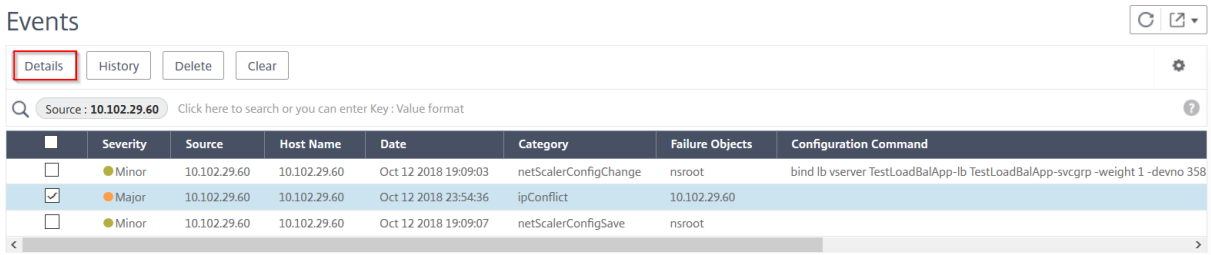
ネットワークインスタンスでコマンドが正常に実行されると、アドバイスの隣にあるチェックボックスが消えます。



ネットワークインスタンスで実行されるコマンドの詳細を表示するには、**[ネットワーク]** > **[インスタンス]** > **<Instance_Type>** に移動し、インスタンスの IP アドレスを選択し、**[Select Actions]** ドロップダウンリストから **[Show Events]** をクリックします。



[**Events**] ページでは、構成変更の詳細を表示できます。



ネットワーク機能

May 7, 2021

ネットワーク機能を使用すると、管理対象の Citrix Application Delivery Controller（Citrix ADC）インスタンスで構成されたエンティティの状態を監視できます。負荷分散仮想サーバーのトランザクション詳細、接続詳細、スループットなどの統計を表示できます。また、メンテナンスの計画時にはエンティティを有効または無効にすることもできます。

ネットワーク機能ダッシュボードには、次のグラフが表示されます。

- クライアント接続が多い上位 5 つの仮想サーバー
- サーバー接続が多い上位 5 つの仮想サーバー
- スループット（MB/秒）が高い上位 5 つの仮想サーバー
- スループット（MB/秒）が低い下位 5 つの仮想サーバー
- 仮想サーバーが多い上位 5 つのインスタンス
- 仮想サーバーの状態
- 負荷分散仮想サーバーの正常性
- プロトコル
- 負荷分散方式
- 負荷分散の永続性
- ほとんどのフロントエンドを持つ上位 5 つの HAProxy インスタンス
- 大部分のサーバーを持つ上位 5 つの HAProxy インスタンス

負荷分散エンティティのレポートを生成する

May 7, 2021

Citrix Application Delivery Management（Citrix ADM）では、すべてのレベルで Citrix アプリケーション Delivery Controller（Citrix ADC）インスタンスエンティティのレポートを表示できます。**Citrix ADM** ／ネットワーク機能でダウンロードできるレポートには、統合レポートと個別レポートの 2 種類があります。

統合レポート: Citrix ADC インスタンスで管理されているすべてのエンティティについて、統合レポートまたは要約レポートをダウンロードして表示できます。

このレポートでは、Citrix ADC インスタンス、パーティション、およびネットワークに存在する対応する負荷分散エンティティ（仮想サーバー、サービスグループ、サービス）間のマッピングの概要を確認できます。

次の画像は、概要レポートの例を示しています。

Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	cs_lb1#0.0.0.0:0		cs_svc1#192.168.4.56:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	cs_lb2#0.0.0.0:0		cs_svc2#192.168.4.57:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s1#192.168.4.51:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s3#192.168.4.53:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s5#192.168.4.55:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s4#192.168.4.54:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s2#192.168.4.52:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	cs_lb3#0.0.0.0:0		cs_svc3#192.168.2.58:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s4#192.168.2.54:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s1#192.168.2.51:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s2#192.168.2.52:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s3#192.168.2.53:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s5#192.168.2.55:80	

統合レポートは、CSV 形式です。各列のエントリの説明は次のとおりです。

- **Citrix ADC IP** アドレス：Citrix ADC インスタンスの IP アドレスがレポートに表示されます
- **Citrix ADC** ホスト名：ホスト名がレポートに表示されます。
- パーティション: 管理パーティションの IP アドレスが表示されます。
- 仮想サーバー: <name_of_the_virtual_server>#virtual_IP_address:port_number
- サービス: <name_of_the_service>#service-IP_address:port_number
- サービスグループ: <name_of_service_group>#server_member1_IP_address:port,server_member2_IP_addre

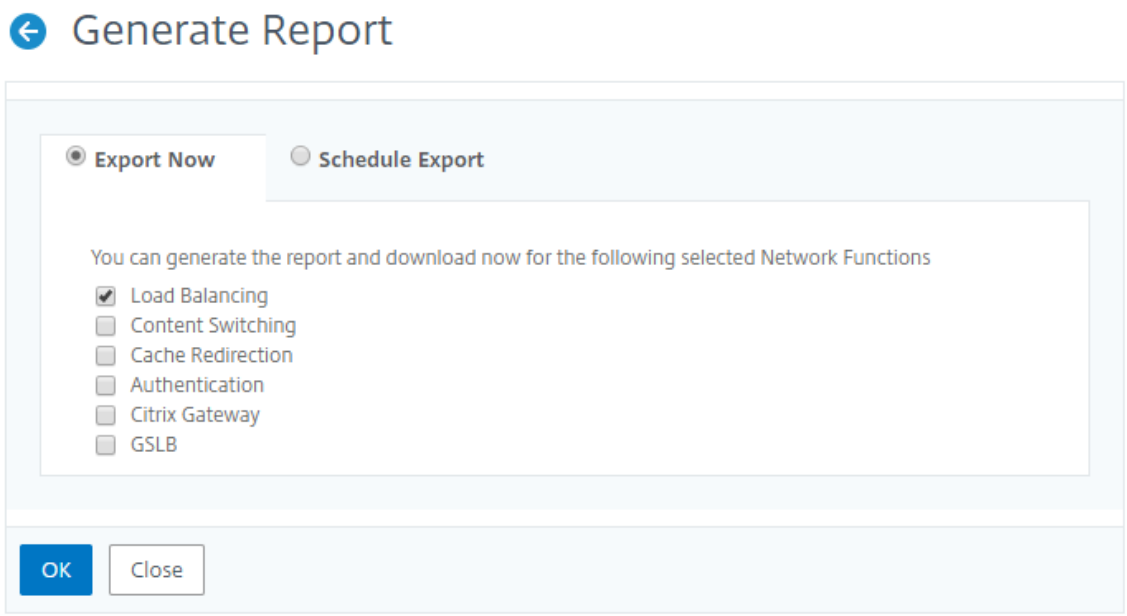
> 注
>
> - 利用可能なホスト名がない場合は、対応する IP アドレスが表示されます。
> - 空白の列は、その Citrix ADC インスタンスに対してそれぞれのエンティティが構成されていないことを示します。

個別レポート: すべてのインスタンスとエンティティの独立したレポートをダウンロードして表示することもできます。たとえば、負荷分散仮想サーバー、負荷分散サービス、負荷分散サービスグループのいずれかのみのレポートをダウンロードできます。

Citrix ADM を使用すると、レポートを即座にダウンロードできます。1 日 1 回、1 週間に 1 回、または 1 か月に 1 回の頻度で、特定の時間にレポートが生成されるようにスケジュールを設定することもできます。

結合された負荷分散レポートの生成

1. Citrix ADM で、［ネットワーク］>［ネットワーク機能］に移動します。
2. [レポートの生成] をクリックします。



3. 開かれる [レポートの生成] ページでは、レポートを表示するための 2 つのオプションがあります。

   a) ［今すぐエクスポート］タブで［負荷分散］を選択し、［**OK**］をクリックします。

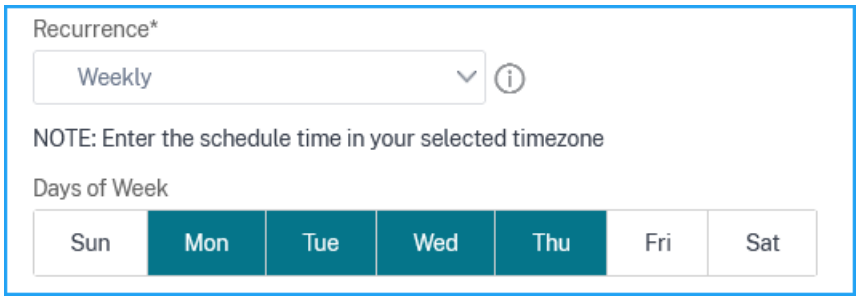
      システムに統合レポートがダウンロードされます。

   b) レポートを生成およびエクスポートするスケジュールを定期的に作成するには、[レポートのスケジュール] を選択します。レポート生成の繰り返し設定を指定し、レポートのエクスポート先のメールプロファイルを作成します。

      i.「スケジュールを有効にする」を選択します。

      ii. [繰り返し]: リストから [毎日]、[毎週]、または [毎月] を選択します。

      > 注
      >
      > [毎週の繰り返し] を選択した場合は、レポートをスケジュールする平日を選択してください。

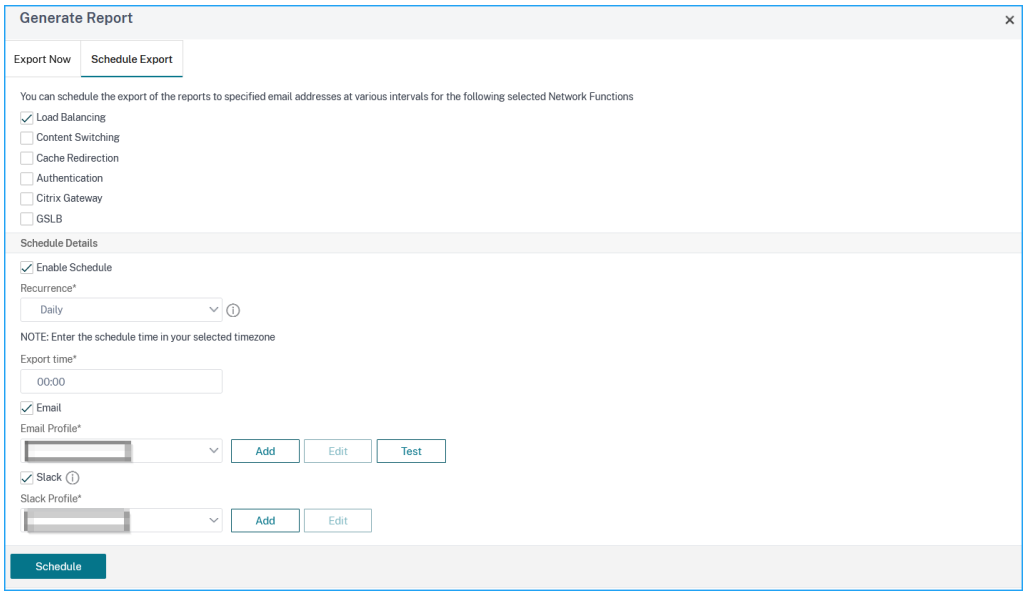
      > 注
      >
      > [毎月の繰り返し] を選択した場合は、必ず 1 から 31 までの値で、月の日数を入力します。

      iii. エクスポート時間 -時間を 24 時間形式で時間: 分形式で入力します。

iv. 電子メール -チェックボックスをオンにし、一覧からプロファイルを選択するか、[追加] をクリックして電子メールプロファイルを作成します。

v. [**Slack**]: [Slack] チェックボックスをオンにし、リストボックスからプロファイルを選択するか、[追加] をクリックしてプロファイルを作成します。

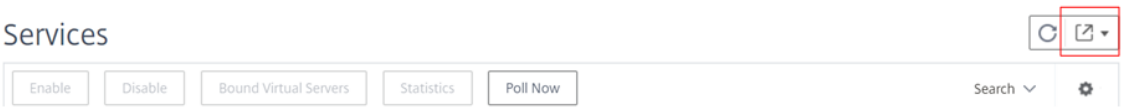
vi. [スケジュール] をクリックしてプロセスを完了します。



個々の負荷分散エンティティレポートを生成する

インスタンスに関連付けられた特定の種類のエンティティを対象に、個別レポートを生成してエクスポートできます。たとえば、ネットワークのすべての負荷分散サービスの一覧を表示するとします。

1. Citrix ADM で、［ネットワーク］>［ネットワーク機能］>［負荷分散］>［サービス］に移動します。
2. [サービス] ページで、右上隅にある [エクスポート] ボタンをクリックします。



この瞬間にレポートを生成して表示する場合は、[**Export Now**] タブを選択します。

> 注
>
> レポートは、メールの添付ファイルとしてのみ、ダウンロードまたはエクスポートできます。Citrix ADM GUI でレポートを表示することはできません。

ネットワーク機能レポートのエクスポートまたはスケジュール設定

May 7, 2021

Citrix Application Delivery Management（Citrix ADM）では、負荷分散、コンテンツスイッチング、キャッシュリダイレクト、グローバルサーバー負荷分散（GSLB）、認証、Citrix Gateway などの特定のネットワーク機能に関する包括的なレポートを生成できます。このレポートでは、ネットワークに存在するインスタンス、パーティション、および対応するバインドされたエンティティ（仮想サーバー、サービスグループ、サービス）間のマッピングの高レベルビューを表示できます。これらのレポートは、.csv ファイル形式でエクスポートできます。

このレポートには、次の仮想サーバデータが表示されます。

- Citrix ADC IP アドレス
- ホスト名
- パーティション・データ
- 仮想サーバ名
- 仮想サーバのタイプ
- 仮想サーバ
- ターゲット LB 仮想サーバー

  > 注:
  >
  > コンテンツスイッチングおよびキャッシュリダイレクト仮想サーバーの場合、[ターゲット LB 仮想サーバー] 列には、すべての LB サーバー (デフォルトサーバーとポリシーベースサーバーの両方) が表示されます。

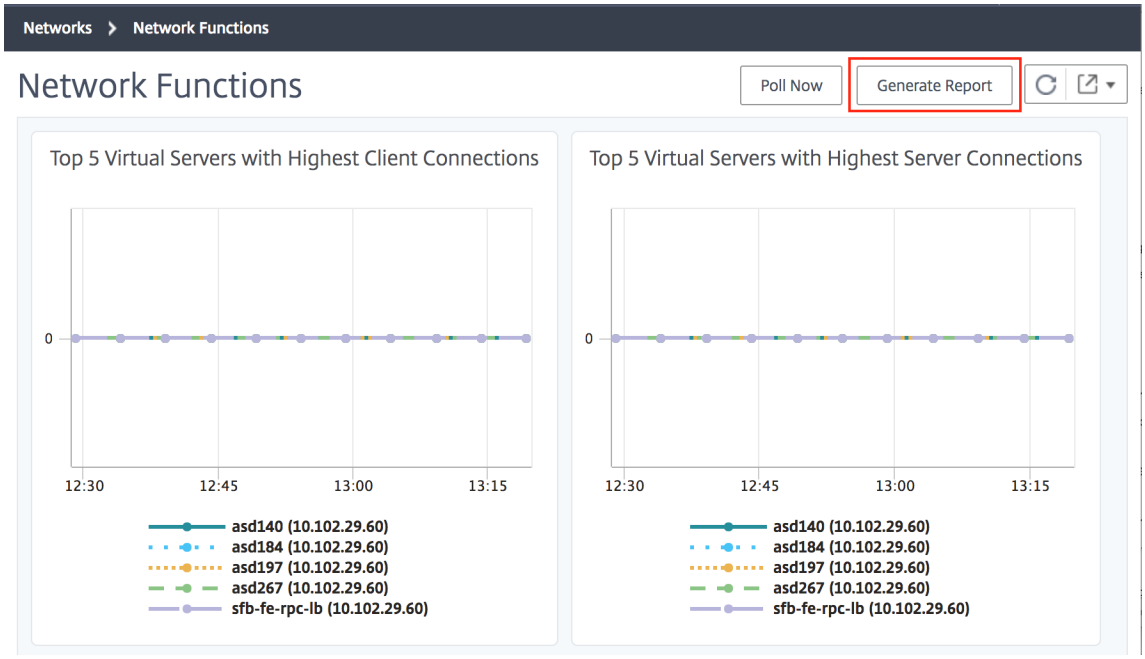
- サービス名
- サービスグループ名

これらのレポートを指定された電子メールアドレスに異なる間隔でエクスポートするようにスケジュールできます。

> 注
>
> - GSLB 仮想サーバーの場合、ネットワーク機能レポートには GSLB 仮想サーバーと関連サービスのみが表示されます。
> - コンテンツスイッチングおよびキャッシュリダイレクト仮想サーバーの場合、レポートには関連付けられた LB サーバーへのバインディングのみが表示されます。
> - SSL 仮想サーバーはこのレポートには表示されません。これは、Citrix ADM で SSL 仮想サーバーの一覧が保持されていないためです。
> - 新しいレポートが生成されると、古いレポートは自動的にアカウントから削除されます。
> - HAProxy のネットワーク機能レポートを生成することはできません。

ネットワーク機能レポートをエクスポートおよびスケジュールする手順は、次のとおりです。

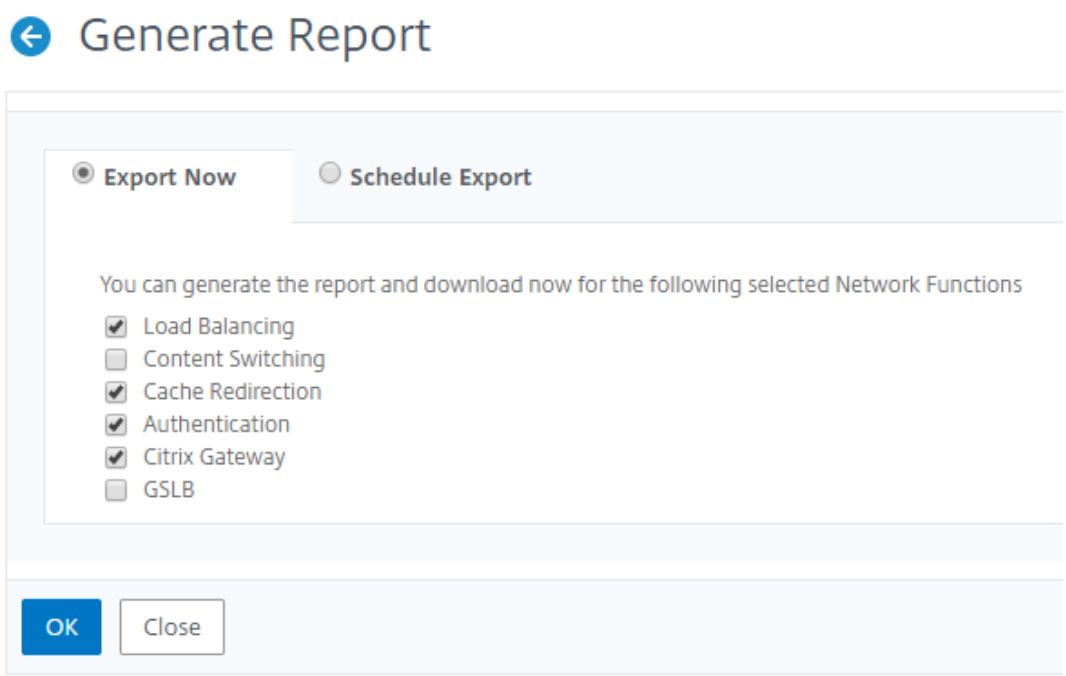
1. [ネットワーク] > [ネットワーク機能] に移動します。
2. [ネットワーク機能] ページの右ペインで、ページの右上隅にある [レポートの生成] をクリックします。



3. [レポートの生成] ページには、次の 2 つのオプションがあります。

   a) [今すぐエクスポート] タブを選択し、[**OK**] をクリックします。

   レポートがシステムにダウンロードされます。



次の図は、ネットワーク機能レポートの例を示しています。

Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
121.123.020.85	121.123.020.85		Load Balancing				
121.123.020.100	NS		Load Balancing				
121.123.020.101	admin-NetScalerVPX-10.102.122.101		Load Balancing				
121.123.020.111	PartitionsHost-sp-final-NetScalerVPX	121.123.020.111-partition_	Load Balancing				
121.123.020.115	121.123.020.115	121.123.020.115-partition-	Load Balancing				
121.123.020.139	NS1		Load Balancing				
121.123.020.49	NS1		Load Balancing				

b) [スケジュールレポート] を選択して、定期的にレポートを生成およびエクスポートするスケジュールを作成します。レポート生成の繰り返し設定を指定し、レポートのエクスポート先のメールプロファイルを作成します。

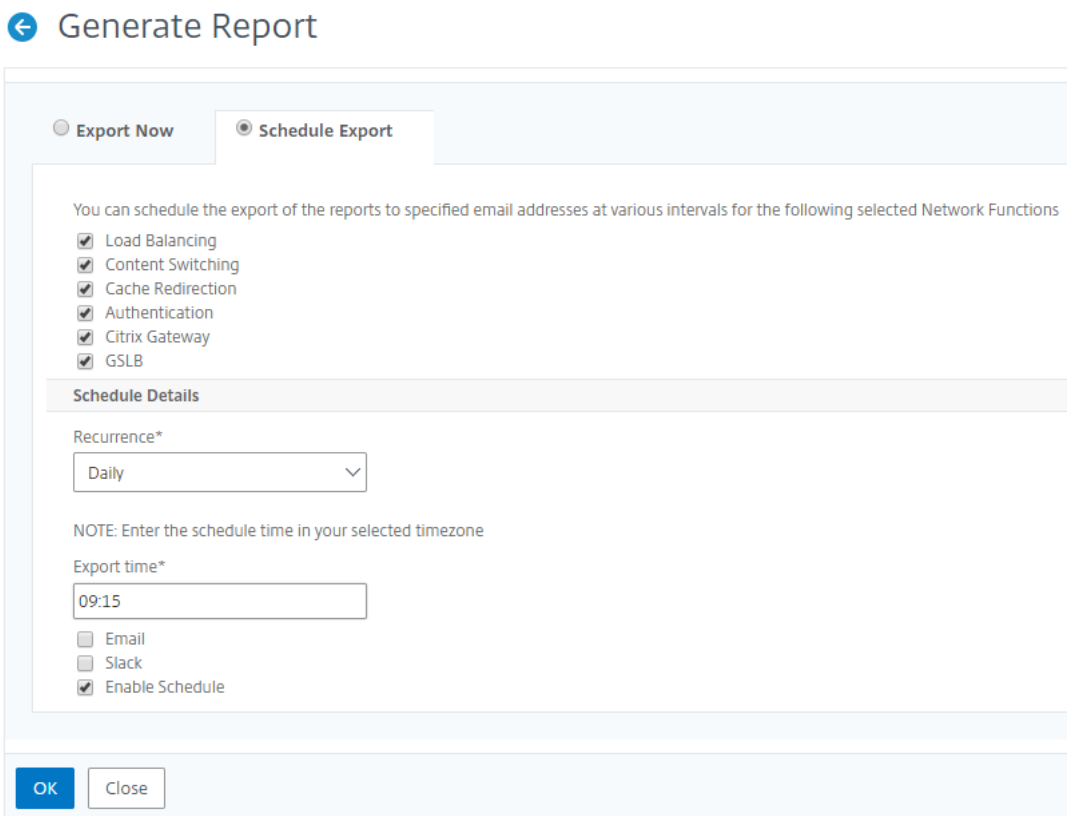
i. 繰り返し -ドロップダウンリストボックスから、[毎日]、[毎週]、または **[**毎月**]** を選択します。

ii. [繰り返し時間]-時間を 24 時間形式で入力します。

iii. 電子メール -チェックボックスをオンにし、ドロップダウンリストボックスからプロファイルを選択するか、[追加] をクリックして電子メールプロファイルを作成します。

iv. **Slack** -チェックボックスをオンにし、ドロップダウンリストボックスからプロファイルを選択するか、[追加] をクリックして電子メールプロファイルを作成します。

[スケジュールを有効にする] をクリックしてレポートをスケジュールし、[**OK**] をクリックします。[**Enable Schedule**] チェックボックスをオンにすると、選択したレポートを生成できます。



ネットワークレポート

May 7, 2021

Citrix Application Delivery Management（Citrix ADM）でネットワークレポートを監視することで、リソースの使用を最適化できます。多数のアプリケーションを複数の場所に展開する、分散展開環境を使用する場合があります。アプリケーションのパフォーマンスを最適化するために、複数の Citrix Application Delivery Controller（Citrix ADC）インスタンスをデプロイして、トラフィックの負荷分散、コンテンツの切り替え、または圧縮を行います。ネットワークのパフォーマンスは、アプリケーションのパフォーマンスに影響を与える可能性があります。アプリケーションのパフォーマンスを維持し続けるには、ネットワークパフォーマンスを定期的に監視し、すべてのリソースが最適に使用されていることを確認する必要があります。

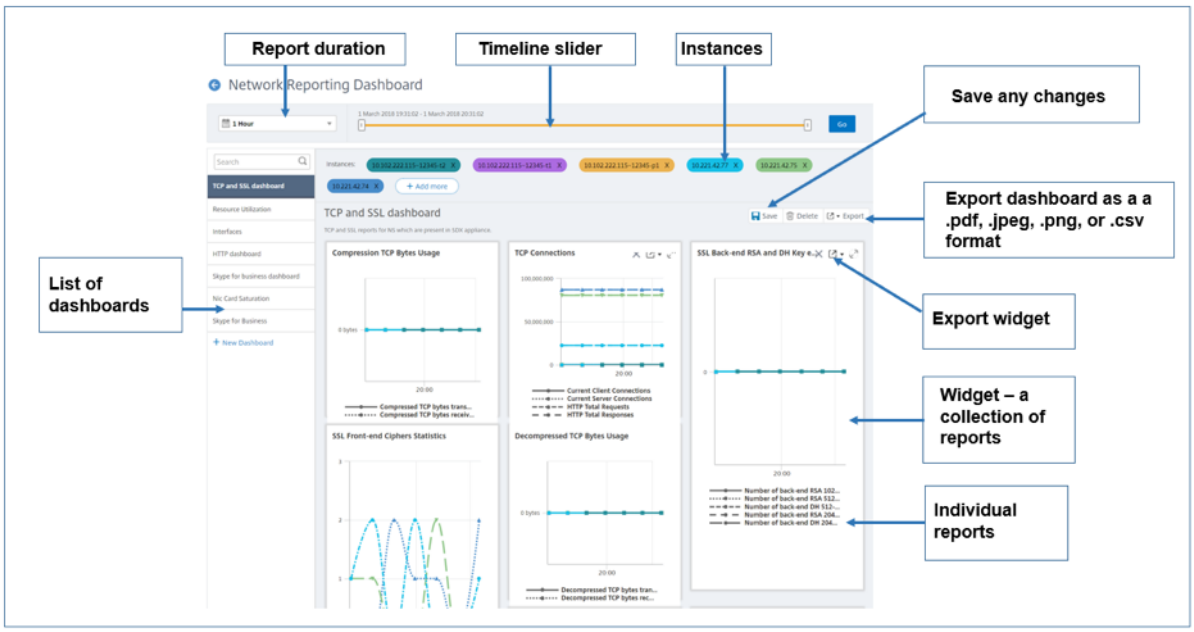
Citrix ADM では、グローバルレベルのインスタンスだけでなく、仮想サーバーやネットワークインターフェイスなどのエンティティについてもレポートを生成できます。インスタンスファミリーは、Citrix ADC インスタンスと SD-WAN インスタンスの両方で構成されます。レポートを生成できる仮想サーバーは次のとおりです。

- サーバ、サービス、およびサービスグループの負荷分散
- コンテンツ・スイッチ・サーバ
- キャッシュリダイレクトサーバー
- グローバルサービス負荷分散（GSLB）
- 認証
- Citrix Gateway

ADM のネットワークレポートダッシュボードは、高度にカスタマイズできます。さまざまなインスタンス、仮想サーバー、およびその他のエンティティに対して、複数のダッシュボードを作成できます。

ネットワークレポートダッシュボード

次の図は、ダッシュボードのさまざまな機能を示しています。

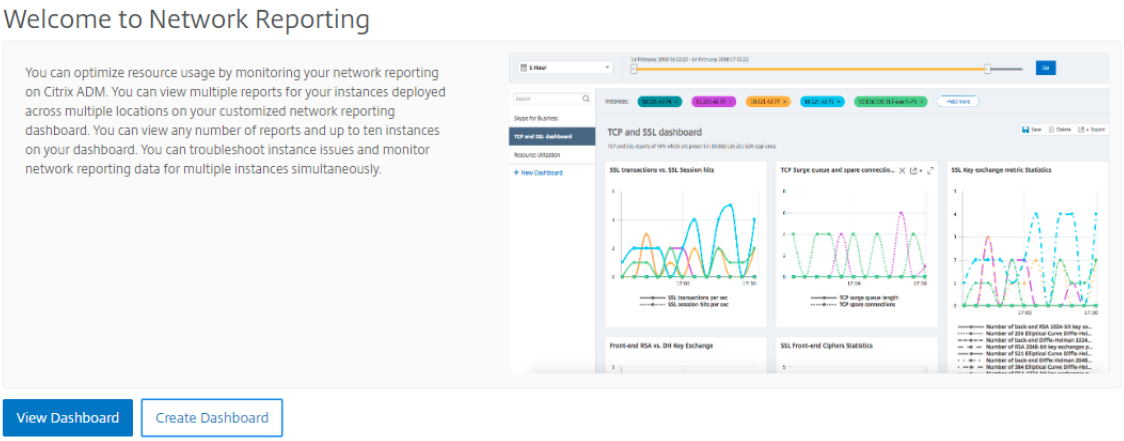


- 左側のパネルには、Citrix ADM で作成されたすべてのカスタムダッシュボードが表示されます。これらのいずれかをクリックすると、ダッシュボードを構成するさまざまなレポートを表示できます。たとえば、TCP および SSL ダッシュボードには、TCP および SSL プロトコルに関連するさまざまなレポートが含まれています。
- 複数のウィジェットを使用して各ダッシュボードをカスタマイズして、さまざまなレポートを表示できます。ウィジェットは、より関連性のあるレポートのコレクションであるダッシュボード上のレポートを表します。たとえば、圧縮 TCP バイト使用状況レポートには、1 秒あたりに転送および受信された圧縮された TCP バイトに関するレポートが含まれます。
- 1 時間、1 日、1 週間、または 1 か月分のレポートを表示できます。さらに、タイムラインスライダーオプションを使用して、Citrix ADM で生成されるレポートの持続時間をカスタマイズできるようになりました。
- 「X」をクリックすると、レポートを削除できます。レポートを.pdf、.jpeg、.png、.csv 形式でシステムにエクスポートすることもできます。また、レポートを生成する時刻と繰り返しをスケジュールすることもできます。また、レポートの送信先となる電子メール配布リストを構成することもできます。
- ダッシュボードの上部にある [Instances] セクションには、レポートが生成されるすべてのインスタンスの IP アドレスが一覧表示されます。
- [X] をクリックしてインスタンスを削除するか、レポートにインスタンスを追加できます。しかし、現在、Citrix ADM では、10 インスタンスのレポートを表示できます。
- ダッシュボード全体を.pdf、.jpeg、.png、.csv 形式でシステムにエクスポートすることもできます。ダッシュボードに加えた変更はすべて保存する必要があります。［保存］をクリックして変更を保存します。

次のセクションでは、ダッシュボードの作成、レポートの生成、およびレポートのエクスポートのタスクについて詳しく説明します。

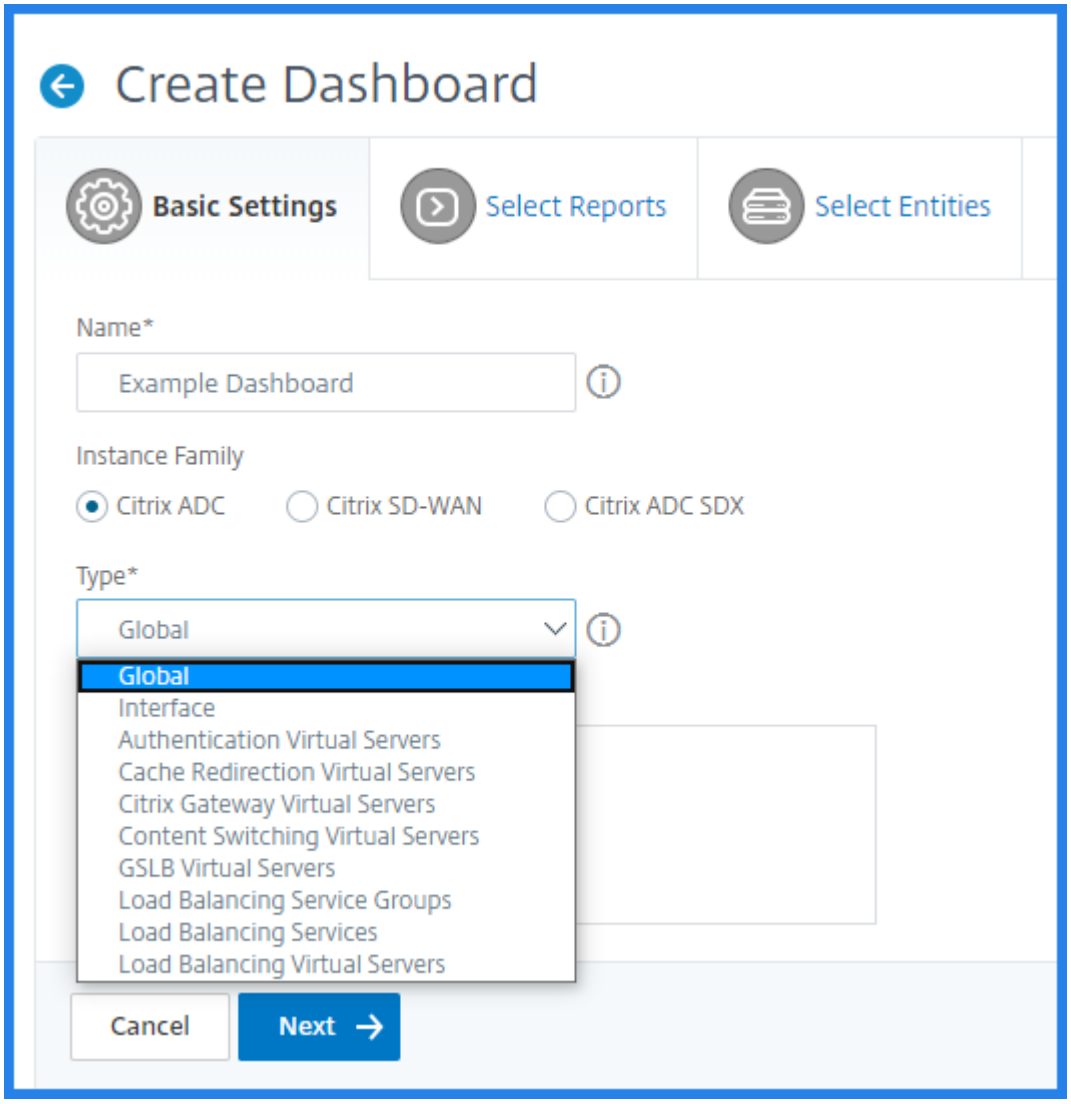
ダッシュボードを表示または作成する手順は、次のとおりです。

1. Citrix ADM で、［ネットワーク］>［ネットワークレポート］に移動します。



2. 既存のダッシュボードを表示するには、[ダッシュボードの表示] をクリックします。[ネットワークレポートダッシュボード] ページが開き、すべてのダッシュボードとレポートウィジェットを表示できます。
3. ダッシュボードを作成するには、「ダッシュボードの作成」をクリックします。

   「ダッシュボードの作成」ページが開きます。



4. [基本設定] タブで、次の詳細を入力します。

   a) 名前。ダッシュボードの名前を入力します。

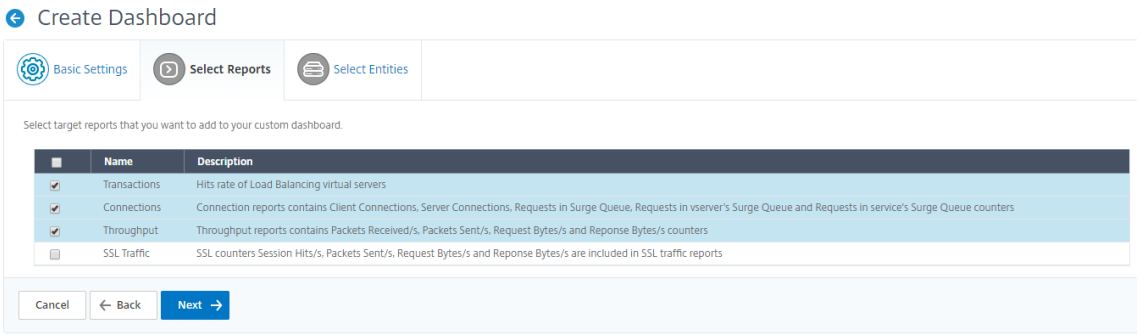
   b) インスタンスファミリ。インスタンスのタイプ（Citrix ADC、Citrix SD-WAN、または Citrix ADC SDX）を選択します。

   c) タイプ。レポートを生成するエンティティタイプを選択します。この例では、[負荷分散仮想サーバー] を選択します。

   d) 説明。ダッシュボードのわかりやすい説明を入力します。

5. [次へ] をクリックします。

6. **[** レポートの選択] タブで、必要なレポートを選択します。この例では、トランザクション、接続、およびスループットを選択できます。［次へ］ をクリックします。



7. **[** エンティティの選択] タブで、[追加] をクリックします。

   [基本設定] タブで選択したエンティティタイプに応じて、エンティティリストを含むウィンドウが表示されます。この例では、[**LB** 仮想サーバーの選択] ウィンドウが表示されます。

8. 監視するエンティティを選択します。

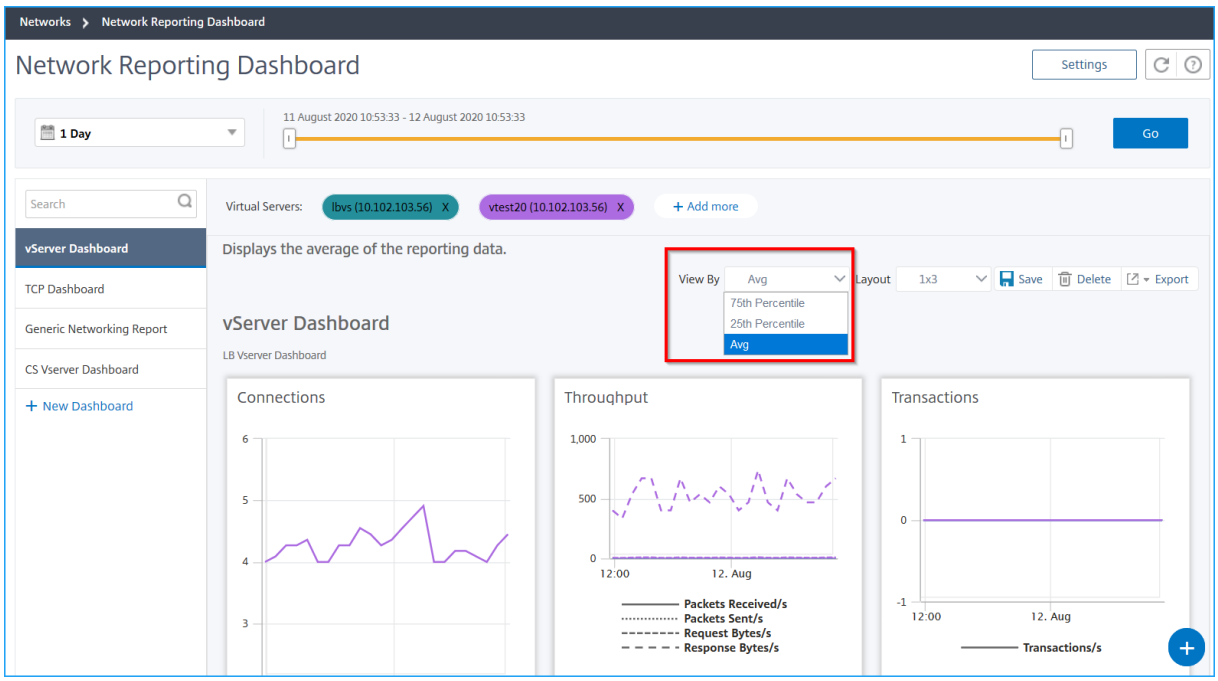
9. [作成] をクリックします。

ダッシュボードが作成され、選択したすべてのレポートが表示されます。

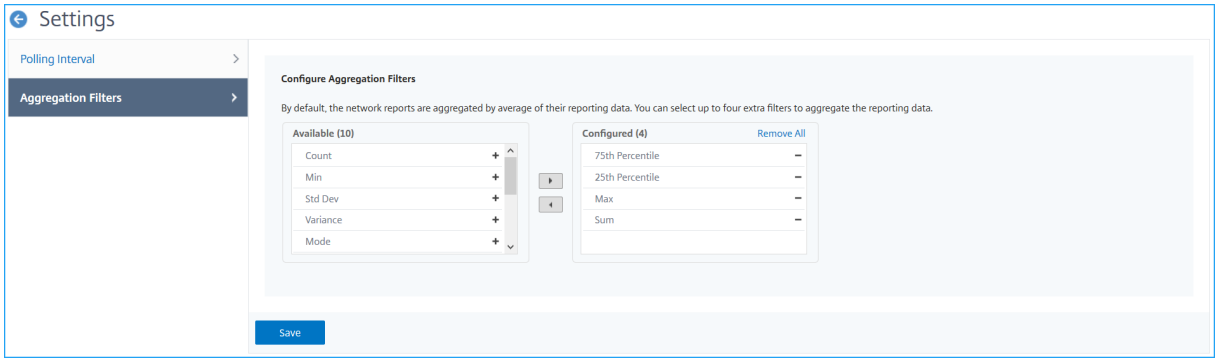
> 注:
>
> 現在のところ、凡例またはフィルタに加えた変更は保存できません。

集約を適用してネットワークレポートデータを表示する

ネットワークパフォーマンスデータに集約を適用し、ダッシュボードでアプリケーションのパフォーマンスを表示できます。要件に基づいて結果をエクスポートすることもできます。データに適用されたこれらの集計を使用して、すべてのリソースが最適に利用されているかどうかを分析し、確認することができます。[ネットワーク] **>** [ネットワークレポート] に移動し、1 日またはそれ以降の期間を選択して [表示方法] オプションを表示します。



既存の平均データでは、「表示別」(**View** By) リストからオプションを選択して集計を適用できます。集計を適用すると、ダッシュボードの各指標のデータが更新されます。[設定] をクリックし、[集約フィルタ] を選択します。



追加できる集計を次に示します。

- Count
- 最大
- 最小
- SUM

- 標準開発
- 差異
- Mode
- 中央値
- 第 25 パーセンタイル
- 第 75 パーセンタイル
- 第 95 パーセンタイル
- 第 99 パーセンタイル
- 第 1
- 最終

ダッシュボードには、最大 4 つの集計オプションを追加できます。集約オプションを追加した後、選択した集約オプションのレポートが生成されるまでに約 1 時間かかります。

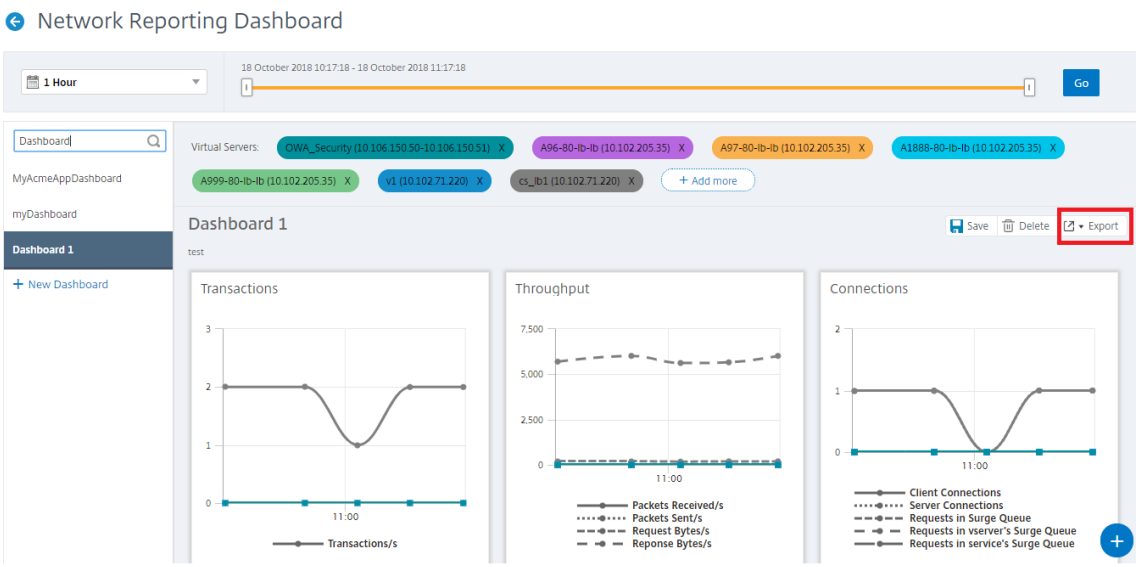
ネットワークレポートのエクスポート

ウィジェットレポートを.pdf、.png、.jpeg、.csv 形式でエクスポートできますが、ダッシュボード全体を.pdf、.jpeg、.png 形式でのみエクスポートできます。

> 注
>
> 読み取り専用権限がある場合は、Citrix ADM でレポートをエクスポートできません。Citrix ADM でファイルを作成し、ファイルをエクスポートできるようにするには、編集権限が必要です。

ダッシュボード・レポートをエクスポートするには、次の手順に従います。

1. [ネットワーク] > [ネットワークレポート] に移動します。
2. [ダッシュボードの表示] をクリックして、作成したすべてのダッシュボードを表示します。
3. 左側のペインで、ダッシュボードをクリックします。この例では、[ダッシュボード **1**] をクリックします。
4. ページの右上隅にある [エクスポート] ボタンをクリックします。
5. [今すぐエクスポート] タブで、必要な形式を選択し、[エクスポート] をクリックします。



[エクスポート] ページでは、次のいずれかの操作を実行できます。

6. [今すぐエクスポート] タブを選択します。レポートを PDF、JPEG、PNG、または CSV 形式で表示して保存します。
7. [スケジュールエクスポート] タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、電子メールまたは余裕期間メッセージでレポートを送信するには。

   [ネットワークレポートダッシュボード] ページのエクスポートは、定期的にスケジュールできます。たとえば、特定の時間に過去 1 時間のダッシュボードレポートを毎週生成するオプションを設定できます。レポートは毎週生成され、ダッシュボードの状態が表示されます。ユーザーが設定した日時スタンプは、レポートによって上書きされます。

> 注
>
> - [毎週の繰り返し] を選択した場合は、レポートをスケジュールする平日を選択してください。
> - 繰り返しで［Monthly］を選択した場合は、レポートのスケジュールを設定するすべての日にちを、コンマ区切りで入力していることを確認します。

ネットワークレポートをスケジュールするときに、[**Subject**] フィールドにテキスト文字列を入力して、レポートの見出しをカスタマイズできます。スケジュールされた時刻に作成されたレポートには、この文字列が名前になります。

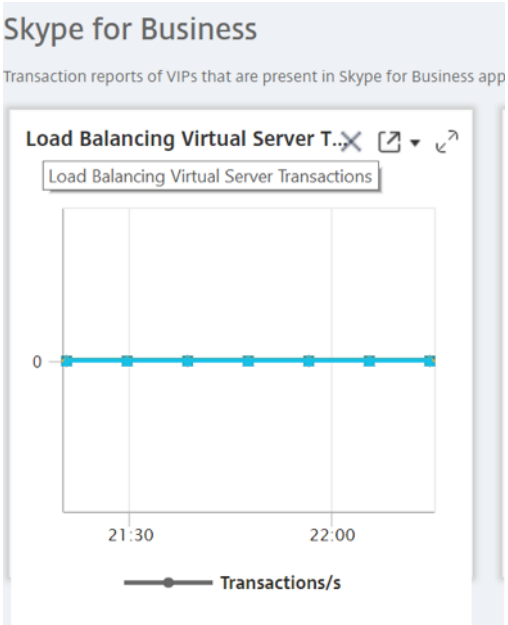
たとえば、特定の仮想サーバからのネットワークレポートの場合、サブジェクトに「認証レポート-10.106.118.120」と入力します。ここで、10.106.118.120 は監視対象の仮想サーバの IP アドレスです。

> 注
>
> ：現在、このオプションは、レポートのエクスポートをスケジュールする場合にのみ使用できます。即座にエクスポートするときに、レポートに見出しを追加することはできません。

ウィジェット・レポートをエクスポートするには、次の手順に従います。

1. [ネットワーク] > [ネットワークレポート] に移動します。

2. [ダッシュボードの表示] をクリックして、作成したすべてのダッシュボードを表示します。
3. 左側のペインで、ダッシュボードをクリックします。この例では、**Skype for Busin**ess をクリックします。
4. ウィジェットを選択します。たとえば、[仮想サーバートランザクションの負荷分散] を選択します。
5. ページの右上隅にある [エクスポート] ボタンをクリックします。
6. [今すぐエクスポート] タブで、必要な形式を選択し、[エクスポート] をクリックします。



Citrix ADM でネットワークレポートのしきい値を管理する方法

Citrix ADC インスタンスの状態を監視するには、カウンターのしきい値を設定し、しきい値を超えたときに通知を受信します。Citrix ADM では、しきい値を構成し、しきい値を表示、編集、削除できます。

たとえば、コンテンツスイッチング仮想サーバーの Connections カウンターが指定した値に達すると、電子メール通知を受信できます。特定のインスタンスタイプに対してしきい値を定義できます。選択したインスタンスから特定のカウンタメトリックスに対して生成するレポートを選択することもできます。

カウンタの値が（規則で指定された）しきい値を超えたり、下回ったりすると、指定した重大度のイベントが生成され、パフォーマンスに関連する問題を示します。カウンター値が正常と見なされる値に戻ると、イベントはクリアされます。これらのイベントは、[ネットワーク] > [イベント] > [レポート] の順に選択して表示できます。[レポート] ページで、[重要度別イベント] ドーナツをクリックすると、重大度別にイベントを表示できます。

また、しきい値を超えたときに電子メールや SMS メッセージを送信するなど、アクションをしきい値に関連付けることもできます。

しきい値を作成するには、次の手順に従います。

1. Citrix ADM で、［ネットワーク］ **>** ［ネットワークレポート］ **>** ［しきい値］ に移動します。［**Thresholds**］の［**Add**］ をクリックします。

2. **[** しきい値の作成] ページで、次の詳細を指定します。

    - 名前。しきい値の名前。
    - インスタンスタイプ。［Citrix ADC］または［Citrix SD-WAN WO］を選択します。
    - レポート名。このしきい値に関する情報を提供するパフォーマンスレポートの名前。

3. イベントを生成またはクリアするタイミングを指定するルールを設定することもできます。[規則の構成] セクションで、次の詳細を指定できます。

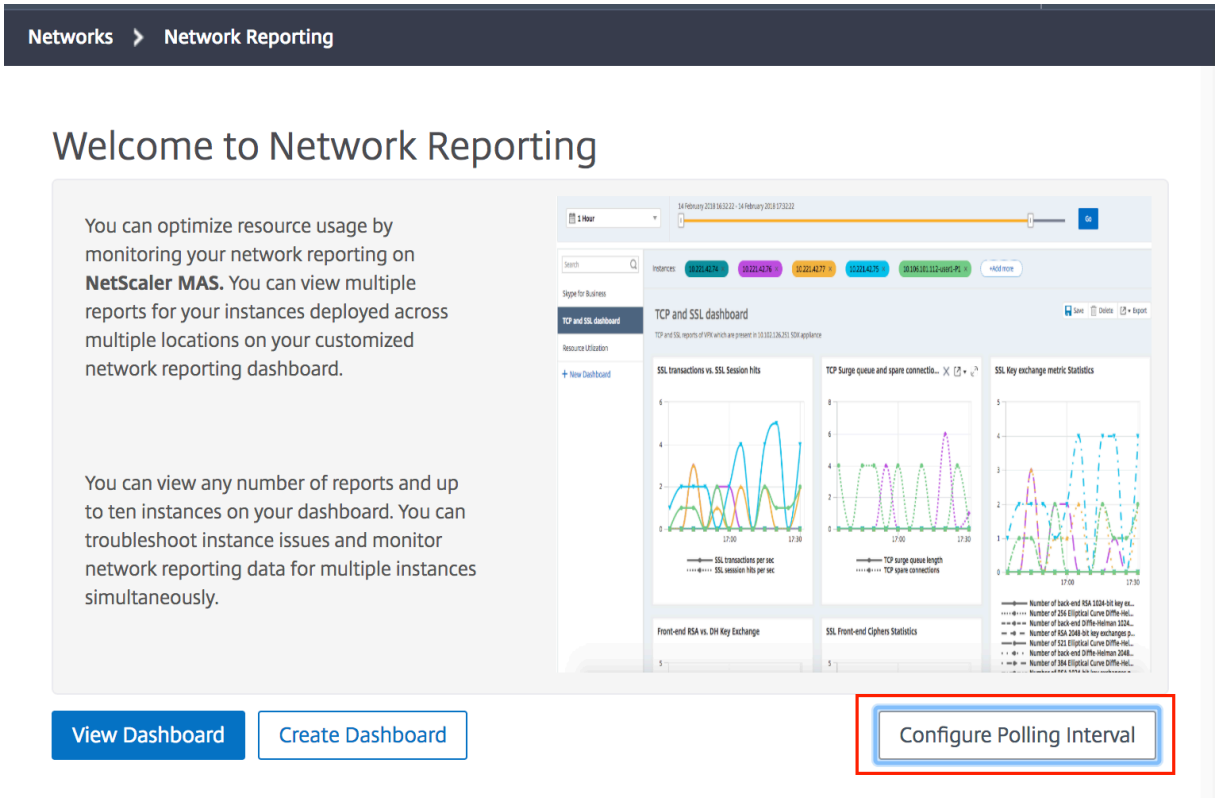
    - メトリック。しきい値を設定するメトリックを選択します。
    - コンパレータ。コンパレータを選択して、モニタする値がしきい値以下かどうかをチェックします。
    - しきい値。イベントの重大度を計算する値を入力します。たとえば、現在のクライアント接続の監視対象の値が 80%に達すると、重大なイベント重大度を持つイベントを生成することができます。この場合、しきい値として 80 を入力します。「重大な重大度」イベントは、**[**ネットワーク**] > [**イベント**] > [**レポート] の順に選択して表示できます。[レポート] ページで、[重要度別イベント] ドーナツをクリックすると、重大度別にイベントを表示できます。
    - **[** 値をクリア**]:** 値をクリアするタイミングを示す値を入力します。たとえば、監視対象の値が 50%に達すると、現在のクライアント接続のしきい値をクリアすることができます。この場合、クリア値として 50 を入力します。
    - イベントの重大度。しきい値に設定するセキュリティレベルを選択します。

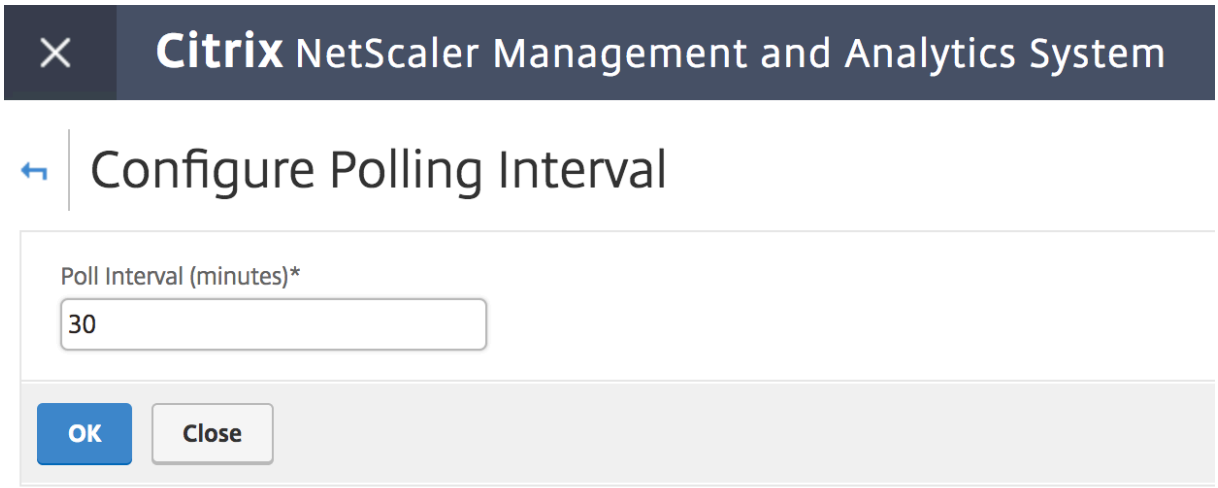
4. しきい値を設定するインスタンスの IP アドレスを選択します。
5. イベントメッセージを追加することもできます。しきい値に達したときに表示するメッセージを入力します。Citrix ADM により、監視対象の値としきい値がこのメッセージに追加されます。
6. アラームを生成するためのしきい値を有効にするには、**[Enable]** を選択します。
7. オプションで、メールや Slack 通知などのアクションを設定できます。
8. ［作成］をクリックします。

ネットワークレポートのパフォーマンスポーリング間隔の設定

デフォルトでは、NITRO 呼び出しは 5 分ごとにネットワークレポート用のパフォーマンスデータを収集します。ADM は、カウンタ情報などのインスタンス統計を取得し、1 分単位、時間単位、日単位、週単位で集計します。この集計データを事前定義されたレポートで表示できます。

パフォーマンスポーリング間隔を設定するには、[ネットワーク] > [ネットワークレポート] に移動し、[ポーリング間隔の構成] をクリックします。ポーリング間隔は 5 分未満または 60 分を超えることはできません。





ネットワークレポートプルーニング設定の構成

Citrix ADM でネットワークレポートデータの消去間隔を構成できます。この間隔は、Citrix ADM サーバーのデータベースに保存されるネットワークレポートデータの量を制限します。デフォルトでは、ネットワークが履歴データをレポートする場合、プルーニングは 24 時間ごと（01.00 時間ごと）実行されます。

> 注
>
> 指定できる値は、90 日を超えるか、1 日未満にすることはできません。

オーケストレーション

July 7, 2020

Citrix ADM で Kubernetes 入力構成を管理する

May 7, 2021

Kubernetes (K8s) は、クラウドネイティブアプリケーションのデプロイ、スケーリング、管理を自動化する、オープンソースのコンテナーオーケストレーションプラットフォームです。

Kubernetes は Ingress 機能を提供し、クラスタ外のクライアントトラフィックが Kubernetes クラスタ内で実行されているアプリケーションのマイクロサービスにアクセスできるようにします。ADC インスタンスは、Kubernetes クラスタ内で実行されているアプリケーションへの入力として機能できます。ADC インスタンスは、クライアントから Kubernetes クラスター内の任意のマイクロサービスに南北トラフィックをロードバランシングし、コンテンツでルーティングできます。

> 注
>
> - Citrix ADM は、Kubernetes バージョン 1.14 以降のクラスタで入力機能をサポートしています。
> - Citrix ADM は、入力デバイスとして Citrix ADC VPX および MPX アプライアンスをサポートしています。
> - Kubernetes 環境では、Citrix ADC インスタンスは「NodePort」サービスタイプのみを負荷分散します。

複数の ADC インスタンスを、同じクラスタまたは異なるクラスタまたは名前空間上で入力デバイスとして動作するように設定できます。インスタンスを設定したら、Ingress ポリシーに基づいて各インスタンスを異なるアプリケーションに割り当てることができます。

Kubernetes `kubectl` または API を使用して、入力設定を作成してデプロイできます。また、Citrix ADM からの入力を構成して展開することもできます。

ADM で Kubernetes 統合の次の側面を指定できます。

- クラスタ — ADM が入力設定をデプロイできる Kubernetes クラスタを登録または登録解除できます。Citrix ADM にクラスターを登録する場合は、Kubernetes API サーバー情報を指定します。次に、Kubernetes クラスタに到達できる ADM エージェントを選択し、Ingress 構成を展開します。
- ポリシー — Ingress ポリシーは、Ingress 設定をデプロイするクラスタまたは名前空間に基づいて ADC インスタンスを選択するために使用されます。ポリシーを追加するときに、クラスタ、サイト、およびインスタンスの情報を指定します。
- 入力設定：この設定は Kubernetes 入力設定です。この設定には、コンテンツスイッチングルールと、マイクロサービスとそのポートの対応する URL パスが含まれます。Kubernetes シークレットリソースを使用し

て、（ADC インスタンスでの SSL 処理の負荷を軽減するために）SSL/TLS 証明書を指定することもできます。

Citrix ADM は、入力ポリシーを使用して、入力構成を ADC インスタンスに自動的にマッピングします。

入力構成が成功するたびに、Citrix ADM はスタイルブック構成パックを生成します。ConfigPack は、入力設定に対応する ADC インスタンスに適用される ADC 設定を表します。ConfigPack を表示するには、「アプリケーション」**>**「スタイルブック」**>**「構成」に移動します。

はじめに

Citrix ADC インスタンスを Kubernetes クラスターの入力デバイスとして使用するには、以下の機能があることを確認してください。

- Kubernetes クラスターが存在する。
- ADM と Kubernetes クラスターまたは管理対象インスタンス間の通信を有効にするように、Citrix ADM エージェントがインストールおよび構成されています。データセンターまたはクラウドに存在するマネージドインスタンスを使用できます。
- Citrix ADM に登録された Kubernetes クラスター。

Kubernetes クラスタに登録するための **Citrix ADM** エージェントの設定

Kubernetes クラスタと Citrix ADM 間の通信を有効にするには、Citrix ADM エージェントをインストールして構成する必要があります。エージェントは、次のプラットフォームにデプロイできます。

- ハイパーバイザ（ESX、XenServer、KVM、Hyper-V）
- パブリッククラウドサービス（Microsoft Azure、AWS など）

プロシージャに従って、エージェントを設定します。

> 注
>
> 既存の ADM エージェントが既に展開されている場合は、そのエージェントを使用することもできます。

秘密トークンを使用して **Citrix ADM** を構成し、**Kubernetes** クラスタを管理する

Citrix ADM が Kubernetes からイベントを受信できるようにするには、Kubernetes で Citrix ADM 用のサービスアカウントを作成する必要があります。また、クラスタで必要な RBAC アクセス許可を使用してサービスアカウントを構成します。

1. Citrix ADM サービスアカウントを作成します。たとえば、サービスアカウント名は`citrixadm-sa`になります。サービスアカウントを作成するには、複数のサービスアカウントの使用を参照してください。
2. `cluster-admin` ロールを使用して、Citrix ADM サービスアカウントをバインドします。このバインディングは、クラスタ全体で`ClusterRole`をサービスアカウントに付与します。次に、`cluster-admin` ロールをサービスアカウントにバインドするコマンドの例を示します。


```
kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole
    =cluster-admin --serviceaccount=default:citrixadm-sa
<!--NeedCopy-->
```

Citrix ADM サービスアカウントを `cluster-admin` ロールにバインドすると、そのサービスアカウントはクラスター全体にアクセスできるようになります。詳細については、[`kubectl` create `clusterrolebinding`] (https://kubernetes.io/docs/reference/access-authn-authz/rbac/#kubectl-create-clusterrolebinding) を参照してください。

3. 作成したサービスアカウントからトークンを取得します。

   たとえば、次のコマンドを実行して、`citrixadm-sa` サービスアカウントのトークンを表示します。

```
kubectl describe sa citrixadm-sa
<!--NeedCopy-->
```

4. 次のコマンドを実行して、トークンのシークレット文字列を取得します。

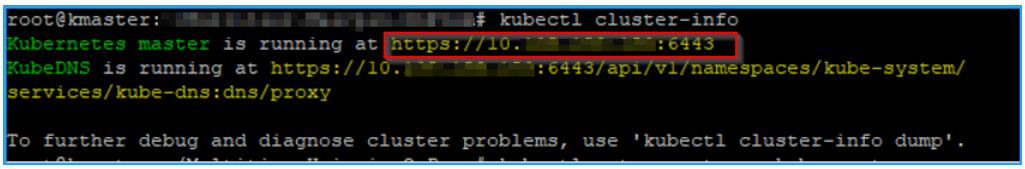
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

Citrix ADM で Kubernetes クラスターを追加する

Citrix ADM エージェントを構成して静的ルートを構成したら、Citrix ADM に Kubernetes クラスターを登録する必要があります。

Kubernetes クラスタを登録するには:

1. 管理者の資格情報を使用して Citrix ADM にログオンします。
2. [オーケストレーション] > [**Kubernetes**] > [クラスタ] に移動します。
   「クラスタ」ページが表示されます。
3. [追加] をクリックします。
4. **[** クラスタの追加] ページで、次のパラメータを指定します。
   a) [名前]: 任意の名前を指定します。
   b) **API** サーバー **URL** -Kubernetes マスターノードから API サーバー URL の詳細を取得できます。
      i. Kubernetes マスターノードで、コマンド`kubectl cluster-info`を実行します。



ii.「**Kubernetes** マスターが実行中です。」と表示される **URL** を入力します。

c) 認証トークン -Kubernetes クラスタを管理するための Citrix ADM の設定を実行する間、ユーザーが取得する認証トークン文字列を指定します。認証トークンは、Kubernetes クラスタと Citrix ADM 間の通信へのアクセスを検証するために必要です。認証トークンを生成する手順は、次のとおりです。

i. Kubernetes マスターノードで、次のコマンドを実行します。

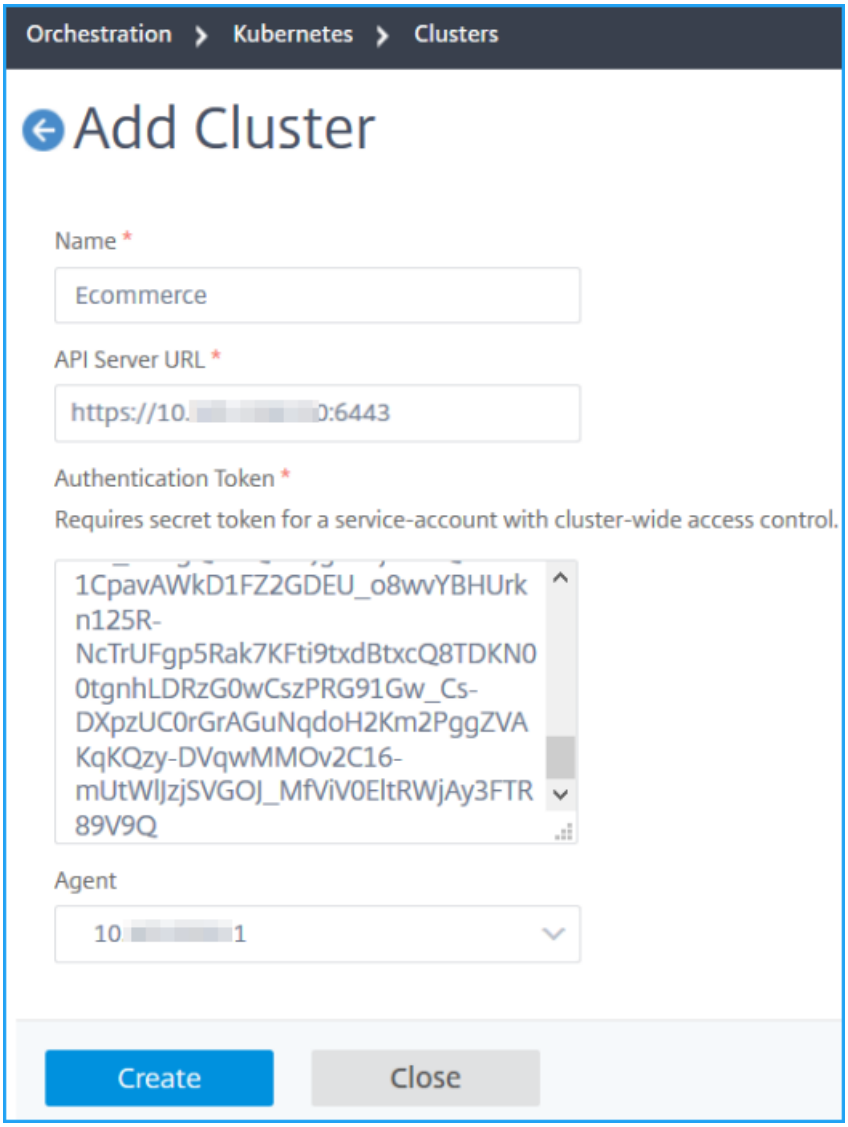
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

ii. 生成されたトークンをコピーし、認証トークンとして貼り付けます。

詳しくは、Kubernetesのドキュメントを参照してください。

d) リストからエージェントを選択します。

e)［作成］をクリックします。



入力ポリシーの定義

入力ポリシーは、入力クラスターまたは名前空間、またはその両方に基づいて、入力構成の展開に使用する Citrix ADC を決定します。

1. [オーケストレーション**] > [Kubernetes] > [**ポリシー**]** に移動します。
2. [**Add**] をクリックしてポリシーを作成します。
   a) ポリシー名を指定します。
   b) 入力設定を Kubernetes クラスターにデプロイするための 条件を定義します。これらの条件は、通常、入力クラスタと名前空間に基づいています。
   c) [インフラストラクチャ] パネルでは、
      - サイト -リストからサイトを選択します。

- インスタンス -リストから ADC インスタンスを選択します。

[サイト] リストと [インスタンス] リストには、[条件] パネルのクラスタ選択に基づいてオプションが表示されます。

これらのリストには、Kubernetes クラスターで構成された Citrix ADM エージェントに関連付けられているサイトまたはインスタンスが表示されます。

d) [**Choose Net**work] で、ADM が仮想 IP アドレスを入力構成に自動的に割り当てるネットワークを選択します。

このリストには、[ネットワーク **] > [IPAM]** で作成したネットワークが表示されます。

e) [作成] をクリックします。

入力構成のデプロイ

`kubectl`を使用して Kubernetes から入力設定をデプロイするには、Kubernetes API、またはその他のツールを使用します。入力構成は、Citrix ADM から直接展開することもできます。

1. オーケストレーション **> Kubernetes > Ingress**es に移動します。
2. [追加] をクリックします。
3. [入力の作成] フィールドで、次の詳細を指定します。
   a) 入力の名前を指定します。
   b) [クラスタ] で、入力をデプロイする Kubernetes クラスタを選択します。
   c) リストから [クラスタネームスペース] を選択します。このフィールドには、指定した Kubernetes クラスターに存在する名前空間が一覧表示されます。
   d) 必要に応じて、[フロントエンド **IP** アドレスの自動割り当て] を選択します。
   e) リストから [入力プロトコル] を選択します。[**HTTPS**] を選択した場合は、**TLS** シークレットを指定します。

   このシークレットは、HTTPS 証明書と秘密キーを埋めている Kubernetes シークレットリソースを埋め込みます。

   HTTPS 入力には、Kubernetes クラスタで設定された TLS ベースのシークレットが必要です。サーバ証明書と証明書キーをそれぞれ含める`tls.crt`フィールドと`tls.key`フィールドを指定します。
   f) コンテンツルーティングの場合は、次の詳細を指定します。
      - **URL** パス -Kubernetes サービスおよびポートに関連付けられているパスを指定します。
      - **Kubernetes** サービス -目的のサービスを指定します。
      - ポート -サービスポートを指定します。

- **LB** メソッド -選択した Kubernetes サービスに対する優先ロードバランシング方式を選択します。

  選択したメソッドは、入力仕様を適切な注釈で更新します。たとえば、**ROUNDROBIN** メソッドを選択すると、Citrix の注釈は次のように表示されます。

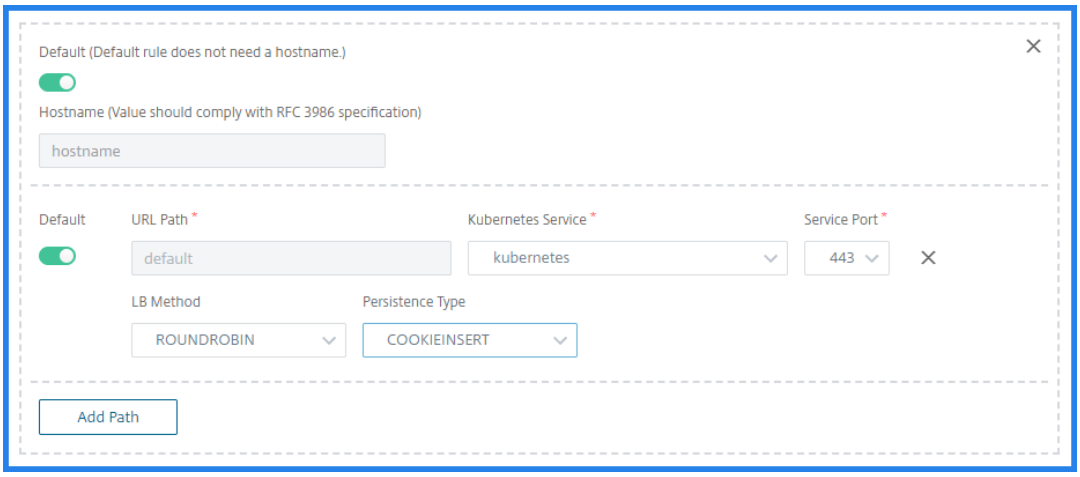
```
"lbmethod":"ROUNDROBIN"
<!--NeedCopy-->
```

- 持続性タイプ -選択した Kubernetes サービスに対して優先する負荷分散持続性タイプを選択します。

  選択した永続性タイプによって、入力スペシフィケーションが適切な注釈で更新されます。たとえば、「**COOKEEINSERT**」を選択すると、Citrix アノテーションは次のように表示されます。

```
"persistenceType":"COOKIEINSERT"
<!--NeedCopy-->
```

[**Add**] をクリックして、入力設定に URL パスとポートを追加します。



展開後、Ingress 設定は、次の内容に基づいてクライアントトラフィックを特定のサービスにリダイレクトします。

- 要求された URL パスとポート。
- 定義された LB メソッドと永続性タイプ。

> 注:
>
> 入力構成で使用される Kubernetes サービスは、NodePort タイプであることが予想されます。

g) オプションで、入力の説明を指定します。

h) [デプロイ] をクリックします。

展開する前に構成を確認する場合は、[入力スペックの生成] をクリックします。指定された入力設定が YAML 形式で表示されます。構成を確認したら、[**Deploy**] をクリックします。

> 注:
> Ingress 構成を使用して作成された仮想サーバーにライセンスを適用します。ライセンスを適用するには、次の手順に従います。
>
> 1. **[** システム**] > [**ライセンスと分析] の順に選択します。
> 2. [仮想サーバーライセンスの概要] で、**[**仮想サーバーの自動選択**]** を有効にします。

ADM 監査ログを使用してインフラストラクチャの管理と監視

May 7, 2021

Citrix ADM サービスを使用すると、ADM のすべてのイベントと、ADM で管理される ADC インスタンスで生成された syslog イベントを追跡できます。これらのメッセージは、インフラストラクチャの管理と監視に役立ちます。しかし、ログメッセージは確認する場合にのみ優れた情報源であり、ADM はログメッセージの確認方法を簡素化します。

フィルタを使用して、ADM syslog メッセージと監査ログメッセージを検索できます。フィルタは、結果を絞り込み、探しているものをリアルタイムで見つけるのに役立ちます。組み込みの Search ヘルプでは、ログをフィルタリングできます。ログメッセージを表示するもう 1 つの方法は、PDF、CSV、PNG、および JPEG 形式でエクスポートすることです。また、指定した電子メールアドレスにさまざまな間隔でこれらのレポートをエクスポートするようにスケジュールすることもできます。

ADM GUI から次のタイプのログメッセージを確認できます。

- ADC インスタンス関連の監査ログ
- ADM 関連の監査ログ
- アプリケーション監査ログ

ADC インスタンス関連の監査ログ

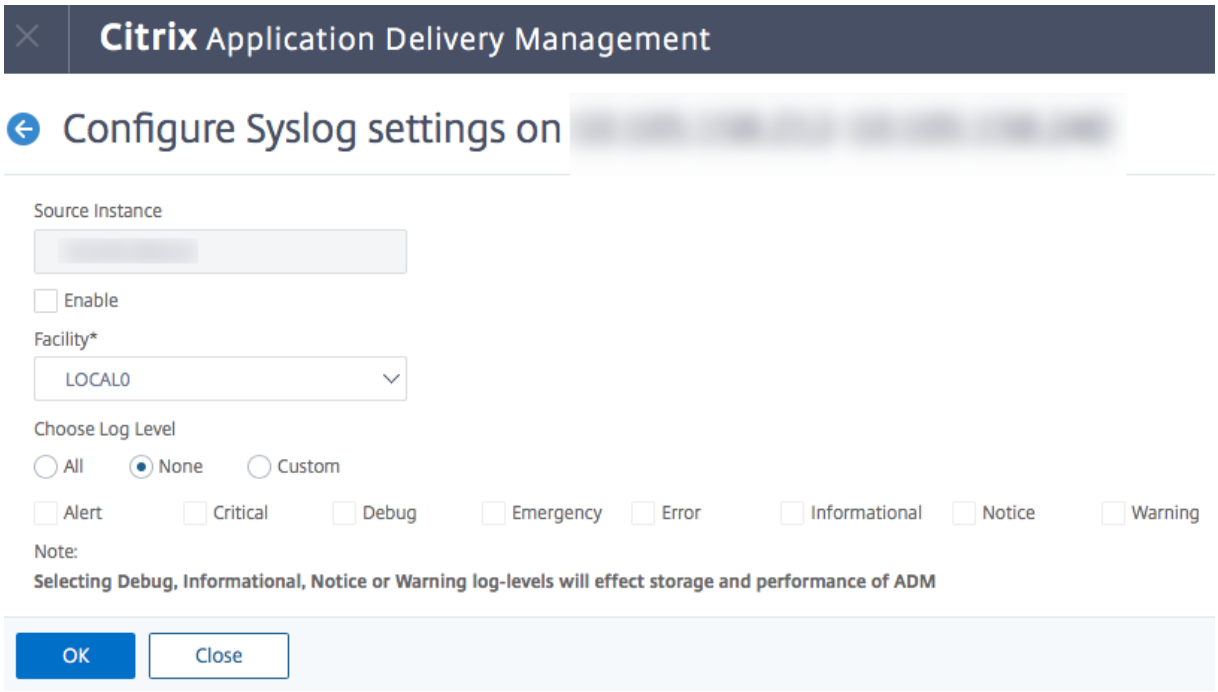
ADM からの ADC インスタンス関連の syslog メッセージを表示する前に、Citrix ADM サービスを Citrix ADC インスタンスの syslog サーバーとして構成してください。設定が完了すると、すべての syslog メッセージがインスタンスから ADM にリダイレクトされます。

ADM を **Syslog** サーバとして設定する

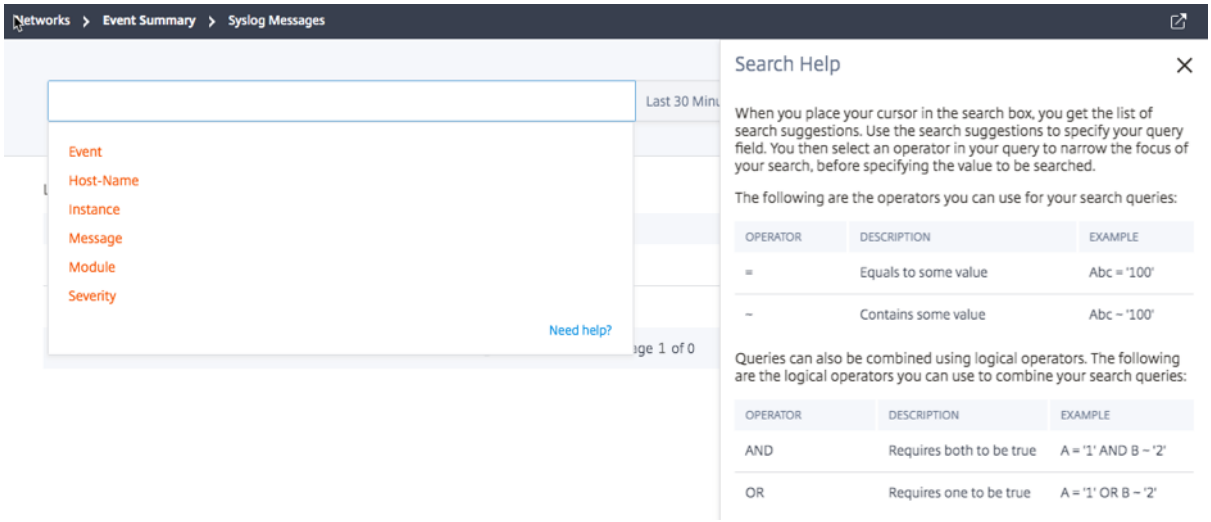
ADM を syslog サーバとして設定するには、次の手順を実行します。

1. ADM GUI から、[ネットワーク**] > [**インスタンス**]** に移動します。
2. Syslog メッセージを収集して Citrix ADM に表示する Citrix ADC インスタンスを選択します。
3. **[** アクションの選択] リストで、[**Syslog** の構成] を選択します。
4. [有効] をクリックします。
5. [**Facility**] ドロップダウンリストで、ローカルまたはユーザレベルのファシリティを選択します。

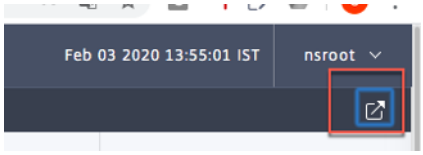
6. syslog メッセージに必要なログレベルを選択します。
7. [**OK]** をクリックします。



以下の手順では、Citrix ADC インスタンス内のすべての syslog コマンドを構成し、Citrix ADM が syslog メッセージの受信を開始します。メッセージを表示するには、[ネットワーク**] > [**イベント**] > [Syslog** メッセージ**]** に移動します。[ヘルプが必要ですか**?]** をクリックします。をクリックして、組み込みの検索ヘルプを開きます。詳しくは、「syslog メッセージの表示とエクスポート」を参照してください。



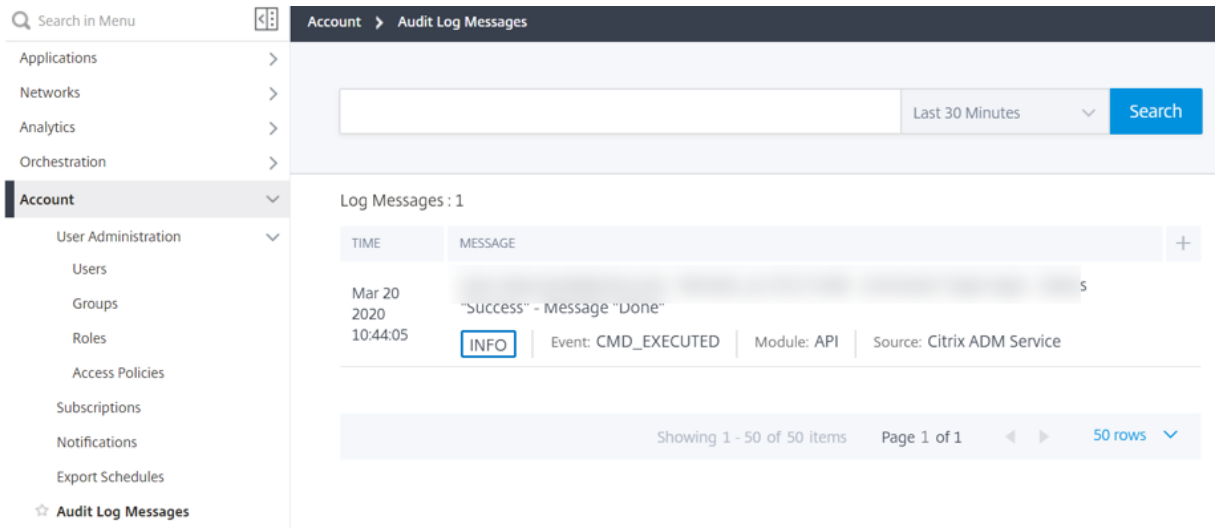
ログメッセージをエクスポートするには、右上隅にある矢印アイコンをクリックします。



次に、[今すぐエクスポート] または [エクスポートのスケジュール] をクリックします。詳しくは、「syslog メッセージのエクスポート」を参照してください。

ADM 関連の監査ログ

ADM は、事前設定されたルールに基づいて、上のすべてのイベントの監査ログメッセージを生成し、インフラストラクチャの健全性を監視できるようにします。ADM に存在するすべての監査ログメッセージを表示するには、[アカウント] → [監査ログメッセージ] に移動します。

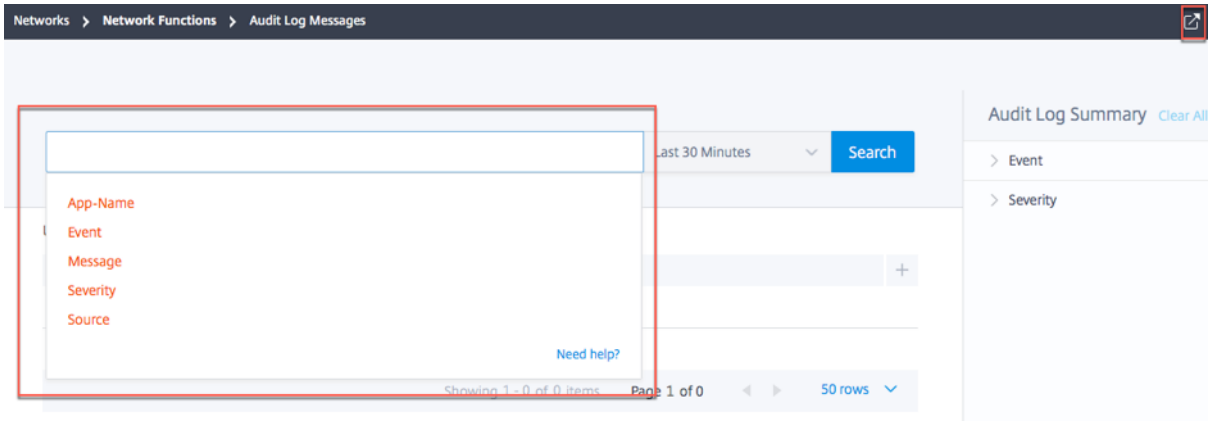


ログメッセージをエクスポートするには、右上隅にある矢印アイコンをクリックします。

アプリケーション関連の監査ログ

すべての ADM アプリケーションまたは特定のアプリケーションの監査ログメッセージを表示できます。

- ADM に存在するすべてのアプリケーションに関するすべての監査ログメッセージを表示するには、[ネットワーク] → [ネットワーク機能] → [監査] に移動します。



- ADM の特定のアプリケーションの監査ログメッセージを表示するには、[アプリケーション] > [ダッシュボード] **>** [仮想サーバーをダブルクリックする] **>** [監査ログ] に移動します。

> 注:
>
> ADM 監査ログメッセージを外部サーバに転送できます。詳しくは、「監査情報の表示」を参照してください。

Analytics

May 7, 2021

Citrix Application および Delivery Management（ADM）分析は、Citrix ADC インスタンスのデータのさまざまなインサイトを調べて、アプリケーションのパフォーマンスを記述、予測、改善するための簡単でスケーラブルな方法を提供します。Citrix ADM では、1 つ以上の分析機能を同時に使用できます。次の表は、Citrix ADM でサポートされているさまざまな分析機能について説明します。

分析機能	説明
Web Insight	Web Insight を使用すると、エンタープライズ Web アプリケーションを可視化し、IT 管理者はアプリケーションの統合されたリアルタイム監視を提供することで、Citrix ADC によって提供されるすべての Web アプリケーションを監視できます。
HDX Insight	HDX Insight は、Citrix ADC を通過する ICA トラフィックのエンドツーエンドの可視性を提供します。管理者は、HDX Insight を通じて、リアルタイムのクライアントとネットワークの遅延測定基準、履歴レポート、エンドツーエンドのパフォーマンスデータを確認し、パフォーマンスの問題をトラブルシューティングできます。

分析機能	説明
Gateway Insight	Gateway Insight は、Citrix Gateway Gateway へのログオン時に、アクセスモードに関係なく、すべてのユーザーが遭遇した障害を可視化します。
Security Insight	Security Insight は、アプリケーションのセキュリティ状況を判断し、是正処置を実施してアプリケーションを保護するための統一管理コンソールソリューションです。
SSL Insight	SSL Insight は、セキュアな Web トランザクション（HTTPS）を可視化し、IT 管理者は、セキュアな Web トランザクションのリアルタイムおよび履歴の統合監視を提供することで、Citrix ADC によって提供されるすべてのセキュアな Web アプリケーションを監視できます。

ライセンス要件

May 7, 2021

次の表に、Citrix Application Delivery Management（ADM）に関するさまざまな分析レポートを表示するために ADC インスタンスで必要なライセンス要件について説明します。

Citrix ADM Analytics の機能	ADC ライセンス要件
Web Insight	Citrix ADM Web Insight レポートは、すべての ADC ライセンスエディション（スタンダード/アドバンスド、プレミアム）でサポートされています。
HDX Insight	Citrix ADM に関する HDX Insight レポートは、アドバンスドエディション（1 時間未満のレポート）またはプレミアムエディション（レポート無制限の場合）のいずれかの ADC ライセンスでサポートされます。 **注:** 標準ライセンスエディションはサポートされていません。

Citrix ADM Analytics の機能	ADC ライセンス要件
Security Insight	Citrix ADM Security Insight レポートは、Premium Edition または Advanced Edition で App Firewall ライセンスでサポートされています。**注:** 標準ライセンスエディションおよびスタンドアロンアプリケーションファイアウォールライセンスはサポートされていません。
SSL Insight	Citrix ADM に関する SSL Insight レポートは、すべての ADC ライセンスエディション（標準/詳細/プレミアム）でサポートされています。
Gateway Insight	Citrix ADM に関する Gateway Insight レポートは、アドバンスドエディション（1 時間未満のレポート）またはプレミアムエディション（レポート無制限の場合）のいずれかの ADC ライセンスでサポートされます。**注:** 標準ライセンスエディションはサポートされていません。
TCP Insight	TCP Insight レポートは、すべての ADC ライセンスエディション (スタンダード/アドバンスド、プレミアム) でサポートされています。
Video Insight	Citrix ADM に関する Video Insight レポートは、ADC プレミアム（ADC-T 1000 シリーズ、VPX-T）エディションでサポートされています。
WAN Insight	Citrix ADM に関する WAN Insight レポートは、ADC SD-WAN WO エディション（WAN 最適化エディション）でサポートされています。

ログストリームの概要

May 7, 2021

Citrix ADC インスタンスは AppFlow レコードを生成し、データセンター内のすべてのアプリケーショントラフィックの中心的な制御ポイントです。**IPFIX** とログストリームは、これらの AppFlow レコードを Citrix ADC インスタンスから Citrix ADM に転送するプロトコルです。詳しくは、「AppFlow」を参照してください。

- **IPFIX** は、RFC 5101 で定義されたオープンインターネットエンジニアリングタスクフォース (IETF) 標準です。**IPFIX** は、一方向のデータフローに使用される信頼できない転送プロトコルである UDP プロトコルを使

用しています。IPFIX は UDP プロトコルを使用するため、IPFIX 標準に準拠すると、Citrix ADM でより多くのリソースを処理できます。

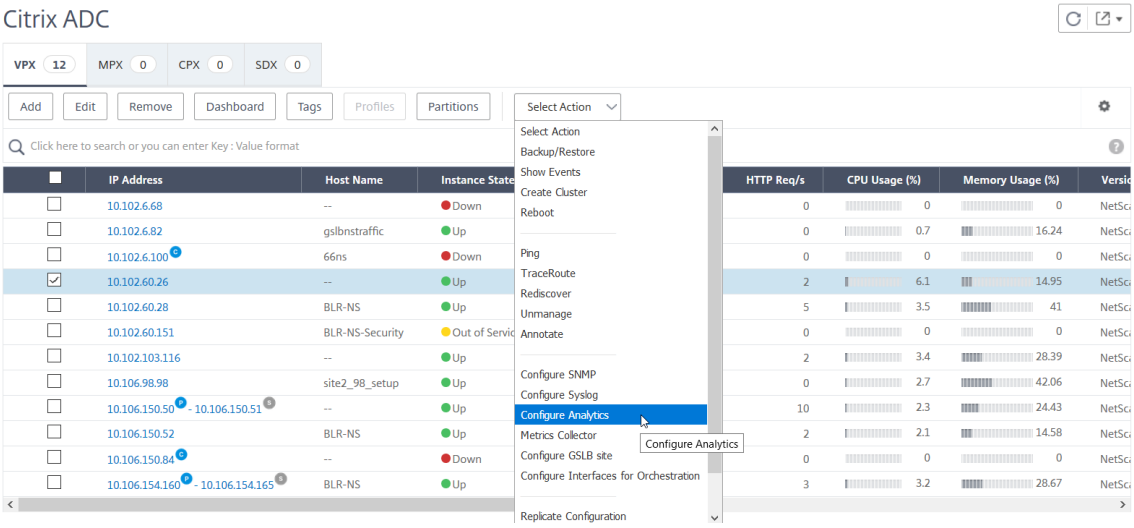
- ログストリームは、Citrix ADC インスタンスから Citrix ADM に効率的に分析ログデータを転送するためのトランスポートモードの 1 つとして使用される Citrix 所有のプロトコルです。**Logstream** は、信頼性の高い TCP プロトコルを使用し、データを処理するのにより少ないリソースを必要とします。

11.1 ビルド **47.14** と **11.1** ビルド **62.8** の間の **Citrix**ADC の場合、Web Insight（HTTP）を有効にするデフォルトの転送モードはログストリームであり、IPFIX は他のインサイトを有効にする唯一の転送モードです。**12.0** から最新バージョンの Citrix ADC では、転送モードとして ログストリームまたは **IPFIX** のいずれかを選択できます。

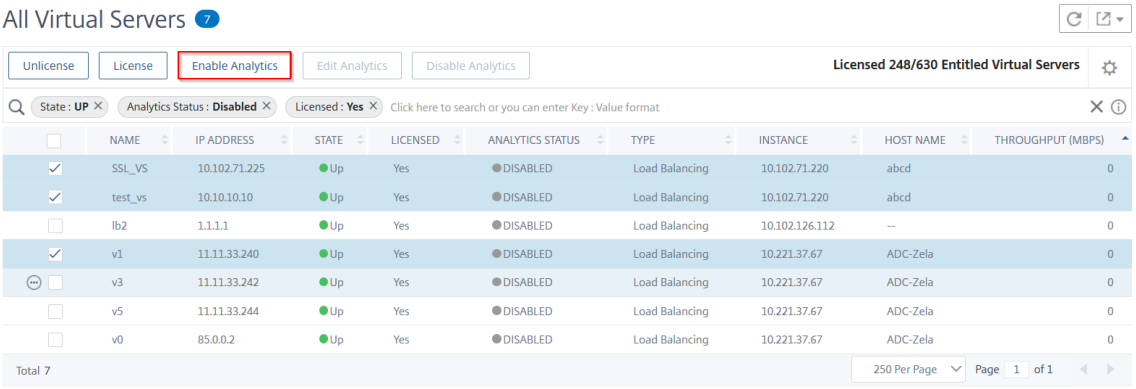
> 注
>
> Citrix ADM のバージョンとビルドは、Citrix ADC のバージョンおよびビルドと同じかそれ以上である必要があります。たとえば、Citrix ADC 12.1 ビルド 50.28/50.31 をインストールした場合は、Citrix ADM 12.1 ビルド 50.39 以降がインストールされていることを確認してください。

ログストリームを転送モードとして有効にする

1. [ネットワーク] > [インスタンス] に移動し、分析を有効にする ADC インスタンスを選択します。
2. **[** アクションの選択] リストから、[**Analytics** の設定] を選択します。



3. 仮想サーバーを選択し、[**Analytics** を有効にする] をクリックします。



4. **[Analytics** の有効化] ウィンドウで、次の操作を行います。

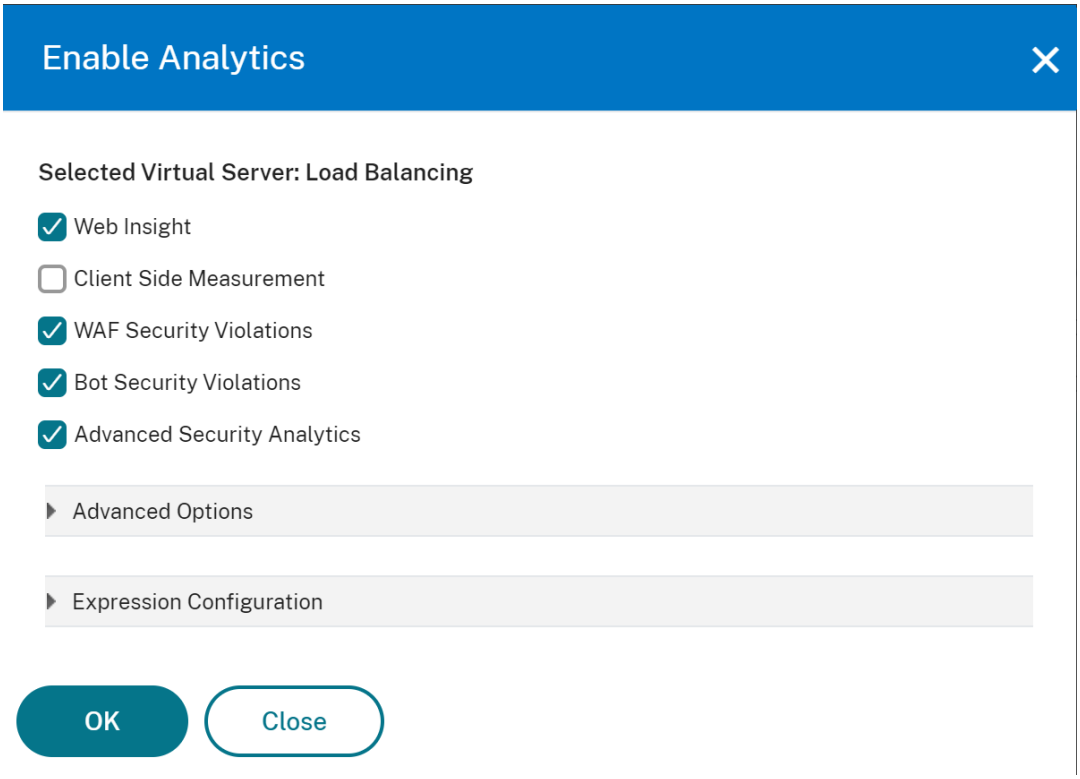
   a) インサイトの種類 (Web Insight または Security Insight) を選択します。

   b) 転送モードとして **Logstream** を選択します

   > 注
   >
   > **11.1** ビルド **47.14** と **11.1** ビルド **62.8** の間の **Citrix**ADC の場合、Web Insight（HTTP）を有効にするデフォルトの転送モードはログストリームであり、IPFIX は他のインサイトを有効にする唯一の転送モードです。**12.0** から最新バージョンの Citrix ADC では、転送モードとして ログストリームまたは **IPFIX** のいずれかを選択できます。

   c) 式はデフォルトで true です

   d) [**OK**] をクリックします。



注

- ライセンスされていない仮想サーバーを選択した場合、まずCitrix ADM はこれらの仮想サーバーのライセンスを取得してから、分析を有効にします

- 管理パーティションの場合、 **Web Insight** のみがサポートされます

- キャッシュリダイレクト、認証、GSLB などの仮想サーバーでは、分析を有効にできません。エラーメッセージが表示されます。

次の表では、**Logstream** をトランスポートモードとしてサポートする **Citrix** ADM の機能について説明します。

機能	**IPFIX**	**Logstream**
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	未サポート	•
CR Insight	•	•
IP レピュテーション	•	•
AppFirewall	•	•
クライアント側の測定	•	•
Syslog/Auditlog	•	•

分析のためのセルフサービス診断

May 7, 2021

Citrix ADM は、セルフサービス診断を実行して、次の分析機能について、管理対象インスタンスのライセンスと構成の問題を特定します。

- Web Insight
- HDX Insight

- Gateway Insight
- Security Insight
- ボットインサイト
- SSL Forward Proxy Analytics

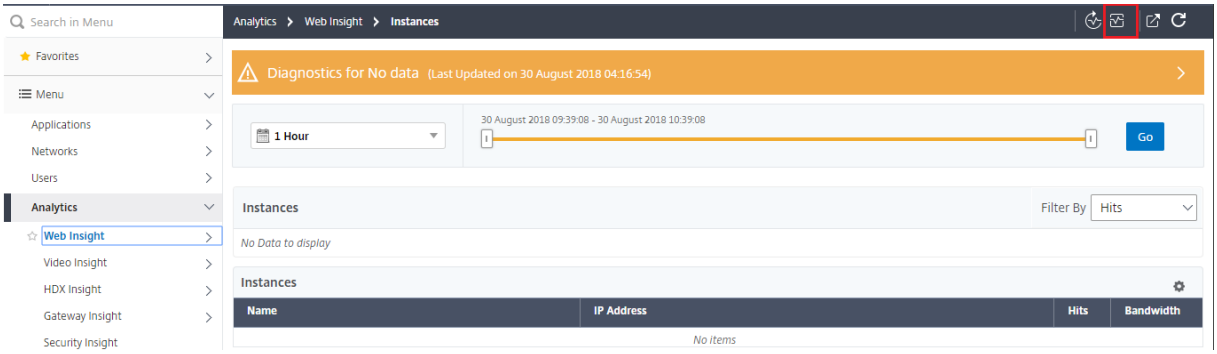
セルフサービス診断は 12 時間ごとに実行され、指定した分析機能ごとに問題が見つかった場合に診断レポートを生成します。診断レポートには、問題の発生源、問題の種類、および問題を解決するための是正措置が示されます。セルフサービス診断を使用すると、問題を迅速に特定してトラブルシューティングできます。

たとえば、AppFlow ポリシーが仮想サーバーにバインドされていない場合、または仮想サーバーにライセンスがない場合、Citrix ADM は Web Insight 監視に必要なデータを取得しません。セルフサービス診断によって問題が特定され、診断レポートが生成されます。診断レポートを表示して、問題をチェックし、修正処理を実行できます。

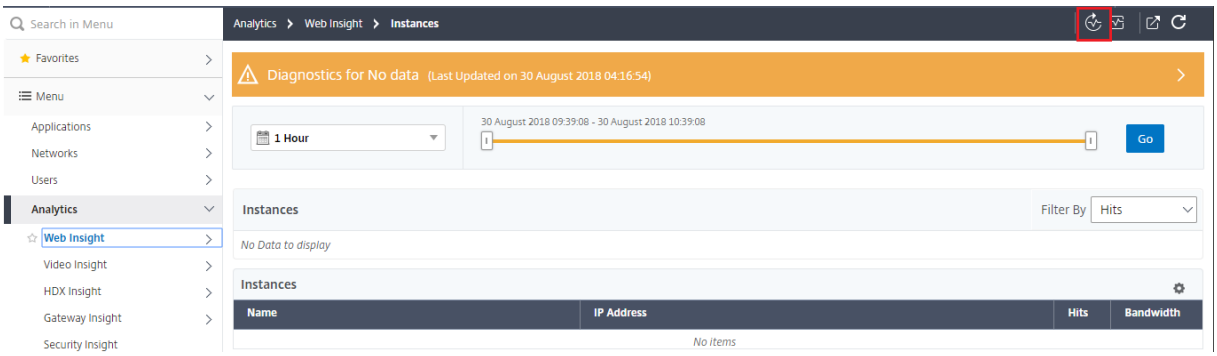
診断レポートを表示する

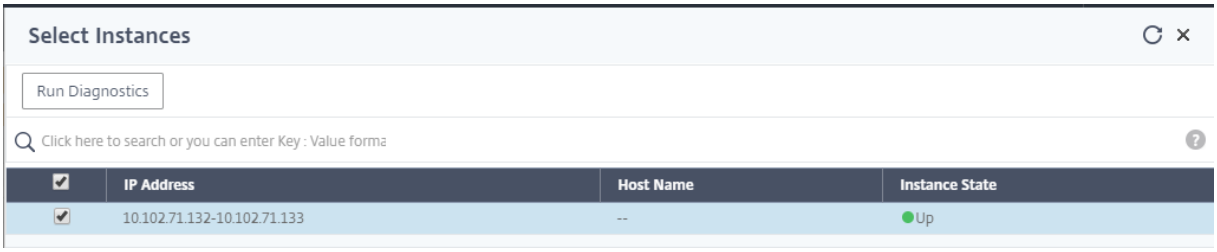
指定した分析機能の診断レポートを表示するには、Citrix ADM ダッシュボードでそれぞれの分析モードに移動します。

たとえば、Web Insight の診断レポートを表示するには、**[Analytics] > [Web Insight]** に移動します。[Web Insight] ページで、[診断の表示] アイコンを選択します。



問題をチェックする場合は、インスタント診断を実行することもできます。[診断の実行] をクリックします。インスタンスを選択し、[**Run Diagnostics**] を選択します。





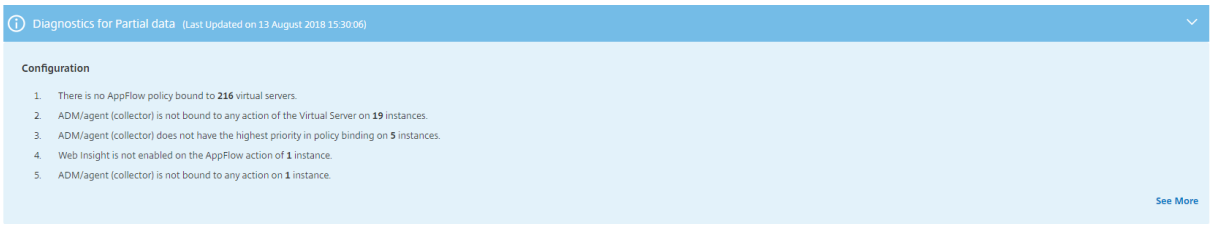
診断レポートの分析

セルフサービス診断では、問題の重要度に応じて、オレンジ色または青色の背景で診断レポートが表示されます。

オレンジ色の背景にある診断レポートは、青色の背景よりも重要度が高いことを示します。

たとえば、Citrix ADC インスタンスには 5 つの仮想サーバーが設定されています。仮想サーバーで AppFlow パラメーターを有効にしていない場合、Citrix ADM は分析用の Web Insight および Security Insight のトラフィックを受信しません。セルフサービス診断では、構成の問題が重大であることが特定されます。診断レポートは、Web Insight と Security Insight 機能でオレンジ色の背景で表示されます。

いずれかの仮想サーバーで AppFlow を有効にしている場合、Citrix ADM は分析用のデータを受信します。少なくとも 1 つの仮想サーバーが分析のためにトラフィックを送信しているため、青色の背景で診断レポートが表示されます。

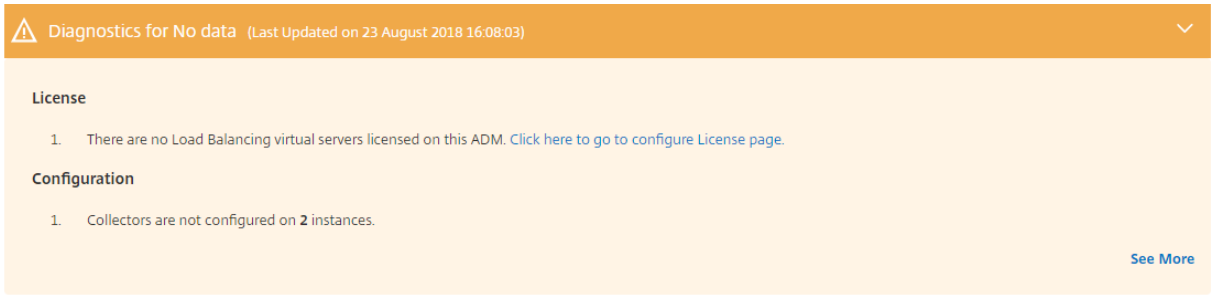


> 重要
>
> セルフサービス診断では、トラフィックフローはチェックされません。管理対象インスタンスの指定した分析機能に関連するライセンスまたは設定の問題のみをチェックします。仮想サーバーを通過するアクティブなトラフィックがないため、分析データが表示されないことがあります。

診断レポートには、概要ページと詳細情報ページがあります。

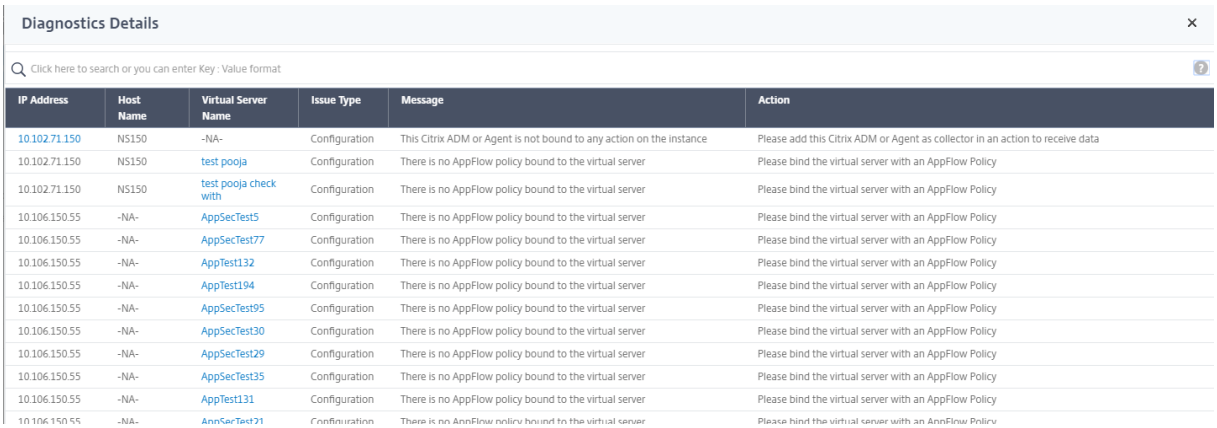
サマリページには、ライセンスの種類や構成に関する概要が表示されます。このページには、関連する設定ページに移動するハイパーリンクが含まれている場合があります。

たとえば、負荷分散仮想サーバのライセンスがない場合は、概要ページに [**System Licenses**] ページに移動するハイパーリンクが表示されます。

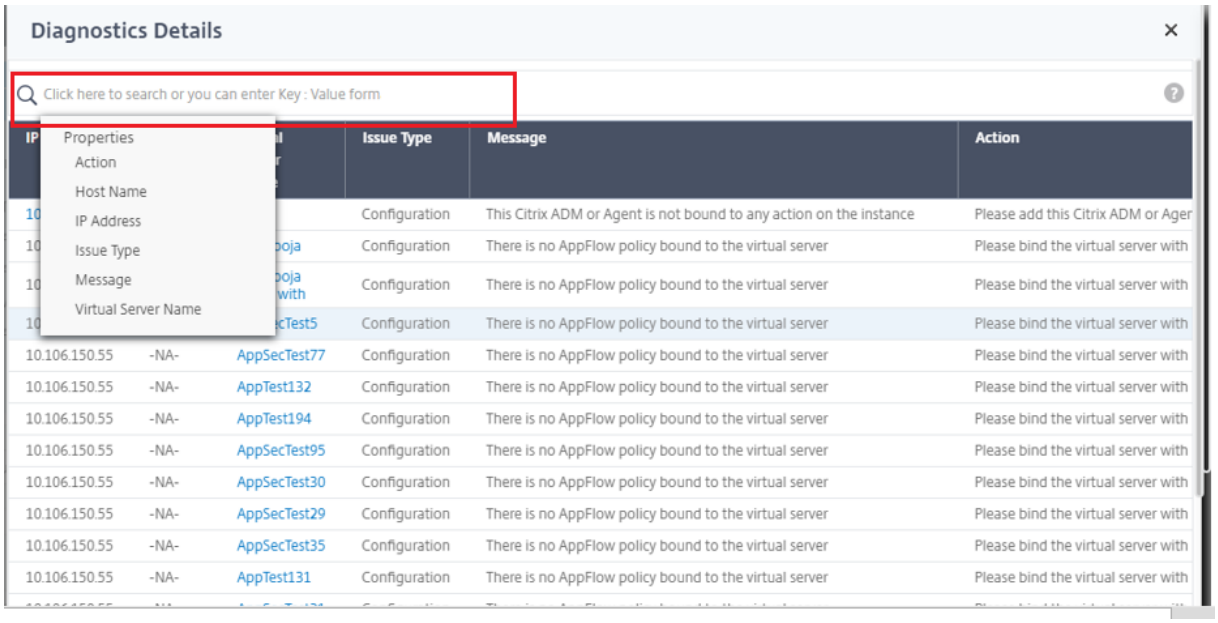


問題に関する詳細情報を表示するには、サマリページの [詳細を表示] をクリックします。

詳細情報ページには、問題に関する完全な情報と、実行する必要のある推奨アクションが表示されます。各問題に対するハイパーリンクをクリックして、管理対象インスタンスまたは仮想サーバーを構成できます。



アクション、ホスト名、IP アドレス、問題の種類などに基づいて問題を検索することもできます。



問題を解決したら、インスタント診断を実行して最新の診断レポートを生成する必要があります。

Web Insight

May 7, 2021

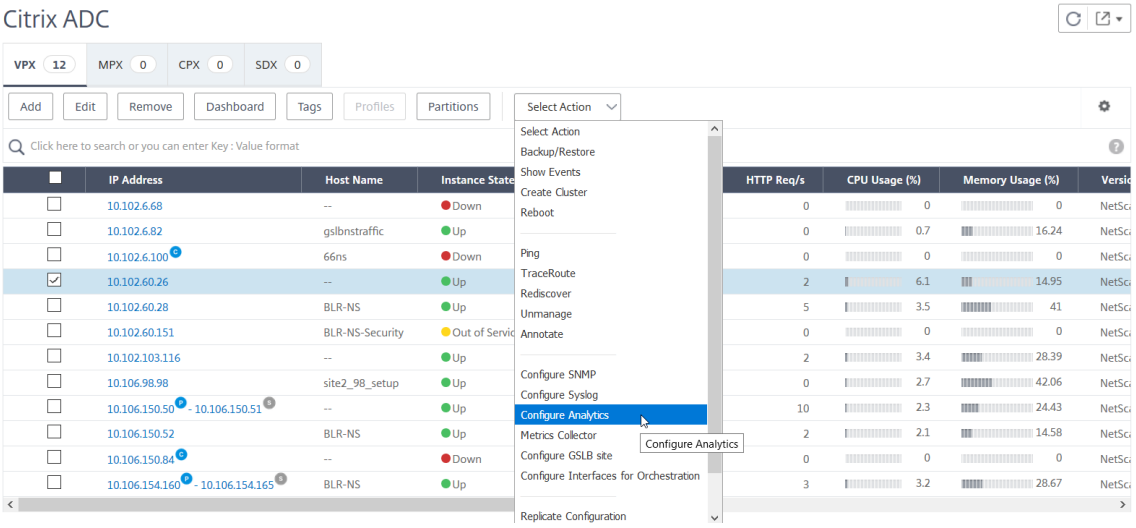
Web Insight を使用すると、管理者は Citrix ADC インスタンスによって提供されるすべての Web アプリケーションを監視できます。管理者は、Citrix ADC インスタンスからアプリケーションをリアルタイムで統合監視できます。Web Insight は、クライアントのネットワーク遅延やサーバーの応答時間などの重要な情報を提供します。これにより、アプリケーションのパフォーマンスを監視して改善できます。分析に使用されるデータは、Citrix ADC インスタンスによって処理される各 HTTP、HTTPS トランザクションから取得されます。分析データを使用すると、環境内の Citrix ADC インスタンス、アプリケーション、URL、クライアント、サーバーのパフォーマンスを分析できます。

Web Insight を使用してデータを表示できるユースケースを次に示します。

- SharePoint などのアプリケーションへのアクセス中に待機時間が長くなるクライアントのリスト
- 1 時間以内に最もヒットしたトップアプリケーション
- クライアントからアクセスされるアプリケーションと URL のリスト
- 特定のクライアントが使用するオペレーティングシステムとブラウザ
- 最もエラー関連の応答を送信するアプリケーションまたはサーバー
- 特定のクライアントでのアクセシビリティの問題
- 特定のクライアントからの少数のアプリケーションまたはすべてのアプリケーションにおけるアクセシビリティの問題
- 特定のクライアントとバックエンドサーバーからのアプリケーションのいくつかのページが遅い
- 特定のクライアントとバックエンドサーバーからアクセスすると、アプリケーションが遅くなる

選択したインスタンス上の特定の仮想サーバーに対して Web Insight を有効にして、Web アプリケーション上のトラフィックを監視できます。Web Insight 機能は、Citrix ADM の仮想サーバーの統計情報を提供します。Web Insight を有効にするには、次の手順に従います。

1. [ネットワーク] > [インスタンス] > [**Cit**rix ADC] に移動し、分析を有効にする Citrix ADC インスタンスを選択します。
2. **[** アクションの選択] リストから、[**Analytics** の設定] を選択します。



3. [仮想サーバーでの分析の設定] ページで、次の操作を行います。

   a) Web Insight を有効にする仮想サーバーを選択し、[アナリティクスの有効化] をクリックします

   [アナリティクスを有効にする] ウィンドウが表示されます。

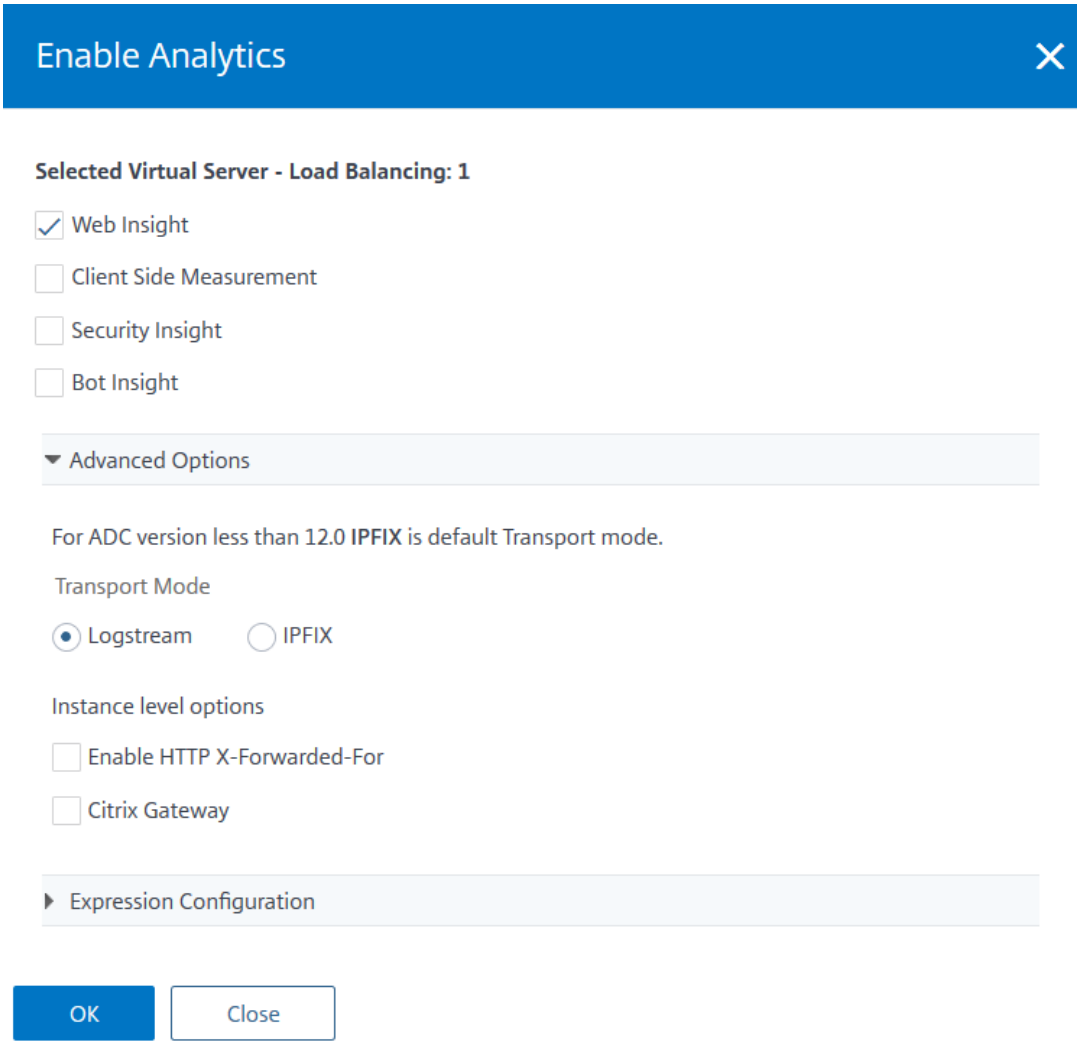
   b) **Web Insight** の選択

   c) [詳細オプション] で、トランスポートモードとして [ログストリーム] または [**IPFIX**] を選択します

   > 注
   >
   > Citrix ADC 12.0 以前の場合、**IPFIX** はトランスポートモードのデフォルトのオプションです。Citrix ADC 12.0 以降では、トランスポートモードとして［ログストリーム］または［**IPFIX** ］を選択できます。
   >
   > **IPFIX** および **Logstream** の詳細については、「ログストリームの概要」を参照してください。

   d) 式はデフォルトで true です

   e) ［**OK**］をクリックします。



Web アプリケーションの問題を分析する

管理者が特定する必要がある一般的な問題の 1 つは、遅延の問題です。管理者は、レイテンシーの問題がサーバーネットワーク、クライアントネットワーク、またはサーバーの応答時間にあるかどうかを調べる必要があります。Citrix ADM を使用して、[**Analytics**] > [**Web Insight**] に移動して、この情報を識別できます。

[**Analytics**] > [**Web Insight**] に移動すると、Web Insight が有効になっている Citrix ADC インスタンスが表示されます。IP アドレス、ホスト名、総ヒット数、帯域幅など、インスタンスの詳細情報を表示できます。

リストを使用して、インスタンスのインサイトを表示する期間を選択できます。

スライダを使用して時間をカスタマイズし、[**Go**] をクリックして結果を表示することもできます。

インスタンスのグラフまたは IP アドレスをクリックすると、インスタンスに関する詳細情報が表示されます。次のインサイトを表示できます。

- 総ヒット数

- 帯域幅
- アプリケーション
- ドメイン
- **URL**
- **HTTP** 要求メソッド
- **HTTP** 応答の状態
- クライアント
- サーバー
- オペレーティングシステム
- ユーザーエージェント

GUI でレポートを表示する **Web Insight** エンティティを選択することもできます。

1. [**Analytics**] > [**Web Insight] > [**設定**]** に移動します。
2. [**Analytics** データレコードログの構成] をクリックします。
3. [**Web Insight** レポートの設定**]** で、GUI でレポートを表示するエンティティを選択します。
4. [**OK**] をクリックします。

詳細な分析のためにドリルダウンするには、GUI の [Web Insight] の下の各インサイトカテゴリをクリックします。たとえば、構成済みサーバーの問題をチェックする場合は、次のようにします。

1. [**Analytics**] > [**Web Insight**] > [サーバー] に移動します。
2. [Servers] ページには、設定済みのすべてのサーバが表示されます。
3. グラフの IP アドレスをクリックします。テーブルから IP アドレスをクリックすることもできます。

   選択したサーバーの詳細なインサイトビューが表示されます。このビューでは、次のような複数のインサイトを確認できます。

   - サーバーが受信したヒットの合計数
   - 帯域幅
   - サーバー処理時間
   - サーバーネットワークの待ち時間
   - サーバ用に構成された仮想サーバ
   - サーバにアクセスするクライアントの合計数
   - サーバーによって提供される応答コードの合計数

ユースケース **1-**内部サーバーエラー

Web アプリケーションでユーザーにアクセスできないエラー 500 が発生しているシナリオを考えてみましょう。エラー 500（見つかりません）は、Web サーバー上の問題を示す HTTP 応答ステータスエラーですが、サーバーは問題を明示的に示しません。実際の問題を特定してドリルダウンするには、次の手順に従います。

1. [**Analytics**] > [**Web Insight**] > [応答ステータス] に移動します。

   ダッシュボードページが表示されます。ダッシュボードには、処理される HTTP トランザクションの成功と失敗の分析に使用できるメトリックが表示されます。

2. グラフで [見つかりません] をクリックします。
3. 下にスクロールして [サーバー**]** グラフを表示し、[フィルタ] リストから [サーバーネットワーク遅延] を選択します。

   グラフは、すべてのアプリケーションサーバーが Web アプリケーションの取得に問題を抱えていたため、Web サーバーの応答時間が長くなっていることを示しています。この問題は、Web サーバーがどのサーバーからの要求にも応答しないことが原因である可能性があります。

ユースケース **2-Web** アプリケーションへのアクセスが遅くなるユーザー

Web アプリケーションが 10 の異なる Web サーバーを介してホストされているシナリオを考えてみましょう。複数のユーザーが同時にアプリケーションにアクセスすると、1 人以上のユーザーがアプリケーションの速度が低下することがあります。管理者として、問題の根本原因を理解するのには、次のシナリオを分析する必要があります。

シナリオ **1-**サーバーの処理時間:

複数のリクエストが同時に 10 台の異なる Web サーバーにヒットした場合、リクエストのロードにかかる時間は、次の条件によって異なります。

- キュー内のリクエスト数。
- HTTP トランザクションを処理するために各要求によって消費される帯域幅。

  サーバーグラフは、サーバーによって処理された要求に対する各サーバーの処理時間を理解するのに役立ちます。同様に、アプリケーショングラフには、ヒット、応答時間、および HTTP トランザクションごとに消費された帯域幅が表示されます。

1. [**Analytics**] > [**Web Insight**] > [サーバー] に移動します。
2. グラフからサーバを選択します。
3. サーバーの処理時間を分析するには、[サーバーの処理時間] をクリックします。

シナリオ **2-**クライアントの待ち時間:

アプリケーションの応答時間と合計ヒット数が、アプリケーションのアクセスが遅くなる原因になる可能性があります。クライアントのネットワーク遅延を確認し、クライアントのネットワーク遅延のメトリックを分析できます。根本原因を分析するには:

1. [**Analytics**] > [**Web Insight**] > [クライアント] に移動します。
2. グラフからクライアントを選択します。
3. [クライアントネットワーク遅延] をクリックして、高遅延を分析します。

   この例では、管理者として、クライアントネットワークのレイテンシーが高いことを示すため、クライアントネットワークからの問題の根本原因を確認できます。

ユースケース **3-Web** アプリケーションへのアクセスが遅い

Windows ユーザー用の Web サーバーと Mac ユーザー用の Web サーバーがあり、ユーザーが Web アプリケーションへのアクセスが遅くなることを報告しているシナリオを考えてみましょう。管理者は、次のことを認識しています。

- Windows ユーザー用のコンテンツスイッチング仮想サーバーを構成しました。
- Mac ユーザー用のコンテンツスイッチング仮想サーバーを設定しました。
- Windows および Mac ユーザーに基づいて要求をリダイレクトするために、仮想サーバーにバインドされた関連サービスを構成しました。

Web アプリケーションの遅延問題の根本原因を分析するには:

1. [**Analytics**] > [**Web Insight**] > [アプリケーション] に移動します。
2. コンテンツスイッチング仮想サーバーを選択します。
   たとえば、イメージ内の`CSTOLBTarget`アプリケーションは、他の負荷分散仮想サーバーにバインドされたコンテンツスイッチング仮想サーバーです。
3. コンテンツスイッチング仮想サーバーをクリックして、他の負荷分散仮想サーバーを表示します。テーブル内のアプリケーション名をクリックすることもできます。

バインドされた負荷分散サーバーをクリックして、それらのアプリケーションの Web Insight の詳細を表示できます。

ブラウザとオペレーティングシステムのインサイトを分析する

Web Insight を使用すると、L7 遅延の問題を分離して、モバイルデバイスの使用状況を理解できます。管理者として、この洞察は、ユーザーベース全体でさまざまなオペレーティングシステムの導入状況を把握するのに役立ちます。

[**Analytics**] > [**Web Insight**] > [オペレーティングシステム] に移動して、ユーザーアクセスが遅くなる理由と、特定のブラウザー間の互換性がないことが原因かどうかを確認します。また、特定のクライアントで使用されているオペレーティングシステムや、アクセスされているブラウザーを確認することもできます。異なるブラウザ間でレンダリング時間を比較し、さらに特定のブラウザにドリルダウンして、そのブラウザで最も長いレンダリング時間に関連付けられているアプリケーションページを特定できます。

たとえば、**Google Chrome** を選択し、特定のアプリケーションの異なる URL ページの対応するレンダリング時間を確認できます。

高可用性モードでデプロイされた **Citrix ADC** インスタンス

Citrix ADM は、高可用性モードで展開された ADC インスタンスのレポートを提供します。高可用性モードのインスタンスの集約レポートは、すべての分析でサポートされます。

高可用性にあるインスタンスの名前をクリックすると、詳細を表示できます。

クラスターモードでデプロイされた **Citrix ADC** インスタンス

Citrix ADM は、クラスターモードで展開された ADC インスタンスのレポートを提供します。クラスターモードのインスタンスの集約レポートは、すべての分析でサポートされます。

CLIP ホスト名をクリックして、クラスターモードでデプロイされた ADC インスタンスに関するすべての詳細を表示することもできます。

> 注
>
> - Citrix ADM 12.1 build 503.x にアップグレードする前に以前に収集されたすべてのデータは、データが保持されるまで独立したレポートとして引き続き表示されます。
> - クラスタモードでデプロイされた ADC インスタンスの場合、オブザベーションドメイン ID/オブザベーションドメイン名は CLIP ホスト名と CLIP に置き換えられます。以前に収集されたすべてのデータは、引き続き観測ドメイン ID/観測ドメイン名を報告します。

Web Insight 地理マップの設定

Citrix ADM ジオマップ機能は、マップ上の異なる地理的場所にわたる Web アプリケーションの使用状況を表示します。管理者は、この情報を使用して、アプリケーション使用率の傾向を把握し、容量計画を立てることができます。

地域マップは、国、州、および都市に固有の次の指標に関する情報を提供します。

- 合計ヒット数：アプリケーションがアクセスされた合計回数。
- 帯域幅: クライアント要求の処理中に消費される総帯域幅
- 応答時間：クライアント要求への応答の送信に要した平均時間。

ジオマップは、次のようないくつかのユースケースに対処するために使用できる情報を提供します。

- アプリケーションにアクセスするクライアント数が最大であるリージョン
- 応答時間が最も高いリージョン
- 最も帯域幅を消費するリージョン

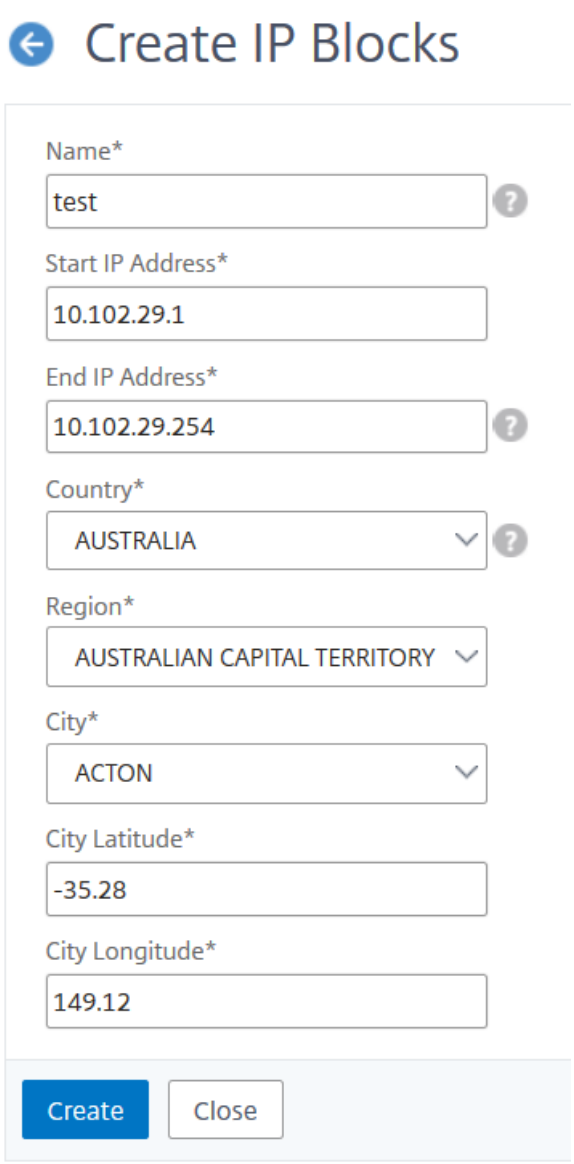
Citrix **ADM** では、**Web Insight** を有効にすると、プライベート IP アドレスまたはパブリック IP アドレスのジオマップが自動的に有効になります。

プライベート **IP** ブロックを作成する

Citrix ADM は、クライアントのプライベート IP アドレスが Citrix ADM サーバーに追加されると、クライアントの場所を認識できます。たとえば、クライアントの IP アドレスが A 市に関連付けられたプライベート IP アドレスブロックの範囲内にある場合、Citrix ADM はこのクライアントの A 市町からトラフィックが発信していることを認識します。

IP ブロックを作成するには、次の手順を実行します。

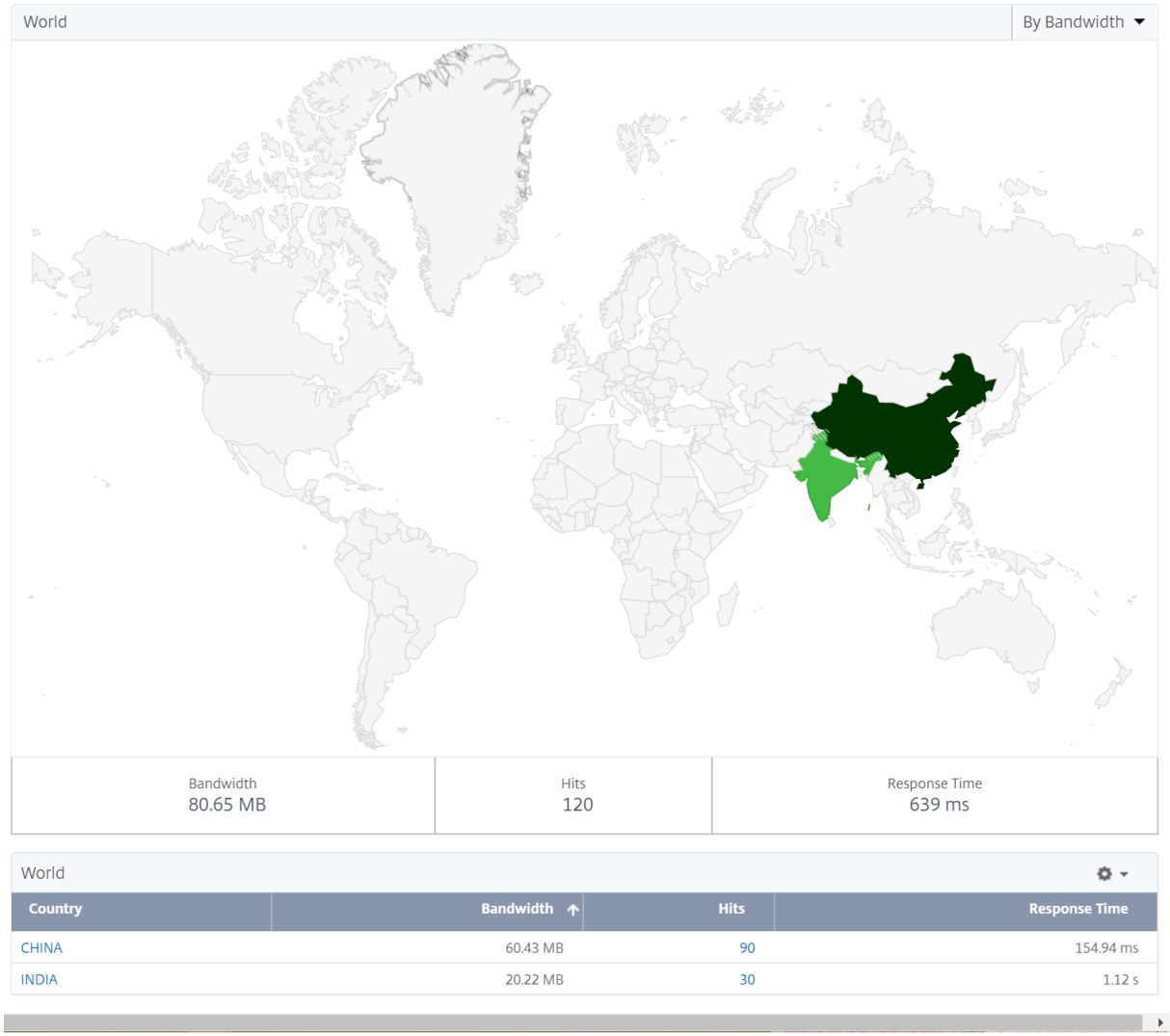
1. Citrix ADM で、[**Analytics**] > [設定] > [**IP** ブロック] の順に選択し、[追加] をクリックします。
2. **[IP** ブロックの作成] ページで、次のパラメータを指定します。
    - 名前。プライベート IP ブロックの名前を指定します。
    - 開始 **IP** アドレス。IP ブロックの最小の IP アドレス範囲を指定します。
    - 終了 **IP** アドレス。IP ブロックの最大の IP アドレス範囲を指定します。
    - 国。リストから国を選択します。
    - 地域。国に基づいて、地域は自動的に入力されますが、地域を選択できます。
    - 市。地域に基づいて、都市は自動入力されますが、都市を選択できます。
    - 都市の緯度と都市の経度。選択した都市に基づいて、緯度と経度が自動的に設定されます。
3. [**Create**] をクリックすると、作業が終了します。



パブリック **IP** ブロック

クライアントがパブリック IP アドレスを使用している場合、Citrix ADM はクライアントの場所を認識することもできます。Citrix ADM には組み込みの場所 CSV ファイルがあり、これはクライアントの IP アドレス範囲に基づいて場所と一致します。パブリック IP ブロックを使用する場合、唯一の要件は、[Configure Insight] ページから **[**地理的データ収集を有効にする] を有効にする必要があります。

> 注
>
> Citrix ADM では、特定の地理的場所のジオマップを表示するためにインターネット接続が必要です。GeoMap を.pdf、.png、または.jpg 形式でエクスポートするには、インターネット接続も必要です。



このダッシュボードのレポートをエクスポートするには、次の手順に従います。

このページのレポートをエクスポートするには、このページの右上にある エクスポートアイコンをクリックします。[エクスポート] ページでは、次のいずれかの操作を実行できます。

1. [今すぐエクスポート] タブを選択します。レポートを PDF、JPEG、PNG、または CSV 形式で表示して保存します。
2. [スケジュールエクスポート] タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、電子メールまたは余裕メッセージでレポートを送信する。

> 注
>
> - [毎週の繰り返し] を選択した場合は、レポートをスケジュールする平日を選択してください。
> - [毎月の繰り返し] を選択した場合は、レポートをスケジュールするすべての日をカンマで区切って入力します。

しきい値の構成

しきい値を作成し、しきい値が違反したときに通知を受け取ることができます。一般的な展開では、しきい値を次の値に設定できます。

- さまざまなアプリケーションメトリックの追跡
- プランニングの促進
- アプリケーションメトリック値が設定されたしきい値を超えた場合に通知を受け取る

しきい値を設定するには、次の手順を実行します。

1. [**Analytics**] > [設定**]** > [しきい値] に移動します。
2. [しきい値] ページで、[追加] をクリックします。

   「しきい値の作成」ページが表示されます。
3. 次の詳細を指定します。
   a) [名前]: イベントを作成するための名前を指定します。
   b) [トラフィックの種類]-リストから [WEB] を選択します。
   c) エンティティ -リストから、カテゴリまたはリソース・タイプを選択します。デフォルトでは、エンティティとして「アプリケーション」が選択されています。
   d) 参照キー -参照キーは、選択したトラフィックタイプとエンティティに基づいて自動的に生成されます。
   e) 期間 -リストから、エンティティを監視する時間間隔を選択します。エンティティは、1 時間、1 日、または 1 週間の期間を監視できます。
   f) [**Configure Rule**] セクションで、メトリック、必要なコンパレータを選択してルールを作成し、しきい値を指定します。
   g) ［通知の設定］セクションで、［しきい値の有効化］を選択し、アラートを取得するアラート・モードを選択します。
4. ［作成］をクリックします。

SSL Insight

May 7, 2021

SSL Insight は、セキュアな Web トランザクション（HTTPS）を可視化し、IT 管理者は、セキュアな Web トランザクションのリアルタイムおよび履歴の統合監視を提供することで、Citrix ADC によって提供されるすべてのセキュアな Web アプリケーションを監視できます。状態を把握することで管理者は以下の評価を行うことができます。

- 構成の変更がお客様の使用状況に与える影響を特定します。管理者は、SSLv3 をオフにするか、RC4-MD5 のような暗号を削除するなど、構成変更を行った場合の、クライアントへの影響を理解できます。そのためには、このプロトコルと暗号に関する履歴トランザクションデータを評価します。
- クライアントのパフォーマンスを定量化します。管理者は、使用された SSL 暗号/プロトコル、またはネゴシエートされた証明書に基づいて、アプリケーション応答時間への影響を把握できます。
- アプリケーションセキュリティ。セキュリティが低いプロトコル、暗号、または弱いキー強度で実行されているトランザクションがあるアプリケーションがあるかどうかを評価します。

ADC インスタンスで SSL Analytics を有効にすると、SSL トランザクションごとに SSL 統計が記録され、ログに記録されます。この統計により SSL フローの詳細が分かります。また、成功した接続はすべてログに記録され、Citrix Application Delivery Management（ADM）によって表示されます。

SSL Insight は、Citrix ADM Analytics によって表示される次の重要な情報を提供します。

- ネゴシエートされた SSL プロトコルバージョン
- ネゴシエートされた暗号と暗号強度
- 使用された証明書の署名ハッシュアルゴリズム
- 証明書の種類とサイズ
- SSL フロントエンドおよびバックエンドエラー

> 注
>
> SSL 接続が成功すると、SSL AppFlow ロギングはすべてのトランザクションの最後に発生します。

前提条件

- SSL Insight を構成する Citrix ADC インスタンスでは、Citrix ADC ソフトウェアリリース 11.1 51.21 以降が実行されている必要があります。11.1 51.21 を実行する ADC インスタンスで次のコマンドを実行して、SSL Insight トランスポートタイプとして **Logstream** を有効にします。

1. `enable ns mode ulfd`
2. `add ulfd server <IP Address of the ADM>`

   バージョン 12.0 以降を実行する ADC インスタンスの場合は、ADM から AppFlow を有効にしながら、トランスポートタイプとして **Logstream** を選択します。

- Citrix ADM のバージョンとビルドは、Citrix ADC のバージョンとビルドと同等かそれ以上である必要があります。たとえば、Citrix ADM 11.1 ビルド 61.7 をインストールしている場合は、Citrix ADC 11.1 ビルド 60.14 以前がインストールされていることを確認します。

SSL Insight の構成

次の要素を有効にした場合、SSL Insight メトリックスは Web Insight レポートに含まれます。

- 各 ADC インスタンスで Web Insight 用の AppFlow を有効にします。

- 各 ADC インスタンスで ULFD モードを有効にします。
- 各 ADC インスタンスで必要な AppFlow パラメーターを有効にします。

インサイトの有効化

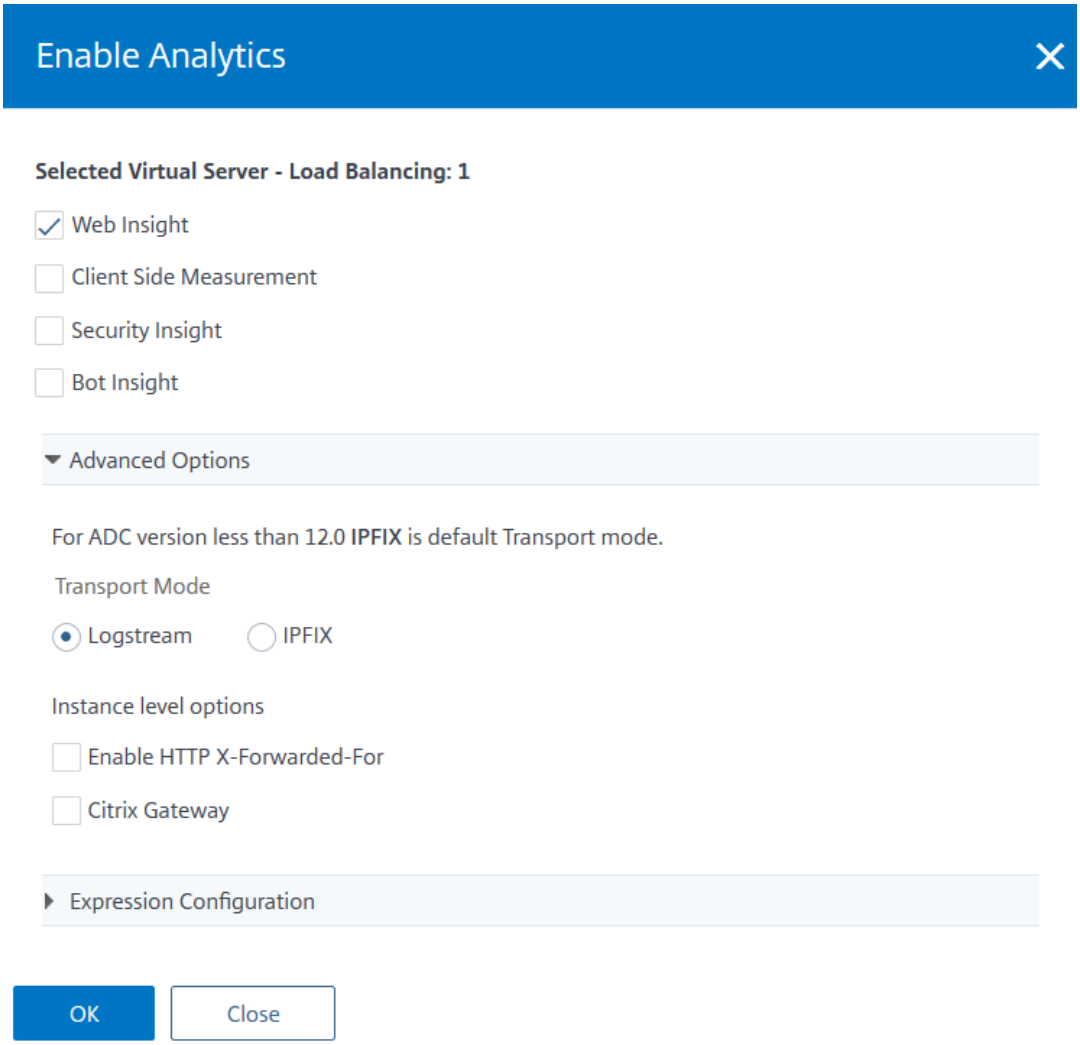
> 注
>
> AppFlow 機能は、Citrix ADM または各 ADC インスタンスから有効にできます。

Citrix ADM から **AppFlow** 機能を有効にする

1. [ネットワーク] > [インスタンス] に移動し、分析を有効にする ADC インスタンスを選択します。
2. **[** アクションの選択] リストから、[**Analytics** の設定] を選択します。
3. [仮想サーバーでの分析の設定] ページで、次の操作を行います。
   a) Web Insight を有効にする仮想サーバーを選択し、[アナリティクスの有効化] をクリックします

      [アナリティクスを有効にする] ウィンドウが表示されます。
   b) **Web Insight** の選択
   c) [詳細オプション] で、トランスポートモードとして [ログストリーム] または [**IPFIX**] を選択します

      > 注
      >
      > Citrix ADC 12.0 以前の場合、**IPFIX** はトランスポートモードのデフォルトのオプションです。Citrix ADC 12.0 以降では、トランスポートモードとして［ログストリーム］または［**IPFIX** ］を選択できます。
      >
      > **IPFIX** および **Logstream** の詳細については、「ログストリームの概要」を参照してください。
   d) 式はデフォルトで true です
   e) ［**OK**］をクリックします。



> 注
>
> 仮想サーバーの動作状態が［UP］以外の場合は、仮想サーバーでデータ収集を有効にできません。

ADC GUI を使用して **AppFlow** 機能を有効にする

ADC インスタンスの GUI で、[構成] > [システム] > [設定] に移動し、[高度な機能の構成] をクリックし、[**AppFlow**] を選択します。

ULFD モードの有効化

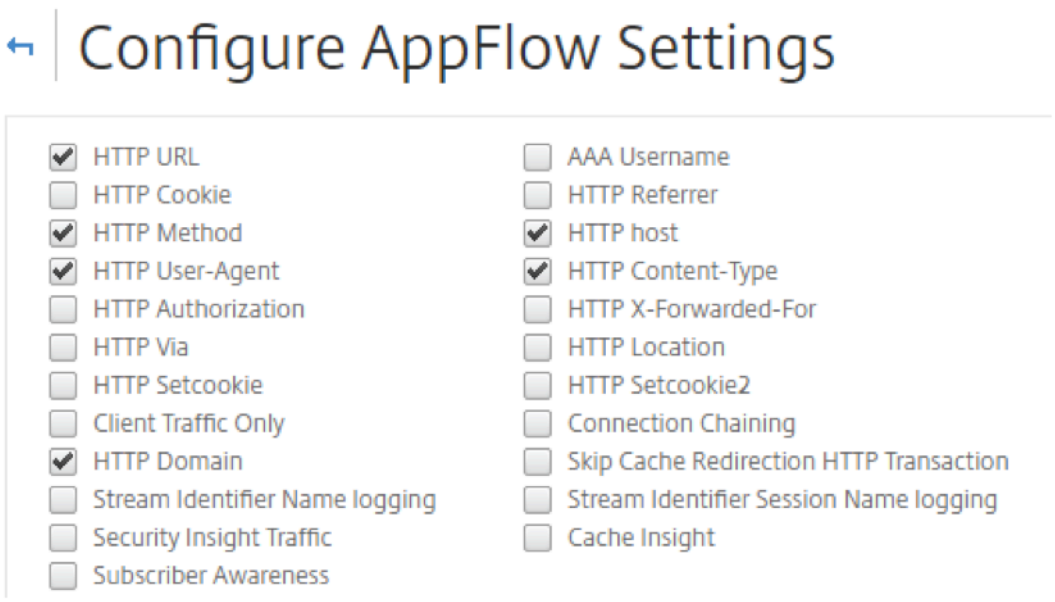
仮想サーバーが構成されている ADC インスタンスで ULFD モードを有効にすると、ULFD サーバーは分析データを ADC インスタンスから Citrix ADM にストリームします。

SSL Insight パラメータの有効化

各 ADC インスタンスで、いくつかの HTTP パラメータを有効にして、Citrix ADM で SSL Insight レコードを表示する必要があります。

ADC 構成ユーティリティから **SSL Insight** ・パラメータを有効にする

1. 「構成」>「システム」>「**AppFlow**」に移動し、「**AppFlow** 設定の変更」をクリックします。
2. [**HTTP** ドメイン]、**[HTTP** ホスト]、**[HTTP** メソッド]、**[HTTPURL]**、**[HTTP** ユーザーエージェント]、[**HTTP** コンテンツタイプ] のチェックボックスをオンにします。
3. [**OK**] をクリックします。



SSL Insight メトリックスの表示

Citrix ADM SSL Insight メトリックは、ADC インスタンスによって処理される SSL トランザクションのパフォーマンスの詳細ビューを提供します。クライアント、サーバー、またはアプリケーションレベルの SSL Insight メトリック、および SSL 成功トランザクションと失敗トランザクションのメトリックスを表示できます。これらのメトリックの助けを借りて、ADC HTTPS 設定と SSL 証明書の設定を分析および最適化し、パフォーマンスの問題を追跡できます。

> 注:
>
> グループを作成するときに、グループに役割を割り当てたり、グループへのアプリケーションレベルのアクセスを提供したり、ユーザーをグループに割り当てたりすることができます。Citrix ADM 分析では、仮想 IP アドレスベースの認証がサポートされるようになりました。ユーザーは、権限のあるアプリケーション（仮想サー

> バー）のみのすべての Insight のレポートを表示できるようになりました。グループとグループへのユーザーの割り当てについて詳しくは、Citrix ADM でのグループの構成を参照してください。

Citrix ADM で **SSL Insight** メトリックスを監視する

1. [分析] タブで、[Web Insight] に移動し、[クライアント]、[サーバー]、または [アプリケーション] ノードをクリックして、クライアント、サーバー、またはアプリケーションに関するメトリックスをそれぞれ表示します。
2. 左上のペインのメニューから、メトリックを表示する時間枠を選択します。期間は、スライダーを使用してカスタマイズできます。［**Go**］をクリックします。
3. SSL Insight のメトリックが円グラフとして表示されます。このグラフはクリックして詳細を確認できます。

   > 注
   >
   > 円グラフには、すべてのアプリケーション、クライアント、またはサーバーのメトリックが表示されます。

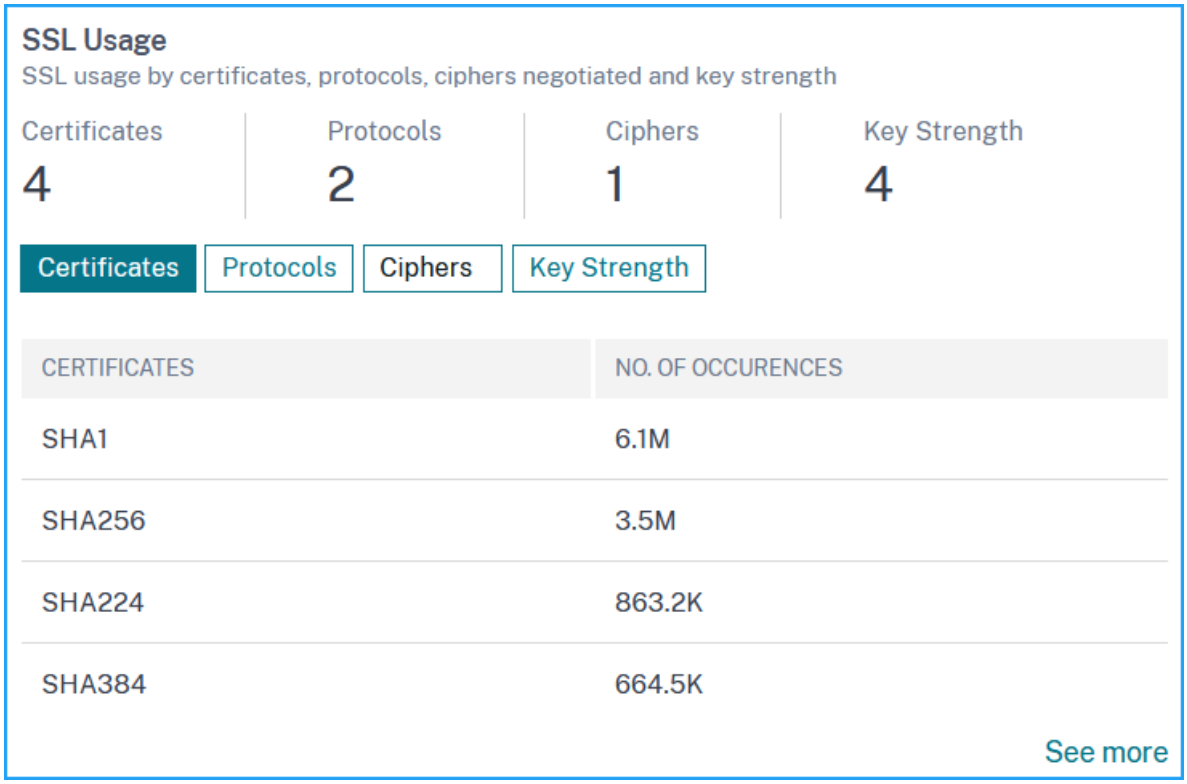
4. 特定のアプリケーション、クライアント、またはサーバーの詳細を表示するには、棒グラフで対応する値をクリックします。
5. 失敗した SSL トランザクションを表示するには、［SSL］セクションのラジオボタンを選択します。

ユースケース**:** アプリケーション、クライアント、またはサーバーの **SSL** トランザクションの概要を取得します

次のユースケースでは、Security Insight を使用して、アプリケーション、クライアント、およびサーバーのさまざまな SSL パラメーターの使用状況を評価し、セキュリティ対策を向上させる方法を説明します。

通信に SSL トランザクション（HTTPS）を使用している一連のアプリケーションがあり、SSL コンポーネントを監視するように Citrix ADM を構成しているとします。最も注意が必要なアプリケーションに特に注意を払えるように、アプリケーションを頻繁に確認する必要があります。SSL インサイトダッシュボードには、選択した期間、および選択した ADC デバイスについて、アプリケーションが使用するさまざまな SSL パラメータの概要が表示されます。それらは以下のようにリストされています。

- SSL 証明書
- SSL プロトコル
- ネゴシエートされた SSL 暗号
- SSL キーの強度
- SSL 障害 — フロントエンド
- SSL 障害 — バックエンド



次の例では、クライアントの一覧（IP アドレスで識別）とクライアントごとの SSL ヒット数を確認できます。また、右側では、すべてのクライアントの SSL パラメーターを表示できます。

クライアントの SSL 詳細を表示するには、棒グラフまたはグラフの下の表でクライアントを選択します。次の例では、選択したクライアントのトランザクションで SHA1 SSL 証明書と 4 つの主要なプロトコル（TSLv1.2、TSLv1.1、TSLv1、SSLv3）が使用されています。さまざまな強度の暗号がネゴシエートされたことが分かります。色付けによって SSL プロトコルの強度が示されており、弱い暗号と強い暗号に関する情報が分かります。

同様に、失敗した **SSL** トランザクションに関する情報を表示するには、**[SSL]** セクションのオプションボタンを選択します。SSL フロントエンドとバックエンドの障害は、2 つの円グラフで個別に表示されます。次の例では、主要なバックエンド SSL エラーはハンドシェイク失敗であり、主要なフロントエンド SSL エラーは無効なパラメータであることを確認できます。

HDX Insight

May 7, 2021

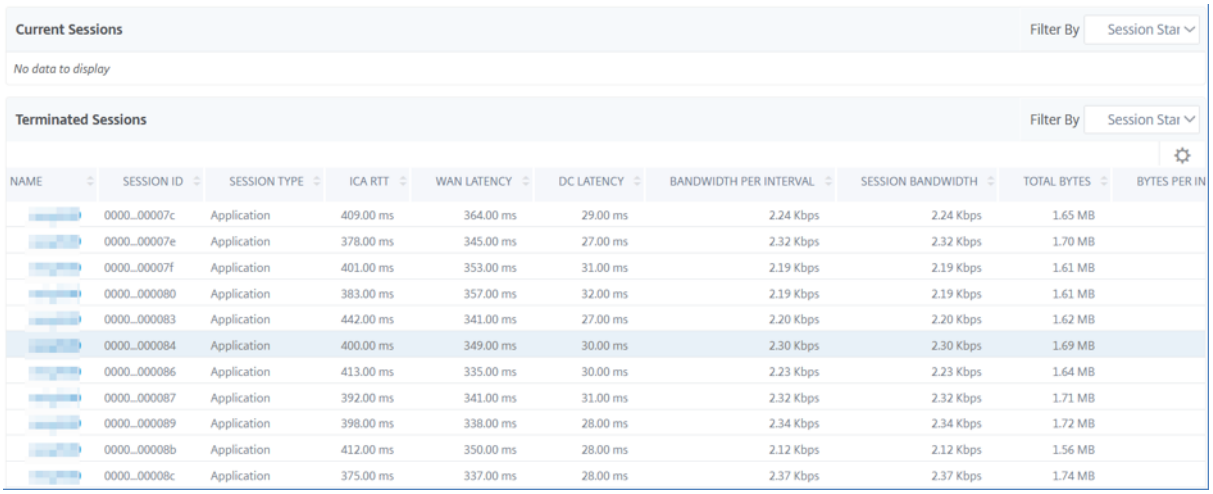
HDX Insight は、Citrix ADC を通過する Citrix Virtual Apps and Desktops への HDX トラフィックのエンドツーエンドの可視性を提供します。管理者は、HDX Insight を通じて、リアルタイムのクライアントとネットワークの遅延測定基準、履歴レポート、エンドツーエンドのパフォーマンスデータを確認し、パフォーマンスの問題をトラブルシューティングできます。リアルタイムの可視性と履歴データの両方を利用できるため、Citrix Application Delivery Management（ADM）はさまざまなユースケースをサポートできます。

データが表示されるようにするには、ADC Gateway 仮想サーバーで AppFlow を有効にする必要があります。AppFlow は、**IPFIX** プロトコルまたは **Logstream** メソッドによって配信できます。

> 注
>
> ICA ラウンドトリップ時間の計算を記録するには、次のポリシー設定を有効にします。
>
> - ICA 往復計算
> - ICA 往復計算間隔
> - アイドル接続の ICA 往復計算

個々のユーザーをクリックすると、選択した時間枠内でユーザーが行った各 HDX セッション（アクティブまたは終了済み）を確認できます。その他の情報には、セッション中に消費されるレイテンシー統計および帯域幅が含まれます。オーディオ、プリンタマッピング、クライアントドライブのマッピングなど、個々の仮想チャネルから帯域幅情報を取得することもできます。

また、アクティブなセッションと終了したすべてのユーザーの統合ビューを表示することもできます。



管理者として、このビューを使用すると、次のことが可能になります。

- 単一ペインビジュアライゼーションですべてのユーザーの詳細を表示する
- 各ユーザーを選択し、アクティブなセッションと終了したセッションの表示に関する複雑さを排除

> 注
>
> グループを作成するときに、グループにロールを割り当てたり、グループへのアプリケーションレベルのアクセスを提供したり、ユーザーをグループに割り当てることができます。Citrix ADM 分析では、仮想 IP アドレスベースの認証がサポートされるようになりました。ユーザーは、権限のあるアプリケーション（仮想サーバー）のみのすべての Insight のレポートを表示できるようになりました。グループとグループへのユーザーの割り当てについて詳しくは、Citrix ADM でのグループの構成を参照してください。

また、[**HDX Insight**] > [アプリケーション] に移動し、[起動期間] をクリックして、アプリケーションの起動にかかった時間を表示することもできます。[**HDX Insight] > [**ユーザー**]** に移動して、接続されているすべてのユーザーのユーザーエージェントを表示することもできます。

> 注:
>
> HDX Insight は、ソフトウェアバージョン 12.0 で実行される ADC インスタンスで構成された Admin パーティションをサポートしています。

次のシンクライアントが HDX Insight をサポートしています。

- WYSE Windows ベースのシンクライアント
- WYSE Linux ベースのシンクライアント
- WYSE Thinos ベースのシンクライアント
- 10ZiG Ubuntu ベースのシンクライアント

パフォーマンス遅延問題の根本原因の特定

シナリオ **1**

Citrix Virtual Apps and Desktops へのアクセス中に遅延が発生している

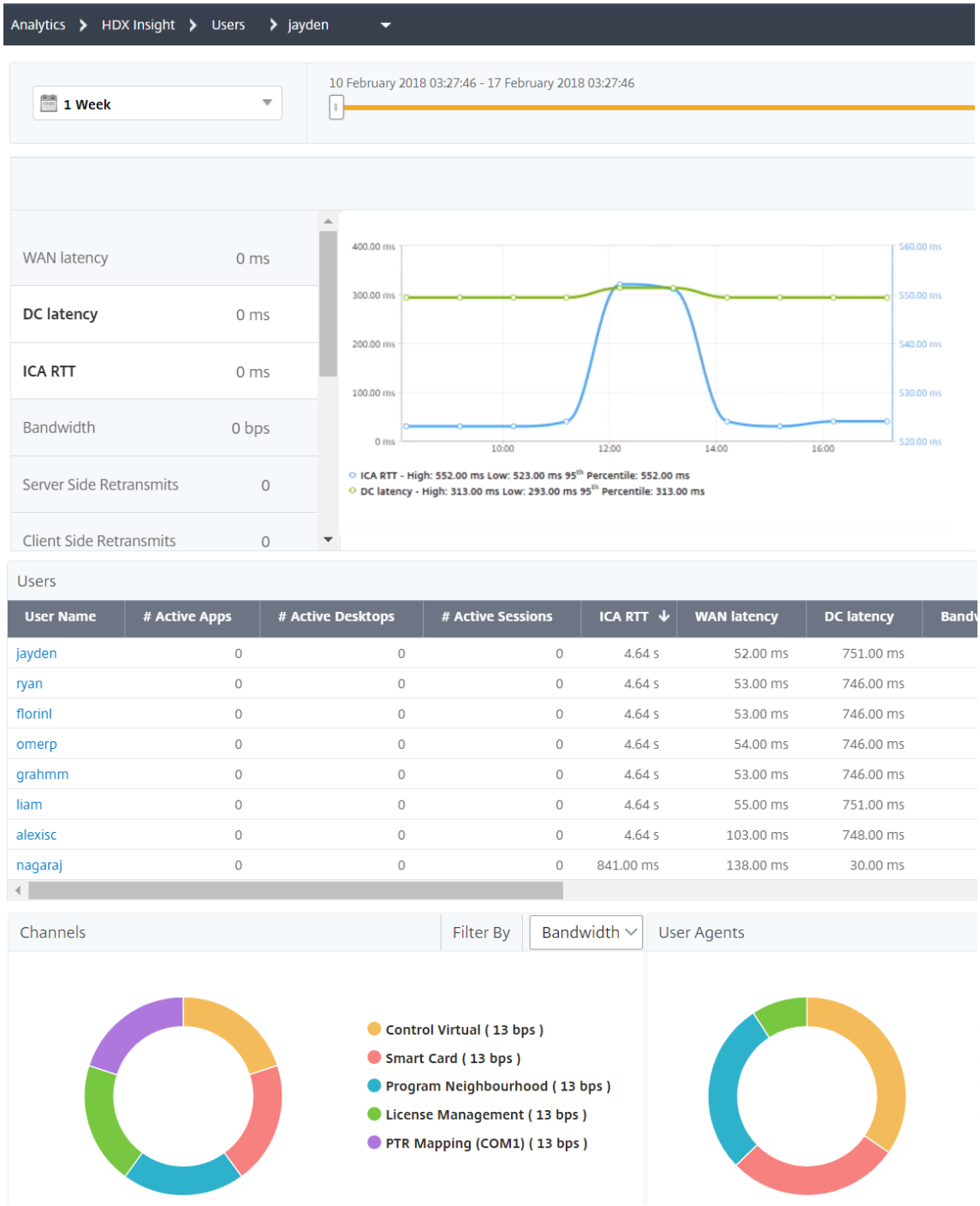
遅延の原因として考えられるのは、サーバーネットワークの遅延、サーバーネットワークに起因する ICA トラフィックの遅延、またはクライアントネットワークの遅延です。

問題の根本原因を特定するために、次の測定基準を分析します。

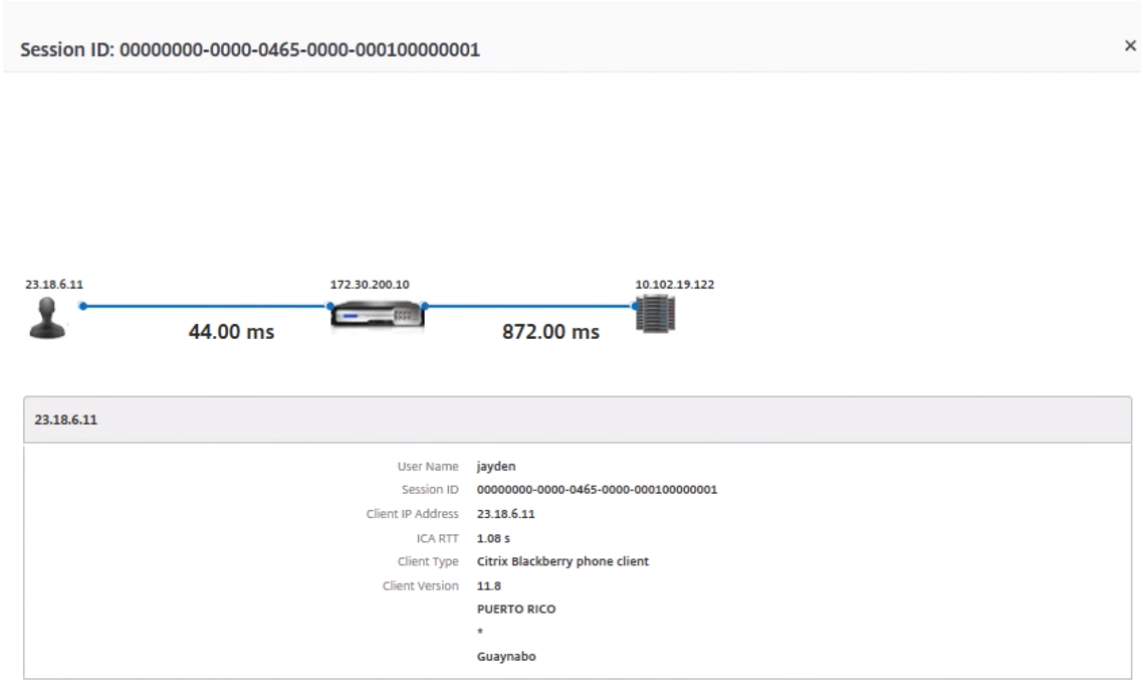
- WAN 遅延
- DC の遅延
- ホストの遅延

クライアント・メトリックを表示する手順は、次のとおりです。

1. [分析] タブで、[**HDX Insight**] > [ユーザー] に移動します。
2. 下にスクロールしてユーザー名を選択し、リストからピリオドを選択します。期間は、1 日、1 週間、1 か月にすることができます。また、データを表示する期間をカスタマイズすることもできます。
3. グラフには、指定した期間におけるユーザーの ICA RTT および DC レイテンシー値がグラフとして表示されます。



4. [現在のアプリケーションセッション] テーブルで、**RTT** 値の上にマウスを置き、ホスト遅延、DC 遅延、および WAN 遅延の値をメモします。
5. 「現在のアプリケーションセッション」(Current Application Sessions) テーブルで、ホップ図の記号をクリックして、クライアントとサーバー間の接続に関する情報 (遅延値を含む) を表示します。



概要**:**

この例では、**DC** 遅延は 751 ミリ秒、**WAN** 遅延は 52 ミリ秒、ホスト遅延は 6 秒です。これは、サーバネットワークによる平均遅延が原因で、ユーザが遅延していることを示します。

シナリオ **2**

Citrix Virtual Apps または **Desktops** でアプリケーションの起動中に遅延が発生しています

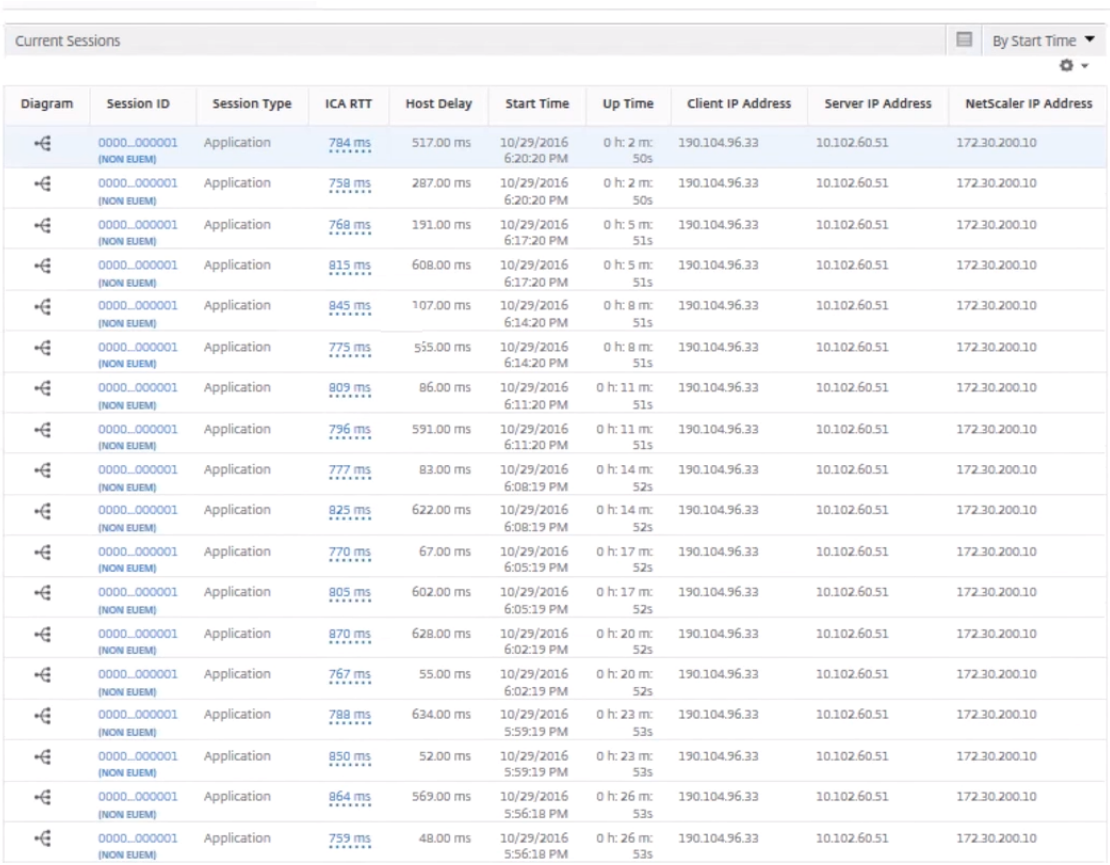
遅延の原因として考えられるのは、サーバーネットワークの遅延、サーバーネットワークに起因する ICA トラフィックの遅延、クライアントネットワークの遅延、またはアプリケーションの起動にかかる時間です。

問題の根本原因を特定するために、次の測定基準を分析します。

- WAN 遅延
- DC 遅延
- ホスト遅延

ユーザー・メトリックを表示する手順は、次のとおりです。

1. [分析] タブで、[**HDX Insight**] > [ユーザー] に移動します。
2. 下にスクロールし、ユーザー名をクリックします。
3. グラフに示されている該当するセッションの WAN の遅延、DC の遅延、RTT の値を書き留めます。
4. [現在のアプリケーションセッション] テーブルで、ホストの遅延が大きいことに注意してください。



Current Sessions — By Start Time

Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
	0000...000001 (NON EUEM)	Application	784 ms	517.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	758 ms	287.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	768 ms	191.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	815 ms	608.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	845 ms	107.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	775 ms	555.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	809 ms	86.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	796 ms	591.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	777 ms	83.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	825 ms	622.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	770 ms	67.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	805 ms	602.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	870 ms	628.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	767 ms	55.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	788 ms	634.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	850 ms	52.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	864 ms	569.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	759 ms	48.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10

概要:

この例では、**DC** 遅延は 1 ミリ秒、**WAN** 遅延は 12 ミリ秒ですが、ホスト遅延は 517 ミリ秒です。DC および WAN のレイテンシーが低い RTT が高いのは、ホストサーバ上のアプリケーションエラーを示します。

> 注:
>
> ソフトウェア 11.1 ビルド 51.21 以降を実行している Citrix ADM を使用している場合、HDX Insight は、WAN ジッタやサーバー側の再送信など、より多くのユーザーメトリックも表示されます。これらの指標を表示するには、[**Analytics**] > [**HDX Insight**] > [ユーザー] の順に選択し、ユーザー名を選択します。** ユーザーの測定基準がグラフの隣の表に表示されます。

HDX Insight の地情報マップ

Citrix ADM の地理マップ機能は、マップ上の異なる地理的場所における Web アプリケーションの使用状況を表示します。管理者は、この情報を使用して、アプリケーションの使用率の傾向を把握し、キャパシティプランニングを行うことができます。

地域マップは、国、州、および都市に固有の次の指標に関する情報を提供します。

- 合計ヒット数：アプリケーションがアクセスされた合計回数。
- 帯域幅: クライアント要求の処理中に消費される総帯域幅
- 応答時間：クライアント要求への応答の送信に要した平均時間。

地理マップは、次のようないくつかのユースケースに対処するために使用できる情報を提供します。

- アプリケーションにアクセスするクライアント数が最大であるリージョン
- 応答時間が最も高いリージョン
- 最も帯域幅を消費するリージョン

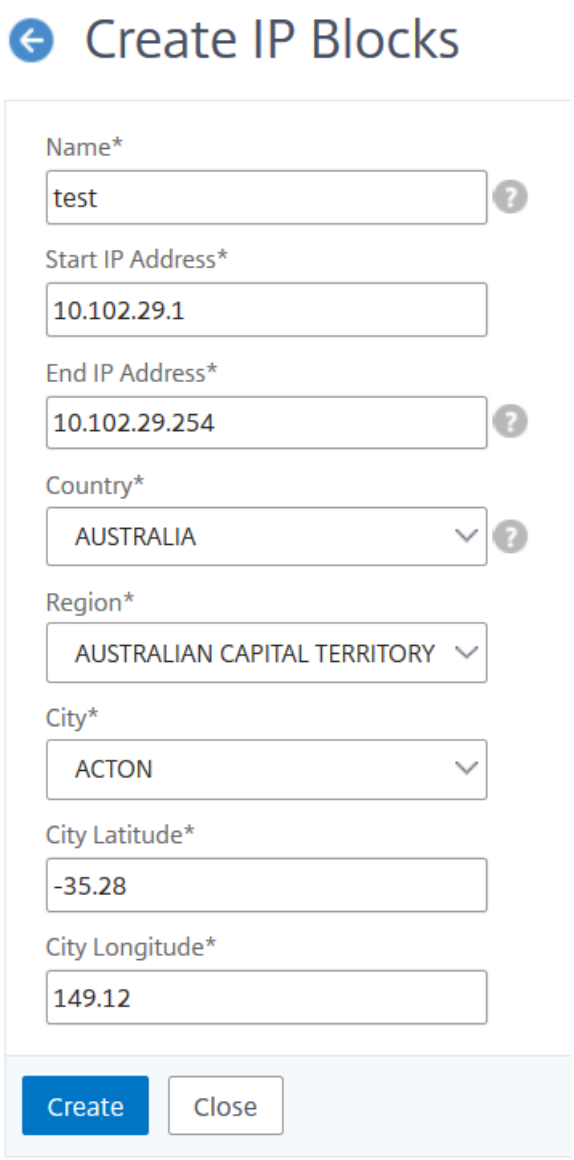
Citrix ADM では、**Web** インサイトを有効にすると、プライベート IP アドレスまたはパブリック IP アドレスのジオマップが自動的に有効になります。

プライベート **IP** ブロックを作成する

Citrix ADM は、クライアントのプライベート IP アドレスが Citrix ADM サーバーに追加されると、クライアントのロケーションを認識できます。たとえば、クライアントの IP アドレスが A 市に関連付けられたプライベート IP アドレスブロックの範囲内にある場合、Citrix ADM はこのクライアントの A 市町からトラフィックが発信していることを認識します。

IP ブロックを作成するには、次の手順を実行します。

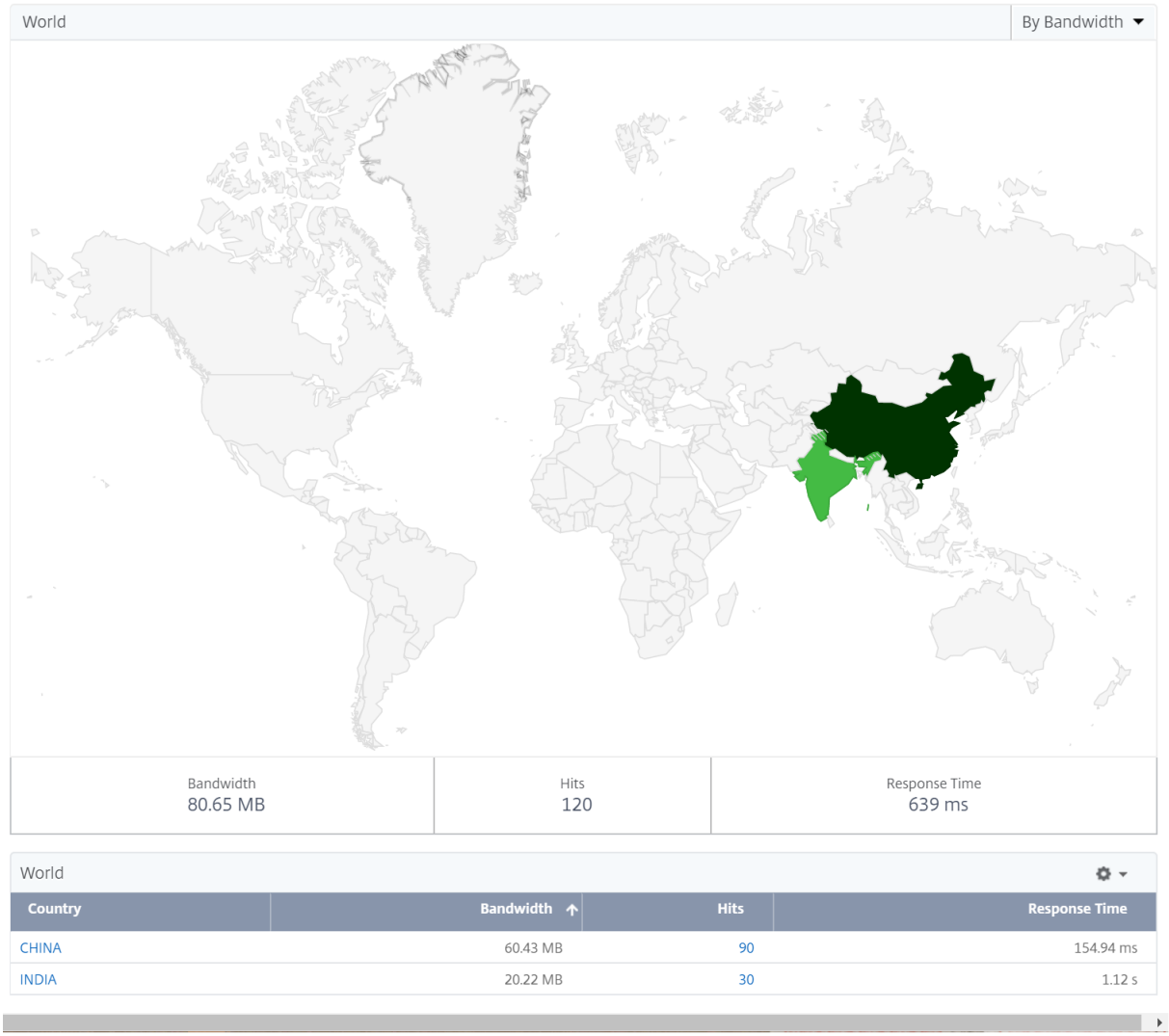
1. Citrix ADM で、[**Analytics**] > [設定] > [**IP** ブロック] の順に選択し、[追加] をクリックします。
2. **[IP** ブロックの作成] ページで、次のパラメータを指定します。
    - 名前。プライベート IP ブロックの名前を指定します。
    - 開始 **IP** アドレス。IP ブロックの最小の IP アドレス範囲を指定します。
    - 終了 **IP** アドレス。IP ブロックの最大の IP アドレス範囲を指定します。
    - 国。リストから国を選択します。
    - 地域。国に基づいて、地域は自動的に入力されますが、地域を選択できます。
    - 市。地域に基づいて、都市は自動入力されますが、都市を選択できます。
    - 都市の緯度と都市の経度。選択した都市に基づいて、緯度と経度が自動的に設定されます。
3. [**Create**] をクリックすると、作業が終了します。



パブリック **IP** ブロック

クライアントがパブリック IP アドレスを使用している場合、Citrix ADM はクライアントの場所を認識することもできます。Citrix ADM には組み込みの場所 CSV ファイルがあり、これはクライアントの IP アドレス範囲に基づいて場所と一致します。パブリック IP ブロックを使用するには、[Insight の設定] ページから **[**地理的データ収集を有効にする] を有効にする必要があります。

> 注
>
> Citrix ADM では、特定の地理的場所のジオマップを表示するためにインターネット接続が必要です。GeoMap を.pdf、.png、または.jpg 形式でエクスポートするには、インターネット接続も必要です。



このダッシュボードのレポートをエクスポートするには、次の手順に従います。

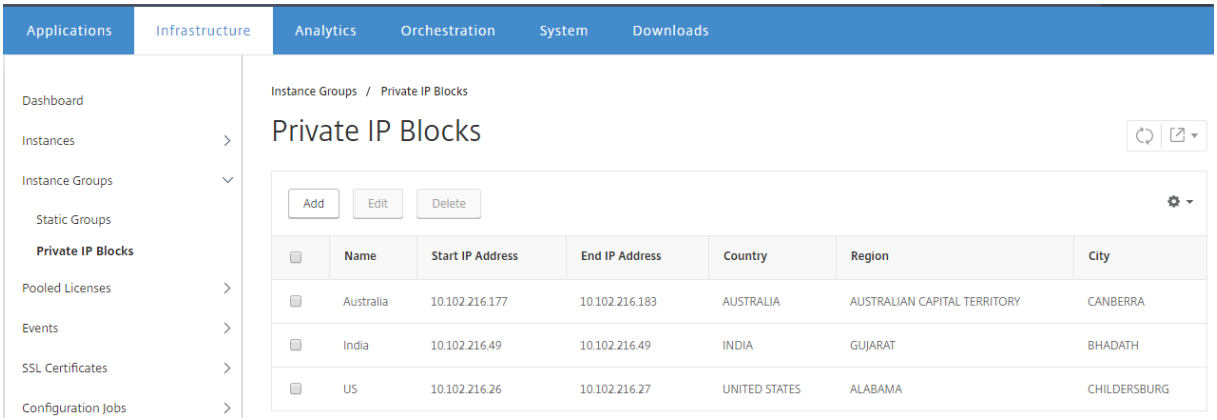
このページのレポートをエクスポートするには、このページの右上にある エクスポートアイコンをクリックします。[エクスポート] ページでは、次のいずれかの操作を実行できます。

1. [今すぐエクスポート] タブを選択します。レポートを PDF、JPEG、PNG、または CSV 形式で表示して保存します。
2. [スケジュールエクスポート] タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、電子メールまたは余裕メッセージでレポートを送信する。

> 注
>
> - [毎週の繰り返し] を選択した場合は、レポートをスケジュールする平日を選択してください。
> - [毎月の繰り返し] を選択した場合は、レポートをスケジュールするすべての日をカンマで区切って入力します。

データセンターの **geomap** を設定するには、次の手順に従います。

[ネットワーク] タブで、[サイト] > [プライベート **IP** ブロック] の順に選択し、特定の場所のジオマップを構成します。



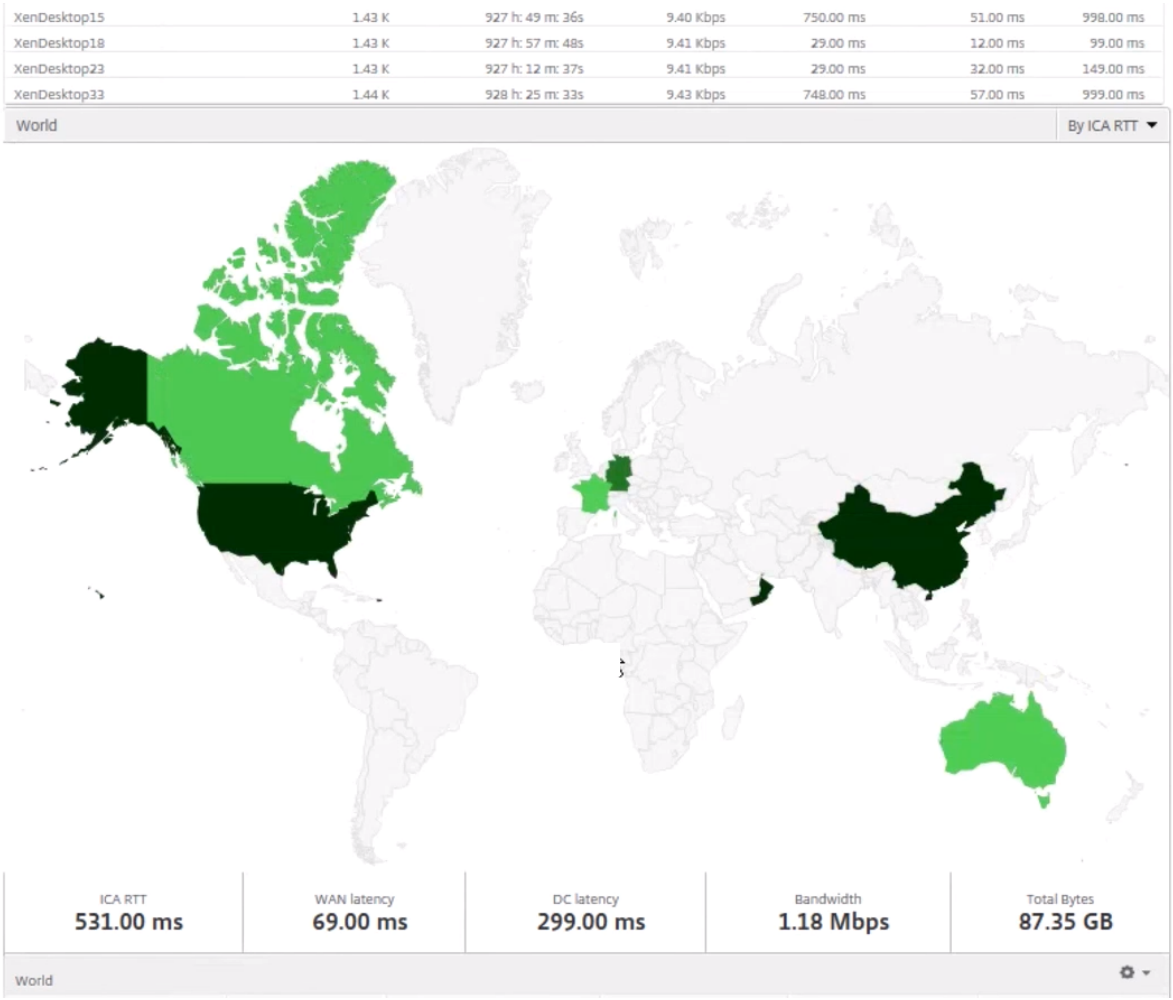
使用例

このシナリオでは 2 つの支店を持つ ABC という名前の企業を扱います。ABC はサンタクララとインドにオフィスを構えています。

サンタクララのユーザーは、SClara.x.com の ADC ゲートウェイアプライアンスを使用して VPN トラフィックにアクセスします。インドのユーザーは、India.x.com の ADC Gateway アプライアンスを使用して VPN トラフィックにアクセスします。

サンタクララでは、午前 10 時から午後 5 時などの特定の時間帯に SClara.x.com に接続し、VPN トラフィックにアクセスします。ほとんどのユーザーは同じ ADC Gateway にアクセスするため、VPN への接続に遅延が生じる。そのため、Sclara.x.com ではなく India.x.com に接続するユーザーもいる。

トラフィックを分析する ADC 管理者は、地理マップ機能を使用して、サンタクララオフィスのトラフィックを表示できます。マップは、サンタクララオフィスでの応答時間が高いことを示しています。これは、サンタクララオフィスには、ユーザーが VPN トラフィックにアクセスできる ADC ゲートウェイアプライアンスが 1 つしかないためです。したがって、管理者は、別の ADC ゲートウェイをインストールして、VPN にアクセスするための 2 つのローカル ADC ゲートウェイアプライアンスをユーザに割り当てることができます。



制限事項

ADC インスタンスに Advanced ライセンスがある場合、分析データが収集されるのは 1 時間だけであるため、Citrix ADM for HDX Insight に設定されたしきい値はトリガーされません。

このダッシュボードのレポートをエクスポートするには、次の手順に従います。

このページのレポートをエクスポートするには、このページの右上にある エクスポートアイコンをクリックします。[エクスポート] ページでは、次のいずれかの操作を実行できます。

1. [今すぐエクスポート] タブを選択します。レポートを PDF、JPEG、PNG、または CSV 形式で表示して保存します。
2. [スケジュールエクスポート] タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、電子メールまたは余裕メッセージでレポートを送信する。

> 注
>
> - [毎週の繰り返し] を選択した場合は、レポートをスケジュールする平日を選択してください。

> - [毎月の繰り返し] を選択した場合は、レポートをスケジュールするすべての日をカンマで区切って入力します。

HDX Insight データ収集を有効にする

May 7, 2021

HDX Insight を使用すると、管理者は Citrix ADC または Citrix SD-WAN アプライアンスを通過する ICA トラフィックをエンドツーエンドで可視化することで、優れたユーザーエクスペリエンスを提供できます。

HDX Insight は、ネットワーク、仮想デスクトップ、アプリケーション、アプリケーションファブリックに対して、魅力的で強力なビジネスインテリジェンスと障害分析機能を提供します。HDX Insight はユーザーの問題を優先度によってすぐに選別すると同時に、仮想デスクトップ接続に関するデータを収集し、AppFlow レコードを生成して、それらをビジュアルレポートとして提示します。

ADC インスタンスでデータ収集を有効にする構成は、デプロイメント・トポロジにおけるアプライアンスの位置によって異なります。このトピックは、次の詳細について説明します。

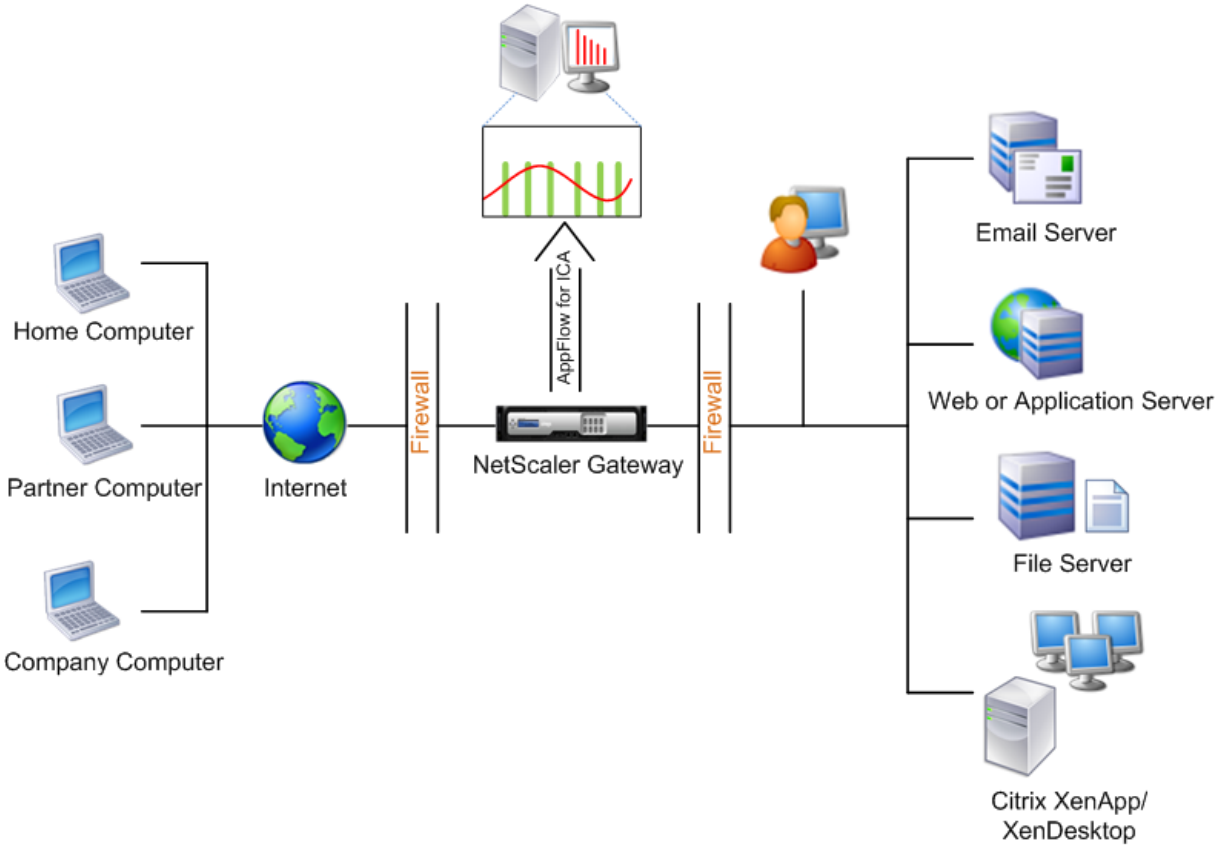
- 透過モードで展開された Citrix ADC を監視するためのデータ収集の有効化
- シングルホップモードで展開された Citrix ADC Gateway アプライアンスのデータ収集の有効化
- ダブルホップモードで展開された Citrix ADC Gateway アプライアンスのデータ収集の有効化
- LAN ユーザーモードで展開された Citrix ADC を監視するためのデータ収集の有効化

シングルホップモードで展開された Citrix ADC Gateway アプライアンスのデータ収集を有効にする

May 7, 2021

Citrix ADC Gateway がシングルホップモードで展開されている場合、ADC Gateway はネットワークのエッジにあり、デスクトップ配信インフラストラクチャへの ICA 接続をプロキシします。この配置は、最も単純で最も一般的な展開です。このモードは、外部ユーザーが組織の内部ネットワークにアクセスを試みた場合のセキュリティを実現します。シングル・ホップ・モードでは、ユーザーは仮想プライベート・ネットワーク（VPN）を介して ADC アプライアンスにアクセスします。

レポートの収集を開始するには、ADC Gateway アプライアンスを Citrix Application Delivery Management（ADM）インベントリに追加し、ADM で AppFlow を有効にする必要があります。次の図は、シングルホップモードで展開された Citrix ADM を示しています



Citrix ADM から **AppFlow** 機能を有効にする

1. [インフラストラクチャ] > [インスタンス] に移動し、分析を有効にする ADC インスタンスを選択します。
2. 「アクション」リストから「**Insight** の有効化/無効化」を選択します。
3. VPN 仮想サーバーを選択し、[**AppFlow** を有効にする] をクリックします。
4. 「**AppFlow** を有効にする」フィールドに「**true**」と入力し、「**ICA**」を選択します。
5. [**OK**] をクリックします。

> 注:
>
> シングルホップモードで AppFlow を有効にすると、次のコマンドがバックグラウンドで実行されます。トラブルシューティングのため、こちらにそのコマンドを明記します。
>
> - `add appflow collector \<name\> -IPAddress \<ip\\_addr\>`
> - `add appflow action \<name\> -collectors \<string\>`
> - `set appflow param -flowRecordInterval \<secs\>`
> - `disable ns feature AppFlow`
> - `enable ns feature AppFlow`
> - `add appflow policy \<name\> \<rule\> \<expression\>`

- `set appflow policy \<name\> -rule \<expression\>`
- `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >-priority \<positive\\_integer\>`
- `set vpn vserver \<name\> -appflowLog ENABLED`
- `save ns config`

透過モードで展開された **Citrix ADC** を監視するためのデータ収集を有効にする

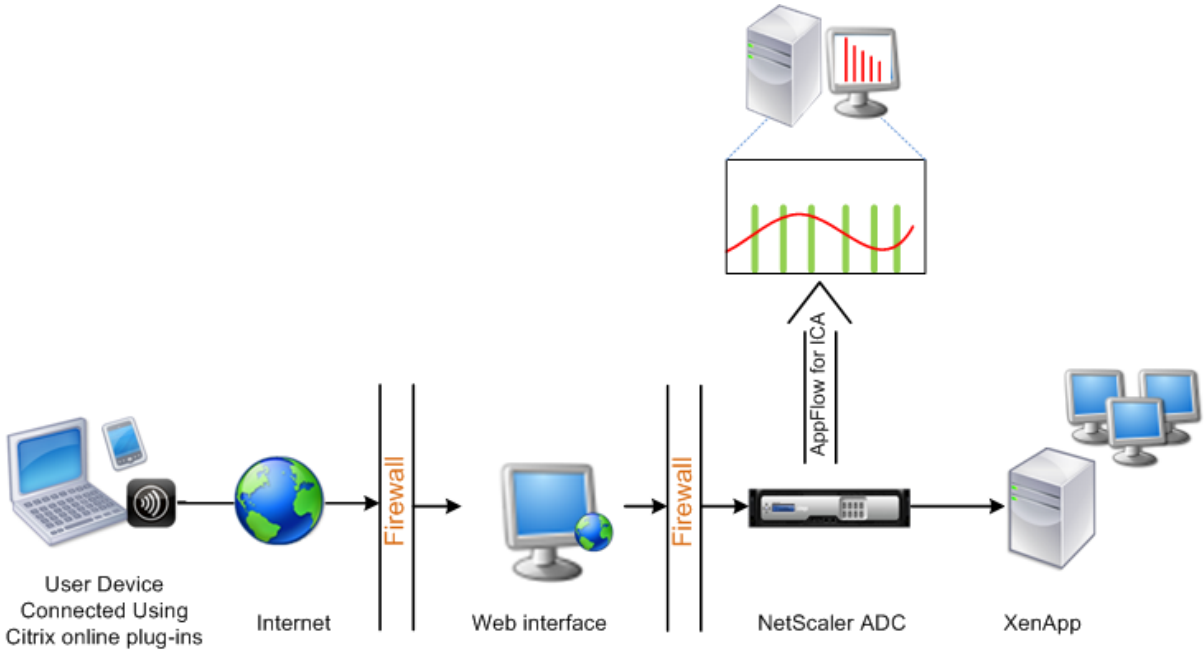
May 7, 2021

Citrix ADC を透過モードで展開すると、クライアントは仮想サーバーを介さず、直接サーバーにアクセスできます。Citrix ADC アプライアンスが Citrix Virtual Apps and Desktops 環境で透過モードで展開されている場合、ICA トラフィックは VPN 経由で送信されません。

Citrix ADC を Citrix Application Delivery Management（ADM）インベントリに追加した後、データ収集用に AppFlow を有効にする必要があります。データ収集を有効にできるかどうかは、デバイスとモードによって決まります。その場合は、Citrix ADM を AppFlow コレクタとして各 Citrix ADC アプライアンスに追加する必要があります。また、AppFlow ポリシーを構成して、アプライアンスを通過するすべての ICA トラフィックまたは特定の ICA トラフィックを収集する必要があります。

> 注
>
> - Citrix ADM 構成ユーティリティを使用して、透過モードで展開された Citrix ADC でデータ収集を有効にすることはできません。
> - コマンドとその使用方法について詳しくは、コマンドリファレンスを参照してください。
> - ポリシー式の詳細については、ポリシーと表現を参照してください。

次の図は、Citrix ADC が透過モードで展開された場合の Citrix ADM のネットワーク展開を示しています。



コマンドラインインターフェイスを使用して **Citrix ADC** アプライアンスでデータ収集を構成するには:

コマンドプロンプトで、次の操作を行います。

1. アプライアンスにログオンします。
2. Citrix ADC アプライアンスがトラフィックをリッスンする ICA ポートを指定します。

```
set ns param --icaPorts <port>...
<!--NeedCopy-->
```

例:

```
set ns param -icaPorts 2598 1494
<!--NeedCopy-->
```

> 注
>
> - このコマンドでは、最大 10 個のポートを指定できます。
> - デフォルトのポート番号は 2598 です。ポート番号は、必要に応じて変更できます。

3. Citrix ADC アプライアンスで、NetScaler Insight Center を AppFlow コレクタとして追加します。

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

例:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```


> 注:
>
> Citrix ADC アプライアンスで構成された AppFlow コレクタを表示するには、**show appflow** コレクタコマンドを使用します。

4. AppFlow アクションを作成し、コレクタをアクションに関連付けます。

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

例:

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. AppFlow ポリシーを作成して、トラフィックを生成するためのルールを指定します。

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

例:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. AppFlow ポリシーをグローバルバインドポイントにバインドします。

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```

例:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> 注:
>
> ICA トラフィックに適用するには、**TYPE** の値は ICA_REQ_OVERRIDE または ICA_REQ_DEFAULT である必要があります。

7. AppFlow の flowRecordInterval パラメーターの値を 60 秒に設定します。

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. 構成を保存します。


```
save ns config
<!--NeedCopy-->
```

ダブルホップモードで展開された **Citrix ADC Gateway** アプライアンスのデータ収集を有効にする

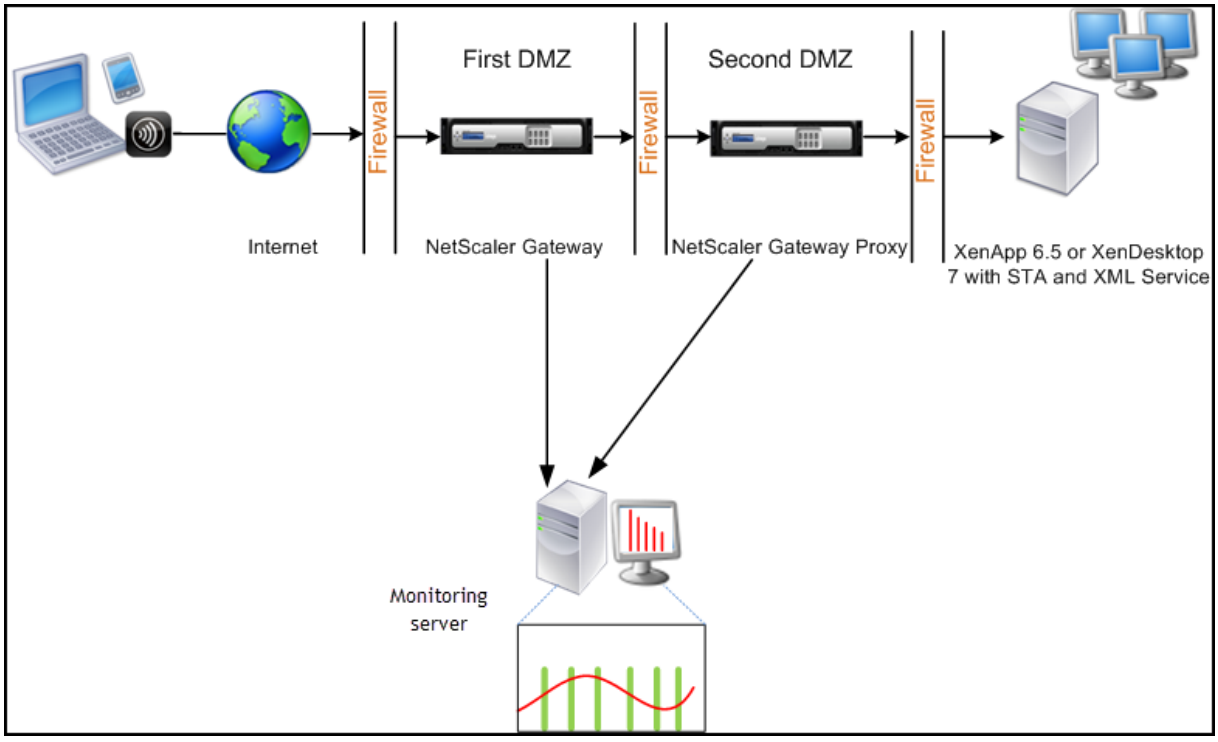
May 7, 2021

Citrix ADC Gateway のダブルホップモードでは、攻撃者が複数のセキュリティゾーンまたは非武装ゾーン（DMZ）を侵入して安全なネットワーク内のサーバーに到達する必要があるため、組織の内部ネットワークをさらに保護します。

管理者は、Citrix ADM を使用して、次のデータを分析できます。

- ICA 接続が通過するホップ数（Citrix ADC ゲートウェイアプライアンス）
- 各 TCP 接続のレイテンシーと、クライアントが認識する合計 ICA 遅延に対してそれがどのようにフェアされるかの詳細

次の図は、最初の DMZ の Citrix ADM と Citrix ADC ゲートウェイが同じサブネットに展開されていることを示しています。



最初の DMZ の Citrix ADC Gateway は、ユーザー接続を処理し、SSL VPN のセキュリティ機能を実行します。こ

の Citrix ADC Gateway は、ユーザー接続を暗号化し、ユーザーの認証方法を決定し、内部ネットワークのサーバーへのアクセスを制御します。

2 つ目の DMZ の Citrix ADC Gateway は、Citrix ADC ゲートウェイプロキシデバイスとして機能します。この Citrix ADC Gateway を使用すると、ICA トラフィックが 2 番目の DMZ を通過してサーバーファームへのユーザー接続を完了できます。

Citrix ADM は、最初の DMZ の Citrix ADC ゲートウェイアプライアンスに属するサブネット、または Citrix ADC ゲートウェイアプライアンスの 2 番目の DMZ に属するサブネットのいずれかに展開できます。

ダブルホップモードでは、Citrix ADM は 1 つのアプライアンスから TCP レコードを、もう 1 つのアプライアンスから ICA レコードを収集します。Citrix ADC Gateway アプライアンスを Citrix ADM インベントリに追加してデータ収集を有効にすると、各アプライアンスはホップカウントと接続チェーン ID を追跡してレポートをエクスポートします。

Citrix ADM がレコードをエクスポートするアプライアンスを識別するために、各アプライアンスはホップ数で指定され、各接続は接続チェーン ID で指定されます。ホップカウントは、クライアントからサーバーへのトラフィックが流れる Citrix ADC Gateway アプライアンスの数を表します。接続チェーン ID は、クライアントとサーバー間のエンドツーエンド接続を表します。

Citrix ADM は、ホップカウントと接続チェーン ID を使用して、Citrix ADC Gateway アプライアンスのデータを相互に関連付け、レポートを生成します。

このモードで展開されている Citrix ADC Gateway アプライアンスを監視するには、まず Citrix ADC ゲートウェイを Citrix ADM インベントリに追加し、Citrix ADM で AppFlow を有効にして、Citrix ADM ダッシュボードでレポートを表示する必要があります。

Citrix ADM でのデータ収集の有効化

両方のアプライアンスから ICA 詳細の収集を開始するように Citrix ADM を有効にすると、収集された詳細情報は冗長になります。この状況を克服するには、最初の Citrix ADC Gateway アプライアンスで AppFlow for ICA を有効にし、次に 2 番目のアプライアンスで AppFlow for TCP を有効にする必要があります。これにより、一方のアプライアンスが ICA AppFlow レコードをエクスポートし、もう一方のアプライアンスが TCP AppFlow レコードをエクスポートします。これにより、ICA トラフィックを解析するときの処理時間も短縮されます。

Citrix ADM から **AppFlow** 機能を有効にするには:

1. ［インフラストラクチャ］>［インスタンス］に移動し、分析を有効にする Citrix ADC インスタンスを選択します。
2. 「アクション」リストから「**Insight** の有効化/無効化」を選択します。
3. VPN 仮想サーバーを選択し、[**AppFlow** を有効にする] をクリックします。
4. 「**AppFlow** を有効にする」フィールドに「**true**」と入力し、ICA トラフィック用の **ICA/TCP** 、TCP トラフィック用の ICA/TCP をそれぞれ選択します。

> 注:
>
> Citrix ADC アプライアンスの各サービスまたはサービスグループで AppFlow ログが有効になっていない場合、［インサイト］列に［有効］と表示されていても、Citrix ADM ダッシュボードにレコードが表示されません。

5. ［**OK**］をクリックします。

データをエクスポートするように **Citrix ADC** ゲートウェイアプライアンスを構成する

Citrix ADC Gateway アプライアンスをインストールした後、Citrix ADC ゲートウェイアプライアンスで次の設定を構成して、レポートを Citrix ADM にエクスポートする必要があります。

- 最初の DMZ と 2 番目の DMZ の Citrix ADC Gateway アプライアンスの仮想サーバーを相互に通信するように構成します。
- 2 番目の DMZ の Citrix ADC Gateway 仮想サーバーを、最初の DMZ の Citrix ADC Gateway 仮想サーバーにバインドします。
- 2 番目の DMZ の Citrix ADC Gateway でダブルホップを有効にします。
- 2 番目の DMZ の Citrix ADC Gateway 仮想サーバーでの認証を無効にします。
- いずれかの Citrix ADC ゲートウェイアプライアンスで ICA レコードをエクスポートできるようにする
- 他の Citrix ADC ゲートウェイアプライアンスを有効にして、TCP レコードをエクスポートします。
- 両方の Citrix ADC Gateway アプライアンスで、接続チェーンを有効にします。

コマンドラインインターフェイスを使用して **Citrix ADC Gateway** を構成します。

1. 最初の DMZ の Citrix ADC Gateway 仮想サーバーを構成して、2 番目の DMZ の Citrix ADC Gateway 仮想サーバーと通信します。

   add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [**-secure** (ON|OFF)] [**-imgGifToPng**] …

   ```
   add vpn nextHopServer nh1 10.102.2.33 8443  -secure ON
   <!--NeedCopy-->
   ```

2. 2 番目の DMZ の Citrix ADC Gateway 仮想サーバーを、最初の DMZ の Citrix ADC Gateway 仮想サーバーにバインドします。最初の DMZ の Citrix ADC Gateway で次のコマンドを実行します。

   bind vpn vserver <name> **-nextHopServer** <name>

   ```
   bind vpn vserver vs1 -nextHopServer nh1
   <!--NeedCopy-->
   ```


3. 2 番目の DMZ の Citrix ADC Gateway でダブルホップと AppFlow を有効にします。

   set vpn vserver <name> [**- doubleHop** (ENABLED |DISABLED)] [**- appflowLog** (ENABLED |DISABLED)]

```
set vpn vserver vpnhop2  -doubleHop ENABLED  -appFlowLog ENABLED
<!--NeedCopy-->
```

4. 2 番目の DMZ の Citrix ADC Gateway 仮想サーバーでの認証を無効にします。

   VPN サーバを設定する <name> [**-**認証 (オン)|OFF)]

```
set vpn vserver vs -authentication OFF
<!--NeedCopy-->
```

5. いずれかの Citrix ADC ゲートウェイアプライアンスで TCP レコードをエクスポートできるようにします。

   bind vpn vserver<name> [**-policy **<string> **-priority **<positive_integer>] [**-type **<type>]

```
bind vpn vserver vpn1 -policy appflowpol1 -priority 101  -type
   OTHERTCP_REQUEST
<!--NeedCopy-->
```

6. 他の Citrix ADC Gateway アプライアンスで ICA レコードをエクスポートできるようにします。

   bind vpn vserver<name> [**-policy **<string> **-priority **<positive_integer>] [**-type **<type>]

```
bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
   ICA_REQUEST
<!--NeedCopy-->
```

7. Citrix ADC Gateway アプライアンスの両方の接続チェーンを有効にします。

set appFlow param [**-connectionChaining** (ENABLED DISABLED)]

```
set appflow param -connectionChaining ENABLED
<!--NeedCopy-->
```

構成ユーティリティを使用した **Citrix ADC Gateway** の構成:

1. 最初の DMZ の Citrix ADC Gateway を構成して、2 番目の DMZ の Citrix ADC Gateway と通信し、2 番目の DMZ の Citrix ADC ゲートウェイを最初の DMZ の Citrix ADC Gateway にバインドします。

a) ［構成］タブで ［**Citrix ADC** ゲートウェイ］を展開し、［仮想サーバー］をクリックします。

b) 右側のウィンドウで、仮想サーバーをダブルクリックし、[詳細設定] グループで [公開アプリケーション] を展開します。

c) ［ネクストホップサーバー］をクリックし、ネクストホップサーバーを 2 番目の Citrix ADC Gateway アプライアンスにバインドします。

2. 2 番目の DMZ の Citrix ADC Gateway でダブルホップを有効にします。

a) ［構成］タブで ［**Citrix ADC** ゲートウェイ］を展開し、［仮想サーバー］をクリックします。

b) 右側のウィンドウで、仮想サーバーをダブルクリックし、[基本設定] グループの [編集] アイコンをクリックします。

c) [詳細] を展開し、[ダブルホップ] を選択して [**OK**] をクリックします。

3. 2 つ目の DMZ の Citrix ADC Gateway 上の仮想サーバーでの認証を無効にします。

a) ［構成］タブで ［**Citrix ADC** ゲートウェイ］を展開し、［仮想サーバー］をクリックします。

b) 右側のウィンドウで、仮想サーバーをダブルクリックし、[基本設定] グループの [編集] アイコンをクリックします。

c) [詳細] を展開し、[認証を有効にする] をオフにします。

4. いずれかの Citrix ADC ゲートウェイアプライアンスで TCP レコードをエクスポートできるようにします。

a) ［構成］タブで ［**Citrix ADC** ゲートウェイ］を展開し、［仮想サーバー］をクリックします。

b) 右側のウィンドウで、仮想サーバーをダブルクリックし、[詳細設定] グループで [ポリシー] を展開します。

c) ［+］アイコンをクリックし、［ポリシーの選択］リストから［**AppFlow** ］を選択し、［タイプの選択］リストから［その他の **TCP** 要求］を選択します。

d) ［続行］をクリックします。

e) ポリシーバインドを追加し、[**Close**] をクリックします。

5. 他の Citrix ADC Gateway アプライアンスで ICA レコードをエクスポートできるようにします。

a) ［構成］タブで ［**Citrix ADC** ゲートウェイ］を展開し、［仮想サーバー］をクリックします。

b) 右側のウィンドウで、仮想サーバーをダブルクリックし、[詳細設定] グループで [ポリシー] を展開します。

c) ［+］アイコンをクリックし、［ポリシーの選択］リストから［**AppFlow** ］を選択し、［タイプの選択］リストから［その他の **TCP** 要求］を選択します。

d) ［続行］をクリックします。

e) ポリシーバインドを追加し、[**Close**] をクリックします。

6. 両方の Citrix ADC Gateway アプライアンスで、接続チェーンを有効にします。

   a) [構成] タブで、[システム] > [**Appflow**] に移動します。

   b) 右側のウィンドウの [設定] で、[**Appflow** 設定の変更] をクリックします。

   c)「接続チェーン」を選択し、「**OK**」をクリックします。

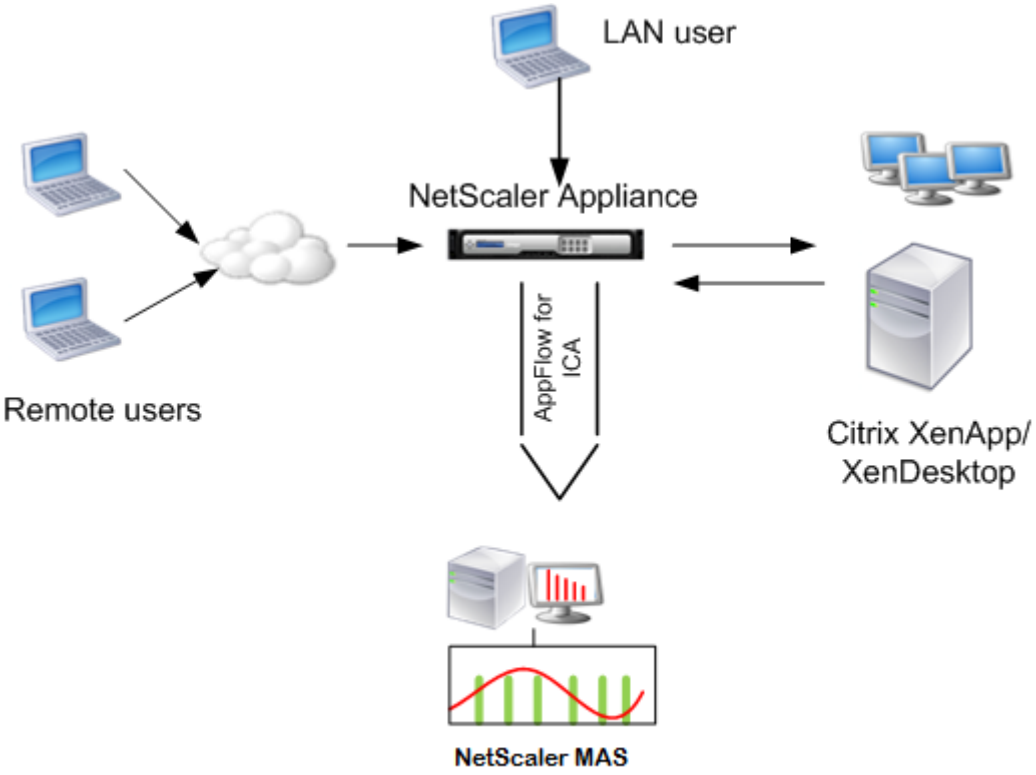
LAN ユーザーモードで展開された **Citrix ADC** を監視するためのデータ収集を有効にする

May 7, 2021

Citrix Virtual App またはデスクトップアプリケーションにアクセスする外部ユーザーは、Citrix ADC Gateway で自分自身を認証する必要があります。ただし、内部ユーザーは ADC Gateway にリダイレクトする必要がない場合があります。また、透過モードの展開では、管理者が手動でルーティングポリシーを適用して、要求が Citrix ADC アプライアンスにリダイレクトされるようにする必要があります。

これらの課題を克服し、LAN ユーザーが Citrix Virtual App およびデスクトップアプリケーションに直接接続できるようにするには、キャッシュリダイレクト仮想サーバーを構成して、ADC アプライアンスを LAN ユーザーモードで展開できます。キャッシュリダイレクト仮想サーバーは、ADC Gateway アプライアンスの SOCKS プロキシとして機能します。

次の画像は、**LAN** ユーザーモードで展開された **Citrix**Application Delivery Management（ADM）を示しています。



> 注
>
> Citrix ADC Gateway プライアンスが Citrix ADM エージェントに到達できる必要があります。

このモードで展開された Citrix ADC アプライアンスを監視するには、まず Citrix ADC アプライアンスを Citrix ADC Insight インベントリに追加し、AppFlow を有効にして、ダッシュボードにレポートを表示します。

Citrix ADC アプライアンスを Citrix ADM インベントリに追加した後、データ収集のために AppFlow を有効にする必要があります。

> 注
>
> - Citrix ADM 構成ユーティリティを使用して、LAN ユーザーモードで展開された Citrix ADC でデータ収集を有効にすることはできません。
> - コマンドとその使用法について詳しくは、「コマンドリファレンス」を参照してください。
> - ポリシー式については、「ポリシーと式」を参照してください。

コマンドラインインターフェイスを使用して **Citrix ADC** アプライアンスでデータ収集を構成するには:

コマンドプロンプトで、次の操作を行います。

1. Citrix ADC アプライアンスにログオンします。
2. プロキシ IP およびポートを指定してフォワードプロキシキャッシュリダイレクト仮想サーバーを追加します。また、サービスタイプとして HDX を指定します。


```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
    cacheType <cachetype>] [ - cltTimeout <secs>]
<!--NeedCopy-->
```

例:

```
add cr vserver cr1 HDX 10.12.2.2 443  - cacheType FORWARD  -
    cltTimeout 180
<!--NeedCopy-->
```

> 注:
>
> Citrix ADC Gateway アプライアンスを使用して LAN ネットワークにアクセスする場合は、VPN トラフィックに一致するポリシーを適用するアクションを追加します。

```
add vpn trafficAction** <name> <qual> [-HDX ( ON | OFF )]

add vpn trafficPolicy** <name> <rule> <action>
<!--NeedCopy-->
```

例:

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
<!--NeedCopy-->
```

3. Citrix ADM を AppFlow コレクタとして Citrix ADC アプライアンスに追加します。

```
add appflow collector** <name> \*\*-IPAddress\*\* <ip_addr>
<!--NeedCopy-->
```

例:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

4. AppFlow アクションを作成し、コレクタをアクションに関連付けます。

```
add appflow action** <name> \*\*-collectors\*\* <string> ...
<!--NeedCopy-->
```

例:

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```


5. AppFlow ポリシーを作成して、トラフィックを生成するためのルールを指定します。

```
add appflow policy** <policyname> <rule> <action>
<!--NeedCopy-->
```

例:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. AppFlow ポリシーをグローバルバインドポイントにバインドします。

```
bind appflow global** <policyname> <priority> \*\*-type\*\* <type>
<!--NeedCopy-->
```

例:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> 注:
>
> ICA トラフィックに適用するには、TYPE の値は ICA_REQ_OVERRIDE または ICA_REQ_DEFAULT である必要があります。

7. AppFlow の flowRecordInterval パラメーターの値を 60 秒に設定します。

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

例:

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. 構成を保存します。

```
save ns config
<!--NeedCopy-->
```

HDX Insight のしきい値を作成してアラートを構成する

May 7, 2021

Citrix Application Delivery Management（ADM）の HDX Insight を使用すると、Citrix ADC インスタンスを通過する HDX トラフィックを監視できます。Citrix ADM では、Insight トラフィックの監視に使用するさまざまなカウンターのしきい値を設定できます。ADM でルールを構成し、アラートを作成することもできます。

HDX トラフィックの種類は、アプリケーション、デスクトップ、ゲートウェイ、ライセンス、ユーザーなどのさまざまなエンティティに関連付けられます。すべてのエンティティには、それらに関連付けられた異なるメトリックを含めることができます。たとえば、アプリケーションエンティティは、複数のヒット、アプリケーションによって消費される帯域幅、およびサーバーの応答時間に関連付けられます。ユーザーエンティティは、WAN 遅延、DC 遅延、ICA RTT、およびユーザーが消費する帯域幅に関連付けることができます。

Citrix ADM HDX Insight のしきい値管理により、事前にルールを作成し、しきい値を超えたときにアラートを構成することができました。今回のリリースでは、このしきい値管理が拡張され、しきい値規則のグループを設定できます。個々のルールではなく、グループを監視できるようになりました。しきい値ルールグループは、ユーザー、アプリケーション、デスクトップなどのエンティティから選択したメトリックに対して、1 つ以上のユーザー定義しきい値ルールで構成されます。各ルールは、ルールの作成時に入力した期待値に対して監視されます。ユーザーエンティティでは、しきい値グループをジオロケーションに関連付けることもできます。

Citrix ADM でアラートが生成されるのは、構成されたしきい値グループ内のすべてのルールに違反した場合のみです。たとえば、アプリケーションの合計セッション起動回数と、アプリケーションの起動回数を 1 つのしきい値グループとして監視できます。両方のルールに違反した場合にのみ、アラートが生成されます。これにより、エンティティに対してより現実的なしきい値を設定できます。

以下に、いくつかの例を挙げる。

- しきい値ルール 1: ユーザー (エンティティ) の ICA RTT (メトリック) は 100 ミリ秒以下である必要があります
- しきい値ルール 2: ユーザー (エンティティ) の WAN 遅延 (メトリック) は 100 ミリ秒以下である必要があります

しきい値グループの例は次のようになります。{しきい値ルール 1 + しきい値ルール 2}

ルールを作成するには、最初に監視するエンティティを選択する必要があります。次に、ルールの作成時にメトリックスを選択します。たとえば、アプリケーションエンティティを選択し、[合計セッション起動数] または [アプリケーション起動数] を選択できます。エンティティとメトリックの組み合わせごとに 1 つのルールを作成できます。提供されたコンパレータ（>、<、>=、<=）を使用して、各メトリックのしきい値を入力します。

> 注
>
> 1 つのグループ内の複数のエンティティを監視しない場合は、エンティティごとに個別のしきい値ルールグループを作成する必要があります。

カウンターの値がしきい値を超えると、Citrix ADM はしきい値違反を示すイベントを生成し、イベントごとにアラートを作成します。

アラートの受信方法を構成する必要があります。アラートを Citrix ADM に表示したり、メールまたは両方、または SMS としてモバイルデバイス上でアラートを受信したりできます。最後の 2 つの操作では、Citrix ADM で電子メールサーバーまたは SMS サーバーを構成する必要があります。

閾値グループは、ユーザーエンティティの地理固有の監視のためにジオロケーションにバインドすることもできます。

ユースケースの例

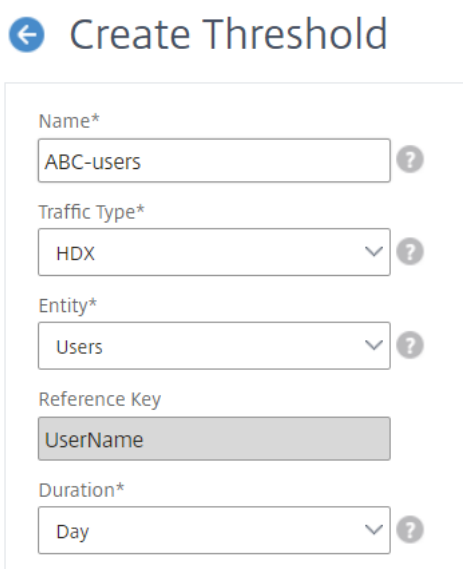
ABC Inc. はグローバル企業で、50 カ国以上にオフィスを構えています。同社は、シンガポールとカリフォルニア州に Citrix Virtual Apps and Desktops をホストする 2 つのデータセンターを持っています。同社の従業員は、Citrix ADC ゲートウェイと GSLB ベースのリダイレクトを使用して、世界中の Citrix Virtual Apps and Desktops にアクセスします。ABC Inc. の Citrix Virtual Apps and Desktops 管理者であるエリックは、すべてのオフィスのユーザーエクスペリエンスを追跡し、いつでもどこでもアクセスできるようにアプリとデスクトップ配信を最適化したいと考えています。また、ICA の RTT やレイテンシーなどのユーザーエクスペリエンス指標をチェックし、偏差を積極的に引き上げたいと考えています。

ABC Inc. のユーザーは、分散した存在感を持っています。データセンターの近くにいるユーザーもあれば、データセンターから離れた場所にいるユーザーもいます。ユーザーベースが広く分散されているため、メトリックと対応するしきい値もこれらの場所によって異なります。たとえば、データセンターに近いロケーションの ICA RTT は 5〜10 ミリ秒ですが、リモートロケーションの ICA RTT は約 100 ミリ秒です。

HDX Insight のしきい値ルールグループ管理機能を使用すると、地域ごとに地域固有のしきい値ルールグループを設定し、エリアごとの違反について電子メールまたは SMS でアラートを受け取ることができます。また、Eric は、しきい値ルールグループ内で複数のメトリックの追跡を組み合わせて、根本原因をキャパシティの問題に絞り込むこともできます。Eric は、すべての Citrix Virtual Apps and Desktops ポートフォリオの指標を手動で調べる複雑さを心配することなく、あらゆる偏差をプロアクティブに追跡できるようになりました。

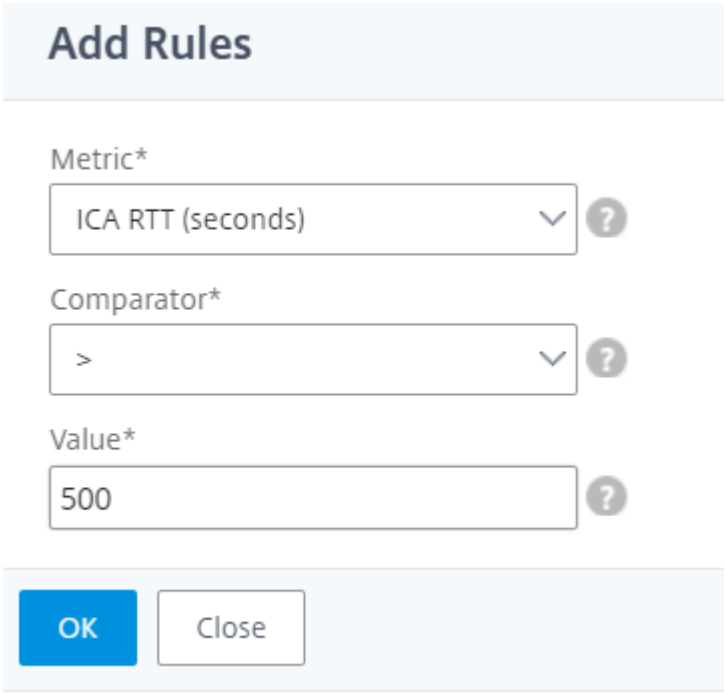
Citrix ADM を使用してしきい値ルールグループを作成し、**HDX Insight** のアラートを構成する

1. Citrix ADM で、[**Analytics**] > ［設定］> ［しきい値］に移動します。[しきい値] ページが表示されたら、[追加] をクリックします。
2. ［**Create Thresholds and Alerts**］ページで次の詳細を指定します。
    a) 名前。Citrix ADM がアラートを生成するイベントを作成するための名前を入力します。
    b) トラフィックタイプ。ドロップダウンリストボックスから、[HDX] を選択します。
    c) エンティティ。ドロップダウンリストボックスから、カテゴリまたはリソースタイプを選択します。エンティティは、以前に選択したトラフィックタイプごとに異なります。
    d) 参照キー。参照キーは、選択したトラフィックタイプとエンティティに基づいて自動的に生成されます。
    e) 期間。ドロップダウンリストボックスから、エンティティを監視する時間間隔を選択します。エンティティは、1 時間、1 日、または 1 週間の期間を監視できます。

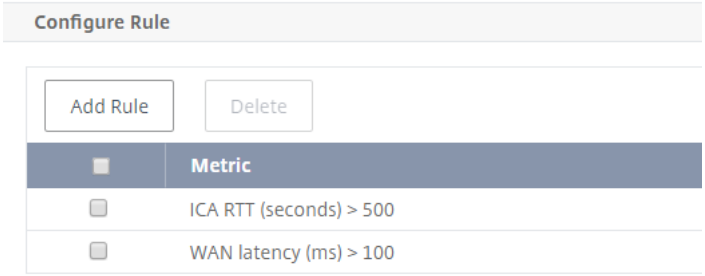


3. すべてのエンティティのしきい値ルールグループを作成しています。

   HDX トラフィックの場合は、[**Add Rule]** をクリックしてルールを作成する必要があります。表示される [**Add Rules**] ポップアップウィンドウに値を入力します。

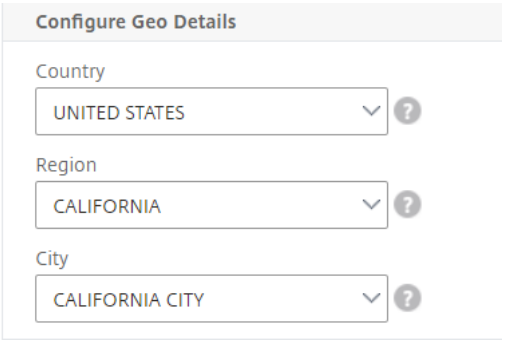


   複数のルールを作成して、各エンティティを監視できます。1 つのグループに複数のルールを作成すると、個々のルールではなくしきい値ルールのグループとしてエンティティを監視できます。[**OK**] をクリックしてウィンドウを閉じます。

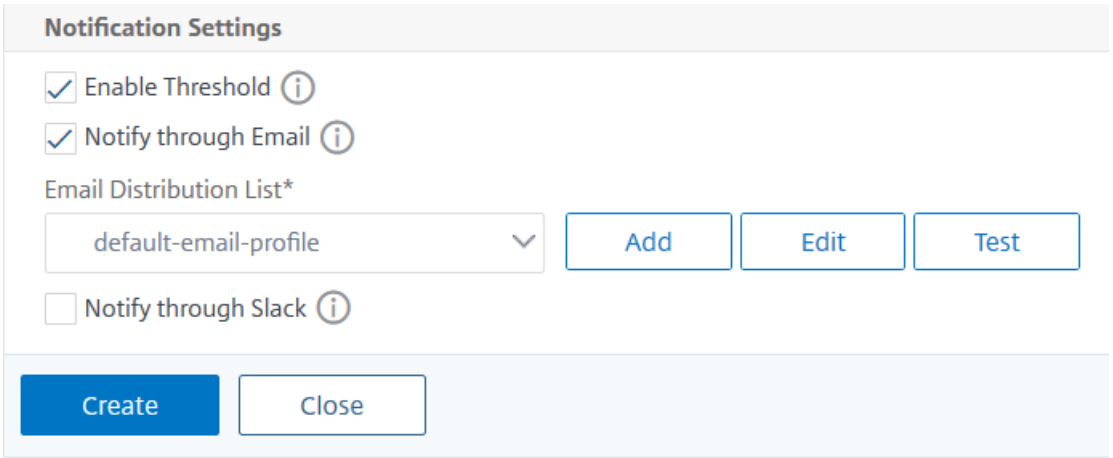


4. ユーザーエンティティのジオロケーションタグの設定**:**

   必要に応じて、[地理詳細の構成] セクションで、ユーザーエンティティの場所ベースのアラートを作成できます。次の図は、米国西海岸のユーザーの WAN レイテンシーのパフォーマンスを監視するジオロケーションベースのタグ付けを作成する例を示しています。



5. ［しきい値を有効にする］をクリックして、Citrix ADM でエンティティの監視を開始できるようにします。
6. オプションで、メールや Slack 通知などのアクションを設定します。



7. [**Create**] をクリックして、しきい値ルールグループを作成します。

HDX Insight レポートとメトリックスを表示

May 7, 2021

HDX Insight は、Citrix ADC インスタンス上の HDX トラフィックに関するレポートとメトリックスを完全に可視化します。

選択した任意のエンティティについて、HDX メトリックを確認できます。各ビューには、次のカテゴリのエンティティが含まれます。

- ユーザー：選択した期間内に Citrix Virtual Apps and Desktops にアクセスするすべてのユーザーのレポートを表示します。
- アプリケーション：アプリケーションの合計数のレポートと、指定した時間間隔内にアプリケーションが起動された合計回数など、関連するすべての関連情報を表示します。
- **Instances**: 着信トラフィックのゲートウェイとして機能する ADC インスタンスに関するレポートを表示します。
- デスクトップ：選択した期間内に使用されたデスクトップのレポートを表示します。
- [**L**icenses]：指定したタイムスロット内で使用された SSL VPN ライセンスの合計に関するレポートを表示します。

> 注
>
> ライセンス値は、ADC SD-WAN アプライアンスには適用されません。

このドキュメントは、次のセクションで構成されています。

- ［User］ビューのレポートとメトリック
- Application ビューのレポートとメトリクス
- デスクトップビューのレポートおよびメトリクス
- インスタンスビューのレポートおよびメトリクス
- ライセンスビューのレポートおよびメトリクス

Application ビューのレポートとメトリクス

May 7, 2021

このビューのレポートとメトリックは、Citrix Virtual Apps に焦点を当てています。[分析] > [**HDX Insight**] > [アプリケーション] に移動します

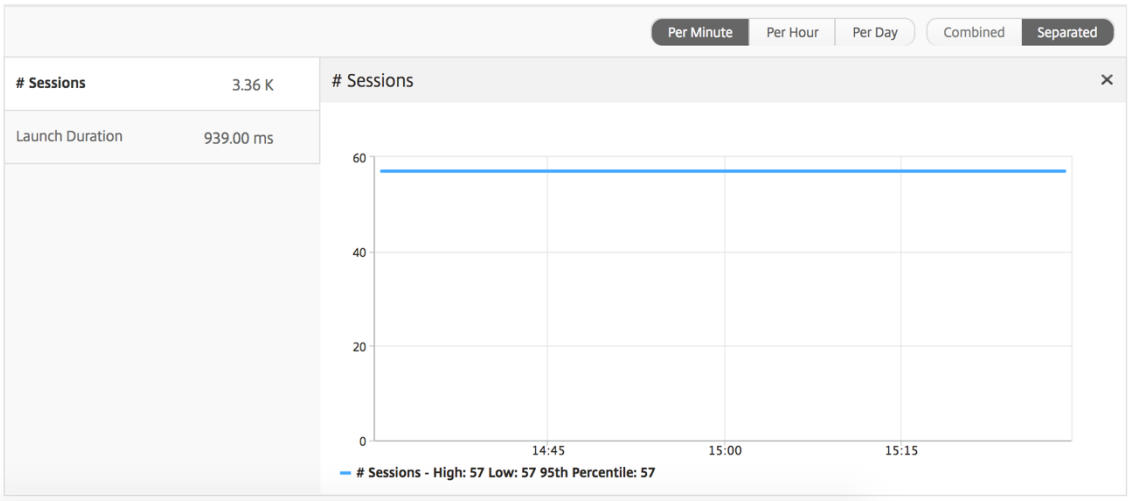
［**Summary**］ビュー

Summary ビューには、選択した期間中にログインしたすべてのアプリケーションのレポートが表示されます。

明示的に言及しない限り、すべての指標/レポートには、選択した期間に対応する値が含まれます。

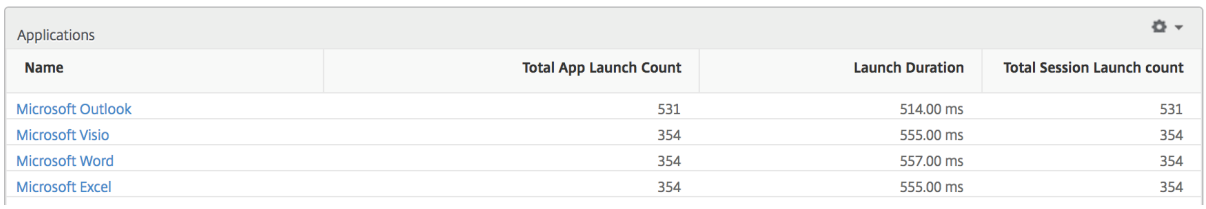
折れ線グラフ

メトリック	説明
セッション数	特定の期間の合計セッション数。
起動時間	アプリケーションの起動にかかった平均時間。



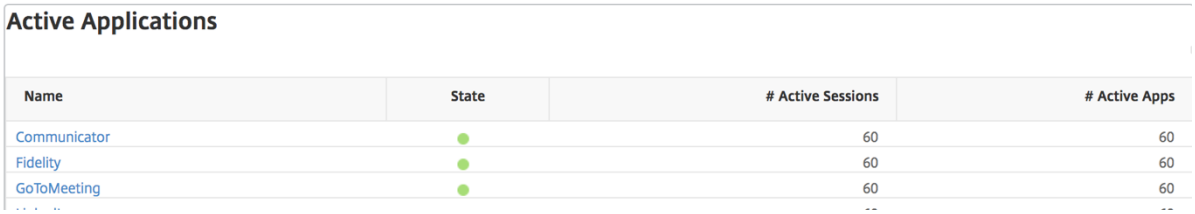
Applications Summary レポート

メトリック	説明
名前	Citrix Virtual App の名前。
セッションの起動数合計	指定した期間中のアクティブな Citrix Virtual App セッションの総数。
アプリケーションの起動数合計	指定した期間中に起動された Citrix Virtual App アプリケーションの合計数。
起動期間	Citrix Virtual App の起動に要した平均時間。



Active Application レポート

メトリック	説明
名前	Citrix Virtual App の名前。
状態	アプリケーションの状態 (緑-アクティブ、赤-非アクティブ) を表示します。
アクティブなセッション数	特定の期間にこのアプリケーションを使用したアクティブなユーザーセッション数。
アクティブなアプリケーション数	このアプリケーションのアクティブなセッション数。

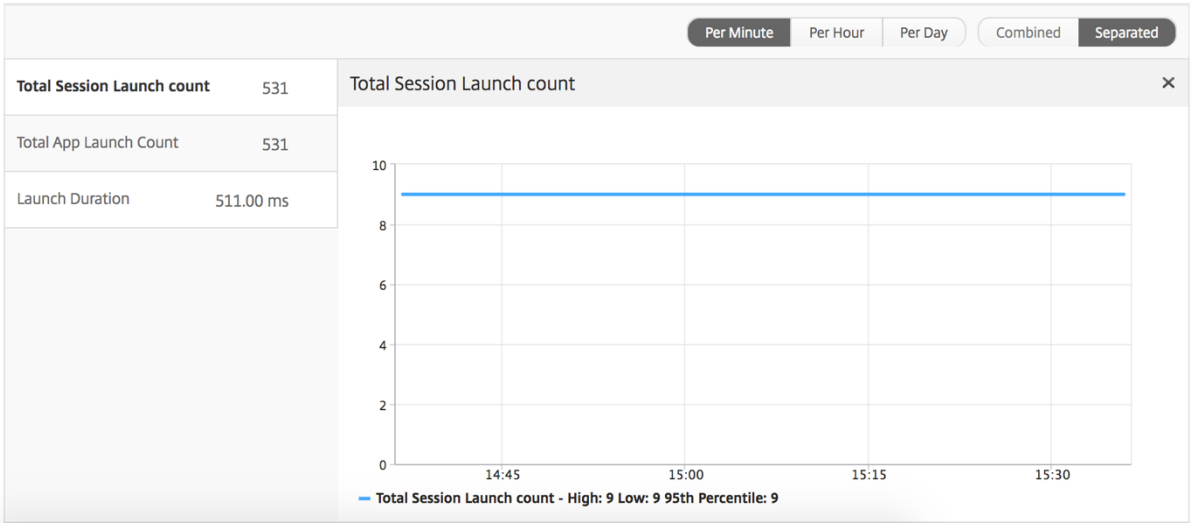


しきい値レポート

しきい値レポートは、選択した期間内にエンティティが「アプリケーション」として選択されている場合に、違反したしきい値の数を表します。<!— 詳細については、「しきい値とアラートの作成方法」(/en-us/citrix-application-delivery-management-service/analytics/analytics-how-to-articles/how-to-create-thresholds-and-alerts-using-mas.html) を参照してください。。—>

折れ線グラフ

メトリック	説明
アクティブなセッション数	この数値は、アクティブな Citrix Virtual App and Desktop セッションの数を示します。
起動時間	アプリケーションの起動にかかった平均時間。

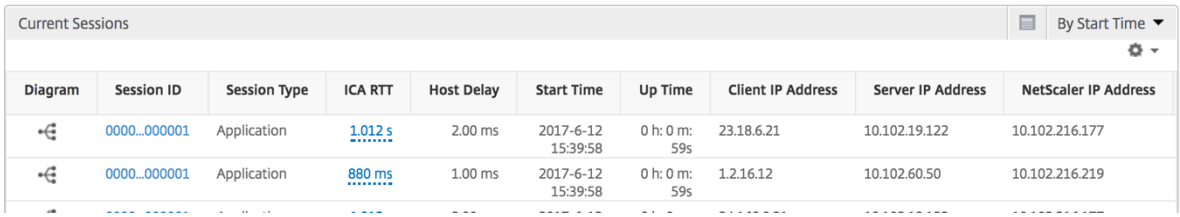


Current Sessions レポート

メトリック	説明
セッション ID	ICA セッションの一意の ID。
セッションの種類	アプリケーション/デスクトップ。
状態	緑はアクティブなセッション、赤は非アクティブなセッション。
ホストの遅延	サーバーネットワークが原因で、Citrix ADC を通過する ICA トラフィックの平均遅延。
間隔あたりの帯域幅	特定の期間にセッションで使用された帯域幅です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
間隔あたりのバイト数	特定の期間にセッションで使用されたバイト数。
開始時刻	セッションの開始時間。
アップタイム	セッションの実行時間
クライアント IP アドレス	エンドユーザーの IP。
サーバー IP アドレス	バックエンド/ Citrix Virtual App サーバー IP。
NetScaler IP Address	NetScaler の管理 IP（NSIP）。
クライアントの種類	レシーバタイプ-Citrix Windows クライアント。
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値（[Yes] または [No]）。セッションがマルチストリーム ICA かどうかを表します。

メトリック	説明
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスの種類	ICA セッションのアクセスモードを表示します。たとえば、Citrix ADC ゲートウェイのユーザー/透過モードなどです。
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB の状態	緑はアクティブ、赤は非アクティブ。
許可された USB インスタンス数	受け入れられた USB インスタンス数。
拒否された USB インスタンス数	拒否された USB インスタンス数。
停止された USB インスタンス数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェイルオーバーカウント	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、Citrix ADC からエンドユーザーへ。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、Citrix ADC からバックエンドサーバーまでです。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。
サーバー側の再転送	Citrix ADC とバックエンドサーバー間の接続で再送信されたパケット数。

メトリック	説明
クライアント側の再転送	Citrix ADC とエンドユーザー間の接続で再送信されたパケット数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
クライアント側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがアドバタイズした回数を表します。
Client side fast RTO	Citrix ADC とエンドユーザー間の接続で再送信タイムアウトが発生した回数。
サーバー側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウサイズがゼロであることをサーバーがアドバタイズした回数を表します。
Server side fast RTO	Citrix ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。
ユーザー名	この特定の Citrix Virtual App にアクセスするユーザーのユーザー名。
セッション ID	Citrix Virtual App セッションの一意の識別子。
セッションの種類	「アプリケーション」になります。
状態	セッション状態：緑はアクティブ、赤はアクティブです。
違反の最大遅延	定義済みしきい値の違反が一定期間に発生した場合の、L7 遅延の最大値。
違反の平均遅延	システムが「L7 遅延時間を超過」した状態のときの、L7 遅延の平均値。
L7 しきい値違反数	L7 のしきい値違反が発生した回数。
L7 Client-side Latency	ICA クライアントと Citrix ADC インスタンスの間で観測された平均 L7 遅延時間。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。
L7 Server-side Latency	Citrix ADC デバイスと Citrix Virtual App 間で観測された平均 L7 レイテンシー。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。



Per Application Session ビュー

Per Application Session ビューには、選択した特定のアプリケーションセッションのレポートが表示されます。

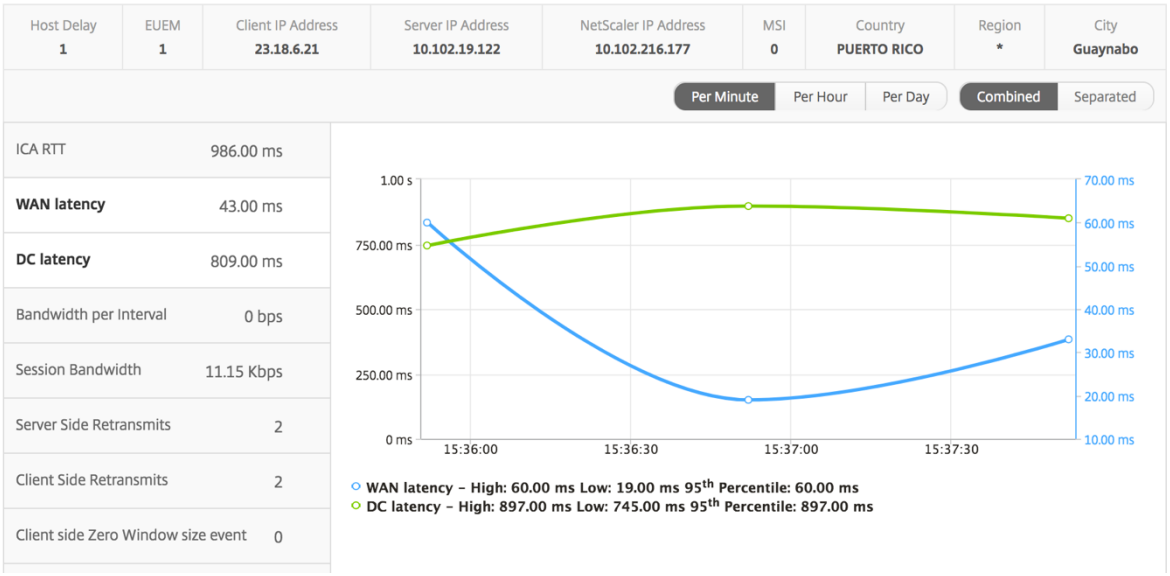
セッション・レポートを表示するには、次の手順に従います。

1. 「**Analytics** 」>「**HDX Insight** 」>「アプリケーション」の順に選択します。
2. Application Summary レポートから特定のユーザーを選択します。
3. Current Sessions レポートからセッションを選択します。

折れ線グラフ

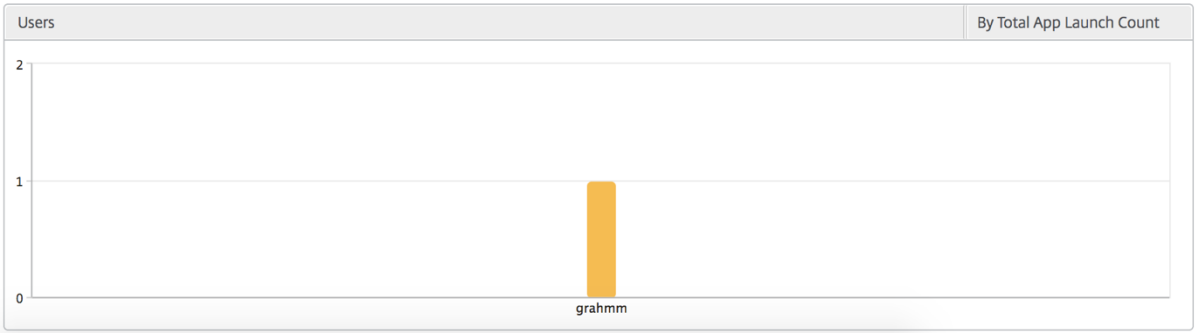
メトリック	説明
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、Citrix ADC からエンドユーザーへ。
サーバー側のゼロウィンドウサイズイベント	ネットワークのサーバー側に起因する遅延ですつまり、Citrix ADC からバックエンドサーバーまでです。
間隔あたりの帯域幅	特定の期間にセッションで使用された帯域幅です。
サーバー側の再転送	Citrix ADC とバックエンドサーバー間の接続で再送信されたパケット数。
クライアント側の再転送	Citrix ADC とエンドユーザー間の接続で再送信されたパケット数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。

メトリック	説明
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
サーバー側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウサイズがゼロであることをサーバーがアドバタイズした回数を表します。
Client side fast RTO	Citrix ADC とエンドユーザー間の接続で再送信タイムアウトが発生した回数。
Server side fast RTO	Citrix ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。
クライアント側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがアドバタイズした回数を表します。



ユーザー棒グラフ

ユーザー棒グラフは、この特定のアプリにログインしているユーザーを表します。



デスクトップビューのレポートおよびメトリクス

May 7, 2021

このビューのレポートと指標は、Citrix Virtual Desktop に重点を置いています。[分析] > [**HDX Insight**] > [デスクトップ] に移動します

［**Summary**］ビュー

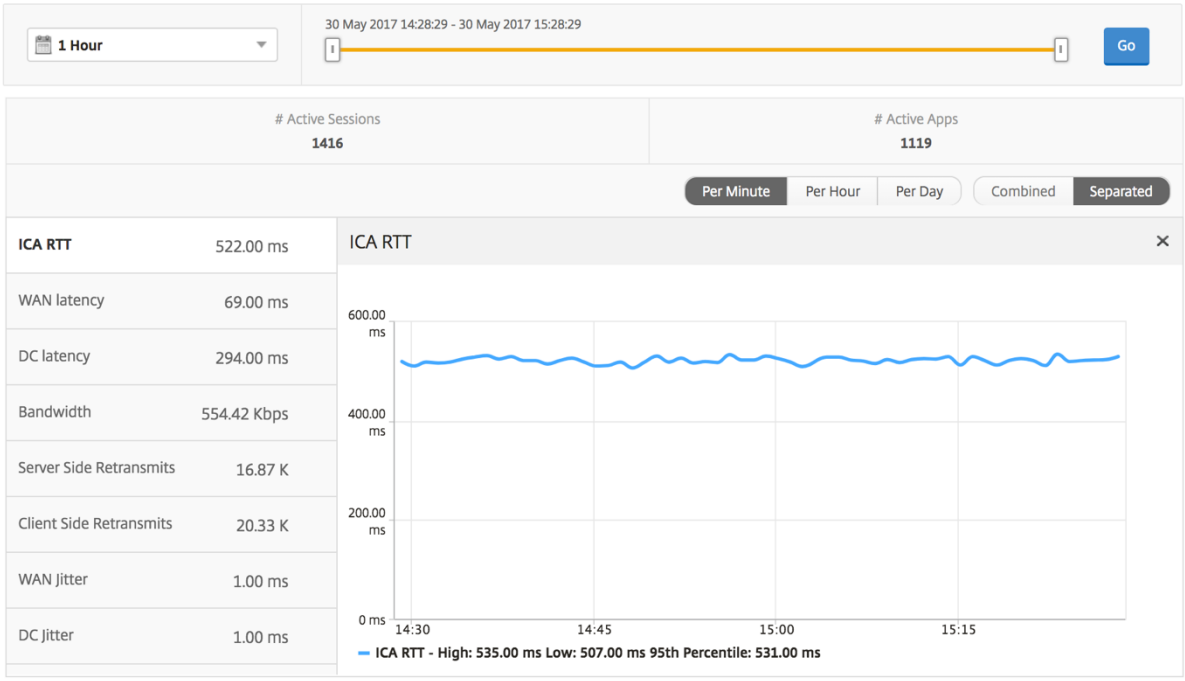
概要ビューには、選択したタイムラインでログインしたすべての Citrix Virtual Desktops に関するレポートが表示されます。

以下のメトリクスとレポートでは、明確な記載がない限り選択した期間の対応する値が表示されます。

折れ線グラフ

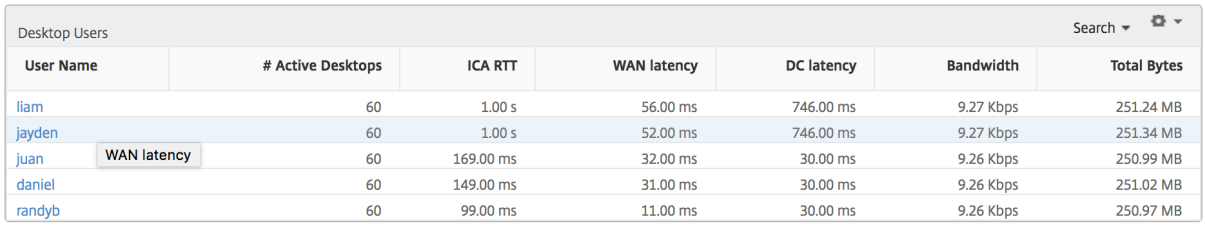
メトリック	説明
アクティブなセッション数	この数値は、アクティブな Citrix Virtual Apps and Desktops セッションの数を示します。
アクティブなアプリケーション数	この数値は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、Citrix ADC からエンドユーザーへ。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、Citrix ADC からバックエンドサーバーまでです。

メトリック	説明
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
サーバー側の再転送	Citrix ADC とバックエンドサーバー間の接続で再送信されたパケット数。
クライアント側の再転送	Citrix ADC とエンドユーザー間の接続で再送信されたパケット数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	Citrix ADC とエンドユーザー間の接続で再送信タイムアウトが発生した回数。
Server side fast RTO	Citrix ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。
クライアント側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがアドバタイズした回数を表します。
サーバー側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウサイズがゼロであることをサーバーがアドバタイズした回数を表します。



デスクトップ概要レポート

メトリック	説明
アクティブなセッション	一定期間中のアクティブな Citrix Virtual Desktop セッションの総数。
Active Desktops	特定の時間間隔におけるアクティブな Citrix Virtual Desktops 合計数。
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、Citrix ADC からエンドユーザーへ。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、Citrix ADC からバックエンドサーバーまでです。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。



しきい値レポート

しきい値レポートは、選択した期間内に エンティティが Desktop として選択された場合に、違反したしきい値の数を表します。

［**Per Dekstop**］ビュー

デスクトップごとの表示では、選択した Citrix Virtual Desktop に関する詳細なエンドユーザーエクスペリエンスレポートが提供されます。

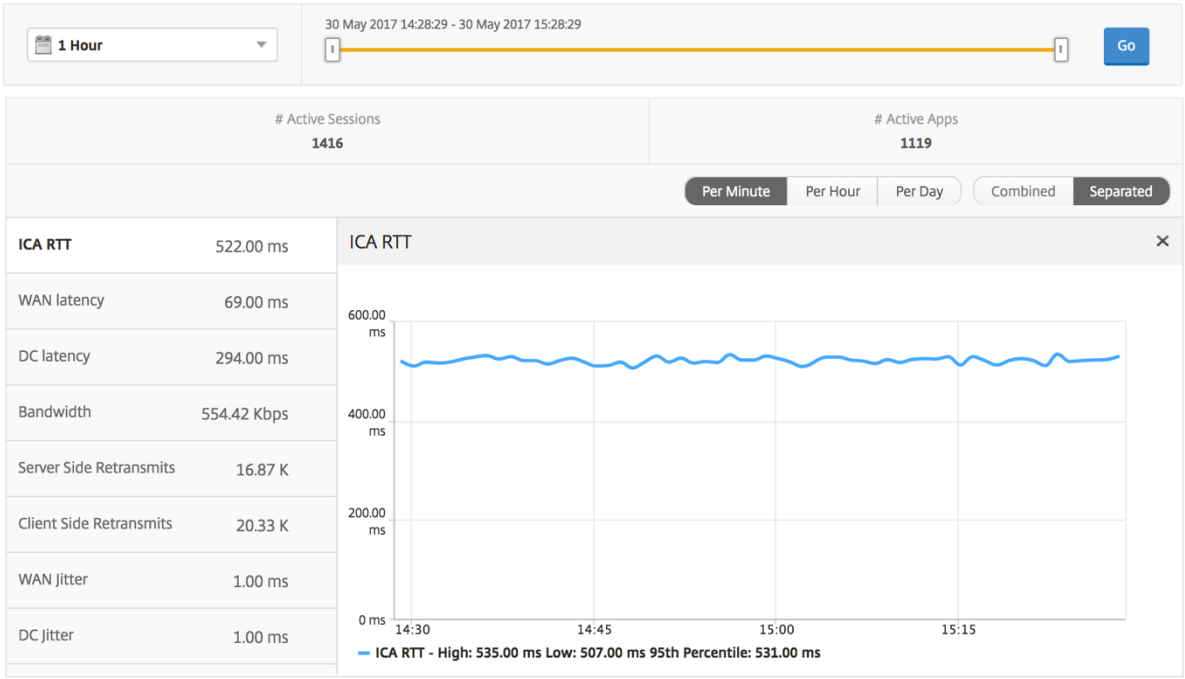
特定のデスクトップ・ビューに移動するには:

1. [**Analytics > [HDX Insight] > [**デスクトップ**]** に移動します。
2. デスクトップの概要レポートから特定のデスクトップを選択します。

折れ線グラフ

メトリック	説明
アクティブなセッション数	この数値は、アクティブな Citrix Virtual Apps and Desktops セッションの数を示します。
アクティブなアプリケーション数	この数値は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、Citrix ADC からエンドユーザーへ。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、Citrix ADC からバックエンドサーバーまでです。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
サーバー側の再転送	Citrix ADC とバックエンドサーバー間の接続で再送信されたパケット数。
クライアント側の再転送	Citrix ADC とエンドユーザー間の接続で再送信されたパケット数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	Citrix ADC とエンドユーザー間の接続で再送信タイムアウトが発生した回数。
Server side fast RTO	Citrix ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。
クライアント側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがアドバタイズした回数を表します。

メトリック	説明
サーバー側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウサイズがゼロであることをサーバーがアドバタイズした回数を表します。

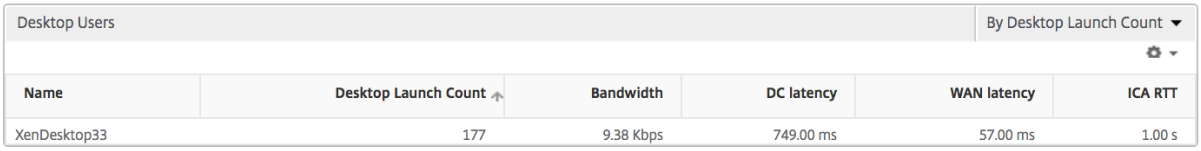


デスクトップユーザーレポート

この表は、特定のユーザーの Citrix Virtual Desktop セッションに関する洞察を示しています。以下のメトリクスは［Desktop Launch Count］および［Bandwidth］を基準にしてソートできます。

メトリック	説明
名前	Citrix Virtual Desktop の名前。
デスクトップの起動数	デスクトップが起動された回数です。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、Citrix ADC からバックエンドサーバーまでです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、Citrix ADC からエンドユーザーへ。

メトリック	説明
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。



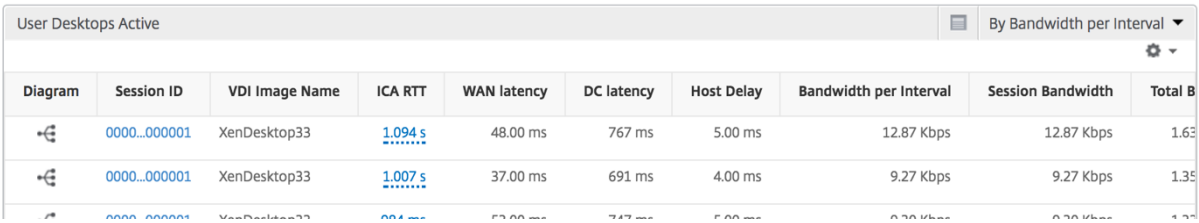
ユーザーデスクトップのアクティブ/非アクティブレポート

以下のメトリクスは、[Bandwidth per Interval]、[Session Reconnects]、および［ACR Counts］を基準にしてソートできます。

メトリック	説明
セッション ID	ICA セッションの一意の ID。
セッションの種類	アプリケーション/デスクトップ。
状態	緑はアクティブなセッション、赤は非アクティブなセッション。
ホストの遅延	サーバーネットワークが原因で、Citrix ADC を通過する ICA トラフィックの平均遅延。
間隔あたりの帯域幅	特定の期間にセッションで使用された帯域幅です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
間隔あたりのバイト数	特定の期間にセッションで使用されたバイト数。
開始時刻	セッションの開始時間。
アップタイム	セッションの実行時間
クライアント IP アドレス	エンドユーザーの IP。
サーバー IP アドレス	バックエンド/ Citrix Virtual App サーバー IP。
NetScaler IP Address	NetScaler の管理 IP（NSIP）。
クライアントの種類	レシーバタイプ-Citrix Windows クライアント
クライアントのバージョン	Receiver のバージョン。

メトリック	説明
MSI	ブール値（[Yes］または［No]）。セッションがマルチストリーム ICA かどうかを表します。
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスの種類	ICA セッションのアクセスモードを表示します。たとえば、Citrix ADC ゲートウェイのユーザー/透過モードなどです。
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB の状態	緑はアクティブ、赤は非アクティブ。
許可された USB インスタンス数	受け入れられた USB インスタンス数。
拒否された USB インスタンス数	拒否された USB インスタンス数。
停止された USB インスタンス数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェイルオーバーカウント	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、Citrix ADC からエンドユーザーへ。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、Citrix ADC からバックエンドサーバーまでです。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。
サーバー側の再転送	Citrix ADC とバックエンドサーバー間の接続で再送信されたパケット数。

メトリック	説明
クライアント側の再転送	Citrix ADC とエンドユーザー間の接続で再送信されたパケット数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
クライアント側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがアドバタイズした回数を表します。
Client side fast RTO	Citrix ADC とエンドユーザー間の接続で再送信タイムアウトが発生した回数。
サーバー側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウサイズがゼロであることをサーバーがアドバタイズした回数を表します。
Server side fast RTO	Citrix ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。
VDI イメージ名	ユーザーが接続している Citrix Virtual Desktop の名前
ダイアグラム	



［**Per Dekstop Session**］ビュー

デスクトップごとのセッションビューでは、選択した特定の Citrix Virtual Desktop セッションのレポートが表示されます。

デスクトップ・セッション・ビューに移動するには：

1. [分析] > [**HDX Insight**] > [デスクトップ] に移動します。
2. デスクトップ 概要レポートから特定のデスクトップを選択します。
3. 現在のセッションレポートからセッションを選択します。

時系列グラフ

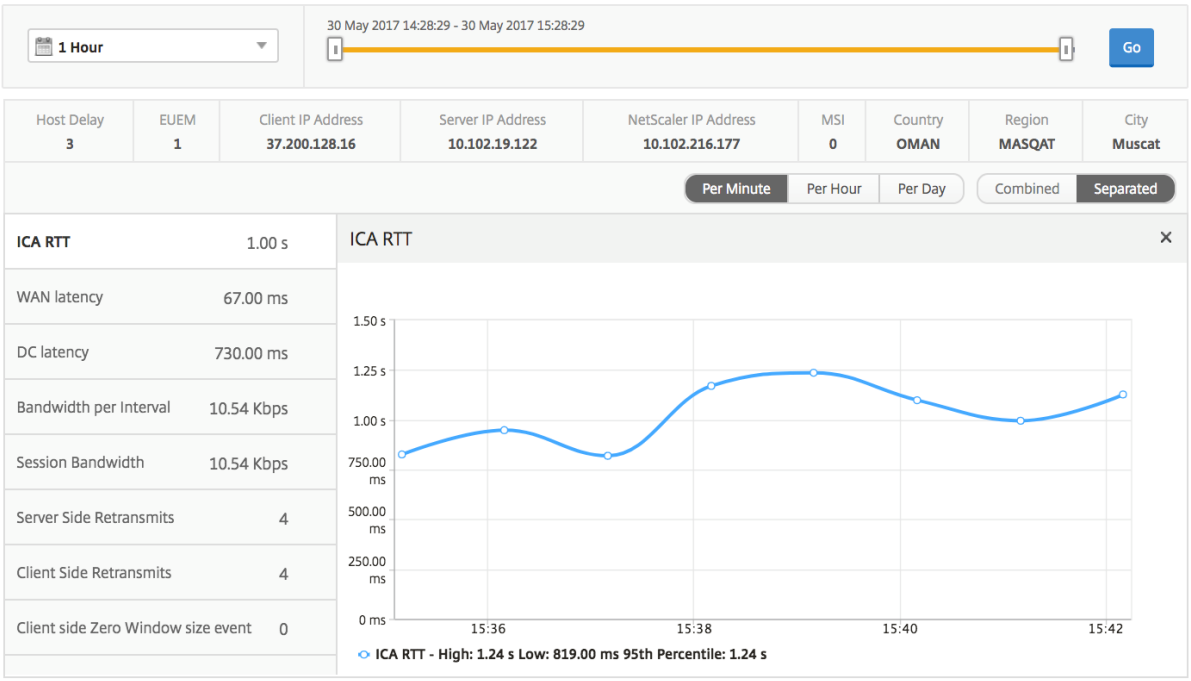
ユーザーごとのセッションビューには、選択した特定のユーザーのセッションに関するレポートが表示されます。

選択したユーザーのセッションのメトリックを表示する手順は、次のとおりです。

1. [**Analytics**] > [**HDX Insight**] > [ユーザー] に移動します。
2.「ユーザー 概要レポート」セクションから特定のユーザーを選択します。
3.「現在のセッション」列または「終了したセッション」列からセッションを選択します。

メトリック	説明
セッション再接続	この数値は、アクティブな Citrix Virtual Apps and Desktops セッションの数を示します。
ACR 数	この数値は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、Citrix ADC からエンドユーザーへ。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、Citrix ADC からバックエンドサーバーまでです。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
サーバー側の再転送	Citrix ADC とバックエンドサーバー間の接続で再送信されたパケット数。
クライアント側の再転送	Citrix ADC とエンドユーザー間の接続で再送信されたパケット数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	Citrix ADC とエンドユーザー間の接続で再送信タイムアウトが発生した回数。
Server side fast RTO	Citrix ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。
間隔あたりの帯域幅	特定の期間にセッションで使用された帯域幅です。

メトリック	説明
サーバー側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウサイズがゼロであることをサーバーがアドバタイズした回数を表します。
クライアント側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがアドバタイズした回数を表します。



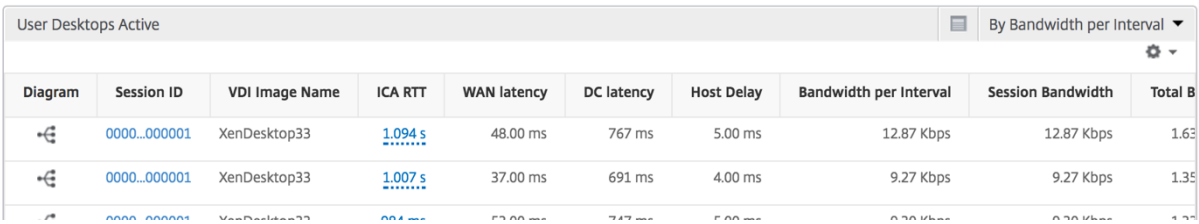
関連デスクトップセッションレポート

以下のメトリクスは、[Bandwidth per Interval]、[Session Reconnects]、および［ACR Counts］を基準にしてソートできます。

メトリック	説明
セッション ID	ICA セッションの一意の ID。
セッションの種類	アプリケーション/デスクトップ。
状態	緑はアクティブなセッション、赤は非アクティブなセッション。
ホストの遅延	サーバーネットワークが原因で、Citrix ADC を通過する ICA トラフィックの平均遅延。

メトリック	説明
間隔あたりの帯域幅	特定の期間にセッションで使用された帯域幅です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
間隔あたりのバイト数	特定の期間にセッションで使用されたバイト数。
開始時刻	セッションの開始時間。
アップタイム	セッションの実行時間
クライアント IP アドレス	エンドユーザーの IP。
サーバー IP アドレス	バックエンド/ Citrix Virtual App サーバー IP。
NetScaler IP Address	NetScaler の管理 IP（NSIP）。
クライアントの種類	レシーバタイプ-Citrix Windows クライアント
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値（[Yes］または［No]）。セッションがマルチストリーム ICA かどうかを表します。
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。
ユーザーアクセスの種類	ICA セッションのアクセスモードを表示します。たとえば、Citrix ADC ゲートウェイのユーザー/透過モードなどです。
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB の状態	緑はアクティブ、赤は非アクティブ。
許可された USB インスタンス数	受け入れられた USB インスタンス数。
拒否された USB インスタンス数	拒否された USB インスタンス数。
停止された USB インスタンス数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェイルオーバーカウント	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。

メトリック	説明
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、Citrix ADC からエンドユーザーへ。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、Citrix ADC からバックエンドサーバーまでです。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。
サーバー側の再転送	Citrix ADC とバックエンドサーバー間の接続で再送信されたパケット数。
クライアント側の再転送	Citrix ADC とエンドユーザー間の接続で再送信されたパケット数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
クライアント側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがアドバタイズした回数を表します。
Client side fast RTO	Citrix ADC とエンドユーザー間の接続で再送信タイムアウトが発生した回数。
サーバー側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウサイズがゼロであることをサーバーがアドバタイズした回数を表します。
Server side fast RTO	Citrix ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。
VDI イメージ名	ユーザーが接続している Citrix Virtual Desktop の名前

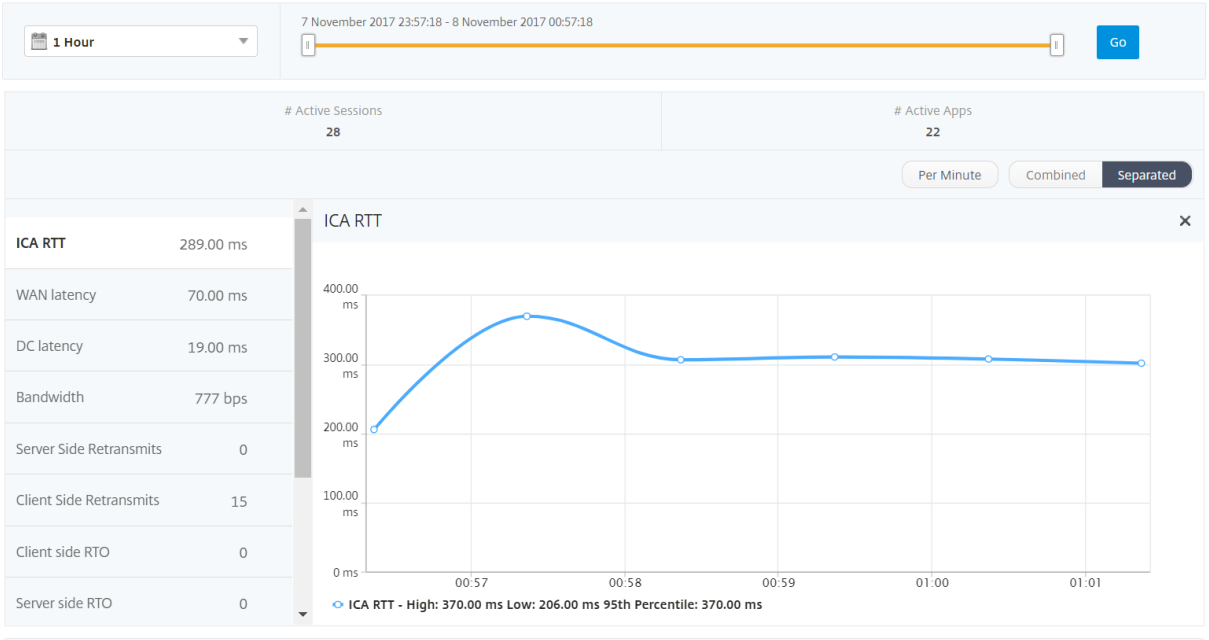


［**User**］ビューのレポートとメトリック

May 7, 2021

このビューのレポートと指標は、Citrix Virtual App またはデスクトップユーザーごとに表示されます。

Analytics > **HDX Insight** > ユーザー



［**Summary**］ビュー

［Summary］ビューには、選択した期間中にログインしたすべてのユーザーのレポートが表示されます。このビューのすべての指標/レポートには、特に指定されていない限り、選択した期間の指標/レポートに対応する値が表示されます。

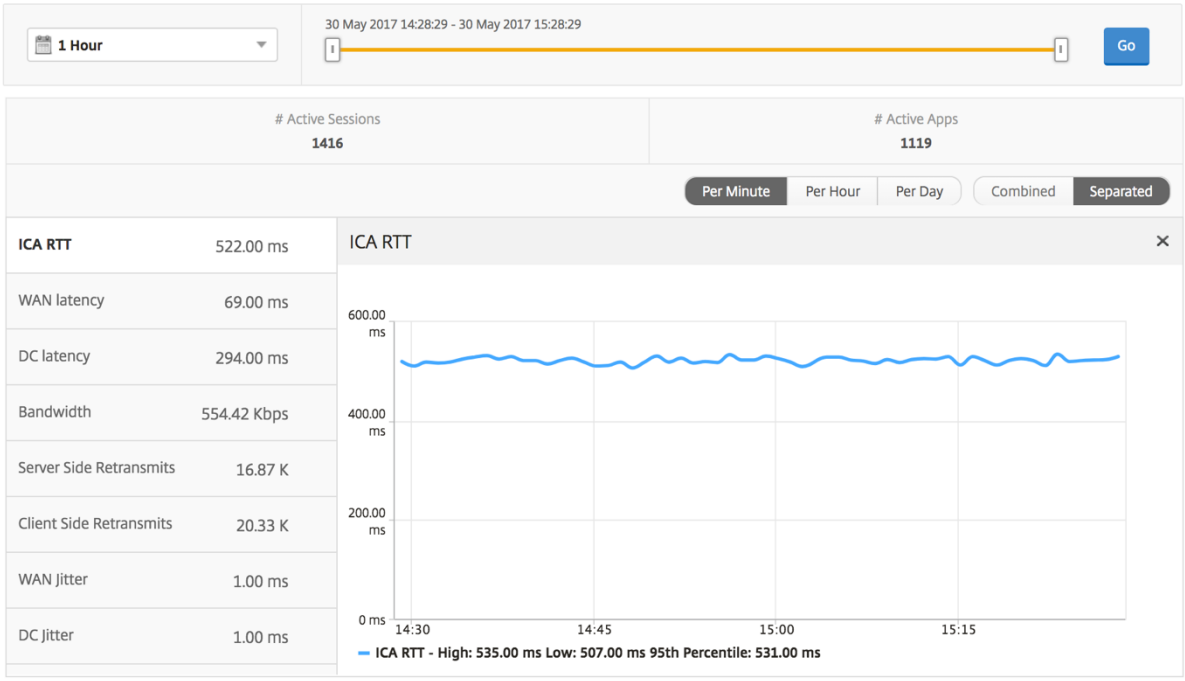
選択した期間を変更するには、次の手順に従います。

1. 期間リストまたはタイムスライダを使用して、目的の時間間隔を設定します。
2. ［**Go**］をクリックします。

折れ線グラフ

メトリック	説明
アクティブなセッション数	この数値は、アクティブな Citrix Virtual Apps and Desktops セッションの数を示します。

メトリック	説明
アクティブなアプリケーション数	この数値は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、Citrix ADC からエンドユーザーへ。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、Citrix ADC からバックエンドサーバーまでです。
帯域幅	選択した時間間隔におけるエンドツーエンド通信で取得されたビット/秒の合計数。
サーバー側の再転送	Citrix ADC とバックエンドサーバー間の接続で再送信されたパケット数。
クライアント側の再転送	Citrix ADC とエンドユーザー間の接続で再送信されたパケット数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	Citrix ADC とエンドユーザー間の接続で再送信タイムアウトが発生した回数。
Server side fast RTO	Citrix ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。
クライアント側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがアドバタイズした回数を表します。
サーバー側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウサイズがゼロであることをサーバーがアドバタイズした回数を表します。



［**User Summary**］レポート

このレポートに固有のメトリックは以下のとおりです。

メトリック	説明
アクティブなセッション数	この数値は、アクティブな Citrix Virtual Apps and Desktops セッションの数を示します。
アクティブなアプリケーション数	この数値は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、Citrix ADC からエンドユーザーへ。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、Citrix ADC からバックエンドサーバーまでです。
帯域幅	選択した時間間隔におけるエンドツーエンド通信で取得されたビット/秒の合計数。
サーバー側の再転送	Citrix ADC とバックエンドサーバー間の接続で再送信されたパケット数。

メトリック	説明
クライアント側の再転送	Citrix ADC とエンドユーザー間の接続で再送信されたパケット数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	Citrix ADC とエンドユーザー間の接続で再送信タイムアウトが発生した回数。
Server side fast RTO	Citrix ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。
クライアント側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがアドバタイズした回数を表します。
サーバー側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウサイズがゼロであることをサーバーがアドバタイズした回数を表します。
アプリケーションの起動数合計	指定した期間にユーザーによって起動された合計アプリ数です。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。
Active Desktops	特定の時間間隔におけるアクティブな Citrix Virtual Desktops 合計数。

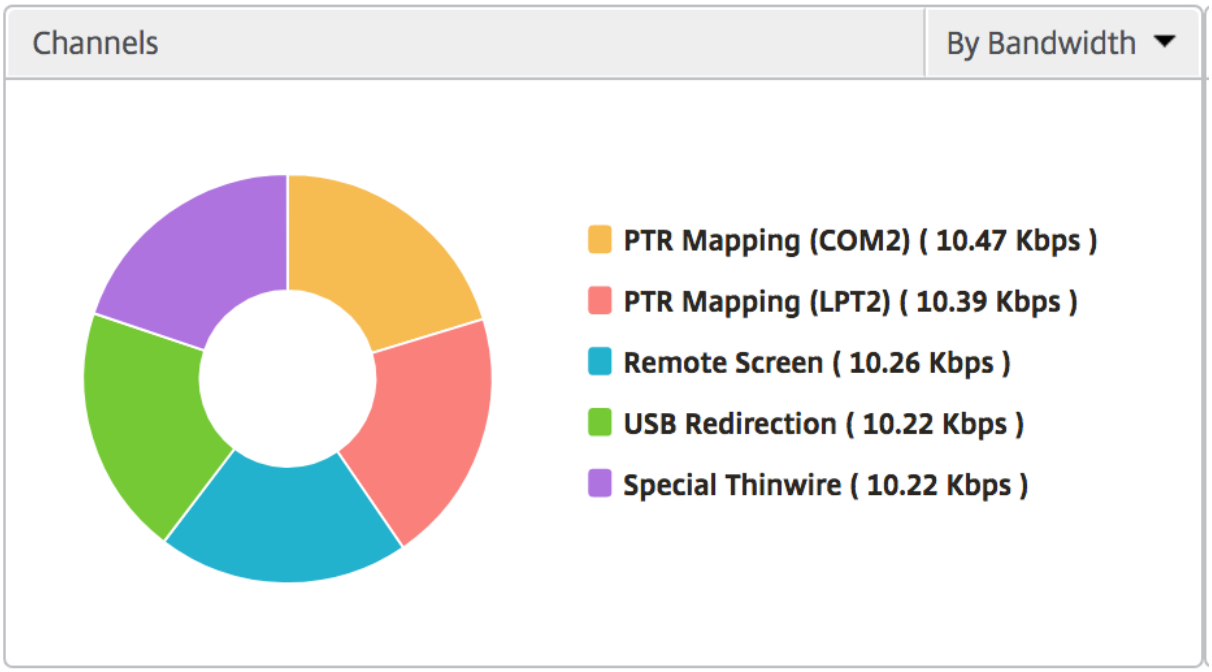
Users

Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

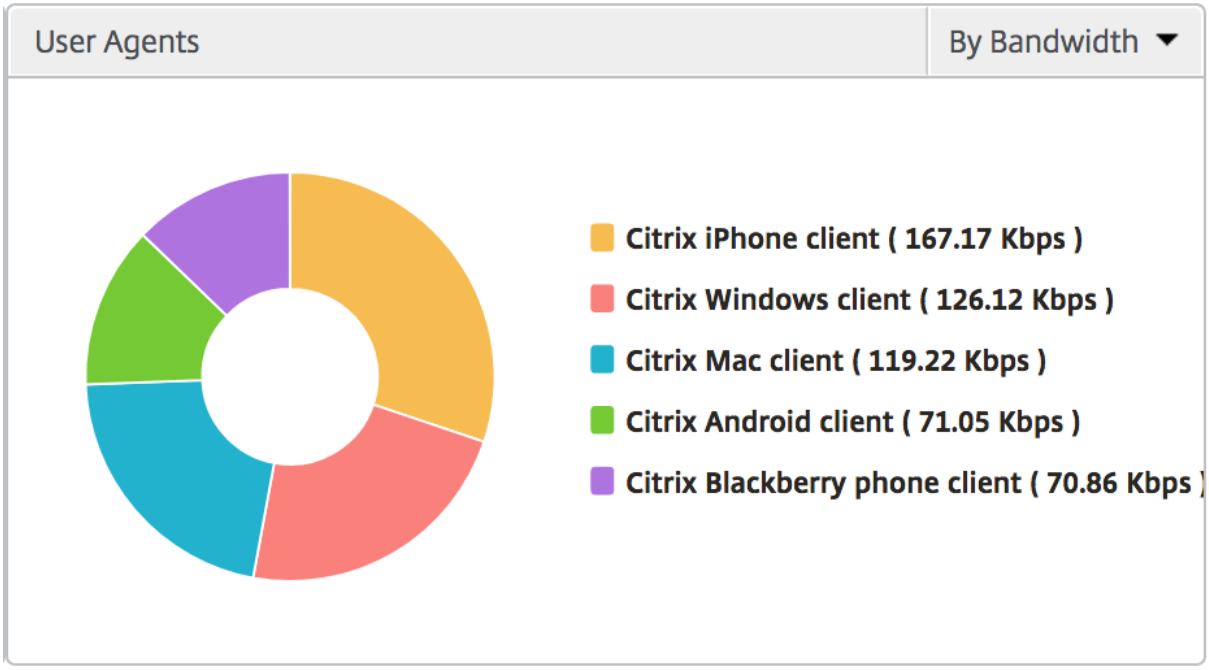
チャネル

Channels では、各 ICA 仮想チャネルで消費された全帯域幅または総バイト数をドーナツグラフ形式で表します。これらのメトリックは、［Bandwidth］または［Total bytes］で並べ替えることができます。



ユーザーエージェント

ユーザーエージェントは、各エンドポイントで消費される全体の帯域幅/合計ビットをドーナツグラフで表します。これらのメトリックは、［Bandwidth］または［Total bytes］で並べ替えることができます。



Thresholds Breach Count

［Thresholds Breach Count］メトリックは、指定した期間において違反があったしきい値の数を表します。<!— 詳細については、「しきい値とアラートの作成方法」(/en-us/citrix-application-delivery-management-service/analytics/analytics-how-to-articles/how-to-create-thresholds-and-alerts-using-mas.html) を参照してください。。—>

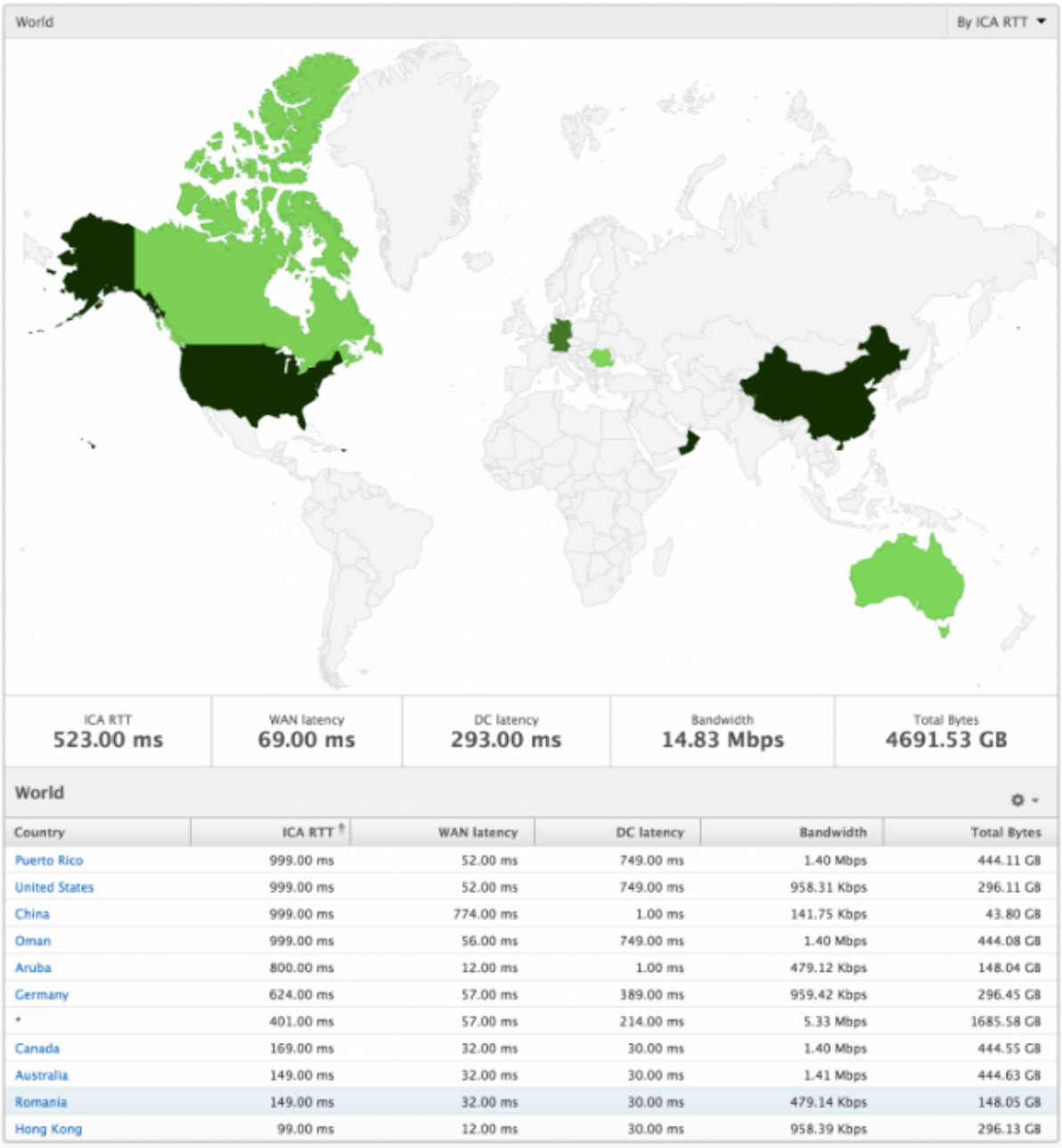
World Map

HDX Insight の［World Map］ビューでは、管理者が地理的な観点からユーザー履歴およびアクティブユーザーの詳細を確認できます。管理者は、単に地域をクリックするだけで、システムのワールドビューを表示したり、特定の国や都市にドリルダウンすることができます。管理者はさらにドリルダウンして、都市および州別に情報を表示できます。Citrix ADM バージョン 12.0 以降では、地理的な場所から接続しているユーザーにドリルダウンできます。

HDX Insight のワールドマップでは、以下の詳細を表示できます。また、各指標の密度はヒートマップの形式で表示されます。

- ICA 往復時間
- WAN 遅延
- DC の遅延
- 帯域幅

- バイト数合計



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

［**Per User**］ビュー

[Per User］ビューには、選択した特定のユーザーについて詳細なエンドユーザーエクスペリエンスに関するレポートが示されます。

特定のユーザーのメトリックスに移動するには、次の手順に従います。

1. [**Analytics**] > [**HDX Insight**] > [ユーザー] に移動します。

2.［User Summary］レポートで目的のユーザーを選択します。

折れ線グラフ

折れ線グラフには、指定した期間における選択したユーザーのメトリックすべての概要が表示されます。

［**Current/Terminated Sessions**］レポート

このレポートは、選択したユーザーの現在/終了済みのユーザーセッションすべてに関係します。これらのメトリックは、Start Time、Session Reconnects、ACR Counts を基準にして並べ替えることができます。

メトリック	説明
セッション ID	ICA セッションの一意の ID。
セッションの種類	アプリケーション/デスクトップ。
状態	緑はアクティブなセッション、赤は非アクティブなセッション。
ホストの遅延	サーバーネットワークが原因で、Citrix ADC を通過する ICA トラフィックの平均遅延。
間隔あたりの帯域幅	特定の期間にセッションで使用された帯域幅です。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
間隔あたりのバイト数	特定の期間にセッションで使用されたバイト数。
開始時刻	セッションの開始時間。
アップタイム	セッションの実行時間
クライアント IP アドレス	エンドユーザーの IP。
サーバー IP アドレス	バックエンド/ Citrix 仮想アプリサーバーの IP。
NetScaler IP Address	NetScaler の管理 IP（NSIP）。
クライアントの種類	レシーバタイプ-Citrix Windows クライアント
クライアントのバージョン	Receiver のバージョン。
MSI	ブール値（［Yes］または［No］）。セッションがマルチストリーム ICA かどうかを表します。
セッション再接続	セッションが再接続された回数。
ACR 数	クライアントでユーザーが切断されたセッションに自動的に再接続した回数の合計。

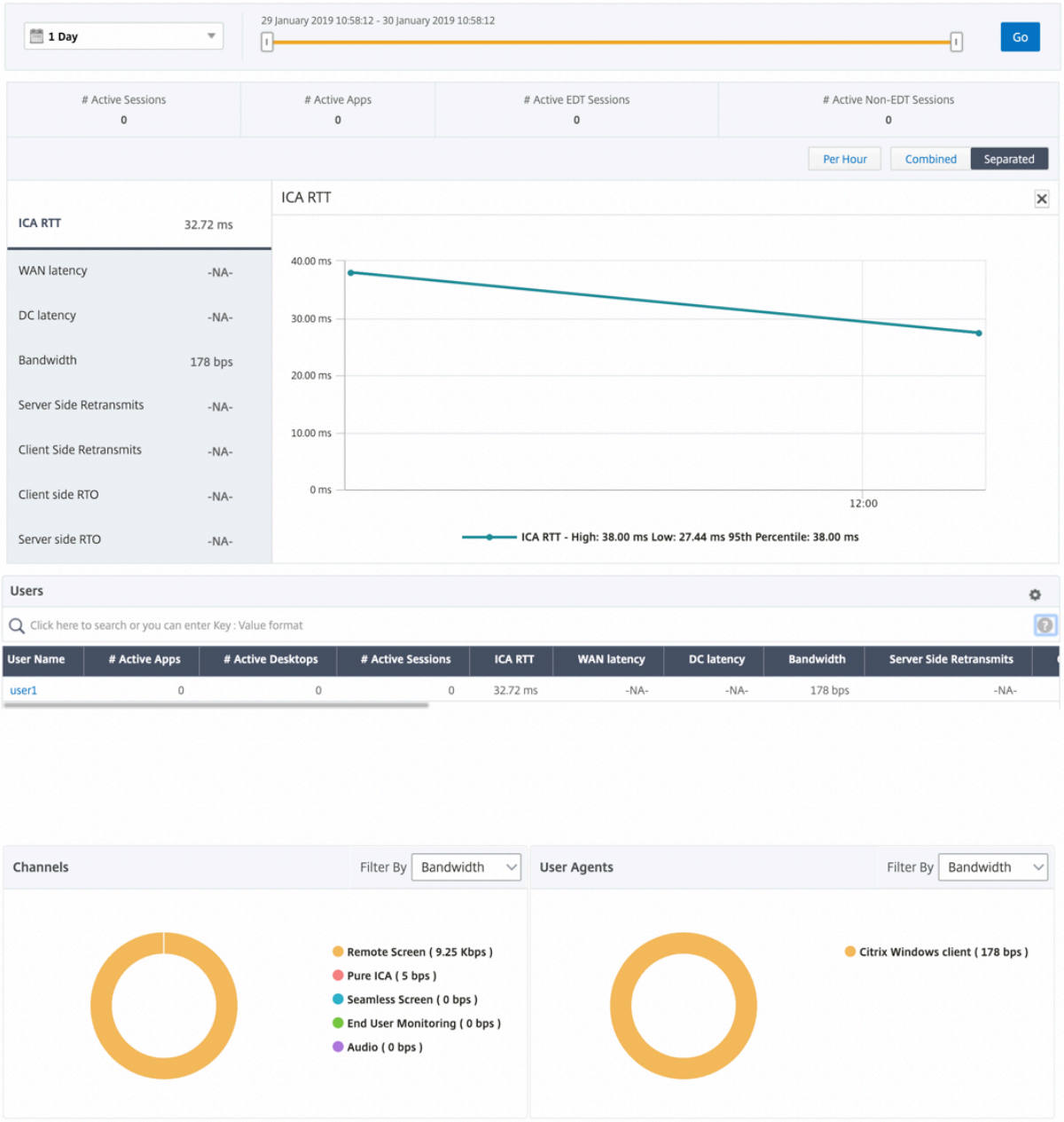
メトリック	説明
ユーザーアクセスの種類	ICA セッションのアクセスモードを表示します。たとえば、Citrix ADC ゲートウェイのユーザー/透過モードなどです。
国	セッションが確立された国。
リージョン	セッションが確立されたリージョン。
市区町村	セッションが確立された市区町村。
USB の状態	緑はアクティブ、赤は非アクティブ。
許可された USB インスタンス数	受け入れられた USB インスタンス数。
拒否された USB インスタンス数	拒否された USB インスタンス数。
停止された USB インスタンス数	停止した USB インスタンス数。
クライアントホスト名	クライアントのホスト名。
HA フェイルオーバーカウント	HA フェールオーバーが発生した回数。
終了の理由	セッション終了の理由を表示します。たとえば、「ICA Session Timeout」、「Session terminated by the user」などと表示されます。
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、Citrix ADC からエンドユーザーへ。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、Citrix ADC からバックエンドサーバーまでです。
バイト数合計	選択した期間にユーザーによって使用された合計バイト数です。
サーバー側の再転送	Citrix ADC とバックエンドサーバー間の接続で再送信されたパケット数。
クライアント側の再転送	Citrix ADC とエンドユーザー間の接続で再送信されたパケット数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。

メトリック	説明
クライアント側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがアドバタイズした回数を表します。
Client side fast RTO	Citrix ADC とエンドユーザーの間の接続で再送信タイムアウトが発生した回数。
サーバー側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウサイズがゼロであることをサーバーがアドバタイズした回数を表します。
Server side fast RTO	Citrix ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。

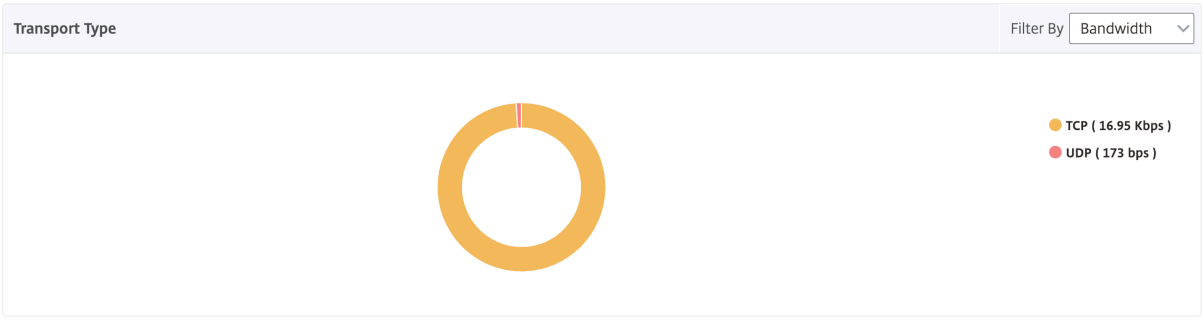
HDX Insight での **EDT** のサポート

Citrix Application Delivery Management（ADM）では、HDX Insight ight の分析を表示するための啓発データトランスポート（EDT）がサポートされるようになりました。つまり、ADM は UDP プロトコルと TCP プロトコルの両方をサポートするようになりました。Citrix Gateway の EDT サポートにより、Citrix Receiver を実行しているユーザーの仮想デスクトップの高品位インセッションユーザーエクスペリエンスが保証されます。

HDX Insight で、アクティブなセッションレポートの一部として EDT セッション数と非 EDT セッション数が表示されるようになりました。「ユーザー」(Users) テーブルには、システム内のすべてのユーザーの詳細なレポートが表示されます。この表には、WAN レイテンシー、DC レイテンシー、再送信、RTO などのメトリックが示されています。これらのメトリックのいくつかは、現在 TCP スタックから計算されるため、EDT セッションを持つユーザーには使用できません。したがって、彼らは「NA」として登場する。

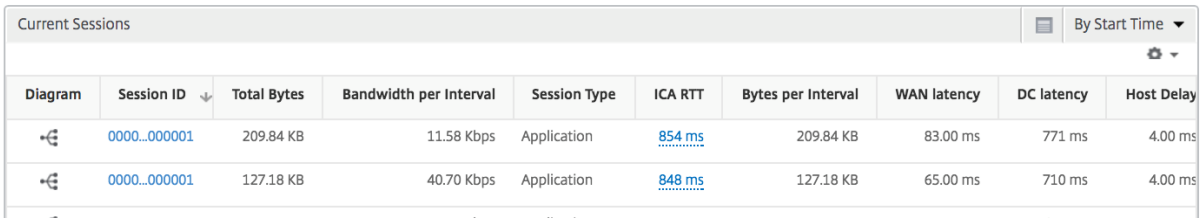


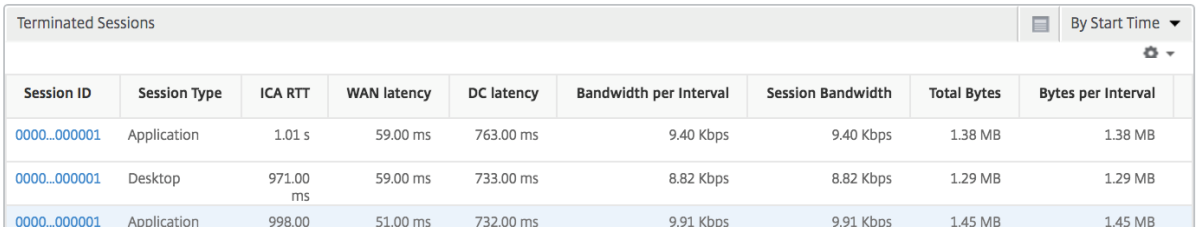
新しいドーナツチャートが導入され、ユーザが消費する帯域幅と、ユーザが使用するプロトコルのタイプに基づく合計バイト数を確認できるようになりました。



HDX Insight 指標は **Citrix ADM 12.0** 以降から入手可能

L7 Client-side Latency	ICA クライアントと Citrix ADC インスタンスの間で観測された平均 L7 遅延時間。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。
L7 Server-side Latency	Citrix ADC デバイスと Citrix Virtual App 間で観測された平均 L7 レイテンシー。このメトリックは、Citrix 以外のデバイスが配信パスに存在する場合に役立ちます。
違反の最大遅延	定義済みしきい値の違反が一定期間に発生した場合の、L7 遅延の最大値。
違反の平均遅延	システムが「L7 遅延時間を超過」した状態のときの、L7 遅延の平均値。
L7 しきい値違反数	L7 のしきい値違反が発生した回数。

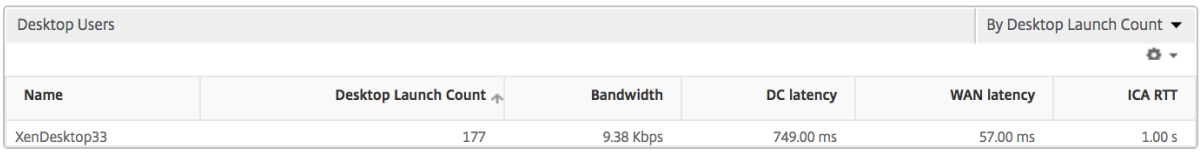




デスクトップユーザー

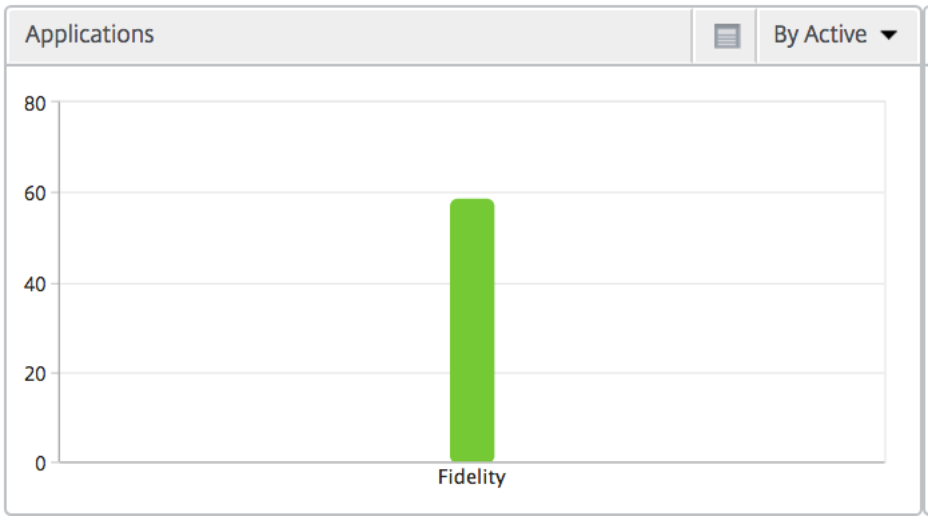
この表は、特定のユーザーの Citrix Virtual Desktop セッションに関する洞察を示しています。以下のメトリクスは［Desktop Launch Count］および［Bandwidth］を基準にしてソートできます。

メトリック	説明
名前	Citrix Virtual Desktop の名前。
デスクトップの起動数	デスクトップが起動された回数です。
帯域幅	選択した時間間隔におけるエンドツーエンド通信で取得されたビット/秒の合計数。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、Citrix ADC からバックエンドサーバーまでです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、Citrix ADC からエンドユーザーへ。
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。



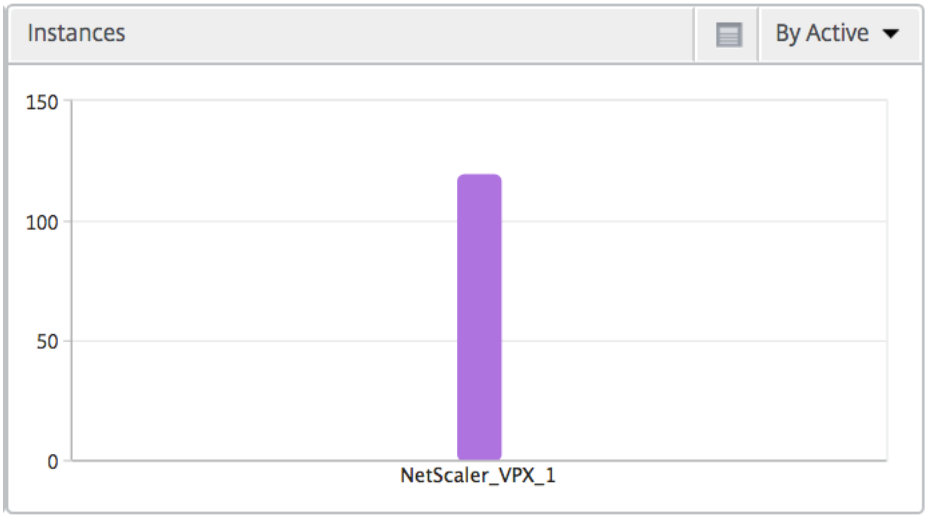
アプリケーション

アクティブでソートされたアプリ、合計セッション起動数、合計アプリ起動数、および起動期間を表す棒グラフ。



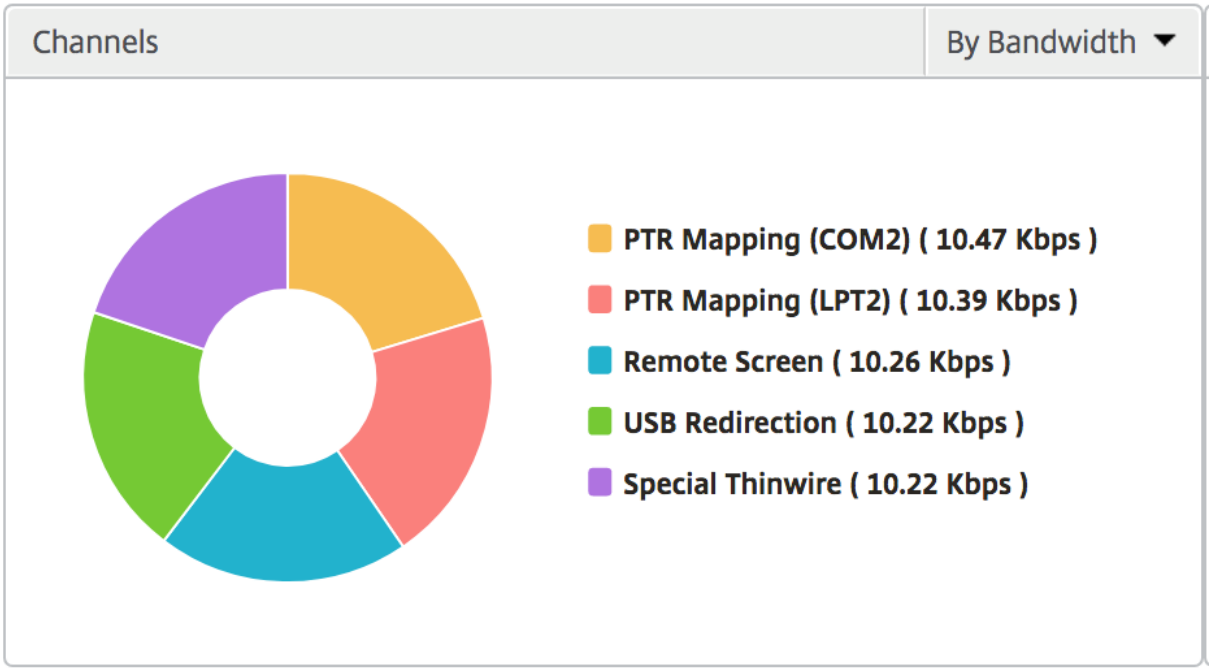
インスタンス

アクティブおよびアプリ総数でソートされた ADC インスタンスを表す棒グラフ



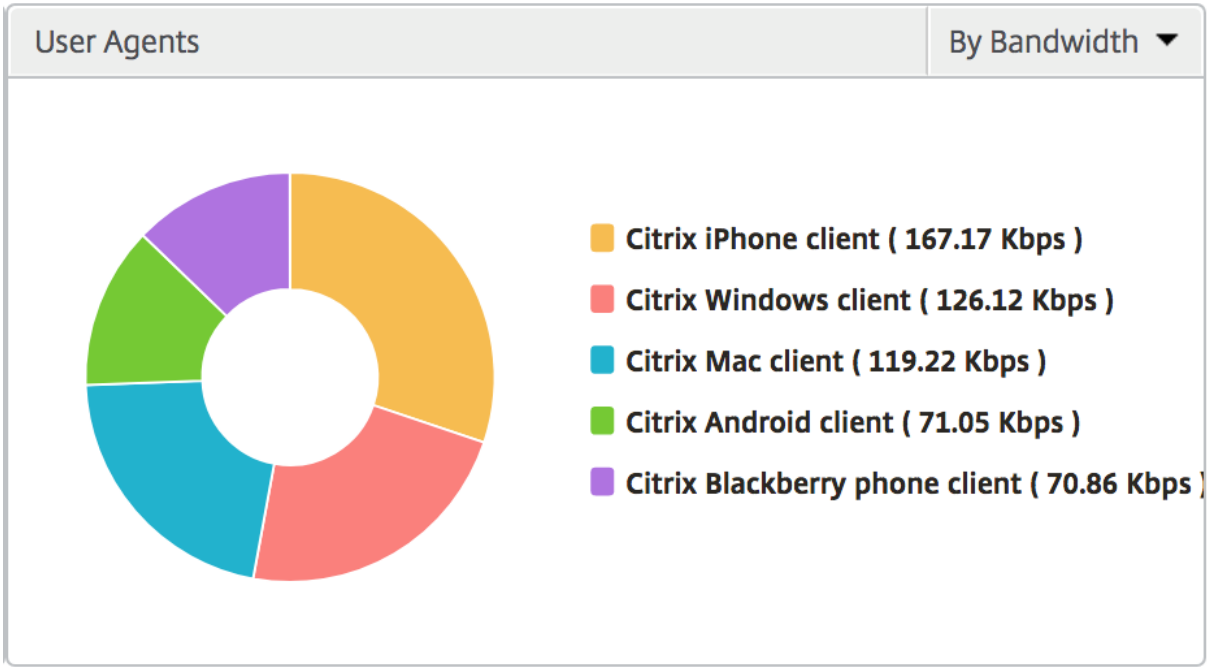
チャネル

チャネルは、全体帯域幅または各 ICA 仮想チャネルによって消費される総ビットをドーナツグラフで表します。帯域幅または合計ビットでメトリックを並べ替えることもできます。



ユーザーエージェント

ユーザーエージェントは、各エンドポイントで消費される全体の帯域幅/合計ビットをドーナツグラフで表します。帯域幅または合計ビットでメトリックを並べ替えることもできます。



Per User Session ビュー

ユーザーごとのセッションビューには、選択した特定のユーザーのセッションに関するレポートが表示されます。

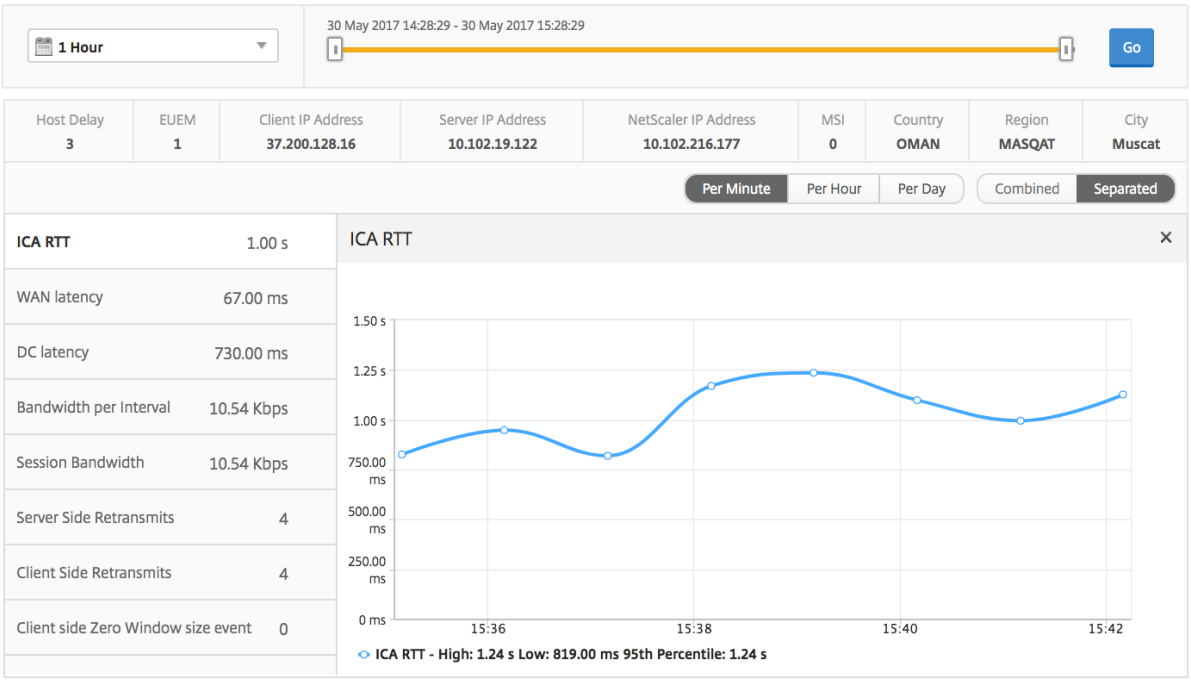
選択したユーザーのセッションのメトリックを表示する手順は、次のとおりです。

1. [**Analytics**] > [**HDX Insight**] > [ユーザー] に移動します。
2.「ユーザー 概要レポート」セクションから特定のユーザーを選択します。
3.「現在のセッション」列または「終了したセッション」列からセッションを選択します。

時系列グラフ

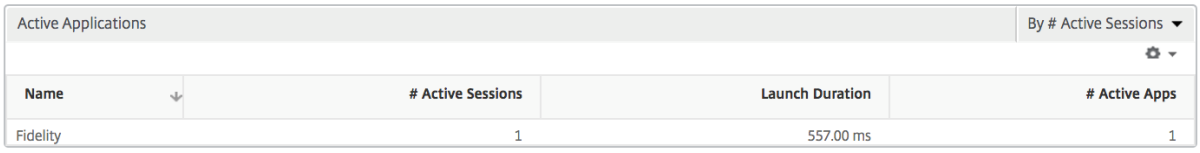
メトリック	説明
セッション再接続	この数値は、アクティブな Citrix Virtual Apps and Desktops セッションの数を示します。
ACR 数	この数値は、アクティブな Citrix Virtual App セッションの数を示します。
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、Citrix ADC からエンドユーザーへ。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、Citrix ADC からバックエンドサーバーまでです。
セッション帯域幅	期間に関係なく、セッションで使用された帯域幅です。
サーバー側の再転送	Citrix ADC とバックエンドサーバー間の接続で再送信されたパケット数。
クライアント側の再転送	Citrix ADC とエンドユーザー間の接続で再送信されたパケット数。このメトリックの値が大きい場合、ユーザーエクスペリエンスがシームレスではないということではなく、再送信により帯域幅の使用率が増加していることを示します。
Client side fast RTO	Citrix ADC とエンドユーザー間の接続で再送信タイムアウトが発生した回数。
Server side fast RTO	Citrix ADC とバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。

メトリック	説明
間隔あたりの帯域幅	特定の期間にセッションで使用された帯域幅です。
サーバー側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウサイズがゼロであることをサーバーがアドバタイズした回数を表します。
クライアント側のゼロウィンドウサイズイベント	このカウンターは、TCP ウィンドウのサイズがゼロであることをクライアントがアドバタイズした回数を表します。



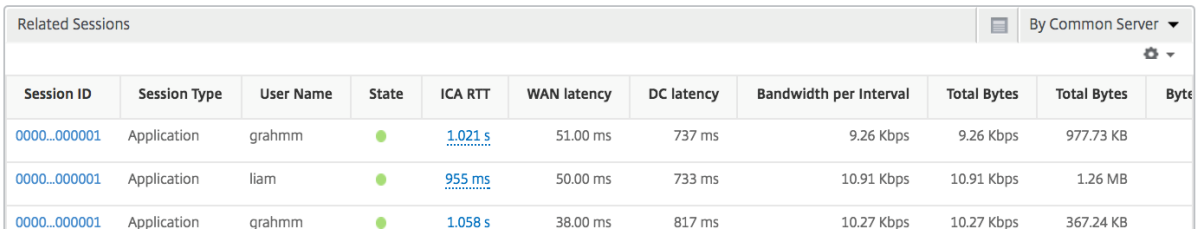
Active Applications

「アクティブなアプリケーション」セクションには、選択したユーザーのアクティブなアプリケーションが表示されます。これらのアプリケーションは、アクティブなセッション数および起動時間で並べ替えることができます。



関連セッション

「関連セッション」セクションには、選択したユーザーのセッションの関連セッションが表示されます。このリレーションシップは、共通サーバーまたは共通 Citrix ADC として選択できます。



Session ID	Session Type	User Name	State	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Total Bytes	Total Bytes	Byte
0000...000001	Application	grahmm		1.021 s	51.00 ms	737 ms	9.26 Kbps	9.26 Kbps	977.73 KB	
0000...000001	Application	liam		955 ms	50.00 ms	733 ms	10.91 Kbps	10.91 Kbps	1.26 MB	
0000...000001	Application	grahmm		1.058 s	38.00 ms	817 ms	10.27 Kbps	10.27 Kbps	367.24 KB	

インスタンスビューのレポートおよびメトリクス

May 7, 2021

インスタンスビューのレポートとメトリックスは、1 つ以上の Citrix ADC インスタンスに焦点を当てています。

[インスタンス**]** ビューにナビゲートするには、次の手順を実行します。

1. サポートされている Web ブラウザを使用して、Citrix ADM にログオンします。
2. [分析] > [**HDX Insight**] > [インスタンス] に移動します。

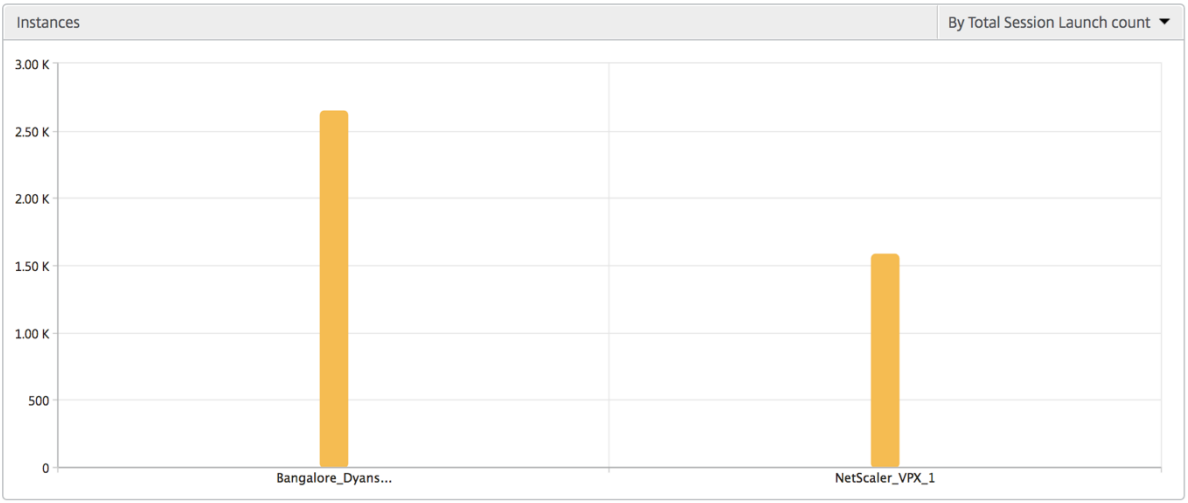
インスタンス概要ビュー

このビューは、Citrix ADM に追加されたすべての ADC インスタンスのレポートを表示するので、概要ビューと呼ばれます。

明示的に言及しない限り、これらすべての指標/レポートには、選択した期間に対応する値があります。

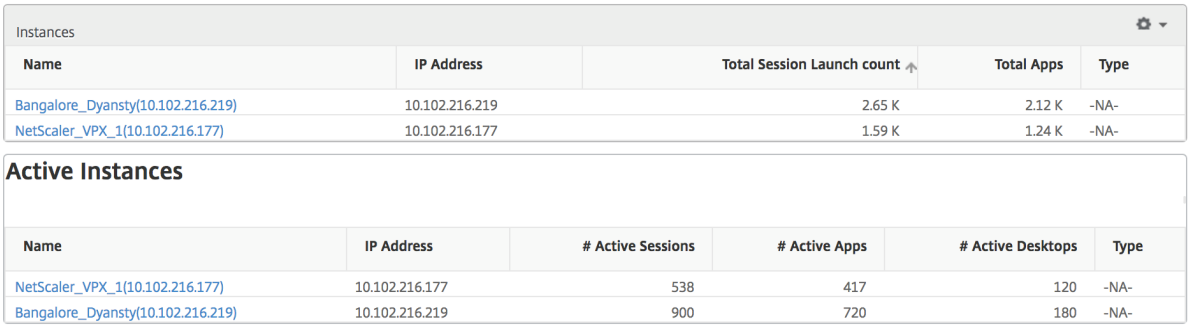
インスタンス棒グラフ

このグラフには、グラフキャンバスの右上にあるリストから、インスタンスと [セッション起動の合計数] と [合計アプリ数] が表示されます。



インスタンス/アクティブインスタンス概要レポート

メトリック	説明
名前	ADC インスタンスのホスト名。
IP アドレス	NetScaler の IP アドレスです。
セッションの起動数合計	特定の期間に作成された一意のユーザーセッションの合計数です。
アプリケーション合計数	特定の期間に起動された一意のアプリケーションの合計数です。
種類	-


Instances

Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

しきい値レポート

しきい値レポートは、選択した期間内に エンティティがインスタンスとして選択された場合に、違反したしきい値の数を表します。詳しくは、「しきい値とアラートの作成方法」を参照してください。

スキップされたフロー

スキップフローは、ICA 接続の解析が省略されたレコードのことです。このフローは、サポートされていない Citrix Virtual App または Desktop のバージョン、サポートされていないバージョンのレシーバまたはレシーバの種類を使用するなど、複数の理由で発生する可能性があります。このテーブルでは、IP アドレスとスキップフロー数が示されます。これらの受信機は、許可リスト受信機の一部ではない場合があります。したがって、これらのセッションはモニタリングからスキップされます。

ICA 解析に関連する問題の詳細については、Citrix ADC チェックリストでの HDX/ICA トラフィックのレコード生成に関する問題を参照してください。

Skipped Flows

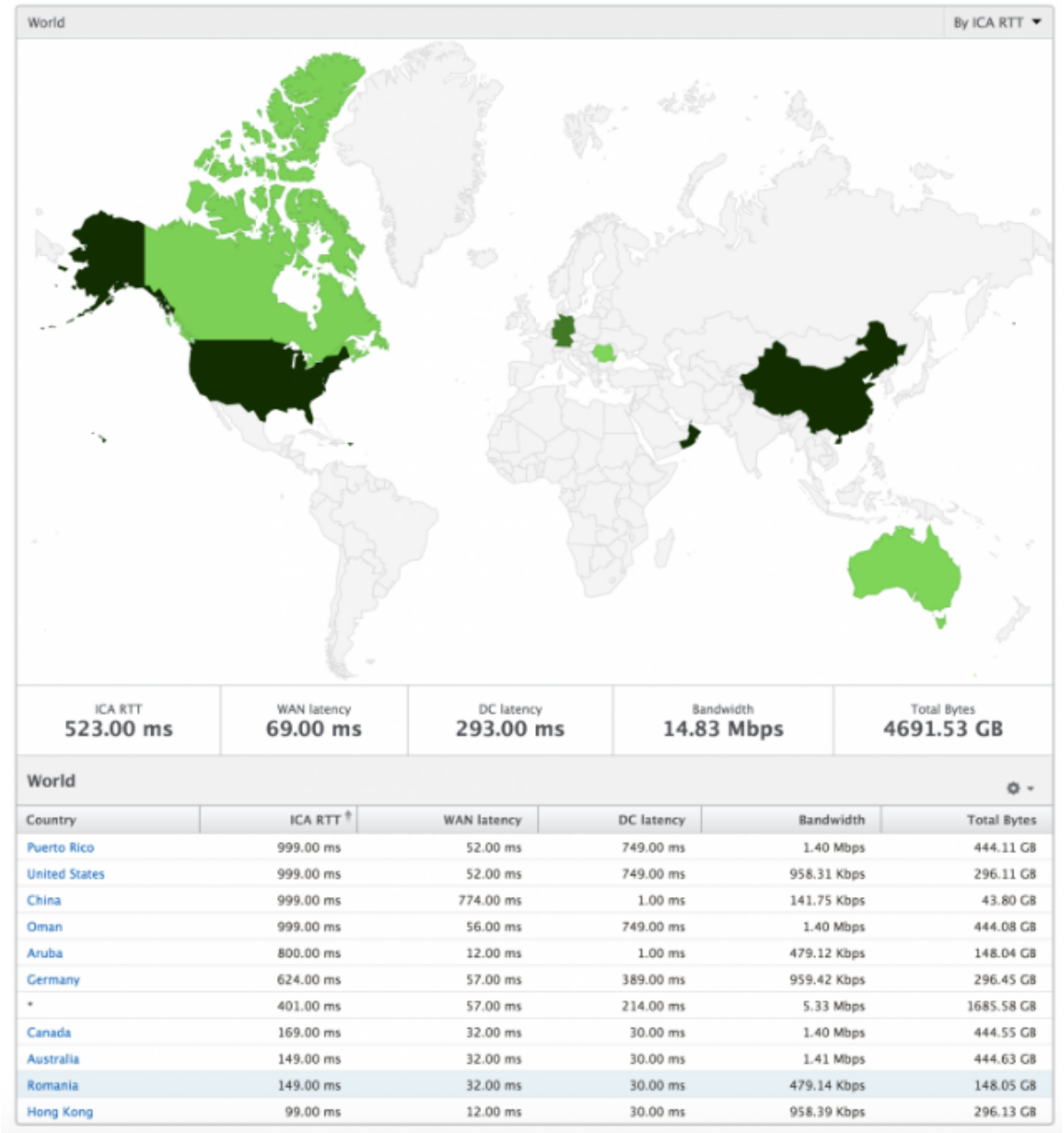
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

世界ビュー

HDX Insight の世界地図ビューでは、管理者が地理的な観点からユーザー履歴およびアクティブユーザーの詳細を確認できます。管理者は、地域をクリックすることで、システムのワールドビューを表示したり、特定の国や都市にドリルダウンしたりできます。管理者はさらにドリルダウンして、都市および州別に情報を表示できます。Citrix ADM バージョン 12.0 以降では、地理的な場所から接続しているユーザーにドリルダウンできます。

HDX Insight のワールドマップでは、以下の詳細を表示できます。また、各指標の密度はヒートマップの形式で表示されます。

- ICA 往復時間
- WAN 遅延
- DC の遅延
- 帯域幅
- バイト数合計



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

インスタンス別ビュー

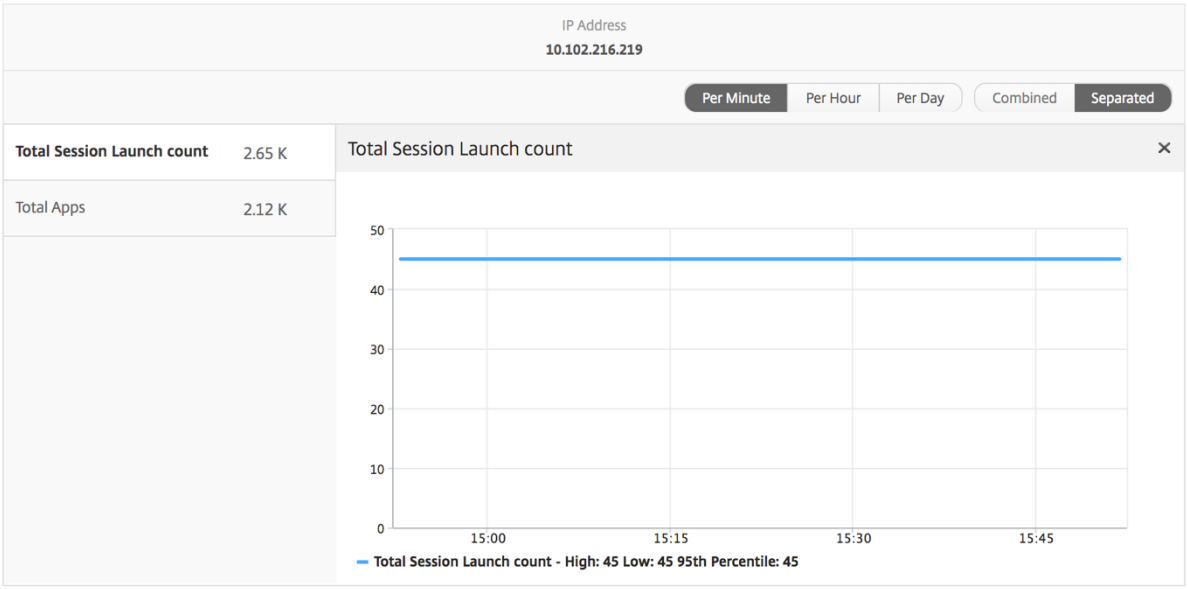
インスタンスごとのビューでは、選択した特定の ADC インスタンスについて、詳細なエンド・ユーザー・エクスペリエンス・レポートが提供されます。

[インスタンス**]** ビューにナビゲートするには、次の手順を実行します。

1. [分析] > [**HDX Insight**] > [インスタンス] に移動します。
2. インスタンスの概要レポートから特定のインスタンスを選択します。

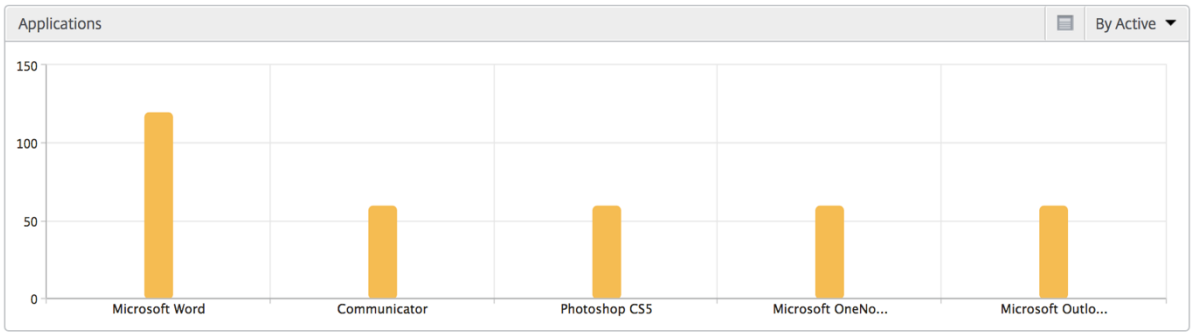
折れ線グラフ

メトリック	説明
IP アドレス	選択したインスタンスの NetScaler IP アドレスを表します。
Total session launch count	指定した期間中のアクティブな Citrix Virtual App セッションの総数。
アプリケーション合計数	特定の期間に起動された一意のアプリケーションの合計数です。



アプリケーション棒グラフ

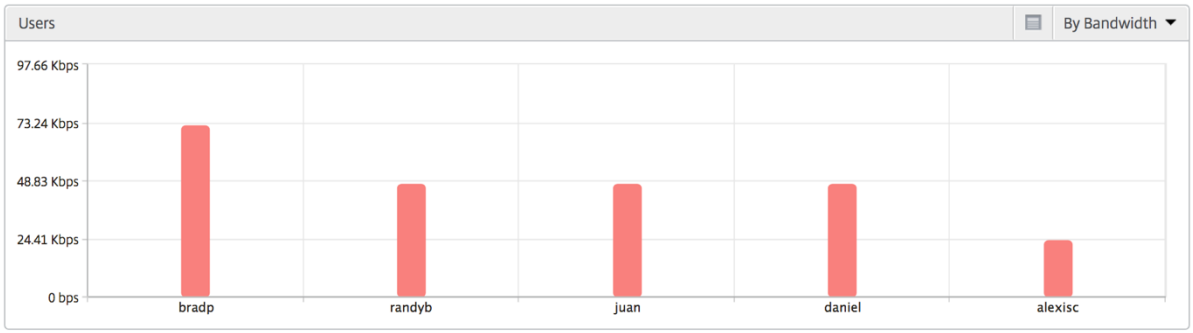
アクティブなアプリ、セッションの合計起動数、アプリの起動回数の合計、または起動期間に基づいて、上位 5 つのアプリケーションが表示されます。



ユーザー棒グラフ

ユーザー棒グラフには、以下の基準別に上位 5 人のユーザーが表示されます。

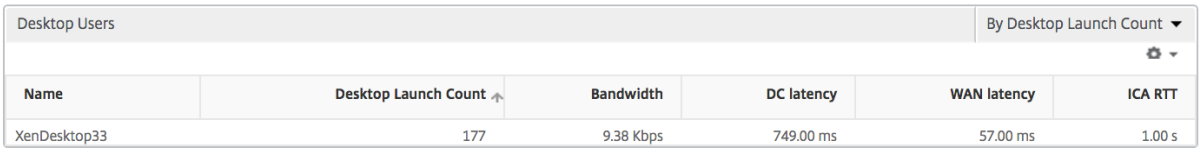
- 帯域幅
- WAN 遅延
- DC の遅延
- ICA 往復時間



デスクトップユーザーレポート

この表は、特定のユーザーの Citrix Virtual Desktop セッションに関する洞察を示しています。以下のメトリクスは［Desktop Launch Count］および［Bandwidth］を基準にしてソートできます。

メトリック	説明
名前	Citrix 仮想デスクトップの名前。
デスクトップの起動数	デスクトップが起動された回数です。
帯域幅	指定した期間中にエンドツーエンド通信で使用された時間あたりの総バイト数です。
DC 遅延	ネットワークのサーバー側に起因する遅延ですつまり、Citrix ADC からバックエンドサーバーまでです。
WAN 遅延	ネットワークのクライアント側に起因する遅延ですつまり、Citrix ADC からエンドユーザーへ。
ICA 往復時間	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーに表示される画面の遅れです。

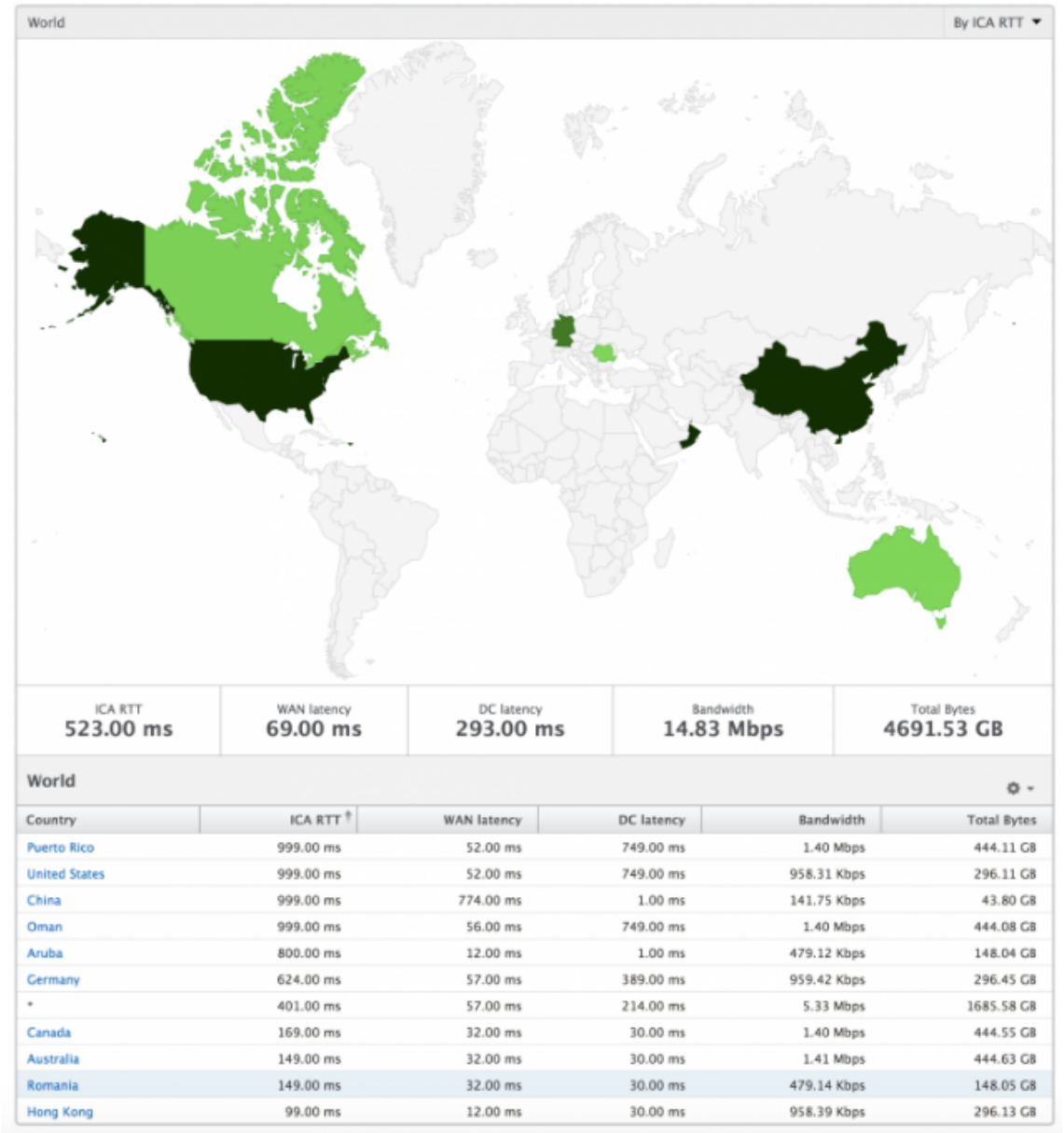


世界ビュー

HDX Insight の世界地図ビューでは、管理者が地理的な観点からユーザー履歴およびアクティブユーザーの詳細を確認できます。管理者は、地域をクリックすることで、システムのワールドビューを表示したり、特定の国や都市にドリルダウンしたりできます。管理者はさらにドリルダウンして、都市および州別に情報を表示できます。Citrix ADM バージョン 12.0 以降では、地理的な場所から接続しているユーザーにドリルダウンできます。

HDX Insight のワールドマップでは、以下の詳細を表示できます。また、各指標の密度はヒートマップの形式で表示されます。

- ICA 往復時間
- WAN 遅延
- DC の遅延
- 帯域幅
- バイト数合計



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

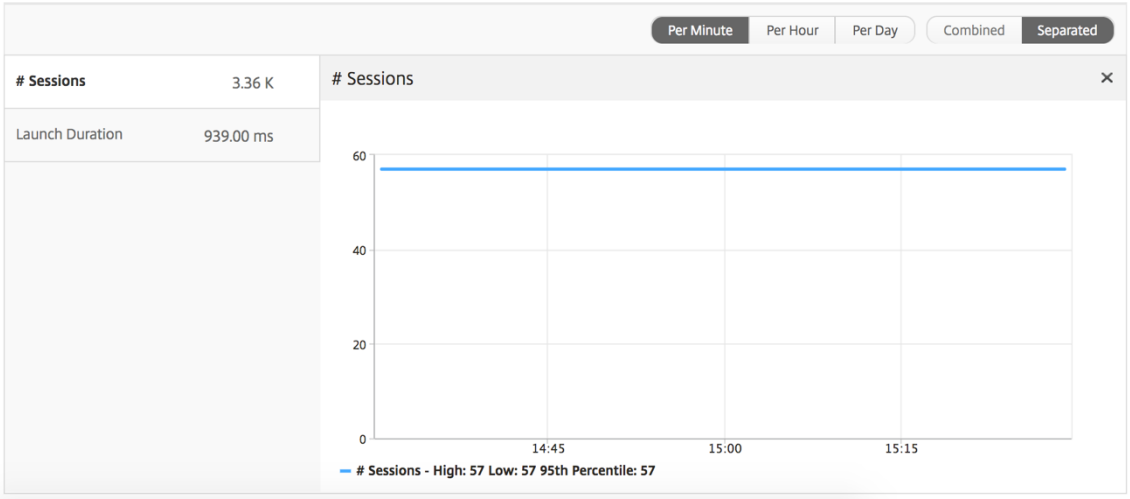
ライセンスビューのレポートおよびメトリクス

May 7, 2021

ライセンスビューには、Citrix ADC Gateway ライセンス情報の詳細が表示されます。[分析] > [**HDX Insight**] > [ライセンス] に移動します。

折れ線グラフ

メトリック	説明
使用中のライセンス	選択したタイムラインで使用されている Citrix ADC ゲートウェイ CCU ライセンス。各カウントは、ユーザーセッションの数を表します。このカウントには、各ユーザーが起動したアプリケーションセッションおよびデスクトップセッションは含まれません。
総ライセンス数	お客様が利用できる Citrix ADC ゲートウェイ CCU ライセンスの総数。



しきい値レポート

しきい値レポートは、選択した期間内に エンティティがライセンスとして選択されている場合に、違反したしきい値の数を表します。<!— 詳細については、「しきい値とアラートの作成方法」(/en-us/citrix-application-delivery-management-service/analytics/analytics-how-to-articles/how-to-create-thresholds-and-alerts-using-mas.html) を参照してください。。—>

HDX Insight の問題のトラブルシューティング

May 7, 2021

HDX Insight ソリューションが期待どおりに機能しない場合は、次のいずれかの問題が発生している可能性があります。トラブルシューティングについては、各セクションのチェックリストを参照してください。

- HDX Insight 構成。
- Citrix ADC と Citrix ADM 間の接続。

- Citrix ADC での HDX/ICA トラフィックのレコード生成。
- Citrix ADM 内のレコードの移入数。

HDX Insight 構成チェックリスト

- Citrix ADC で AppFlow 機能が有効になっていることを確認します。詳しくは、「AppFlow の有効化」を参照してください。
- Citrix ADC の実行構成で HDX Insight 構成を確認します。

  `show running | grep -i <appflow_policy>` コマンドを実行して、HDX Insight の設定を確認します。バインドタイプが ICA REQUEST であることを確認します。たとえば、

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  トランスペアレントモードの場合、バインドタイプは ICA_REQ_DEFAULT である必要があります。たとえば、

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```

- シングルホップ/アクセスゲートウェイまたはダブルホップ展開の場合は、HDX/ICA トラフィックが流れる VPN 仮想サーバーに HDX Insight AppFlow ポリシーがバインドされていることを確認します。
- 透過モードまたは LAN ユーザーモードの場合は、ICA ポート 1494 と 2598 が設定されていることを確認します。
- Citrix `appflowlog` Gateway または VPN 仮想サーバーのチェックパラメータは、Access Gateway またはダブルホップ展開で有効になっています。詳しくは、「仮想サーバーの AppFlow の有効化」を参照してください。
- ダブルホップ Citrix ADC で「接続チェーン」が有効になっていることを確認します。詳しくは、「データをエクスポートするための Citrix Gateway アプライアンスの構成」を参照してください。
- 高可用性フェイルオーバー後、HDX Insight の詳細が解析されスキップされている場合は、ICA パラメータ「EnablesronHaFailover」が有効になっていることを確認します。詳しくは、「Citrix ADC の高可用性ペアのセッション画面の信頼性」を参照してください。

Citrix ADC と **Citrix ADM** の間の接続チェックリスト

- Citrix ADC で AppFlow コレクタのステータスを確認します。詳しくは、「Citrix ADC と AppFlow コレクタ間の接続状態を確認する方法」を参照してください。
- HDX Insight の AppFlow ポリシーヒットを確認します。

  コマンド`show appflow policy <policy_name>`を実行して、AppFlow ポリシーのヒットをチェックします。

  GUI で [システム] **> [AppFlow] > [**ポリシー**]** に移動して、AppFlow ポリシーのヒットを確認することもできます。

- AppFlow ポート 4739 または 5557 をブロックしているファイアウォールを検証します。

Citrix ADC チェックリストでの HDX/ICA トラフィックのレコード生成

`tail -f /var/log/ns.log | grep -i "default ICA Message"` ログ検証のためにコマンドを実行します。生成されたログに基づいて、この情報をトラブルシューティングに使用できます。

- ログ: **ICA** 接続の解析をスキップしました**-**このホストでは **HDX Insight** がサポートされていません

  原因: サポートされていない Citrix Virtual Apps and Desktops バージョン

  回避策: Citrix Virtual Apps and Desktops サーバーをサポートされているバージョンにアップグレードします。

- ログ: クライアントタイプが **0x53** を受信しました。サポートされていません。

  原因: サポートされていないバージョンの Citrix Workspace アプリ

  解決策: Citrix Workspace アプリをサポートされているバージョンにアップグレードします。詳しくは、「Citrix Workspace アプリ」を参照してください。

- ログ: 展開パケットからのエラー**-**このフローのすべての **hdx** 処理をスキップします

  原因: ICA トラフィックの圧縮解除に関する問題

  解決方法: 新しいセッションが確立されるまで、この ICA セッションのレポートは利用できません。

- ログ: 無効な遷移**:NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID-> NS_ICA_ST_UNINIT**」

  原因: ICA ハンドシェイクの解析に関する問題

  解決方法: 新しいセッションが確立されるまで、この特定の ICA セッションのレポートは利用できません。

- ログ: **EUEM ICA RTT** が見つかりません

  原因: エンドユーザーエクスペリエンスの監視チャネルデータを解析できません。

  解決方法: Citrix Virtual Apps and Desktops サーバーでエンドユーザーエクスペリエンス監視サービスが開始されていることを確認します。サポートされているバージョンの Citrix Workspace アプリを使用していることを確認します。

- ログ: 無効なチャネルヘッダー

  原因: チャネルヘッダーを識別できません。

  解決方法: 新しいセッションが確立されるまで、この特定の ICA セッションのレポートは利用できません。

- ログ: コードをスキップ

  スキップコードに次のいずれかの値が表示された場合、Insight の詳細はスキップ解析されます。

  > スキップコード 0 は、レコードが Citrix ADC から正常にエクスポートされたことを示します。

コードをスキップ	エラーメッセージ	エラーの原因
100	NS_ICA_ERR_NULL_FRAG	ICA フラグメント処理エラー（メモリ状態による可能性が高い）
101	NS_ICA_ERR_INVALID_HS_CMD	無効なハンドシェイクコマンドを受信しました
102	NS_ICA_ERR_REDUC_PARAM_C	V3 エクスパンダの初期化に指定されたパラメータが無効です
103	NS_ICA_ERR_REDUC_INIT	V3 エクスパンダを正しく初期化できません
104	NS_ICA_ERR_REDUC_PARAM_B	チャネルにコーダを割り当てるのに十分なバイト数
105	NS_ICA_ERR_INVALID_CHANNEL	無効な ICA チャネル番号
106	NS_ICA_ERR_INVALID_DECODE	チャネルに無効なデコーダが指定されました
107	NS_ICA_ERR_INVALID_TW_PARAM	Thinwire チャネルに指定されたパラメータ数が無効です
108	NS_ICA_ERR_INVALID_TW_DEC	Thinwire チャネルの無効なデコーダ
109	NS_ICA_ERR_REDUC_NO_DECODER	チャネルにデコーダが定義されていません
110	NS_ICA_ERR_REDUC_V3_EXPAN	チャネルデータの拡張に失敗しました
111	NS_ICA_ERR_REDUC_BYTES_V3_LOOK	エクスパンダエラー: 使用可能なバイト数を超過した消費バイト
112	NS_ICA_ERR_REDUC_BYTES_O	エラー: 非圧縮データのオーバーラン
113	NS_ICA_ERR_REDUCE_INVALID_CMD	[未定義の拡張] コマンド
114	NS_ICA_ERR_CGP_FILL_HOLE	分割された CGP フレームの処理中にエラーが発生しました
115	NS_ICA_ERR_MEM_NSB_ALLOC	NSB 割り当てエラー — メモリ不足のため
116	NS_ICA_ERR_MEM_REDUC_CTX である	エクスパンダコンテキストのメモリ割り当てエラー
117	NS_ICA_ERR_ICA_OLD_SERVER	古いサーバ、機能ブロックはサポートされていません

コードをスキップ	エラーメッセージ	エラーの原因
118	NS_ICA_ERR_PIR_MANY_FRAG	パケット初期化要求はフラグメント化されており、処理できません
119	NS_ICA_ERR_INIT_ICA_CAPS	ICA 機能の初期化エラー
120	NS_ICA_ERR_NO_MSI_SUPPOR	ホストは MSI 機能をサポートしていません。6.5 より低いバージョンの XenApp または 5.0 より低いバージョンの XenDesktop を示します。
121	NS_ICA_ERR_CGP_INVALID_CMD	無効な CGP コマンドが検出されました
122	NS_ICA_ERR_INSUFFICENT_CH	チャネルを超えるバイト数が不足
123	NS_ICA_ERR_CHANNEL_DATA	EUEM、コントロール、またはシームレスチャネル上のデータが正しくありません
124	NS_ICA_ERR_INVALID_PURE_C	純粋な ICA チャネルデータの処理中に無効なコマンドを受信しました
125	NS_ICA_ERR_INVALID_PURE_LEN	純粋な ICA チャネルデータの処理中に無効な長さが検出されました
126	NS_ICA_ERR_INVALID_PURE_LI	PURE ICA チャネルデータの処理中に無効な長さが検出されました
127	NS_ICA_ERR_INVALID_CLNT_DATA	クライアントから無効なデータ長を受け取りました
128	NS_ICA_ERR_MSI_GUID_SZ	MSI GUID サイズのエラー
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	無効なチャネルヘッダーが検出されました
130	NS_ICA_ERR_CGP_PARSE_REC	再接続されたセッションの取得に失敗しました
131	NS_ICA_ERR_DISABLE_SR_NON_NS_RECONNECT	レジストリの無効化中にエラーが発生しました
132	NS_ICA_ERR_REDUC_NOT_V3	サポートされていない ICA レデューサのバージョン
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	圧縮が無効になり、ホストが優先されない

コードをスキップ	エラーメッセージ	エラーの原因
134	NS_ICA_ERR_IDENT_PROTO	ICA または CGP プロトコルを識別できません。受信機が正しくありません。
135	NS_ICA_ERR_INVALID_SIGNATURE	ICA 署名またはマジック文字列が正しくありません
136	NS_ICA_ERR_PARSE_RAW	ICA ハンドシェイクパケットの解析中にエラーが発生しました
137	NS_ICA_ERR_INCOMPLETE_PKT	ハンドシェイクで受信された不完全なパケット
138	NS_ICA_ERR_ICAFRAME_TOO_I	ICA フレームが大きすぎます。1,460 バイトを超えています
139	NS_ICA_ERR_FORWARD	ICA データの転送中にエラーが発生しました
135	NS_ICA_ERR_MAX_HOLES	CGP コマンドがサポートされている制限を超えて分割されているため処理できません
141	NS_ICA_ERR_ASSEMBLE_FRAME	ICA フレームを正しく再構成できません
142	NS_ICA_ERR_UNSUPPORTED_F	許可リストにないため、このレシーバ（クライアント）に対する ICA 解析をスキップしました
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	クライアント再接続クッキーの解析状態を検出できません
144	NS_ICA_ERR_SYNCUP_RECONN	クライアントの再接続後に無効な再接続クッキーの長さが検出されました
145	NS_ICA_ERR_INVALID_RECONNECT_ID	クライアントの再接続クッキーが必要な制約を逃しました
146	NS_ICA_ERR_INVALID_CLIENT_	クライアントから受信された受信者のバージョン文字列が無効です
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	無効な製品 ID を受け取りました
148	NS_ICA_ERR_V3_HDR_CORRUP	拡張後のチャネル長が無効です
110	NS_ICA_ERR_SPECIAL_THINWIRE	解凍エラー

コードをスキップ	エラーメッセージ	エラーの原因
150	NS_ICA_ERR_SEAMLESS_INSUF	シームレスコマンドのバイトが不足しています
151	NS_ICA_ERR_EUEM_INSUFFBYTE	EUEM コマンドのバイトが不足しています
152	NS_ICA_ERR_SEAMLESS_INVAL	シームレスなチャネル解析のための無効なイベント
153	NS_ICA_ERR_CTRL_INVALID_EVENT	CTRL チャネル解析のイベントが無効です
154	NS_ICA_ERR_EUEM_INVALID_E	EUEM チャネル解析の無効なイベント
155	NS_ICA_ERR_USB_INVALID_EVENT	USB チャネル解析のイベントが無効です
156	NS_ICA_ERR_PURE_INVALID_E	純粋なチャネル解析のイベントが無効です
157	NS_ICA_ERR_VCP_INVALID_EVENT	仮想チャネル解析のイベントが無効です
158	NS_ICA_ERR_ICAP_INVALID_EV	ICA データ解析のイベントが無効です
159	NS_ICA_ERR_CGPP_INVALID_EVENT	CGP データ解析のイベントが無効です
160	NS_ICA_ERR_BASICCRYPT_INV	基本暗号化の crypt コマンドの状態が無効です
161	NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD	基本暗号化の crypt コマンドが無効です
162	NS_ICA_ERR_ADVCRYPT_INVAL	RC5 暗号化の crypt コマンドの状態が無効です
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	RC5 暗号化の crypt コマンドが無効です
164	NS_ICA_ERR_ADVCRYPT_ENC	RC5 暗号化/復号化のエラー
165	NS_ICA_ERR_ADVCRYPT_DEC	RC5 暗号化/復号化のエラー
166	NS_ICA_ERR_SERVER_NOT_RE	VDA はリデューサーバージョン 3 をサポートしていません
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	UCE-V3 はリデューサーバージョン 3 をサポートしていません

コードをスキップ	エラーメッセージ	エラーの原因
168	NS_ICA_ERR_ICAP_INSUFFBYTI	ICA ハンドシェイクで予期しないバイト数
169	NS_ICA_ERR_HIGHER_RECONSEQ	ピア再接続後の CGP 再開シーケンス番号が高い
170	NS_ICA_ERR_DESCSRINFO_ABS	再接続後の ICA 解析状態を復元できません
171	NS_ICA_ERR_NSAP_PARSING	Insight チャネルデータの解析中にエラーが発生しました
172	NS_ICA_ERR_NSAP_APP です	Insight チャネルデータからアプリの詳細を解析中にエラーが発生しました
173	NS_ICA_ERR_NSAP_ACR	Insight チャネルデータからの ACR 詳細の解析中にエラーが発生しました
174	NS_ICA_ERR_NSAP_SESSION_E	Insight チャネルデータからのセッション終了詳細の解析中にエラーが発生しました
175	NS_ICA_ERR_NON_NSAP_SN	Insight チャネルサポートがないため、サービスノードでの ICA 解析をスキップしました
176	NS_ICA_ERR_NON_NSAP_CLIEI	NSAP はクライアントでサポートされていません
252	NS_ICA_ERR_NON_NSAP_SERVEI	NSAP は VDA でサポートされていません
178	NS_ICA_ERR_NSAP_NEG_FAIL	NSAP データネゴシエーション中のエラー
179	NS_ICA_ERR_SN_RECONNECT_TKT_FETCH	サービスノードでサービスの再接続チケットを取得中にエラーが発生しました
180	NS_ICA_ERR_SN_HIGHER_REC(	サービスノードでより高い再接続シーケンス番号を受信するとエラー

コードをスキップ	エラーメッセージ	エラーの原因
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_ON_NS	NS 上の接続で HDX Insight を無効にしているときにエラーが発生しました

サンプルログ:

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT ns-223
 0-PPE-2 : default ICA Message 1234 0 : "Session setup data send: Session
GUID [57af35043e624abab409f5e6af7fd22c], Client IP/Port [10.105.232.40/52314],
 Server IP/Port [10.106.40.215/2598], MSI Client Cookie [Non-MSI], Session
 setup time [01/09/2020:22:56:49 GMT], Client Type [0x0052], Receiver
Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [WIN2K12
-215], Ctx Flags [0x8820220228], Track Flags [0x1775010c3fc], Skip Code [0]
"

Jan 9 22:55:41 <local0.notice> 10.106.40.223 01/09/2020:22:55:41 GMT ns-223
 0-PPE-0 : default ICA Message 156 0 : "Skipping ICA flow: Session GUID
[4e3a91175ebcbe686baf175eec7e0200], Client IP/Port [10.105.232.40/60059],
Server IP/Port [10.106.40.219/2598], MSI Client Cookie [Non-MSI], Session
 setup time [01/09/2020:22:55:39 GMT], Client Type [0x0052], Receiver
Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [10.106.40.219],
 Ctx Flags [0x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```

エラーカウンタ

ICA 解析では、さまざまなカウンタがキャプチャされます。次の表に、ICA 解析用の各種カウンタを示します。コマンドを実行して `nsconmsg -g hdx -d statswt0`、カウンタの詳細を表示します。

HDX カウンタ名	目的	カテゴリ（ステータス/エラー/診断）
hdx_tot_ica_conn	NS によって検出された純粋な ICA 接続の合計数を示します。クライアント PCB 上の ICA 署名に基づく ICA 接続が検出されるたびにインクリメントされます。	Stats

HDX カウンタ名	目的	カテゴリ（ステータス/エラー/診断）
hdx_tot_cgp_conn	NS によって検出された CGP 接続の合計数を示します (セッション画面の保持オン)。クライアント PCB 上の CGP シグニチャに基づく CGP 接続が検出されるたびにインクリメントされます。	Stats
hdx_dbg_tot_udt_conn	NS によって検出された UDP ICA 接続の合計数を示します	Stats
hdx_dbg_tot_nsap_conn	NS によって検出された NSAP でサポートされている接続の合計数を示します。	Stats
hdx_tot_skip_conn	無効な ICA または CGP 署名のためにパーサーによってスキップされた ICA 接続の数を示します。	Stats
hdx_dbg_active_conn	その瞬間のアクティブな EDT/CGP/ICA 接続の合計。	Stats
hdx_dbg_active_nsap_conn	その時点でのアクティブな EDT/CGP/ICA NSAP 接続の合計。	Stats
hdx_dbg_skip_appflow_disabled	AppFlow を無効にしたために AppFlow がセッションからデタッチされたインスタンスの総数	ステータス/診断
hdx_dbg_transparent_user	透過的なユーザー・アクセスの総数	ステータス/診断
hdx_dbg_ag_user	アクセスゲートウェイのユーザーアクセスの総数	ステータス/診断
hdx_dbg_lan_user	LAN ユーザー・モード・アクセスの総数	ステータス/診断
hdx_basic_enc	基本暗号化を使用する ICA 接続の数を示します。	ステータス/診断
hdx_advanced_enc	高度な RC5 ベースの暗号化を使用する ICA 接続の数を示します。	ステータス/診断
dx_dbg_wanscaler_on_clientside	クライアント側で Citrix SD-WAN を持つ CGP/ICA 接続の合計数	ステータス/診断

HDX カウンタ名	目的	カテゴリ（ステータス/エラー/診断）
hdx_dbg_wanscaler_on_server	Citrix SD-WAN サーバー側を持つ CGP/ICA 接続の合計数	ステータス/診断
hdx_dbg_reconnected_session	Citrix ADC エラーのないクライアントからの再接続要求の総数	ステータス/診断
hdx_dbg_host_rejected_ns_rec	クライアント別の再接続要求を拒否したホストの総数	ステータス/診断
hdx_euem_Available	エンドユーザーエクスペリエンス監視チャネルが使用可能な接続数を示します。ICA RTT などの統計情報を収集するには、エンドユーザーエクスペリエンス監視チャネルが必要です。	ステータス/診断
hdx_err_disabled_sr	`nsapimgr`ノブを使用してセッション画面の保持が無効になります。セッションはこのセッションでは機能しません。	エラー
hdx_err_skip_no_msi	XA/XD サーバに MSI 機能がありません。これは古いサーバーバージョンを示しており、HDX Insight はこの接続をスキップします。	エラー
hdx_err_skip_old_server	古いサポートされていないサーバーのバージョン	エラー
hdx_err_clnt_not_whitelist	クライアント受信機が許可リストにない、HDX Insight はこの接続をスキップします	エラー
hdx_sm_ica_cam_channel_dis	SmartAccess ポリシーによって無効化された NS_ICA_CAM_CHANNEL の総数	診断
hdx_sm_ica_usb_channel_disabled	SmartAccess ポリシーによって無効化された NS_ICA_USB_CHANNEL の総数	診断

HDX カウンタ名	目的	カテゴリ（ステータス/エラー/診断）
hdx_sm_ica_clip_channel_disa	SmartAccess ポリシーによって無効化された NS_ICA_CLIP_CHANNEL の総数	診断
hdx_sm_ica_ccm_channel_disabled	SmartAccess ポリシーによって無効化された NS_ICA_CCM_CHANNEL の総数	診断
hdx_sm_ica_cdm_channel_dis	SmartAccess・ポリシーによって無効化された NS_ICA_CDM_CHANNEL の総数	診断
hdx_sm_ica_com1_channel_disabled	SmartAccess ポリシーによって無効化された NS_ICA_COM1_CHANNEL の総数	診断
hdx_sm_ica_com2_channel_di	SmartAccess ポリシーによって無効化された NS_ICA_COM2_CHANNEL の総数	診断
hdx_sm_ica_cpm_channel_disabled	SmartAccess ポリシーによって無効化された NS_ICA_CPM_CHANNEL の総数	診断
hdx_sm_ica_lpt1_channel_disa	SmartAccess・ポリシーによって無効化された NS_ICA_LPT1_CHANNEL の総数	診断
hdx_sm_ica_lpt2_channel_disabled	SmartAccess・ポリシーによって無効化された NS_ICA_LPT2_CHANNEL の総数	診断
dx_dbg_sm_ica_msi_disabled	SmartAccess ポリシーで MSI が無効になっているケースの総数	診断

HDX カウンタ名	目的	カテゴリ（ステータス/エラー/診断）
hdx_sm_ica_file_channel_disabled	SmartAccess・ポリシーによって NS_ICA_FILE_CHANNEL の総数が無効になっている	診断
hdx_dbg_usb_accept_device	受け入れられた USB デバイスの総数	診断
hdx_dbg_usb_reject_device	拒否された USB デバイスの総数	診断
hdx_dbg_usb_reset_endpoint	リセットされた USB エンドポイントの総数	診断
hdx_dbg_usb_reset_device	リセットされた USB デバイスの総数	診断
hdx_dbg_usb_stop_device	停止した USB デバイスの総数	診断
hdx_dbg_usb_stop_device_response	停止した USB デバイスからの応答である	診断
hdx_dbg_usb_device_gone	USB デバイスの合計数	診断
hdx_dbg_usb_device_stopped	停止した USB デバイスの総数	診断

nstrace 検証

CFLOW プロトコルをチェックして、すべての AppFlow レコードが Citrix ADC から出力されることを確認します。

Citrix ADM チェックリスト内のレコードの移入数

- コマンドを実行し、`tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"`ログをチェックして、Citrix ADM が AppFlow レコードを受信していることを確認します。
- Citrix ADC インスタンスが Citrix ADM に追加されていることを確認します。
- Citrix ゲートウェイ/VPN 仮想サーバーが Citrix ADM でライセンスされていることを検証します。
- ダブルホップのマルチホップパラメータ設定が有効になっていることを確認します。
- ダブルホップ展開で、Citrix Gateway がセカンドホップでクリアされていることを確認します。

Citrix テクニカルサポートに連絡する前に

迅速な解決のために、Citrix テクニカルサポートに連絡する前に、次の情報を確認してください。

- 展開とネットワークトポロジの詳細。
- Citrix ADC および Citrix ADM バージョン。
- Citrix Virtual Apps and Desktops サーバーのバージョン。
- クライアントレシーバのバージョン。
- 問題が発生したときのアクティブな ICA セッションの数。
- Citrix `show techsupport` ADC コマンドプロンプトでコマンドを実行して取得されたテクニカルサポートバンドル。
- Citrix ADM 用にキャプチャされた技術サポートバンドル。
- すべての Citrix ADC でキャプチャされたパケットトレース。
  パケットトレースを開始するには、`start nstrace -size 0'`
  「パケットトレースを停止するには」と入力します。`stop nstrace`
- `show arp` コマンドを実行して、システムの ARP テーブル内のエントリを収集します。

既知の問題

HDX Insight の既知の問題については、Citrix ADC リリースノートを参照してください。

しきい値のメトリック情報

May 7, 2021

Web

メトリック	エンティティ	説明
アプリケーション	ヒット数	仮想サーバ（アプリケーション）が受信したヒット数の合計
	帯域幅 (MB)	仮想サーバ（アプリケーション）によって消費された合計帯域幅
	応答時間（ミリ秒）	仮想サーバが応答するのに要した時間
クライアント	要求	クライアントが受信したリクエストの合計数
	レンダリング時間 (ミリ秒)	クライアントによるサーバ応答のレンダリングにかかった時間

メトリック	エンティティ	説明
	クライアントネットワーク遅延	クライアントネットワークからの要求にかかった時間
デバイス	ヒット数	デバイスが受信したヒットの合計数。例：ラップトップ、携帯電話
	帯域幅 (MB)	デバイスによって消費された合計帯域幅
ドメイン	ヒット数	ネットワークドメインが受信したヒット数の合計
	帯域幅 (MB)	ネットワークドメインによって消費された合計帯域幅
	応答時間（ミリ秒）	ネットワークドメインからの要求の応答に要した時間
オペレーティングシステム	ヒット数	オペレーティングシステムが受信したヒット数の合計
	帯域幅 (MB)	オペレーティングシステムによって消費された合計帯域幅
	レンダリング時間 (ミリ秒)	オペレーティングシステムによるサーバ応答のレンダリングにかかった時間
要求メソッド	ヒット数	要求メソッドによって受信された要求の総数。例:GET、POST
	帯域幅 (MB)	要求方式によって消費された合計帯域幅
応答の状態	ヒット数	レスポンスコードで受信されたヒット数の合計
	帯域幅 (MB)	応答コードによって消費された合計帯域幅
サーバー	ヒット数	サーバが受信したリクエスト/ヒットの総数
	帯域幅 (MB)	サーバによって消費された合計帯域幅
	サーバーネットワーク遅延 (ミリ秒)	サーバーネットワークからの要求にかかった時間

メトリック	エンティティ	説明
	サーバ処理時間 (ミリ秒)	サーバーが要求に応答するのに要した時間
URL	ヒット数	URL によって受信されたヒットの総数。例:www.Citrix.com
	ロード時間 (ミリ秒)	URL がサーバーからロードされるまでに要した時間
	レンダリング時間 (ミリ秒)	URL のレンダリングと表示にかかった時間
ユーザーエージェント	ヒット数	ユーザーエージェントが受信した要求の総数。例:Chrome ウェブブラウザ
	帯域幅 (MB)	ユーザーエージェントによって消費された合計帯域幅
	レンダリング時間 (ミリ秒)	ユーザーエージェントによるサーバー応答のレンダリングにかかった時間

セキュリティ

測定基準	エンティティ	説明
アプリケーション	脅威指数	アプリケーションに対する攻撃の重要度を示す 1 桁の評価システム。アプリケーションに対する攻撃の重大度が高いほど、そのアプリケーションの脅威指数は大きくなります。値の範囲は 1 ～7 です。
	安全性指数	外部からの脅威や脆弱性からアプリケーションを保護するために、Citrix ADC インスタンスをどのように安全に構成したかを示す 1 桁の評価システム。アプリケーションのセキュリティリスクが小さいほど、安全性指数は高くなります。値の範囲は 1 ～7 です。

APPANALYTICS

測定基準	エンティティ	説明
アプリケーション	AppScore	App Score は、アプリケーションのパフォーマンスを定義し、応答性の点でアプリケーションがうまく動作しているかどうかを示します。値の範囲は 0 ～80 です。

HDX

HDX しきい値について詳しくは、HDX Insight のしきい値を作成してアラートを構成するを参照してください。

Gateway Insight

May 7, 2021

Citrix Gateway の展開では、ユーザーアクセスの詳細を可視化することは、アクセス障害の問題のトラブルシューティングに不可欠です。ネットワーク管理者は、ユーザーが Citrix Gateway にログオンできないタイミングと、ユーザーアクティビティとログオン失敗の理由を知りたいが、通常、その情報はユーザーが解決の要求を送信しない限り利用できません。

Gateway Insight は、Citrix Gateway Gateway へのログオン時に、アクセスモードに関係なく、すべてのユーザーが遭遇した障害を可視化します。あらゆる期間を対象にして、すべての有効なユーザーの一覧、アクティブユーザーの数、アクティブセッションの数、ユーザー全体によって使用されたバイト数とライセンス数を表示できます。ユーザーごとの EPA（End Point Analysis：エンドポイント分析）、認証、SSO（Single Sign On：シングルサインオン）、アプリケーション起動のエラーを表示できます。また、ユーザーごとのアクティブセッションと終了したセッションの詳細を表示できます。

さらに、Gateway Insight は、仮想アプライアンスのアプリケーション起動エラーの理由に関する情報を提供します。これは、あらゆる種類のログオンまたはアプリケーション起動におけるエラーの問題のトラブルシューティングに役立ちます。起動済みアプリケーション数、セッション全体数、アクティブセッション数、アプリケーションによって使用された合計バイト数と帯域幅を表示できます。アプリケーションごとのユーザー、セッション、帯域幅、起動のエラーの詳細を表示できます。

ADC Gateway アプライアンスに関連付けられたすべてのゲートウェイが使用したゲートウェイ数、アクティブ・セッション数、合計バイト数、帯域幅をいつでも表示できます。ゲートウェイごとの EPA、認証、SSO、アプリケーション起動のエラーについて表示できます。また、ゲートウェイに割り当てられたすべてのユーザーの詳細と、ユーザーのログオンアクティビティを表示できます。

すべてのログメッセージは Citrix Application Delivery Management（ADM）データベースに格納されるため、任意の期間のエラーの詳細を表示できます。また、ログオンエラーの概要を表示して、エラーが発生したログオンプロセスの段階を特定できます。

注意事項:

- Gateway Insight は、次のデプロイメントでサポートされます。
  - Access Gateway
  - Unified Gateway
- ADM リリースおよびビルドは、Citrix Gateway アプライアンスのリリースおよびビルドと同じか、それ以降である必要があります。
- Advanced ライセンスのある ADC インスタンスについては、Gateway Insight レポートを 1 時間表示することができます。Gateway Insight レポートを 1 時間以上表示するには、プレミアムライセンスが必要です。

制限事項:

- 認証方法が証明書ベースの認証として構成されている場合、Citrix Gateway Gateway は Gateway Insight をサポートしません。
- 仮想 ICA アプリケーションおよびデスクトップに関する成功したユーザーログオン、遅延、アプリケーションレベルの詳細は、HDX Insight Users ダッシュボードでのみ確認できます。
- ダブルホップモードでは、2 つ目の DMZ にある ADC ゲートウェイ・アプライアンスの障害を可視化できません。
- RDP（Remote Desktop Protocol：リモートデスクトッププロトコル）のデスクトップアクセスの問題は報告されません。
- SAML 認証の Gateway Insight レコードはレポートされません。
- Gateway Insight は、次の認証タイプでサポートされています。これら以外の認証タイプが使用されている場合、Gateway Insight にいくつかの不一致が表示されることがあります。
  - ローカル
  - LDAP
  - RADIUS
  - TACACS
  - SAML
  - ネイティブ OTP

Gateway Insight の有効化

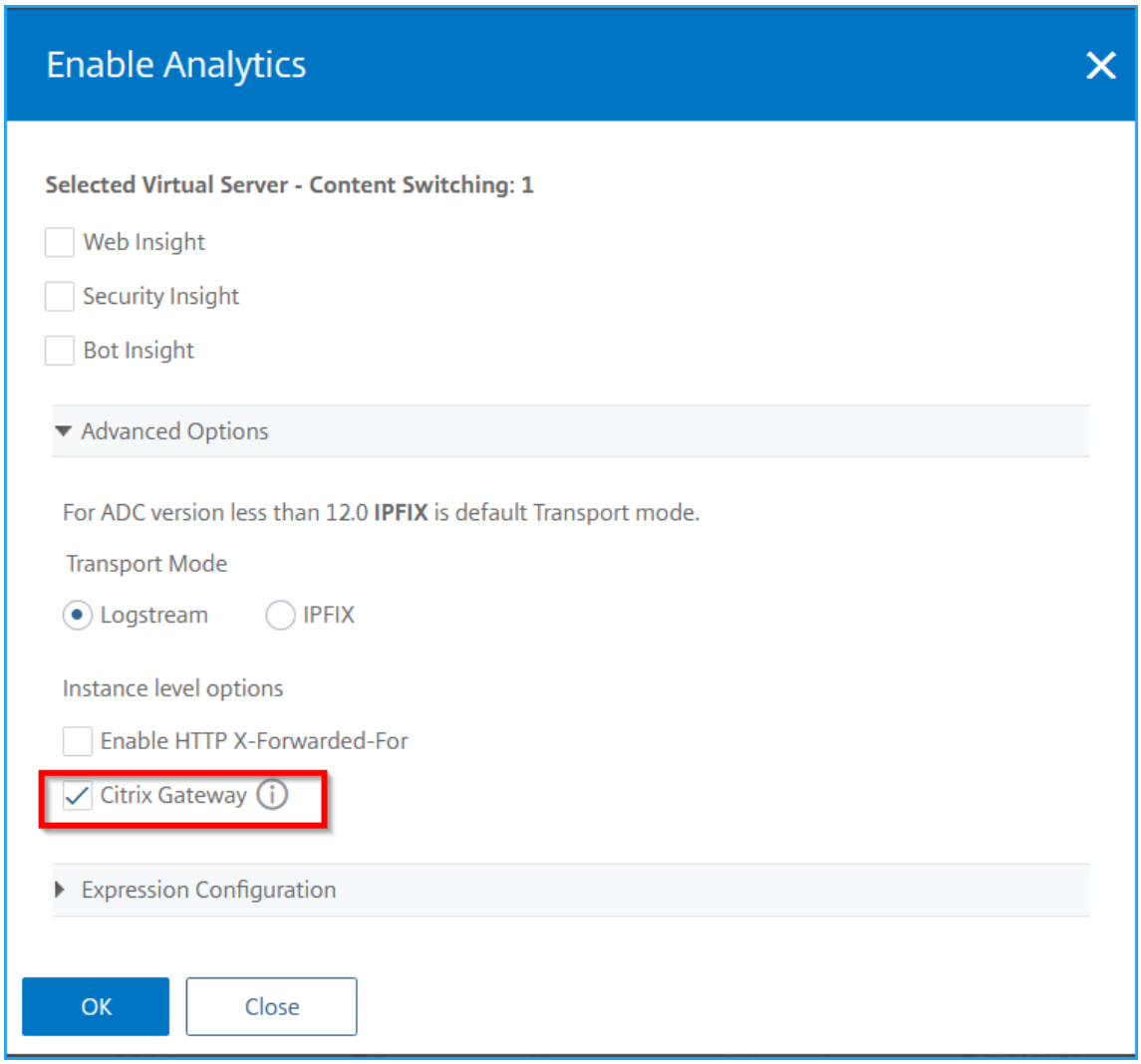
Citrix Gateway アプライアンスの Gateway Insight を有効にするには、まず ADC Gateway アプライアンスを ADM に追加する必要があります。次に、VPN アプリケーションを代表する仮想サーバー向けに AppFlow を有効にしてください。ADM へのデバイスの追加については、インスタンスの追加を参照してください。

> 注
>
> Citrix ADM でエンドポイント分析（EPA）の障害を表示するには、AppFlow 認証、承認、アクセス制御ユー

> ザー名を有効にする必要があります（ADC ゲートウェイアプライアンスにログオンしているユーザー名）。

ADM で仮想サーバーの AppFlow を有効にする

1. ［ネットワーク］ > ［インスタンス］ > ［**Citrix ADC**］の順に選択し、AppFlow を有効にするインスタンスを選択します。
2. **[** アクションの選択] リストから、[**Analytics** の設定] を選択します。
3. 仮想サーバーを選択し、[アナリティクスを有効にする] をクリックします。
4. [詳細オプション] で、[**Citrix Gateway**



5. ［OK］をクリックします。

GUI を使用して ADC ゲートウェイアプライアンスで AppFlow ユーザー名ログを有効にする

1. [構成] > [システム] > [AppFlow] > [設定] に移動し、[**AppFlow** 設定の変更] をクリックします。

2. [**AppFlow** 設定の構成] 画面で、[**AAA** ユーザ名] を選択し、[**OK**] をクリックします。

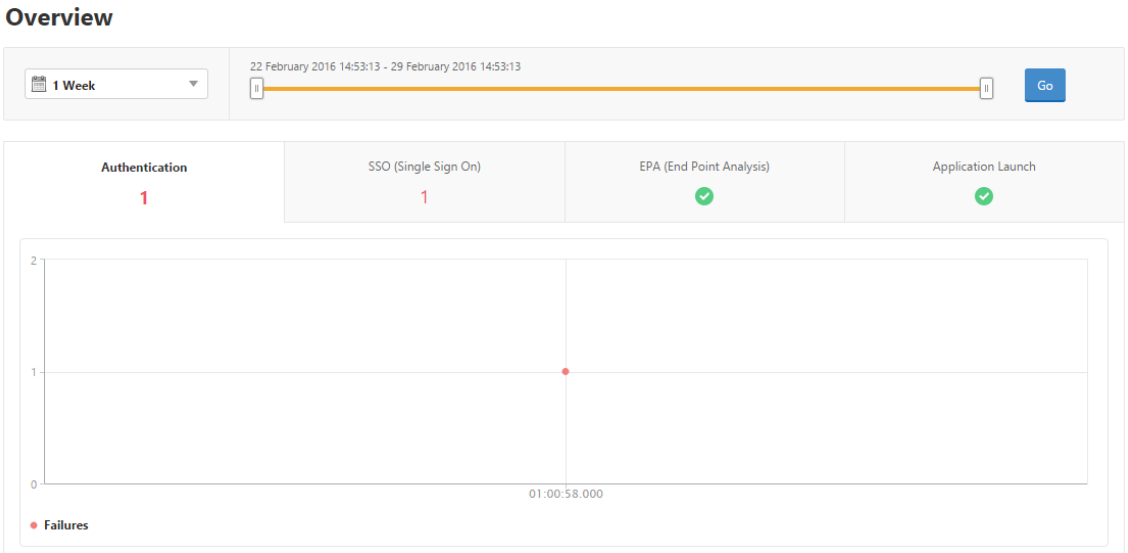
Gateway Insight レポートの表示

Citrix ADM では、ADC Gateway アプライアンスに関連付けられたすべてのユーザー、アプリケーション、ゲートウェイに関するレポートを表示し、特定のユーザー、アプリケーション、またはゲートウェイの詳細を表示できます。「概要」セクションでは、EPA、SSO、認証、およびアプリケーション起動の失敗を表示できます。ユーザーがログオンに使用したさまざまなセッションモードの概要、クライアントの種類、時間ごとのログオンしたユーザーの数を表示することもできます。

> 注
>
> グループを作成するときに、グループにロールを割り当てたり、グループへのアプリケーションレベルのアクセスを提供したり、ユーザーをグループに割り当てることができます。Citrix ADM 分析では、仮想 IP アドレスベースの認証がサポートされるようになりました。ユーザーは、権限のあるアプリケーション（仮想サーバー）のみのすべての Insight のレポートを表示できるようになりました。グループとグループへのユーザーの割り当てについて詳しくは、Citrix ADM でのグループの構成を参照してください。

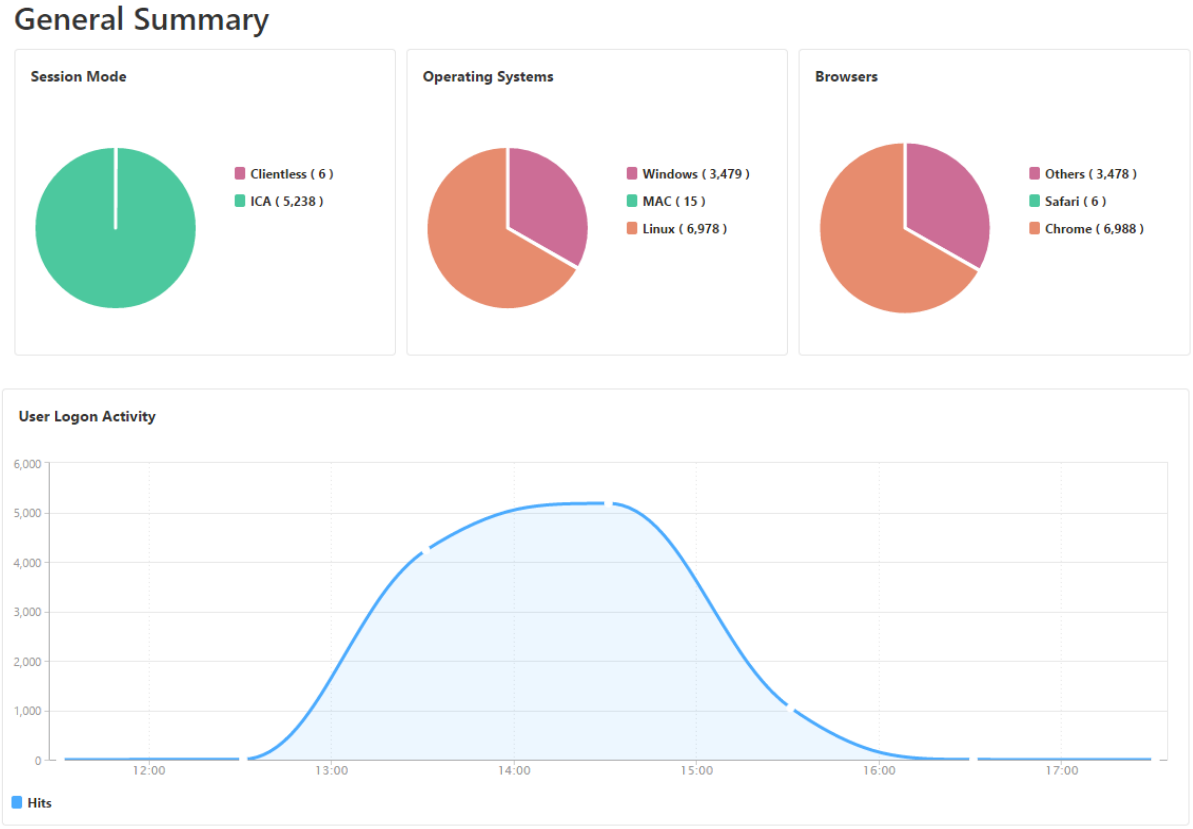
EPA、**SSO**、認証、承認、およびアプリケーション起動の失敗の表示

1. Citrix ADM で、[**Analytics] > [Gateway Insight**] に移動します。
2. ユーザーの詳細を表示する期間を選択します。時間スライダーを使用して選択する期間をカスタマイズできます。[**Go**] をクリックします。
3. [EPA (End Point Analysis)]、[Authentication]、[Authorization]、[SSO (Single Sign On)]、[Application Launch] タブのいずれかをクリックして、エラーの詳細を表示します。



セッションモード、クライアント、およびユーザー数の概要の表示

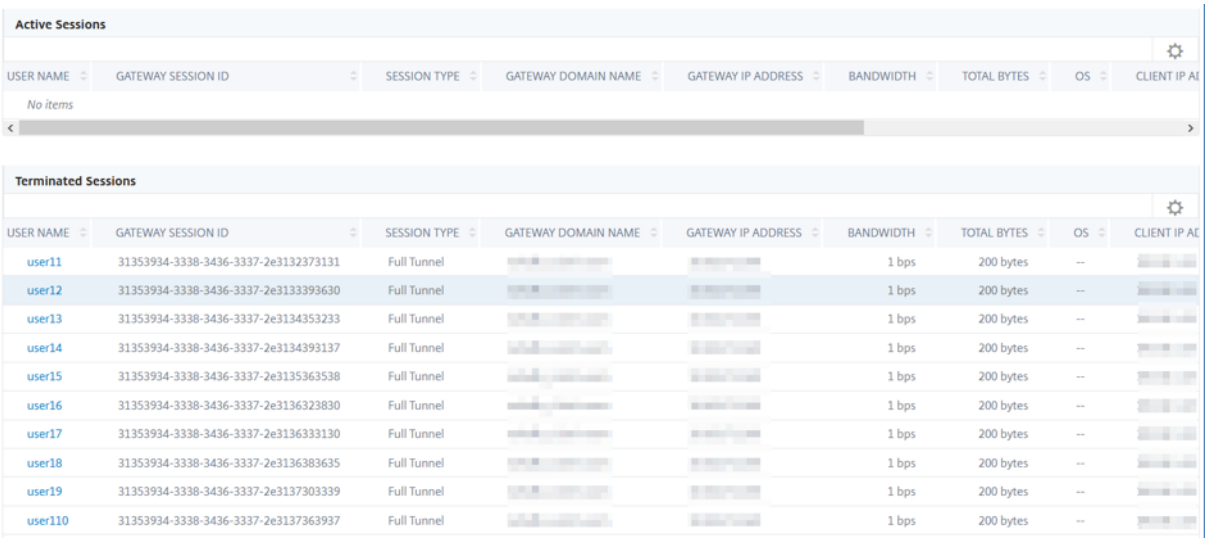
Citrix ADM で、[**Analytics] > [Gateway Insight**] に移動し、下にスクロールしてレポートを表示します。



ユーザー

ADC Gateway アプライアンスに関連付けられているユーザーの完全なレポートを表示できます。ユーザーの EPA、認証、SSO、アプリケーションの起動失敗などを表示できます。

また、アクティブなセッションと終了したすべてのユーザーの統合ビューを表示することもできます。

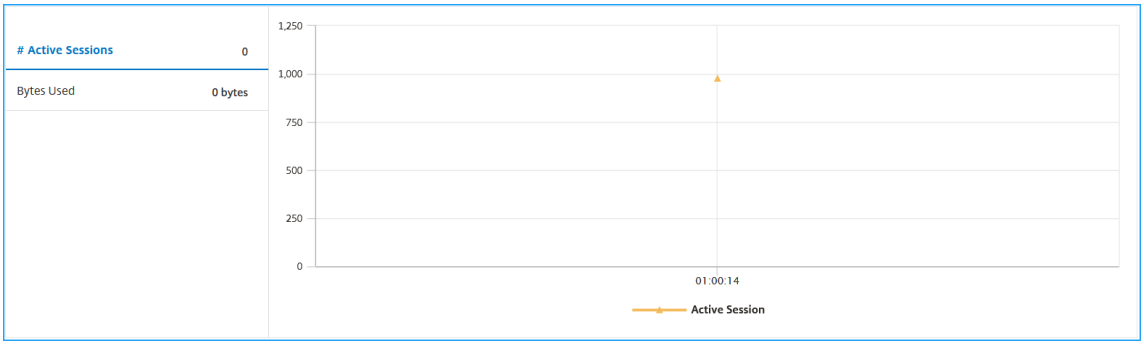


管理者として、このビューを使用すると、次のことが可能になります。

- 単一ペインビジュアライゼーションですべてのユーザーの詳細を表示する
- 各ユーザーを選択し、アクティブなセッションと終了したセッションの表示に関する複雑さを排除

ユーザーの詳細の表示

1. Citrix ADM で、[**Analytics] > [Gateway Insight] > [**ユーザー**]** に移動します。
2. ユーザーの詳細を表示する期間を選択します。時間スライダーを使用して選択する期間をカスタマイズできます。[**Go**] をクリックします。
3. 期間中のアクティブなユーザー数、アクティブなセッション数、および全ユーザーのバイト数を表示できます。

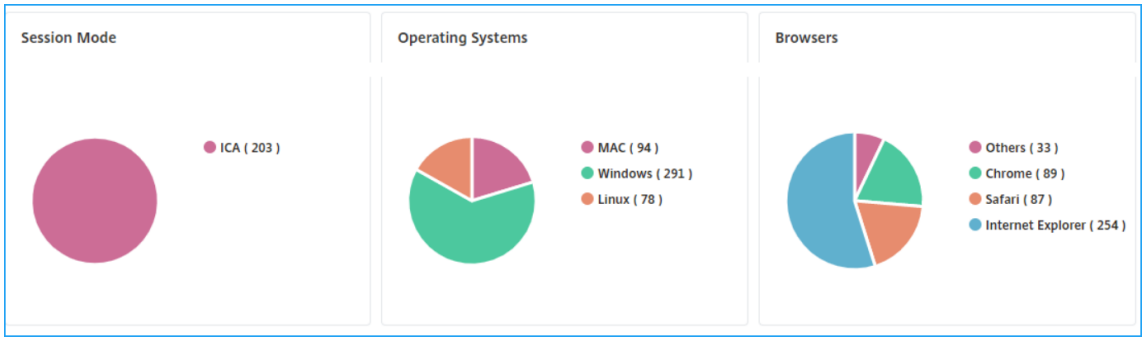


下にスクロールすると、有効なユーザーとアクティブユーザーの一覧が表示されます。

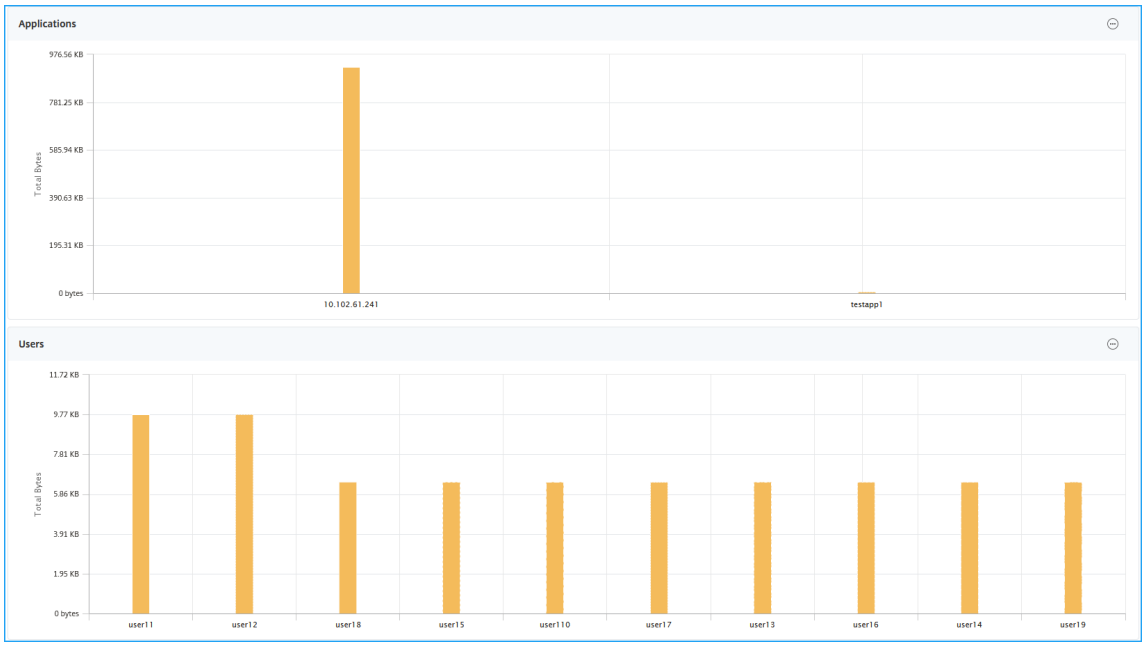
User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

[ユーザー] または [アクティブなユーザー] タブで、ユーザーをクリックして、次のユーザーの詳細を表示します。

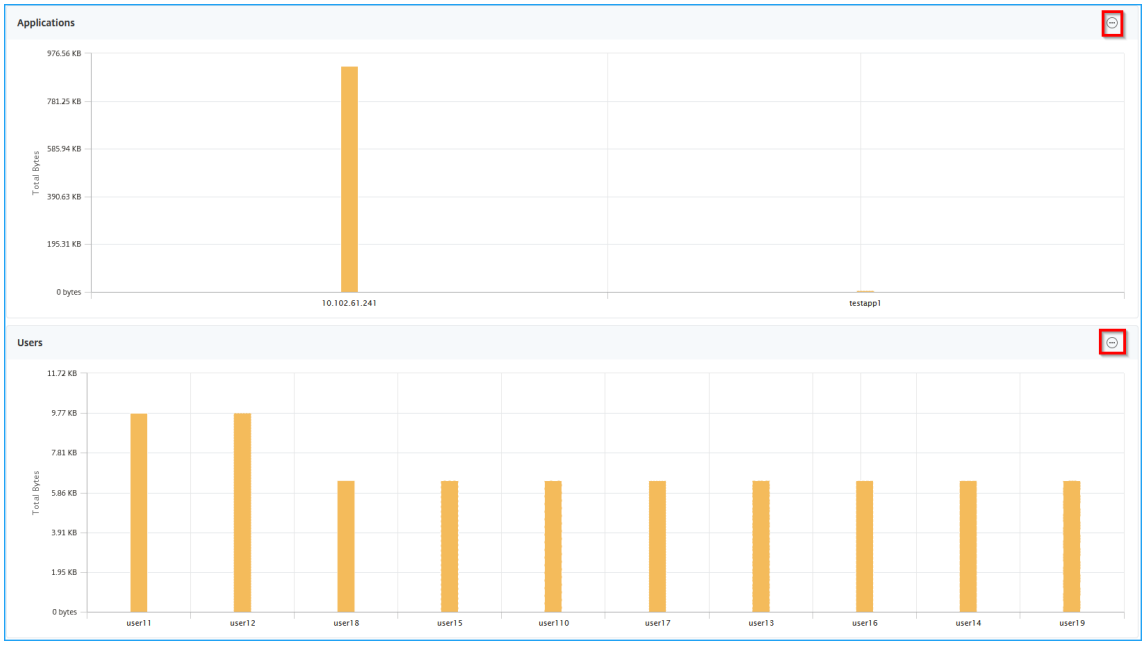
- ユーザーの詳細 -ADC Gateway アプライアンスに関連付けられた各ユーザーのインサイトを表示できます。[分析] > [**Gateway Insight**] >**[ユーザー]** に移動し、ユーザーをクリックして、セッションモード、オペレーティングシステム、ブラウザーなど、選択したユーザーのインサイトを表示します。



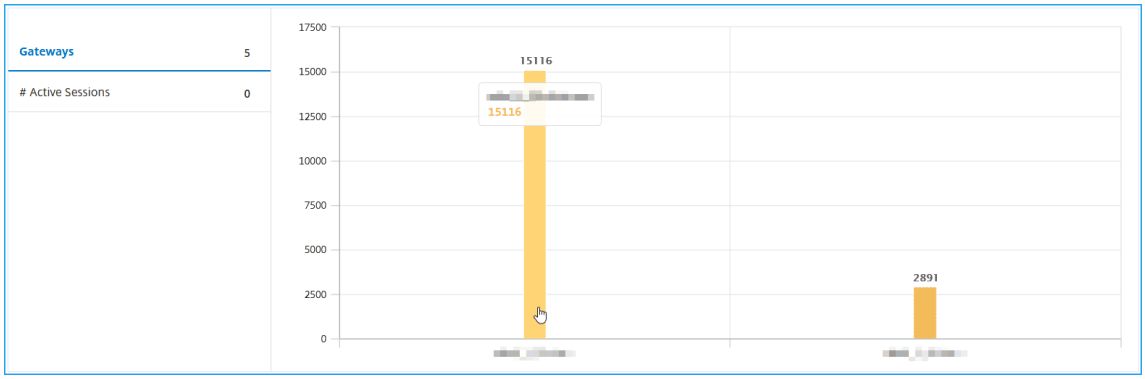
- 選択したゲートウェイのユーザーとアプリケーション-[**Analytics**] > [**Gateway Insight**] >**[Gateway]** に移動し、ゲートウェイドメイン名をクリックして、選択したゲートウェイに関連付けられている上位 10 のアプリケーションと上位 10 人のユーザーを表示します。



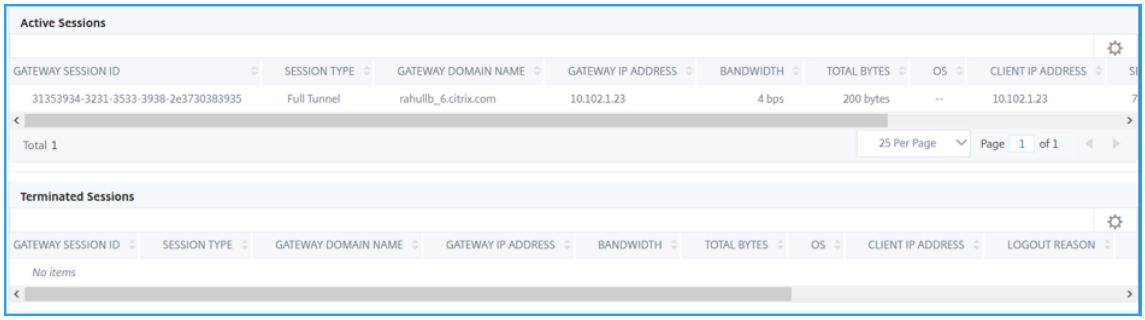
- アプリケーションとユーザーの表示オプション — 10 を超えるアプリケーションおよびユーザーの場合、[アプリケーションとユーザー] の [詳細] アイコンをクリックすると、選択したゲートウェイに関連付けられているすべてのユーザーとアプリケーションの詳細を表示できます。



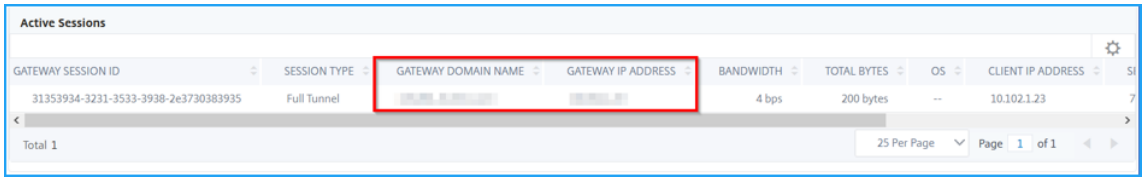
- 棒グラフをクリックして詳細を表示 — 棒グラフをクリックすると、関連する詳細を表示できます。たとえば、[アナリティクス] **> [Gateway Insight] >** [ゲートウェイ] の順に選択し、ゲートウェイの棒グラフをクリックしてゲートウェイの詳細を表示します。



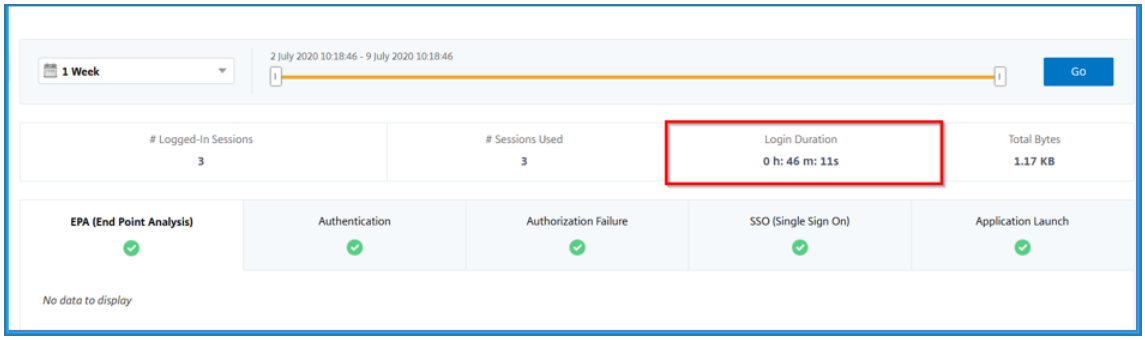
- ユーザーのアクティブセッションと終了したセッション。



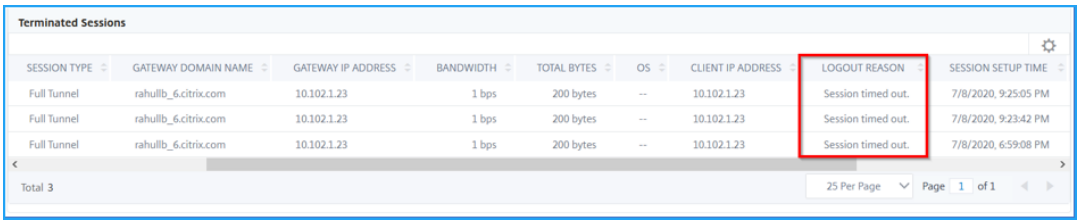
- アクティブセッションのゲートウェイドメイン名とゲートウェイの IP アドレス。



- ユーザーのログイン時間。



- ユーザーのログアウトセッションの理由。ログアウトの理由は次のとおりです。
  - セッションのタイムアウト
  - 内部エラーのためログアウトしました
  - 非アクティブセッションがタイムアウトしたためログアウトしました
  - ユーザーがログアウトしました
  - 管理者がセッションを停止しました



検索バーと地理マップビュー

次の項目を表示できます。

- ユーザー名に基づいて結果をフィルタリングできる検索バー。[分析] **> [Gateway Insight] > [**ユーザー**]** に移動して、**[**ユーザー**]** と [アクティブユーザー] の検索バーを表示します。検索バーにマウスポインタを置き、[ユーザー名] を選択し、ユーザー名を入力して結果をフィルタリングします。

- ユーザーの地理的位置に基づいてユーザー情報を表示する地理マップ。管理者として、この地理マップを使用すると、特定の場所のユーザー合計、アプリ合計、セッション総数のサマリー、合計セッションを表示できます。

  1. [アナリティクス] **> [Gateway Insight**] に移動して、地域マップを表示します。
  2. 国をクリックします。たとえば、米国

     地域マップには、選択した国のユーザーリスト、アクティブなセッション、終了したセッション、アプリケーションなどの詳細が表示されます。

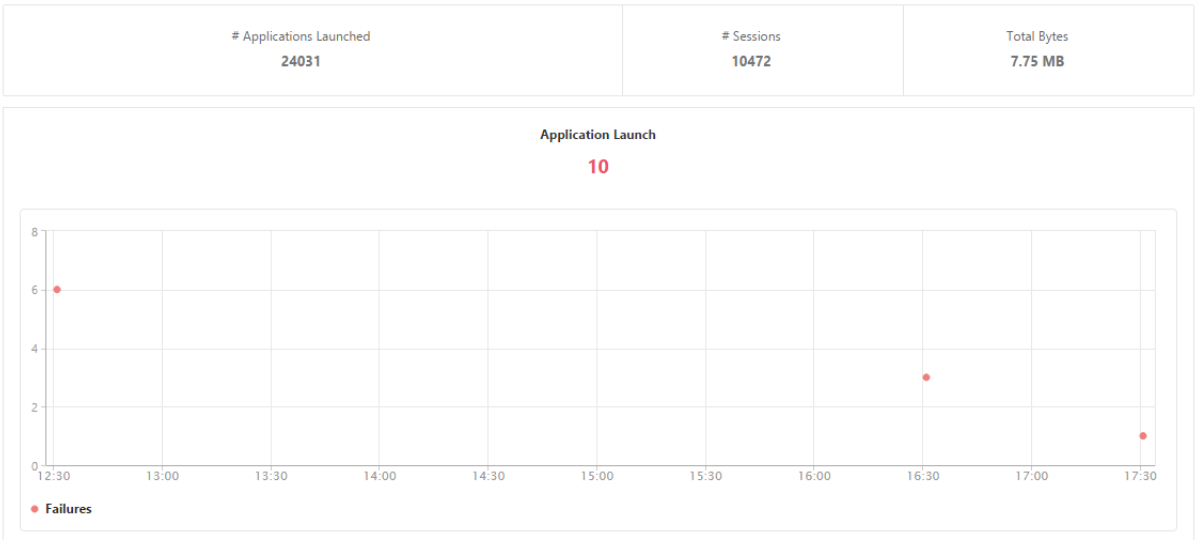
アプリケーション

起動済みアプリケーション数、セッション全体数、アクティブセッション数、アプリケーションによって使用された合計バイト数と帯域幅を表示できます。アプリケーションごとのユーザー、セッション、帯域幅、起動のエラーの詳細を表示できます。

アプリケーション詳細の表示

1. Citrix ADM で、［分析］**>**［**Gateway Insight**］**>**［アプリケーション］に移動します。
2. アプリケーションの詳細を表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。［**Go**］をクリックします。

起動済みアプリケーション数、セッション全体数、アクティブセッション数、アプリケーションによって使用された合計バイト数と帯域幅が表示されます。



下にスクロールすると、ICA とその他のアプリケーションによって使用されたセッション数、帯域幅、合計バイト数が表示されます。

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	3972	52 bps	3.79 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB

[その他のアプリケーション] タブで、[名前] 列でアプリケーションをクリックすると、そのアプリケーションの詳細を表示できます。

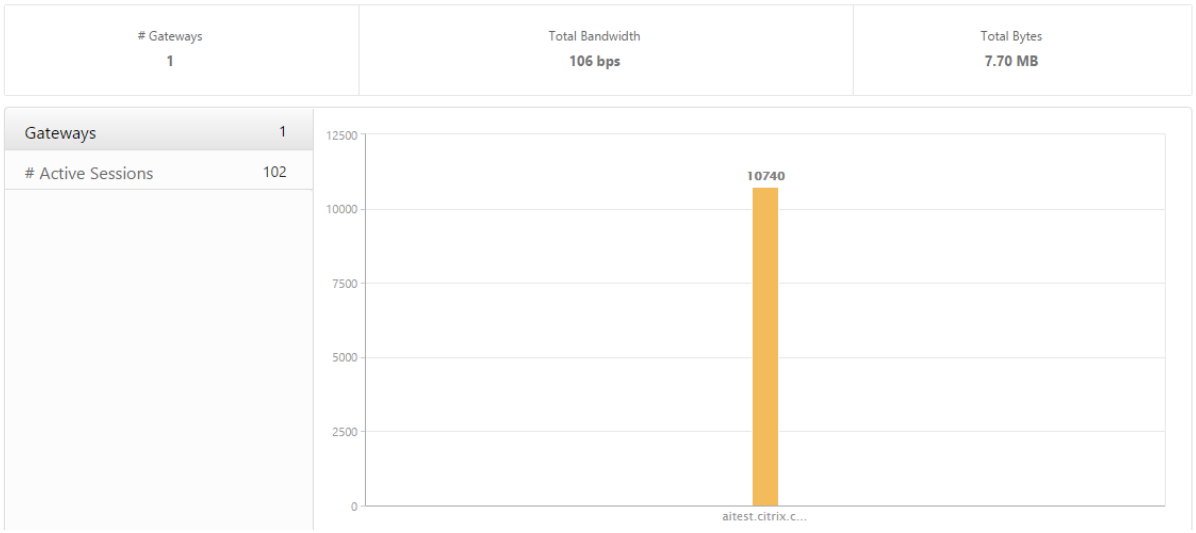
ゲートウェイ

ADC Gateway アプライアンスに関連付けられたすべてのゲートウェイが使用したゲートウェイ数、アクティブなセッション数、合計バイト数、帯域幅をいつでも表示できます。ゲートウェイごとの EPA、認証、SSO、アプリケーション起動のエラーについて表示できます。また、ゲートウェイに割り当てられたすべてのユーザーの詳細と、ユーザーのログオンアクティビティを表示できます。

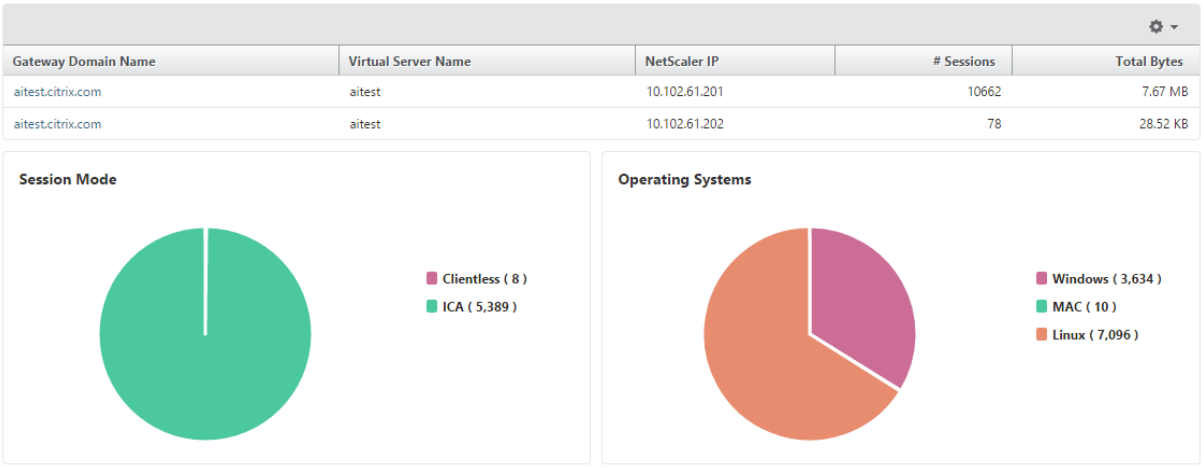
ゲートウェイの詳細を表示する

1. Citrix ADM で、［分析］**>**［**Gateway Insight**］**>**［ゲートウェイ］に移動します。
2. ゲートウェイの詳細を表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。［**Go**］をクリックします。

これで、ADC Gateway アプライアンスに関連付けられたすべてのゲートウェイが使用したゲートウェイ数、アクティブなセッション数、合計バイト数、帯域幅をいつでも表示できます。



下にスクロールして、ゲートウェイドメイン名、仮想サーバー名、ADC IP アドレス、セッションモード、合計バイト数などのゲートウェイの詳細を表示します。



「Gateway **Domain Name**」列で **G** ateway をクリックすると、EPA、認証、シングル・サインオン、アプリケーション起動の失敗、およびゲートウェイに関するその他の詳細を表示できます。

ゲートウェイの地情報マップを表示して、特定の場所に基づいてユーザーをフィルタリングすることもできます。

1. [分析] **> [Gateway Insight] > [**ゲートウェイ**]** に移動します。
2. ゲートウェイドメイン名を選択して geo マップを表示します
3. 国をクリックします。たとえば、米国

   地域マップには、選択した国のユーザーリスト、アクティブなセッション、終了したセッション、アプリケーションなどの詳細が表示されます。

レポートのエクスポート

GUI に表示されるすべての詳細情報を含む Gateway Insight レポートを、ローカルコンピュータに PDF、JPEG、PNG、または CSV 形式で保存できます。また、指定された電子メールアドレスへのレポートのエクスポートを、さまざまな間隔でスケジュール設定することができます。

> 注
>
> - 読み取り専用アクセス権のユーザーは、レポートをエクスポートすることができません。
> - 地理マップレポートは、ADM にインターネット接続がある場合にのみエクスポートされます。

レポートのエクスポート

1. [ダッシュボード] タブの右ペインで、[エクスポート] ボタンをクリックします。
2. [今すぐエクスポート] で、必要な形式を選択し、[エクスポート] をクリックします。

エクスポートをスケジュールするには、次の手順に従います。

1. [ダッシュボード] タブの右ペインで、[エクスポート] ボタンをクリックします。
2. [エクスポートのスケジュール] で詳細を指定し、[スケジュール] をクリックします。

エクスポートスケジュールを編集するには、次の手順に従います。

1. ［構成］タブで、［構成］>［**NetScaler Insight Center** ］>［スケジュールのエクスポート］に移動します。
2. 使用可能なリストからレポートを選択し、[編集] をクリックします。
3. 編集後、[保存] をクリックします。

> 注**:**
>
> レポートをスケジュールする前に、[システム] > [通知] > [電子メール] に移動し、[追加] をクリックして、電子メールサーバーの設定を構成します。

電子メールサーバーまたは電子メール配布リストを追加するには、次の手順を実行します。

1. [構成] タブで、[システム] > [通知] > [電子メール] に移動します。
2. 右側のウィンドウで、[電子メールサーバー**]** を選択して電子メールサーバーを追加するか、[電子メール配布リスト] を選択して電子メール配布リストを作成します。
3. 詳細を指定し、[作成] をクリックします。

Gateway Insight ダッシュボード全体をエクスポートするには:

1. [ダッシュボード] タブの右ペインで、[エクスポート] ボタンをクリックします。
2. [今すぐエクスポート] で [**PDF** 形式] を選択し、[エクスポート] をクリックします。

Gateway Insight のユースケース

次のユースケースは、Gateway Insight を使用して、ADC Gateway アプライアンス上のユーザーのアクセス詳細、アプリケーション、ゲートウェイを可視化する方法を示しています。

1. ユーザーが **ADC Gateway** アプライアンスまたは内部 **Web** サーバにログオンできない

ADC Gateway アプライアンスを監視している ADC Gateway 管理者で、ユーザーがログインできない理由や、ログインプロセスのどの段階でエラーが発生したかを確認する必要があります。

ADM では、ログインプロセスの次の段階で、ユーザログインエラーの詳細を表示できます。

- 認証
- エンドポイント分析（EPA）
- シングルサインオン

ADM では、特定のユーザーを検索し、そのユーザーの詳細をすべて表示できます。

ユーザーを検索するには、次の手順に従います。

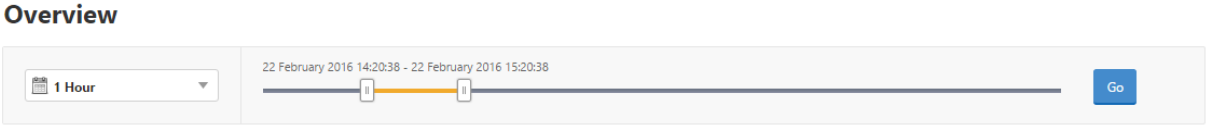
Citrix ADM で、[**Analytics**] **>** [**Gateway Insight**] に移動し、[ユーザーの検索] テキストボックスで検索するユーザーを指定します。

認証エラー

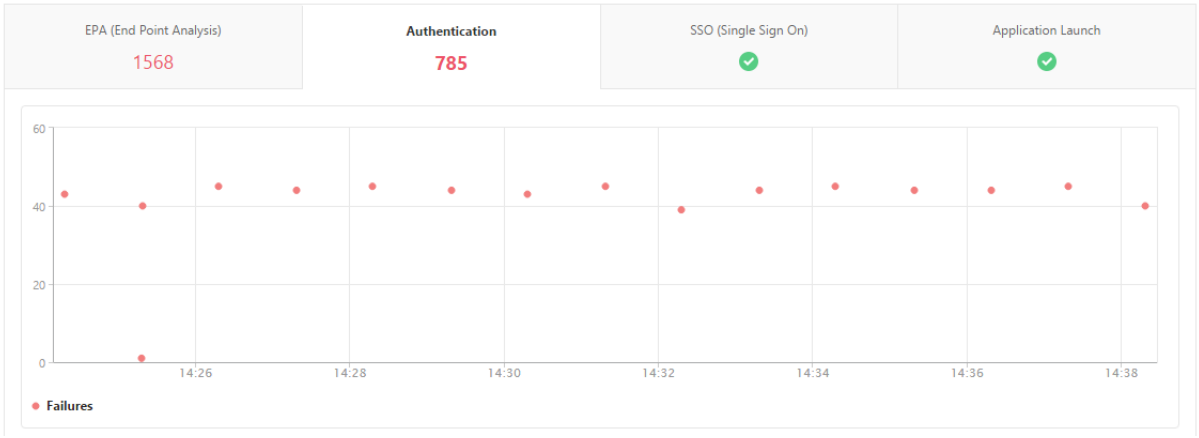
資格情報が正しくない、または認証サーバーから応答がないなどの認証エラーについて確認できます。2 段階認証を設定している場合、いずれの段階で認証できなかったのか、または両方の段階で認証できなかったのかを確認できます。

認証失敗の詳細を表示する

1. Citrix ADM で、[**Analytics] > [Gateway Insight**] に移動します。
2. [概要] セクションで、認証エラーを表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。[**Go**] をクリックします。



1. [認証] タブをクリックします。[失敗] グラフでは、任意の時点における認証エラーの数を表示できます。



そのタブのまま下にスクロールすると、**Username**、**Client IP Address**、**Error Time**、**Authentication Type**、**Authentication Server IP Address** などの各認証エラーの詳細を表で確認できます。表の [エラーの説明] 列にはログオン失敗の理由が表示され、[状態] 列には、2 段階認証のどの段階でエラーが発生したかが表示されます。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

[Us **ername**] 列でユーザーをクリックすると、そのユーザーの認証エラーやその他の詳細を表示できます。

次の図に示すように、リストの矢印を使用して、テーブルをカスタマイズして列を追加または削除できます。

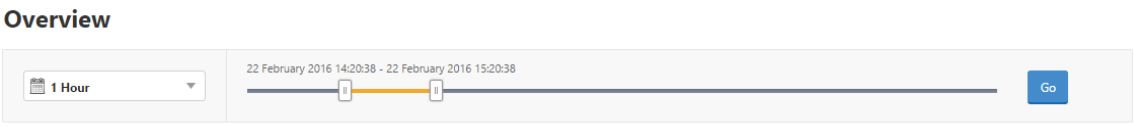
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

EPA エラー

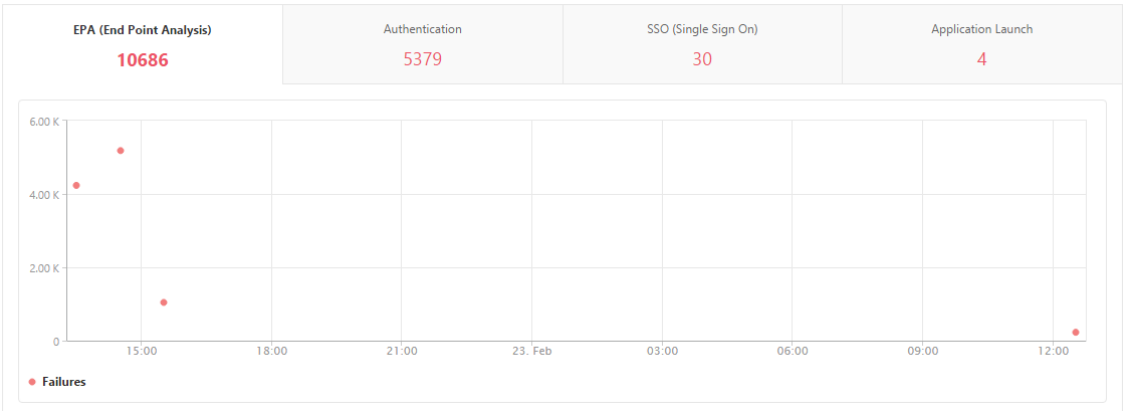
認証前段階または認証後の段階で EPA の障害を表示できます。

EPA 障害の詳細の表示

1. Citrix ADM で、[**Analytics] > [Gateway Insight**] に移動します。
2. [Overview] セクションで EPA エラーを表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。[**Go**] をクリックします。



3. [**EPA (**終点解析**)**] タブをクリックします。特定の時点における EPA エラーの数は、障害グラフで表示できます。

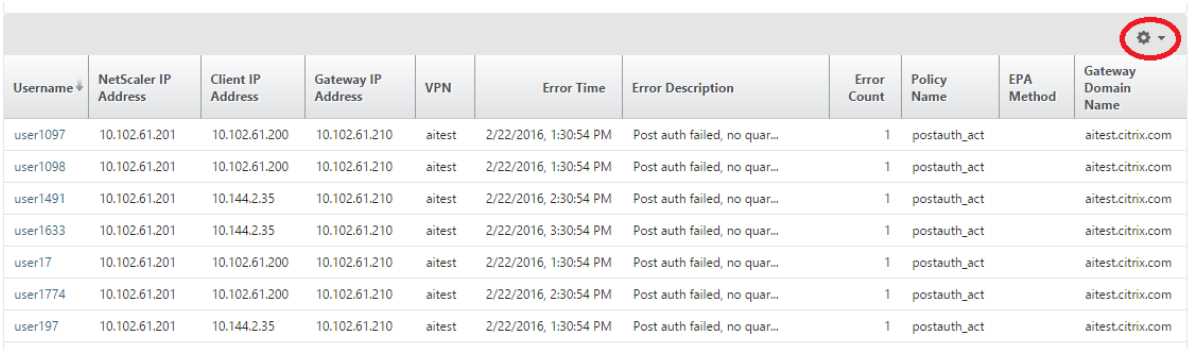


同じタブのテーブルから、ユーザー名、**ADC IP** アドレス、ゲートウェイ **IP** アドレス、**VPN**、エラー時間、ポリシー名、ゲートウェイドメイン名など、各 EPA エラーの詳細を表示するには、下にスクロールします。表の [**Error Description**] 列には EPA エラーの理由が記載されており、[**Policy Name**] 列にはエラーの原因となったポリシーが示されています。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

[Us **ername**] 列でユーザーをクリックすると、そのユーザーの EPA エラーやその他の詳細を表示できます。

次の図に示すように、リストの矢印を使用して、テーブルをカスタマイズして列を追加または削除できます。



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

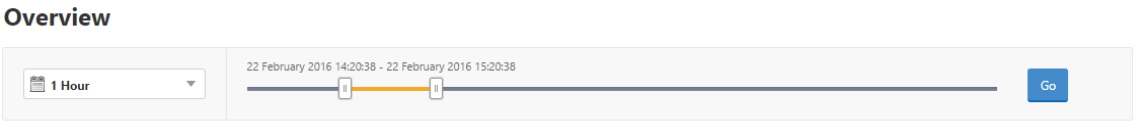
> 注
>
> 「ClientSecurity」式が VPN セッションポリシールールとして構成されている場合、ADC Gateway は EPA 障害を報告しません。

SSO エラー

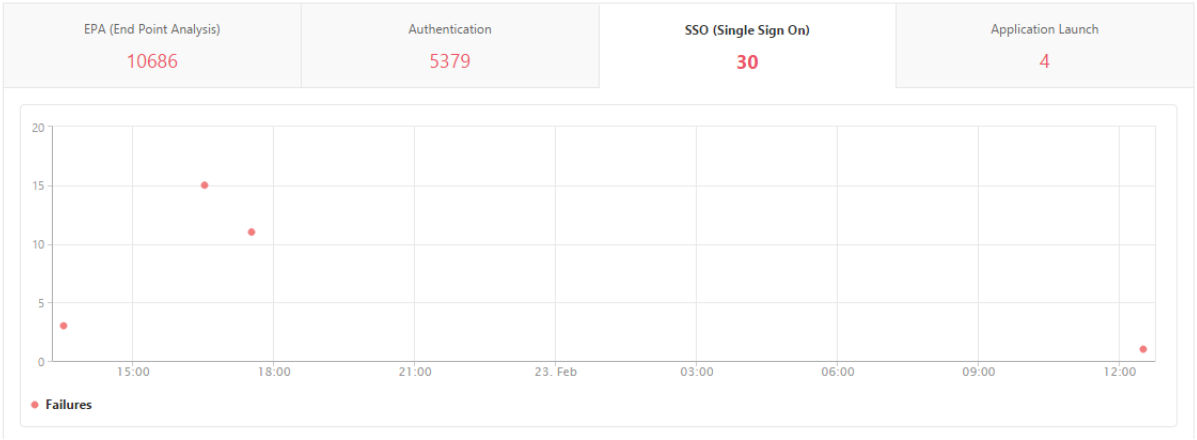
ADC Gateway アプライアンスを介してアプリケーションにアクセスするユーザーについて、どの段階でも SSO 障害をすべて表示できます。

SSO エラーの詳細の表示

1. Citrix ADM で、[**Analytics] > [Gateway Insight**] に移動します。
2. [Overview] セクションで SSO エラーを表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。[**Go**] をクリックします。



3. [**SSO (**シングルサインオン**)**] タブをクリックします。特定の期間における SSO エラーの数が、[Failures] のグラフに表示されます。



同じタブのテーブルから、ユーザー名、**ADC IP** アドレス、エラー時間、エラーの説明、リソース名などの各 **SSO** エラーの詳細を表示するには、下にスクロールします。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

[Username] カラムで ユーザをクリックすると、そのユーザの SSO エラーやその他の詳細を表示できます。

次の図に示すように、リストの矢印を使用して、テーブルをカスタマイズして列を追加または削除できます。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

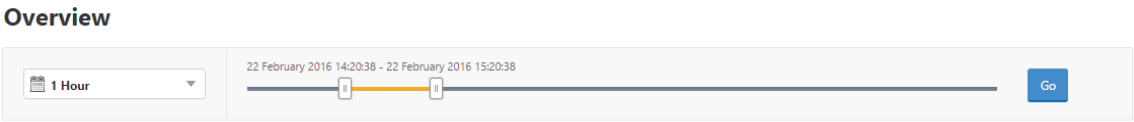
2. ADC Gateway に正常にログオンした後、ユーザーは仮想アプリケーションを起動できない

アプリケーションの起動に失敗した場合、アクセスできないセキュアチケット機関（STA）または Citrix Virtual App サーバー、または無効な STA チケットなどの理由を把握できます。エラーの時間や詳細、STA 検証ができなかったリソースについて確認できます。

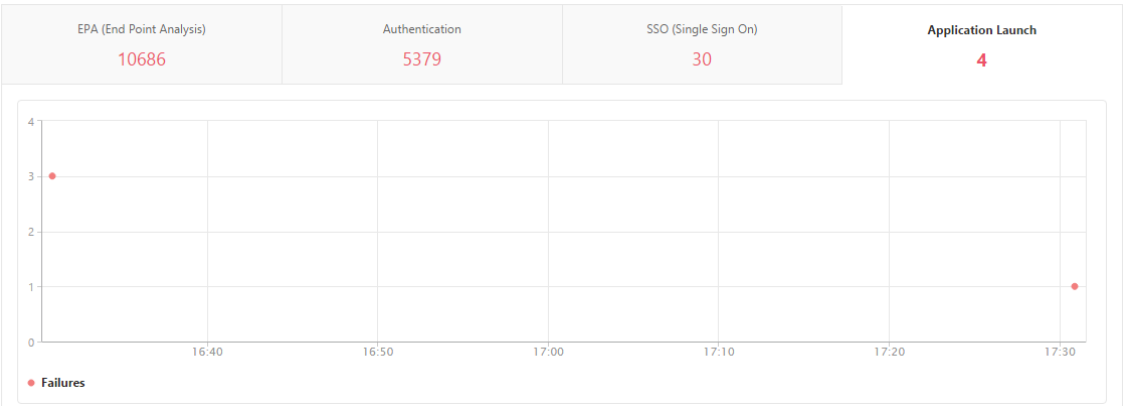
アプリケーションの起動失敗の詳細を表示する

1. Citrix ADM で、[**Analytics] > [Gateway Insight**] に移動します。

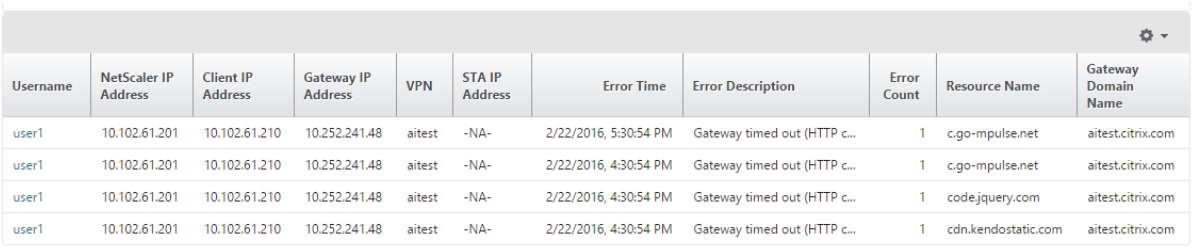
2. [概要] セクションで、SSO エラーを表示する期間を選択します。時間スライダーを使用すると、選択した期間をさらに調整できます。[**Go**] をクリックします。



3. [アプリケーションの起動] タブをクリックします。[失敗] グラフでは、任意の時点でのアプリケーション起動の 失敗数を表示できます。



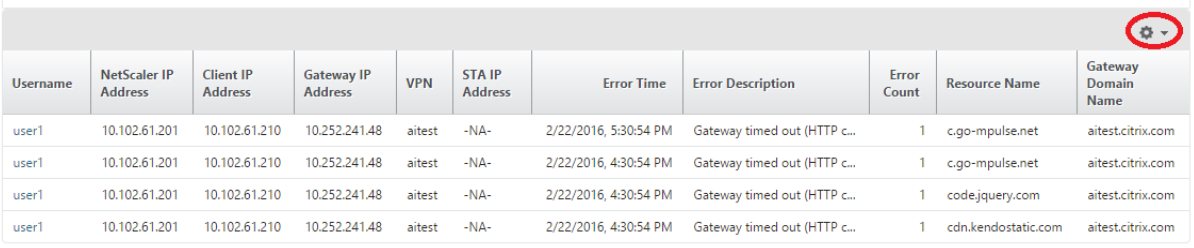
同じタブのテーブルから、**ADC IP** アドレス、エラー時間、エラーの説明、リソース名、ゲートウェイドメイン名など、各アプリケーションの起動エラーの詳細を表示するには、下にスクロールします。表の [**Error Description**] 列には STA サーバーの IP アドレスが、[**Resource Name**] 列には STA 検証ができなかったリソースの詳細が表示されています。



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

[Us **ername**] 列でユーザーをクリックすると、アプリケーションの起動エラーとそのユーザーのその他の詳細を表示できます。

次の図に示すように、リストの矢印を使用して、テーブルをカスタマイズして列を追加または削除できます。



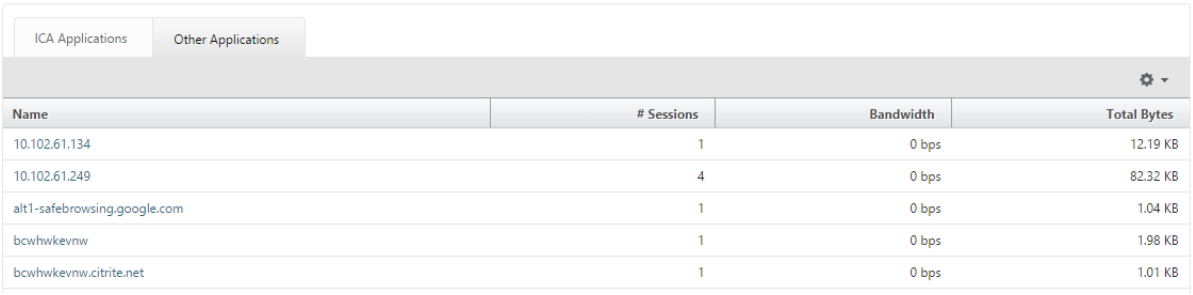
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

3. 新しいアプリケーションを正常に起動した後、ユーザーは、そのアプリケーションによって消費された合計バイト数と帯域幅を表示したい

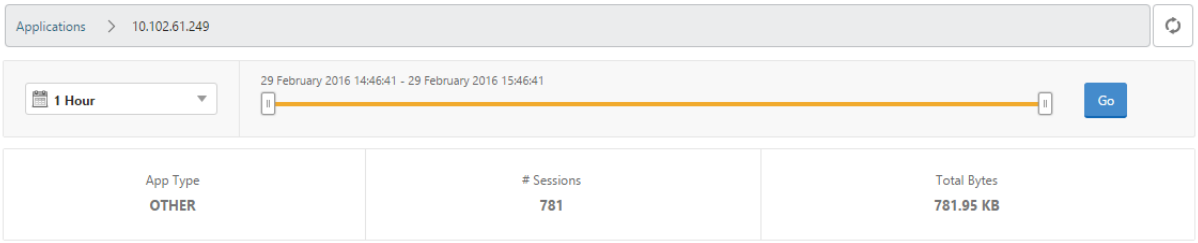
新しいアプリケーションを正常に起動したら、Citrix ADM で、そのアプリケーションによって消費された合計バイト数と帯域幅を表示できます。

アプリケーションによって消費された合計バイト数と帯域幅の表示

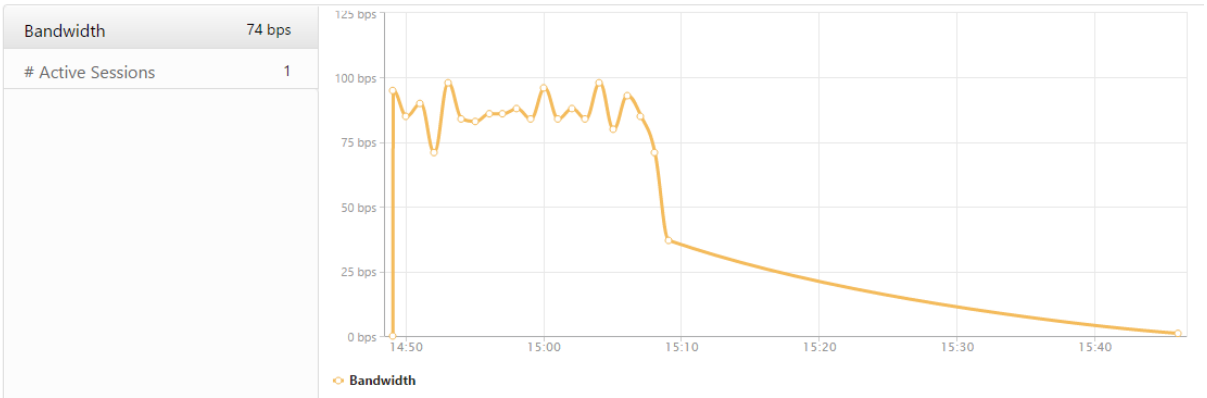
Citrix ADM で、[**Analytics] > [Gateway Insight] > [**アプリケーション] に移動し、下にスクロールして、[その他のアプリケーション] タブで詳細を表示するアプリケーションをクリックします。



そのアプリケーションが使用したセッション数と合計バイト数が表示されます。



そのアプリケーションが使用した帯域幅も表示されます。

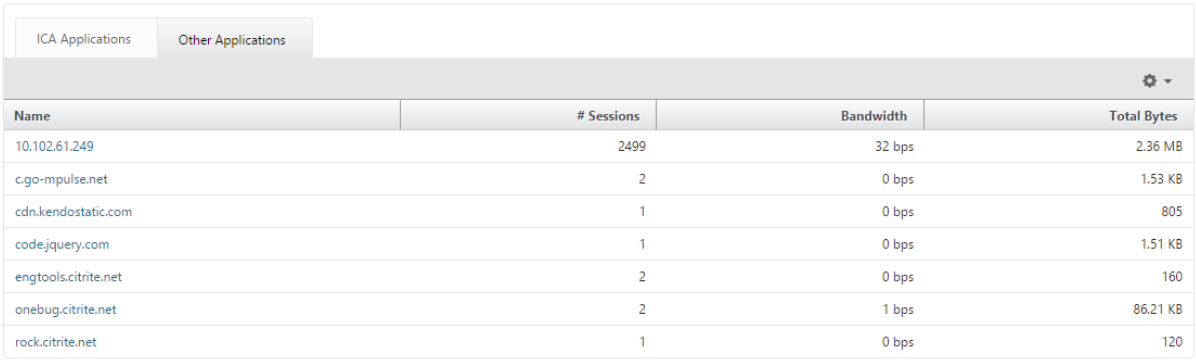


4. ユーザーが **ADC Gateway** に正常にログオンしましたが、内部ネットワークの特定のネットワークリソースにアクセスできません

Gateway Insight では、ユーザーがネットワークリソースにアクセスできるかどうかを特定できます。また、エラーの原因となったポリシーの名前を確認できます。

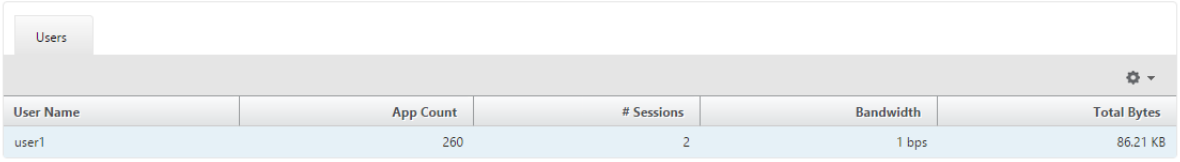
リソースに対するユーザーアクセスの表示

1. Citrix ADM で、[**Analytics] > [Gateway Insight] > [**アプリケーション**]** に移動します。
2. 表示画面を下にスクロールして、[**Other Applications**] タブでユーザーがログオンできなかったアプリケーションを選択します。



Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	2499	32 bps	2.36 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB
rock.citrite.net	1	0 bps	120

表示される画面を下にスクロールし、「ユーザー」(Users) テーブルに、そのアプリケーションにアクセスできるすべてのユーザーが表示されます。



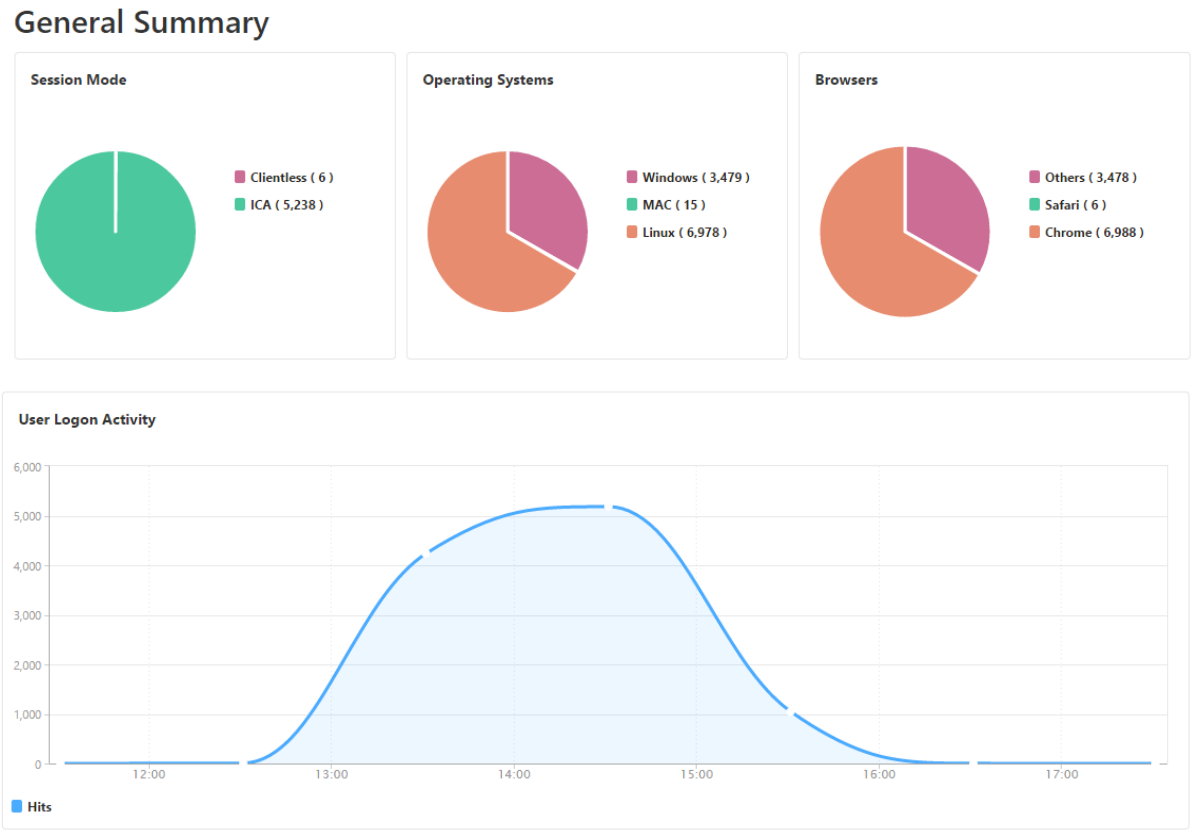
User Name	App Count	# Sessions	Bandwidth	Total Bytes
user1	260	2	1 bps	86.21 KB

5. 異なるユーザーが異なる **ADC Gateway** 配置を使用しているか、異なるアクセス・モードを介して **ADC** ゲートウェイにログオンしている可能性があります。管理者は、展開の種類とアクセスモードの詳細を表示できる必要があります

Gateway Insight では、ユーザーがログオンに使用したさまざまなセッションモードの概要、クライアントの種類、時間ごとのログオンしたユーザー数を確認できます。また、ユーザーの配置がユニファイドゲートウェイ配置か、従来の ADC Gateway 配置かを判断することもできます。Unified Gateway の展開では、コンテンツスイッチ仮想サーバーの名前と IP アドレス、VPN 仮想サーバー名を確認できます。

セッションモード、クライアントの種類、ログオンしているユーザー数の概要を表示する

1. Citrix ADM で、[**Analytics] > [Gateway Insight**] に移動します。
2. [概要] セクションで、下にスクロールして、[セッションモード**]**、**[**オペレーティングシステム**]**、**[**ブラウザ]、および [ユーザーログオンアクティビティ**]** の各グラフに、ユーザーがログオンするために使用するさまざまなセッションモード、クライアントの種類、および 1 時間ごとにログオンしたユーザー数が表示されます。



Gateway Insight の問題のトラブルシューティング

May 7, 2021

Gateway Insight ソリューションが期待どおりに機能しない場合は、次のいずれかの問題が発生している可能性があります。トラブルシューティングについては、各セクションのチェックリストを参照してください。

- Gateway Insight 設定。
- Citrix ADC と Citrix ADM の間の接続に関する問題。
- Citrix ADC でのレコード生成。
- Citrix ADM での検証。

Gateway Insight 設定チェックリスト

- Citrix ADC で AppFlow 機能が有効になっていることを確認します。詳しくは、「AppFlow の有効化」を参照してください。
- Citrix ADC の実行構成で Gateway Insight 構成を確認します。

`show running | grep -i <appflow_policy>` コマンドを実行して、Gateway Insight の設定を確認します。バインドタイプが REQUEST であることを確認します。たとえば、

```
bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
```

- シングルホップ、アクセスゲートウェイ、または Unified Gateway の展開では、Gateway Insight AppFlow ポリシーが VPN トラフィックが流れる VPN 仮想サーバーにバインドされていることを確認します。詳しくは、「HDX Insight データ収集の有効化」を参照してください。
- Citrix Gateway/VPN 仮想サーバーの`appflowlog`パラメータをチェックします。詳しくは、「仮想サーバーの AppFlow の有効化」を参照してください。

Citrix ADC と Citrix ADM の間の接続チェックリスト

- Citrix ADC で AppFlow コレクタのステータスを確認します。詳しくは、「Citrix ADC と AppFlow コレクタ間の接続状態を確認する方法」を参照してください。
- Gateway Insight AppFlow ポリシーヒットをチェックします。

  コマンド`show appflow policy <policy_name>`を実行して、AppFlow ポリシーのヒットをチェックします。

  GUI で [システム] **> [AppFlow] > [**ポリシー**]** に移動して、AppFlow ポリシーのヒットを確認することもできます。
- AppFlow ポート 4739 または 5557 をブロックしているファイアウォールを検証します。

Citrix ADC チェックリストでのレコード生成

- `nsconmsg -d stats -g ai_tot`コマンドを実行し、Citrix ADC で統計値の増分を確認します。
- `nstrace`ログをキャプチャし、CFLOW パケットをチェックして、Citrix ADC が AppFlow レコードをエクスポートすることを確認します。

Citrix ADM での検証

- `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` コマンドを実行して、ログをチェックして、Citrix ADM が AppFlow レコードを受信していることを確認します。
- Citrix ADC インスタンスが Citrix ADM に追加されていることを確認します。
- Citrix Gateway/VPN 仮想サーバーが Citrix ADM でライセンスされていることを確認します。

Gateway Insight の統計情報

次の Gateway Insight 統計が利用できます。

- ai_tot_preauth_epa_export

- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_fileinfo_export
- ai_tot_app_launch_failure
- ai_tot_logout_export
- ai_tot_skip_appflow_export
- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export
- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_mismatch
- ai_tot_appflow_disabled

Citrix テクニカルサポートに問い合わせてください

迅速な解決のために、Citrix テクニカルサポートに連絡する前に、次の情報を確認してください。

- 展開とネットワークトポロジの詳細。
- Citrix ADC および Citrix ADM バージョン。
- Citrix ADC および Citrix ADM のテクニカルサポートバンドル。
- `nstrace`は問題発生中にキャプチャします。

既知の問題

Gateway Insight の既知の問題については、Citrix ADC リリースノートを参照してください。

アプリケーションのセキュリティ違反の詳細を表示する

May 7, 2021

インターネットにさらされている Web アプリケーションは、攻撃に対して非常に脆弱になっています。Citrix ADM を使用すると、アクション可能な違反の詳細を視覚化し、アプリケーションを攻撃から保護できます。単一ペインソリューションの [分析] > [セキュリティ**] > [**セキュリティ違反] に移動して、次の操作を行います。

- セキュリティインサイトとボットインサイトの両方に関連する脅威の詳細を完全に可視化して、アプリケーションを可視化
- ネットワーク、ボット、**WAF** などのカテゴリに基づいてアプリケーションのセキュリティ違反にアクセスする
- アプリケーションを保護するための是正措置を講じる

「セキュリティ違反」ページには、次のオプションがあります。

- [**Application** Overview]：違反合計、WAF および Bot 違反の合計、国別の違反など、アプリケーションの概要を表示します。詳しくは、「アプリケーションの概要」を参照してください。
- 「すべての違反」— アプリケーションのセキュリティ違反の詳細を表示します。詳しくは、「すべての違反」を参照してください。

セットアップする

Citrix ADM で次の違反を表示するには、［高度なセキュリティ分析］を有効にして［**Web** トランザクション設定］を［すべて］に設定する必要があります。

- 異常に高いアップロードトランザクション (WAF)
- 異常に高いダウンロードトランザクション (WAF)
- 過度なユニーク IP（WAF）
- アカウント乗っ取り (BOT)
- ウェブサイトスキャナ (BOT)
- コンテンツスクレーパー (BOT)

その他の違反については、メトリック・コレクタが有効になっていることを確認します。デフォルトでは、メトリックスコレクターは Citrix ADC インスタンスで有効になっています。詳しくは、「インテリジェントアプリ分析の構成」を参照してください。

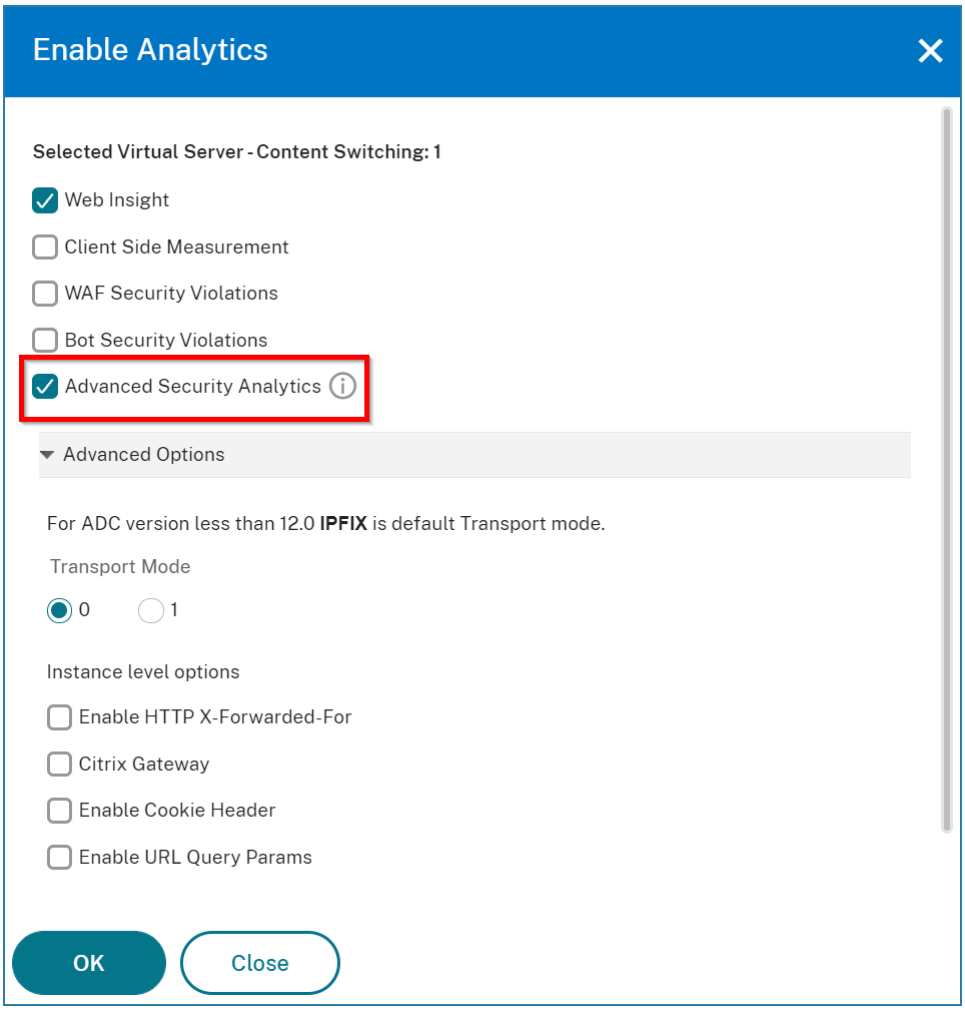
高度なセキュリティ分析を有効にする

1. [ネットワーク] > [インスタンス] > [**Citrix ADC**] に移動し、インスタンスタイプを選択します。たとえば、MPX。
2. Citrix ADC インスタンスを選択し、［アクションの選択］リストから［アナリティクスの構成］を選択します。
3. 仮想サーバーを選択し、[**Analytics** の有効化] をクリックします。
4. **[Analytics** の有効化] ウィンドウで、次の操作を行います。
   a) [**Web Insight**] を選択します。[Web Insight] を選択すると、読み取り専用の [高度なセキュリティ分析] オプションが自動的に有効になります。

      > 注
      >
      > [**Advanced Security Analytics**] オプションは、プレミアムライセンスの ADC インスタンスに対してのみ表示されます。

   b) 転送モードとして **Logstream** を選択します
   c) 式はデフォルトで true です

d) [**OK**] をクリックします。

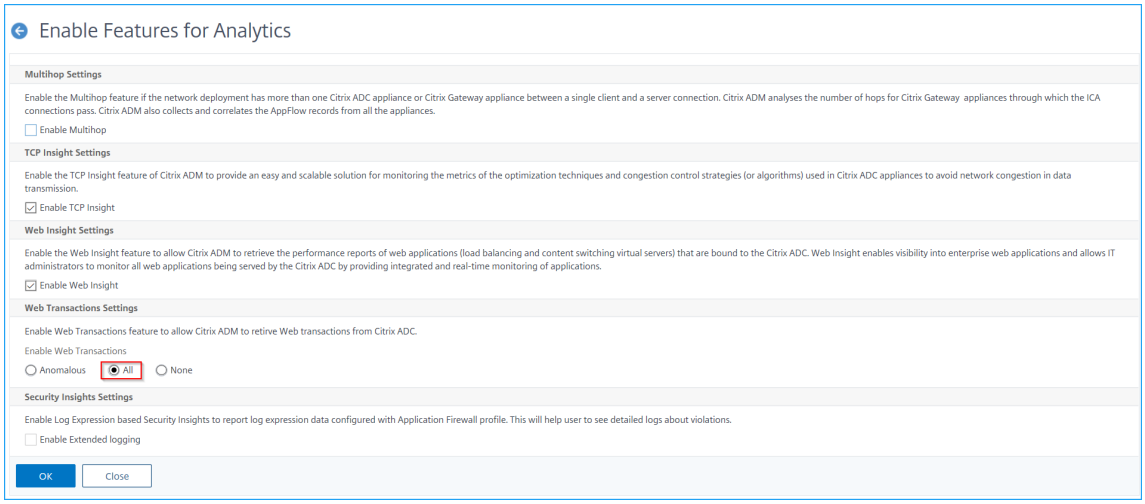


Web トランザクション設定を有効にする

1. [**Analytics**] > [設定] に移動します。

   [設定] ページが表示されます。

2. [分析機能の有効化] をクリックします。
3. 「**Web** トランザクション設定」で、「すべて」を選択します。



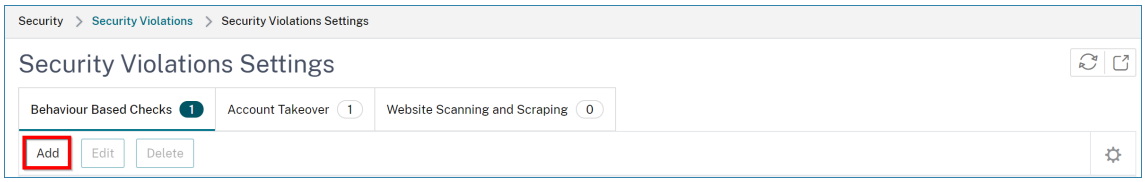
4. [**OK]** をクリックします。

動作確認プロファイルの設定

Citrix ADM では、動作ベースの違反を選択できます。過剰なクライアント接続、**Web** サイトのスキャン、異常に高いアップロードトランザクション、およびダウンロードトランザクション違反が非常に高い場合は、感度レベルを [低]、[中]、[高] として選択できます。プロファイルを作成することで、これらの違反に対する異常の総数を Citrix ADM で報告する方法を決定できます。

この設定を構成するには、次の手順に従います。

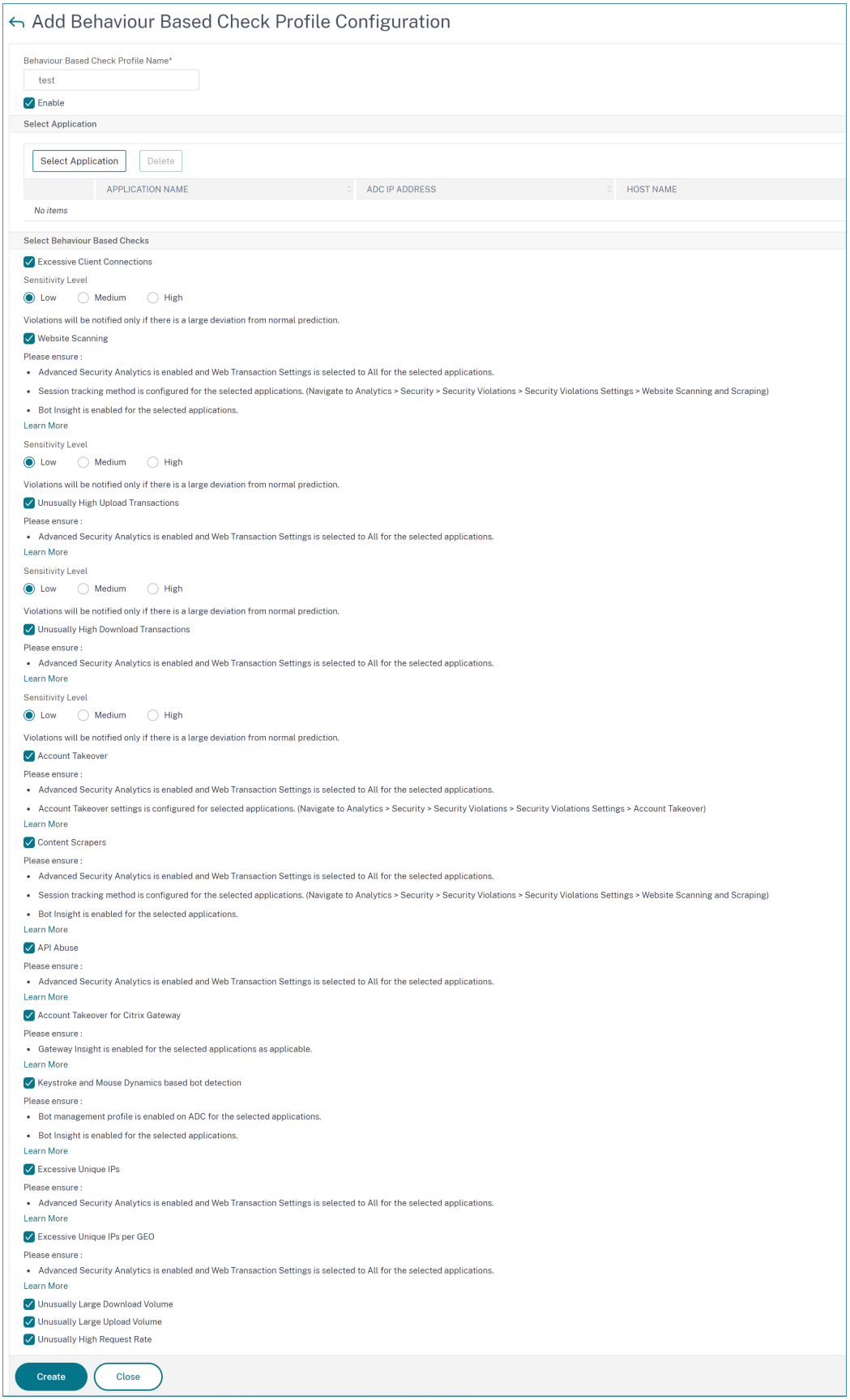
1. [分析] **>** [セキュリティ] **>** [セキュリティ違反] に移動します。
2. 時間リストの横にある設定アイコンをクリックします。
3. [動作ベースのチェック] で、[追加] をクリックします。



4. 次のパラメータを指定します。
   a)「動作ベースのチェックプロファイル名」— 任意のプロファイル名を指定します。
   b) [有効] オプションを選択します。デフォルトではこのオプションが選択されています。
   c) [アプリケーションの選択] で、プロファイルを適用するアプリケーションを選択します。
   d)「動作ベースのチェックの選択」で、「低」、「中」または「高」を選択して、これらの違反の感度レベルを定義します。

> 注
>
> デフォルトでは、他のすべての動作ベースの違反も有効になります。違反を無効にすると、Citrix ADM は通常の予測に基づいてのみ、これらの違反の異常を検出します。

e)［作成］をクリックします。



WAF 学習エンジン

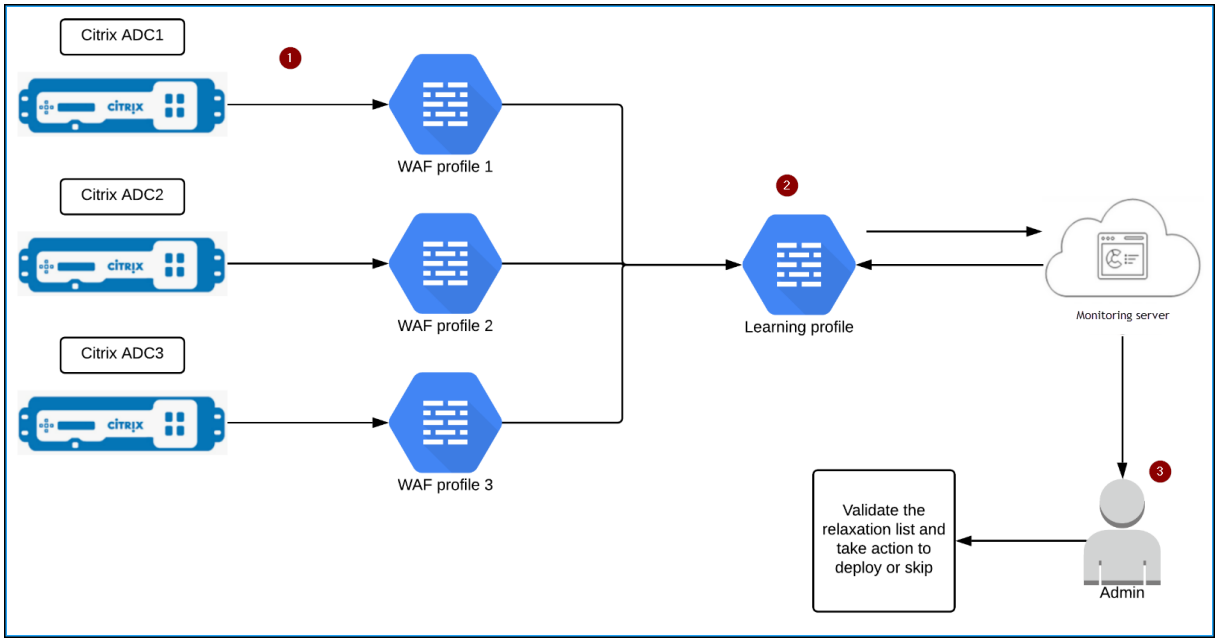
May 7, 2021

Citrix Web App Firewall（WAF）は、SQL インジェクションやクロスサイトスクリプティングなどの悪意のある攻撃から Web アプリケーションを保護します。データ漏洩を防ぎ、適切なセキュリティ保護を提供するには、トラフィックを監視して、脅威や攻撃に関するリアルタイムの実用的なデータを監視する必要があります。報告された攻撃は偽陽性であり、例外として提供する必要がある場合があります。

Citrix ADM 学習エンジンは、WAF が Web アプリケーションの動作（通常のアクティビティ）を学習できるようにする反復パターンフィルターです。エンジンは、モニタリングに基づいて、HTTP トラフィックに適用されるセキュリティチェックごとに推奨されるルールまたは例外のリストを生成します。

ラーニングエンジンを使用して緩和ルールを展開する方が、必要なリラックスとして手動で展開するよりも、はるかに簡単です。

次の画像は、Citrix ADM での WAF ラーニングの仕組みに関する高レベルの情報を示しています。



1 — WAF プロファイルを持つ Citrix ADC インスタンス

2 — Citrix ADM で学習プロファイルを構成し、WAF プロファイルを追加し、緩和ルールの自動展開または手動展開を選択します。

3 — 管理者は Citrix ADM で緩和ルールを検証し、展開するかスキップするかを決定できる

導入

学習機能を展開するには、まず Citrix ADC アプライアンスで Web App Firewall プロファイル（セキュリティ設定のセット）を構成する必要があります。詳しくは、「Web App Firewall プロファイルの作成」を参照してください。

Citrix ADM は、セキュリティチェックごとに例外（緩和）のリストを生成します。管理者は、Citrix ADM で例外の一覧を確認し、展開するかスキップするかを決定できます。

Citrix ADM WAF ラーニング機能を使用すると、次のことができます。

- 次のセキュリティチェックを使用して学習プロファイルを設定します。
  - 開始 URL
  - クッキーの一貫性
  - クレジットカード

    > 注
    >
    > クレジットカードのセキュリティチェックを行うには、Citrix ADC インスタンスで`doSecureCreditCardLogging`を構成し、設定が **OFF** になっていることを確認する必要があります。

  - コンテンツの種類
  - フォームフィールドの一貫性
  - フィールドの書式
  - CSRF フォームタグ付け
  - HTML クロスサイトスクリプティング

    > 注
    >
    > クロスサイトスクリプトの場所の制限は、FormField のみです。

  - HTML SQL インジェクション

    > 注
    >
    > HTML SQL インジェクションチェックでは、Citrix ADC インスタンスで`set -sqlinjectionTransformSpecialChars ON`と`set -sqlinjectiontype sqlspclcharorkeywords`を構成する必要があります。

- Citrix ADM で緩和ルールを確認し、必要なアクション（展開またはスキップ）を実行することを決定する
- メール、slack、ServiceNow で通知を受け取る
- 「処理要約」ページを使用して、緩和の詳細を表示します。

Citrix ADM で WAF ラーニングを使用するには：

1. ラーニングプロファイルの設定
2. 緩和ルールを見る
3. WAF ラーニングアクションの概要ページを使用する

TCP Insight

May 7, 2021

Citrix Application Delivery Management（ADM）の TCP Insight 機能は、データ伝送におけるネットワークの輻輳を回避するために、Citrix ADC アプライアンスで使用される最適化手法と輻輳制御戦略（またはアルゴリズム）のメトリックを監視するための簡単でスケーラブルなソリューションを提供します。この機能では、TCP を最適化して、またはしないで TCP ファイルのダウンロードやアップロードのパフォーマンスを測定する「TCP スピードレポート」機能を使用します。

データボリューム、スループット、速度などの主要なトランスポート層メトリックを表示し、この情報を使用して Citrix ADC インスタンスが処理するトラフィック量を測定し、TCP Optimization の利点を検証できます。上記のメトリックには、ストリーム方向（クライアントから Citrix ADC および Citrix ADC からオリジンサーバーへ）、TCP ポート、および仮想 LAN による分類が提供されます。

前提条件

TCP Insight 機能の構成を開始する前に、以下の前提条件が満たされていることを確認してください。

- Citrix ADC インスタンスは、ソフトウェアバージョン 11.1 ビルド 51.21 以降で実行されています。
- ソフトウェアバージョン 11.1 ビルド 51.21 以降で実行されている Citrix ADM をインストールしている。
- アプリケーション用に構成されているすべての仮想サーバーには、Citrix ADM の管理と監視のライセンスが付与されます。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。

Citrix ADM のハードウェア要件：

コンポーネント	条件
RAM	8GB
仮想 CPU	4
	注：パフォーマンスを向上させるには、8 つの CPU をお勧めします。
記憶域	120 GB
	注：パフォーマンスを向上させるには、500 GB をお勧めします。

TCP Insight の有効化

TCP Insight メトリックを表示する前に、Citrix ADM でこの機能を有効にする必要があります。

TCP Insight を有効にするには:

1. Web ブラウザで、Citrix ADM 仮想アプライアンスの IP アドレス（例: `http://192.168.100.1`）を入力します。
2. [**User Name**] と [**Password**] に管理者の資格情報を入力します。
3. [**Analytics**] > [設定] に移動し、[**Analytics** の機能を有効にする] をクリックします。
4. [**Analytics** の機能を有効にする] ページで、[**TCP Insight** を有効にする] を選択します。
5. 確認ウィンドウで、[**OK**] をクリックします。

Citrix ADM での **TCP Insight** メトリックの表示

Citrix ADM で TCP Insight を有効にすると、トラフィックモード（インターネットまたはモバイルデータ）、データボリューム、スループット、インターフェイス、ポート、平均アップロード速度、平均ダウンロード速度などの主要なトランスポート層情報を表示できます。

Citrix ADM で **TCP Insight** メトリックを表示するには:

[**Analytics**] > [**TCP Insight**] に移動します。

棒グラフにマウスポインターを合わせると、対応するトランスポートテクニックのデータ量が表示されます。また、グラフの下の表にデータボリュームとその他のメトリックを表示できます。

> 注**:** グラフに表示される指標をカスタマイズするには、表の [設定] アイコンを使用します。メトリックに関連する期間を選択したり、タイムスライダーを使用して期間を調整することもできます。

TCP Insight リストから選択して、インターフェイス、ポート、ビットレートなどのメトリックを表示することもできます。

使用例

以下のユースケースは、Citrix ADC アプライアンス上で TCP Insight を使用する方法の一部を示しています。

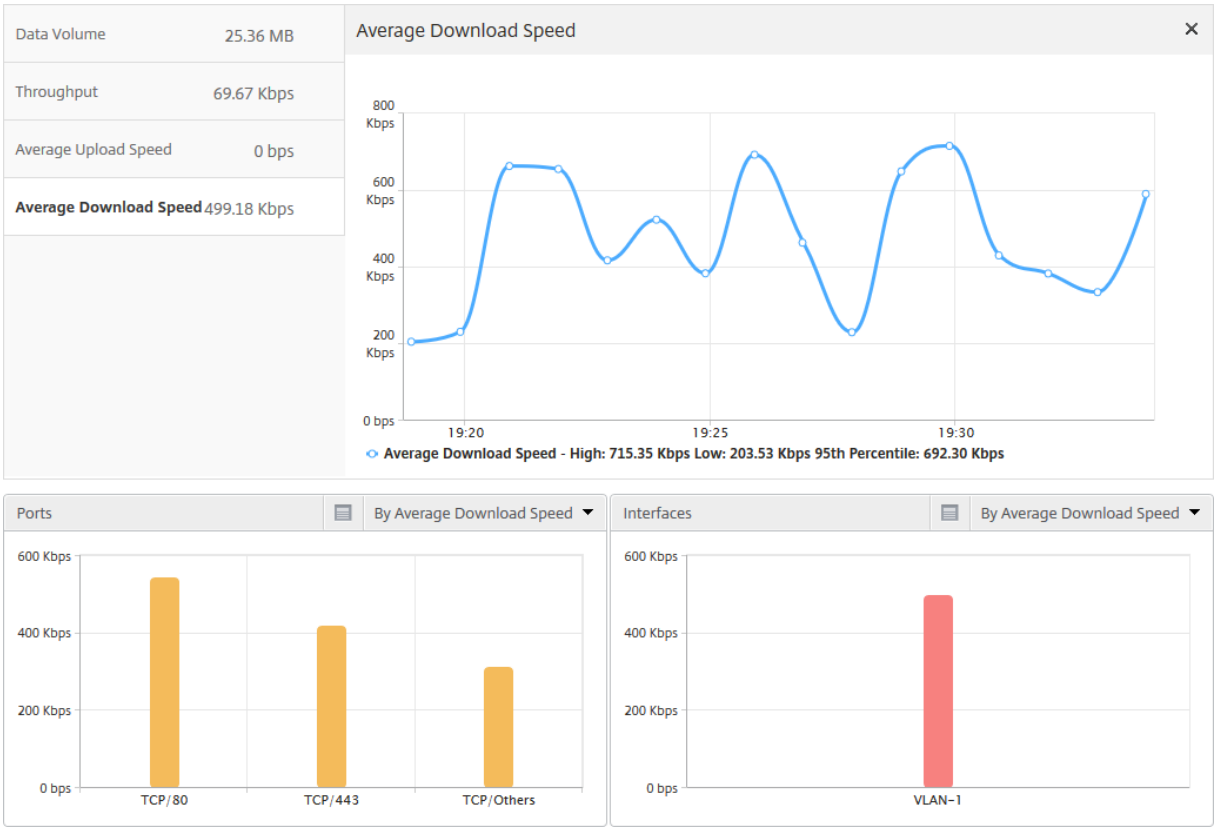
- TCP 最適化の利点の評価
- TCP パラメータの調整
- トラフィック量に対する TCP 最適化の影響を測定

TCP 最適化の利点の評価

Citrix ADC TCP 最適化は、実際にモバイル（無線）またはエンタープライズネットワーク（インターネット）にどの程度のメリットがあるか。TCP 経由で発生するデータ転送の速度を表示して、最適化されていないパフォーマンスと最適化されたパフォーマンスを比較できます。これらの測定は、ダウンロード方向とアップロード方向（常に無線/ク

ライアント側から）や異なる宛先ポート（HTTP (80) と HTTPS (443)）で個別に表示されます。
TCP Insight メトリックスを調べることで、TCP フローを最適化することで得られる速度の向上を数値化できます。

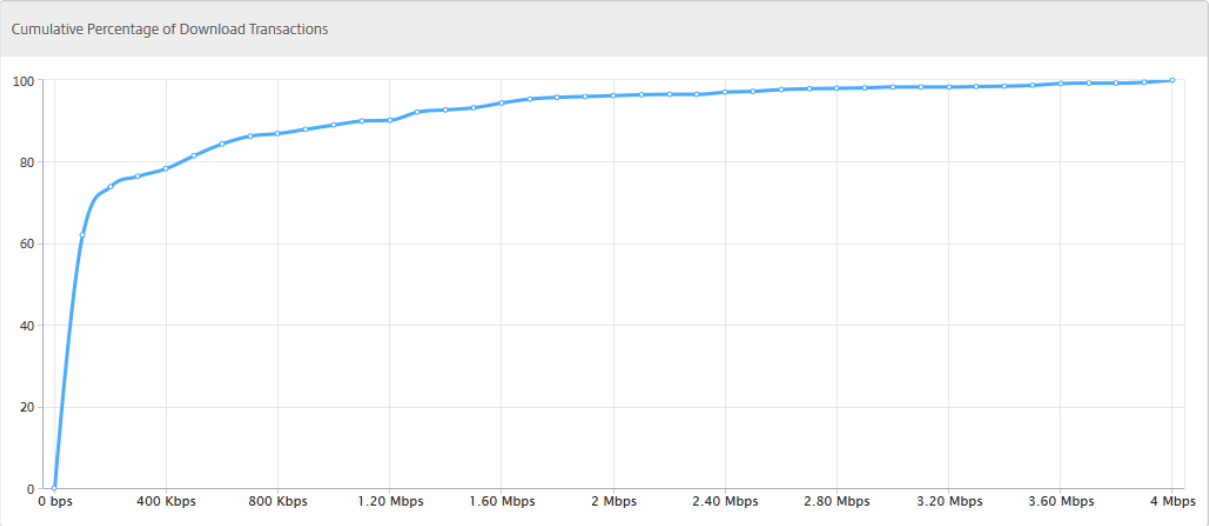
これらのパラメーターの概要を表示するには、Citrix ADM にログオンし、[**TCP Insight**] タブをクリックします。次に、[側面] をクリックし、棒グラフまたはグラフの下の表から [インターネット] または [ラジオ] を選択します。



TCP パラメータの調整

異なる TCP プロファイルを使用すると、同じトラフィックから異なる出力が生成されます。このような状況では、Citrix ADC で異なる TCP 最適化プロファイルが実行されている期間の速度測定値を表示および比較することができます。それらの結果を利用して、転送速度が上がるように TCP パラメーターを調整したり、特定のお客様のネットワークでのユーザー体験を最大限に高める TCP プロファイルを作成したりできます。

レポートを表示するには、Citrix ADM にログオンします。次に、[**TCP Insight**] タブで [**Bitr**ate] をクリックし、棒グラフまたはグラフの下のテーブルから目的のビットレートを選択します。

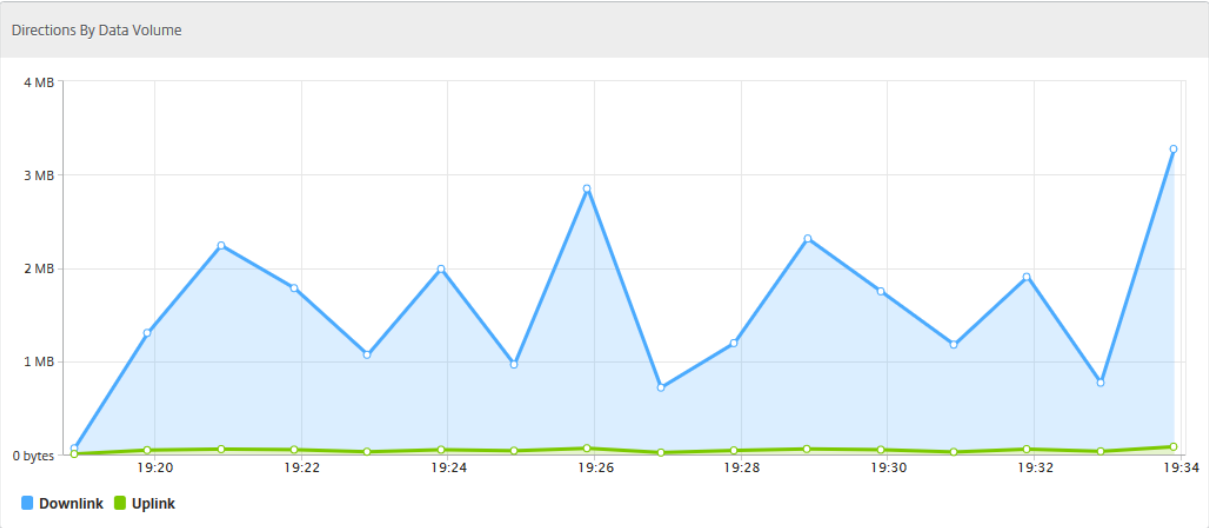


トラフィック量に対する **TCP** 最適化の影響を測定

Citrix ADC インスタンスが処理する IP 層データボリューム/スループットの測定値を異なる期間間で比較して、TCP 最適化がサブスクライバデータ消費に与える影響を評価できます。測定は、ネットワークの各サイド（無線サイドとインターネットサイド）、さまざまなトラフィックセグメント（さまざまなインターフェイスや VLAN によって線引き）、各方向（ダウンリンクとアップリンク）、さまざまな宛先ポート（HTTP と HTTPS）に個別に適用できます。この比較を利用して、TCP 最適化によりサブスクライバーのデータ消費が促進されていることを確認できます。

測定値の概要を表示するには、Citrix ADM にログオンし、[**TCP Insight**] タブで［側面］をクリックし、棒グラフまたはグラフの下の表から［インターネット］または［無線］を選択します。

タイムリストから別のタイムフレームを選択することもできます。期間は、スライダーを使用してカスタマイズできます。



WAN Insight

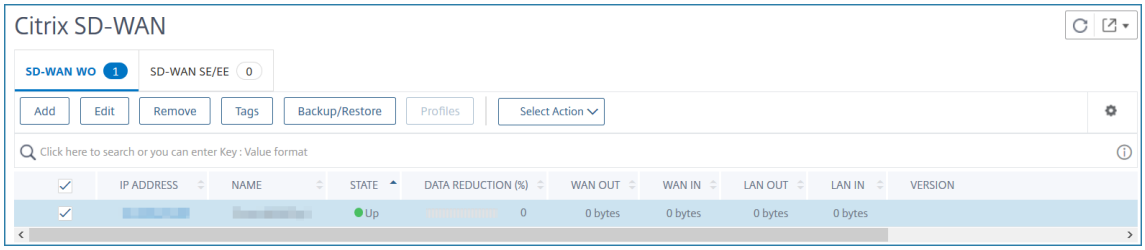
May 7, 2021

Citrix SD-WAN WAN 最適化（WO）アプライアンスは、データセンターとブランチサイト間のネットワークを介したデータフローの効率を向上させることにより、WAN を介した多数のアプリケーションの配信を最適化します。WAN Insight 分析により、管理者はデータセンターとブランチの WAN 最適化アプライアンスの間を流れる高速化および高速化されていない WAN トラフィックを簡単に監視できます。WAN Insight は、ネットワーク上のクライアント、アプリケーション、ブランチを可視化し、ネットワークの問題を効果的にトラブルシューティングできるようにします。ライブレポートと履歴レポートにより、問題があればプロアクティブに解決できます

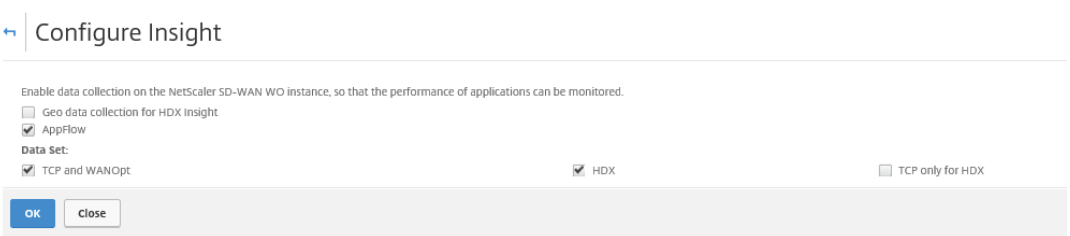
データセンター WAN 最適化アプライアンスで分析を有効にすると、Citrix Application Delivery Management（ADM）がデータを収集し、データセンターおよびブランチ WAN 最適化アプライアンスのレポートと統計を提供できるようになります。

WAN 最適化アプライアンス上で分析を有効にするには:

1. ［ネットワーク］>［インスタンス］**>**［**Citrix SD-WAN**］の順に選択し、SD-WAN WO インスタンスを選択します。



2. **[** アクションの選択**]** リストから、[インサイトを有効にする] を選択します。
3. 必要に応じて以下のパラメーターを選択します。
   - **HDX Insight** の地情報データ収集: クライアントの IP アドレスを Google Geo API と共有します。
   - **AppFlow**: WAN 最適化インスタンスからのデータの収集を開始します。
   - **TCP** および **WanOt**: TCP および **WAonPt** インサイトレポートを提供します。
   - **HDX**: HDX Insight レポートを提供します。
   - **HDX** のみの **TCP**: **HDX**Insight レポートにのみ TCP を提供します。



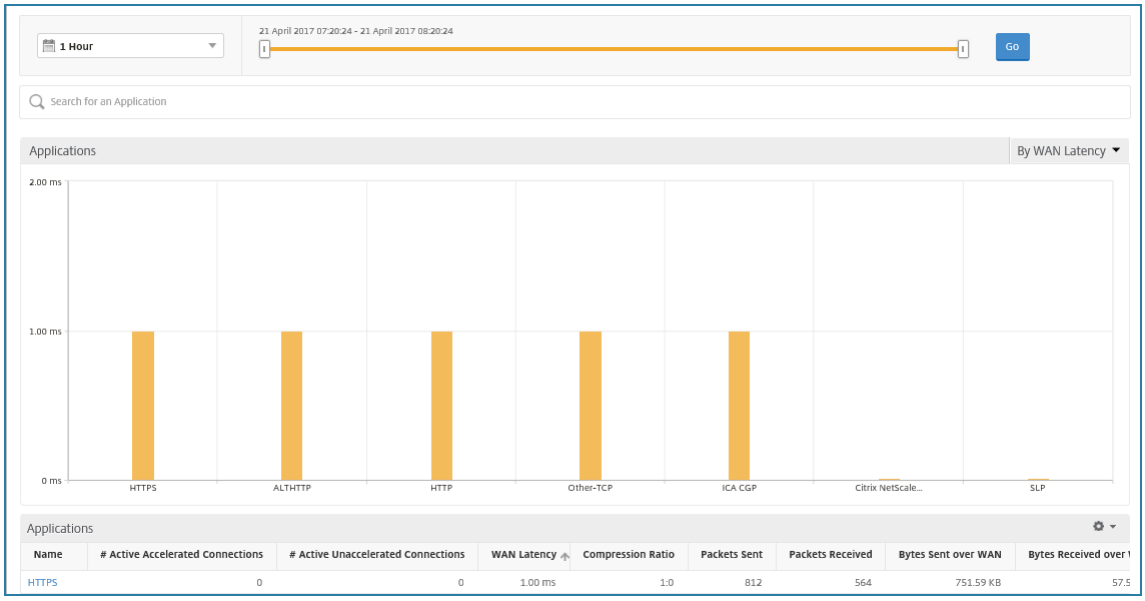
4. [**OK**] をクリックします。

WAN Insight レポートを表示するには、[分析] > [**WAN Insight**] に移動します。

> 注
>
> WAN Insight オプションは、SD-WAN WO インスタンスを Citrix ADM に追加した後にのみ表示されます。

次のレポートを表示できます。

- アプリケーション -選択した期間におけるすべてのアプリケーションの使用状況とパフォーマンスの統計を表示します。
- **Br** anches-すべての WAN 最適化ブランチアプライアンスの使用状況とパフォーマンスの統計情報を表示します。
- **Clients** -各ブランチで、WAN 最適化アプライアンスにアクセスするすべてのクライアントの使用状況とパフォーマンスの統計情報を表示します。



次のメトリックが表示されます。

測定基準	説明
Active Accelerated Connections	アクセラレーションが有効なアクティブ WAN 接続の数です。
Active Unaccelerated Connections	アクセラレーションが無効なアクティブ WAN 接続の数です。
WAN 遅延	アプリケーションとの対話中にユーザーに生じる遅延（ミリ秒単位）です。
圧縮率	選択した期間における、ブランチオフィスとデータセンターアプライアンス間のデータ圧縮率。

測定基準	説明
送信済みパケット	選択した期間に WAN 最適化アプライアンスからネットワーク経由で送信されたパケットの数です。
受信済みパケット	選択した期間に WAN 最適化アプライアンスがネットワークから受信したパケットの数です。
WAN で送信されたバイト数	選択した期間に Citrix WAN 最適化アプライアンスが WAN 経由で送信したバイト数。
WAN で受信したバイト数	選択した期間に WAN 最適化アプライアンスが WAN から受信したバイトの数です。
LAN RTO	選択した期間に WAN 最適化アプライアンスから LAN への再送信がタイムアウトになった回数です。
WAN RTO	選択した期間に WAN 最適化アプライアンスから WAN への再送信がタイムアウトになった回数です。
再転送パケット (LAN)	選択した期間に WAN 最適化アプライアンスから LAN ネットワークに再送信されたパケットの数です。
再転送パケット (WAN)	選択した期間に WAN 最適化アプライアンスから WAN ネットワークに再送信されたパケットの数です。

Video Insight

May 7, 2021

Video Insight 機能は、Citrix ADC アプライアンスで使用されるビデオ最適化テクニックのメトリックを監視するための簡単でスケーラブルなソリューションを提供し、顧客体験と運用効率を向上させます。これにより、次のようなメリットが得られます。

- ピーク時間における混雑時にネットワークを管理する。
- 動画再生の一貫性を向上させ動画の再生速度低下を抑える。
- 新しい動画サービスオファリング（Binge-on 動画サービスなど）を有効にする。
- 顧客が持続可能で最適な動画品質を選択できるようにする。
- サブスクライバーに一貫性のあるユーザーエクスペリエンスを提供する。

Citrix ADC アプライアンスは、ビデオトラフィックを最適化する際に、ビデオビットレートを動的にペースさせる特別なメカニズムと、ランダムサンプリング手法を使用して、最適化手法による節約額を推定します。Citrix ADC ビデオ最適化機能について詳しくは、ビデオの最適化を参照してください。Citrix ADC アプライアンスを Citrix

Application Delivery Management（ADM）と統合すると、Citrix ADC アプライアンスを介して流れるビデオデータから重要な情報を収集します。この情報を使用することで、最適化している場合としていない場合の ABR 動画トラフィックのパフォーマンスを比較したり、最適化による削減率を求めたりすることができます。

> 注
>
> Citrix ADM で提供される最適化されていないセッションの統計情報は、Citrix ADC アプライアンスでランダムサンプリングで選択したセッションに対応します。ランダムサンプリングについて詳しくは、ビデオの最適化を参照してください。

Citrix ADM Video Insight は、次の種類のビデオトラフィックに関するメトリックを提供します。

- HTTP 経由でのプログレッシブダウンロード（PD）動画
- HTTP 経由の ABR 動画
- HTTPS 経由の ABR 動画
- QUIC 経由の YouTube ABR 動画

Video Insight の構成

> 注
>
> Video Insight は、Citrix ADC Premium ライセンスを持つ Citrix ADC インスタンスでサポートされています。Citrix ADC Premium ライセンスは、Citrix ADC Telco プラットフォーム（VPX T1000 および VPX-T）でサポートされています。

Citrix ADC インスタンスでビデオインサイトを構成するには、まず AppFlow 機能を有効にし、AppFlow コレクター、アクション、およびポリシーを構成し、ポリシーをグローバルにバインドします。コレクタを構成するときは、レポートを監視する Citrix ADM サーバーの IP アドレスを指定する必要があります。

Citrix ADC インスタンスでビデオインサイトを構成するには、次のコマンドを実行して AppFlow プロファイルとポリシーを構成し、AppFlow ポリシーをグローバルにバインドします。

add appflow collector <name> **-IPAddress** <ipaddress> **-port** <port_number> **-Transport** logstream

set appflow param -**videoInsight** ENABLED

add appflow action <name> **-collectors** <string> **-videoAnalytics** ENABLED

add appflow policy <name> <rule> <action>

bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

enable ns mode ulfd

機能を有効にする AppFlow

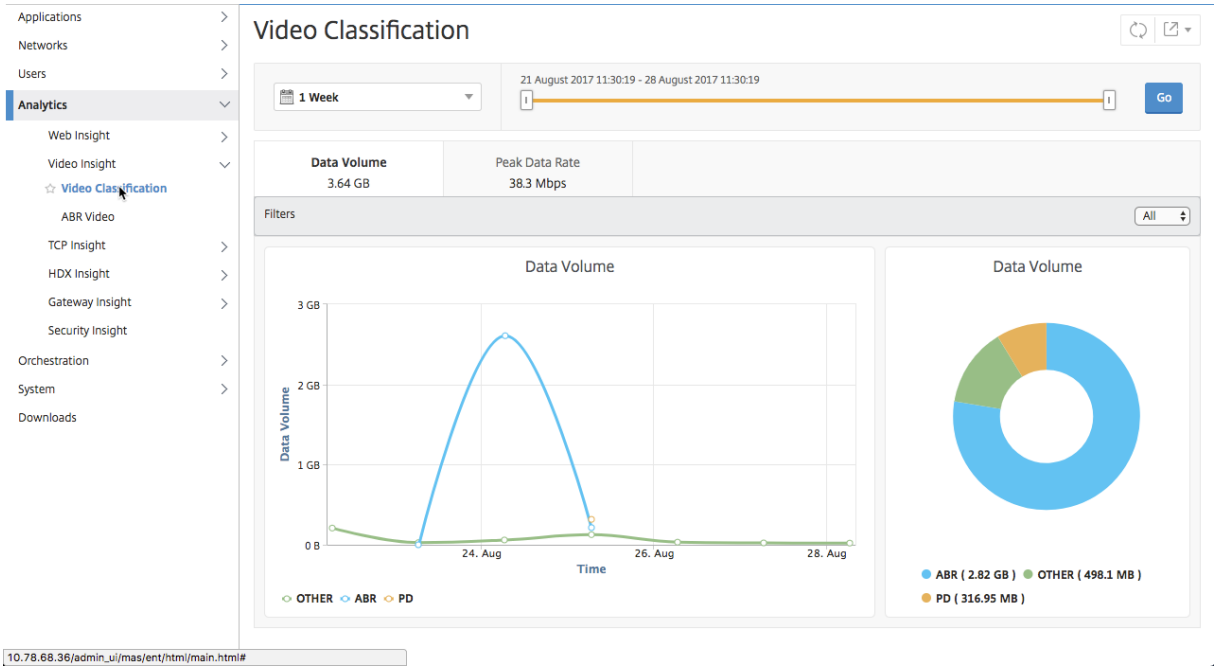
サンプル


```
add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -
    Transport logstream
set appflow param -videoInsight ENABLED
add appflow action act1 -collectors col1 -videoAnalytics ENABLED
add appflow policy appol true act1
bind appflow global appol 1
enable ns mode ulfd
enable feature appflow
<!--NeedCopy-->
```

Citrix ADM での Video Insight メトリックの表示

Citrix ADM で Video Insight を有効にすると、ビデオの分類、データボリューム、ピークデータレート、ABR ビデオの再生などのビデオの最適化指標を表示できます。これらのメトリックにより、ネットワークを分析して動画を最適化し、サブスクライバーのエクスペリエンス、操作の効率、その他のパフォーマンス基準を改善することができます。

Citrix ADM で Video Insight 指標を表示するには、［分析］**>**［**Video Insight**］の順に移動します。



> 注
>
> チャート内の凡例 O **th** er によって提供される値は、選択したフィルタに応じて、ビデオトラフィックの非 ABR および非 PD データを表します。
>
> - **All**： ビデオトラフィック内の非 ABR（HTTP、HTTPS、および QUIC）および非 PD（HTTP）データの合計。
> - **HTTP**： ビデオトラフィック内の非 ABR データと非 PD データの合計。

- **HTTPS**： ビデオトラフィック内の ABR 以外のビデオデータの合計。
- **QUIC** — ビデオトラフィック内の ABR 以外のビデオデータの合計。

ネットワーク効率の表示

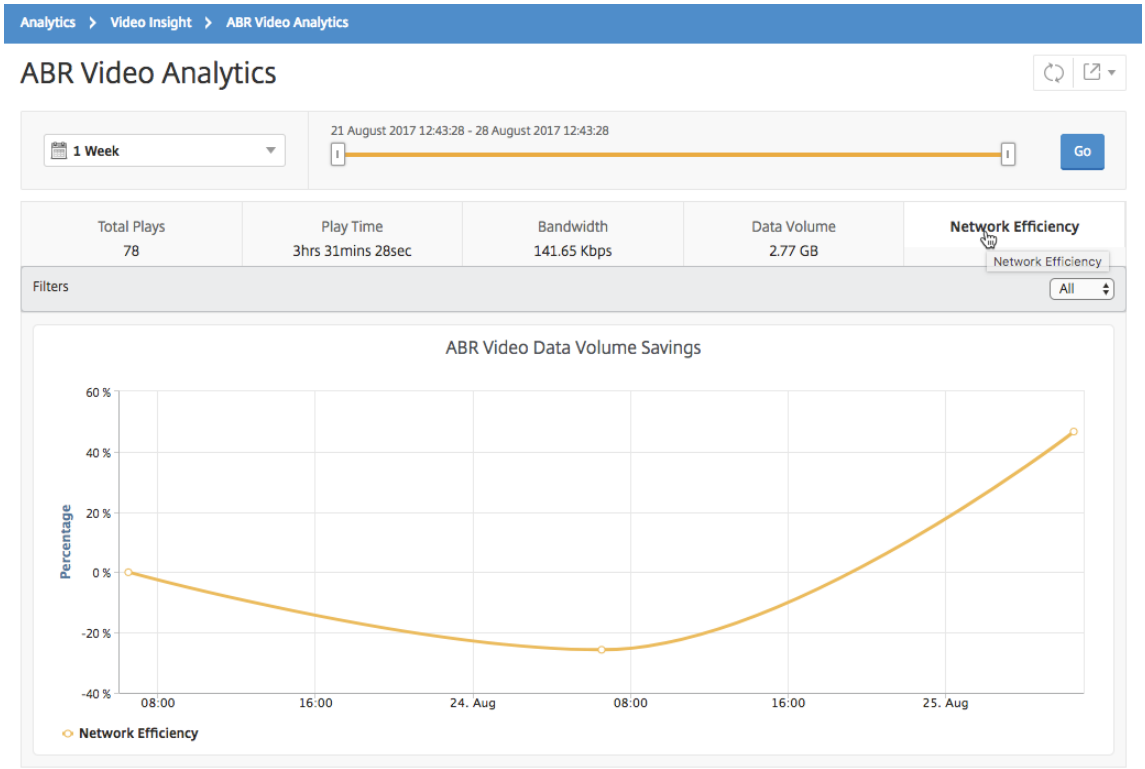
May 7, 2021

Citrix Application Delivery Management（ADM）は、特定の期間において、その期間における最適化されたビデオセッションと最適化されていないビデオセッションの比率を示すグラフを提供します。グラフには、最適化により削減された帯域幅の割合も表示されます。削減された帯域幅の割合は、次の式により計算されます。

保存帯域幅の割合 = 最適化された **ABR** ビデオデータボリュームの平均/最適化されていない **ABR** ビデオデータボリュームの平均。

最適化によって節約された帯域幅の割合を確認するには、次の手順を実行します。

1. [**Analytics] > [Video Insight**] に移動し、[**ABR Video**] をクリックします。
2. 右側のペインで、リストから時間枠を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。
3. [**Go**] をクリックし、[ネットワーク効率] タブを選択します。



最適化された **ABR** ビデオと最適化されていない **ABR** ビデオで使用されるデータ量を比較する

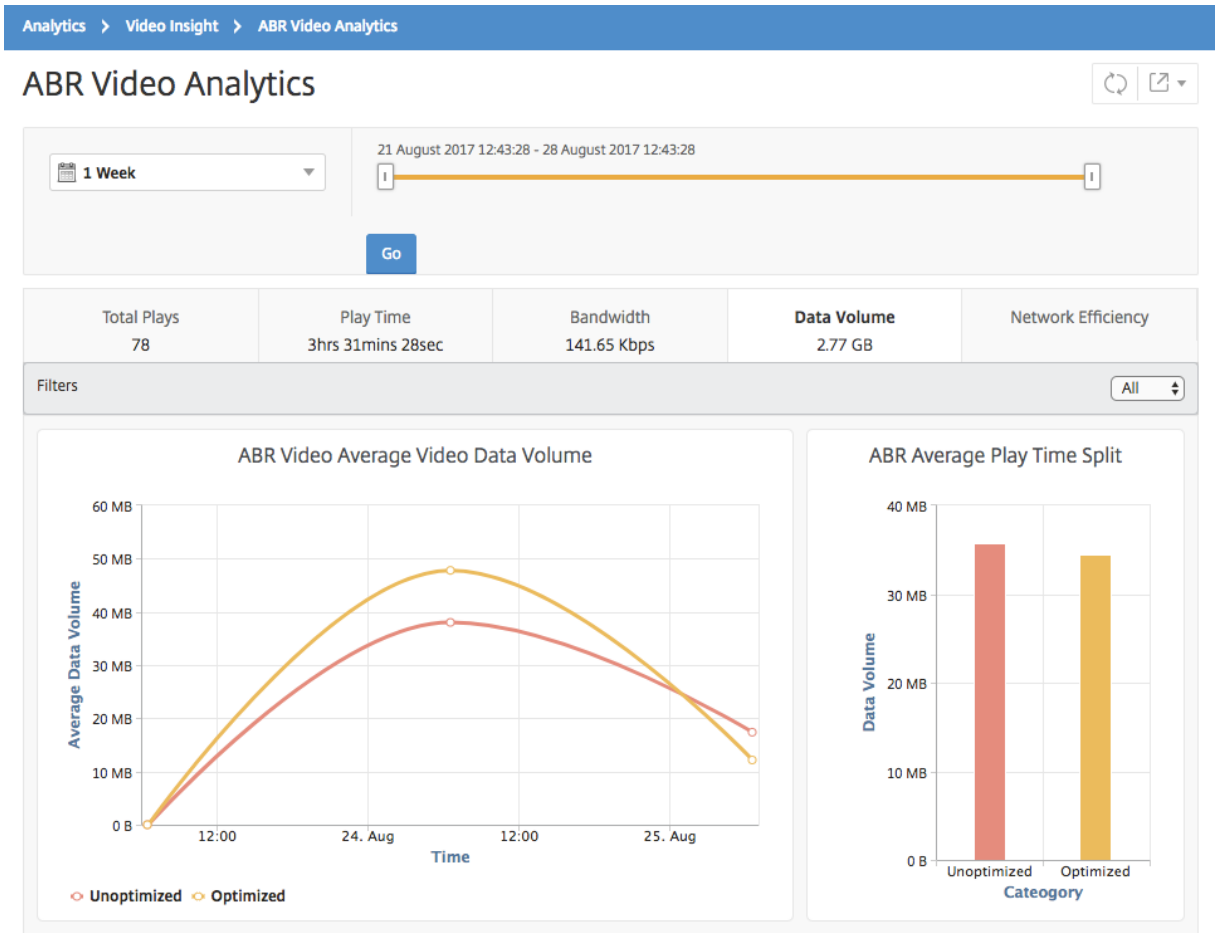
May 7, 2021

Citrix Application Delivery Management（ADM）では、最適化された ABR ビデオと最適化されていない ABR ビデオで使用されるデータ量が表示され、2 つのボリュームを比較できます。

ABR ビデオで使用されるデータ量を確認するには、次の操作を行います。

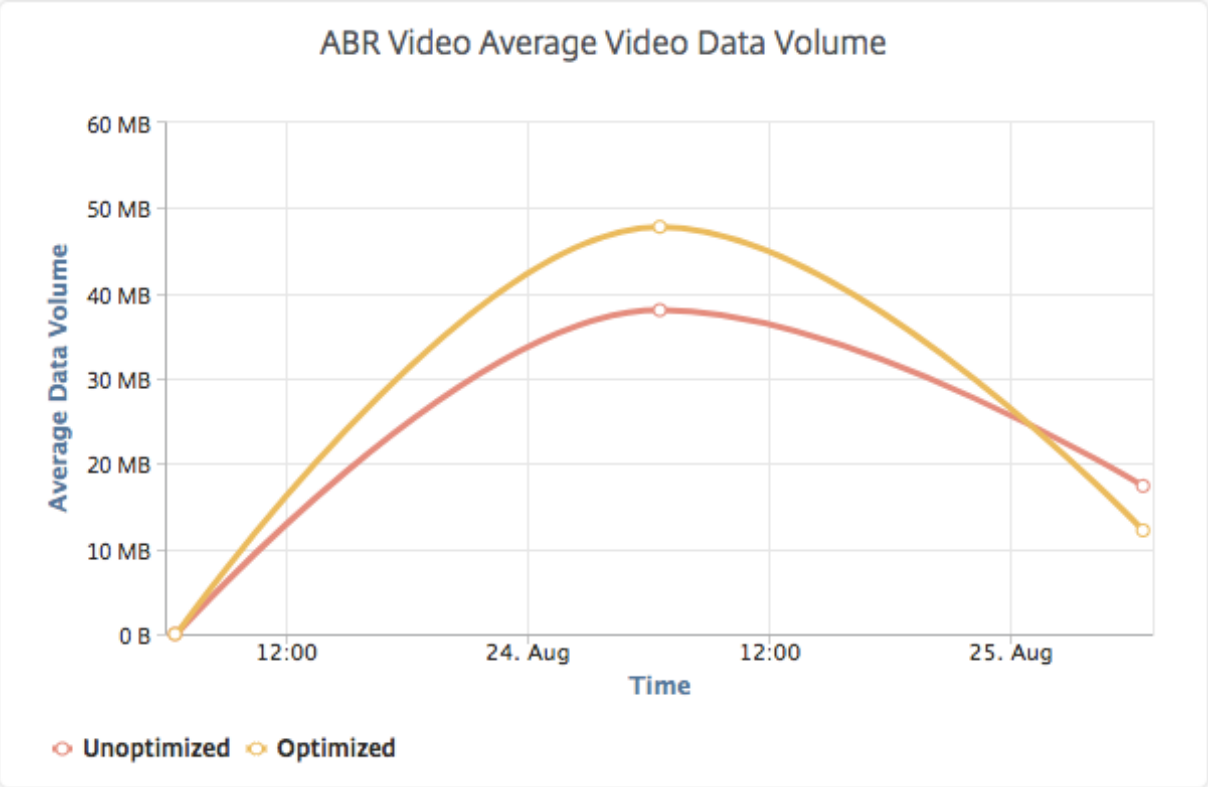
1. [**Analytics] > [Video Insight**] に移動し、[**ABR Video**] をクリックします。
2. 右側のペインで、リストから時間枠を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。
3. 「実行」をクリックし、「データボリューム」タブを選択します。

[フィルタ] リストを使用して、HTTP、HTTPS、または QUIC ABR ビデオを選択できます。



[**Data Volume**] タブには、ABR ビデオで使用される平均データ量、および選択した時間枠におけるネットワークからの最適化および最適化されていない ABR ビデオによって消費されるデータ量を示す折れ線グラフと円グラフが

表示されます。マウスポインタ ― を折れ線グラフに重ねると、特定の期間に使用された平均データボリュームを確認できます。



ストリーミングされる動画の種類とネットワークから消費されるデータ量の表示

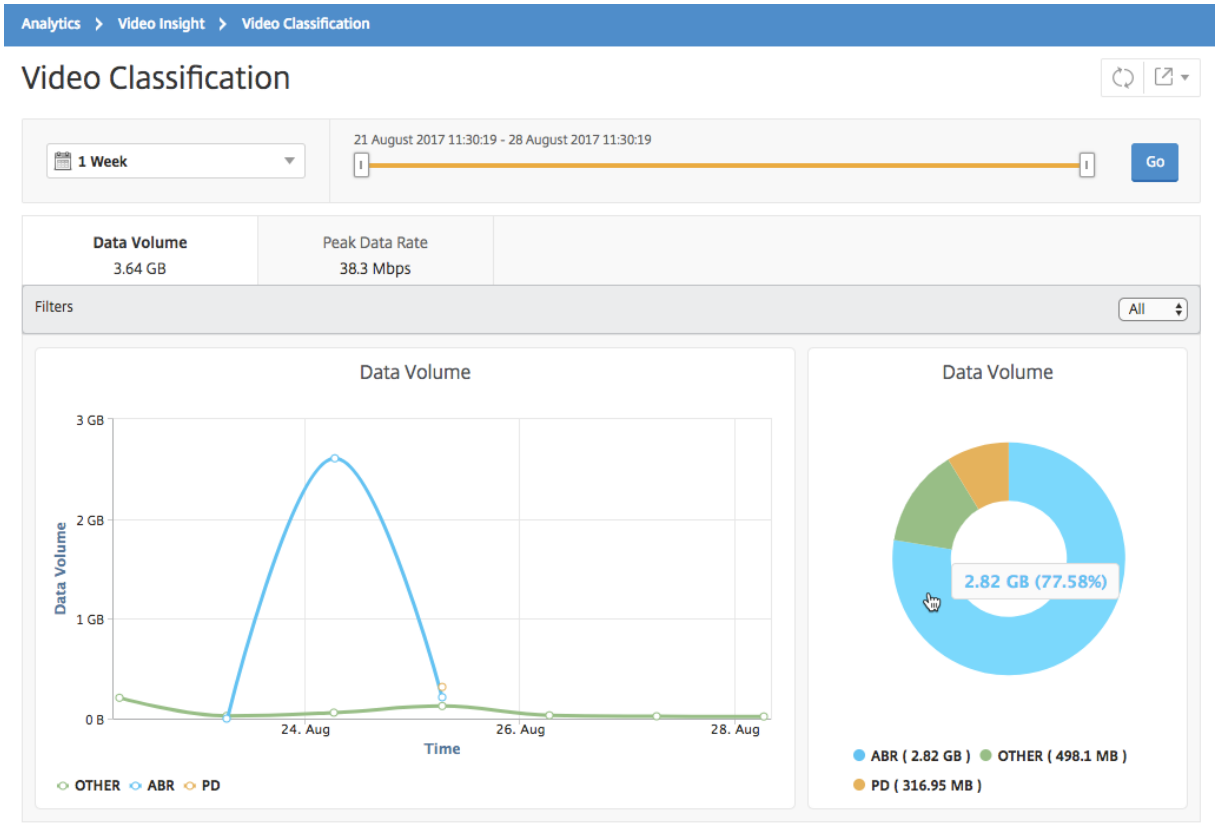
May 7, 2021

Citrix ADC アプライアンスは、ネットワーク内の暗号化または暗号化されていないビデオトラフィックと、ビデオストリーミングの種類（PD または ABR）を検出します。Citrix Application Delivery Management（ADM）では、これらのメトリックと、定義された期間内にビデオトラフィックによって消費されるデータ量が表示されます。

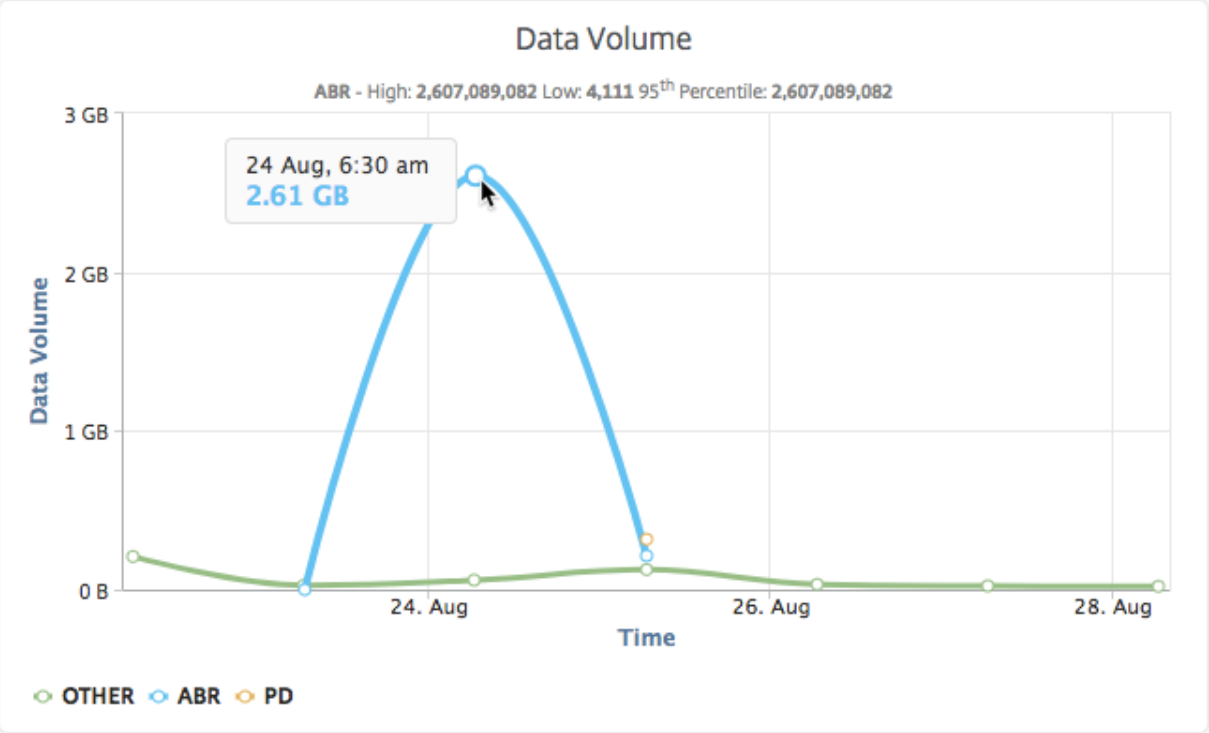
ビデオの種類と消費されたデータ量を表示するには：

1. [**Analytics] > [Video Insight**] に移動し、[**Video Classification**] をクリックします。
2. 右側のペインで、リストから時間枠を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。
3. [**Go**] をクリックします。

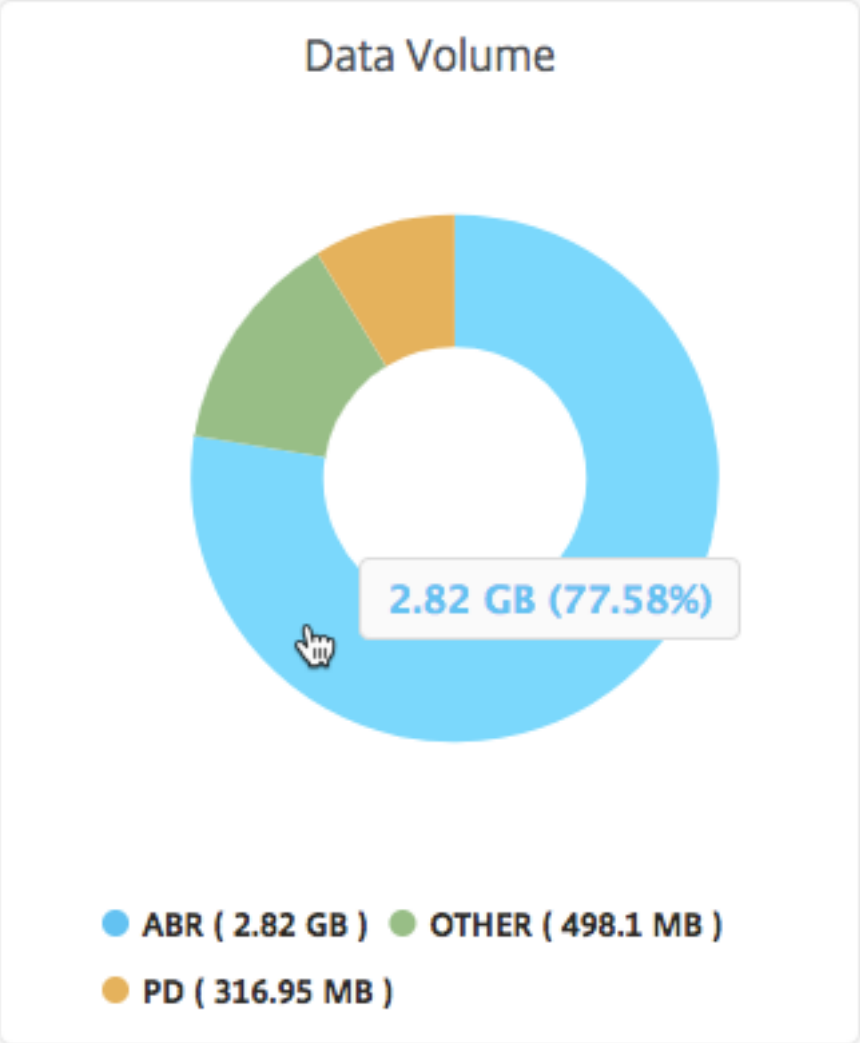
[フィルタ] リストを使用して、HTTP、HTTPS、または QUIC トラフィックを選択できます。



[**Data Volume**] タブには、ネットワークからストリーミングされるビデオトラフィックの種類と、ネットワークによって消費されるデータ量を示す折れ線グラフと円グラフが表示されます。マウスポインタ ― を折れ線グラフに重ねると、特定の期間に使用されたデータを確認できます。



また、円グラフにマウスポインタを置くと、特定の種類のビデオトラフィックで消費されたデータボリュームの割合を確認できます。



ABR ビデオの最適化と非最適化の再生時間を比較する

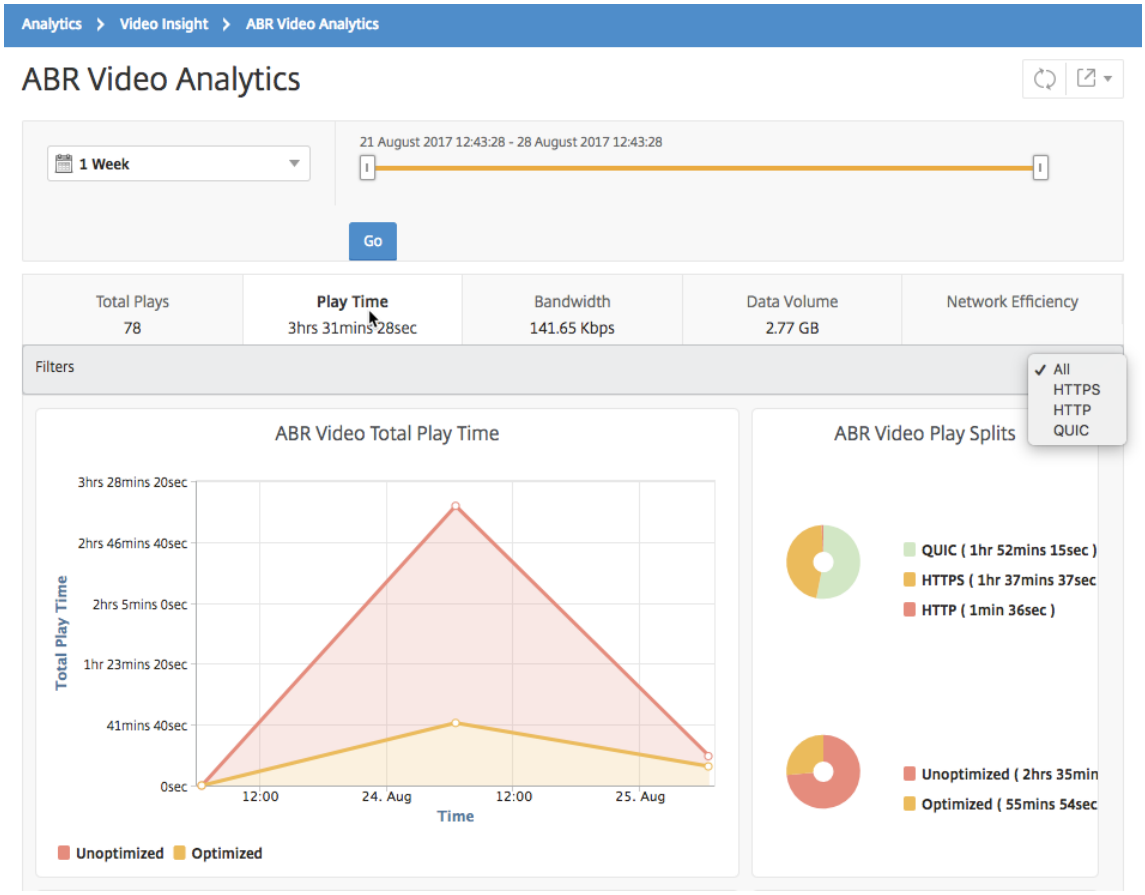
May 7, 2021

Citrix Application Delivery Management（ADM）は、特定の期間において、ABR ビデオの再生時間を提供し、ネットワーク内の最適化された ABR ビデオと最適化されていない ABR ビデオの再生時間を比較することもできます。

再生時間を表示するには:

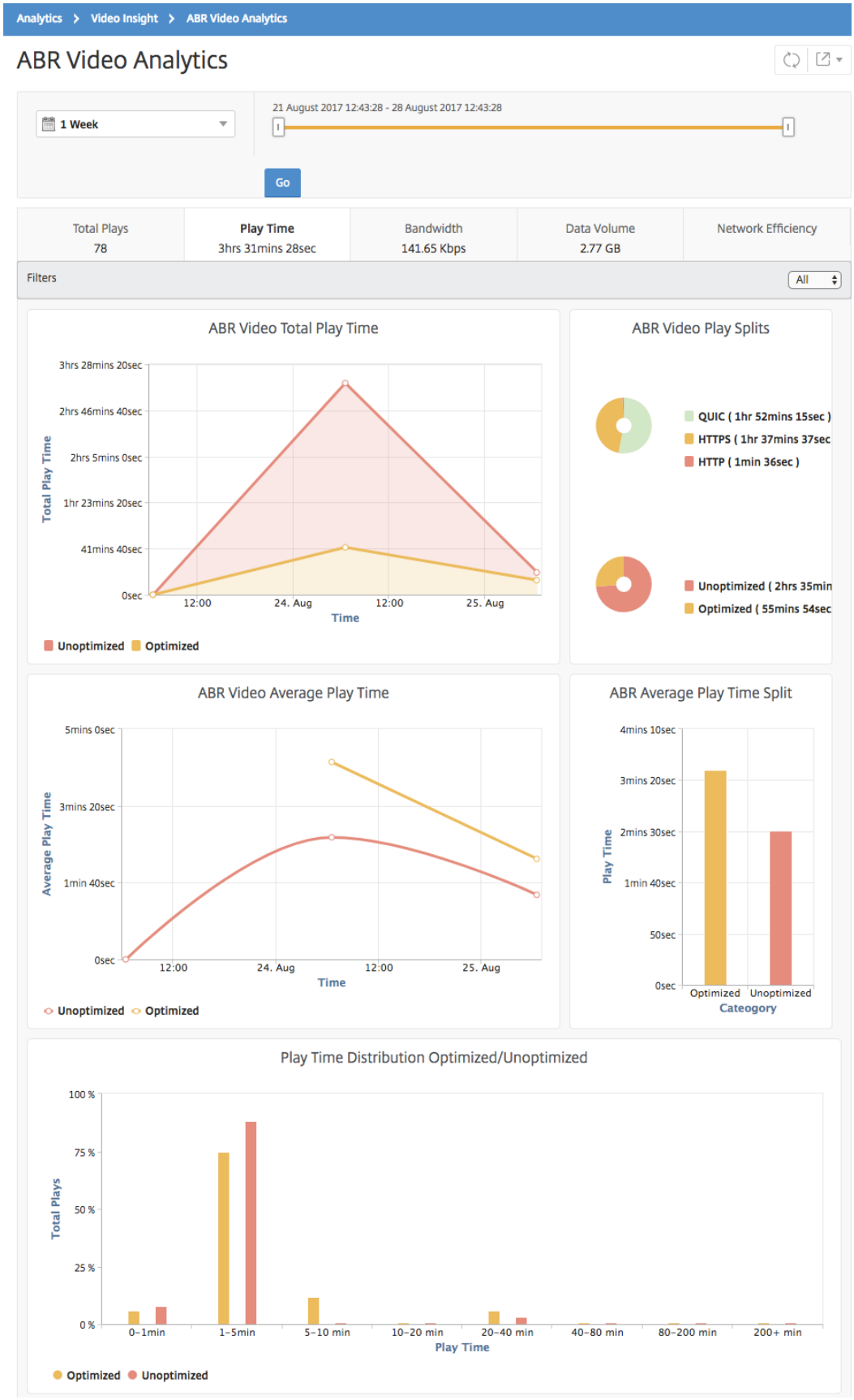
1. [**Analytics] > [Video Insight**] に移動し、[**ABR Video**] をクリックします。
2. 右側のペインで、リストから時間枠を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。
3. [移動] をクリックし、[再生時間] タブを選択します。

   [フィルタ] リストを使用して、HTTP、HTTPS、または QUIC ABR ビデオを選択できます。



選択した時間枠の [**Play Time**] タブには、次の内容を示す折れ線グラフと円グラフが表示されます。

- ネットワークからの ABR ビデオの再生時間の合計
- 選択した時間枠での、ネットワークからの ABR ビデオの最適化および非最適化再生の合計再生時間
- 暗号化および暗号化されていない ABR 動画の総再生時間
- ABR ビデオの平均再生時間
- ABR ビデオの最適化および非最適化された再生の、平均再生時間
- 暗号化および暗号化解除された ABR ビデオの平均再生時間
- 最適化および非最適化された ABR ビデオ間の再生時間の分布



最適化された **ABR** ビデオと最適化されていない **ABR** ビデオの帯域幅消費の比較

May 7, 2021

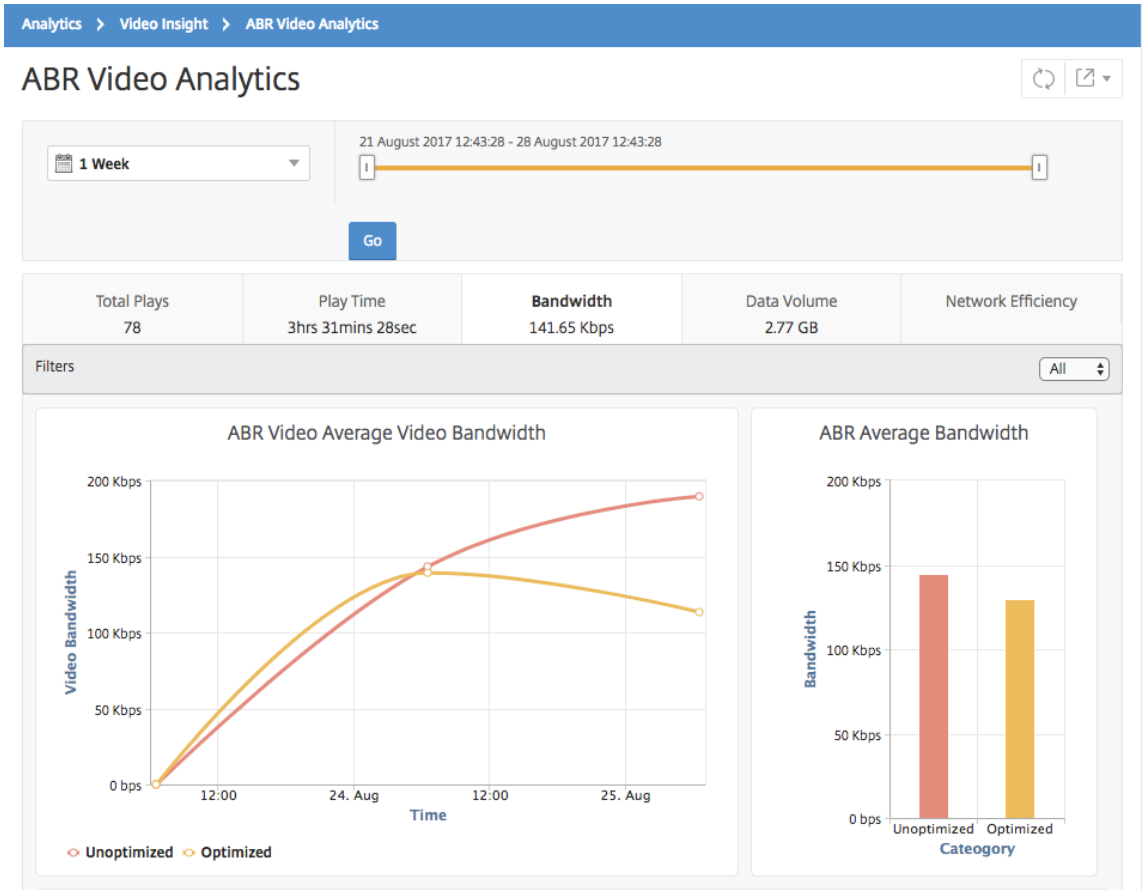
Citrix Application Delivery Management（ADM）は、特定の時間枠において、ABR ビデオの最適化および非最適化によって消費される帯域幅を提供します。また、ネットワーク内で最適化された ABR ビデオと最適化されていない ABR ビデオによって消費される帯域幅を、以下に基づいて比較することもできます。

- 再生時間
- データ量

帯域幅の消費量を表示するには、次の手順を実行します。

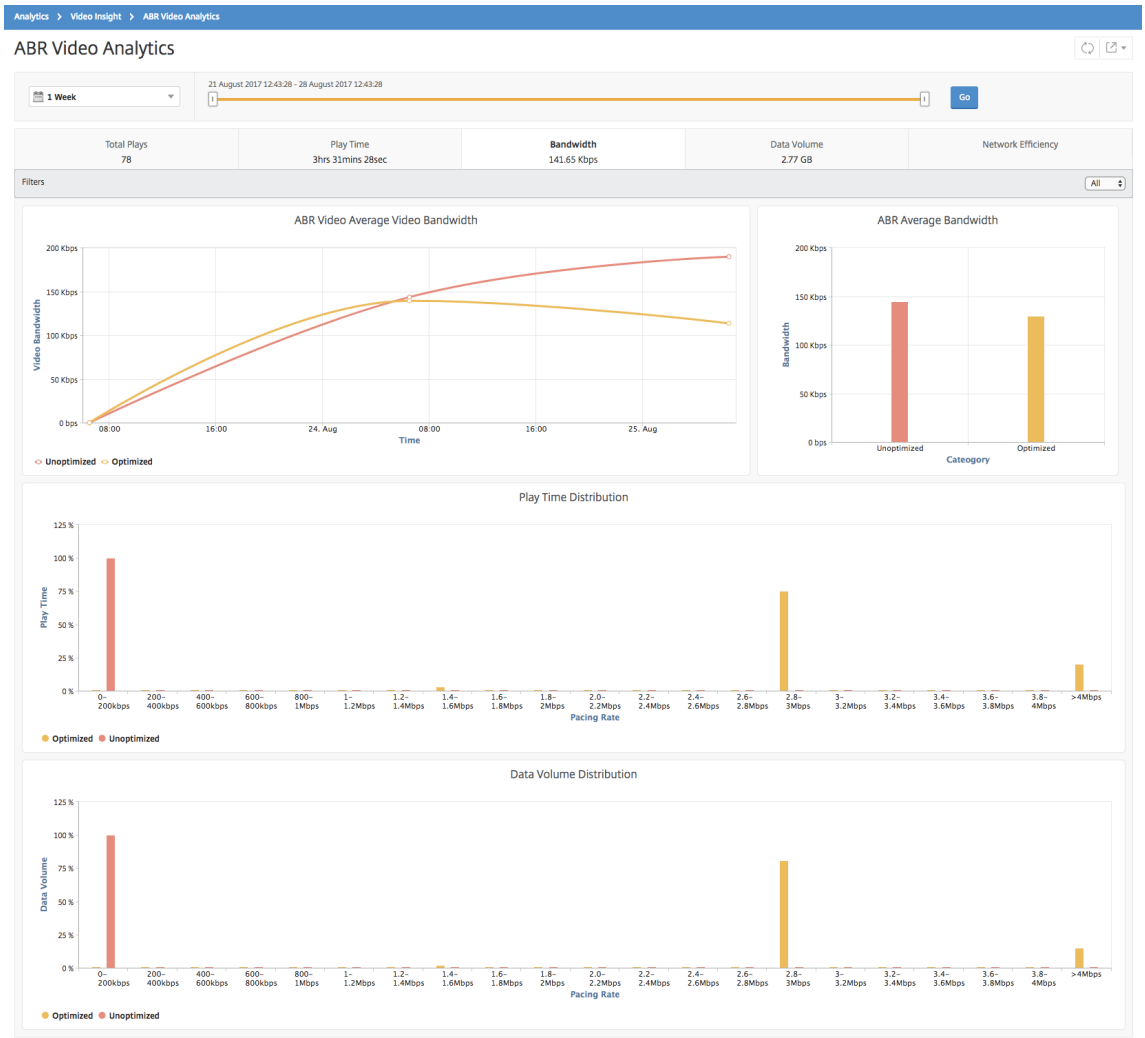
1. [**Analytics] > [Video Insight**] に移動し、[**ABR Video Analytics**] をクリックします。
2. 右側のペインで、リストから時間枠を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。
3. [移動] をクリックし、[帯域幅] タブを選択します。

   [フィルタ] リストを使用して、HTTP、HTTPS、または QUIC ABR ビデオを選択できます。



選択した時間枠の [帯域幅] タブには、次の内容を示す折れ線グラフと円グラフが表示されます。

- 最適化および非最適化された ABR ビデオによって消費された平均帯域幅。
- 最適化および非最適化された ABR ビデオ間の再生時間の分布に基づく、帯域幅消費。
- 最適化および非最適化された ABR ビデオ間のデータボリュームの分布に基づく、帯域幅消費。



ABR ビデオの再生の最適化数と非最適化数を比較する

May 7, 2021

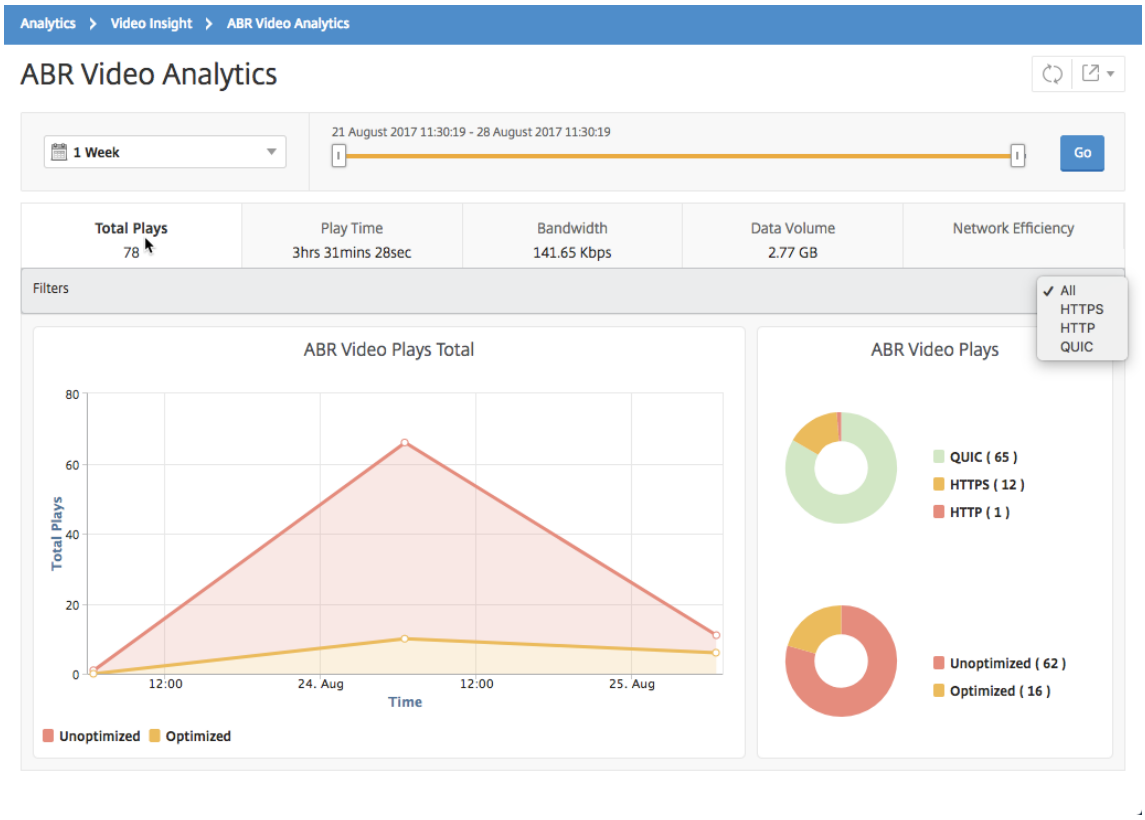
特定の期間において、Citrix Application Delivery Management（ADM）は ABR ビデオの再生数を表示し、ネットワーク内の最適化された再生数と最適化されていない再生数を比較できます。

再生数を表示するには:

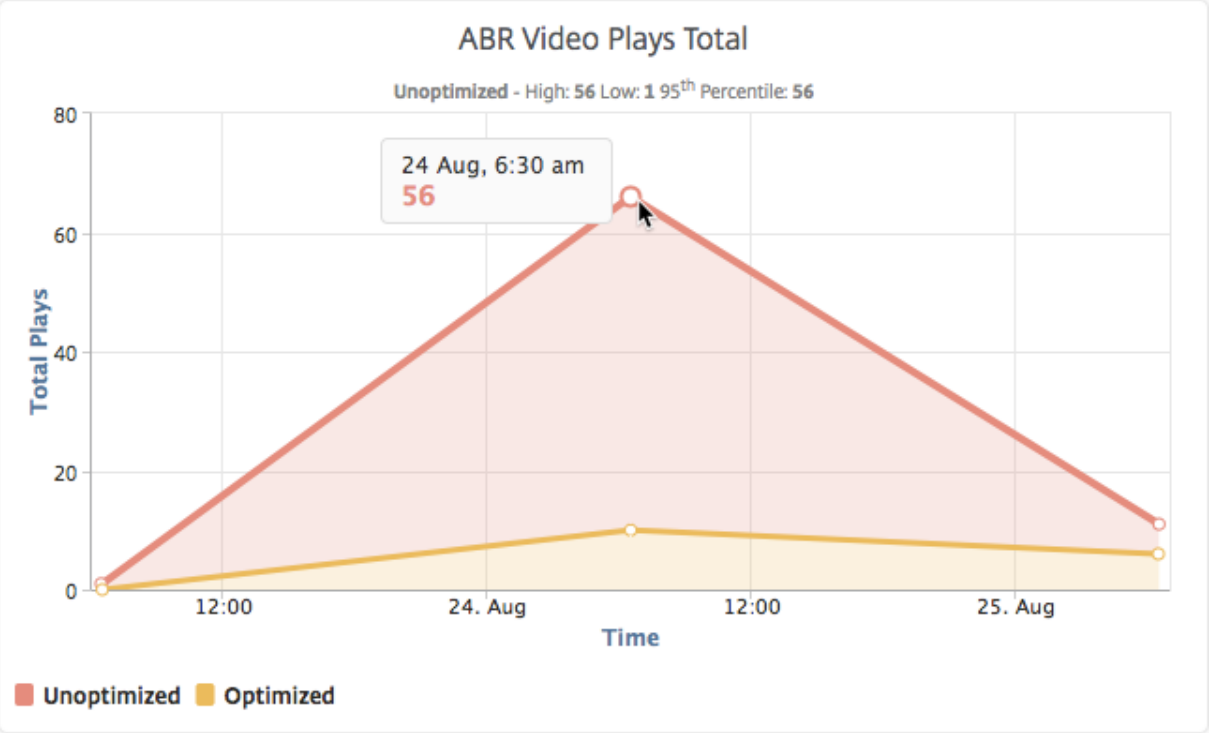
1. [**Analytics] > [Video Insight**] に移動し、[**ABR Video Analytics**] をクリックします。

2. 右側のペインで、リストから時間枠を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。
3. [移動] をクリックし、[再生数] タブを選択します。

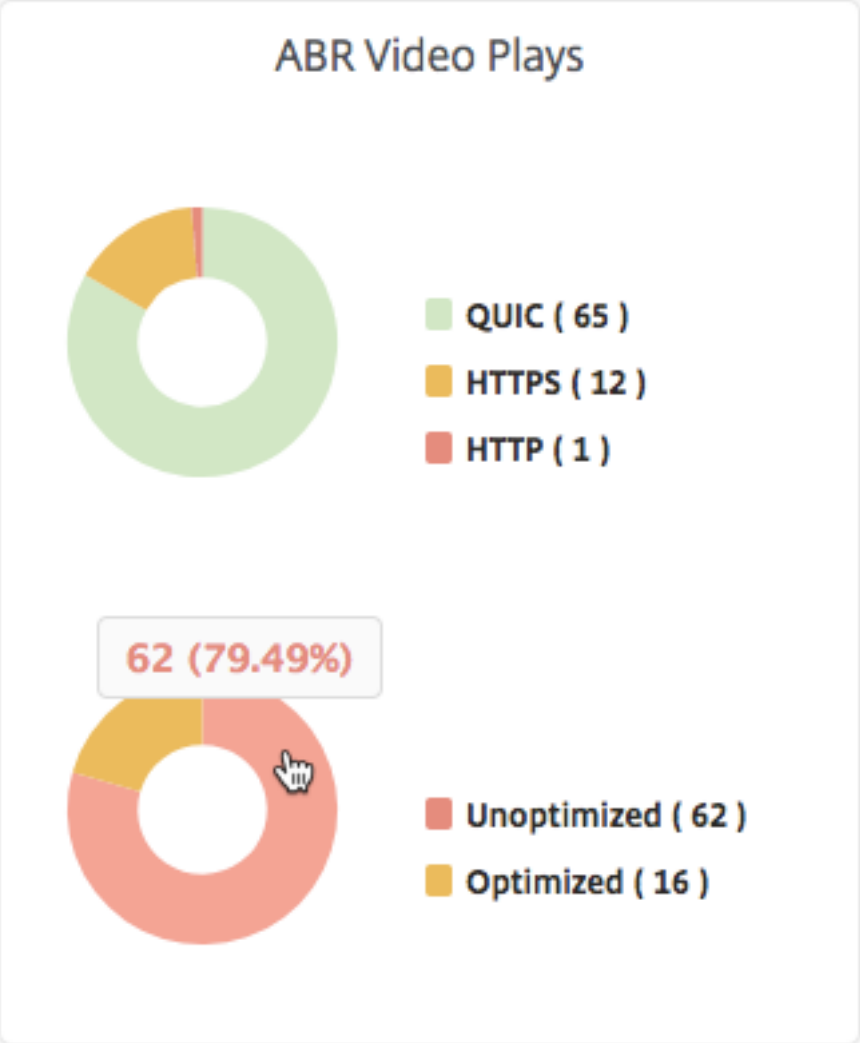
   [フィルタ] リストを使用して、HTTP、HTTPS、または QUIC ABR ビデオを選択できます。



[再生数] タブには、ネットワークからの ABR ビデオの再生数、および選択した時間枠における ABR ビデオの最適化および非最適化再生数を示す折れ線グラフと円グラフが表示されます。マウスポインタ — を折れ線グラフに重ねると、特定の期間の再生回数を確認できます。



また、マウスポインターを円グラフに重ねると、選択した期間に最適化および非最適化された再生の割合と、暗号化および暗号化解除された ABR ビデオの割合を確認できます。



特定の時間枠のピークデータレートを表示する

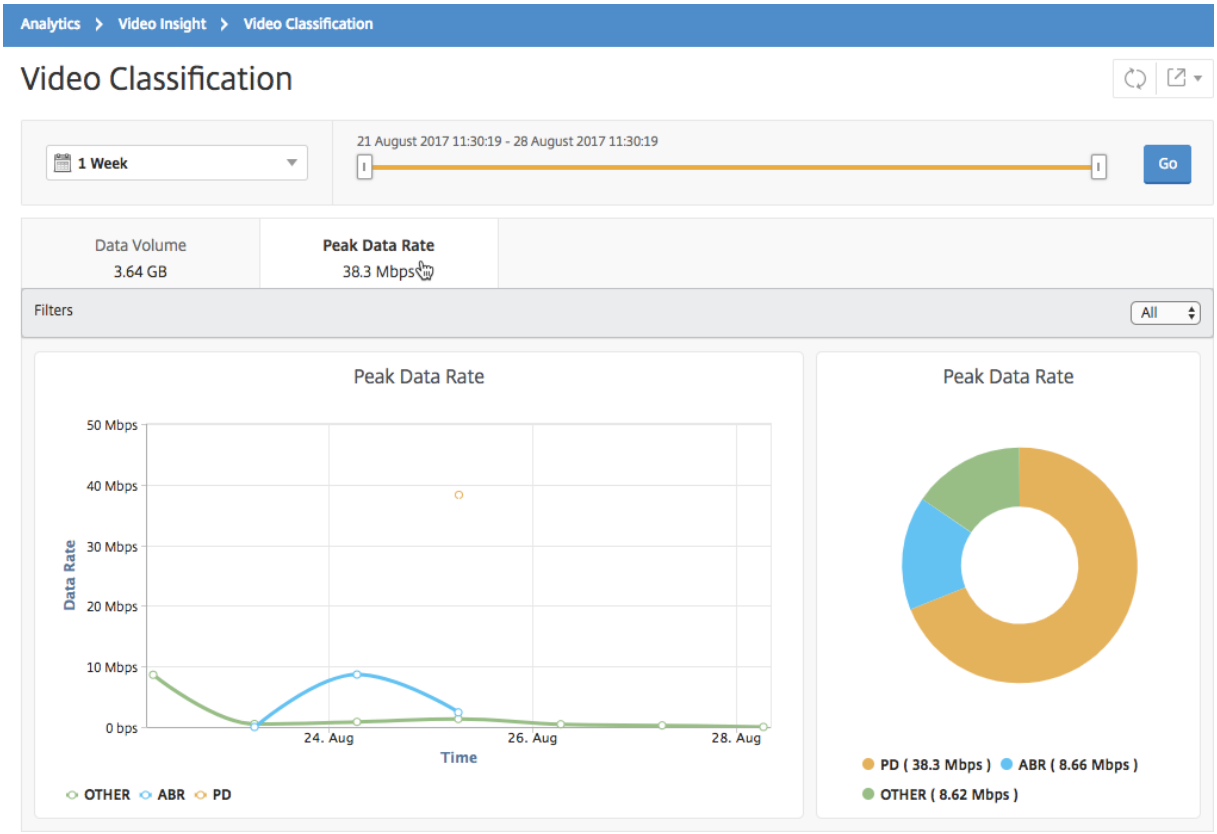
May 7, 2021

Citrix Application Delivery Management（ADM）では、ネットワーク内のビデオトラフィックのピークスループットまたはデータレートが表示されます。

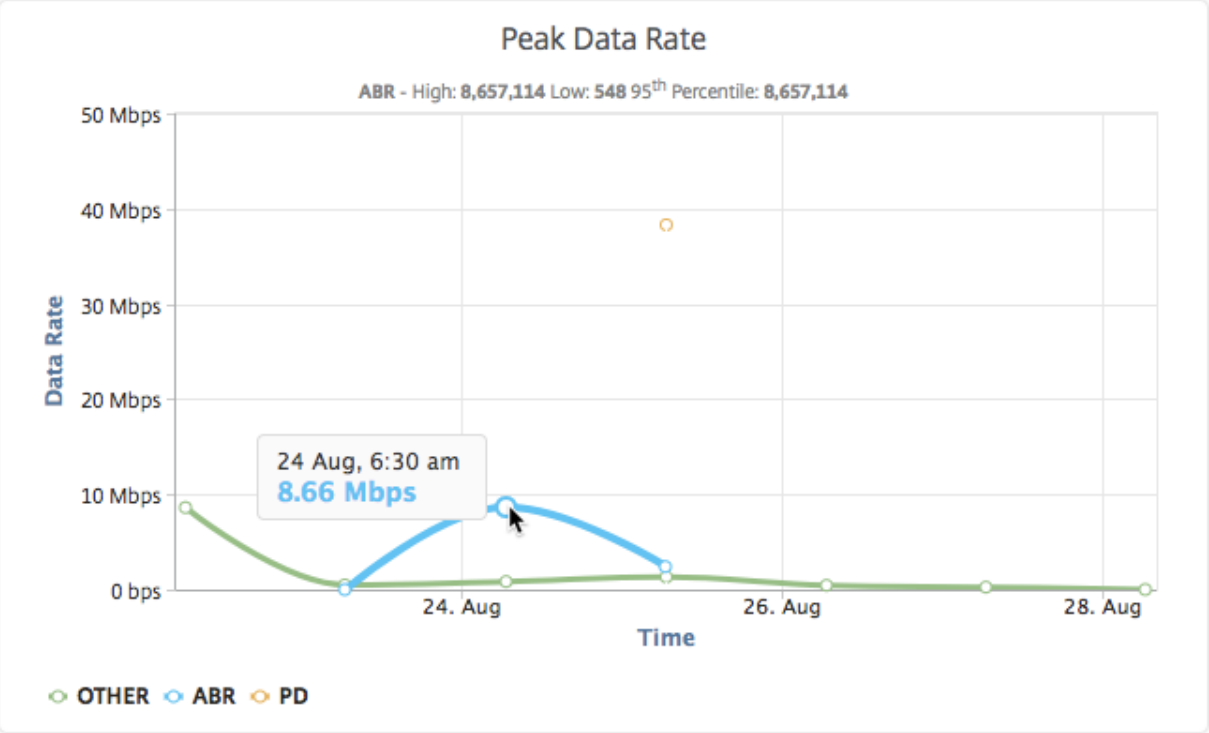
ビデオトラフィックのピークデータレートを確認するには：

1. [**Analytics] > [Video Insight**] に移動し、[**Video Classification**] をクリックします。
2. 右側のペインで、リストから時間枠を選択します。期間は、スライダーを使用してより詳細にカスタマイズできます。
3. 「進む」をクリックし、「ピークデータレート」タブを選択します。

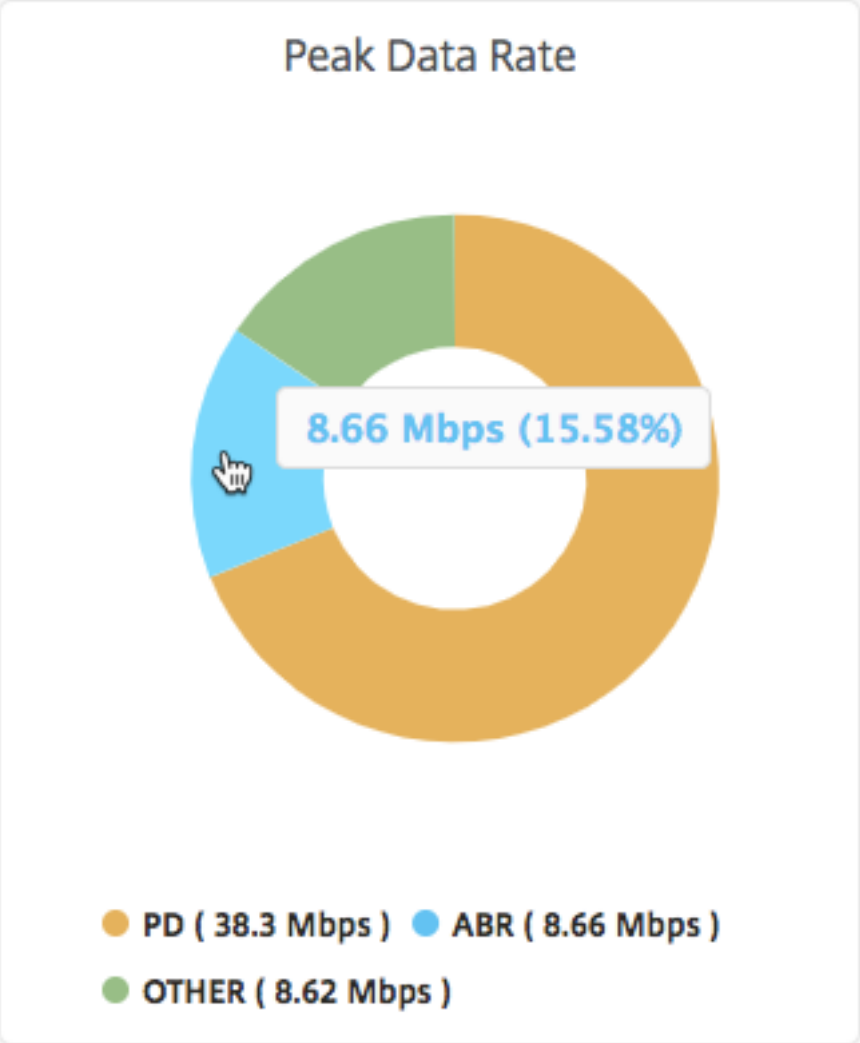
[フィルタ] リストを使用して、HTTP、HTTPS、または QUIC トラフィックを選択できます。



[**Peak Data Rate**] タブには、ネットワークからストリーミングされるビデオトラフィックのタイプのピークデータレートと、選択した時間枠におけるネットワーク上のビデオトラフィックのピークデータレートを示す折れ線グラフと円グラフが表示されます。マウスポインタ ― を折れ線グラフに重ねると、特定の期間における最大データレートを確認できます。



また、円グラフにマウスポインターを重ねると、選択した期間に特定の種類の動画トラフィックで消費された最大データレートの割合を確認できます。



SSL フォワードプロキシ分析

May 7, 2021

企業ネットワークのエッジにある Citrix ADC アプライアンスは、インターネットプロキシとして機能します。このアプライアンスは透過プロキシモードまたは明示的プロキシモードで動作し、HTTPS を含むインターネットトラフィックの傍受を制御できるようにします。任意の要求を傍受するか、バイパスするか、禁止するかの決定は、アプライアンスに設定されたポリシーに基づいて行われます。ユーザーは社内ネットワークにログオンする前に認証されます。すべての要求と応答はユーザーにタグ付けされ、ユーザーのアクティビティはアプライアンスで記録されます。詳しくは、「Citrix の SSL 転送プロキシ」を参照してください。

Citrix Application Delivery Management（ADM）を Citrix ADC アプライアンスに統合すると、ログストリームを使用してアプライアンス上のログユーザーアクティビティと後続のレコードが **Citrix**ADM にエクスポートされます。Citrix ADM は、訪問した Web サイトや消費された帯域幅など、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。また、帯域幅の使用量と検出された脅威（マルウェアやフィッシングサイトなど）をレポートします。これらの主要なメトリックを使用して、ネットワークを監視し、Citrix ADC アプライアンスで修正措置を講じることができます。

Citrix ADC アプライアンスと **Citrix ADM** を統合するには：

1. Citrix ADC アプライアンスで、SSL 転送プロキシを構成するときに、**Analytics** を有効にして、分析に使用する Citrix ADM インスタンスの詳細を入力します。
2. Citrix ADM で、Citrix ADC アプライアンスをインスタンスとして Citrix ADM に追加します。詳しくは、「Citrix ADM へのインスタンスの追加」を参照してください。

ダッシュボード

May 7, 2021

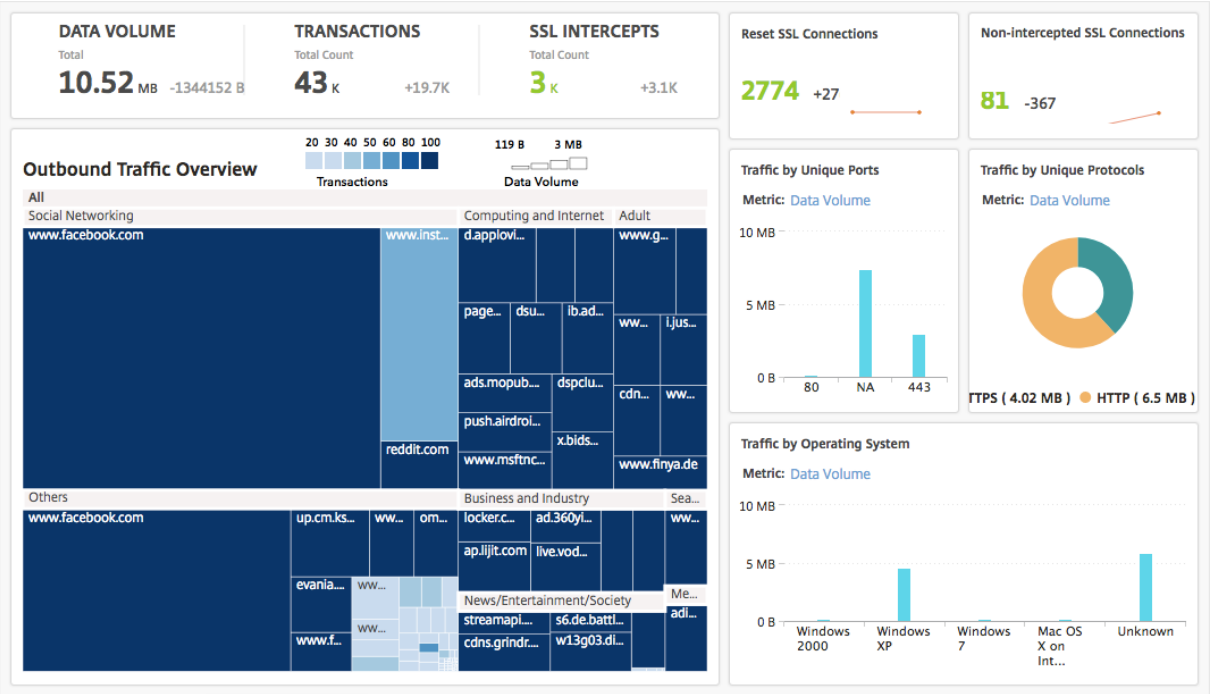
Citrix Application Delivery Management（ADM）には、送信トラフィックダッシュボードとユーザーダッシュボードの **2** つのダッシュボードがあります。これらのダッシュボードには、組織内ネットワークからアクセスされた Web サイトとアプリケーション、およびネットワーク内のユーザーが実行したアクティビティの概要を示す複数のグラフが表示されます。

アウトバウンドトラフィックダッシュボード

アウトバウンドトラフィックダッシュボードには、ネットワークからアクセスされた URL またはドメインの概要が表示されます。このダッシュボードでは、URL またはドメインで使用されたトランザクション数別またはデータボリューム別に URL とドメインの全体像を確認できます。
また、以下の詳細も表示されます。

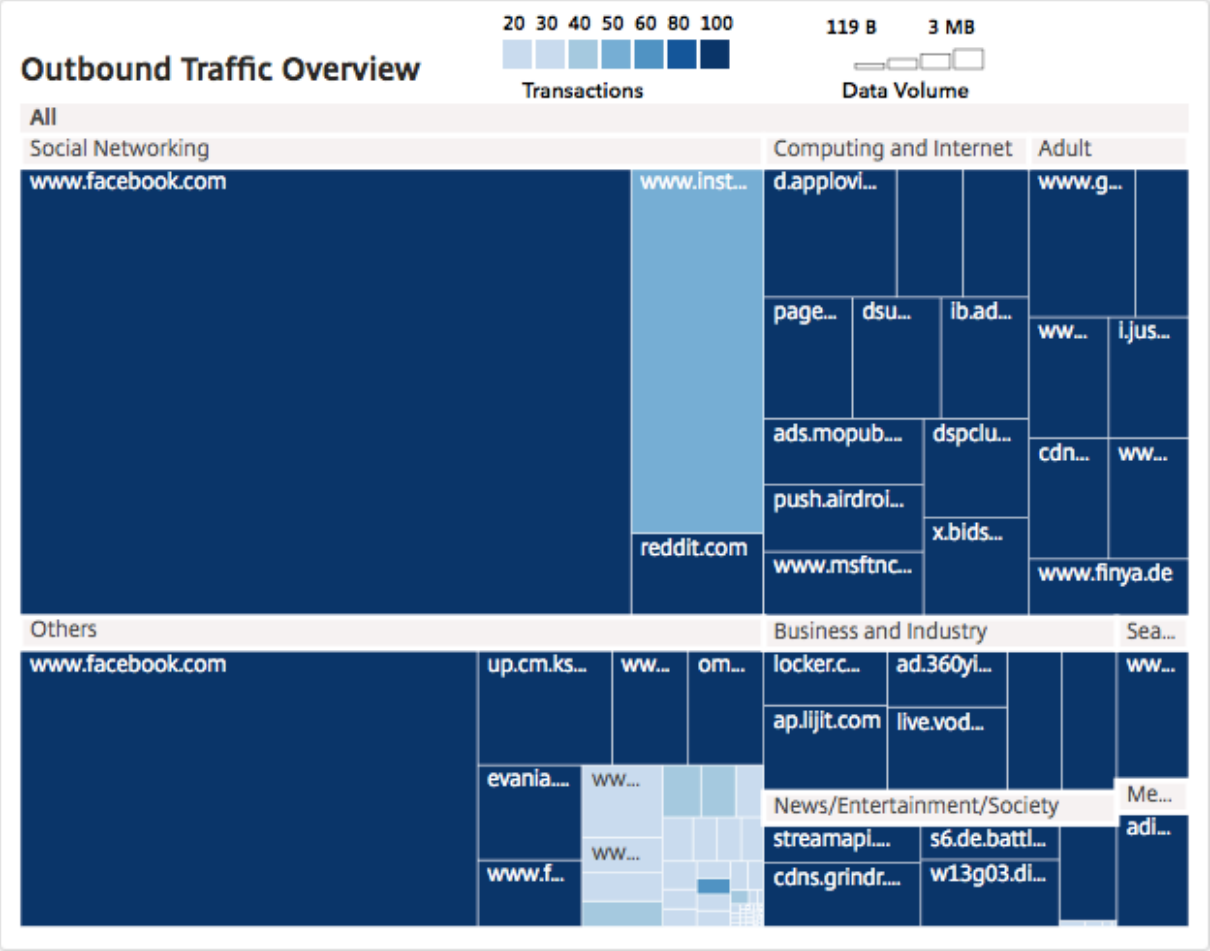
1. ネットワークからアクセスされた URL またはドメインで使用された帯域幅の量
2. ネットワークから URL およびドメインへのアクセス中に発生したトランザクション数
3. トランザクション中に Citrix ADC アプライアンスが傍受した SSL 接続の数。
4. トランザクション中に Citrix ADC アプライアンスによって傍受されなかった SSL 接続の数。
5. トランザクション中に Citrix ADC アプライアンスによってリセットされた SSL 接続の数。
6. トラフィックの送信に使用されたポート、Web トラフィックにより使用されたプロトコル、およびトラフィックの送信に使用されたクライアントオペレーティングシステムごとの Web トラフィックの送信量

アウトバウンドトラフィックダッシュボードにアクセスするには、「アプリケーション」**>**「アウトバウンドトラフィックダッシュボード」に移動します。



ネットワークからのアウトバウンドトラフィックを表示する

アウトバウンドトラフィックダッシュボードには、アウトバウンドトラフィックの概要ペインがあります。Citrix ADM アウトバウンドトラフィックの概要］ペインでは、アクセスした URL またはドメインが、ショッピング、ニュース、ソーシャルネットワーキングなどのカテゴリにグループ化されます。[**Outbound Traffic Overview**] ペインには、ネットワークからアクセスされた URL またはドメインが URL カテゴリのノードとして表示されます。ノードのサイズは、URL またはドメインへのアクセスで使用されたデータボリュームに応じて決まります。ノードの色は、URL またはドメインへのアクセス中に発生したトランザクションの回数を示しています。



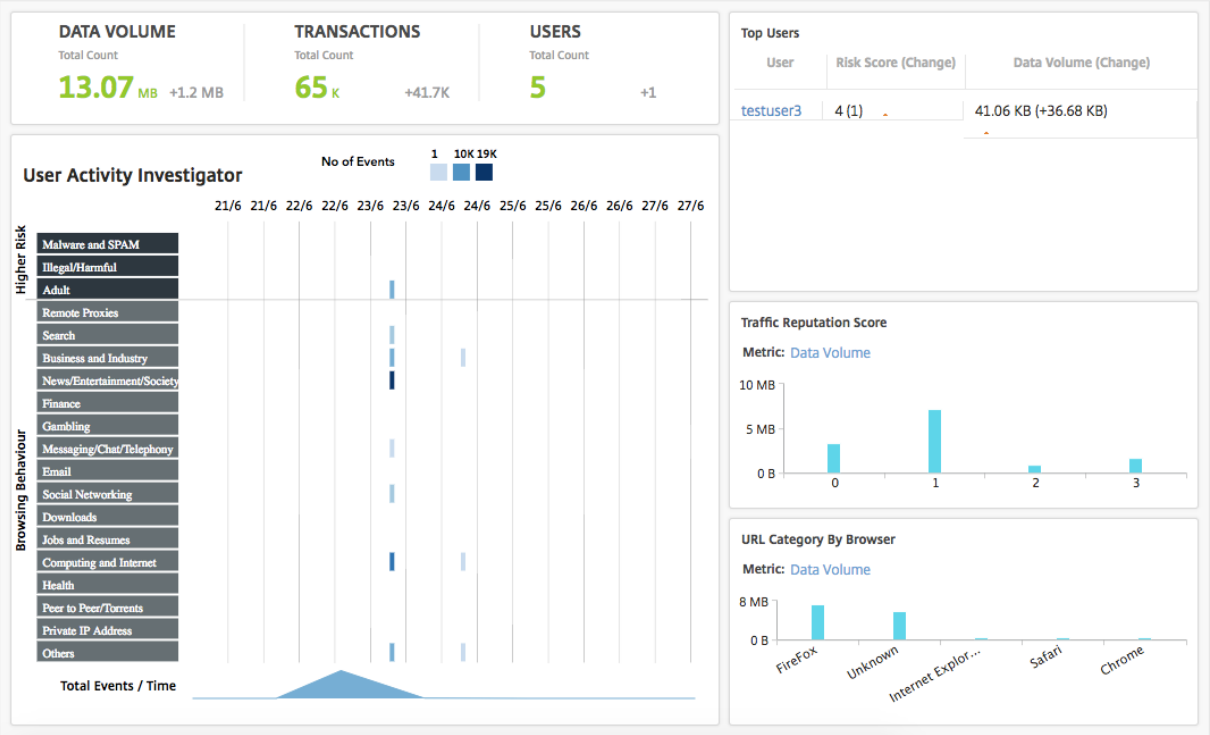
カテゴリをクリックすると、チャートをフィルタリングして、指定した時間枠のカテゴリに関連する詳細を表示できます。

ユーザーダッシュボード

ユーザー・ダッシュボードには、企業内のユーザーが実行したアクティビティの概要が表示されます。このダッシュボードにはキーメトリックが用意されており、これらを使用して以下を確認することができます。

1. 社内ユーザーのブラウジング行動
2. 社内ユーザーがアクセスした URL カテゴリ。
3. リスクスコアおよび使用帯域幅量に基づく上位 5 名のユーザー。リスクスコアについて詳しくは、「リスクスコア」を参照してください。
4. URL またはドメインへのアクセスに使用された Web ブラウザー。
5. トラフィックレピュテーションスコアに基づく、ユーザーにより生成された Web トラフィックの量

ユーザーダッシュボードにアクセスするには、「ユーザー」**>**「ダッシュボード」に移動します。

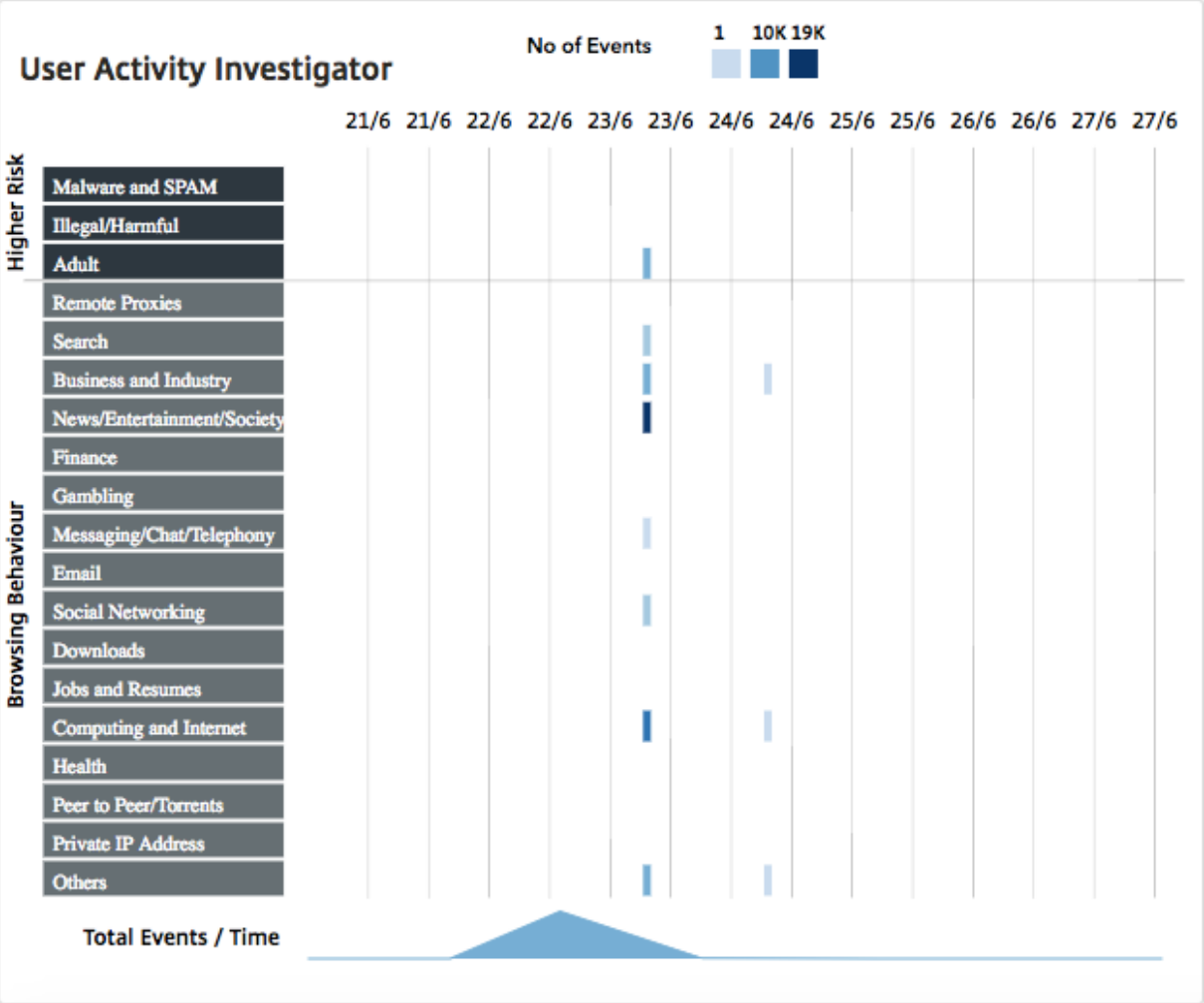


[**Top Users**] ペインでユーザーをクリックすると、グラフをフィルタリングして、指定した時間枠内でユーザーが実行した Web アクティビティの詳細を表示できます。

ユーザー活動調査員

ユーザーダッシュボードには、ユーザーによって実行されたさまざまな **Web** アクティビティを表示する「ユーザーアクティビティ調査」ペインがあります。このペインには、選択した時間内にユーザーがアクセスした URL カテゴリーと、URL カテゴリーごとの実行された各種イベントが表示されます。イベントをクリックすると、トランザクションレベルの詳細が表示されます。

User Activity Investigator は、URL カテゴリごとに、ユーザーの閲覧行動、ユーザーによるリスクの高いアクティビティ、トリガーされたイベントなどの重要な情報を表示します。イベントは、グラフ上に長方形の凡例として表示されます。凡例はそれぞれ、選択した期間が 1 時間の場合は 1 分間隔、選択した期間が 1 日の場合は 1 時間間隔で集計されます。



集計された凡例は、イベントの発生回数に応じて色分けされます。凡例にマウスポインターを重ねると、時間や選択した凡例について集計されたイベント数などの詳細が表示されます。期間リストから時間を選択することで、グラフの期間をカスタマイズできます。

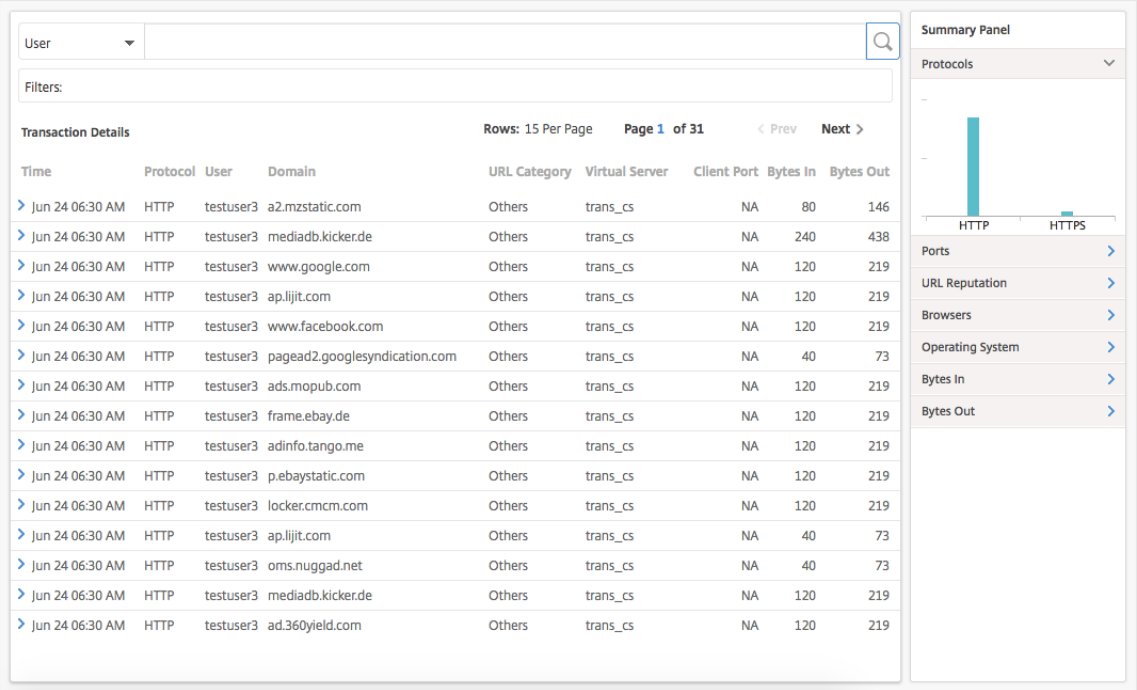
イベントをクリックすると、トランザクションの詳細をさらにドリルダウンできます。

ユーザートランザクション

[User Transactions] ペインには、ネットワーク内のユーザートランザクションの詳細が表示されます。このペインでは、以下のようなトランザクションレベルの詳細が示されます。

1. トランザクションの発生日時
2. トランザクションに使用されたプロトコル
3. ユーザー名
4. ユーザーがアクセスするドメイン
5. URL カテゴリー

6. トランザクションの傍受に使用されたプロキシサーバー
7. クライアントポートの詳細
8. 受信バイト数
9. 送信バイト数



Summary panel

[サマリー] パネルには、[トランザクションの 詳細] ペインに表示されるトランザクションのすべてのメトリックが表示されます。このパネルでは、メトリックを選択または選択解除して、[トランザクション詳細] ペインでトランザクションをソートおよび表示できます。サマリー・パネルには、次のメトリックが表示されます。

メトリック	説明
プロトコル	トランザクションで使用されたプロトコル
ポート	トランザクションで使用されたポート
URL レピュテーション	URL レピュテーションスコア
Web ブラウザー	トランザクションで使用された Web ブラウザー
オペレーティングシステム	トランザクションで使用されたオペレーティングシステム
受信バイト数	Citrix ADC アプライアンスを介して受信したデータの量。

メトリック	説明
送信バイト数	Citrix ADC アプライアンスを介して送信されたデータの量。

リスクスコア

リスクスコアは、Citrix ADM で企業内のユーザーに関連するリスクを判断するために使用するスコアリングシステムです。Citrix ADM は、ネットワーク上のユーザーがアクセスする URL に対して、Citrix ADC アプライアンスによって割り当てられた URL レピュテーションスコアに基づいて、リスクスコアを割り当てます。URL レピュテーションスコアについては、「URL レピュテーションスコア」を参照してください。次の表では、Citrix ADM によって割り当てられるリスクスコアについて説明します。

リスクスコア	説明
1	ユーザーの Web アクティビティについて脅威は認められず異常ではありません。
2	ユーザーのウェブアクティビティは脅威を認識していないか、異常ではありませんが、ユーザーは URL レピュテーションスコアがない「不明なサイト」にアクセスしています。
3	ユーザーの Web アクティビティに脅威は検出されていませんが、ユーザーは潜在的な危険性があるサイトにアクセスしようとしたか、こうしたサイトと関係しています。
4	ユーザーが侵害を受けた可能性があります。
5	ユーザーの Web アクティビティは異常であり、ユーザーは既知の悪意のあるサイトにアクセスしました。

使用例

May 7, 2021

SSL インターセプトの監視

Citrix ADC アプライアンスを使用すると、暗号化された送信トラフィックを検査できます。アプライアンスで設定されたポリシーに基づいて、HTTPS リクエストを代行受信、バイパス、またはブロックできます。Citrix Application

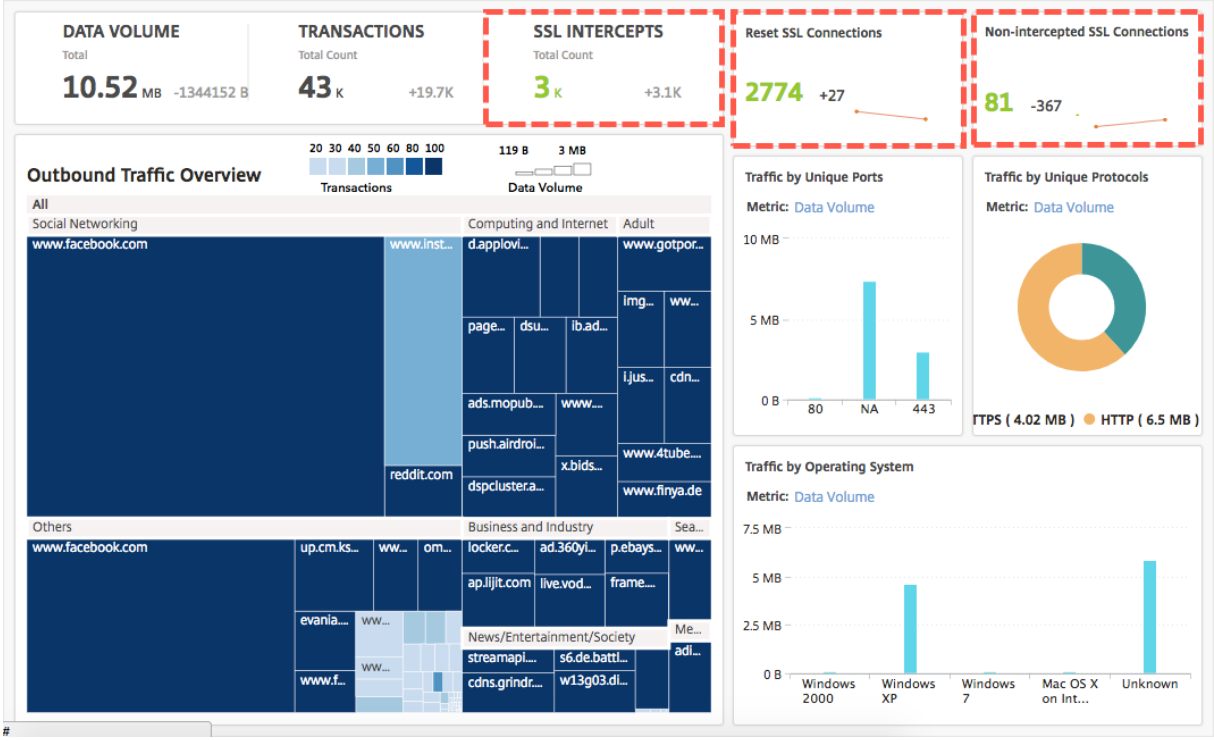
Delivery Management（ADM）では、選択した期間における 送信トラフィックダッシュボードの SSL 接続に関する次の詳細が提供されます。

- Citrix ADC アプライアンスによって傍受され、傍受されず、リセットされる SSL 接続の数
- SSL 接続のトランザクションの詳細

これらの詳細を使用して、Citrix ADC アプライアンスのポリシーをさらに微調整して、暗号化された送信トラフィックを効率的に検査できます。詳しくは、「Citrix の SSL 転送プロキシ」を参照してください。

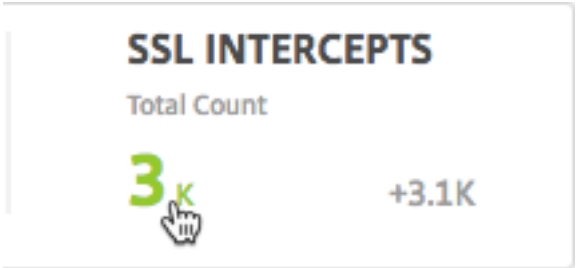
傍受された、傍受されていない、およびリセットされた **SSL** 接続の数を表示するには、以下を行います。

「アプリケーション」>「アウトバウンドトラフィックダッシュボード」に移動します。Outboard Traffic Dashboard には、傍受された、傍受されていない、リセットされた SSL 接続の数が表示されます。

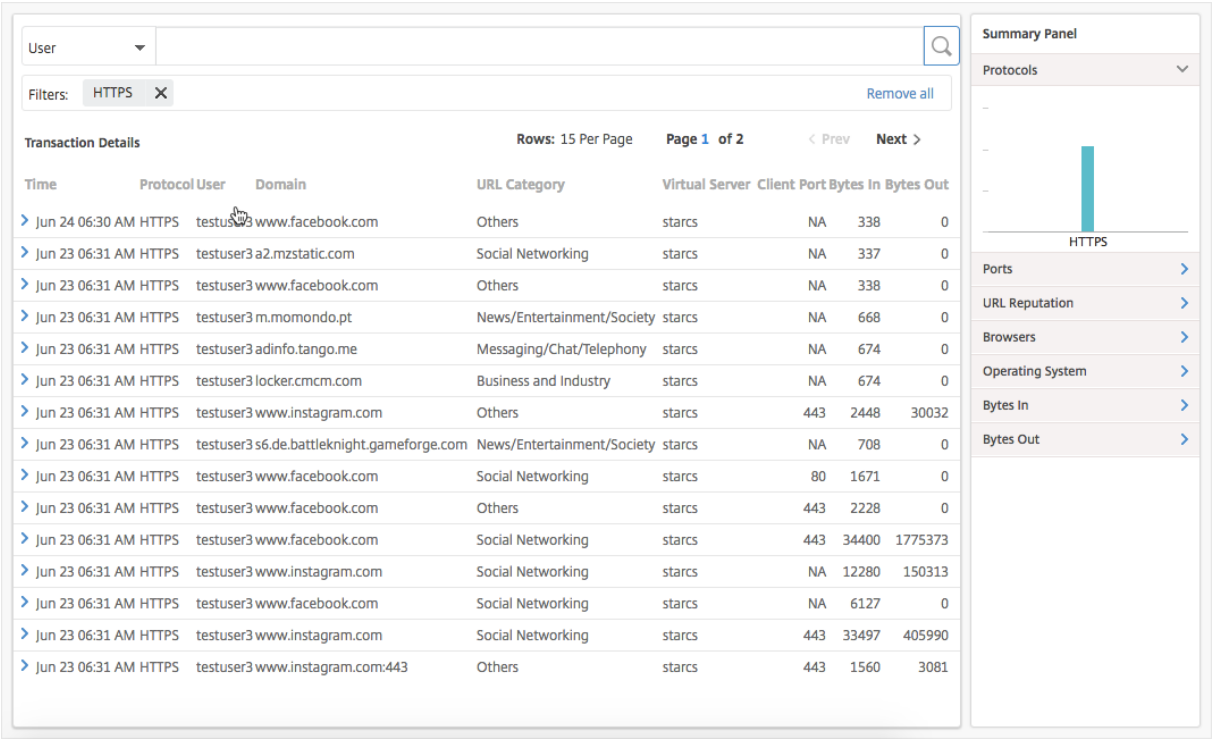


傍受された **SSL** 接続のトランザクションの詳細を表示するには、以下を行います。

1. 「アプリケーション」>「アウトバウンドトラフィックダッシュボード」に移動します。
2. 送信トラフィックダッシュボードで、「**SSL** インターセプト」セクションの合計数をクリックします。



選択した期間中に傍受された SSL 接続のトランザクション詳細が、[トランザクション詳細] ページに表示されます。

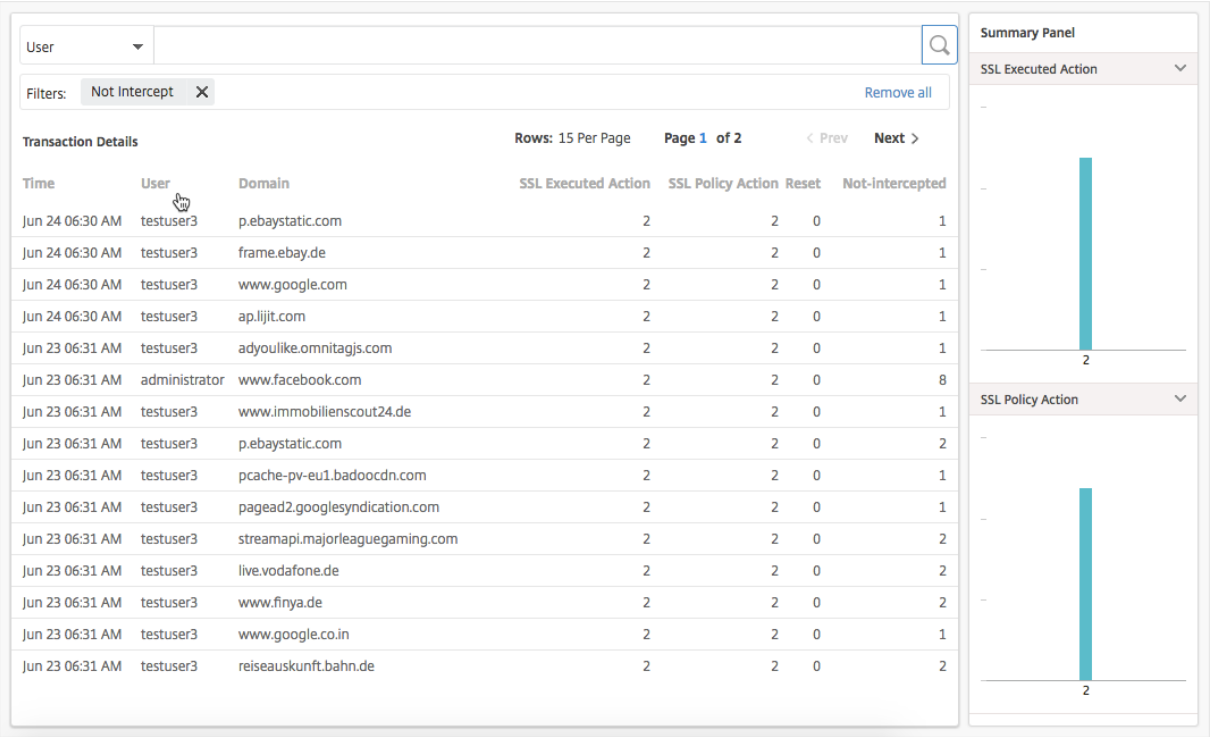


トランザクションの詳細をユーザーや URL カテゴリでさらにフィルターできます。

トラフィックが傍受されなかった **SSL** 接続のトランザクション詳細を表示するには、次の手順を実行します。

1. 「アプリケーション」**>**「アウトバウンドトラフィックダッシュボード」に移動します。
2. 送信トラフィックダッシュボードで、代行受信されていない **SSL** 接続セクションの合計数をクリックします。

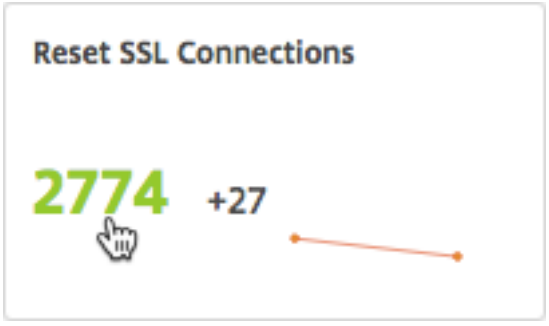
選択した期間中にトラフィックが傍受されなかった SSL 接続のトランザクションの詳細は、[**Transaction Details**] ページに表示されます。



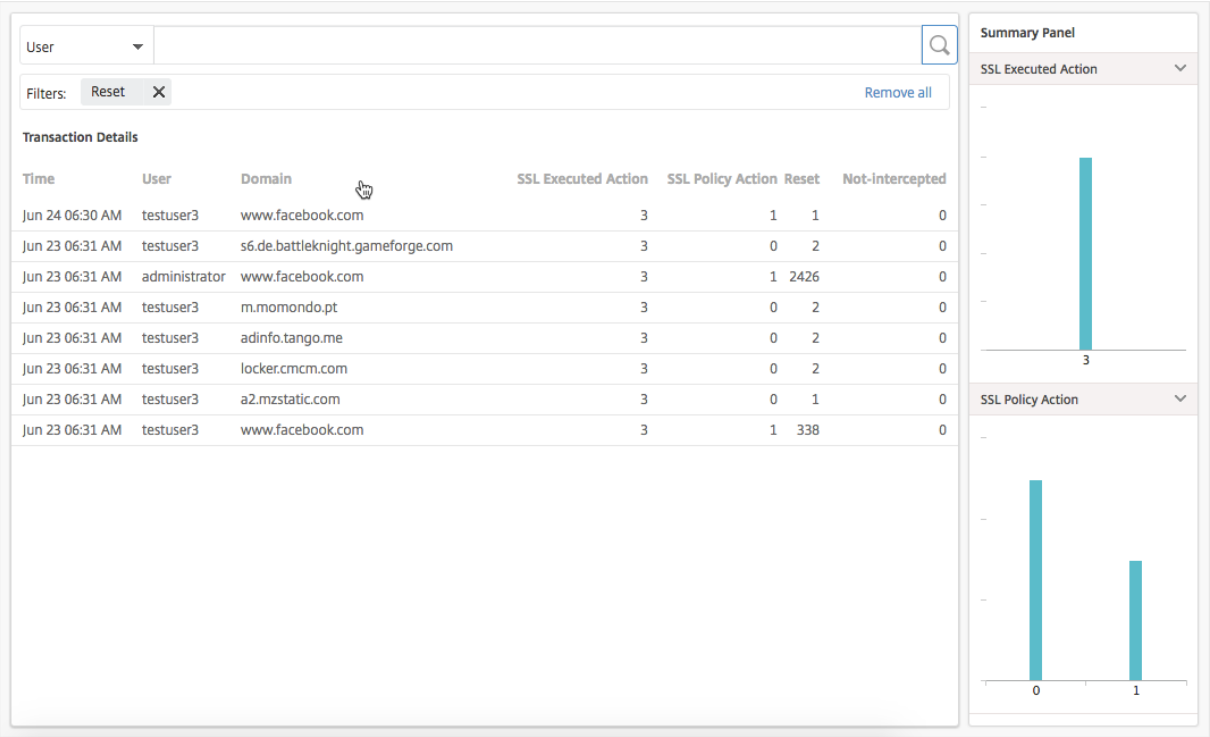
トランザクションの詳細をユーザーや URL カテゴリでさらにフィルターできます。

リセットされた **SSL** 接続のトランザクション詳細を表示するには、次の手順を実行します。

1. 「アプリケーション」**>**「アウトバウンドトラフィックダッシュボード」に移動します。
2. 送信トラフィックダッシュボードで、[**SSL** 接続のリセット] セクションで合計数をクリックします。



選択した期間中にトラフィックが傍受されなかった SSL 接続のトランザクションの詳細は、[**Transaction Details**] ページに表示されます。



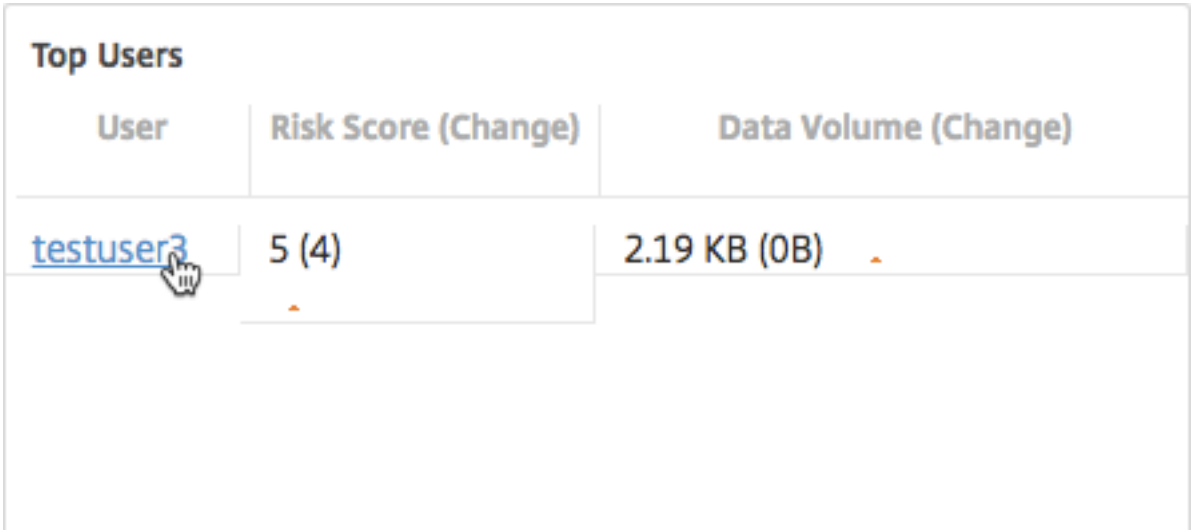
トランザクションの詳細をユーザーや URL カテゴリでさらにフィルターできます。

エンドポイントの検査

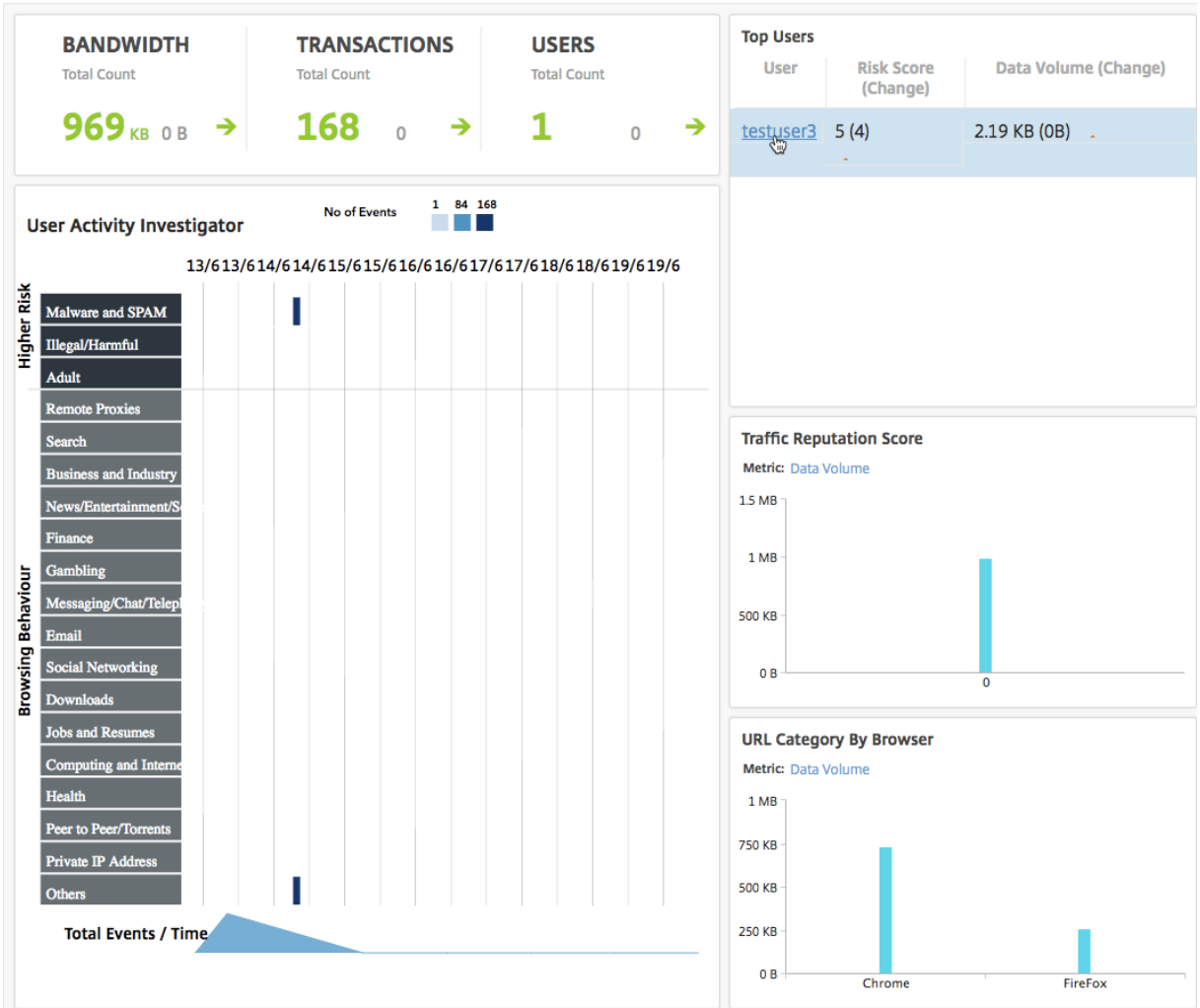
Citrix ADC アプライアンスに構成したポリシーは、企業で実行されたすべてのユーザーアクティビティをアプライアンスがログに記録する方法を指定します。Citrix ADM は、次の項目を決定するために使用できる主要なメトリックを提供します。

1. 社内ユーザーのブラウジング行動
2. 社内ユーザーがアクセスした URL カテゴリ。
3. リスクスコアおよび使用帯域幅量に基づく上位 5 名のユーザー。詳しくは、リスクスコアを参照してください。
4. URL またはドメインへのアクセスに使用された Web ブラウザー。
5. トラフィックレピュテーションスコアに基づく、ユーザーにより生成された Web トラフィックの量

たとえば、ユーザー ID testuser3 のユーザーが企業内のマルウェア関連サイトに常にアクセスする場合、Citrix ADM はそのユーザーを危険度の高いアクティビティユーザーとして識別し、より高いリスクスコアを割り当てます。testuser3 情報は、ユーザーダッシュボードの「上位ユーザー」セクションに表示されます。

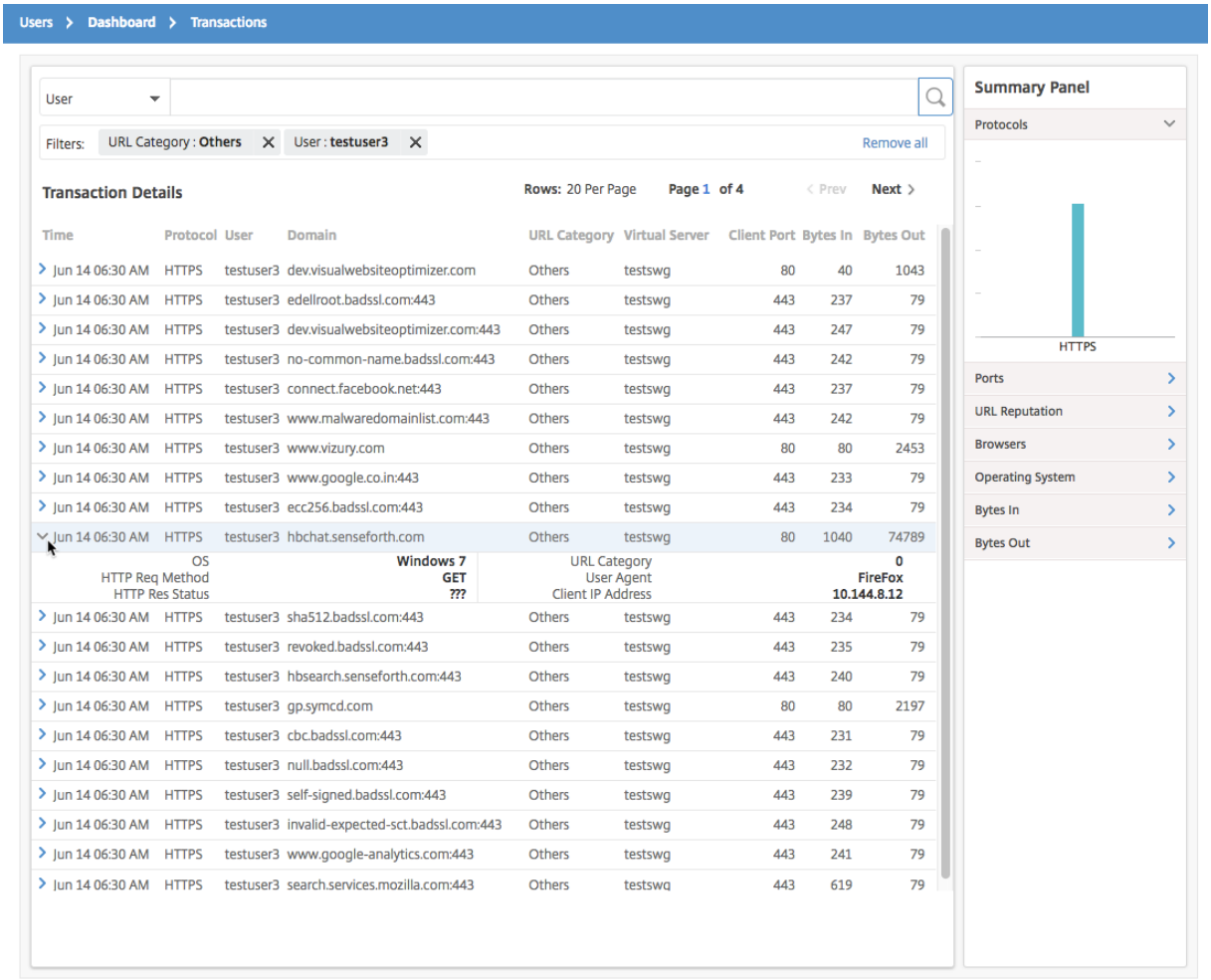


testuser3 をクリックすると、ユーザーダッシュボードをフィルタリングして、testuser3 に関連するすべての主要なメトリックを表示できます。



[ユーザーアクティビティの調査] ペインでは、testuser3 の高リスクアクティビティが、それぞれの URL カテゴリにイベントとして表示されます。

イベントにカーソルを合わせると、イベントの数が表示されます。イベントをクリックすると、イベント中に発生したトランザクションを調査できます。

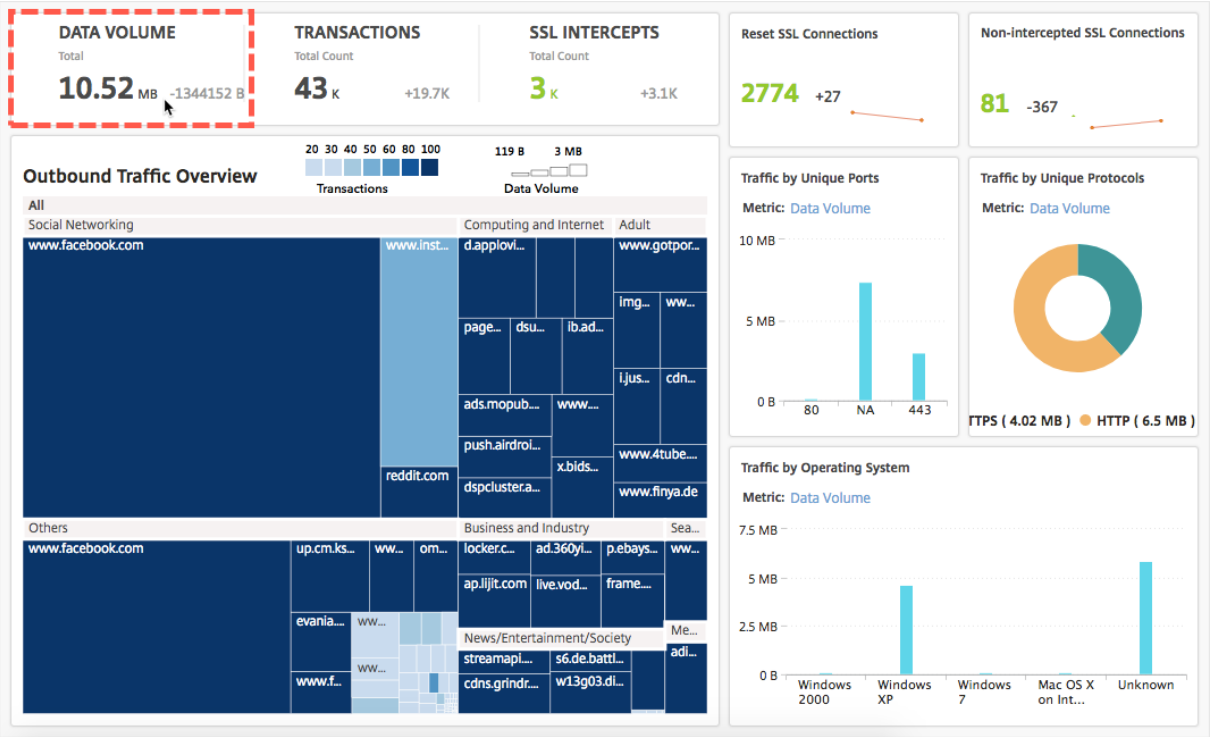


この情報を使用して、システムがマルウェアに感染しているかどうかを判断したり、ユーザーの帯域幅消費パターンを把握したり、Citrix ADC ポリシーを微調整したりできます。詳しくは、「Citrix SSL 転送プロキシのドキュメント」を参照してください。

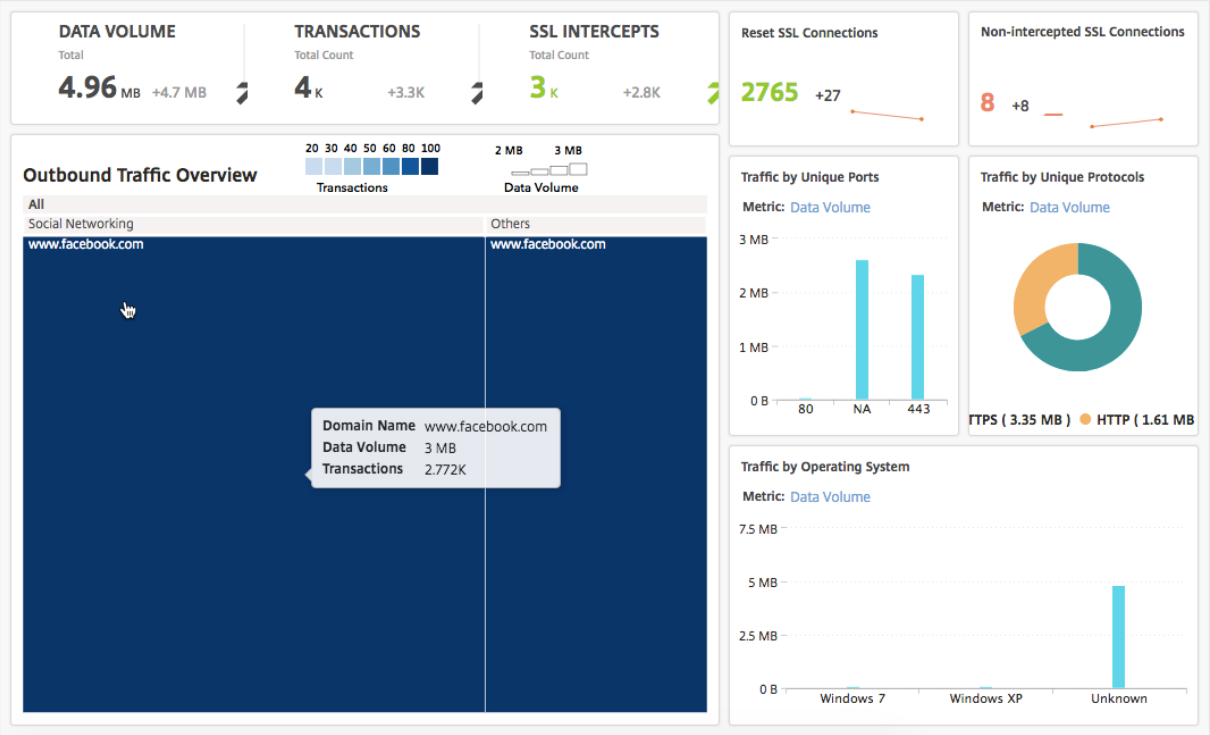
帯域幅消費のレポート

Outbound TrafficDashboard と **User Dashboard** には、企業ネットワークからアクセスした Web サイトやアプリケーション、およびネットワーク内のユーザーが実行したアクティビティをまとめた複数のグラフが用意されています。

Outbound Traffic Dashboard には、ネットワークからアクセスされた URL またはドメインによるデータ量消費の詳細が表示されます。「アプリケーション」**>**「アウトバウンドトラフィックダッシュボード」に移動します。「データボリューム」セクションに データボリュームの詳細が表示されます。

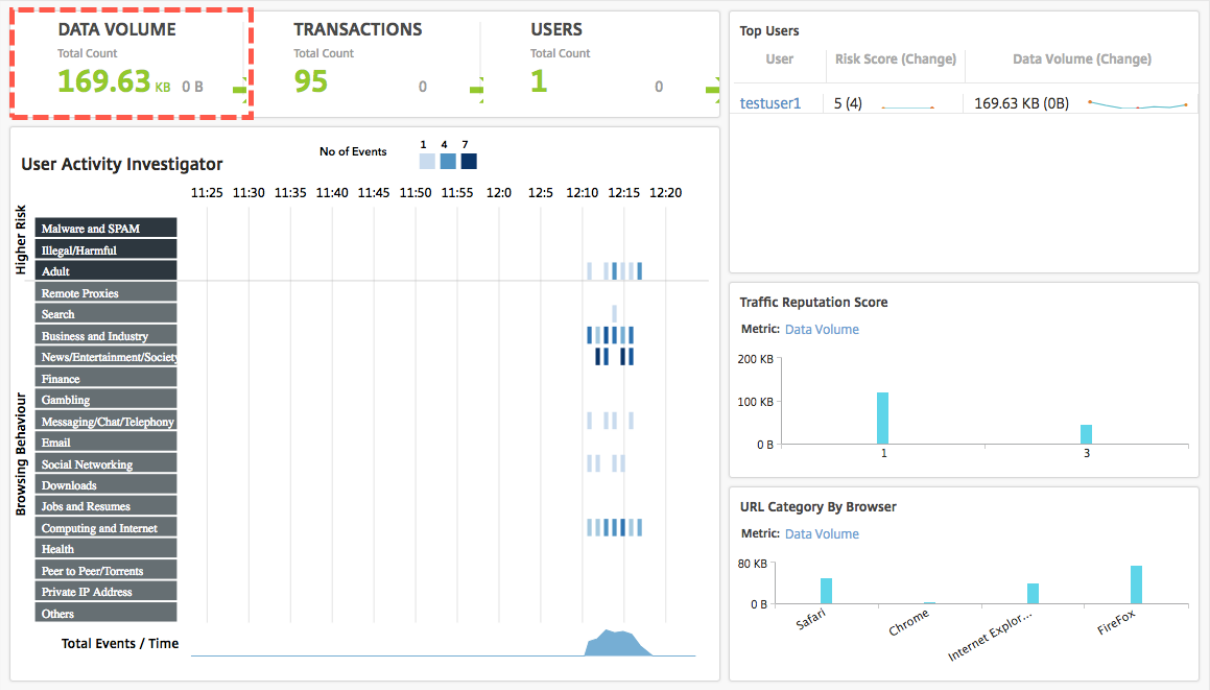


[**Outbound Traffic Overview**] ペインで、ドメインまたは URL をクリックすると、ドメインまたは URL によって消費されるデータボリュームの詳細を表示できます。

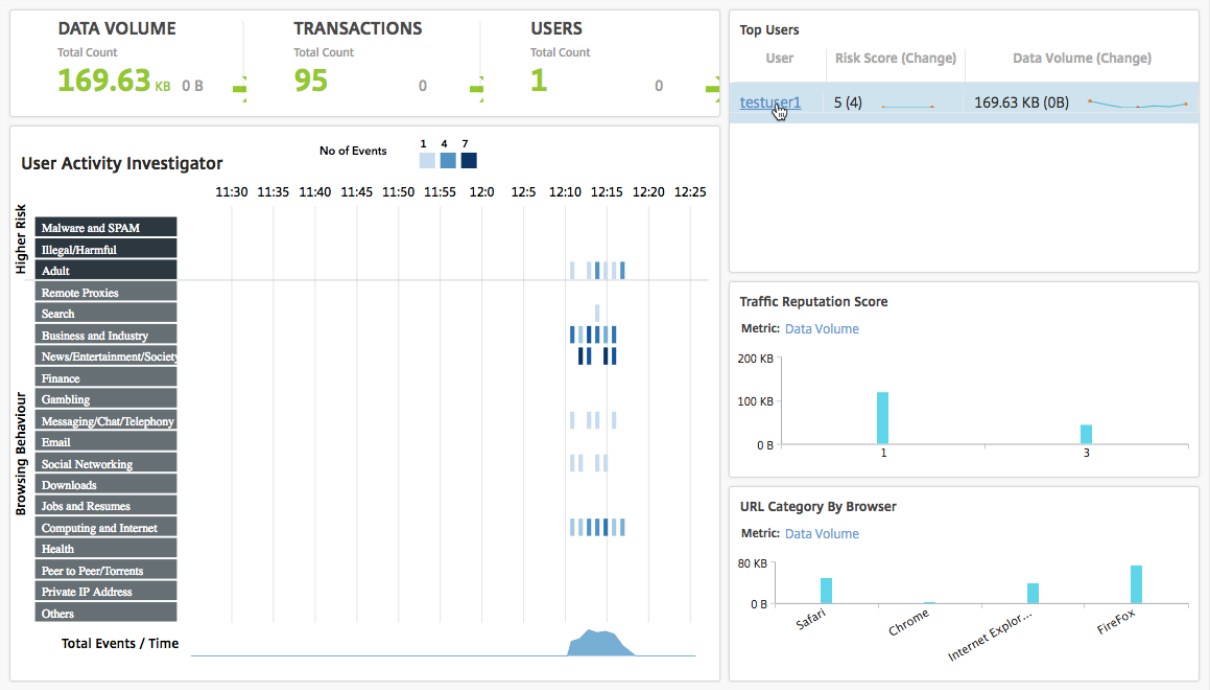


User Dashboard には、ネットワーク内のユーザが消費する帯域幅の詳細が表示されます。「ユーザー」>「ダッシュボード」に移動し、「ユーザー ダッシュボード」の「**D**ATA VOLUME」セクションにユーザーが消費した帯域幅の

詳細を表示します。



[**Top Users**] セクションからユーザーを選択すると、ユーザーが消費した帯域幅の詳細を表示できます。グラフ内の D **ATA VOLUME** セクションおよびその他の主要なメトリックは、選択したユーザーに対してフィルタリングされます。



これらの詳細を使用して、消費帯域幅とその消費理由を把握できます。たとえば、ユーザーがソーシャルネットワーキング Web サイトにアクセスしていて、これにより帯域幅の消費量が多くなっている場合、管理者は Citrix ADC ア

プライアンスにアクセスし、URL リスト機能を設定して Web サイトへのアクセスを制御できます。詳しくは、「ユースケース: カスタム URL セットトピックを使用した URL フィルタリング」を参照してください。

アウトバウンドトラフィック分散の表示

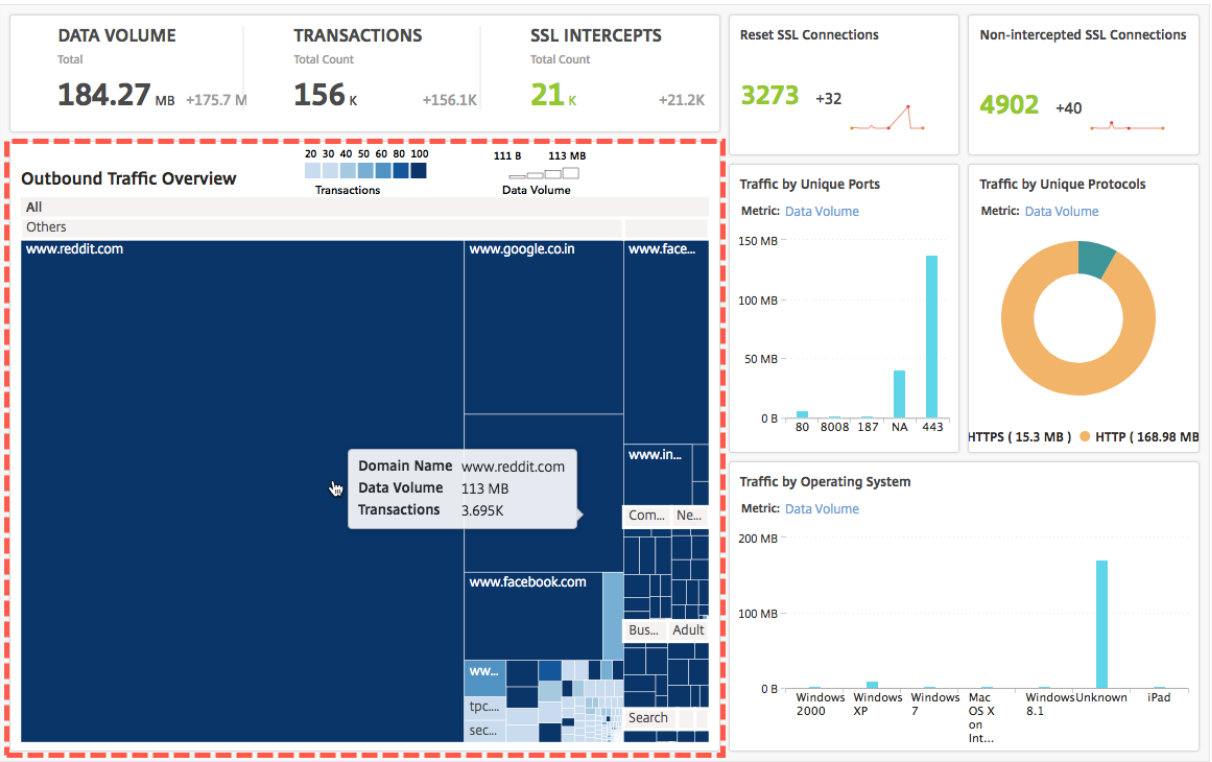
Citrix ADC アプライアンスには、ネットワークからアクセスされる URL の分類とフィルタリング機能があります。Citrix ADM では、送信トラフィックダッシュボードに [送信トラフィックの概要] ペインが表示されます。Citrix ADM では、[アウトバウンドトラフィックの概要] ペインで、アクセスした URL またはドメインがショッピング、ニュース、モバイルなどのカテゴリにグループ化され、ネットワーク内のアウトバウンドトラフィックの分布が表示されます。選択した期間について、URL をクリックすると、次の内容を理解できます。

1. URL へのアクセスによって消費された帯域幅
2. URL にアクセス中に発生したトランザクション
3. URL にアクセス中に傍受された、傍受されていない、およびリセットされた SSL 接続の数

この情報により、送信トラフィックパターンを把握できるほか、特定の URL をブロックすべきかどうかなどの適切な意思決定を行うことができます。

アウトバウンド・トラフィックの分散を表示するには、次の手順に従います。

「アプリケーション」>「アウトバウンドトラフィックダッシュボード」に移動します。[アウトボードトラフィックダッシュボード] の [アウトバウンドトラフィックの概要] ペインに URL が表示されます。



特定の URL の詳細を表示する場合には、その URL を選択します。

この情報を使用して、送信トラフィックパターンを理解し、Citrix ADC アプライアンスで構成された URL フィルターを使用してネットワークトラフィックを制御できます。詳しくは、「URL フィルタリング」を参照してください。

プールされた容量

May 7, 2021

Citrix ADC のプール容量は、Citrix Application Delivery Management（ADM）でホストされ、提供される共通の帯域幅とインスタンスプールから構成されるライセンスフレームワークです。この共通プールから、データセンター内の各 ADC インスタンスは、プラットフォームやフォームファクタに関係なく、1 つのインスタンスライセンスをチェックアウトし、必要な帯域幅だけをチェックアウトします。ライセンスファイルと、したがって、帯域幅はインスタンスにバインドされません。インスタンスでこれらのリソースが不要になった場合、インスタンスはリソースを共通プールにチェックインし、このリソースを必要とする他のインスタンスが利用できるようになります。

> 注
>
> ADM サービスでは、エージェントの 1 つがライセンスサーバーです。オンプレミスの ADM では、オンプレミスサーバーはライセンスサーバーです (エージェントが展開されている場合でも)。

このライセンスフレームワークは、インスタンスに要件を超える帯域幅が割り当てられないようにすることで、帯域幅の使用率を最大化します。ADC インスタンスは、共通プールのライセンスと帯域幅をチェックする機能によって、インスタンスのプロビジョニングを自動化することもできます。

トラフィックに影響を与えることなく、実行時にインスタンスに割り当てられる帯域幅を増減できます。プール内のライセンスを 1 つのインスタンスから別のインスタンスに転送することもできます。

プールされた容量の構成

May 7, 2021

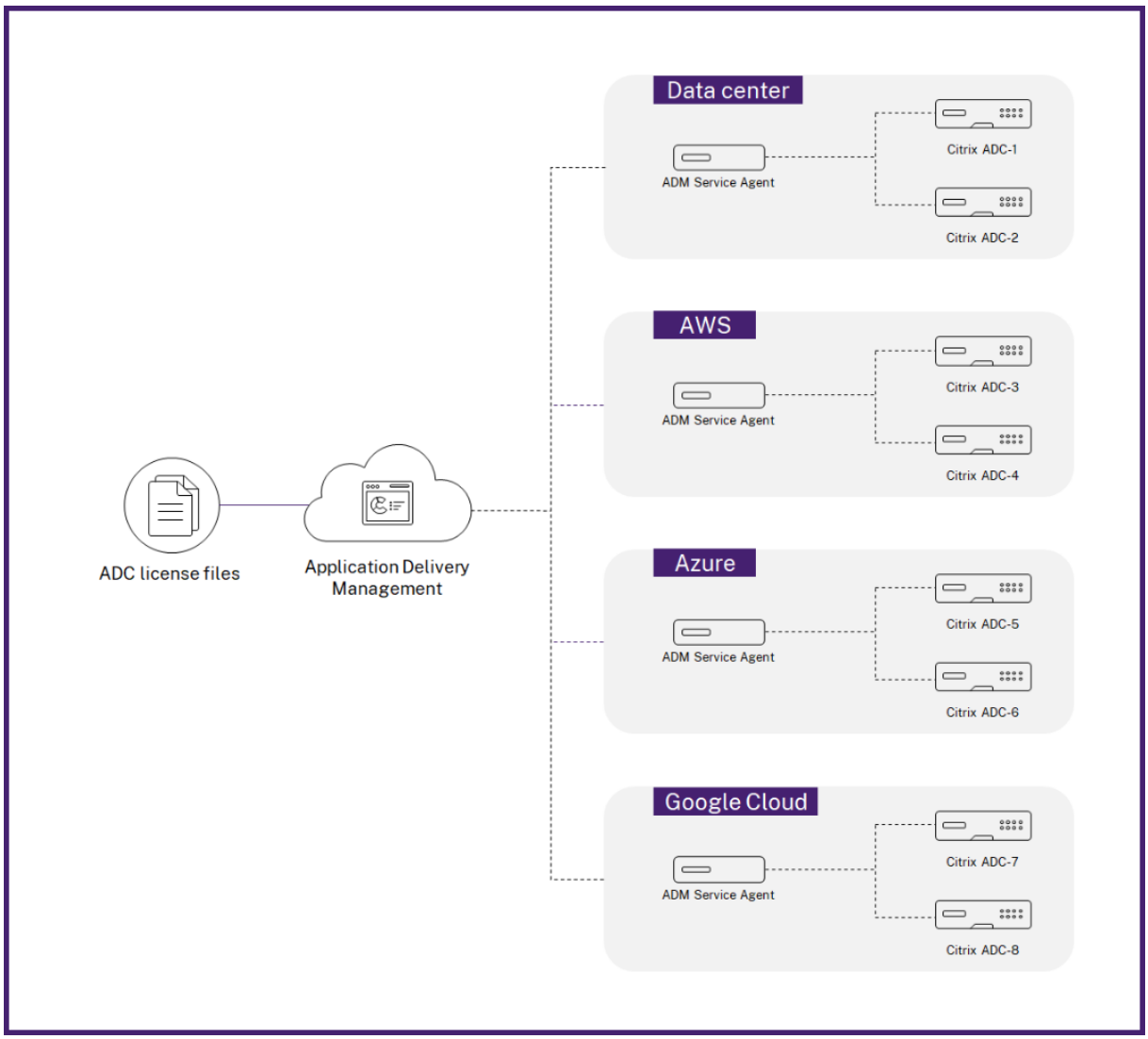
Citrix ADC プール容量により、異なる ADC フォームファクタ間で帯域幅またはインスタンスライセンスを共有できます。仮想 CPU サブスクリプションベースのインスタンスの場合、インスタンス間で仮想 CPU ライセンスを共有できます。このプールされた容量は、データセンターまたはパブリッククラウドにあるインスタンスに使用します。インスタンスがリソースを必要としなくなった場合、割り当てられた容量を共通プールにチェックし直します。解放された容量を、リソースを必要とする他の ADC インスタンスに再利用します。

プールライセンスを使用して、必要な帯域幅をインスタンスに割り当てることにより、帯域幅の使用率を最大限に高めることができます。トラフィックに影響を与えずに、実行時にインスタンスに割り当てられる帯域幅を増減します。プール容量ライセンスを使用すると、インスタンスの Provisioning を自動化できます。

ADC プールされた容量を使用するには、必ず ADM エージェントを ADC インスタンスに接続してください。ADC インスタンスは、エージェントを介して ADM サービスからライセンスをチェックインおよびチェックアウトします。

ADC FIPS インスタンスには、プールされた容量ライセンスを使用することもできます。ADM サービスでは、次のタスクを実行できます。

- プールされたキャパシティライセンスファイル（帯域幅プールまたはインスタンスプール）をライセンスサーバーにアップロードします。
- ライセンスプールから ADC インスタンスにオンデマンドでライセンスを割り当てます。
- インスタンスの最小容量と最大容量に基づいて、ADC インスタンス（MPX-Z /SDX-Z/VPX/CPX/BLX）からライセンスをチェックアウトします。



ADC プール容量に関する問題

プール容量状態は、ADC インスタンスのライセンス要件を示します。プール容量が設定された ADC インスタンスは、次のいずれかの状態を表示します。

- **Optimum**: インスタンスは適切なライセンス容量で実行されています。

- 容量の不一致: インスタンスは、ユーザーが構成した容量より少ない容量で実行されています。
- **Grace**: インスタンスは猶予ライセンスで実行されています。
- **Grace & Mismatch**: インスタンスは猶予で実行されていますが、キャパシティはユーザー設定よりも小さくなっています。
- 使用不可: インスタンスが管理のために ADM に登録されていないか、ADM からインスタンスに対する NITRO 通信が機能していません。
- 未割り当て: ライセンスはインスタンスに割り当てられません。

はじめに

プール容量を構成する前に、次のことを確認してください。

- エージェントを ADM サービスにインストールして登録します。エージェントをインストールして登録するには、「はじめに」を参照してください。
- 27000および7279ポートは、ADM からインスタンスにライセンスをチェックアウトできます。「システム要件」を参照してください。

ステップ **1-ADM** でライセンスを適用する

1. Citrix ADM で、［ネットワーク］>［ライセンス］に移動します。
2. [ライセンスファイル] セクションで、[ライセンスファイルの追加] を選択し、次のいずれかのオプションを選択します。
   - ローカルコンピュータからライセンスファイルをアップロードします。ライセンスファイルがローカルコンピュータに既に存在する場合は、ADM にアップロードできます。
   - ライセンスアクセスコードを使用します。Citrix から購入したライセンスのライセンスアクセスコードを指定します。次に、[ライセンスの取得] を選択します。次に、[完了] を選択します。

   > 注:
   >
   > ライセンス 設定から ADM にライセンスを追加できます。
3. ［完了］をクリックします。

   ライセンスファイルが ADM に追加されます。[ライセンスの有効期限情報] タブには、ADM に存在するライセンスと有効期限の残りの日数が一覧表示されます。
4. [ライセンスファイル] で、適用するライセンスファイルを選択し、[ライセンスの適用] をクリックします。

   この操作により、ADC インスタンスは選択したライセンスをプール容量として使用できます。

ステップ **2-**ライセンスサーバーとして **ADM** サービスを登録する

エージェントを使用して、ADM サービスをライセンスサーバーとして Citrix ADC インスタンスに登録できます。

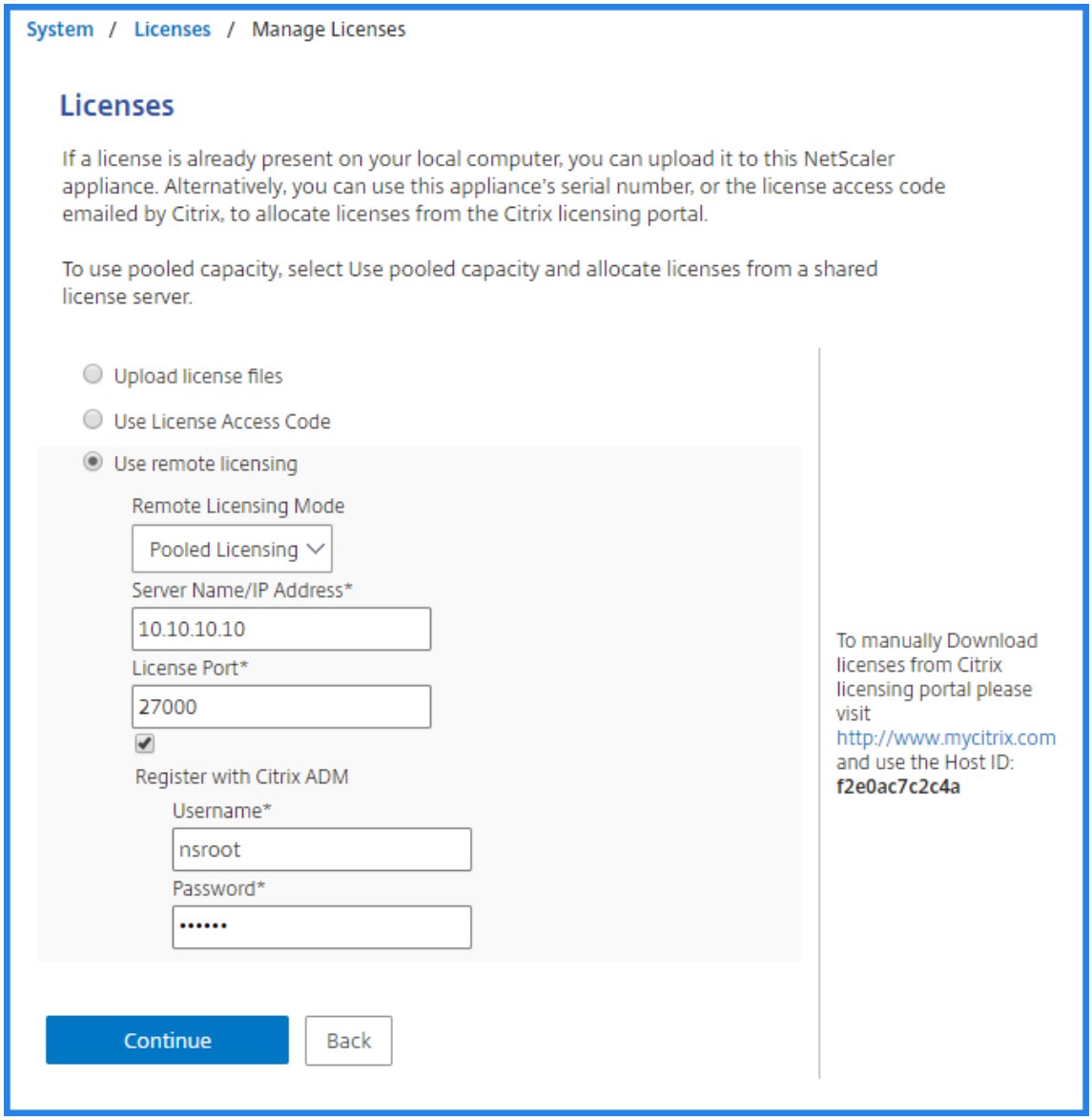
次のいずれかの手順を使用して、ADM サービスをライセンスサーバーとして登録します。

- GUI を使用する
- CLI を使用

GUI を使用して **ADM** エージェントを登録する

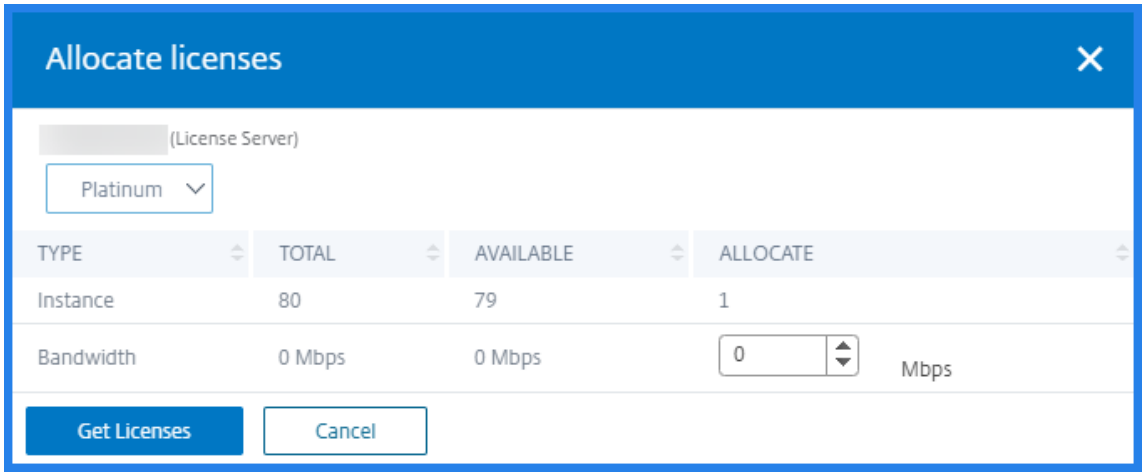
ADM GUI で、ADC インスタンスに関連付けられた ADM エージェントを登録します。

1. Citrix ADC GUI にログインします。
2. [システム] > [ライセンス**] > [**ライセンスの管理] に移動します。
3. [新しいライセンスを追加] をクリックします。
4. [リモートライセンスを使用する] を選択し、リストからリモートライセンスモードを選択します。
5. [サーバー名**/IP** アドレス] フィールドで、ADM サービスに登録されている ADM エージェントの IP アドレスを指定します。
6. [**Citrix ADM** に登録］を選択します。
7. ADM 認証情報を入力して、Citrix ADM にインスタンスを登録し、[**Continue**］をクリックします。



8. [ライセンスの割り当て] で、ライセンスエディションを選択し、必要な帯域幅を指定します。

   初めて、Citrix ADC でライセンスを割り当てます。ライセンス割り当ては、後で Citrix ADM GUI から変更または解放できます。



9. [ライセンスの取得] をクリックします。

> 重要
>
> ライセンスエディションを変更する場合は、インスタンスをウォーム再起動します。設定の変更は、インスタンスを再起動するまで有効になりません。

CLI を使用して ADM エージェントを追加する

ADC インスタンスに GUI がない場合は、次の CLI コマンドを使用して、インスタンスに関連付けられた ADM エージェントを追加します。

1. Citrix ADC コンソールにログインします。
2. ADM サービスに登録されている、関連する ADM エージェントの IP アドレスを追加します。

```
1 > add ns licenseserver <adm-agent-IP-address> -port <adm-agent-
    license-port-number>
2 <!--NeedCopy-->
```

3. ライセンスサーバーで使用可能なライセンス帯域幅を表示します。

```
1 > sh ns licenseserverpool
2 <!--NeedCopy-->
```

4. 必要なライセンスエディションからライセンス帯域幅を割り当てます。

```
1 > set ns capacity -unit gbps -bandwidth <specify-license-bandwidth
    > edition <specify-license-edition>
2 <!--NeedCopy-->
```

ライセンスエディションは、スタンダード、アドバンス、プレミアムです。

> 重要:
>
> ライセンスエディションを変更する場合は、インスタンスをウォーム再起動します。
>
> ```
> reboot -w
> ```
>
> 設定の変更は、インスタンスを再起動するまで有効になりません。

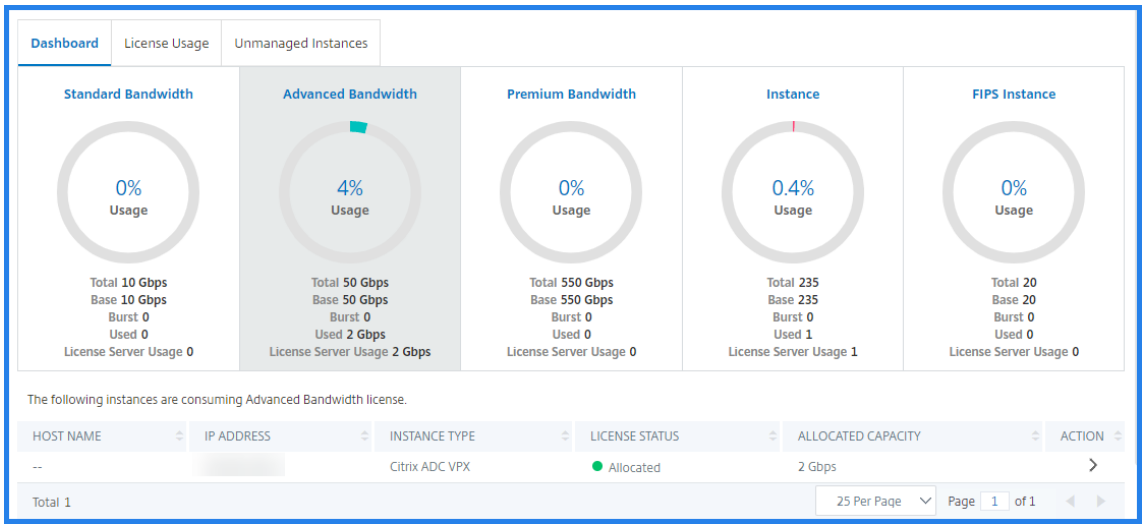
ステップ 3-プールされたライセンスを ADC インスタンスに割り当てる

ADM GUI からプールキャパシティライセンスを割り当てるには、次の手順を実行します。

1. Citrix ADM にログインします。
2. [ネットワーク] > [ライセンス] > [帯域幅ライセンス] > [プール容量] に移動します。

   FIPS インスタンス容量は、FIPS インスタンスライセンスを ADM にアップロードする場合にだけ表示されます。
3. 管理するライセンスプールをクリックします。

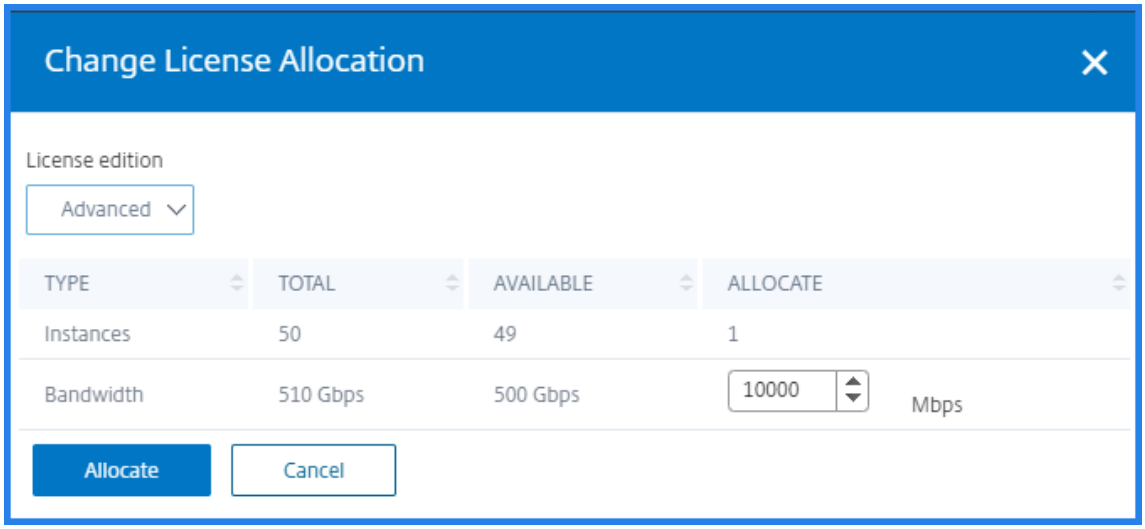
   > 注:
   >
   > [割り当て済み容量] フィールドには、変更された帯域幅がすぐには反映されません。帯域幅の変更は、ADC のウォーム再起動後に有効になります。
   >
   > [**Allocation Details]** で、インスタンスの帯域幅割り当てを変更すると、[リクエスト済み] フィールドと [Appl **ied**] フィールドが更新されます。
4. [**>**] ボタンをクリックして、使用可能なインスタンスのリストから ADC インスタンスを選択します。



[License status] 列には、対応するライセンス割り当てステータスメッセージが表示されます。

> 注:
>
> ［管理対象外のインスタンス］タブには、Citrix ADM で検出され管理されていないインスタンスが表示されます。
>
> 
>

5. [割り当ての変更] または [割り当ての解除] をクリックして、ライセンスの割り当てを変更します。
6. ライセンスサーバーで使用可能なライセンスを示すポップアップウィンドウが表示されます。
7. [Allocate] リストオプションを設定することで、インスタンスへの帯域幅またはインスタンスの割り当てを選択できます。選択が完了したら、[割り当て] をクリックします。
8. 割り当てられたライセンスエディションは、[Change License **Allocation]** ウィンドウのリストのオプションから変更することもできます。



> 注:
>
> ライセンスエディションを変更する場合は、インスタンスをウォーム再起動します。

ADC インスタンスのプール容量を設定する

プール容量ライセンスは、次の ADC インスタンスで設定できます。

- ADC MPX-Z インスタンス
- ADC VPX インスタンス
- ADC の高可用性ペア

Citrix ADC MPX-Z インスタンス

MPX-Z は、プール容量対応の ADC MPX アプライアンスです。MPX-Z は、Premium、Advanced、または Standard エディションのライセンスの帯域幅プールをサポートします。

MPX-Z では、ライセンスサーバーに接続する前にプラットフォームライセンスが必要です。MPX-Z プラットフォームライセンスは、次のいずれかの方法でインストールできます。

- ローカルコンピュータからライセンスファイルをアップロードします。
- インスタンスのハードウェアシリアル番号を使用する。
- インスタンスの GUI の [システム] > [ライセンス] セクションのライセンスアクセスコード。

MPX-Z プラットフォームライセンスを削除すると、プール容量機能は無効になります。インスタンスライセンスがライセンスサーバーに解放されます。

再起動することなく、MPX-Z インスタンスの帯域幅を動的に変更できます。再起動が必要になるのは、ライセンスエディションを変更する場合のみです。

> 注:
>
> インスタンスを再起動すると、設定された容量に必要なプールされたライセンスが自動的にチェックアウトされます。

Citrix ADC VPX インスタンス

プール容量対応 ADC VPX インスタンスは、帯域幅プール（Premium/Advanced/Standard エディション）からライセンスをチェックアウトできます。ADC GUI を使用して、ライセンスサーバからライセンスをチェックアウトできます。

再起動せずに、VPX インスタンスの帯域幅を動的に変更できます。再起動が必要になるのは、ライセンスエディションを変更する場合のみです。

> 注:
>
> インスタンスを再起動すると、設定されたプール容量ライセンスは ADM サーバーから自動的にチェックアウトされます。

Citrix ADC の高可用性ペア

開始する前に、ADM サーバがライセンスサーバとして設定されていることを確認します。詳しくは、「ADM をライセンスサーバとして構成する」を参照してください。

ADC HA ペアに帯域幅を割り当てると、Citrix ADM はプライマリおよびセカンダリインスタンスに同じ帯域幅をチェックアウトします。ADC HA ペアに 10 Mbps の帯域幅を割り当てると、ADM は次の処理を行います。

1. HA ペアに 20 Mbps の帯域幅をチェックアウトします。
2. HA ペアの各インスタンスに 10 Mbps を割り当てます。

ADC HA ペアにプールライセンスを割り当てるには、を参照してくださいプールされたライセンスを ADC インスタンスに割り当てる。

[**Pooled Capacity**] ページには、インスタンスとその割り当て済み容量が別々に表示されます。プライマリ・インスタンスの帯域幅を変更または解放すると、セカンダリ・インスタンスの帯域幅はプライマリ・インスタンスと自動的に同期されます。ただし、セカンダリインスタンスの帯域幅を変更または解放した場合、同期は実行されません。

プールされたライセンス機能に対してのみ **ADM** サービスを構成する

May 7, 2021

管理者は、プールされたライセンス機能に対してのみ ADM サービスを構成できます。この設定では、ADM サービスは ADC インスタンスからライセンスデータのみを受信します。

場合によっては、ADC インスタンスのデータを規制区域から退出することを制限する必要がある規制要件がある場合があります。このような状況では、規制区域に ADM オンプレムサーバーのローカルインスタンスをデプロイして、管理、監視、および分析機能を使用できます。同じ方法でプールライセンス機能を使用する場合は、プールされたライセンスをさまざまな ADM ライセンスサーバー間で分割する必要があります。この方法では、グローバルにデプロイされた ADC インスタンスにプールされたライセンスを柔軟に割り当てることはできません。

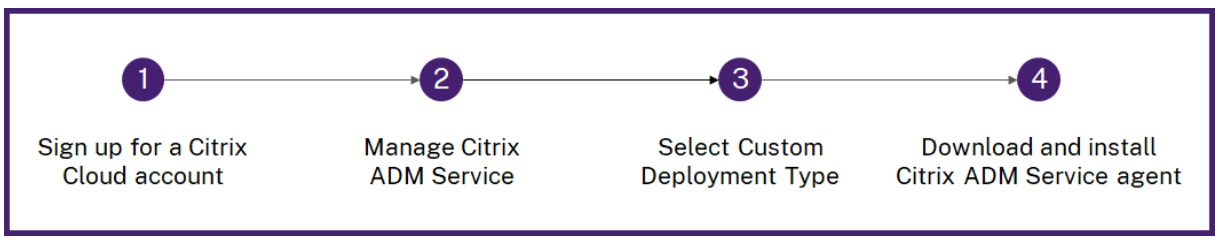
したがって、プールされたライセンス機能に対してのみ ADM サービスを構成します。ADM サービスは、すべての ADC インスタンスからライセンスデータのみを受信します。そのため、規制要件を遵守し、グローバルにデプロイされた ADC インスタンスにプールされたキャパシティーライセンスを動的に割り当てることができます。

このドキュメントでは、プールされたライセンス機能に対してのみ ADM サービスを設定する方法について説明します。

前提条件

プールされたライセンス機能だけに ADM サービスを構成する前に、ADM サービスの初回オンボーディングとセットアップを完了してください。システム要件のエージェント仕様を確認してください。

> 重要
>
> ADM サービスを初めてオンボード、またはセットアップするときは、次の点を確認してください。
>
> - [カスタム配置] オプションが選択されています。
> - この設定手順のステップ 4 を完了した後に追加する ADC インスタンス。



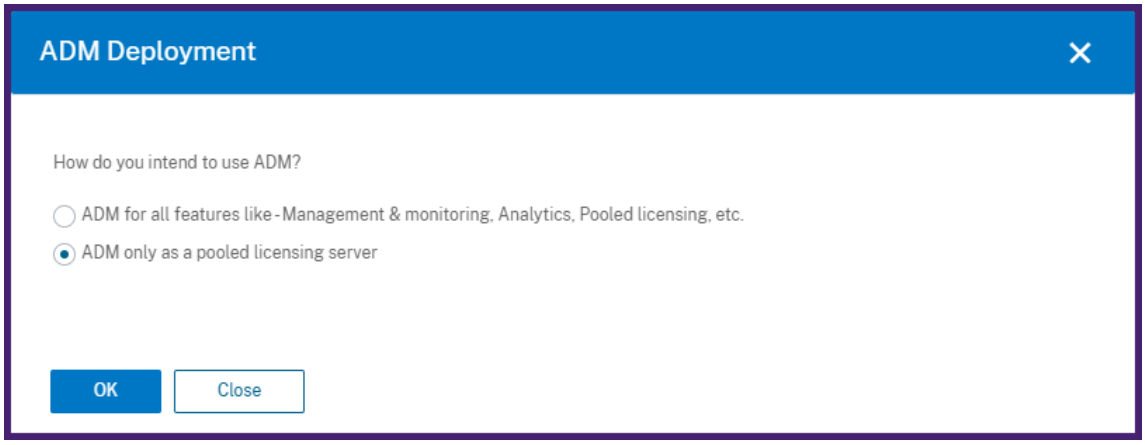
ADM サービスのオンボーディングとセットアップの詳細については、「はじめに」を参照してください。

初期ボーディング手順を完了したら、プールされたライセンス機能に対してのみ ADM サービスを構成します。

プールされたライセンス機能に対してのみ **ADM** サービスを構成する方法

ライセンス機能だけの ADM サービスを構成するには、次の手順を実行します。

1. [アカウント**] > [**管理**]** に移動します。
2. [システム構成] セクションで、[システムの展開] を選択します。
3. [**ADM** 展開] で、プールされたライセンスサーバーとして **[ADM** のみ] を選択します。



4. [**OK**] をクリックします。

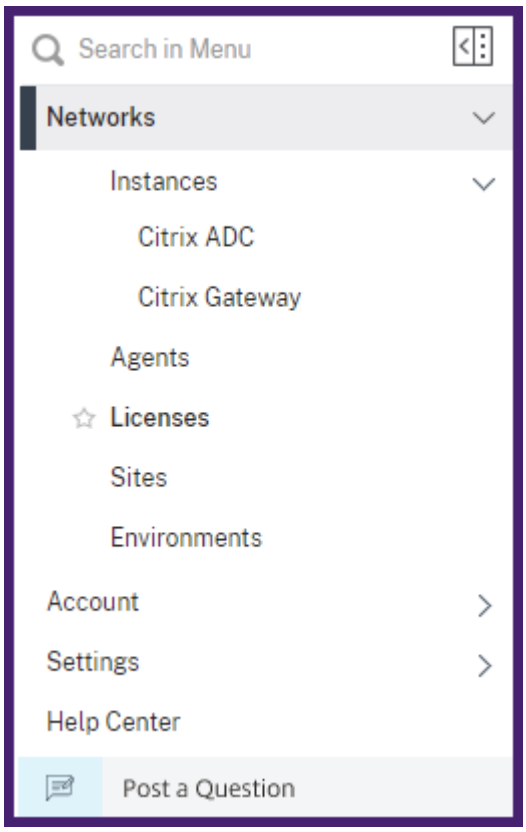
   このアクションでは、プールされたライセンス機能のみが保持され、次の ADM 機能が無効になります。

   - ADM バックアップ
   - イベントの管理
   - SSL 証明書の管理
   - ネットワークレポート
   - ネットワーク機能
   - 構成監査

   > 注:
   >
   > 既定では、ADM 分析機能は無効になっています。この機能を有効にしている場合は、必ず無効にしてください。

   確認ボックスで、[はい] をクリックします。

   ADM GUI には、プールされたライセンス機能だけが表示されます。また、残りのフィーチャは表示されません。



5. ライセンス機能だけに ADM を設定したら、[ネットワーク] **>** [インスタンス] ページで **ADC** インスタンスを追加します。

> 注
>
> - ADC インスタンスは、ADM サービスおよび他の ADM サーバにも追加できます。このような ADC インスタンスのパスワードを変更する場合は、インスタンスが検出されたすべての ADM サーバーでパスワードを更新してください。この注意は、ADM サービスがプールされたライセンス機能だけを使用するように構成されている場合に適用されます。
> - ユーザーは、ADM GUI で無効化された機能の一部の操作を実行できます。たとえば、イベントポーリングや ADC バックアップなどです。スーパー管理者として、このような操作を制限する場合は、適切なアクセスポリシーを使用して他の管理者のユーザーアクセスを無効にします。詳しくは、「Citrix ADM でのアクセスポリシーの構成」を参照してください。

既存のプール容量セットアップ用に新しいライセンスを **ADM** に適用する

May 7, 2021

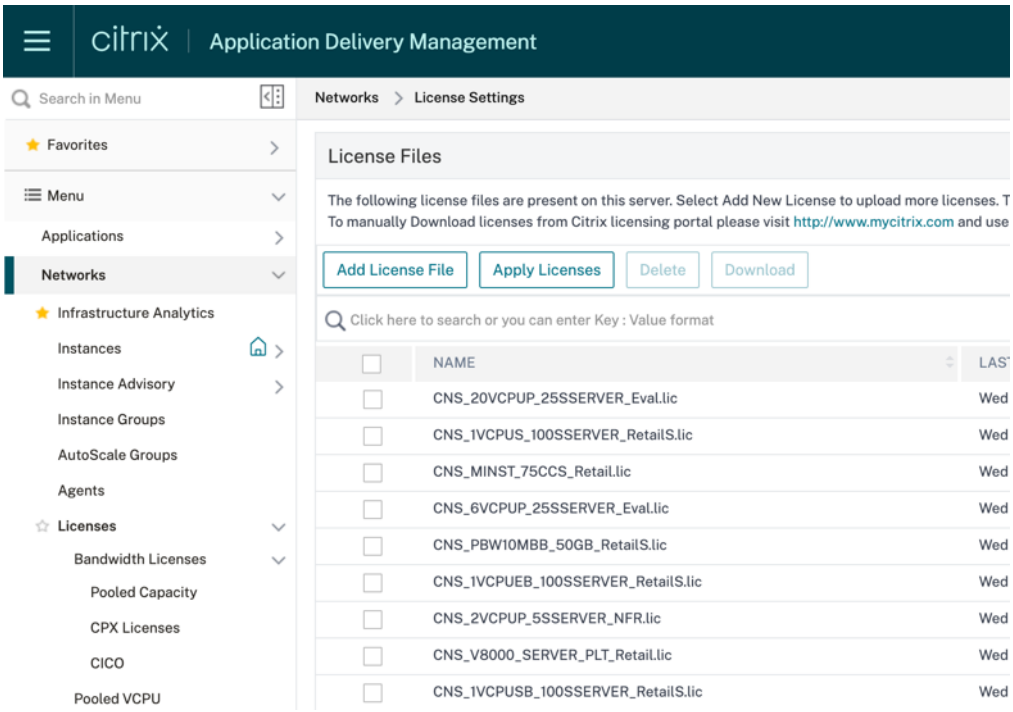
このトピックでは、既存のプール容量セットアップ用に Citrix ADM で新しいライセンスを適用する方法について説明します。ADM に申請する前に、ライセンスファイルが必要です。ライセンスファイルがローカルコンピュータにす

でに存在する場合は、そのファイルを ADM ライセンスサーバーにアップロードできます。または、Citrix からメールで送信されたライセンスアクセスコードを使用して、Citrix ライセンスポータルからライセンスを割り当てることもできます。

[**ADM] > [**ネットワーク**] > [**ライセンス**]** GUI を使用して、プールされたすべての容量ライセンスファイルを管理および展開します。

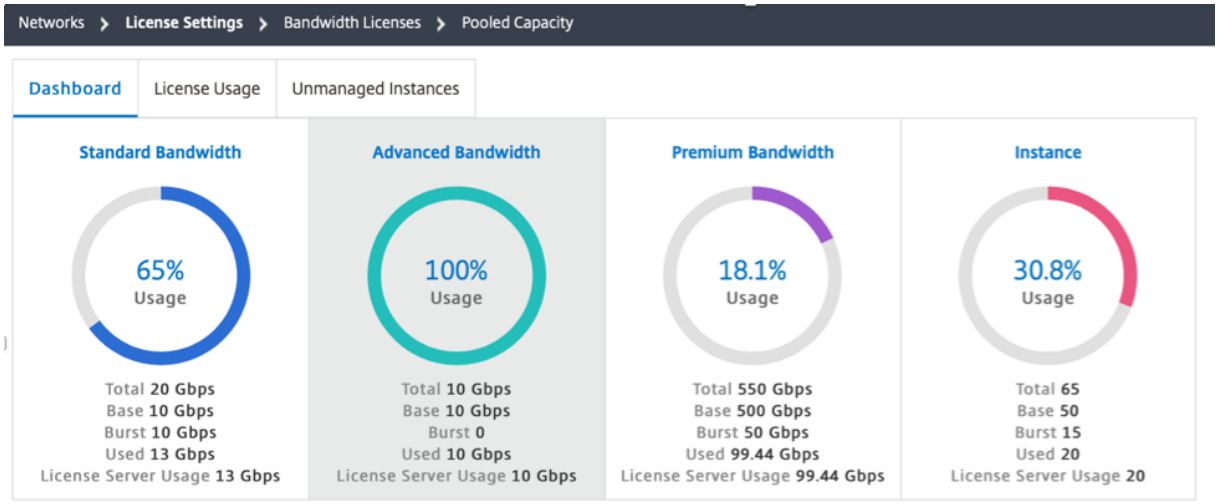
既存のライセンスとプールのステータスを確認する

ADM で利用可能なライセンスを確認するには、**[**ネットワーク**] > [**ライセンス**]** に移動します。



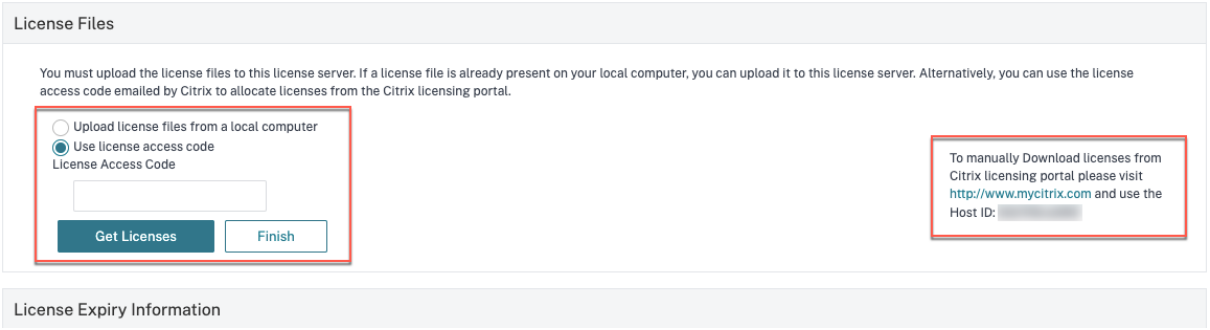
下にスクロールして、ライセンス有効期限情報テーブルで使用可能なライセンスプールを有効期限とともに表示します。

異なるエディションで使用可能なプールを確認するには、[ネットワーク**] > [**ライセンス**] > [**帯域幅ライセンス**] > [**プールされた容量**]** の順に移動します。



新しいライセンスを割り当てる

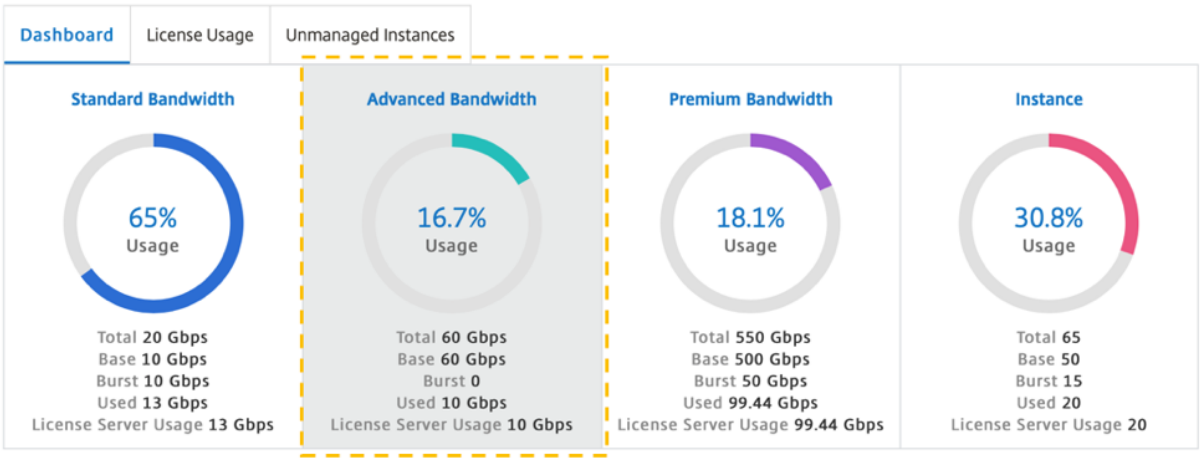
ローカルコンピュータにまだ使用可能なライセンスがない場合は、Citrix が提供するアクセスコードを使用してライセンスを割り当てるか、GUI で指定されたホスト ID を使用して Citrix ライセンスポータルからダウンロードできます。Citrix ライセンスポータルからのライセンスのダウンロードの詳細については、サポート記事Citrix ライセンスサーバーを参照してください。



新しいライセンスを適用する

ダウンロードしたライセンスファイルを適用する手順は、次のとおりです。

1. [ネットワーク**] > [**ライセンス] に移動し、[ライセンスファイルを追加] をクリックします。
2. [**Browse**] をクリックし、新しいライセンスをアップロードします。
3. [完了] をクリックします。[ライセンス設定] ページからいつでもライセンスを追加できます。
4. ライセンスが追加されると、プールされたキャパシティダッシュボードに新しい可用性容量が表示されます。



ライセンスを削除する

既存のライセンスを削除するには、次の手順を実行します。

1. [ネットワーク**]-> [**ライセンス**]** に移動します。
2. ライセンスを選択して [**Delete**] をクリックすると、いつでもライセンスが削除されます。

ADM は、要求された ADC のライセンスを、使用可能な新しいプールから自動的にチェックアウトします。

1. 選択した ADC について、帯域幅割り当てを変更するには、[**Allocate**] をクリックして選択したプールを変更します。

よくある質問とその他のリソース

May 7, 2021

この項では、プールライセンスの設定と運用に関する参考資料を示します。設定および操作の問題に関するサポートについては、これらのドキュメントを参照してください。

構成

1. プールされた容量の概要と機能に関する情報はどこにありますか。

   答え:Citrix ADC プール容量検証済みリファレンスデザインを参照してください。

2. 永続ライセンスをプールされたライセンスに変換または移行するにはどうすればよいですか? 逆の方法ですか?

   回答: 永続ライセンスからプールキャパシティライセンスへの変換は、一方向のライセンスエンタイトルメントプロセスです。プールされたキャパシティライセンスを永続に戻すことはできません。

3. ADM サーバーの展開方法を教えてください。

   答え: はじめに 文書に従ってください。

4. 既存のプールされたライセンスに新しいライセンスを追加して割り当てるには、どうすればよいですか。

   答え: 既存のプール容量セットアップ用に新しいライセンスを ADM に適用する 文書に従ってください。

5. インスタンスで容量と帯域幅を割り当て/増やすにはどうすればよいですか?

   答え: 既存のプール容量セットアップ用に新しいライセンスを ADM に適用する 文書に従ってください。

一般的な問題

1. 接続障害、アップグレード、スプリットブレインなどの理由で猶予モードで実行されているインスタンス。

   答え:Citrix ADC プール容量の設定で説明されている ADM ライセンスサーバの動作を参照してください。

2. ライセンスは、インスタンスに適用または反映されていません。

   答え:ベストプラクティス、コーナーケース、FAQを参照してください。

3. ライセンス割り当てが「同期中」のままになる。

   答え:ベストプラクティス、コーナーケース、FAQを参照してください。

4. ライセンスファイルのホスト ID が間違っているためにエラーが発生しました。

   回答：Citrix Application Delivery Management（ADM）サーバーを識別するには、サーバーにホスト名を割り当てることができます。ホスト名は、Citrix ADM のユニバーサルライセンスに表示されます。詳しくは、「Citrix ADM サーバーへのホスト名の割り当て」を参照してください。

5. 既知または修正されたバグによる問題

   回答: リリースノート、システム要件、ライセンスを確認します。

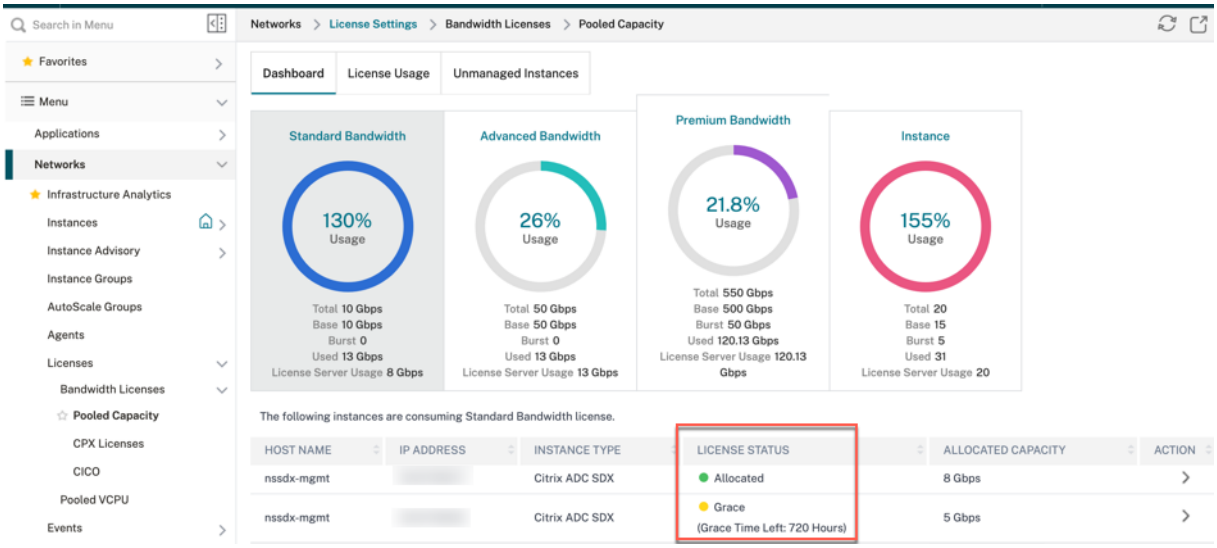
プール容量ライセンスの問題のトラブルシューティング

May 7, 2021

このセクションでは、プールされた容量の一般的な問題を分析およびトラブルシューティングする方法について説明します。

ライセンスステータスの確認

ADM は、ADC プールされたキャパシティライセンスのライセンスサーバとして機能します。ADM GUI を使用して、ライセンスのステータスを確認できます。[ネットワーク] **>** [ライセンス] **>** [プール容量] **>** [ライセンス使用] に移動します。



次の表に、ライセンスステータスの種類とその意味を示します。

ステータス	それはどういう意味ですか
割り当て済み	ライセンスの状態は問題ありません。
割り当て:ADC には適用されない	ライセンスが ADC からチェックアウトまたはチェックインされているにもかかわらず、Citrix ADC がまだ再起動されていない場合は、Citrix ADC の再起動が必要になる場合があります。
割り当てられていません	ライセンスは ADC インスタンスに割り当てられていません。
グレイス	Citrix ADC インスタンスが 30 日間のライセンス猶予期間内にある
同期中	Citrix ADM は、2 分間隔で Citrix ADC から情報をフェッチします。Citrix ADM と Citrix ADC 間のライセンスの同期には、15 分ほどかかる場合があります。Citrix ADM が再起動したか、ADM HAS フェイルオーバーがトリガーされた可能性があります。

ステータス	それはどういう意味ですか
部分的に割り当てられた	Citrix ADC は、最大割り当てで実行されている可能性があるため、割り当てられた容量を受け入れることができません。たとえば、Citrix ADC は 10 Gbps のライセンスプール容量で実行されています。ADC が再起動すると、10 Gbps が ADM ライセンスサーバーにチェックインされます。Citrix ADC がオンラインに戻ると、以前に割り当てられた 10 Gbps を自動的にチェックアウトしようとします。一方、他の ADC インスタンスがその帯域幅をチェックアウトしている可能性があります。この ADC に完全な 10 Gbps または部分的な容量を割り当てるのに十分な容量がライセンスプールにない場合、「部分割り当て」と表示されます。
管理されていない	Citrix ADC は、管理機能のために ADM に追加されません。これは Citrix ADC ライセンスには影響しませんが、ADM からのライセンス監視に影響する可能性があります。
管理されていない	Citrix ADC は、管理機能のために ADM に追加されません。これは Citrix ADC ライセンスには影響しませんが、ADM からのライセンス監視に影響する可能性があります。
接続が失われました	Citrix ADC は、管理性のため、ADM から到達できません。たとえば、ネットワーク接続の問題、NITRO が機能しない、または Citrix ADC パスワードの不一致があります。NITRO が機能しない場合、または Citrix ADC パスワードが一致しない場合、Citrix ADC のライセンスには影響しません。ただし、ADM からのライセンス監視に影響を与える可能性があります。

サーバーステータスの確認

このセクションでは、一般的なサーバーステータスの問題、考えられる理由と修正について説明します。

問題: ADC では、ライセンスサーバーが到達不能と表示され、ライセンスステータスが猶予に変わります。

- ライセンスサーバー (ADM または ADM サービスエージェント) への接続が 15 分以上切断されました。ライセンスサーバーが稼働していて、到達可能であることを確認します。
- ADC はグレースモードです。

問題: ADC は、ライセンスサーバーのステータスを到達可能と表示しますが、ユーザーが割り当てを変更しようとしても効果がありません。[割り当ての変更] をクリックすると、0 0 が返されます。この値により、構成された容量が失われたように見える場合があります。

- ライセンスサーバーへの接続は最近ダウンしましたが、ADC はまだ 2 番目のハートビートを見逃していません。したがって、それは（まだ）猶予期間ではありません。ライセンスサーバーが稼働していて、到達可能であることを確認します。

問題: ADC は容量とインスタンス数を表示しますが、ライセンスサーバーは到達可能/到達不能です。[割り当ての変更] をクリックすると、いくつかの数字が返されますが、構成済みの容量は考慮されません。

- ライセンスサーバへの接続が復元されたが、ADC が 2 回目のハートビートを逃すか、再接続プローブを送信する。

問題: ADC が ADM サービスでプールされたライセンスを構成すると、ライセンスサーバーに接続できません

- ファイアウォールルールをチェックして、ポート 27000 と 7279 が開いていることを確認します。
- エージェントは登録されていません。詳しくは、「はじめに」を参照してください。
- ADM サービスには、ライセンスファイルがアップロードされていません。詳しくは、「Citrix ADC プール容量を構成する」を参照してください。
- ADM のライセンスファイルが正しくありません。

ライセンスの使用状況レポートを確認する

ADM GUI の [ネットワーク] **>** [ライセンス] **>** [プール容量] **>** [ライセンス使用] で、ライセンス使用量の月間ピークを確認できます。このレポートを使用して、ライセンスの使用量を増やしたり、追加ライセンスの購入を計画したりできます。

次に、レポートの生成方法と使用方法の詳細を示します。

ポーリング: ライセンスデータは、15 分ごとに ADC インスタンスからポーリングされます。

1 時間あたりのピークの維持: ADM は、デバイスごとに 1 時間以内に最大ライセンス使用量のみを維持します。

レポート: 特定の時間範囲について、インスタンスごとに GUI レポートを生成できます。

エクスポート: レポートを CSV 形式または XLS 形式でエクスポートできます。

パージ**:ADM** は、毎月最初の午前 **12** 時 **10** 分にデータをパージします。パージ期間は構成可能です（デフォルトの期間は 2 か月です）。

プールされたキャパシティライセンスのカウンタと統計

次のカウンタ、ログ、およびコマンドは、プールライセンスモードでの ADM および ADC インスタンスの両方の動作を示す Citrix ADC プールライセンスメトリックを公開します。

- **SNMP** トラップ: ADC バージョン 13.xx から利用可能。

- レート制限用の **NSCONMSG** カウンタ: ADC バージョン 12.1 57.xx から使用可能
- **ADM** カウンタ ADM コマンドアクションは、Citrix ADC クラウドサービスで使用できます。

SNMP トラップ

次の SNMP トラップ v.13 プールライセンスアラームを構成できます

- `POOLED-LICENSE-CHECKOUT-FAILURE`
- `POOLED-LICENSE-ONGRACE`
- `Configure POOLED-LICENSE-PARTIAL`

これらのアラームの詳細については、Citrix ADC SNMP OID リファレンスを参照してください。

NSCONMSG カウンター

`NCCONMSG` 次のカウンターとその意味を確認します。

- `allnic_err_rl_cpu_pkt_drops`: CPU 制限に達した後に集約 (すべての NIC) パケットドロップ
- `allnic_err_rl_pps_pkt_drops`: 集約パケットは、pps 制限後にシステム全体でドロップします
- `allnic_err_rl_rate_pkt_drops`: 総レートがシステム全体にわたって低下する
- `allnic_err_rl_pkt_drops`: レート、pps、CPU による累積レート制限のドロップ
- `rl_tot_ssl_rl_enforced`: SSL RL が適用された回数 (新しい SSL 接続で)
- `rl_tot_ssl_rl_data_limited`: SSL スループット制限に達した回数
- `rl_tot_ssl_rl_sess_limited`: SSL TPS の制限に達した回数

ADM カウンタ

[コマンドアクションの実行] イベントアクションを選択すると、特定のフィルタ条件に一致するイベントに対して Citrix ADM で実行できるコマンドまたはスクリプトを作成できます。
[コマンドアクションを実行] スクリプトには、次のパラメータを設定することもできます。

パラメーター	説明
$source	このパラメーターは、受信したイベントのソース IP アドレスに相当します。
$category	このパラメーターは、フィルターのカテゴリで定義されているトラップのタイプに対応します。

パラメーター	説明
$entity	このパラメーターは、イベント生成の対象となるエンティティのインスタンスまたはカウンターに相当します。このパラメーターには、しきい値関連のイベントではカウンター名、エンティティ関連のイベントではエンティティ名、すべての証明書関連のイベントでは証明書名が含まれます。
$severity	このパラメーターは、イベントの重要度に相当します。
$failureobj	エラーオブジェクトはイベントの処理方法に影響を与え、通知されたとおりの問題がエラーオブジェクトに反映されるようにします。このオブジェクトを使用すると、単にイベントをありのままレポートするのではなく、問題を素早く突き止めてエラーの原因を特定することができます。

> 注
>
> コマンドの実行中、これらのパラメータは実際の値に置き換えられます。

Citrix ADC VPX チェックインとチェックアウトのライセンス

May 7, 2021

Citrix Application Delivery Management（ADM）からオンデマンドで Citrix ADC VPX インスタンスに VPX ライセンスを割り当てることができます。ライセンスは、拡張性と自動化されたライセンスプロビジョニングを提供するライセンスフレームワークを備えた Citrix ADM によって保存および管理されます。Citrix ADC VPX インスタンスは、Citrix ADC VPX インスタンスがプロビジョニングされたときに Citrix ADM からライセンスをチェックアウトしたり、インスタンスが削除または破棄されたときに Citrix ADM にライセンスをチェックインし直すことができます。

> 前提条件：次の前提条件が満たされていることを確認します。
>
> ソフトウェアバージョン 12.0 を実行している Citrix ADC VPX イメージを使用しています。
> 例：NSVPX-ESX-12.0-xx.xx_nc.zip。

Citrix ADM にライセンスをインストールする

Citrix ADM にライセンスファイルをインストールするには：

1. [ネットワーク] > [ライセンス] に移動し、[ライセンスファイルを追加] をクリックします。

2. [License Files] セクションで次のオプションのいずれかを選択します。

   - ローカルコンピュータからのライセンスファイルのアップロード-ローカルコンピュータにライセンスファイルがすでに存在する場合は、Citrix ADM にアップロードできます。

   ライセンスファイルを追加するには、[参照] をクリックし、追加するライセンスファイル (.lic) を選択します。次に、[完了] をクリックします。

   - ライセンスアクセスコードを使用する-購入したライセンスのライセンスアクセスコードを電子メールで送信します。

   ライセンスファイルを追加するには、テキストボックスにライセンスアクセスコードを入力し、[Get Licenses] をクリックします。

   > 注:
   >
   > ライセンスアクセスコードを使用してライセンスをインストールする前に、インターネットに接続していることを確認してください。

確認

Citrix ADM では、使用可能なライセンスおよび割り当て済みライセンスを表示できます。

ライセンスを表示するには

1. [ネットワーク] > [ライセンス] > [帯域幅ライセンス] > [**VPX** ライセンス] に移動します。

   割り当て済みのライセンスは、利用可能なライセンスのセクションの下の表で表示できます。

ADC GUI を使用して **VPX** ライセンスを **Citrix ADC VPX** インスタンスに割り当てる

1. Citrix ADC VPX インスタンスにログインし、[システム] **>** [ライセンス] **>** [ライセンスの管理] の順に選択し、[新しいライセンスの追加] をクリックして、[リモートライセンスの使用] を選択します。
2. [サーバ名**/IP** アドレス**]** フィールドに、ライセンスサーバの詳細を入力します。

   > 注:
   >
   > Citrix ADM を使用してインスタンスの VPX ライセンスを管理する場合は、[**NetScaler MA Service** 登録] チェックボックスをオンにして、Citrix ADM 資格情報を入力します。

3. [続行] をクリックします。
4. [ライセンスの割り当て] ウィンドウで、ライセンスのタイプを選択します。このウィンドウには、使用可能な仮想 CPU の合計と、割り当て可能な CPU が表示されます。[ライセンスの取得] をクリックします。
5. 次のページで [**Reboot**] をクリックして、ライセンスを申請します。

> 注:
>
> 現在のライセンスをリリースして、別のエディションからチェックアウトすることもできます。たとえば、インスタンスで Standard Edition ライセンスをすでに実行しているとします。そのライセンスをリリースしてから、Advanced Edition からチェックアウトできます。

6. **[** システム**] >[**ライセンス**] > [** ライセンスの管理**]** に移動して、**[**割り当ての変更**]** または **[**割り当ての解除**]** を選択すると、ライセンス割り当てを変更または解放できます。
7. [割り当ての変更] をクリックすると、ポップアップウィンドウに、ライセンスサーバで使用可能なライセンスが表示されます。必要なライセンスを選択し、[ライセンスを取得] をクリックします。

ADC CLI を使用して **Citrix ADC VPX** インスタンスに **VPX** ライセンスを割り当てる

1. SSH クライアントで、Citrix ADC インスタンスの IP アドレスを入力し、管理者の資格情報を使用してログオンします。
2. ライセンスサーバーを追加するには、次のコマンドを入力します。

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    port number >]
<!--NeedCopy-->
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. ライセンスサーバで使用可能なライセンスを表示するには、次のコマンドを入力します。

```
sh licenseserverpool
<!--NeedCopy-->
```



```
> sh licenseserverpool
        Instance Total                      : 0
        Instance Available                  : 0
        Standard Bandwidth Total            : 0 Mbps
        Standard Bandwidth Availabe         : 0 Mbps
        Enterprise Bandwidth Total          : 0 Mbps
        Enterprise Bandwidth Available      : 0 Mbps
        Platinum Bandwidth Total            : 0 Mbps
        Platinum Bandwidth Available        : 0 Mbps
        VPX25S Total                        : 1
        VPX25S Available                    : 1
        VPX200E Total                       : 1
        VPX200E Available                   : 1
        VPX1000S Total                      : 1
        VPX1000S Available                  : 1
        VPX8000E Total                      : 2
        VPX8000E Available                  : 1
 Done
```

4. VPX インスタンスにライセンスを割り当てるには、次のコマンドを入力します。

```
set capacity  -platform V[S/E/P][Bandwidth]
<!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

Citrix ADC VPX チェックイン/チェックアウトライセンスの有効期限チェックを構成する

Citrix ADC VPX ライセンスのライセンス有効期限のしきい値を構成できるようになりました。しきい値を設定することで、ライセンスの有効期限が切れると、Citrix ADM が電子メールまたは SMS で通知を送信します。Citrix ADM でライセンスの有効期限が切れた場合も、SNMP トラップと通知が送信されます。

ライセンス有効期限の通知が送信されると、イベントが生成され、このイベントは Citrix ADM で表示できます。

ライセンスの有効期限チェックを設定するには

1. [ネットワーク] > [ライセンス] に移動します。
2. [ライセンス設定] ページの [ライセンスの有効期限情報] セクションで、期限切れになるライセンスの詳細を確認できます。
   - 機能：有効期限が切れる予定のライセンスのタイプ。
   - Count: 影響を受ける仮想サーバーまたはインスタンスの数。

- 有効期限までの日数: ライセンスの有効期限までの日数。

3. [通知設定] セクションで、[編集] アイコンをクリックし、アラートのしきい値を指定します。プールされたライセンス容量の割合を設定して、管理者に通知することができます。
4. 適切なチェックボックスをオンにして、送信する通知のタイプを選択します。通知の種類を次に示します。
    - メールプロファイル: メールサーバーとプロファイルの詳細を指定します。ライセンスの有効期限が近づくと、メールがトリガーされます。
    - SMS プロファイル: ショートメッセージサービス (SMS) サーバーとプロファイルの詳細を指定します。ライセンスの有効期限が近づくと、SMS メッセージがトリガーされます。
    - Slack: slack チャネルを指定します。ライセンスの有効期限が近づくと、通知が送信されます。
5. 次に、ライセンスの有効期限が切れるまでの通知の受信を開始する日数を指定します。
6. ［保存］をクリックします。

Citrix ADC 仮想 CPU ライセンス

May 7, 2021

お客様のようなデータセンター管理者は、より低いコストと高い拡張性を提供しながら、ネットワーク機能をシンプル化する新しいテクノロジーに移行しています。新しいデータセンターのアーキテクチャには、少なくとも次の機能が含まれている必要があります。

- ソフトウェア定義ネットワーキング（SDN）
- ネットワーク機能の仮想化 (NFV)
- ネットワーク仮想化（NV）
- マイクロサービス

このような動きでは、絶えず変化するビジネスニーズを満たすために、ソフトウェア要件が動的、柔軟性、俊敏性であることが必要です。ライセンスは、使用状況を完全に把握できる中央管理ツールによって管理されることも期待されています。

Citrix ADC VPX の仮想 CPU ライセンス

以前は、Citrix ADC VPX ライセンスは、インスタンスによる帯域幅消費に基づいて割り当てられていました。Citrix ADC VPX は、バインドされているライセンスエディションに基づいて、特定の帯域幅やその他のパフォーマンス指標を使用するように制限されています。使用可能な帯域幅を増やすには、より多くの帯域幅を提供するライセンスエディションにアップグレードする必要があります。特定のシナリオでは、帯域幅の要件は少なくなりますが、SSL TPS、圧縮スループットなど、他の L7 パフォーマンスの要件はより多くなります。このような場合には、Citrix ADC VPX

ライセンスのアップグレードが適切でない場合があります。ただし、CPU 負荷の高い処理に必要なシステムリソースのロックを解除するには、帯域幅が大きいライセンスを購入する必要があります。Citrix Application Delivery Management（ADM）では、仮想 CPU 要件に基づいて、Citrix ADC インスタンスへのライセンスの割り当てがサポートされるようになりました。

仮想 CPU 使用量ベースのライセンス機能では、特定の Citrix ADC VPX が資格を持つ CPU の数がライセンスに指定されます。そのため、Citrix ADC VPX は、ライセンスサーバー上で実行されている仮想 CPU の数だけライセンスをチェックアウトできます。Citrix ADC VPX は、システムで実行されている CPU の数に応じてライセンスをチェックアウトします。Citrix ADC VPX は、ライセンスのチェックアウト中にアイドル状態の CPU を考慮しません。
プールされたライセンス容量と CICO ライセンス機能と同様に、Citrix ADM ライセンスサーバーは個別の仮想 CPU ライセンスを管理します。また、仮想 CPU ライセンスで管理されるエディションは、スタンダード、アドバンス、プレミアムの 3 つのエディションです。これらのエディションは、帯域幅ライセンスのエディションでロック解除された機能と同じ機能のセットをロック解除します。

仮想 CPU の数が変更されたり、ライセンスエディションに変更があったりすることがあります。このような場合、新しいライセンスのセットのリクエストを開始する前に、常にインスタンスをシャットダウンする必要があります。ライセンスをチェックアウトした後、Citrix ADC VPX を再起動します。

GUI を使用して **Citrix ADC VPX** でライセンスサーバーを構成するには

1. Citrix ADC VPX で、［システム］>［ライセンス］に移動し、［ライセンスの管理］をクリックします。
2. [ライセンス] ページで、[新しいライセンスの追加] をクリックします。
3. [ライセンス] ページで、[リモートライセンスを使用する] オプションを選択します。
4. [リモート ****** ライセンスモード**]** リストから **[CPU** ライセンス ******] を選択します。
5. ライセンスサーバーの IP アドレスとポート番号を入力します。
6. ［続行］をクリックします。

   > 注:
   >
   > Citrix ADC VPX インスタンスは常に Citrix ADM に登録します。まだ実行していない場合は、Citrix ADM で登録］を有効にして、Citrix ADM のログイン資格情報を入力します。

7. [ライセンスの割り当て] ウィンドウで、ライセンスのタイプを選択します。このウィンドウには、使用可能な仮想 CPU の合計と、割り当て可能な CPU が表示されます。[ライセンスの取得] をクリックします。

   > 注:
   >
   > ADC HA ペアの場合は、仮想 CPU ライセンスを各ノードに個別に割り当てます。

8. 次のページで [**Reboot**] をクリックして、ライセンスを申請します。

   > 注**:**
   >
   > 現在のライセンスをリリースして、別のエディションからチェックアウトすることもできます。たとえ

> ば、インスタンスで既に Standard Edition ライセンスを実行しているとします。そのライセンスをリリースしてから、アドバンスドエディションからチェックアウトできます。

インスタンス設定

May 7, 2021

検出されたインスタンスを Citrix ADM サービスで管理し、インスタンスのバックアップ設定を構成できます。

インスタンス設定の管理

インスタンス管理では、次のインスタンス構成を変更できます。

- インスタンスとの通信 -Citrix ADM サービスと検出されたインスタンス間の HTTP または HTTPS 通信チャネルを選択できます。
- 証明書のダウンロードを有効にする -検出されたインスタンスから SSL 証明書をダウンロードできます。
- インスタンスログインの資格情報の確認 -Citrix ADM GUI を使用してインスタンスにアクセスすると、インスタンスのログインページが表示されます。インスタンスにアクセスするためのログイン認証情報を指定します。

インスタンスのバックアップ設定の構成

[インスタンスバックアップ設定］で、Citrix ADM で検出された ADC インスタンスのバックアップ設定を構成できます。

[インスタンスバックアップ設定の構成] で、[インスタンスバックアップを有効にする] を選択します。

- バックアップセキュリティ設定 -バックアップファイルを暗号化して、バックアップファイル内のすべての機密情報を安全にします。バックアップファイルを暗号化するには、[ファイルのパスワード保護] を選択します。

  > 注:
  >
  > 暗号化されたバックアップファイルをダウンロードしても、ファイルは Citrix ADM GUI またはテキストエディターで開かれません。このファイルは、Citrix ADM でのみ取得および使用できます。ただし、システム上で暗号化されていないバックアップファイルを開くことはできます。
  >
  > 暗号化されたバックアップファイルを復元するには、バックアップファイルを暗号化するために言及したパスワードを指定します。

- バックアップスケジュール設定-インスタンスバックアップは、次の 2 つの方法でスケジュールできます。
  - 間隔ベース -指定した間隔が経過すると、Citrix ADM でバックアップファイルが作成されます。デフォルトのバックアップ間隔は 12 時間です。
  - ［時間ベース］: Citrix ADM でインスタンスのバックアップを実行する時刻を`hours:minutes`フォーマットで指定します。

- **Citrix ADC** 設定 -このオプションを使用すると、トラップに基づいてバックアップを開始し、GeoDB ファイルをバックアップに含めることができます。この設定は、MPX、VPX、CPX、および BLX インスタンスに適用されます。
  - **NetScalerConfigSave** トラップを受信したときにインスタンスをバックアップする-デフォルトでは、**Citrix ADM** は「NetScalerConfigSave」トラップを受信したときにバックアップファイルを作成しません。ただし、Citrix ADC インスタンスが Citrix ADM に `NetScalerConfigSave` トラップを送信するたびに、バックアップファイルを作成するオプションを有効にできます。

    Citrix ADC インスタンスは、インスタンスの構成が保存されるたびに`NetScalerConfigSave`を送信します。

    トラップのバックアップ遅延を分単位で指定します。受信した`NetScalerConfigSave`トラップが Citrix ADM 上で指定された分間持続する場合、Citrix ADM はインスタンスをバックアップします。
  - **GeoDB** ファイルを含める -デフォルトでは、Citrix ADM はジオデータベースファイルをバックアップしません。このオプションを有効化して、これらのファイルもバックアップファイルを作成することができます。
- **Citrix SDX** 設定 -SDX インスタンスをバックアップするには、［バックアップタイムアウト］を分単位で指定します。SDX インスタンスのバックアップ中、ADM と SDX 間の接続は指定された期間保持されます。

  SDX インスタンスバックアップファイルのサイズが大きい場合は、SDX インスタンスのバックアップを完了するために、ADM と SDX インスタンスの間の接続をより長い期間維持する必要があります。

  > 重要:
  >
  > 接続がタイムアウトすると、バックアップは失敗します。
- 外部転送 -Citrix ADM では、Citrix ADC インスタンスのバックアップファイルを外部の場所に転送できます。
  1. ロケーションの IP アドレスを指定します。
  2. バックアップファイルの転送先となる外部サーバのユーザ名とパスワードを指定します。
  3. 転送プロトコルとポート番号を指定します。
  4. ファイルを格納するディレクトリパスを指定します。
  5. 外部サーバーにファイルを転送した後にバックアップファイルを削除する場合は、[転送後に **Application Delivery Management** からファイルを削除する] を選択します。

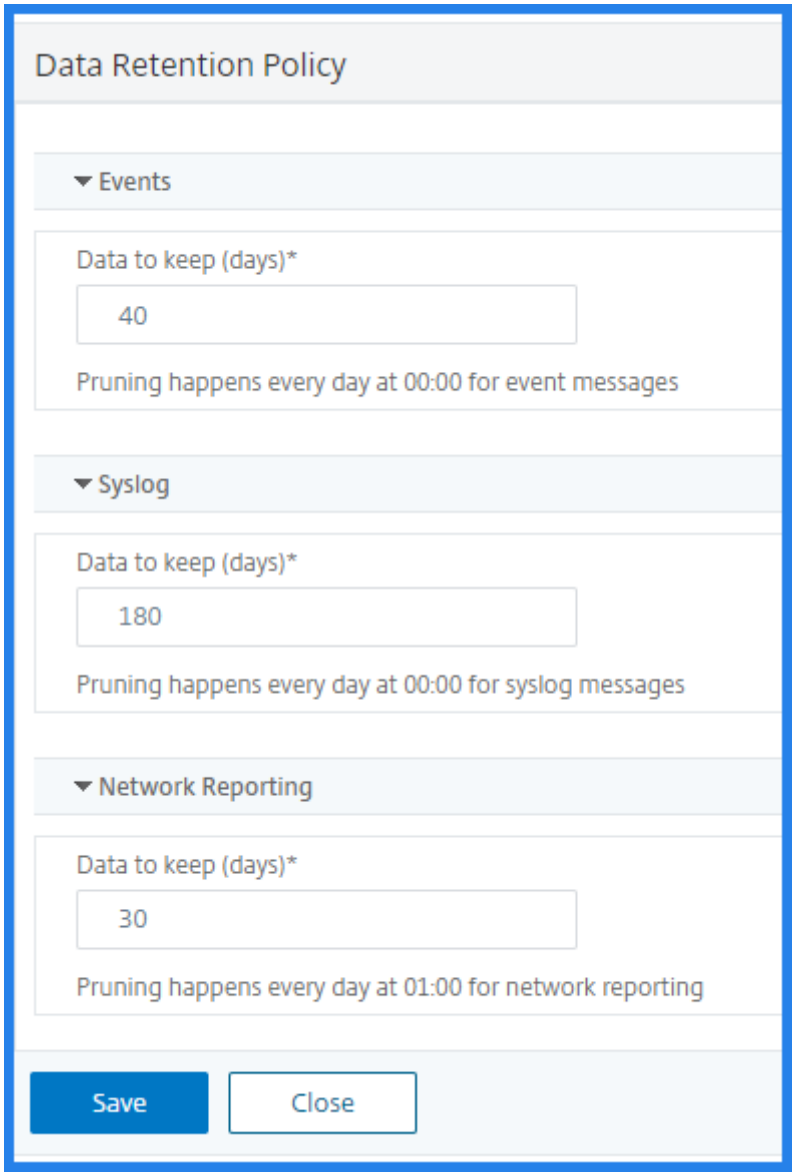
データ保持ポリシー

May 7, 2021

ADM サービスでは、システムイベント、syslog メッセージ、およびネットワークレポートデータに、特定の期間アクセスできます。

1. [設定] **>** [データ保持ポリシー] の順に選択し、データ保持を構成します。
2. [編集] ボタンをクリックします。
3. ADM サービスでデータを保持するには、次のオプションに日を指定します。

オプション	説明
イベント	ADM サービスに保存されるイベントメッセージを 40 日までに制限できます。イベントは、リテンションポリシーの期限が切れた後に ADM から削除されます。クリアされたイベントは 1 日後に削除されます。詳しくは、「イベント」を参照してください。
Syslog	データベースに保存される syslog データの量を最大 180 日に制限できます。詳しくは、「インスタンスでの syslog の設定」を参照してください。
ネットワークレポート作成	Citrix ADM に保存されるネットワークレポートデータを最大 30 日間に制限できます。詳しくは、「ネットワークレポート作成」を参照してください。



> 重要:
>
> Express アカウントでは、データ保存ポリシーを編集することはできません。
>
> アカウントを Express アカウントに変換すると、ADM サービスは最大 500 MB または 1 日のデータのいずれか小さい方のストレージデータを保持します。詳しくは、「Express アカウントを使用して Citrix ADM リソースを管理する」を参照してください。

インスタンス設定

May 7, 2021

検出されたインスタンスを Citrix ADM サービスで管理し、インスタンスのバックアップ設定を構成できます。

インスタンス設定の管理

インスタンス管理では、次のインスタンス構成を変更できます。

- インスタンスとの通信 -Citrix ADM サービスと検出されたインスタンス間の HTTP または HTTPS 通信チャネルを選択できます。
- 証明書のダウンロードを有効にする -検出されたインスタンスから SSL 証明書をダウンロードできます。
- インスタンスログインの資格情報の確認 -Citrix ADM GUI を使用してインスタンスにアクセスすると、インスタンスのログインページが表示されます。インスタンスにアクセスするためのログイン認証情報を指定します。

インスタンスのバックアップ設定の構成

[インスタンスバックアップ設定] で、Citrix ADM で検出された ADC インスタンスのバックアップ設定を構成できます。

[インスタンスバックアップ設定の構成] で、[インスタンスバックアップを有効にする] を選択します。

- バックアップセキュリティ設定 -バックアップファイルを暗号化して、バックアップファイル内のすべての機密情報を安全にします。バックアップファイルを暗号化するには、[ファイルのパスワード保護] を選択します。

  > 注:
  >
  > 暗号化されたバックアップファイルをダウンロードしても、ファイルは Citrix ADM GUI またはテキストエディターで開かれません。このファイルは、Citrix ADM でのみ取得および使用できます。ただし、システム上で暗号化されていないバックアップファイルを開くことはできます。
  >
  > 暗号化されたバックアップファイルを復元するには、バックアップファイルを暗号化するために言及したパスワードを指定します。

- バックアップスケジュール設定-インスタンスバックアップは、次の 2 つの方法でスケジュールできます。
  - 間隔ベース -指定した間隔が経過すると、Citrix ADM でバックアップファイルが作成されます。デフォルトのバックアップ間隔は 12 時間です。
  - [時間ベース]: Citrix ADM でインスタンスのバックアップを実行する時刻を`hours:minutes`フォーマットで指定します。
- **Citrix ADC** 設定 -このオプションを使用すると、トラップに基づいてバックアップを開始し、GeoDB ファイルをバックアップに含めることができます。この設定は、MPX、VPX、CPX、および BLX インスタンスに適用されます。
  - **NetScalerConfigSave** トラップを受信したときにインスタンスをバックアップする**-**デフォルトでは、**Citrix ADM** は「NetScalerConfigSave」トラップを受信したときにバックアップファイルを作成しません。ただし、Citrix ADC インスタンスが Citrix ADM に `NetScalerConfigSave` トラップを送信するたびに、バックアップファイルを作成するオプションを有効にできます。

    Citrix ADC インスタンスは、インスタンスの構成が保存されるたびに`NetScalerConfigSave`を送信します。

トラップのバックアップ遅延を分単位で指定します。受信したNetScalerConfigSaveトラップがCitrix ADM 上で指定された分間持続する場合、Citrix ADM はインスタンスをバックアップします。

- **GeoDB** ファイルを含める -デフォルトでは、Citrix ADM はジオデータベースファイルをバックアップしません。このオプションを有効化して、これらのファイルもバックアップファイルを作成することができます。

- **Citrix SDX** 設定 -SDX インスタンスをバックアップするには、［バックアップタイムアウト］を分単位で指定します。SDX インスタンスのバックアップ中、ADM と SDX 間の接続は指定された期間保持されます。

  SDX インスタンスバックアップファイルのサイズが大きい場合は、SDX インスタンスのバックアップを完了するために、ADM と SDX インスタンスの間の接続をより長い期間維持する必要があります。

  > 重要：
  >
  > 接続がタイムアウトすると、バックアップは失敗します。

- 外部転送 -Citrix ADM では、Citrix ADC インスタンスのバックアップファイルを外部の場所に転送できます。

  1. ロケーションの IP アドレスを指定します。
  2. バックアップファイルの転送先となる外部サーバのユーザ名とパスワードを指定します。
  3. 転送プロトコルとポート番号を指定します。
  4. ファイルを格納するディレクトリパスを指定します。
  5. 外部サーバーにファイルを転送した後にバックアップファイルを削除する場合は、[転送後に **Application Delivery Management** からファイルを削除する] を選択します。

システム構成

May 7, 2021

ADM エージェントのキープアライブ間隔と Citrix ADM サーバーのタイムゾーンを変更できます。

エージェントのキープアライブ間隔を設定する

Citrix ADM サーバーとエージェントは、指定されたキープアライブ間隔の間同じ TCP 接続を維持します。エージェントはこの接続を使用して、管理対象インスタンスのデータを ADM サーバーに送信します。

1. [設定**] > [**システム設定**]** に移動します。
2. [システム構成] で [エージェントとタイムゾーン] を選択します。
3. [**Agent**] で、キープアライブ間隔を 30 ～120 秒の間で指定します。
4. ［保存］をクリックします。

Citrix ADM タイムゾーンを設定する

ADM Web ページ、通知、レポートに時刻を表示するタイムゾーンを選択できます。

1. [設定] > [システム設定] に移動します。
2. [システム構成] で [エージェントとタイムゾーン] を選択します。
3. [タイムゾーン] で、[ローカル] または [GMT タイムゾーン] を選択して、ADM に時刻を表示します。
4. [保存] をクリックします。

ADM 機能の有効化または無効化

May 7, 2021

管理者は、[システム設定] > [構成可能な機能] ページで次の機能を有効または無効にできます。

- エージェントのフェイルオーバー：エージェントのフェイルオーバーは、複数のアクティブなエージェントがあるサイトで実行できます。サイト内でエージェントが非アクティブ（DOWN 状態）になると、Citrix ADM サービスは、非アクティブなエージェントの ADC インスタンスを他のアクティブなエージェントに再配布します。詳しくは、「マルチサイト展開用に Citrix ADM エージェントを構成する」を参照してください。
- エンティティ・ポーリング・ネットワーク機能 -エンティティは、ADC インスタンスにアタッチされたポリシー、仮想サーバ、サービス、またはアクションのいずれかです。デフォルトでは、Citrix ADM は 60 分ごとに構成済みのネットワーク機能エンティティを自動的にポーリングします。詳しくは、「ポーリングの概要」を参照してください。
- インスタンスのバックアップ -Citrix ADC インスタンスの現在の状態をバックアップし、後でバックアップしたファイルを使用して ADC インスタンスを同じ状態に復元します。詳しくは、「Citrix ADC インスタンスのバックアップと復元」を参照してください。
- インスタンス構成の監査 -管理対象の Citrix ADC インスタンスの構成変更を監視し、構成エラーのトラブルシューティングを行い、未保存の構成を復元します。詳しくは、「監査テンプレートの作成」を参照してください。
- インスタンスイベント-イベントは、管理対象 Citrix ADC インスタンスでのイベントまたはエラーの発生を表します。Citrix ADM で受信したイベントは、[イベントの概要] ページ（[ネットワーク] > [イベント]）に表示されます。また、すべてのアクティブなイベントが [イベントメッセージ] ページ ([ネットワーク] > [イベント] > [イベントメッセージ]) に表示されます。詳しくは、「イベント」を参照してください。
- インスタンスネットワークレポート -グローバルレベルでインスタンスのレポートを生成できます。また、仮想サーバーやネットワークインターフェイスなどのエンティティ用。詳しくは、「ネットワークレポート作成」を参照してください。
- インスタンス SSL 証明書 -Citrix ADM では、管理対象のすべての Citrix ADC インスタンスにインストールされた SSL 証明書を一元的に表示できます。詳しくは、「SSL ダッシュボード」を参照してください。

- インスタンス **Syslog** -すべての syslog メッセージを Citrix ADCitrix ADM にリダイレクトするようにデバイスを構成している場合は、Citrix ADC インスタンスで生成された syslog イベントを監視できます。詳しくは、「インスタンスでの syslog の設定」を参照してください。

機能を有効にするには、次の手順を実行します。

1. リストから有効にする機能を選択します。
2. [有効] をクリックします。

> 重要:
>
> 機能が無効になっている場合、ユーザーはその機能に関連付けられた操作を実行できません。

HAProxy インスタンスの管理と監視

May 7, 2021

Citrix Application Delivery Management（ADM）は、HAProxy バージョン 1.4.24 以降をサポートしています。HAProxy インスタンスをプロビジョニングしたホストを Citrix ADM に追加すると、ホスト上の HAProxy インスタンスが検出され、それらの管理および監視が可能になります。Citrix ADM では、インスタンス上の HAProxy 構成に関する次の種類の情報が表示されます。

- フロントエンド：リクエストをバックエンドに転送する方法を定義します。これらは、トラフィックの負荷分散を行う Citrix ADM で検出されたエンティティです。
- バックエンド — 転送された要求を受信するサーバーのセット。
- Servers – HAProxy によりトラフィックの負荷分散が行われるサーバー

詳しくは、「http://www.haproxy.org/download/1.7/doc/configuration.txt」を参照してください。

Citrix ADM には、リアルタイムでフロントエンドを監視できる HAProxy アプリダッシュボードが用意されています。詳細については、「HAProxy アプリダッシュボード」を参照してください。また、HAProxy インスタンスで構成されたフロントエンド、バックエンド、サーバーの詳細を表示することもできます。

HAProxy ホスト上の HAProxy インスタンスを管理および監視するには、HAProxy ホストを Citrix ADM に追加する必要があります。詳しくは、「HAProxy インスタンスの追加」を参照してください。

関連情報

- HAProxy アプリのダッシュボード
- HAProxy インスタンスの監視
- HAProxy インスタンスで構成されたフロントエンドの詳細を表示する
- HAProxy インスタンスで設定されたバックエンドの詳細を表示する
- HAProxy インスタンスで設定されたサーバーの詳細の表示
- フロントエンドまたはサーバーの数が最も多い HAProxy インスタンスを表示する

- HAProxy インスタンスを再起動する

AWS での Citrix ADC VPX インスタンスのプロビジョニング

May 7, 2021

アプリケーションをクラウドに移動すると、アプリケーションの一部であるコンポーネントが増え、分散が増え、動的に管理する必要があります。

AWS 上の Citrix ADC VPX インスタンスを使用すると、L4-L7 ネットワークスタックを AWS にシームレスに拡張できます。Citrix ADC VPX により、AWS はオンプレミスの IT インフラストラクチャの自然な拡張となります。AWS で Citrix ADC VPX を使用すると、世界で最も要求の厳しいウェブサイトやアプリケーションをサポートする同じ最適化、セキュリティ、制御機能と、クラウドの伸縮自在性と柔軟性を組み合わせることができます。

Citrix ADC インスタンスを監視する Citrix Application Delivery Management（ADM）により、アプリケーションの正常性、パフォーマンス、およびセキュリティを可視化できます。ハイブリッドマルチクラウド環境全体で、アプリケーション配信インフラストラクチャのセットアップ、デプロイ、管理を自動化できます。

AWS 用語

以下のセクションでは、このドキュメントで使用される AWS 用語の簡単な説明を示します。

用語	定義
Amazon Machine Image (AMI)	マシンイメージ。クラウド内の仮想サーバーであるインスタンスを起動するのに必要な情報を提供します。
Elastic Compute Cloud（EC2）	クラウドで、安全でサイズ変更できる処理能力を提供する Web サービスです。Web 規模のクラウドコンピューティングを開発者が簡単に実施できるように設計されています。
エラスティックネットワークインターフェイス (ENI)	VPC のインスタンスにアタッチできる、仮想のネットワークインターフェイスです。
インスタンスの種類	Amazon EC2 では、さまざまなユースケースに対応できるよう最適化された幅広い種類のインスタンスを提供してます。インスタンスタイプを構成する CPU、メモリ、ストレージ、およびネットワーク機能の組み合わせはさまざまで、アプリケーションに合わせて最適なリソースの組み合わせを柔軟に選択できます。

用語	定義
Identity and Access Management（IAM）ロール	AWS で ID が実行できること、または実行できないことを決定する許可ポリシーを持つ AWS の ID。IAM ロールを使うことで EC2 インスタンス上で実行されるアプリケーションが、AWS リソースに安全にアクセスできるようになります。
セキュリティグループ	あるインスタンスに対して許可されている、名前が付けられた一連の受信方向のネットワーク接続。
サブネット	EC2 インスタンスをアタッチできる VPC の IP アドレス範囲の一部分。セキュリティと運用上の必要に応じて、サブネットを作成し、インスタンスをグループ分けできます。
Virtual Private Cloud（VPC）	定義した仮想ネットワーク内で AWS リソースを起動できる、AWS クラウドの論理的に隔離されたセクションをプロビジョニングする Web サービス。

サポートされている **Citrix ADC AMI** インスタンスタイプ

より高い帯域幅では、以下のインスタンスタイプをお勧めします。

インスタンスタイプ	帯域幅
M4.X ラージ	プレミアムエディション 10 Mbps
M4.X ラージ	プレミアムエディション 200 Mbps

前提条件

このドキュメントでは、次のことを前提としています。

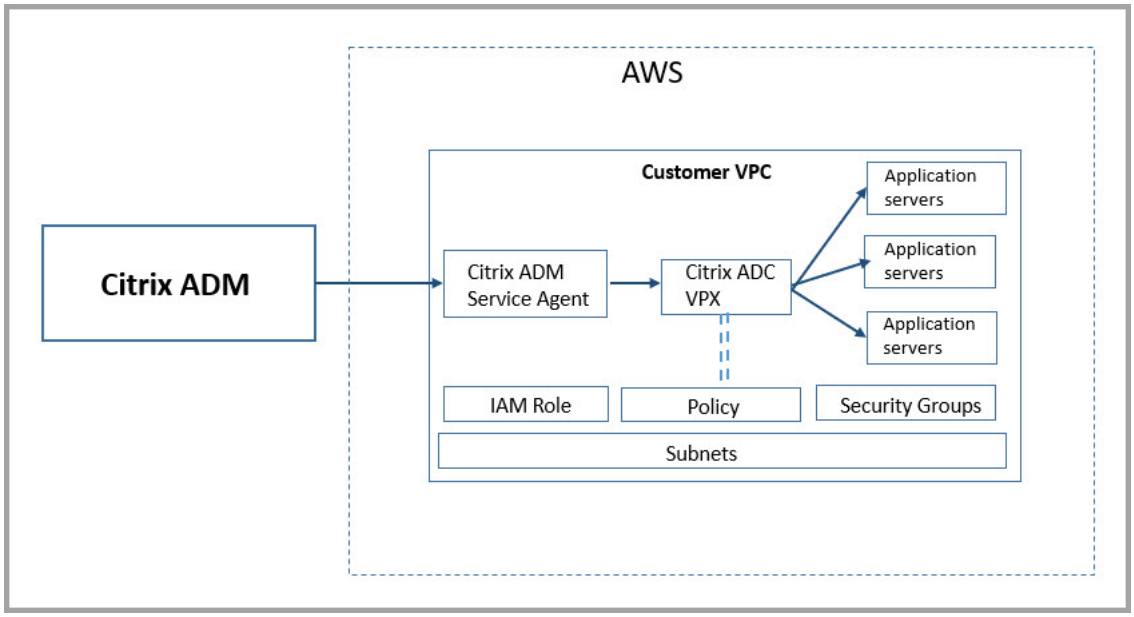
- AWS アカウントを所有している。
- 必要な VPC を作成し、アベイラビリティーゾーンを選択しました。
- AWS に Citrix ADM サービスエージェントを追加しました。

アカウントやその他のタスクの作成方法について詳しくは、「AWS ドキュメント」を参照してください。

AWS に Citrix ADM サービスエージェントをインストールする方法の詳細については、「AWS に Citrix ADM サービスエージェントをインストールする」を参照してください。

アーキテクチャ図

次の画像は、Citrix ADM を AWS に接続して AWS で Citrix ADC VPX インスタンスをプロビジョニングする方法の概要を示しています。



構成タスク

Citrix ADM で Citrix ADC VPX インスタンスをプロビジョニングする前に、AWS で以下のタスクを実行します。

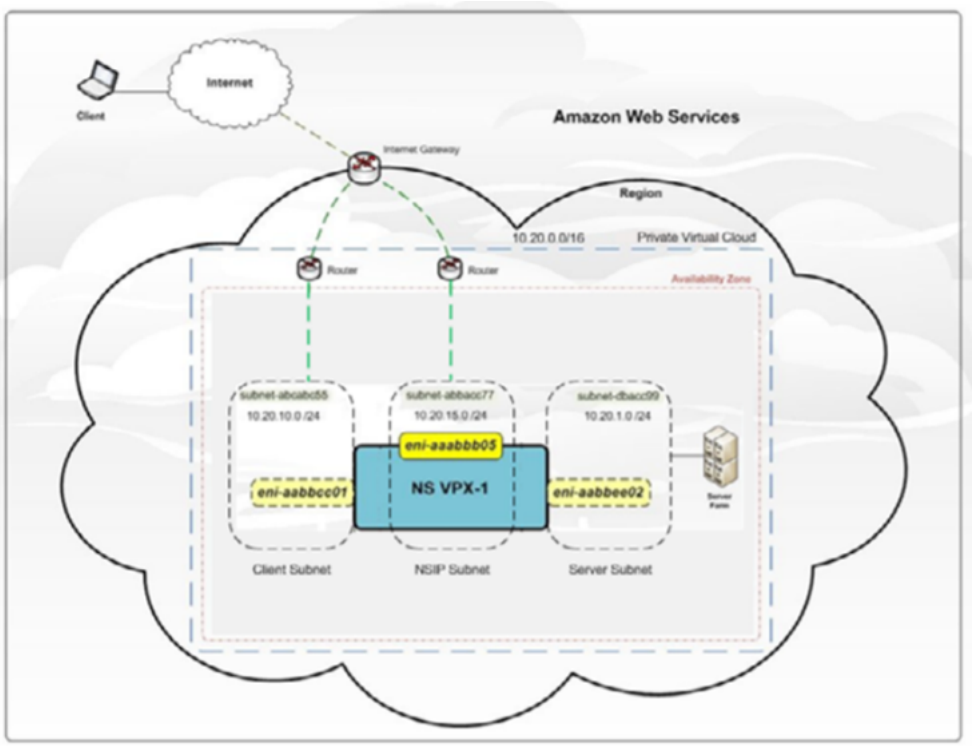
- サブネットの作成
- セキュリティグループの作成
- IAM ロールを作成し、ポリシーを定義する

AWS でインスタンスをプロビジョニングするには、Citrix ADM で以下のタスクを実行します。

- サイトを作成
- AWS での Citrix ADC VPX インスタンスのプロビジョニング

サブネットを作成するには

VPC に 3 つのサブネットを作成します。VPC で Citrix ADC VPX インスタンスをプロビジョニングするために必要なサブネットは、管理、クライアント、サーバーの 3 つです。サブネットごとに VPC で定義されている範囲から IPv4 CIDR ブロックを指定します。サブネットを配置するアベイラビリティーゾーンを指定します。同じアベイラビリティーゾーンに 3 つのサブネットをすべて作成します。次の図は、リージョンで作成された 3 つのサブネットとそのクライアントシステムへの接続を示しています。



VPC とサブネットの詳細については、VPC とサブネットを参照してください。

セキュリティグループを作成するには

セキュリティグループを作成して、Citrix ADC VPX インスタンスのインバウンドトラフィックとアウトバウンドトラフィックを制御します。セキュリティグループは、インスタンスの仮想ファイアウォールとして機能します。サブネットレベルではなく、インスタンスレベルでセキュリティグループを作成します。VPC 内のサブネット内の各インスタンスを、異なるセキュリティグループのセットに割り当てることができます。各セキュリティグループのルールを追加して、クライアントサブネットを通過してインスタンスに通過するインバウンドトラフィックを制御します。また、サーバーサブネットを通過してアプリケーションサーバーに送信するアウトバウンドトラフィックを制御する規則のセットを別個に追加することもできます。インスタンスにはデフォルトのセキュリティグループを使用できますが、グループを作成することもできます。サブネットごとに 1 つずつ、セキュリティグループを 3 つ作成します。制御する着信トラフィックと発信トラフィックの両方のルールを作成します。規則は、必要に応じていくつでも追加できます。

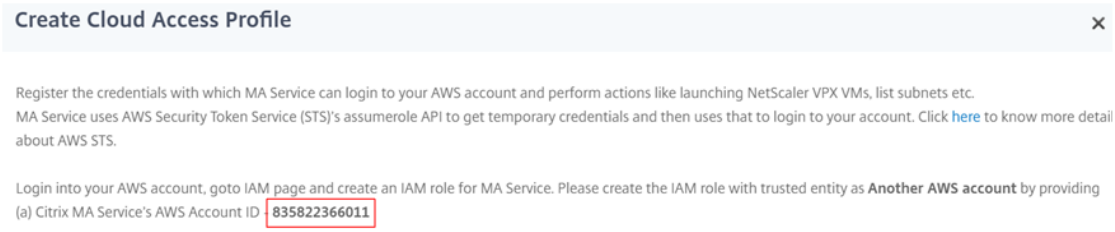
セキュリティグループの詳細については、VPC のセキュリティグループを参照してください。

IAM ロールを作成してポリシーを定義するには

IAM ロールを作成して、ユーザーと Citrix の信頼された AWS アカウント間の信頼関係を確立し、Citrix アクセス許可を使用してポリシーを作成します。

1. AWS で、[サービス] をクリックします。左側のナビゲーションペインで、[**IAM] > [**ロール] を選択し、[ロールの作成] をクリックします。
2. AWS アカウントを Citrix ADM の AWS アカウントに接続しています。そのため、[別の **AWS** アカウント] を選択して、Citrix ADM が AWS アカウントでアクションを実行できるようにします。

   12 桁の Citrix ADM AWS アカウント ID を入力します。Citrix の ID は 835822366011 である。クラウドアクセスプロファイルの作成時に、Citrix ADM で Citrix ID を確認することもできます。



3. サードパーティアカウントへの接続に外部 **ID** を要求する] を有効にします。オプションの外部識別子を必須にすることで、ロールのセキュリティを強化できます。任意の文字を組み合わせて使用できる ID を入力します。
4. [アクセス許可] をクリックします。
5. [アクセス許可ポリシーのアタッチ] ページで、[ポリシーの作成] をクリックします。
6. ポリシーを作成および編集するには、ビジュアルエディターまたは JSON を使用します。

   Citrix からのアクセス許可の一覧は、次のボックスに表示されます。

```
{

"Version": "2012-10-17",
"Statement":
[
    {

          "Effect": "Allow",
         "Action": [
             "ec2:DescribeInstances",
             "ec2:DescribeImageAttribute",
             "ec2:DescribeInstanceAttribute",
             "ec2:DescribeRegions",
             "ec2:DescribeDhcpOptions",
             "ec2:DescribeSecurityGroups",
             "ec2:DescribeHosts",
             "ec2:DescribeImages",
             "ec2:DescribeVpcs",
             "ec2:DescribeSubnets",
             "ec2:DescribeNetworkInterfaces",
             "ec2:DescribeAvailabilityZones",
```



```
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeAddresses",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeTags",
                "ec2:DescribeVolumeStatus",
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumeAttribute",
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:CreateKeyPair",
                "ec2:DeleteKeyPair",
                "ec2:ResetInstanceAttribute",
                "ec2:RunScheduledInstances",
                "ec2:ReportInstanceStatus",
                "ec2:StartInstances",
                "ec2:RunInstances",
                "ec2:StopInstances",
                "ec2:UnmonitorInstances",
                "ec2:MonitorInstances",
                "ec2:RebootInstances",
                "ec2:TerminateInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:AssignPrivateIpAddresses",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:CreateNetworkInterface",
                "ec2:AttachNetworkInterface",
                "ec2:DetachNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:ResetNetworkInterfaceAttribute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:AssociateAddress",
                "ec2:AllocateAddress",
                "ec2:ReleaseAddress",
                "ec2:DisassociateAddress",
                "ec2:GetConsoleOutput"
            ],
                "Resource": "*"
        }

]
 }

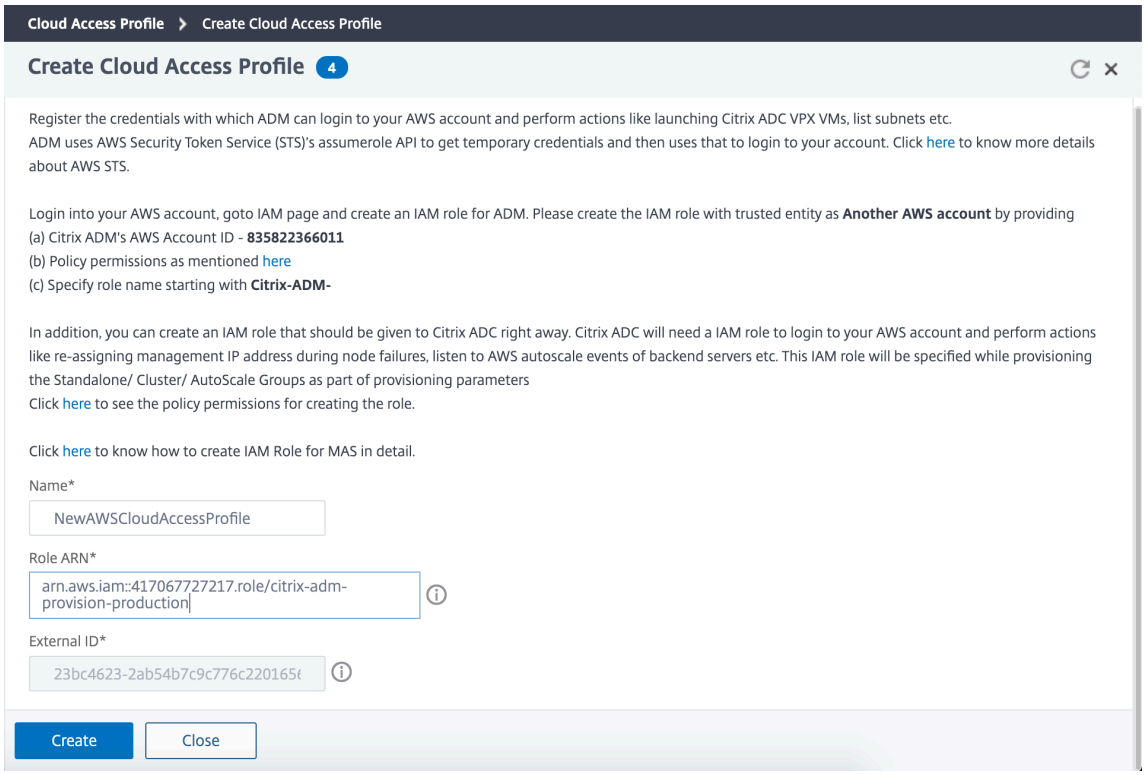
<!--NeedCopy-->
```


7. 「JSON」タブに権限のリストをコピーして貼り付け、「ポリシーの確認」をクリックします。
8. [ポリシーの確認] ページで、ポリシーの名前を入力し、説明を入力して、[ポリシーの作成] をクリックします。

Citrix ADM でサイトを作成するには

Citrix ADM でサイトを作成し、AWS ロールに関連付けられた VPC の詳細を追加します。

1. Citrix ADM で、［ネットワーク］**>**［サイト］に移動します。
2. ［追加］をクリックします。
3. サービスタイプを AWS として選択し、[既存の **VPC** をサイトとして使用] を有効にします。
4. クラウドアクセスプロファイルを選択します。
5. クラウドアクセスプロファイルがフィールドに存在しない場合は、[追加] をクリックしてプロファイルを作成します。
   a) [**Create Cloud Access Prof** ile] ページで、AWS にアクセスするプロファイルの名前を入力します。
   b) AWS で作成したロールに関連付けられた ARN を入力します。
   c) AWS で ID とアクセス管理（IAM）ロールを作成するときに指定した外部 ID を入力します。「IAM ロールを作成してポリシータスクを定義するには」の手順 4 を参照してください。AWS で指定した IAM ロール名が「Citrix-ADM-」で始まり、ロール ARN に正しく表示されることを確認します。



AWS の IAM ロールに関連付けられた VPC の詳細情報（リージョン、VPC ID、名前、CIDR ブロックなど）は、Citrix ADM にインポートされます。

6. サイトの名前を入力します。
7. ［作成］をクリックします。

AWS で **Citrix ADC VPX** をプロビジョニングするには

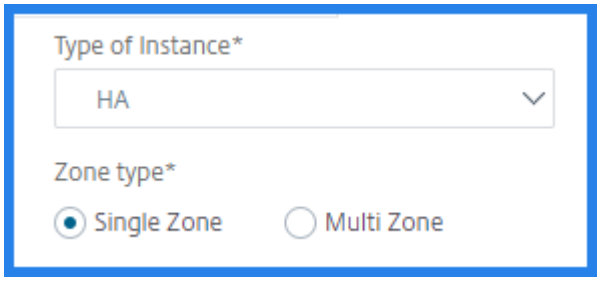
以前に作成したサイトを使用して、AWS で Citrix ADC VPX インスタンスをプロビジョニングします。Citrix ADM サービスエージェントの詳細を提供し、そのエージェントにバインドされたインスタンスをプロビジョニングします。

1. Citrix ADM で、［ネットワーク］>［インスタンス］**>**［**Citrix ADC**］に移動します。
2. [**VPX**] タブで、[プロビジョニング] をクリックします。

   このオプションでは、［クラウドでの **Citrix ADC VPX** のプロビジョニング］ページが表示されます。
3. [**Amazon Web Services (AWS)**] を選択し、[次へ] をクリックします。
4. [基本パラメータ] タブで、
   a) リストから [インスタンスのタイプ] を選択します。
      - スタンドアロン**:** このオプションは、AWS でスタンドアロン Citrix ADC VPX インスタンスをプロビジョニングします。
      - **HA:** このオプションは、AWS で高可用性 Citrix ADC VPX インスタンスをプロビジョニングします。

        Citrix ADC VPX インスタンスを同じゾーンにプロビジョニングするには、［ゾーンの種類］で［シングルゾーン］オプションを選択します。

        複数のゾーンにまたがって Citrix ADC VPX インスタンスをプロビジョニングするには、［ゾーンの種類］で［マルチゾーン］オプションを選択します。[プロビジョニングパラメータ] タブで、AWS で作成された各ゾーンのネットワークの詳細を指定します。

   b) ADC VPX インスタンスの名前を指定します。
   c) [サイト] で、以前に作成したサイトを選択します。
   d)「エージェント」で、ADC VPX インスタンスを管理するために作成されるエージェントを選択します。
   e) [クラウドアクセスプロファイル] で、サイトの作成中に作成されたクラウドアクセスプロファイルを選択します。

f) [デバイスプロファイル] で、認証を提供するプロファイルを選択します。

Citrix ADC VPX インスタンスにログオンする必要がある場合、Citrix ADM はデバイスプロファイルを使用します。

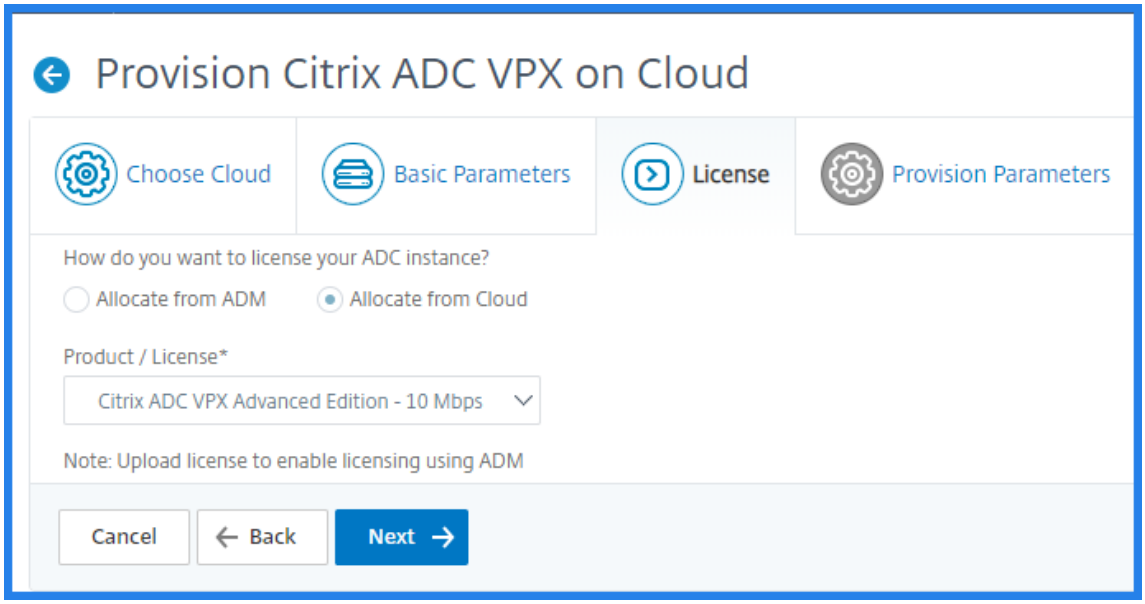
g) ［次へ］をクリックします。

5. [**License**] タブで、次のいずれかのモードを選択して ADC インスタンスにライセンスを適用します。

- **Citrix ADM** を使用する: プロビジョニングするインスタンスは、Citrix ADM からライセンスをチェックアウトします。
- **AWS** クラウドの使用: [クラウドから割り当て] オプションは、AWS マーケットプレイスで利用可能な Citrix 製品ライセンスを使用します。プロビジョニングするインスタンスは、マーケットプレイスのライセンスを使用します。

  AWS マーケットプレイスのライセンスを使用する場合は、[プロビジョニングパラメータ] タブで製品またはライセンスを指定します。

詳しくは、「ライセンス要件」を参照してください。



6. [ライセンス] タブで [**ADM** から割り当て] を選択した場合は、次のように指定します。

- ライセンスタイプ: 帯域幅または仮想 CPU ライセンスのいずれかを選択します。

  帯域幅ライセンス**:** [帯域幅ライセンスタイプ] リストから、次のいずれかのオプションを選択できます。

  - プールされた容量**:** インスタンスに割り当てる容量を指定します。

    ADC インスタンスは、共通プールから 1 つのインスタンス・ライセンスをチェックアウトし、指定された帯域幅だけを指定します。

  - **VPX** ライセンス: Citrix ADC VPX インスタンスがプロビジョニングされると、インスタンスは Citrix ADM からライセンスをチェックアウトします。

仮想 **CPU** ライセンス：プロビジョニングされた Citrix ADC VPX インスタンスは、インスタンスで実行されている CPU の数に応じてライセンスをチェックアウトします。

> 注：
>
> プロビジョニングされたインスタンスが削除または破棄されると、適用されたライセンスは Citrix ADM ライセンスプールに戻ります。これらのライセンスは、新しいインスタンスをプロビジョニングするために再利用することができます。

a) [ライセンスエディション] で、ライセンスエディションを選択します。ADM は、指定されたエディションを使用してインスタンスをプロビジョニングします。

7. ［次へ］をクリックします。

8. [プロビジョニングパラメータ] タブで、

a) AWS で作成された **Citrix IAM** ロールを選択します。IAM ロールは、AWS で ID を実行できる操作と実行できない操作を決定するアクセス権限ポリシーを持つ AWS ID です。

b) ［製品］フィールドで、プロビジョニングする Citrix ADC 製品のバージョンを選択します。

c) [インスタンスタイプ] リストから EC2 インスタンスタイプを選択します。

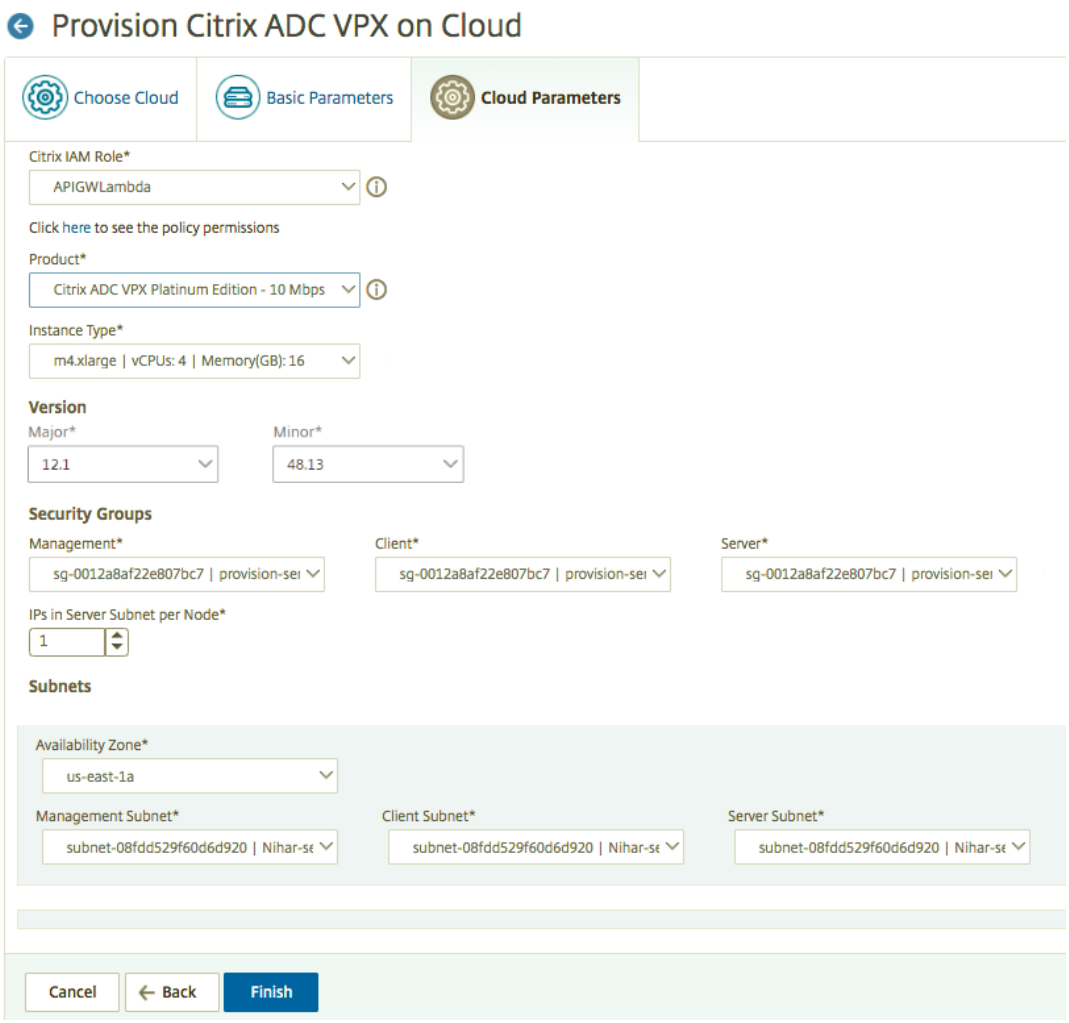
d) プロビジョニングする Citrix **ADC** のバージョンを選択します。Citrix ADC メジャーバージョンとマイナーバージョンの両方を選択します。

e) [セキュリティグループ] で、仮想ネットワークで作成した [管理]、[クライアント]、および [サーバー] セキュリティグループを選択します。

f) [ノードあたりのサーバーサブネットの IP] で、セキュリティグループのノードごとのサーバーサブネット内の IP アドレスの数を選択します。

g) [サブネット] で、AWS で作成された各ゾーンの管理、クライアント、およびサーバーのサブネットを選択します。[**Availability Zone**] リストからリージョンを選択することもできます。

h) ［完了］をクリックします。



これで、Citrix ADC VPX インスタンスが AWS でプロビジョニングされました。

> 注:
>
> 現在、Citrix ADM は AWS からの Citrix ADC インスタンスのプロビジョニング解除をサポートしていません。

AWS でプロビジョニングされた **Citrix ADC VPX** を表示するには

1. AWS ホームページから、[サービス] に移動し、[**EC2**] をクリックします。
2. [リソース] ページで、[実行中のインスタンス] をクリックします。
3. AWS でプロビジョニングされた Citrix ADC VPX を表示できます。

Citrix ADC VPX インスタンスの名前は、Citrix ADM でインスタンスをプロビジョニングするときに指定した名前と同じです。

Citrix ADM でプロビジョニングされた **Citrix ADC VPX** を表示するには

1. Citrix ADM で、［ネットワーク］>［インスタンス］**>**［**Citrix ADC**］に移動します。
2. ［**Citrix ADC VPX** ］タブを選択します。
3. AWS でプロビジョニングされた Citrix ADC VPX インスタンスは、ここに記載されています。

Citrix ADM を使用した **AWS** での **Citrix ADC** の自動スケーリング

May 7, 2021

クラウドでアプリケーションを効率的にホストすると、アプリケーションの必要に応じて、リソースを簡単にコスト効率よく管理できます。たとえば、AWS で実行されている E コマースウェブポータルがあるとします。このポータルは、アプリケーショントラフィックが急増している間に莫大な割引を提供することがあります。これらの提供中にアプリケーショントラフィックが増加した場合、アプリケーションを動的にスケールアウトする必要があり、それに応じてネットワークリソースも増加する必要があります。

Citrix ADM 自動スケーリング機能は、AWS での Citrix ADC インスタンスの Provisioning と自動スケーリングをサポートします。Citrix ADM 自動スケーリング機能は、メモリ使用量、CPU 使用量、スループットなどのしきい値パラメータを常に監視します。これらのパラメータの 1 つを選択することも、複数のパラメータを選択してモニタリングすることもできます。これらのパラメータ値は、ユーザが設定した値と比較されます。パラメータ値が制限に違反すると、それに応じてスケールアウトまたはスケールインがトリガーされます。

Citrix ADM Autoscale 機能アーキテクチャは、各 Autoscale グループのインスタンスの最小数と最大数を構成できるように設計されています。これらの番号を事前に設定すると、アプリケーションが常に起動して実行できるようになります。

> 重要:
>
> 自動スケーリングは、クラスターノード上でスポット設定を必要とする以下の機能を除き、すべての Citrix ADC 機能をサポートします。
>
> - GSLB か
> - Citrix Gateway とその機能
> - Telco 機能
>
> スポッティング設定について詳しくは、ストライプ、部分的にストライプ、およびスポットされた構成を参照してください。

オートスケーリングの利点

アプリケーションの高可用性。自動スケーリングにより、アプリケーションのトラフィック要求を処理するための適切な数の Citrix ADC VPX インスタンスが常に確保されます。これは、トラフィック要求に関係なく、アプリケーションが常に起動して実行されるようにするためです。

スマートなスケーリング決定とゼロタッチ構成。自動スケーリングはアプリケーションを継続的に監視し、要求に応じて動的に Citrix ADC インスタンスを追加または削除します。需要が急増すると、インスタンスは自動的に追加されます。需要が急増すると、インスタンスは自動的に削除されます。
Citrix ADC インスタンスの追加と削除は自動的に行われ、手動によるゼロタッチ構成になります。

自動 **DNS** 管理。Citrix ADM Autoscale 機能は、自動 DNS 管理を提供します。新しい Citrix ADC インスタンスが追加されると、ドメイン名が自動的に更新されます。

グレースフル接続終了。スケールイン中、Citrix ADC インスタンスは正常に削除され、クライアント接続が失われるのを防ぎます。

コスト管理の向上。自動スケーリングは、必要に応じて Citrix ADC インスタンスを動的に増減します。これにより、関連するコストを最適化できます。必要なときにのみインスタンスを起動し、不要になったときにインスタンスを終了することで、コストを節約できます。したがって、使用したリソースに対してのみお支払いいただきます。

観測性。アプリケーションの稼働状態を監視するには、アプリケーションの開発担当者または IT 担当者にとって重要なのは監視です。Citrix ADM の AutoScale ダッシュボードでは、しきい値のパラメーター値、AutoScale トリガーのタイムスタンプ、イベント、および Autocale に参加しているインスタンスを視覚化できます。

サポート性

現在、AutoScale 機能は AWS にデプロイされた Citrix ADC インスタンスでのみサポートされています。

> 注:
>
> AWS で AutoScale グループを作成するための Citrix ADC リリース 12.1 ビルド 50.28 イメージの使用はサポートされていません。

ライセンスの要件

Citrix Autoscale グループ用に作成された Citrix ADC インスタンスは、Citrix ADC アドバンストライセンスまたはプレミアム ADC ライセンスを使用します。Citrix ADC クラスタリング機能は、アドバンストまたはプレミアム ADC ライセンスに含まれています。

次のいずれかの方法を選択して、Citrix ADCCitrix ADM によってプロビジョニングされた Citrix ADC のライセンスを取得できます。

- **Citrix ADM** に存在する **ADC** ライセンスを使用する： Autoscale グループの作成時に、プール容量、VPX ライセンス、または仮想 CPU ライセンスを構成します。したがって、Autocale グループ用に新しいインスタンスがプロビジョニングされると、既に設定されているライセンスタイプがプロビジョニングされたインスタンスに自動的に適用されます。
  - プールされた容量: Autocale グループ内のすべてのプロビジョニングされたインスタンスに帯域幅を割り当てます。新しいインスタンスをプロビジョニングするために必要な帯域幅が Citrix ADM で利用可能であることを確認します。詳しくは、「プール容量を構成する」を参照してください。

Autocale グループの各 ADC インスタンスは、1 つのインスタンス・ライセンスと、指定された帯域幅をプールからチェックアウトします。

- **VPX** ライセンス：新しくプロビジョニングされたインスタンスに VPX ライセンスを適用します。新しいインスタンスをプロビジョニングするために、Citrix ADM で必要な数の VPX ライセンスがあることを確認します。

  Citrix ADC VPX インスタンスがプロビジョニングされると、インスタンスは Citrix ADM からライセンスをチェックアウトします。詳しくは、「Citrix ADC VPX チェックインとチェックアウトのライセンス」を参照してください。

- 仮想 **CPU** ライセンス**:** 新しくプロビジョニングされたインスタンスに仮想 CPU ライセンスを適用します。このライセンスでは、Citrix ADC VPX インスタンスの資格を持つ CPU の数を指定します。新しいインスタンスをプロビジョニングするために必要な数の仮想 CPU が Citrix ADM にあることを確認します。

  Citrix ADC VPX インスタンスがプロビジョニングされると、インスタンスは Citrix ADM から仮想 CPU ライセンスをチェックアウトします。詳しくは、「Citrix ADC 仮想 CPU ライセンス」を参照してください。

プロビジョニングされたインスタンスが破棄またはプロビジョニング解除されると、適用されたライセンスは自動的に Citrix ADM に返されます。

消費されたライセンスを監視するには、[ネットワーク] > [ライセンス] ページに移動します。

- **AWS** サブスクリプションライセンスの使用**:** AutoScale グループの作成時に、AWS マーケットプレイスで使用可能な Citrix ADC ライセンスを設定します。したがって、Autocale グループ用に新しいインスタンスがプロビジョニングされると、ライセンスは AWS Marketplace から取得されます。

AWS 用語

次の表は、この文書で使用されている Auto Scaling 用語のいくつかの簡単な説明です。

用語	説明
AWS Auto Scaling グループ	AWS Auto Scaling グループは、同様の特性を共有する EC2 インスタンスの集合であり、インスタンスのスケーリングおよび管理を目的として論理的なグループとして扱われます。
Amazon Machine Image (AMI)	マシンイメージ。クラウド内の仮想サーバーであるインスタンスを起動するのに必要な情報を提供します。
Elastic Compute Cloud（EC2）	クラウドで、安全でサイズ変更できる処理能力を提供する Web サービスです。Web 規模のクラウドコンピューティングを開発者が簡単に実施できるように設計されています。

用語	説明
Elastic IP（EIP）アドレス	Elastic IP アドレスは、動的なクラウドコンピューティング用に設計された静的なパブリック IPv4 アドレスです。Elastic IP アドレスは、アカウント内の任意の VPC のインスタンスまたはネットワークインターフェイスに関連付けることができます。
エラスティックネットワークインターフェイス (ENI)	VPC のインスタンスにアタッチできる、仮想のネットワークインターフェイスです。
インスタンスの種類	Amazon EC2 では、さまざまなユースケースに対応できるよう最適化された幅広い種類のインスタンスを提供してます。インスタンスタイプを構成する CPU、メモリ、ストレージ、およびネットワーク機能の組み合わせはさまざまで、アプリケーションに合わせて最適なリソースの組み合わせを柔軟に選択できます。
Identity and Access Management（IAM）ロール	AWS で ID が実行できること、または実行できないことを決定する許可ポリシーを持つ AWS の ID。IAM ロールを使うことで EC2 インスタンス上で実行されるアプリケーションが、AWS リソースに安全にアクセスできるようになります。
IAM インスタンスプロファイル	AWS のクラスターでプロビジョニングされた Citrix ADC インスタンスに提供される ID。プロファイルにより、インスタンスが、クライアントリクエストの負荷分散を開始したときに AWS サービスにアクセスできるようになります。
リスナー	リスナーは、構成するプロトコルとポートを使用して、接続要求をチェックするプロセスです。リスナーに対して定義するルールによって、ロードバランサーが 1 つ以上のターゲットグループのターゲットにリクエストをルーティングする方法が決まります。
NLB	ネットワークロードバランサ。NLB は、AWS 環境で使用可能な L4 ロードバランサーです。
国道 53 号	Route 53 は、Amazon の高可用性とスケーラブルなクラウドドメインネームシステム (DNS) ウェブサービスです。
セキュリティグループ	あるインスタンスに対して許可されている、名前が付けられた一連の受信方向のネットワーク接続。

用語	説明
サブネット	EC2 インスタンスをアタッチできる VPC の IP アドレス範囲の一部分。セキュリティと運用上の必要に応じて、サブネットを作成し、インスタンスをグループ分けできます。
Virtual Private Cloud（VPC）	定義した仮想ネットワーク内で AWS リソースを起動できる、AWS クラウドの論理的に隔離されたセクションをプロビジョニングする Web サービス。

Citrix ADC VPX Autoscale の用語

次の表に、このドキュメントで使用されている Citrix ADC VPX オートスケーリング用語の概要を示します。

用語	説明
グループの Autoscale	Autoscale グループは、Citrix ADC インスタンスのグループで、アプリケーションを単一のエンティティとして負荷分散し、しきい値パラメータが制限に違反したときに自動スケーリングをトリガーします。Citrix ADC インスタンスは、Autoscale グループ構成に基づいて動的にスケールアウトまたはスケールインします。注**:** このドキュメントでは、Citrix AutoScale グループは AutoScale グループと呼ばれていますが、AWS AutoScale グループは明示的に AWS AutoScale グループと呼ばれます。
Citrix ADC クラスター	Citrix ADC クラスターは、Citrix ADC VPX インスタンスのグループであり、各インスタンスはノードと呼ばれます。クライアントトラフィックは、高可用性、高スループット、およびスケーラビリティを提供するために、ノード間で分散されます。

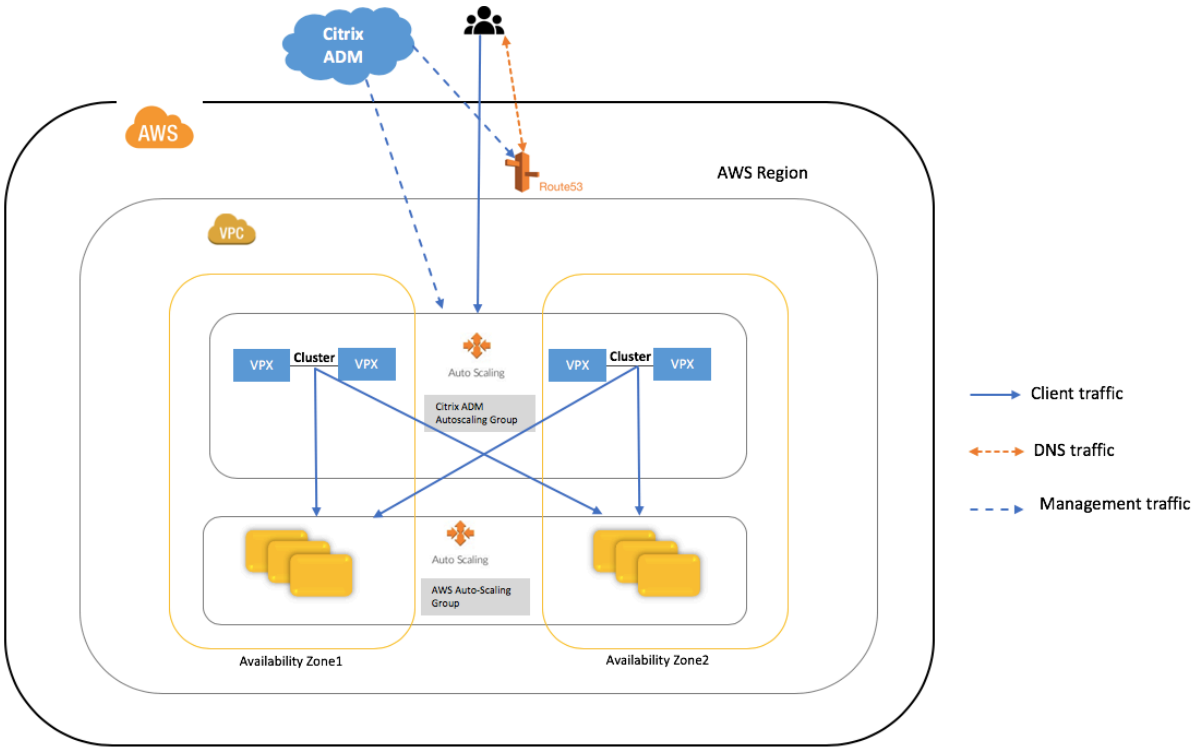
用語	説明
ドレイン接続タイムアウト	スケールイン中、プロビジョニング解除のためにインスタンスが選択されると、Citrix ADM は Autocale グループへの新しい接続の処理からインスタンスを削除し、指定されたドレイン接続のタイムアウト期間が終了するまで待機してからプロビジョニング解除します。これにより、プロビジョニングを解除する前に、このインスタンスへの既存の接続をドレインアウトできます。ドレイン接続タイムアウトの期限が切れる前に接続がドレインされた場合、Citrix ADM はドレイン接続タイムアウトの期限が切れるまで待機してから、新しい評価を開始します。注：ドレイン接続のタイムアウトが切れた後も接続がドレインされない場合は、アプリケーションに影響を与える可能性のあるインスタンスが Citrix ADM によって削除されます。デフォルト値は 5 分で、設定可能です。
クールダウン期間	スケールアウト後、クールダウン期間は、統計の評価を停止する必要がある時間です。これにより、次回のスケーリング決定が行われる前に、現在のインスタンスのセットで現在のトラフィックが安定して平均化できるようになり、Autocale グループの有機的な成長が保証されます。デフォルトのクールダウン期間の値は 10 分で、設定可能です。注：デフォルト値は、スケールアウト後にシステムが安定するのに必要な時間（約 4 分）に Citrix ADC 構成と DNS アドバタイズメントの時間に基づいて決定されます。
タグ	各 Autoscale グループには、キーと値のペアであるタグが割り当てられます。リソースにタグを適用すると、リソースの整理や識別が容易になります。タグは AWS と Citrix ADM の両方に適用されます。例：キー = 名前、値 = ウェブサーバー。開発、実稼働、テストなどのさまざまなグループに属する可能性がある Autoscale グループを容易に追跡するために、一貫したタグセットを使用することをお勧めします。

用語	説明
しきい値パラメータ	スケールアウトまたはスケールインをトリガーするために監視されるパラメータ。パラメータは、CPU 使用率、メモリ使用率、およびスループットです。監視するパラメータを 1 つ以上選択することも、複数のパラメータを選択できます。
生存時間（TTL）	情報のソースを再度参照する必要がある前に、DNS リソースレコードがキャッシュされる時間間隔を指定します。デフォルトの TTL 値は 30 秒で、設定可能です。
総再生時間	スケーリングが発生するために、スケールパラメータのしきい値を超える必要のある時間。この指定された時間内に収集されたすべてのサンプルでしきい値を超えると、スケーリングが行われます。この期間中、しきい値パラメータが最大しきい値よりも高い値にとどまる場合は、スケールアウトがトリガーされます。しきい値パラメータが最小しきい値よりも低い値で動作する場合、スケールインがトリガーされます。デフォルト値は 3 分で、設定可能です。

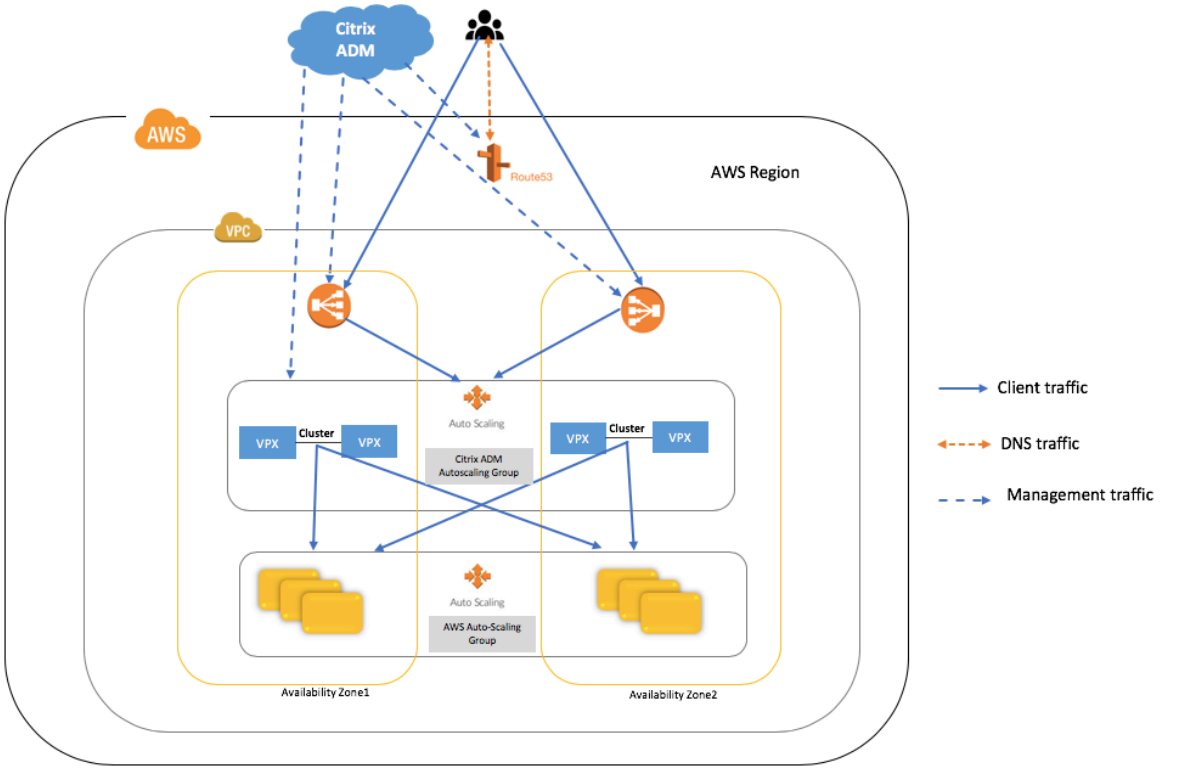
アーキテクチャ

May 7, 2021

次の図は、DNS をトラフィックディストリビューターとして使用する Auto Scaling 機能のアーキテクチャを示しています。



次の図は、トラフィックディストリビューターとして NLB を使用する Auto Scaling 機能のアーキテクチャを示しています。



Citrix Application Delivery Management（ADM）

Citrix Application Delivery Management は、オンプレミスまたはクラウドに展開されるすべての Citrix ADC 展開を管理するための Web ベースのソリューションです。このクラウドソリューションを使用すると、単一の統合された、一元化されたクラウドベースのコンソールから、グローバルアプリケーション配信インフラストラクチャ全体を管理、監視、トラブルシューティングできます。Citrix Application Delivery Management（ADM）は、Citrix ADC 展開環境でのアプリケーション配信のセットアップ、展開、管理に必要なすべての機能を提供し、アプリケーションの正常性、パフォーマンス、およびセキュリティを豊富に分析します。

Autoscale グループは Citrix ADM で作成され、Citrix ADC VPX インスタンスは Citrix ADM からプロビジョニングされます。アプリケーションは、Citrix ADM スタイルブックを通じて展開されます。

トラフィックディストリビュータ（**NLB** または **DNS /**ルート **53**）

NLB または DNS/route53 は、Autoscale グループ内のすべてのノードにトラフィックを分散するために使用されます。詳しくは、「AutoScale トラフィック分散モード」を参照してください。

Citrix ADM はトラフィックディストリビュータと通信し、アプリケーションをフロントエンドする負荷分散仮想サーバーのアプリケーションドメインと IP アドレスを更新します。

Citrix ADM Autoscale グループ

Autoscale グループは、Citrix ADC インスタンスのグループで、アプリケーションを単一のエンティティとして負荷分散し、設定されたしきい値パラメータ値に基づいて自動スケーリングをトリガーします。

Citrix ADC クラスター

Citrix ADC クラスターは、Citrix ADC VPX インスタンスのグループであり、各インスタンスはノードと呼ばれます。クライアントトラフィックは、高可用性、高スループット、およびスケーラビリティを提供するために、ノード間で分散されます。

> 注
>
> - 自動スケーリングの決定は、ノードレベルではなく、クラスターレベルで行われます。
> - 独立したクラスターは異なるアベイラビリティーゾーンでホストされるため、一部の共有状態機能のサポートには制限があります。
>
> ソース IP パーシステンスなどのパーシステンスセッションや Cookie ベースのパーシステンス以外のパーシステンスセッションは、クラスタ間で共有できません。ただし、ロードバランシングメソッドなどのステートレス機能はすべて、複数のアベイラビリティーゾーンで期待どおりに動作します。

AWS Auto Scaling グループ

AWS Auto Scaling グループは、同様の特性を共有する EC2 インスタンスの集合であり、インスタンスのスケーリングおよび管理を目的として論理的なグループとして扱われます。

AWS アベイラビリティーゾーン

AWS アベイラビリティーゾーンは、リージョン内の独立した場所です。各リージョンは、複数のアベイラビリティーゾーンで構成されています。各アベイラビリティーゾーンは 1 つのリージョンに属しています。

トラフィック分散モード

アプリケーションのデプロイをクラウドに移行すると、自動スケーリングはインフラストラクチャの一部になります。アプリケーションがオートスケーリングを使用してスケールアウトまたはスケールインする場合、これらの変更をクライアントに伝播する必要があります。この伝播は、DNS ベースまたは NLB ベースの自動スケーリングを使用して実現されます。

NLB ベースの自動スケーリング

NLB ベースのデプロイモードでは、クラスターノードへのディストリビューション層が AWS ネットワークロードバランサーになります。

NLB ベースの自動スケーリングでは、アベイラビリティーゾーンごとに 1 つの静的 IP アドレスしか提供されません。これは route53 に追加されるパブリック IP アドレスであり、バックエンド IP アドレスはプライベートにすることができます。このパブリック IP アドレスでは、自動スケーリング中にプロビジョニングされた新しい Citrix ADC インスタンスはプライベート IP アドレスを使用して動作し、追加のパブリック IP アドレスは必要ありません。

NLB ベースの自動スケーリングを使用して TCP トラフィックを管理します。DNS ベースの自動スケーリングを使用して UDP トラフィックを管理します。

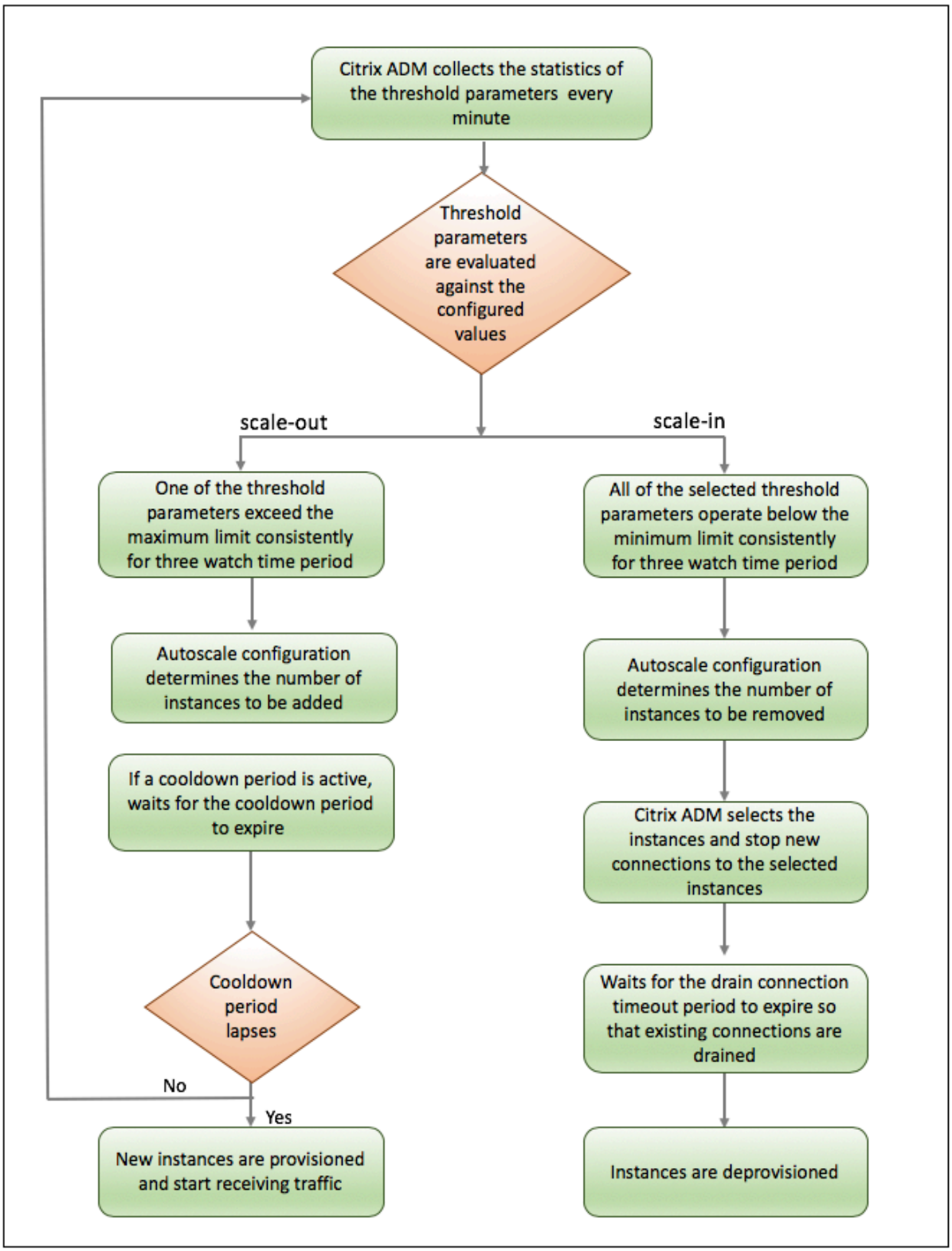
DNS ベースの自動スケーリング

DNS ベースの自動スケーリングでは、DNS は Citrix ADC クラスターノードへのディストリビューションレイヤーとして機能します。スケーリングの変更は、アプリケーションに対応するドメイン名を更新することによってクライアントに伝播されます。現在、DNS プロバイダーは AWS Route53 です。

> 注:
>
> DNS ベースの自動スケーリングでは、各 Citrix ADC インスタンスにはパブリック IP アドレスが必要です。

オートスケーリングの仕組み

次のフローチャートは、オートスケーリングのワークフローを示しています。



Citrix ADM は、Autoscale プロビジョニングされたクラスターから 1 分の間隔で統計（CPU 使用率、メモリ使用率、スループット）を収集します。

統計情報は、設定しきい値に対して評価されます。統計情報が最大しきい値を超えているか、最小しきい値を下回っているかに応じて、スケールアウトまたはスケールインがそれぞれトリガーされます。

- スケールアウトがトリガーされた場合:
  - 新しいノードがプロビジョニングされます。
  - ノードはクラスタに接続され、構成はクラスタから新しいノードに同期されます。
  - ノードは Citrix ADM に登録されます。
  - 新しいノードの IP アドレスは、DNS/NLB で更新されます。

アプリケーションがデプロイされると、IPsetは各アベイラビリティーゾーンのクラスターに作成され、ドメインとインスタンスの IP アドレスは DNS/NLB に登録されます。

- スケールインがトリガーされた場合:
  - 削除対象として特定されたノードの IP アドレスが削除されます。
  - ノードがクラスタから切り離され、プロビジョニング解除された後、Citrix ADM から登録解除されます。

アプリケーションを削除すると、ドメインとインスタンスの IP アドレスが DNS/NLB から登録解除され、IPset が削除されます。

例

次の設定を使用して、単一のアベイラビリティーゾーンに asg_arn という名前の Autoscale グループを作成したとします。

- しきい値パラメータ — メモリ使用量
- 最小制限:40
- 最大制限:85
- 総再生時間 — 3 分
- クールダウン期間 — 10 分
- ドレイン接続タイムアウト — 10 分
- TTL タイムアウト — 60 秒

Autoscale] グループが作成されると、[Autoscale] グループから統計が収集されます。Autocale ポリシーは、Autoscale イベントが進行中かどうかも評価し、自動スケーリングが進行中の場合は、そのイベントが完了するまで待機してから、統計情報を収集します。

ASG ID	Availability zone	Cluster IP address	CPU usage	Throughput	Memory usage	Timestamp
asg_arn	eu-west-2	192.0.2.250	55	65	92	T1
asg_arn	eu-west-2	192.0.2.250	60	50	90	T2
asg_arn	eu-west-2	192.0.2.250	59	45	80	T3
asg_arn	eu-west-2	192.0.2.250	49	75	90	T4
asg_arn	eu-west-2	192.0.2.250	63	70	93	T5
asg_arn	eu-west-2	192.0.2.250	65	80	92	T6
asg_arn	eu-west-2	192.0.2.250	65	85	75	T7
asg_arn	eu-west-2	192.0.2.250	35	70	70	.....
asg_arn	eu-west-2	192.0.2.250	55	70	70	T16
asg_arn	eu-west-2	192.0.2.250	58	55	45	T17
asg_arn	eu-west-2	192.0.2.250	59	65	30	T18
asg_arn	eu-west-2	192.0.2.250	75	45	30	T19
asg_arn	eu-west-2	192.0.2.250	46	64	25	T20
asg_arn	eu-west-2	192.0.2.250	64	65	50	T31
asg_arn	eu-west-2	192.0.2.250	64	65	60	T32
asg_arn	eu-west-2	192.0.2.250	64	65	60	T33

Scale-out event is triggered. Nodes are provisioned.

Evaluation of statistics is skipped for this availability zone from T7 –T16 as the cooldown period is in effect.

Scale-in event is triggered. Drain connection timeout in effect.

イベントのシーケンス**:**

- T1 および T2：メモリ使用量が最大しきい値制限を超えています。
- T3：メモリ使用量が最大しきい値制限を下回っています。
- T6、T5、T4:3 回の総再生時間の間、メモリ使用量が連続して最大しきい値を超えました。
  - スケールアウトがトリガーされます。
  - ノードのプロビジョニングが行われます。
  - クールダウン期間が有効です。
- T7 — T16: クールダウン期間が有効であるため、このアベイラビリティーゾーンの Autoscale 評価は T7 から T16 までスキップされます。
- T18、T19、T20：3 回の総再生時間の間、メモリ使用量が連続して最小しきい値を超えました。
  - スケールインがトリガーされます。
  - ドレイン接続のタイムアウトが有効です。
  - IP アドレスは、DNS/NLB から解放されます。
- T21 — T30: ドレイン接続タイムアウトが有効であるため、このアベイラビリティーゾーンの T21 から T30 までの Autoscale 評価はスキップされます。
- T31

  - DNS ベースの自動スケーリングでは、TTL が有効です。
  - NLB ベースの自動スケーリングでは、インスタンスのプロビジョニング解除が行われます。
- T32
  - NLB ベースの自動スケーリングでは、統計の評価が開始されます。
  - DNS ベースの自動スケーリングでは、インスタンスのプロビジョニング解除が行われます。
- T33: DNS ベースの自動スケーリングの場合、統計情報の評価が開始されます。

Autoscale の構成

May 7, 2021

AWS で Citrix ADC VPX インスタンスの自動スケーリングを開始するには、以下の手順を実行する必要があります。

1. AWS のすべての前提条件を完了する
2. Citrix ADM のすべての前提条件を完了する
3. Autoscale グループの作成
   a) Autoscale 設定の初期化
   b) Autoscale パラメータの構成
   c) ライセンスをチェックアウトする
   d) クラウドパラメータの設定
4. アプリケーションの展開

AWS の前提条件

AutoScale 機能を使用するには、AWS のすべての前提条件を完了していることを確認します。このドキュメントでは、次のことを前提としています。

1. すでに AWS アカウントを所有しています。
2. すべての管理権限を持つ ID とアクセス管理 (IAM) ユーザーを作成しました。

次のいくつかのセクションでは、Citrix ADM で Autoscale グループを作成する前に、AWS で必要なすべてのタスクを実行するのに役立ちます。完了する必要があるタスクは次のとおりです。

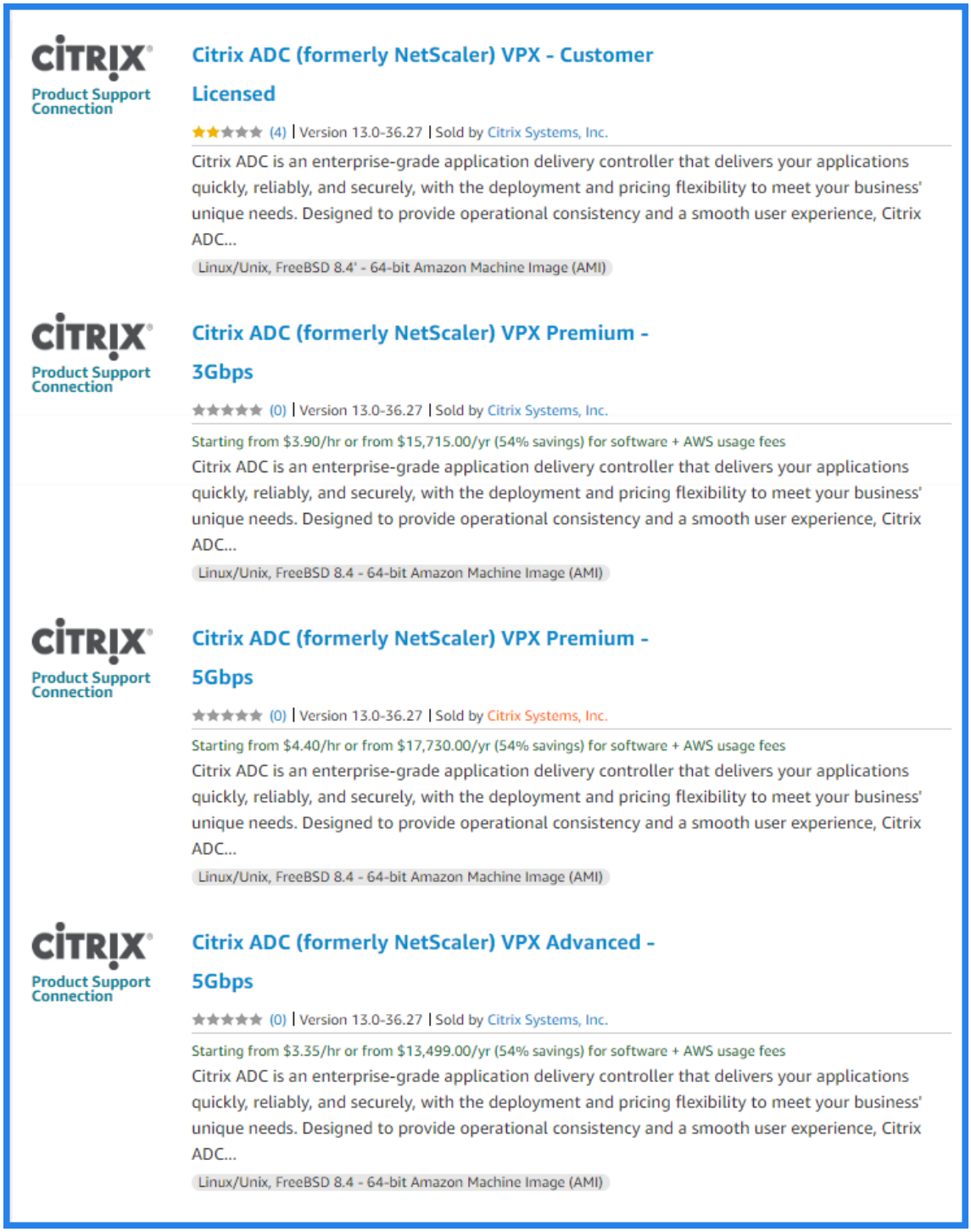
1. AWS で必要な Citrix ADC VPX インスタンスをサブスクライブします。
2. 必要な仮想プライベートクラウド（VPC）を作成するか、既存の VPC を選択します。
3. 対応するサブネットとセキュリティグループを定義します。
4. Citrix ADM 用と Citrix ADC VPX インスタンス用の 2 つの IAM ロールを作成します。

> ヒント
>
> AWS CloudFormation テンプレート t を使用すると、Citrix ADC の自動スケーリングの AWS 前提条件ステップを自動化できます。

VPC、サブネット、およびセキュリティグループの作成方法の詳細については、AWS ドキュメントを参照してください。

AWS で **Citrix ADC VPX** ライセンスをサブスクライブ

1. AWS マーケットプレイスにアクセスします。
2. 資格情報でログオンします。
3. Citrix ADC VPX カスタマーライセンス版、プレミアム版、またはアドバンス版を検索します。



4. Citrix ADC VPX カスタマーライセンス、プレミアムエディション、または Citrix ADC VPX アドバンストエディションのライセンスを購読してください。

> 注 Autocale グループの ADC インスタンスで ADM からライセンスをチェックアウトする場合は、次のことを確認してください。

> - 必要な ADC ライセンスは、ADM で入手できます。
> - **Citrix ADC VPX** カスタマーライセンス製品が登録されています。

サブネットの作成

VPC に 3 つのサブネットを作成します。それぞれ 1 つずつ管理、クライアント、およびサーバー接続に使用します。サブネットごとに VPC で定義されている範囲から IPv4 CIDR ブロックを指定します。サブネットを配置するアベイラビリティーゾーンを指定します。サーバーが存在する各アベイラビリティーゾーンに 3 つのサブネットをすべて作成します。

- 管理。管理専用の仮想プライベートクラウド（VPC）内の既存のサブネット。Citrix ADC は AWS サービスに連絡する必要があり、インターネットアクセスが必要です。NAT Gateway を設定し、このサブネットからのインターネットアクセスを許可するルートテーブルエントリを追加します。

  > 注:
  >
  > Citrix ADM でポート`27000`とポート`7279`を開いてください。これらのポートは、Citrix ADM から Citrix ADC ライセンスをチェックアウトするために使用されます。詳しくは、「ポート」を参照してください。

- クライアント。クライアント側のトラフィック専用の仮想プライベートクラウド（VPC）内の既存のサブネット。通常、Citrix ADC は、インターネットからパブリックサブネット経由でアプリケーションのクライアントトラフィックを受信します。クライアントサブネットを、インターネット Gateway へのルートを持つルートテーブルに関連付けます。このサブネットにより、Citrix ADC はインターネットからアプリケーショントラフィックを受信できます。
- サーバー。サーバー側のトラフィック専用の仮想プライベートクラウド (VPC) の既存のサブネット。ADC は、このサブネットを介してバックエンド・アプリケーション・サーバーにトラフィックを送信します。アプリケーショントラフィックを受信するすべてのアプリケーションサーバーがこのサブネットに存在する必要があります。サーバーがこのサブネットの外側にある場合、アプリケーショントラフィックはサブネットのゲートウェイを介して受信されます。

セキュリティグループの作成

セキュリティグループを作成して、Citrix ADC VPX インスタンスのインバウンドトラフィックとアウトバウンドトラフィックを制御します。Citrix Autoscale グループで制御する受信トラフィックと送信トラフィックの両方のルールを作成します。規則は、必要に応じていくつでも追加できます。

- 管理。Citrix ADC VPX の管理専用のアカウント内の既存のセキュリティグループ。受信規則は、次の TCP ポートおよび UDP ポートで許可されます。
  - TCP: 80、22、443、3008—3011、4001、27000、7279
  - UDP: 67、123、161、500、3003、4500、7000

  セキュリティグループで、Citrix ADM エージェントが VPX にアクセスできるようにすることを確認します。

- クライアント。Citrix ADC VPX インスタンスのクライアント側通信専用のアカウント内の既存のセキュリティグループ。通常、インバウンドルールは TCP ポート 80 および 443 で許可されます。また、ADC インスタンスの状態を監視するには、60000 ポートが必要です。
- サーバー。Citrix ADC VPX サーバー側通信専用のアカウント内の既存のセキュリティグループ。通常、すべてのインバウンドルールをブロックし、アウトバウンドルールが VPC 全体に到達できるようにします。

IAM ロールの作成

AWS アカウントでオペレーションを実行するアクセス許可を ADM および ADC インスタンスに付与する IAM エンティティを作成します。ADM は、AWS アカウントから以下を作成または削除します。

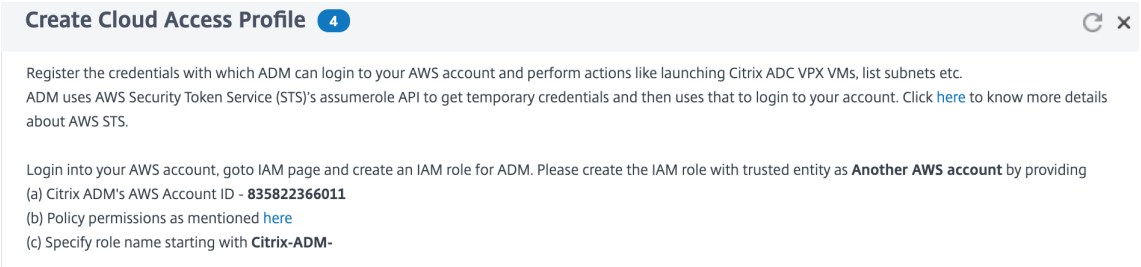
- Citrix ADC EC2 インスタンス
- クラウドロードバランサー
- Route53

> 注:
>
> ロール名が「Citrix-ADM-」で始まり、インスタンスプロファイル名が「Citrix-ADC-」で始まることを確認します。

ADM の **IAM** エンティティを作成するには

IAM ロールを作成します。これにより、AWS アカウントと Citrix の AWS アカウントとの間に信頼関係を確立できます。IAM ポリシーでは、ADM が AWS アカウントでオペレーションを実行するためのアクセス許可を提供します。

1. **AWS** で、[サービス] をクリックします。左側のナビゲーションペインで、[**IAM] > [**ロール] を選択し、[ロールの作成] をクリックします。
2. AWS アカウントを Citrix ADM の AWS アカウントに接続しています。そのため、[別の **AWS** アカウント] を選択して、Citrix ADM が AWS アカウントでアクションを実行できるようにします。
3. 12 桁の Citrix ADM AWS アカウント ID を入力します。Citrix の ID は 835822366011 である。外部 ID は空白のままにしておくことができます。後で IAM ロールを編集する必要があります。ADM でのクラウドアクセスプロファイルの作成時に ADM によって提供される外部 ID を指定します。



4. [アクセス許可] をクリックします。
5. [アクセス許可ポリシーの添付] ページで、[ポリシーの作成] をクリックします。

6. ポリシーを作成および編集するには、ビジュアルエディターまたは JSON を使用します。

   Citrix ADM に対する Citrix のアクセス許可の一覧は、次のボックスに表示されます。

```
{

"Version": "2012-10-17",
"Statement": [
    {

        "Action": [
            "tag:GetResources",
            "tag:TagResources",
            "tag:UntagResources",
            "tag:getTagKeys",
            "tag:getTagValues",
            "ec2:DescribeInstances",
            "ec2:UnmonitorInstances",
            "ec2:MonitorInstances",
            "ec2:CreateKeyPair",
            "ec2:ResetInstanceAttribute",
            "ec2:ReportInstanceStatus",
            "ec2:DescribeVolumeStatus",
            "ec2:StartInstances",
            "ec2:DescribeVolumes",
            "ec2:UnassignPrivateIpAddresses",
            "ec2:DescribeKeyPairs",
            "ec2:CreateTags",
            "ec2:ResetNetworkInterfaceAttribute",
            "ec2:ModifyNetworkInterfaceAttribute",
            "ec2:DeleteNetworkInterface",
            "ec2:RunInstances",
            "ec2:StopInstances",
            "ec2:AssignPrivateIpAddresses",
            "ec2:DescribeVolumeAttribute",
            "ec2:DescribeInstanceCreditSpecifications",
            "ec2:CreateNetworkInterface",
            "ec2:DescribeImageAttribute",
            "ec2:AssociateAddress",
            "ec2:DescribeSubnets",
            "ec2:DeleteKeyPair",
            "ec2:DisassociateAddress",
            "ec2:DescribeAddresses",
            "ec2:DeleteTags",
            "ec2:RunScheduledInstances",
```



```
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeRegions",
                "ec2:DescribeDhcpOptions",
                "ec2:GetConsoleOutput",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeInstanceStatus",
                "ec2:ReleaseAddress",
                "ec2:RebootInstances",
                "ec2:TerminateInstances",
                "ec2:DetachNetworkInterface",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeTags",
                "ec2:AllocateAddress",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeHosts",
                "ec2:DescribeImages",
                "ec2:DescribeVpcs",
                "ec2:AttachNetworkInterface",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeInternetGateways"
            ],
            "Resource": "\*",
            "Effect": "Allow",
            "Sid": "VisualEditor0"
        }
    ,
        {

            "Action": [
                "iam:GetRole",
                "iam:PassRole",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "\*",
            "Effect": "Allow",
            "Sid": "VisualEditor1"
        }
    ,
        {

            "Action": [
```



```
87                "route53:CreateHostedZone",
88                "route53:CreateHealthCheck",
89                "route53:GetHostedZone",
90                "route53:ChangeResourceRecordSets",
91                "route53:ChangeTagsForResource",
92                "route53:DeleteHostedZone",
93                "route53:DeleteHealthCheck",
94                "route53:ListHostedZonesByName",
95                "route53:GetHealthCheckCount"
96                "route53:ListResourceRecordSets",
97                "route53.AssociateVPCWithHostedZone",
98            ],
99            "Resource": "\*",
100           "Effect": "Allow",
101           "Sid": "VisualEditor2"
102       }
103   ,
104       {
105
106           "Action": [
107               "iam:ListInstanceProfiles",
108               "iam:ListAttachedRolePolicies",
109               "iam:SimulatePrincipalPolicy",
110               "iam:SimulatePrincipalPolicy"
111           ],
112           "Resource": "\*",
113           "Effect": "Allow",
114           "Sid": "VisualEditor3"
115       }
116   ,
117       {
118
119           "Action": [
120               "ec2:ReleaseAddress",
121               "elasticloadbalancing:DeleteLoadBalancer",
122               "ec2:DescribeAddresses",
123               "elasticloadbalancing:CreateListener",
124               "elasticloadbalancing:CreateLoadBalancer",
125               "elasticloadbalancing:RegisterTargets",
126               "elasticloadbalancing:CreateTargetGroup",
127               "elasticloadbalancing:DeregisterTargets",
128               "ec2:DescribeSubnets",
129               "elasticloadbalancing:DeleteTargetGroup",
130               "elasticloadbalancing:ModifyTargetGroupAttributes",
131               "elasticloadbalancing:DescribeLoadBalancers",
```



```
132                 "ec2:AllocateAddress"
133             ],
134             "Resource": "*",
135             "Effect": "Allow",
136             "Sid": "VisualEditor4"
137         }
138
139     ]
140   }
141
142
143  <!--NeedCopy-->
```

7. 「JSON」タブに権限のリストをコピーして貼り付け、「ポリシーの確認」をクリックします。
8. [ポリシーの確認] ページで、ポリシーの名前を入力し、説明を入力し、[ポリシーの作成] をクリックします。

   > **注:**
   >
   > 名前が「Citrix-adm-」で始まることを確認します。

9. 「ロールの作成」ページで、ロールの名前を入力します。

   > **注:**
   >
   > 役割名が「Citrix-ADM-」で始まることを確認します。

ADM で作成された **ADC** の **IAM** エンティティを作成するには

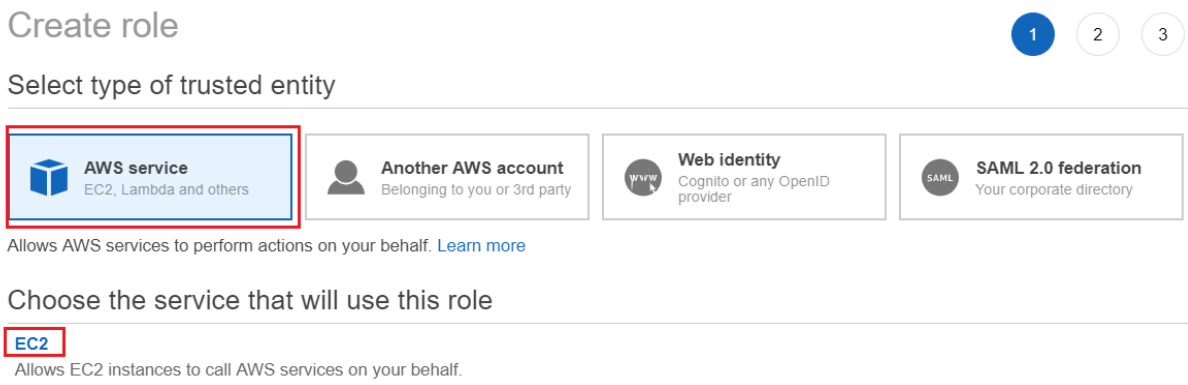
ADC が AWS アカウントでオペレーションを実行するためのアクセス許可を提供する IAM ポリシーで IAM ロールを作成します。このロールは、ADM によって作成される ADC インスタンスにアタッチされ、これにより ADC がお客様のアカウントにアクセスできるようになります。

1. **AWS** で、[サービス] をクリックします。左側のナビゲーションペインで、[**IAM] > [**ロール] を選択し、[ロールの作成] をクリックします。

同様に、「Citrix-ADC-」で始まる別の名前を指定して、Citrix ADC インスタンスのプロファイルを作成します。

[**AWS** サービス**] > [EC2]** を選択していることを確認します。

1. [アクセス許可ポリシーの添付] ページで、[ポリシーの作成] をクリックします。
2. ポリシーを作成および編集するには、ビジュアルエディターまたは JSON を使用します。



Citrix ADC インスタンスの Citrix からのアクセス許可の一覧は、次のボックスに表示されます。

```
{

  "Version": "2012-10-17",
  "Statement": [
    {

      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:SimulatePrincipalPolicy",
        "autoscaling:\*",
        "sns:\*",
        "sqs:\*",
        "cloudwatch:\*",
        "ec2:AssignPrivateIpAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource": "*"
     }

  ]
 }

<!--NeedCopy-->
```


DNS ドメインを登録する

アプリケーションをホストするための DNS ドメインが登録されていることを確認します。

ネットワークに必要な弾性 IP（EIP）の数を評価します。

必要な EIP の数は、DNS ベースの自動スケーリングと NLB ベースの自動スケーリングのいずれをデプロイするかによって異なります。EIP の数を増やすには、AWS でケースを作成します。

- DNS ベースの自動スケーリングの場合、アベイラビリティーゾーンごとに必要な EIP の数は、アプリケーション数に、Autoscale グループで構成する VPX インスタンスの最大数を掛けた値になります。
- NLB ベースの自動スケーリングの場合、必要な EIP の数は、アプリケーションの数に、アプリケーションがデプロイされるアベイラビリティーゾーンの数を掛けた値になります。

インスタンス制限要件の評価

インスタンスの制限を評価する場合は、Citrix ADC インスタンスの容量要件も考慮してください。

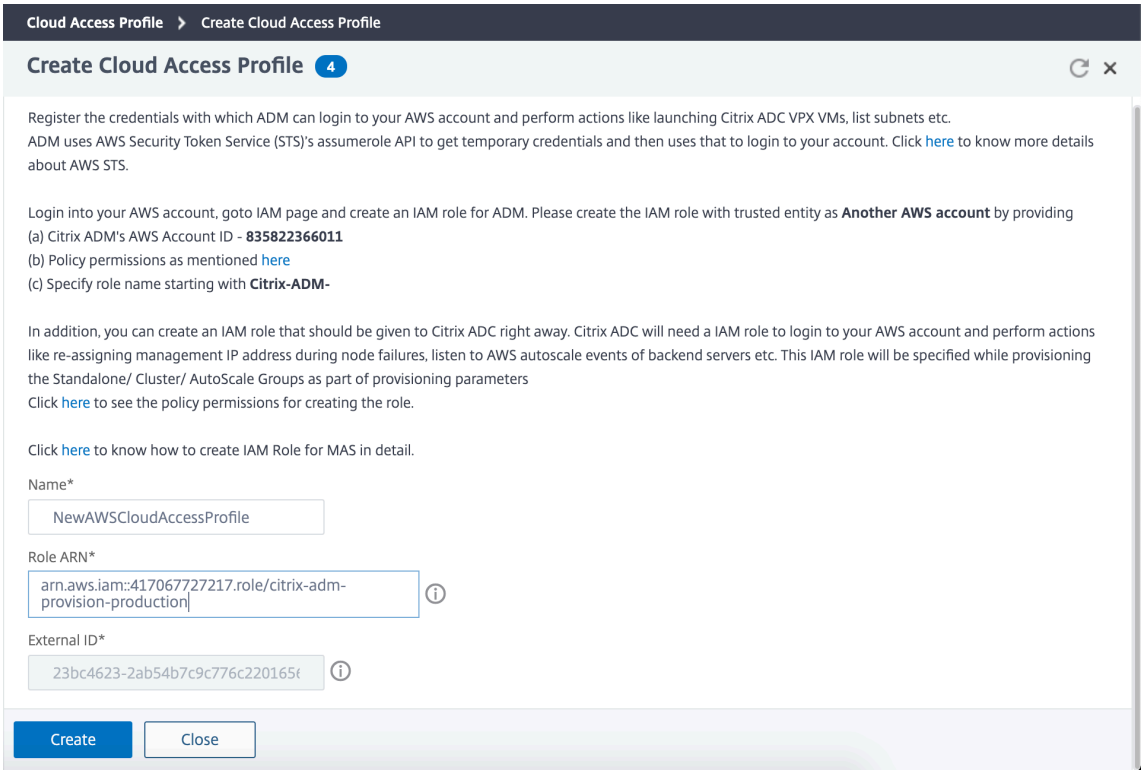
Citrix ADM の前提条件

Autoscale 機能を使用するには、Citrix ADM のすべての前提条件が完了していることを確認します。

サイトを作成する

Citrix ADM でサイトを作成し、AWS ロールに関連付けられた VPC の詳細を追加します。

1. Citrix ADM で、［ネットワーク］**>**［サイト］に移動します。
2. ［追加］をクリックします。
3. サービスタイプを AWS として選択し、[既存の **VPC** をサイトとして使用] を有効にします。
4. クラウドアクセスプロファイルを選択します。
5. クラウドアクセスプロファイルがフィールドに存在しない場合は、[追加] をクリックしてプロファイルを作成します。
   a) [**Create Cloud Access Prof** ile] ページで、AWS にアクセスするプロファイルの名前を入力します。
   b) AWS で作成したロールに関連付けられた ARN を入力します。
   c) 自動生成された外部 **ID** をコピーして IAM ロールを更新します。
6. ［作成］をクリックします。
7. もう一度 [作成] をクリックしてサイトを作成します。
8. 自動生成された外部 **ID** を使用して AWS で IAM ロールを更新します。



a) AWS アカウントにログインし、更新するロールに移動します。

b) [信頼関係] タブで、[信頼関係の編集] をクリックし、`Statement` ブロック内に次の条件を追加します。

```
"Condition": {

  "StringEquals": {

    "sts:ExternalId": "<External-ID>"
   }

 }

<!--NeedCopy-->
```

AWS で IAM ロールの外部 ID を有効にすると、サードパーティアカウントに接続できます。外部 ID は、ロールのセキュリティを強化します。

AWS の IAM ロールに関連付けられた VPC の詳細情報（リージョン、VPC ID、名前、CIDR ブロックなど）は、Citrix ADM にインポートされます。

AWS で **Citrix ADM** エージェントをプロビジョニングする

Citrix ADM サービスエージェントは、Citrix ADM とデータセンターまたはクラウドで検出されたインスタンスの間の仲介として機能します。

1. [ネットワーク**] > [**エージェント**]** に移動します。
2. [プロビジョニング] をクリックします。
3. [**AWS**] を選択し、[次へ] をクリックします。
4. [雲パラメータ] タブで、次の項目を指定します。
    - 名前：Citrix ADM エージェント名を指定します。
    - サイト：エージェントと ADC VPX インスタンスをプロビジョニングするために作成したサイトを選択します。
    - クラウドアクセスプロファイル -リストからクラウドアクセスプロファイルを選択します。
    - アベイラビリティーゾーン -AutoScale グループを作成するゾーンを選択します。選択したクラウドアクセスプロファイルに応じて、そのプロファイルに固有のアベイラビリティーゾーンが設定されます。
    - セキュリティグループ -セキュリティグループは、Citrix ADC エージェントのインバウンドおよびアウトバウンドトラフィックを制御します。制御する着信トラフィックと発信トラフィックの両方のルールを作成します。
    - [**Subnet**]：エージェントをプロビジョニングする管理サブネットを選択します。
    - タグ -AutoScale グループタグのキーと値のペアを入力します。タグは、大文字と小文字を区別するキーと値のペアで構成されます。これらのタグを使用すると、Autoscale グループを簡単に整理して識別できます。タグは AWS と Citrix ADM の両方に適用されます。
5. [完了] をクリックします。

または、AWS マーケットプレイスから Citrix ADM エージェントをインストールすることもできます。詳しくは、「AWS への Citrix ADM エージェントのインストール」を参照してください。

Autoscale グループの作成

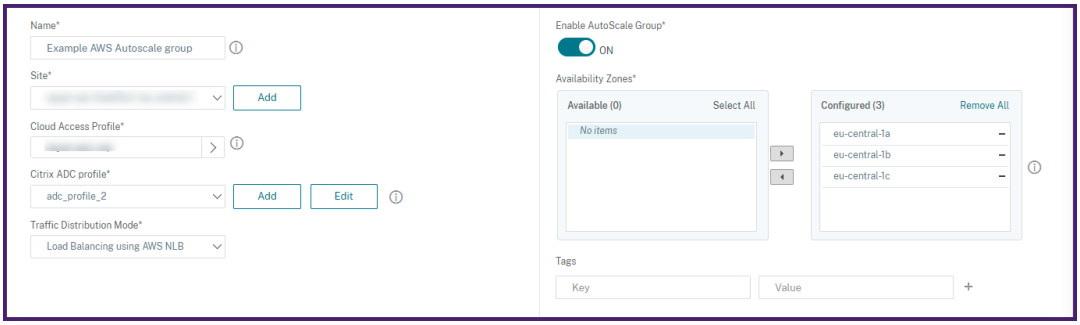
Autoscale 設定の初期化

1. Citrix ADM で、[ネットワーク] **>** [**AutoScale** グループ] に移動します。
2. [追加] をクリックして、Autoscale グループを作成します。**[AutoScale** グループの作成] ページが表示されます。
3. 次の詳細を入力します。
    - 名前。Autoscale グループの名前を入力します。

- サイト。AWS で Citrix ADC VPX インスタンスをプロビジョニングするために作成したサイトを選択します。
- エージェント。プロビジョニングされたインスタンスを管理する Citrix ADM エージェントを選択します。
- クラウドアクセスプロファイル。クラウドアクセスプロファイルを選択します。

> 注。フィールドにクラウドアクセスプロファイルが存在しない場合は、[**Add**] をクリックしてプロファイルを作成します。
>
> - AWS で作成したロールに関連付けられた ARN を入力します。
> - AWS で ID とアクセス管理（IAM）ロールを作成するときに指定した外部 ID を入力します。選択したクラウドアクセスプロファイルに応じて、アベイラビリティーゾーンが設定されます。

- デバイスプロファイル。リストからデバイスプロファイルを選択します。デバイスプロファイルは、インスタンスにログオンする必要がある場合は常に、Citrix ADM によって使用されます。
- トラフィック分散モード。デフォルトのトラフィック 分散モードとして、**[NLB** を使用した負荷分散] オプションが選択されています。アプリケーションが UDP トラフィックを使用している場合は、[**AWS route53** を使用して **DNS**] を選択します。



> 注:
>
> Autoscale の設定後、新しいアベイラビリティーゾーンを追加したり、既存のアベイラビリティーゾーンを削除したりすることはできません。

- **[AutoScale** グループ**]** を有効にします。ASG グループのステータスを有効または無効にします。このオプションはデフォルトで有効になっています。このオプションを無効にすると、自動スケーリングはトリガーされません。
- アベイラビリティーゾーン。Autoscale グループを作成するゾーンを選択します。選択したクラウドアクセスプロファイルに応じて、そのプロファイルに固有のアベイラビリティーゾーンが設定されます。
- タグ。Autoscale グループタグのキーと値のペアを入力します。タグは、大文字と小文字を区別するキーと値のペアで構成されます。これらのタグを使用すると、Autoscale グループを簡単に整理して識別できます。タグは AWS と Citrix ADM の両方に適用されます。

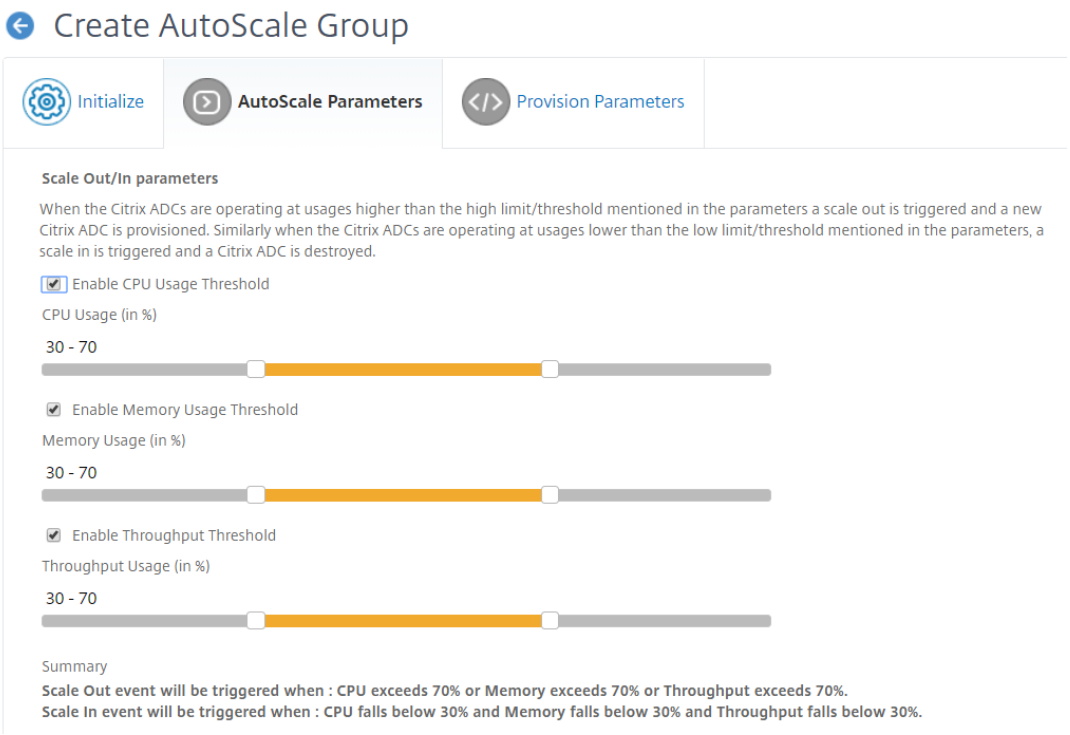
4. ［次へ］をクリックします。

Autoscale パラメータの設定

1. [**Autoscale** パラメータ] タブで、次の詳細を入力します。
2. スケールアウトまたはスケールインをトリガーするために値を監視する必要がある次のしきい値パラメータを 1 つ以上選択します。
   - **CPU** 使用率のしきい値の有効化: CPU 使用率に基づいてメトリックを監視します。
   - メモリ使用量のしきい値の有効化: メモリ使用量に基づいてメトリックを監視します。
   - スループットしきい値の有効化: スループットに基づいてメトリックスを監視します。

     注

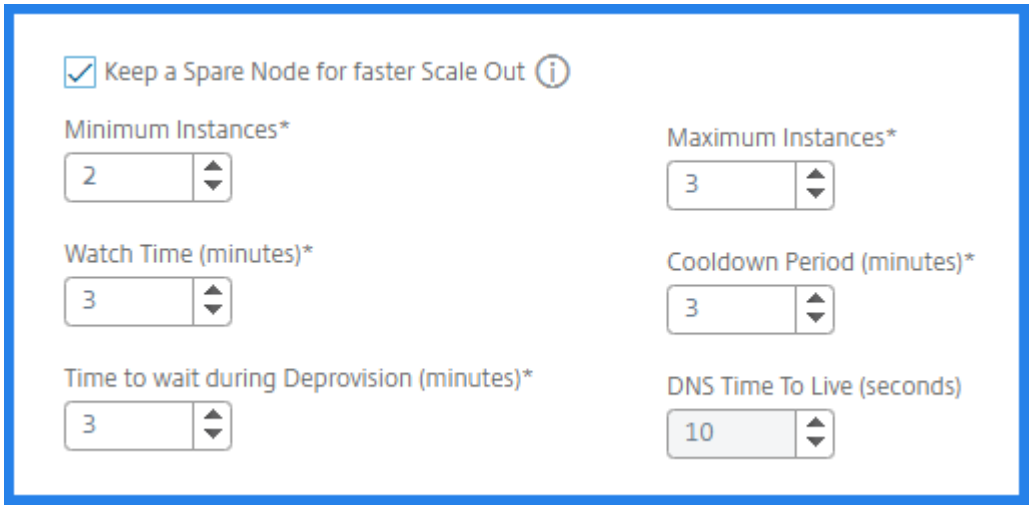
     - デフォルトの最小しきい値制限は 30 で、最大しきい値制限は 70 です。ただし、制限を変更します。
     - 最小しきい値制限は、最大しきい値制限の半分以下である必要があります。
     - 複数のしきい値パラメータをモニタリング用に選択できます。このような場合、しきい値パラメータの少なくとも 1 つが最大しきい値を超えていると、スケールインがトリガーされます。ただし、スケールインがトリガーされるのは、すべてのしきい値パラメータが通常のしきい値を下回っている場合だけです。



   - スケールアウトを高速化するためにスペアノードを保持**:** このオプションは、スケールアウトを高速化するのに役立ちます。ADM は、スケールアウトアクションが発生する前に予備ノードをプロビジョニングし、シャットダウンします。AutoScale グループに対してスケールアウトアクションが発生すると、ADM は、すでにプロビジョニングされているスペアノードを起動します。その結果、スケールアウトに

かかる時間が短縮されます。

- 最小インスタンス。この Autosale グループにプロビジョニングする必要のあるインスタンスの最小数を選択します。
- デフォルトでは、インスタンスの最小数は、選択したゾーンの数と同じです。最小インスタンスは、ゾーン数の倍数だけ増分できます。
- たとえば、アベイラビリティーゾーンの数が 4 の場合、最小インスタンスはデフォルトで 4 です。最小インスタンスを 8、12、16 増やすことができます。
- 最大インスタンス。この Autosale グループにプロビジョニングする必要があるインスタンスの最大数を選択します。
- インスタンスの最大数は、最小インスタンス値以上である必要があります。設定できるインスタンスの最大数は、アベイラビリティーゾーンの数に 32 を掛けた数と同じです。
- インスタンスの最大数 = アベイラビリティーゾーンの数 * 32
- ドレイン接続タイムアウト **(**分**)**。ドレイン接続タイムアウト期間を選択します。スケールイン中、プロビジョニング解除のためにインスタンスが選択されると、Citrix ADM は Autocale グループへの新しい接続を処理するインスタンスを削除し、指定された時間が経過するまで待機してからプロビジョニング解除します。このオプションでは、プロビジョニング解除前にこのインスタンスへの既存の接続をドレインアウトできます。
- クールダウン期間 **(**分**)**。クールダウン期間を選択します。スケールアウト時のクールダウン期間は、スケールアウトが発生した後に統計の評価を停止する必要がある時間です。このスケールアウトにより、次回のスケーリング決定が行われる前に、現在のインスタンスのセットで現在のトラフィックが安定し、平均化できるようになり、Autoscale グループのインスタンスが有機的に増加することが保証されます。
- **DNS** 存続時間 **(**秒**)**。ルータによって廃棄されるまでにパケットがネットワーク内に存在するように設定される時間（秒単位）を選択します。このパラメータは、トラフィック分散モードが AWS route53 を使用した DNS の場合にのみ適用されます。
- 総再生時間 **(**分**)**。総再生時間を選択します。スケーリングが発生するために、スケールパラメータのしきい値を超える必要のある時間。この指定された時間内に収集されたすべてのサンプルでしきい値を超えると、スケーリングが行われます。



3. ［次へ］をクリックします。

Citrix ADC インスタンスを **Provisioning** するためのライセンスの構成

次のいずれかのモードを選択して、AutoScale グループの一部である Citrix ADC インスタンスにライセンスを付与します。

- **Citrix ADM** 使用: Citrix ADC インスタンスの Provisioning 中に、Autoscale グループは Citrix ADM からライセンスをチェックアウトします。
- **AWS** クラウドの使用: [クラウドから割り当て] オプションは、AWS マーケットプレイスで利用可能な Citrix 製品ライセンスを使用します。Citrix ADC インスタンスの Provisioning 時に、Autoscale グループはマーケットプレイスのライセンスを使用します。

  AWS マーケットプレイスのライセンスを使用する場合は、[プロビジョニングパラメータ] タブで製品またはライセンスを指定します。

詳しくは、「ライセンス要件」を参照してください。

Citrix ADM ライセンスを使用する

1. [ライセンス] タブで、[**ADM** から割り当て] を選択します。
2. [ライセンスの種類] で、リストから次のいずれかのオプションを選択します。
   - 帯域幅ライセンス**:** [帯域幅ライセンスタイプ] リストから、次のいずれかのオプションを選択できます。
     - プール容量**:** Autoscale グループ内のすべての新しいインスタンスに割り当てる容量を指定します。

       共通プールから、Autoscale グループの各 ADC インスタンスは 1 つのインスタンス・ライセンスをチェックアウトし、帯域幅が指定されている分だけチェックアウトします。

  - **VPX** ライセンス： Citrix ADC VPX インスタンスがプロビジョニングされると、インスタンスは Citrix ADM からライセンスをチェックアウトします。

- 仮想 **CPU** ライセンス：プロビジョニングされた Citrix ADC VPX インスタンスは、Autoscale グループで実行されているアクティブな CPU の数に応じてライセンスをチェックアウトします。

> 注:
>
> プロビジョニングされたインスタンスが削除または破棄されると、適用されたライセンスは Citrix ADM ライセンスプールに戻ります。これらのライセンスは、次回の Autoscale 時に新しいインスタンスをプロビジョニングするために再利用することができます。

3. [ライセンスエディション] で、ライセンスエディションを選択します。Autoscale グループは、指定されたエディションを使用してインスタンスをプロビジョニングします。
4. ［次へ］をクリックします。

クラウドパラメータの設定

1. [クラウドパラメータ] タブで、次の詳細を入力します。
   - **IAM** ロール: AWS で作成した IAM ロールを選択します。IAM ロールは、AWS で ID を実行できる操作と実行できない操作を決定するアクセス権限ポリシーを持つ AWS ID です。
   - 製品：プロビジョニングする Citrix ADC 製品バージョンを選択します。
   - バージョン：Citrix ADC 製品のリリースバージョンとビルド番号を選択します。リリースバージョンとビルド番号は、選択した製品に基づいて自動的に入力されます。
   - **AWS AMI ID**: 選択したリージョンに固有の AMI ID を入力します。
   - インスタンスタイプ: EC2 インスタンスタイプを選択します。

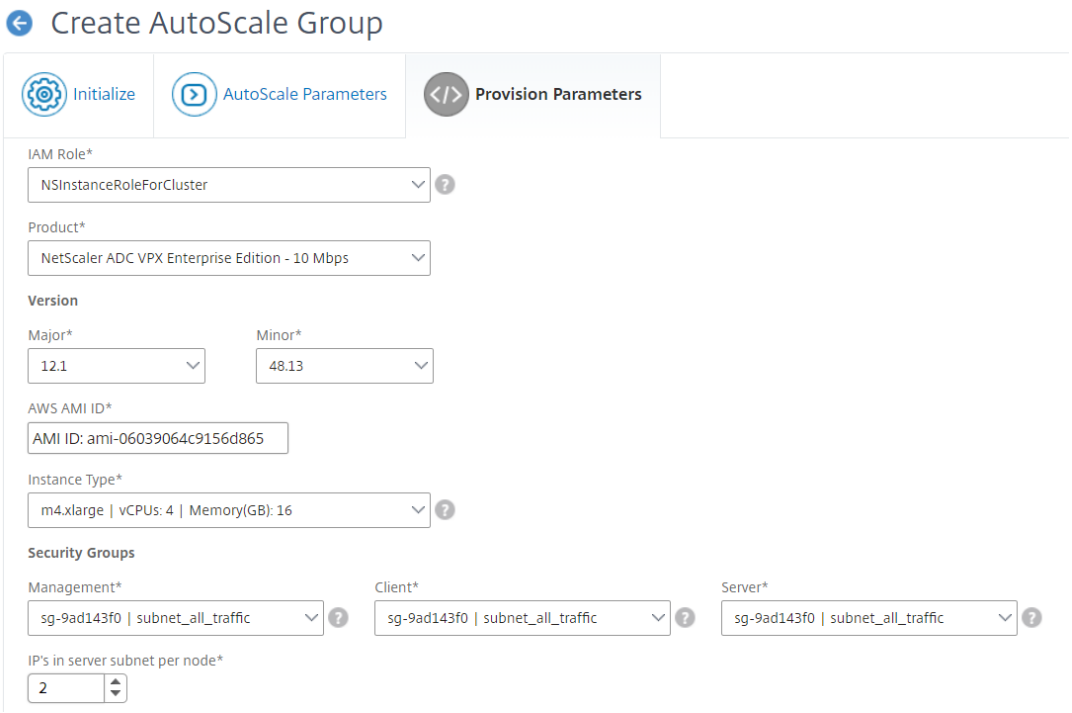
     > 注:
     >
     > 選択した製品の推奨インスタンスタイプは、デフォルトで自動入力されます。

   - セキュリティグループ：セキュリティグループは、Citrix ADC VPX インスタンスのインバウンドトラフィックとアウトバウンドトラフィックを制御します。制御する着信トラフィックと発信トラフィックの両方のルールを作成します。次のサブネットに適切な値を選択します。
   - 管理。Citrix ADC VPX インスタンスの管理専用のアカウント内の既存のセキュリティグループ。受信規則は、次の TCP ポートおよび UDP ポートで許可されます。

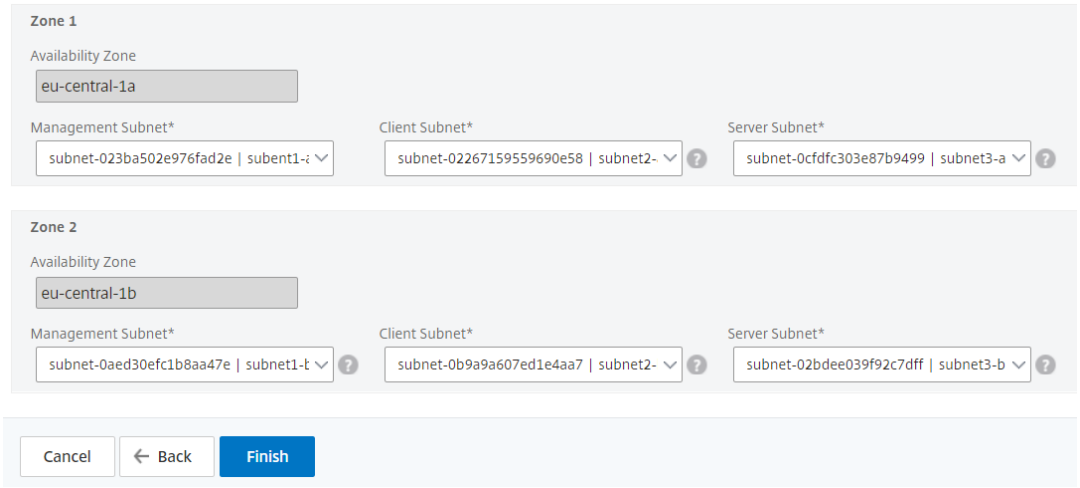
     TCP: 80, 22, 443, 3008—3011, 4001
     UDP: 67, 123, 161, 500, 500, 7000

     セキュリティグループで、Citrix ADM エージェントが VPX にアクセスできるようにすることを確認します。

- クライアント。Citrix ADC VPX インスタンスのクライアント側通信専用のアカウント内の既存のセキュリティグループ。通常、受信規則は TCP ポート 80、22、および 443 で許可されます。
- サーバー。Citrix ADC VPX サーバー側通信専用アカウント内の既存のセキュリティグループ。
- [ノードあたりのサーバーサブネット内の IP]: セキュリティグループのノードごとのサーバーサブネット内の IP アドレスの数を選択します。

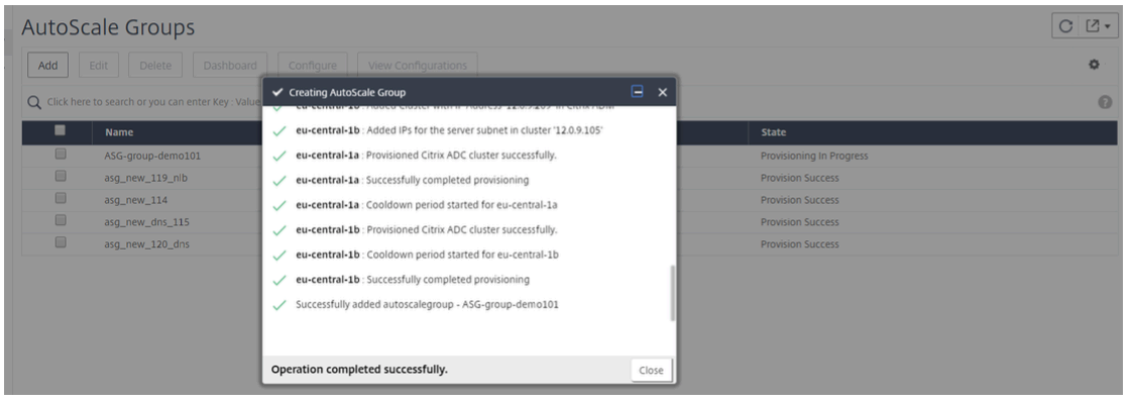


- **Zone**: 移入されるゾーンの数は、選択したアベイラビリティーゾーンの数と同じです。各ゾーンについて、次のサブネットに適切な値を選択します。
- 管理。管理専用の仮想プライベートクラウド（VPC）内の既存のサブネット。Citrix ADC は AWS サービスに連絡する必要があり、インターネットアクセスが必要です。NAT Gateway を設定し、このサブネットからのインターネットアクセスを許可するルートテーブルエントリを追加します。
- クライアント。クライアント側専用の仮想プライベートクラウド（VPC）内の既存のサブネット。通常、Citrix ADC は、インターネットからパブリックサブネット経由でアプリケーションのクライアントトラフィックを受信します。クライアントサブネットを、インターネット Gateway へのルートを持つルートテーブルに関連付けます。このサブネットにより、Citrix ADC はインターネットからアプリケーショントラフィックを受信できます。
- サーバー。アプリケーションサーバーは、サーバーサブネットにプロビジョニングされます。すべてのアプリケーションサーバーがこのサブネットにあり、このサブネット経由で Citrix ADC からアプリケーショントラフィックを受信します。



2. [完了] をクリックします。

   AutoScale グループの作成ステータスを示す進行状況ウィンドウが表示されます。Autocale グループの作成とプロビジョニングには、数分かかる場合があります。



AutoScale グループのアプリケーションを構成する

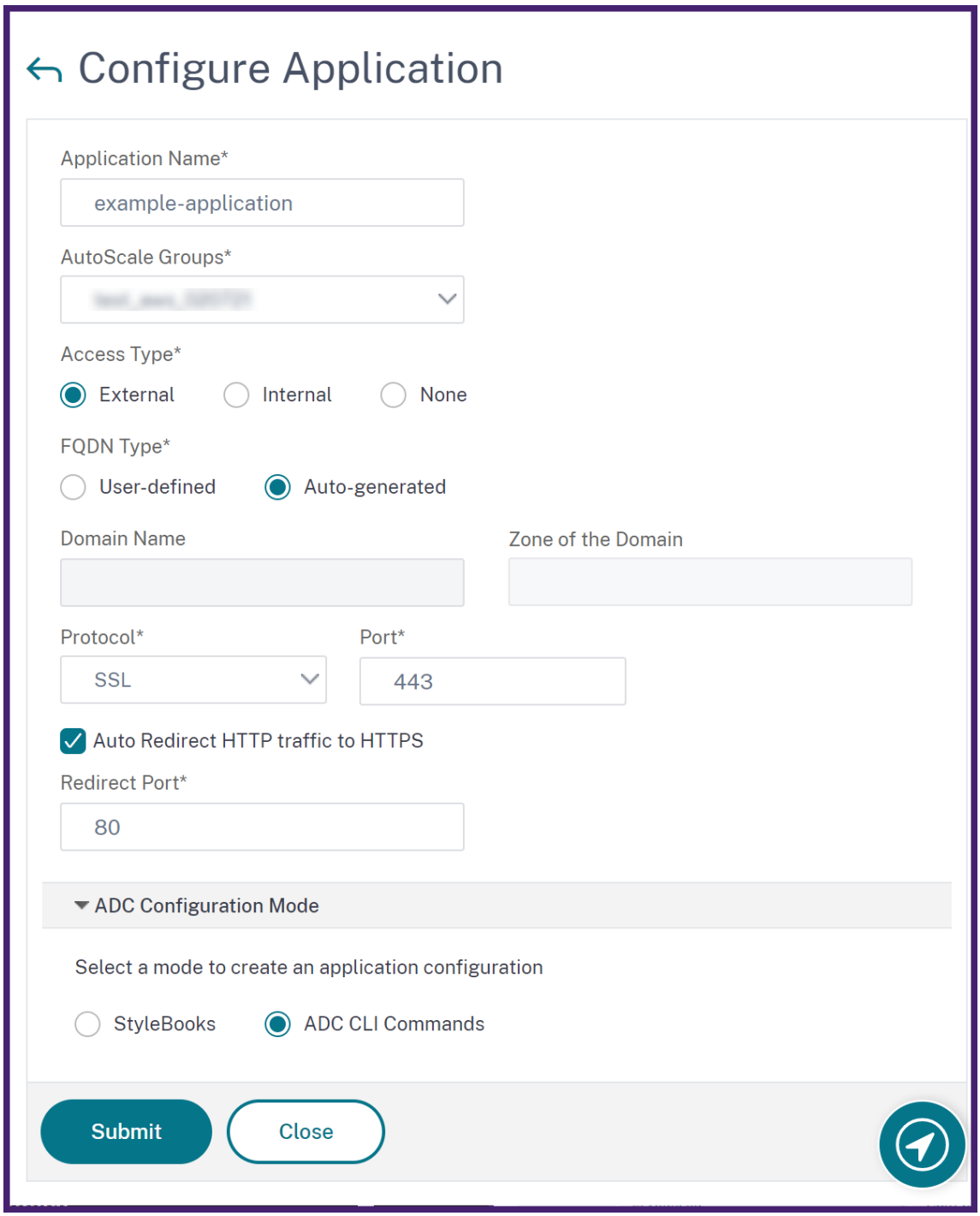
1. Citrix ADM で、[ネットワーク] > [**AutoScale** グループ] に移動します。
2. 作成した Autoscale グループを選択し、[設定] をクリックします。
3. 「アプリケーションの構成」で、次の詳細を指定します。

   - アプリケーション名 -アプリケーションの名前を指定します。
   - アクセスタイプ -ADM Auto Scaling ソリューションは外部アプリケーションと内部アプリケーションの両方に使用できます。必要なアプリケーションアクセスタイプを選択します。
   - **FQDN** タイプ -ドメイン名とゾーン名を割り当てるモードを選択します。

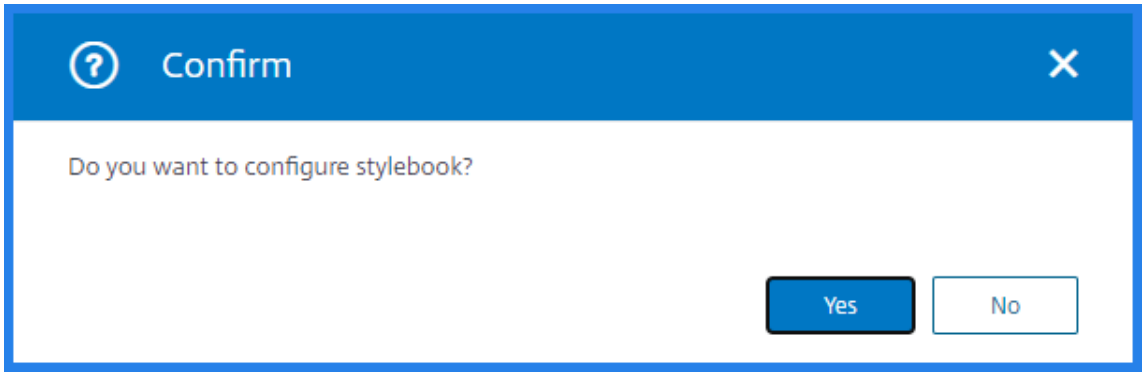
     手動で指定する場合は、[ユーザー定義] を選択します。ドメイン名とゾーン名を自動的に割り当てるには、[自動生成] を選択します。

- ドメイン名 -アプリケーションのドメイン名を指定します。このオプションは、[ユーザ定義 FQDN タイプ] を選択した場合にのみ適用されます。
- **[** ドメインのゾーン]: リストからアプリケーションのゾーン名を選択します。このオプションは、[ユーザ定義 FQDN タイプ] を選択した場合にのみ適用されます。

  このドメインとゾーン名は、AWS の仮想サーバーにリダイレクトされます。たとえば、`app.example.com`でアプリケーションをホストする場合、`app`はドメイン名、`example.com`はゾーン名です。
- **Protocol**： リストからプロトコルタイプを選択します。設定されたアプリケーションは、選択したプロトコルタイプに応じてトラフィックを受信します。
- [ポート]: ポート値を指定します。指定されたポートは、アプリケーションと Autosale グループ間の通信を確立するために使用されます。



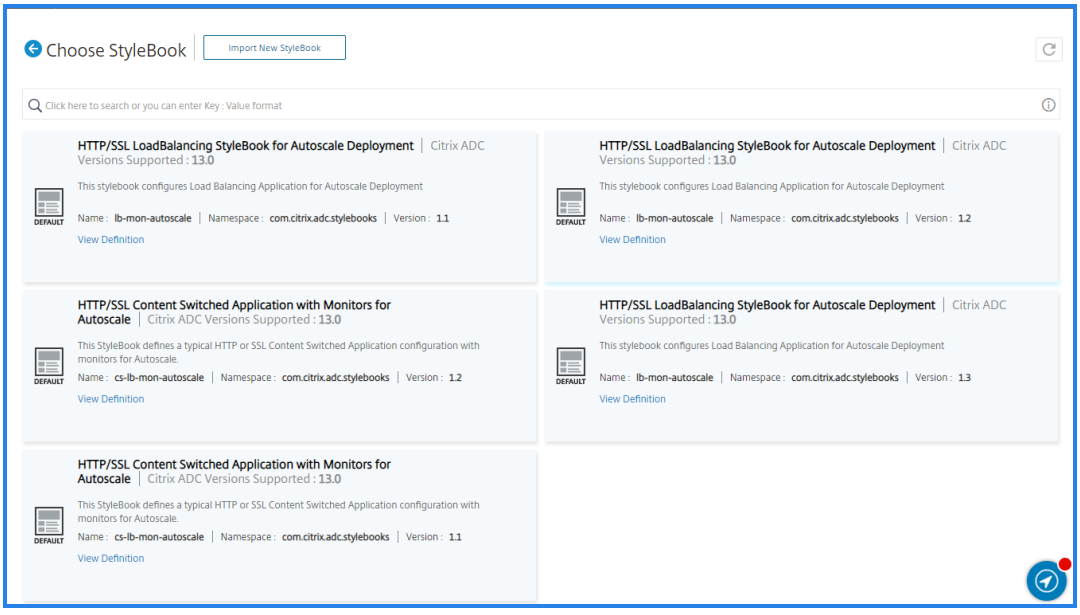
StyleBooks を使用してアプリケーションを構成する場合は、確認ウィンドウで [はい] を選択します。



> メモ今後次の詳細を変更する場合は
>
> 、アプリケーションのアクセスタイプを変更します。
>
> - FQDN タイプ
> - ドメイン名
> - ドメインのゾーン

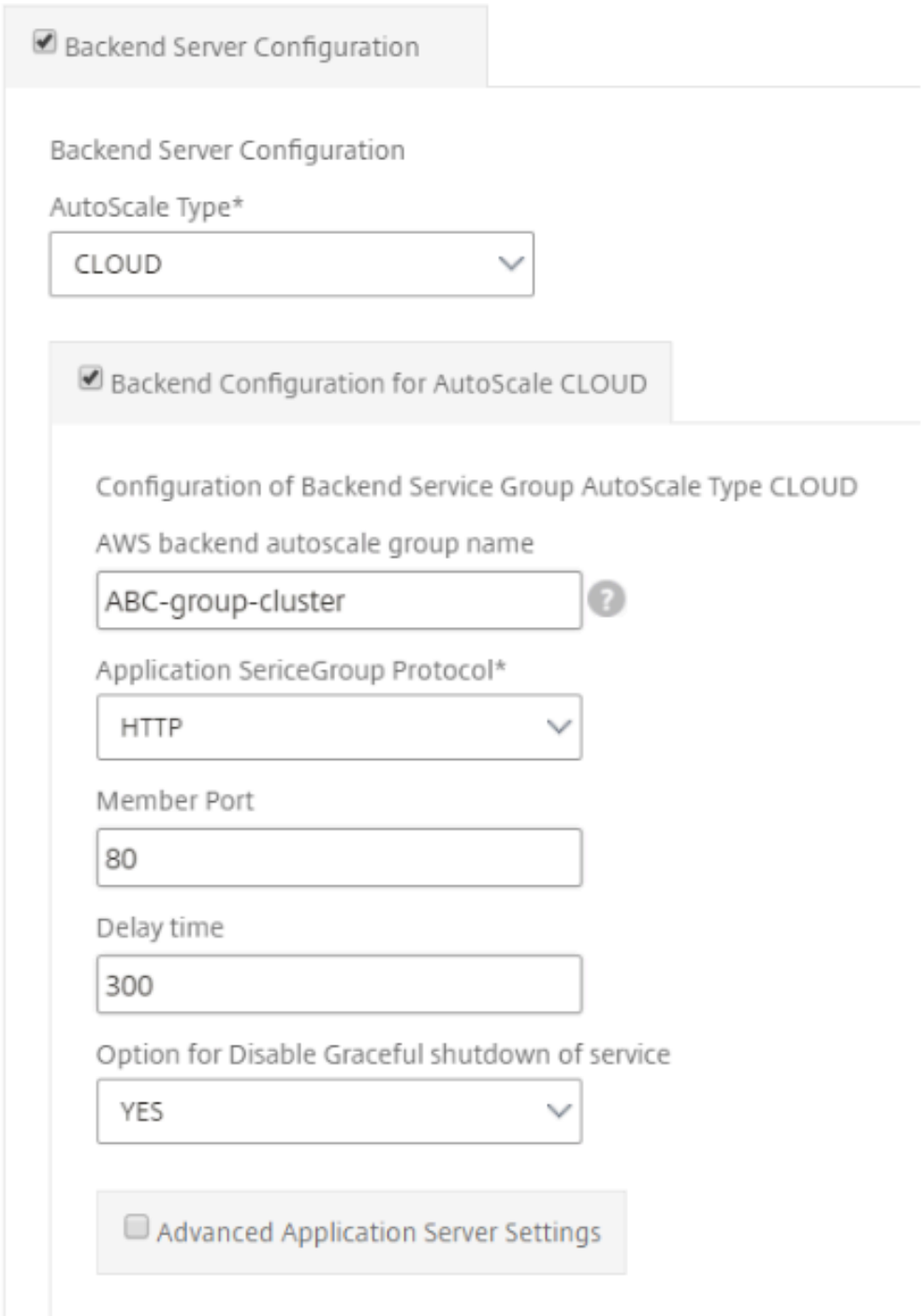
4. [**Choose StyleBook**] ページには、Autoscale クラスターに構成を展開するために使用できるすべての StyleBooks が表示されます。

   - 適切なスタイルブックを選択します。たとえば、**HTTP/SSL** 負荷分散 **StyleBook** を使用できます。新しい StyleBook をインポートすることもできます。



   - StyleBook をクリックして、必要な構成を作成します。
     StyleBook がユーザーインターフェイスページとして開きます。ここで、この StyleBook で定義されているすべてのパラメーターに対して値を入力できます。
   - すべてのパラメータの値を入力します。
   - AWS でバックエンドサーバーを作成する場合は、[バックエンドサーバー設定] を選択します。さらに、

[**AWS EC2** 自動スケーリング] > [クラウド] を選択し、すべてのパラメータに値を入力します。



- 選択した StyleBook によっては、いくつかのオプション設定が必要になる場合があります。たとえば、モニターの作成、SSL 証明書の設定などが必要になる場合があります。
- ［作成］をクリックして、Citrix ADC クラスターで構成を展開します。

- アプリケーションまたは仮想サーバーの FQDN は、構成およびデプロイ後に変更できません。

アプリケーションの FQDN は、DNS を使用して IP アドレスに解決されます。この DNS レコードはさまざまなネームサーバー間でキャッシュされる可能性があるため、FQDN を変更すると、トラフィックがブラックホールになる可能性があります。

- SSL セッション共有は、アベイラビリティーゾーン内で期待どおりに機能しますが、アベイラビリティーゾーン間で機能する場合は、再認証が必要です。

  SSL セッションはクラスター内で同期されます。アベイラビリティーゾーンにまたがる Autosale グループには、各ゾーンに別々のクラスターがあるため、ゾーン間で SSL セッションを同期することはできません。

- 最大クライアントや流出などの共有制限は、アベイラビリティーゾーンの数に基づいて静的に設定されます。手動で計算した後、この制限を設定します。`Limit = \<Limit required\>/\<number of zones\>`。

  共有制限は、クラスター内のノード間で自動的に分散されます。アベイラビリティーゾーンにまたがる Autosale グループには、各ゾーンに別々のクラスターが存在するため、これらの制限を手動で計算する必要があります。

Citrix ADC クラスターのアップグレード

クラスタノードを手動でアップグレードします。まず、既存のノードのイメージをアップグレードしてから、Citrix ADM から AMI を更新します。

> 重要:
>
> アップグレード中は、次のことを確認してください。
>
> - スケールインまたはスケールアウトはトリガーされません。
> - Autoscale グループのクラスタでは、構成の変更を実行しないでください。
> - 以前のバージョンの`ns.conf`ファイルのバックアップを保持します。アップグレードが失敗した場合は、以前のバージョンにフォールバックできます。

Citrix ADC クラスタノードをアップグレードするには、次の手順に従います。

1. MAS ASG ポータルで Autoscale グループを無効にします。
2. アップグレードする Autoscale グループ内のクラスタの 1 つを選択します。
3. トピックCitrix ADC クラスターのアップグレードまたはダウングレードに記載されている手順に従います。

   > 注
   >
   > - クラスタ内の 1 つのノードをアップグレードします。
   > - アプリケーショントラフィックに障害がないか監視します。
   > - 問題や障害が発生した場合は、以前にアップグレードしたノードをダウングレードします。それ以外の場合は、すべてのノードのアップグレードを続行します。

4. Autoscale グループ内のすべてのクラスタのノードのアップグレードを続行します。

> 注:
>
> いずれかのクラスターのアップグレードが失敗した場合は、Autoscale グループ内のすべてのクラスターを以前のバージョンにダウングレードします。トピックCitrix ADC クラスターのアップグレードまたはダウングレードに記載されている手順に従います。

5. すべてのクラスターが正常にアップグレードされたら、MAS ASG ポータルで AMI を更新します。AMI は、アップグレードに使用されたイメージと同じバージョンである必要があります。
6. Autoscale グループを編集し、アップグレードされたバージョンに対応する AMI を入力します。
7. ADM ポータルで Autoscale グループを有効にします。

Autoscale グループ構成の変更

- Autoscale グループ構成を変更したり、Autoscale グループを削除したりできます。変更できるのは、次の Autoscale グループパラメータだけです。
  - トラフィック分散モード
  - しきい値パラメータの最大値と最小値
  - 最小および最大インスタンス値
  - 排水接続期間の値
  - クールダウン期間の値
  - 存続時間の価値 — トラフィック分散モードが DNS の場合
  - ウォッチの継続時間の値
- Autoscale グループは、作成後に削除することもできます。

  Autoscale グループを削除すると、すべてのドメインと IP アドレスが DNS/NLB から登録解除され、クラスターノードのプロビジョニングが解除されます。

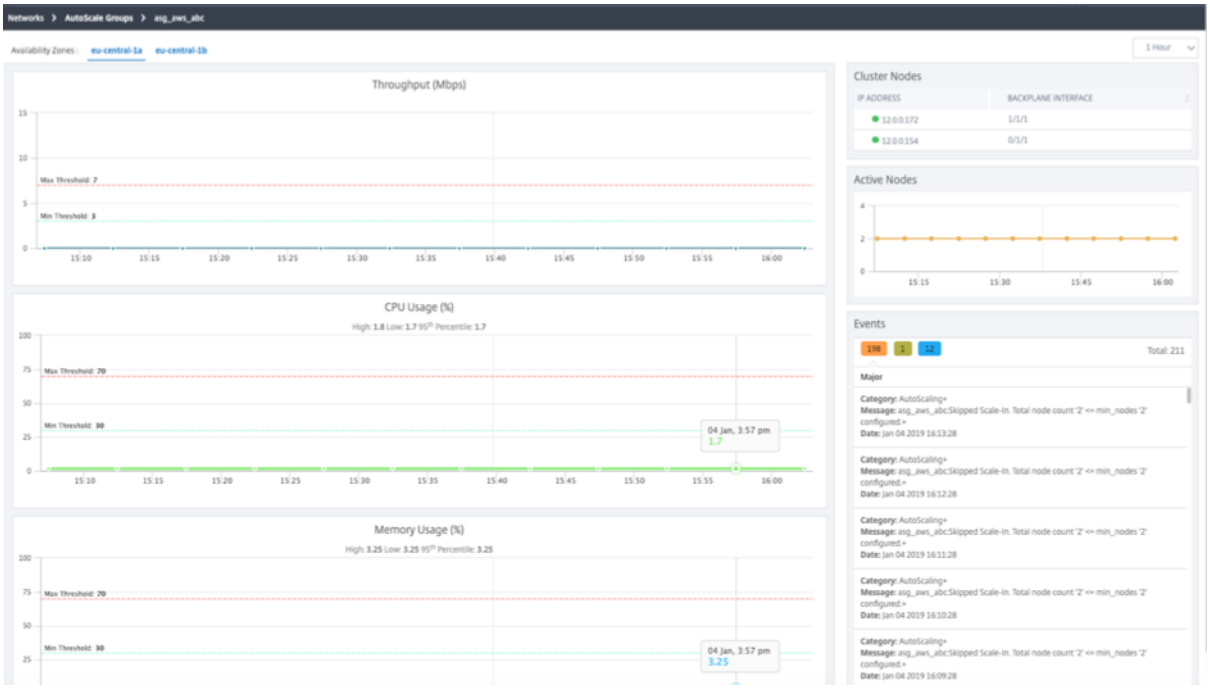
ダッシュボード

May 7, 2021

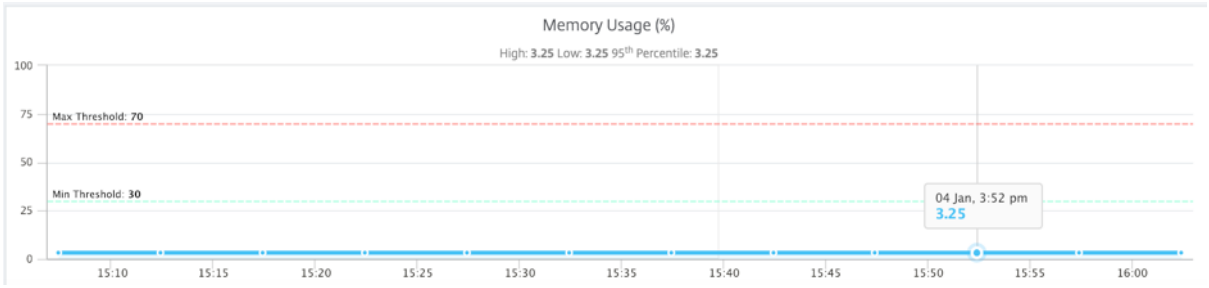
1. Citrix ADM で、［ネットワーク］**>**［グループの **Autoscale**］に移動します。
2. [Autoscale] グループを選択し、[ダッシュボード] をクリックします。

選択したモニタリングパラメータのグラフを表示できます。右側のパネルには、自動スケーリングをトリガーするイベントが表示されます。左側のパネルには、ゾーンごとのクラスタ内のアクティブなノード、アクティブなノードのグラフ、およびイベントが表示されます。

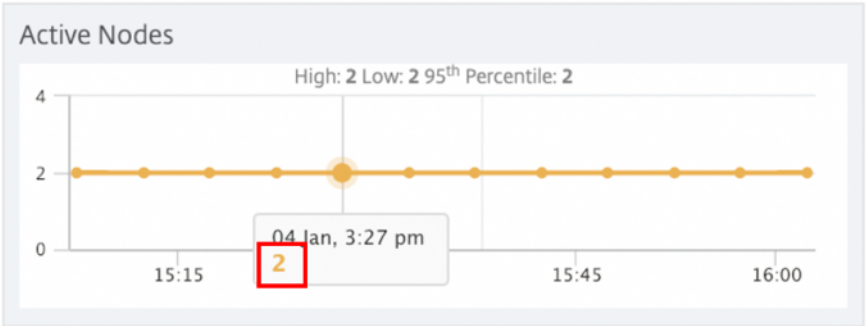
次の図は、サンプルのダッシュボードを示しています。



次の図は、AutoScale ダッシュボードのメモリ使用量イベントを示しています。



次の図は、アクティブなノードのグラフを示しています。タイムスタンプの下の数字は、アクティブノードの数を示します。アベイラビリティーゾーンに含まれるアクティブなノードの数は、いつでも表示できます。



Microsoft Azure での Citrix ADC VPX インスタンスのプロビジョニング

May 7, 2021

Azure でホストされるアプリケーションまたはサービスは、クラウドのメリットとともに、安全なトラフィック管理とネットワークリソースの効率的な最適化が必要です。Microsoft Azure でプロビジョニングされた Citrix ADC VPX インスタンスは、安全なトラフィック管理、リソース消費の最適化、Web アプリケーションの所有コストの削減を実現します。

Citrix ADM を使用すると、Azure での ADC VPX インスタンスのデプロイ、セットアップ、および管理を自動化できます。ADM を使用して Citrix ADC VPX インスタンスをプロビジョニングすると、クラウドの柔軟性と柔軟性と Citrix ADC 制御機能が組み合わされます。

プロビジョニングでサポートされる Citrix ADC Azure 仮想マシンイメージ

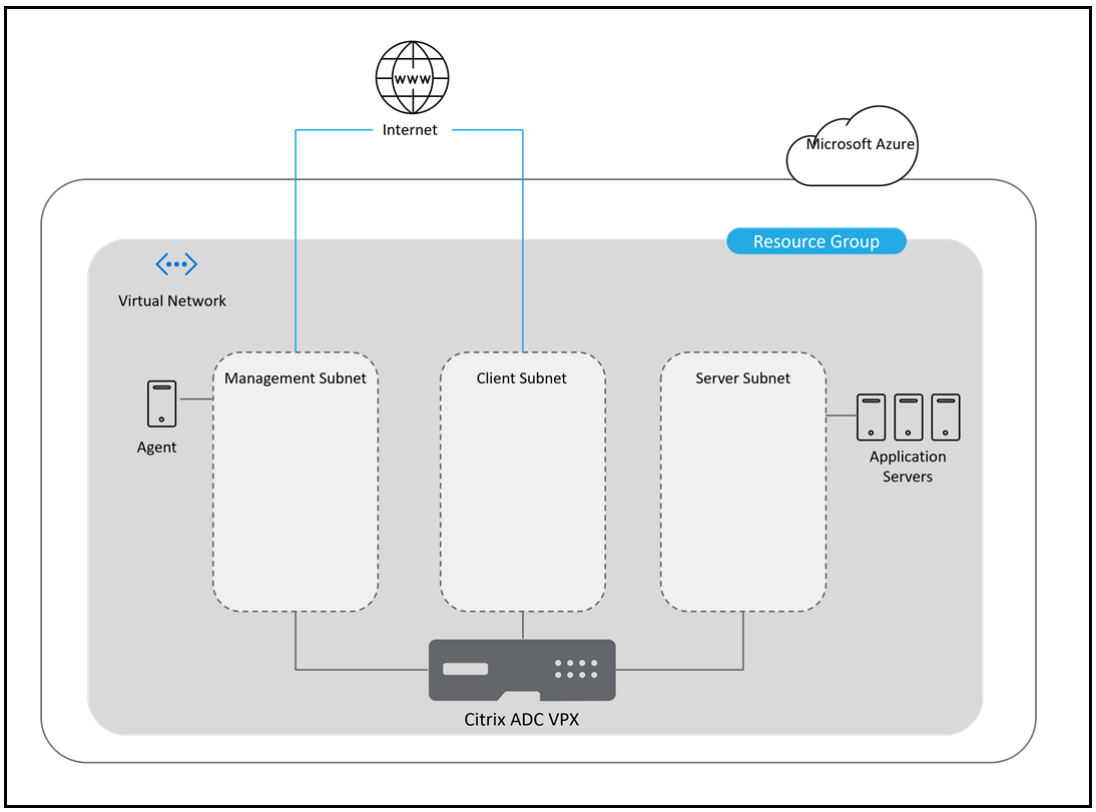
最低 3 つの NIC をサポートする Azure 仮想マシンイメージを使用します。Citrix ADC VPX インスタンスのプロビジョニングは、プレミアムエディションおよびアドバンスエディションでのみサポートされます。Azure 仮想マシンイメージタイプについて詳しくは、「仮想マシンの種類とサイズ (Microsoft ドキュメントを参照)」を参照してください。

プロビジョニングに推奨される仮想マシンサイズは次のとおりです。

- Standard_DS3_v2
- Standard_B2ms
- Standard_DS4_v2

Citrix ADM 展開アーキテクチャ

次の画像は、Microsoft Azure で Citrix ADM と Azure を接続して Citrix ADC VPX インスタンスをプロビジョニングする方法の概要を示しています。



Microsoft Azure で Citrix ADC VPX インスタンスをプロビジョニングおよび管理するには、3 つのサブネットが必要です。サブネットごとにセキュリティグループを作成する必要があります。Citrix Gateway で指定されたルールによって、サブネット間の通信が制御されます。

Citrix ADM サービスエージェントは、Citrix ADC VPX インスタンスのプロビジョニングと管理に役立ちます。

前提条件

このセクションでは、Citrix ADC VPX インスタンスをプロビジョニングする前に、Microsoft Azure および Citrix ADM で完了する必要がある前提条件について説明します。

このドキュメントでは、次のことを前提としています。

- Azure Resource Manager のデプロイモデルをサポートする Microsoft Azure アカウントを持っています。
- Microsoft Azure でリソースグループがあります。

アカウントやその他のタスクの作成方法について詳しくは、「Microsoft Azure ドキュメント」を参照してください。

Microsoft Azure コンポーネントのセットアップ

Citrix ADM で Citrix ADC VPX インスタンスをプロビジョニングする前に、Azure で次のタスクを実行します。

1. 仮想ネットワークを作成する。

2.「セキュリティグループの作成」を参照してください。

3.「サブネットの作成」を参照してください。

4. Microsoft Azure で Citrix ADC VPX ライセンスを購読する。

5. アプリケーションの作成と登録。

6.「Citrix ADM サービスエージェントの設定」を参照してください。

仮想ネットワークを作成する

1. Microsoft Azure ポータルにログオンします。

2. [リソースの作成] を選択します。

3. [ネットワーク] を選択し、[仮想ネットワーク] をクリックします。

4. 必要なパラメータを指定します。

   - [リソースグループ] で、Citrix ADC VPX 製品をデプロイするリソースグループを指定する必要があります。
   - [**Location**] では、アベイラビリティーゾーンをサポートするロケーションを指定する必要があります。
     - 米国中部
     - 米国東部 2
     - フランス中部
     - 北ヨーロッパ
     - 東南アジア
     - 西ヨーロッパ
     - 米国西部 2

   > 注:
   >
   > このリソースグループに存在するアプリケーションサーバー。

5. [作成] をクリックします。

詳しくは、『Microsoft 社のドキュメント』の「Azure 仮想ネットワーク」を参照してください。

セキュリティグループの作成

仮想ネットワーク (VNet) に 3 つのセキュリティグループを作成します。それぞれ 1 つずつ管理、クライアント、およびサーバー接続に使用します。セキュリティグループを作成して、Citrix ADC VPX インスタンスのインバウンドトラフィックとアウトバウンドトラフィックを制御します。規則は、必要に応じていくつでも追加できます。

- 管理： Citrix ADC VPX の管理専用のアカウント内のセキュリティグループ。Citrix ADC は Azure サービスに接続する必要があり、インターネットアクセスが必要です。受信規則は、次の TCP ポートおよび UDP ポートで許可されます。
  - TCP：80、22、443、3008–3011、4001
  - UDP: 67、123、161、500、3003、4500、7000

  > 注
  >
  > セキュリティグループで、Citrix ADM エージェントが VPX にアクセスできるようにすることを確認します。

- クライアント： Citrix ADC VPX インスタンスのクライアント側通信専用のアカウント内のセキュリティグループ。通常、受信規則は TCP ポート 80、22、および 443 で許可されます。
- サーバー： Citrix ADC VPX サーバー側通信専用のアカウント内のセキュリティグループ。

Microsoft Azure でセキュリティグループを作成する方法について詳しくは、「ネットワークセキュリティグループを作成、変更、または削除する」を参照してください。

サブネットの作成

仮想ネットワーク (VNet) に 3 つのサブネットを作成します。各サブネットは管理、クライアント、およびサーバー接続用です。各サブネットについて、VNet で定義されているアドレス範囲を指定します。サブネットを配置するアベイラビリティーゾーンを指定します。

- 管理**:** 仮想ネットワーク (VNet) 内の管理専用のサブネット。Citrix ADC は Azure サービスに接続する必要があり、インターネットアクセスが必要です。
- クライアント**:** クライアント側専用の仮想ネットワーク (VNet) 内のサブネット。通常、Citrix ADC は、インターネットからパブリックサブネット経由でアプリケーションのクライアントトラフィックを受信します。
- サーバー：アプリケーションサーバーがプロビジョニングされるサブネット。すべてのアプリケーションサーバーがこのサブネットに存在し、このサブネットを介して Citrix ADC からのアプリケーショントラフィックを受信します。

> 注
>
> サブネットの作成時に、サブネットに対して適切なセキュリティグループを指定します。

Microsoft Azure でサブネットを作成する方法について詳しくは、「仮想ネットワークサブネットを追加、変更、または削除する」を参照してください。

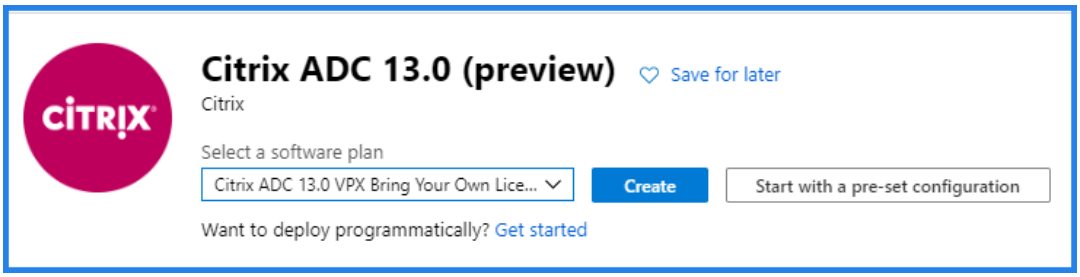
Microsoft Azure で **Citrix ADC VPX** ライセンスを購読する

1. Microsoft Azure ポータルにログオンします。
2. [リソースの作成] を選択します。

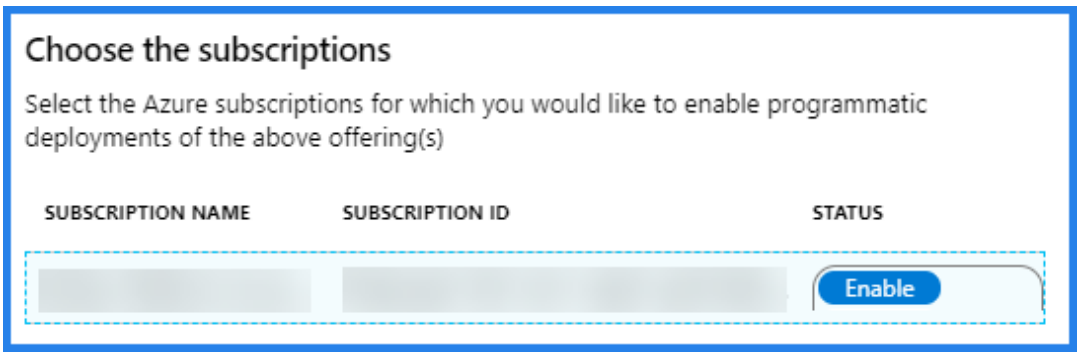
3. マーケットプレイスの検索バーで、`Citrix ADC`を検索して必要な製品バージョンを選択します。
4. **[** ソフトウェアプランの選択] リストで、次のいずれかのライセンスタイプを選択します。
   - 自分のライセンスを持参する
   - 詳細設定
   - Premium

   > 注
   >
   > - ［独自のライセンスを持ち込む］オプションを選択した場合、プロビジョニングするインスタンスは、Citrix ADC インスタンスのプロビジョニング中に Citrix ADM からライセンスをチェックアウトします。
   > - Citrix ADM では、「**Advanced** 」と「Prem **ium** 」は、それぞれ エンタープライズおよび プラチナと同等のライセンスタイプです。

5. 選択した Citrix ADC 製品に対してプログラムによる展開が有効になっていることを確認します。
   a) Bide プログラムで展開したいですか**?** で、[開始] をクリックします。

   b) ［サブスクリプションの選択］で［有効にする］を選択し、選択した Citrix ADC VPX エディションをプログラムで展開します。

   > 重要
   >
   > Azure で Citrix ADC VPX インスタンスをプロビジョニングするには、プログラムによる展開を有効にする必要があります。

   c) ［保存］をクリックします。

   d) **[** プログラムによる配置を設定**]** を閉じます。

6. ［作成］をクリックします。

アプリケーションの作成と登録

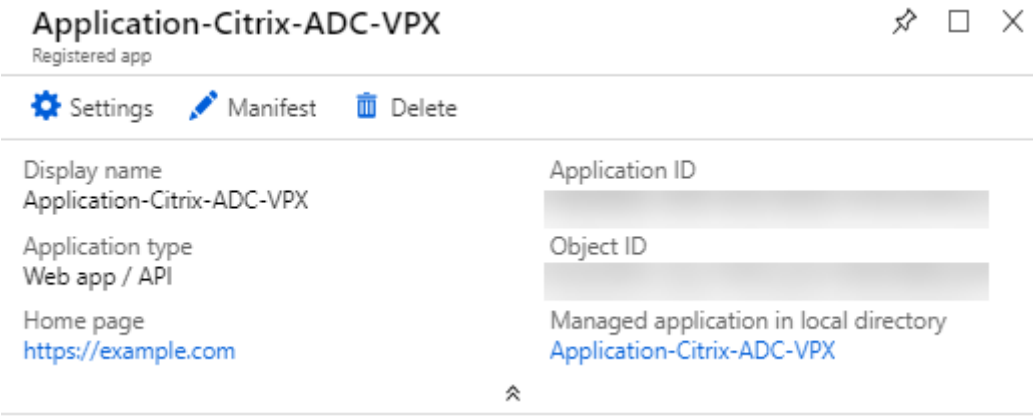
Citrix ADM は、このアプリケーションを使用して、Azure で Citrix ADC VPX インスタンスをプロビジョニングします。

Azure でアプリケーションを作成して登録するには:

1. Azure ポータルで、[**Azure Active Directory**] を選択します。
   このオプションでは、組織のディレクトリが表示されます。
2. アプリの登録を選択:
   a)「 名前 | **Name** | marvel」で、アプリケーションの名前を指定します。
   b) リストから アプリケーションの種類を選択します。
   c) [サインオン URL] で、アプリケーションにアクセスするアプリケーション URL を指定します。
3. [作成] をクリックします。

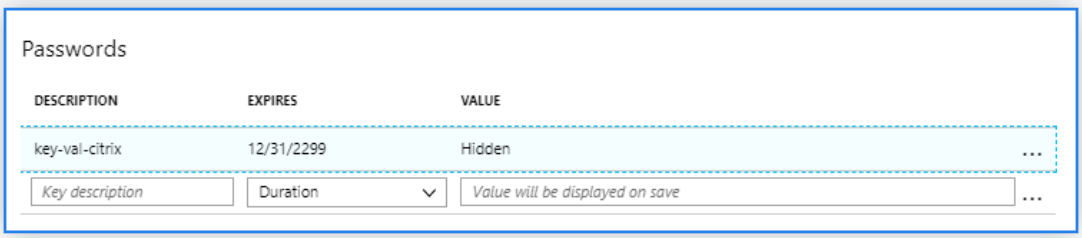
アプリの登録について詳しくは、「Microsoft 社のドキュメント」を参照してください。

Azure は、アプリケーション ID をアプリケーションに割り当てます。以下は、Microsoft Azure に登録されているアプリケーションの例です。



Citrix ADM でクラウドアクセスプロファイルを構成する場合は、次の ID をコピーし、これらの ID を指定します。

- [アプリケーション **ID]:** アプリケーションまたはクライアント ID を取得するための手順。
- ディレクトリ **ID:** ディレクトリ、テナント、またはオブジェクト ID を取得する手順。
- キー**:** キー値またはクライアントシークレット ID を取得する手順。



- サブスクリプション **ID:** ストレージアカウントからサブスクリプション ID をコピーします。

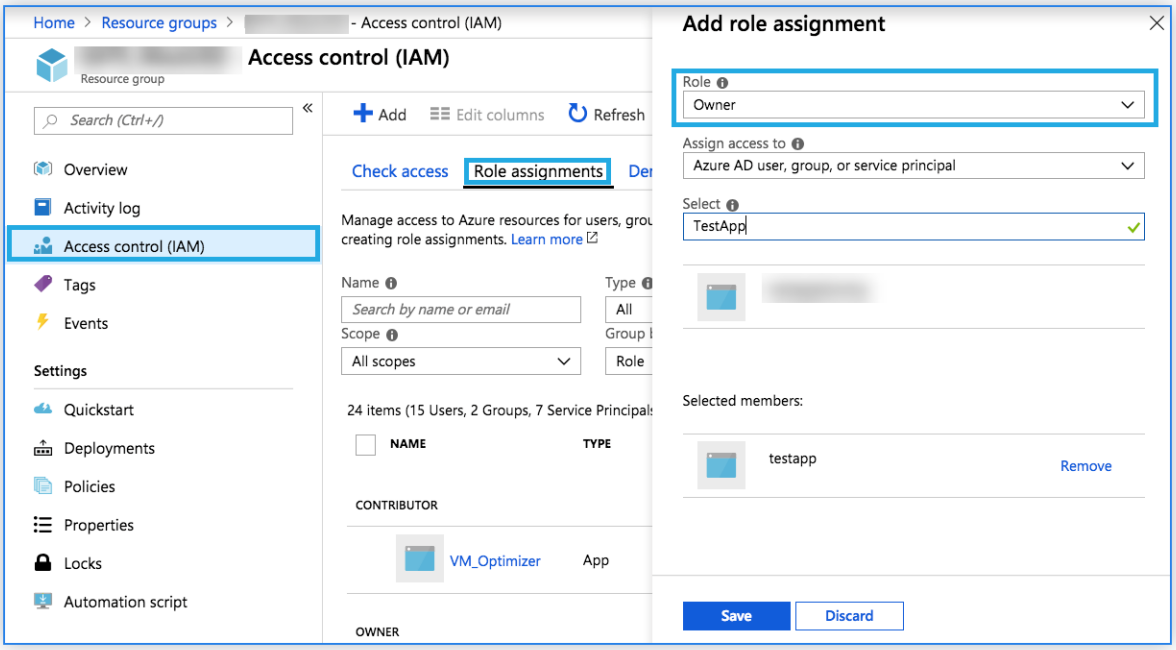
詳しくは、「Microsoft 社のドキュメント」を参照してください。

アプリケーションへのロールのアクセス許可の割り当て

Citrix ADM は、サービスとしてのアプリケーションの原則を使用して、Microsoft Azure で Citrix ADC インスタンスをプロビジョニングします。この権限は、選択したリソースグループにのみ適用されます。

登録済みアプリケーションにロールのアクセス許可を割り当てるには、Microsoft Azure サブスクリプションの所有者である必要があります。

1. Azure ポータルで、[リソースグループ] を選択します。
2. ロール権限を割り当てるリソースグループを選択します。
3. [アクセス制御 **(IAM)**] を選択します。
4. [役割の割り当て] で、[追加] をクリックします。
5. 「ロール」リストから「所有者」を選択します。
6. Citrix ADC インスタンスのプロビジョニングに登録されているアプリケーションを選択します。アプリケーションの作成と登録を参照してください。
7. [保存] をクリックします。



Citrix ADM サービスエージェントの設定

管理サブネットに Citrix ADM サービスエージェントをインストールします。このエージェントは、Citrix Application Delivery Management（Citrix ADM）と Microsoft Azure の管理対象インスタンスの仲介者として動作します。Microsoft Azure に Citrix ADM サービスエージェントをインストールする方法の詳細については、「Microsoft Azure クラウドへの Citrix ADM エージェントのインストール」を参照してください。

Citrix ADM コンポーネントのセットアップ

Citrix ADM で Citrix ADC VPX インスタンスをプロビジョニングする前に、Azure で次のタスクを実行します。

1. サイトを作成する。
2.「Citrix サービスエージェントにサイトを接続する」を参照してください。

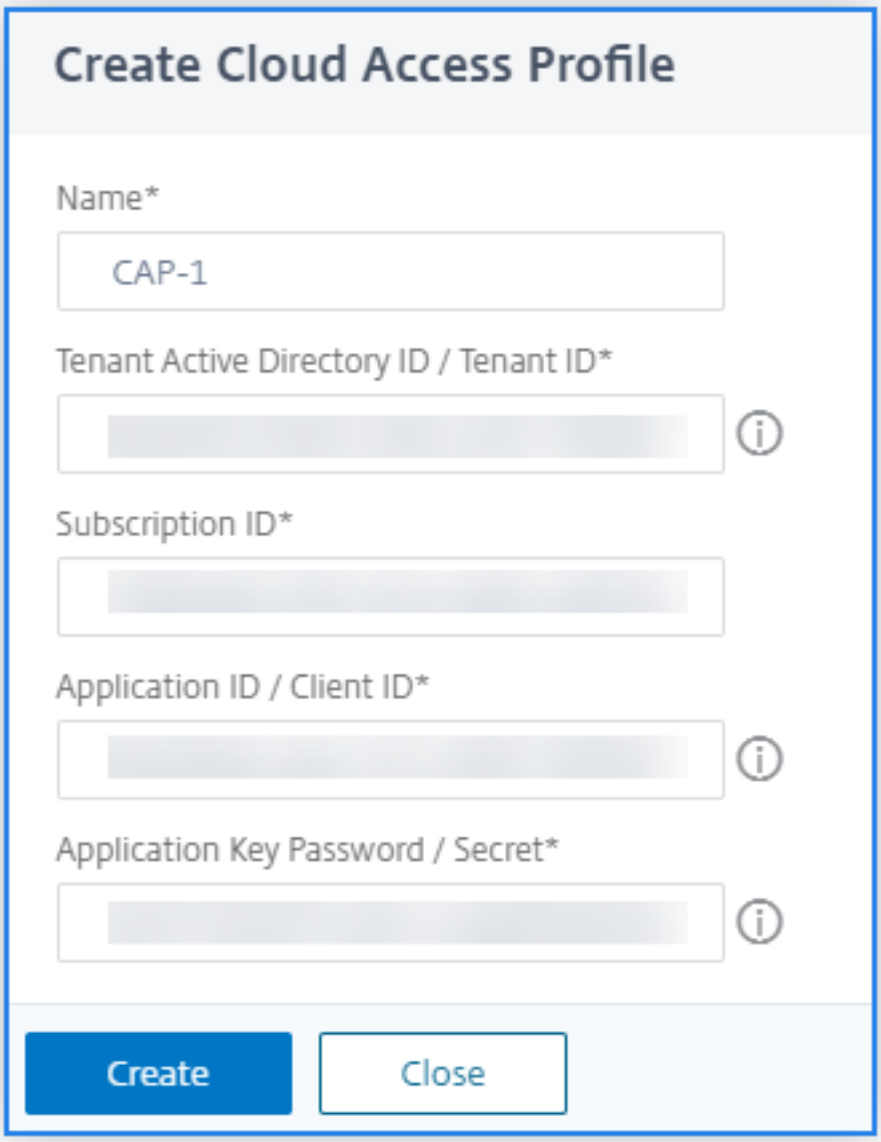
Citrix ADM でサイトを作成する

Citrix ADM でサイトを作成し、Microsoft Azure リソースグループに関連付けられた VNet の詳細を追加します。

1. Citrix ADM で、［ネットワーク］>［サイト］に移動します。
2.［追加］をクリックします。
3. **[** クラウドを選択**]** ペインで、
   a) サイトの種類として [データセンター] を選択します。
   b) [種類] リストから [**Azure**] を選択します。
   c) [**Azure** から **VNet** をフェッチする] チェックボックスをオンにします。
      このオプションを使用すると、Microsoft Azure アカウントから既存の VNet 情報を取得できます。
   d)［次へ］をクリックします。
4. **[** リージョンの選択**]** ペインで、
   a) [クラウドアクセスプロファイル] で、Microsoft Azure アカウント用に作成されたプロファイルを選択します。プロファイルがない場合は、プロファイルを作成します。
   b) クラウドアクセスプロファイルを作成するには、[追加] をクリックします。
   c)［名前］で、Citrix ADM で Azure アカウントを識別する名前を指定します。
   d) [テナント **Active Directory ID /**テナント **ID**] で、テナントの Active Directory ID または Microsoft Azure のアカウントを指定します。
   e) サブスクリプション **ID** を指定します。
   f) アプリケーション **ID** またはクライアント **ID** を指定します。
   g) アプリケーションキーのパスワード**/**シークレットを指定します。

h) ［作成］をクリックします。

詳しくは、「アプリケーションの作成と登録」および「Azure アプリケーションへのクラウドアクセスプロファイルのマッピング」を参照してください。



i) **VNet** で、管理する Citrix ADC VPX インスタンスを含む仮想ネットワークを選択します。

j) サイト名を指定します。

k) ［完了］をクリックします。

Azure アプリケーションへのクラウドアクセスプロファイルのマッピング

Citrix ADM 用語	**Microsoft Azure** 用語
テナント Active Directory ID /テナント ID	ディレクトリ ID
サブスクリプション ID	サブスクリプション ID
アプリケーション ID /クライアント ID	アプリケーション ID
アプリケーションキーのパスワード/シークレット	キーまたは証明書またはクライアントシークレット

Citrix ADM サービスエージェントにサイトを接続する

1. Citrix ADM で、［ネットワーク］>［エージェント］に移動します。
2. サイトをアタッチするエージェントを選択します。
3. [サイトの添付] をクリックします。
4. リストからアタッチするサイトを選択します。
5. ［保存］をクリックします。

構成タスク

Microsoft Azure リソースグループに関連付けられているサイトを使用して、Citrix ADC VPX インスタンスをプロビジョニングします。Citrix ADM サービスエージェントの詳細を提供し、そのエージェントにバインドされたインスタンスをプロビジョニングします。

1. Citrix ADM で、［ネットワーク］>［インスタンス］**>**［**Citrix ADC**］に移動します。
2. [**VPX**] タブで、[プロビジョニング] をクリックします。

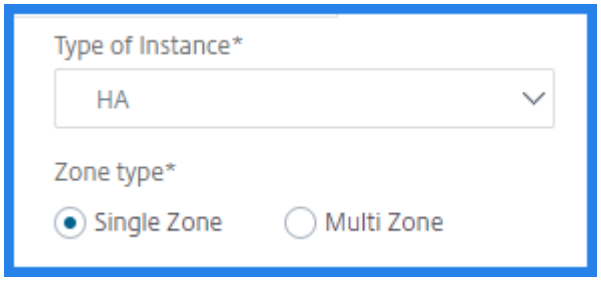
   このオプションでは、［クラウドでの **Citrix ADC VPX** のプロビジョニング］ページが表示されます。
3. [**Microsoft Azure**] を選択し、[次へ] をクリックします。インスタンスをプロビジョニングするために必要なパラメータを指定します。

基本パラメータの設定

1. [基本パラメータ] タブで、次の項目を指定します。
   - インスタンスのタイプ: リストから次のオプションのいずれかを選択します。
     - スタンドアロン -このオプションは、Microsoft Azure 上にスタンドアロンの Citrix ADC VPX インスタンスをプロビジョニングします。
     - **HA:** このオプションは、Microsoft Azure の高可用性 Citrix ADC VPX インスタンスをプロビジョニングします。

Citrix ADC VPX インスタンスを同じゾーンにプロビジョニングするには、［ゾーンの種類］で［シングルゾーン］オプションを選択します。

複数のゾーンにまたがって Citrix ADC VPX インスタンスをプロビジョニングするには、［ゾーンの種類］で［マルチゾーン］オプションを選択します。[クラウドパラメーター] タブで、Microsoft Azure で作成された各ゾーンのネットワークの詳細を指定します。

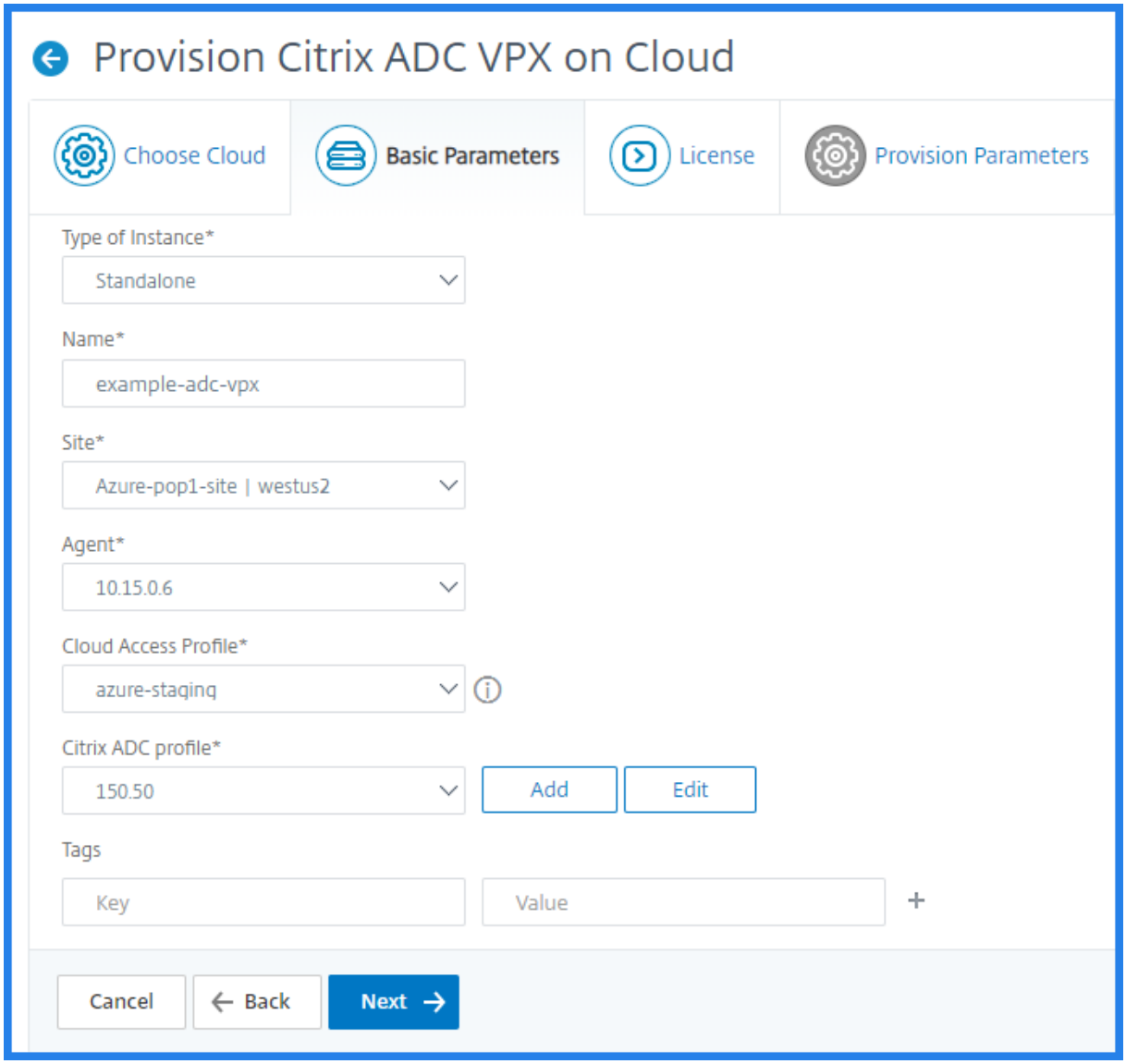


- 名前：ADC VPX インスタンスの名前を指定します。
- [サイト]: 前に作成したサイトを選択します。
- エージェント：Citrix ADC VPX インスタンスを管理するために作成されるエージェントを選択します。
- クラウドアクセスプロファイル -サイト作成時に作成されたクラウドアクセスプロファイルを選択します。
- **Citrix ADC** プロファイル：認証を提供するプロファイルを選択します。

  Citrix ADC VPX インスタンスにログオンする必要がある場合、Citrix ADM はデバイスプロファイルを使用します。

  > 注：
  >
  > 選択したデバイスプロファイルがMicrosoft Azure のパスワードルールに準拠していることを確認します。

2. ［次へ］をクリックします。



ライセンスの設定

ライセンスを ADC インスタンスに適用するには、次のいずれかのモードを選択します。

- **Citrix ADM** を使用する：プロビジョニングするインスタンスは、Citrix ADM からライセンスをチェックアウトします。
- **Microsoft Azure** の使用：［クラウドから割り当て］オプションでは、Azure マーケットプレイスで利用可能な Citrix 製品ライセンスが使用されます。プロビジョニングするインスタンスは、マーケットプレイスのライセンスを使用します。

  Azure Marketplace のライセンスを使用する場合は、[プロビジョニングパラメータ] タブで製品またはライセンスを指定します。

詳しくは、「ライセンス要件」を参照してください。

Citrix ADM ライセンスを使用する

このオプションを使用するには、[Azure でのライセンスソフトウェアの持ち込み] プランで Citrix ADC 製品をサブスクライブしていることを確認します。Microsoft Azure で Citrix ADC VPX ライセンスを購読するを参照してください。

1. [ライセンス] タブで、[**ADM** から割り当て] を選択します。
2. [ライセンスの種類] で、リストから次のいずれかのオプションを選択します。
   - 帯域幅ライセンス**:** [帯域幅ライセンスタイプ] リストから、次のいずれかのオプションを選択できます。
     - プールされた容量**:** インスタンスに割り当てる容量を指定します。

       ADC インスタンスは、共通プールから 1 つのインスタンス・ライセンスをチェックアウトし、指定された帯域幅だけを指定します。
     - **VPX** ライセンス: Citrix ADC VPX インスタンスがプロビジョニングされると、インスタンスは Citrix ADM からライセンスをチェックアウトします。
   - 仮想 **CPU** ライセンス: プロビジョニングされた Citrix ADC VPX インスタンスは、インスタンスで実行されている CPU の数に応じてライセンスをチェックアウトします。

   > 注:
   >
   > プロビジョニングされたインスタンスが削除または破棄されると、適用されたライセンスは Citrix ADM ライセンスプールに戻ります。これらのライセンスは、新しいインスタンスをプロビジョニングするために再利用することができます。
3. [ライセンスエディション] で、ライセンスエディションを選択します。ADM は、指定されたエディションを使用してインスタンスをプロビジョニングします。
4. [次へ] をクリックします。

プロビジョニングパラメータの構成

1. 「プロビジョニングパラメータ」タブで、次の項目を指定します。
   - リソースグループ: Citrix ADC **VPX** インスタンスをプロビジョニングするリソースグループを選択します。
   - [製品**/**ライセンス]- リストから必要なオプションを選択します。

   a) 一覧から、サポートされている仮想マシンのサイズを選択します。

   > 注:
   >
   > サポートされている製品および VM サイズの詳細については、「サポートされている Citrix ADC Azure 仮想マシンイメージ」を参照してください。

   b) ADC 用のクラウドアクセスプロファイルを選択します。

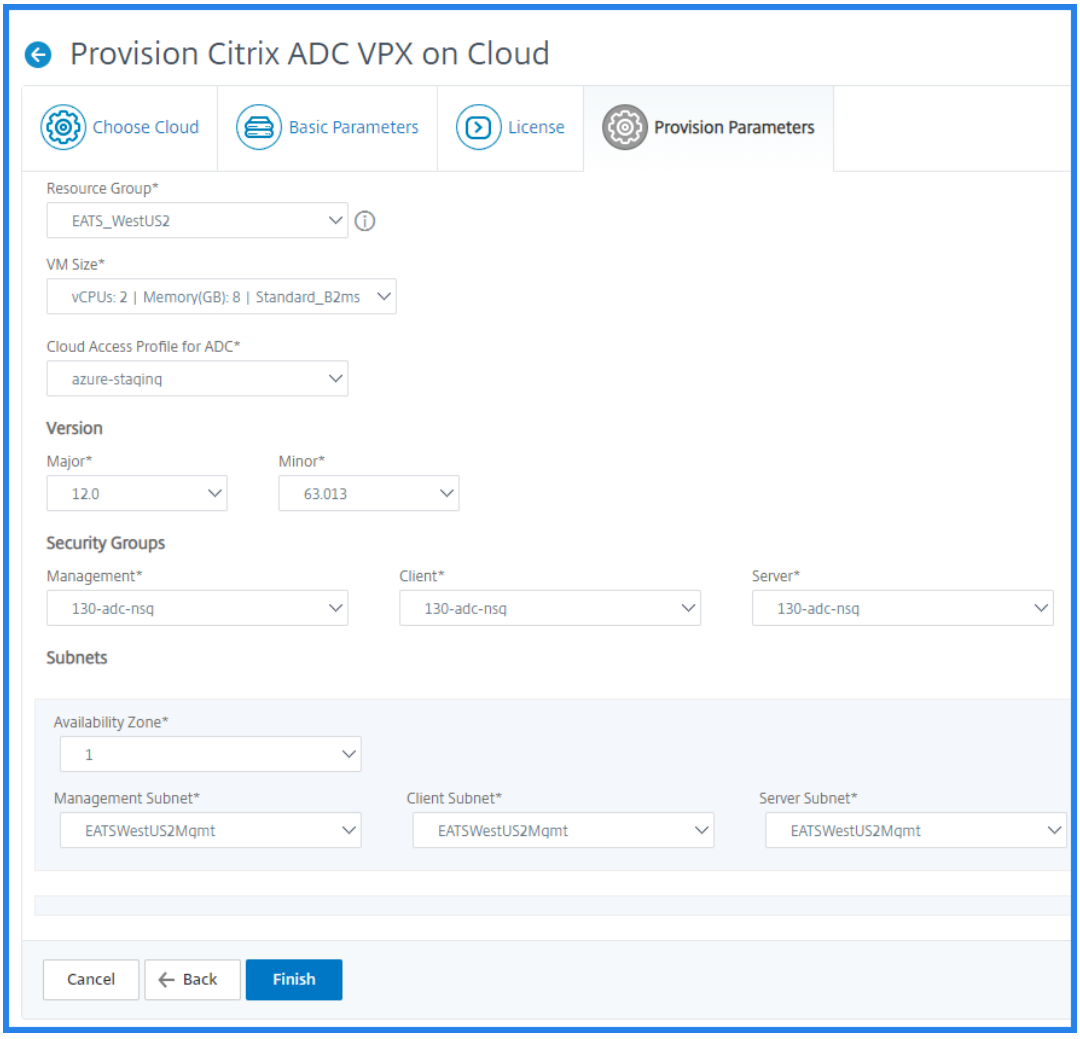
c) プロビジョニングする Citrix **ADC** のバージョンを選択します。Citrix ADC メジャーバージョンとマイナーバージョンの両方を選択します。

d) [セキュリティグループ] で、仮想ネットワークで作成した [管理]、[クライアント]、および [サーバー] セキュリティグループを選択します。

e) [サブネット] で、Azure の必要なアベイラビリティーゾーン数を指定します。

f) [サブネット] で、仮想ネットワーク内に作成した [管理]、[クライアント]、および [サーバー] サブネットを選択します。

g) [完了] をクリックします。



これで、Citrix ADC VPX インスタンスは Microsoft Azure でプロビジョニングされます。

プロビジョニングされた **Citrix ADC VPX** インスタンスの表示

Citrix ADM で表示するには:

1. Citrix ADM で、［ネットワーク］>［インスタンス］**>**［**Citrix ADC**］に移動します。
2. ［**Citrix ADC VPX** ］タブを選択します。

   Microsoft Azure でプロビジョニングされた Citrix ADC VPX インスタンスは、ここに記載されています。

Microsoft Azure で表示するには:

1. Azure ポータルにログオンします。
2. Citrix ADC VPX インスタンスをプロビジョニングするために作成されたリソースグループに移動します。

   このページには、プロビジョニングされた Citrix ADC VPX インスタンスが表示されます。

> 注:
>
> Citrix ADC VPX インスタンスの名前は、Citrix ADM でインスタンスをプロビジョニングするときに指定した名前と同じです。

Citrix ADM を使用した **Microsoft Azure** での **Citrix ADC VPX** のオートスケーリング

May 7, 2021

自動スケーリングは、実際の使用状況に応じて自動的にリソースを追加または削除するクラウドコンピューティング方法です。自動スケーリングは、変動するクライアント要求や処理ジョブ数を満たすために、サイトまたはアプリケーションがオンデマンドのリソース割り当てを必要とする場合に便利です。

Web アプリケーションやサービスの需要は大きく異なる場合があります。トラフィックのニーズに応じて適切な数の Citrix ADC インスタンスを維持することが重要です。需要に応じて、Microsoft Azure のネットワークリソースを増減できます。したがって、パフォーマンスを損なうことなく、コストの最適化を提供します。

Citrix Application Delivery Management（ADM）オートスケーリングでは、リソースの消費量が変動するため、Citrix ADC インスタンスの正確な数が維持されます。Citrix ADM は、変動するリソース消費量に基づいてトラフィックフローを決定し、Citrix ADC インスタンスを動的にスケールアウトまたはスケールインします。したがって、適切な数の Citrix ADC インスタンスを維持するための柔軟性を提供します。

Citrix ADM は、Citrix ADC インスタンスのリソース使用率を監視し、設定されたしきい値と照合します。設定されたリソースの 1 つが指定されたしきい値を超えると、スケールアウトアクションがトリガーされます。

Citrix ADM は、構成されているすべてのリソースの使用量が通常のしきい値を下回った場合にのみ、スケールインアクションをトリガーします。

> 重要:
>
> 自動スケーリングは、クラスターノード上でスポット設定を必要とする以下の機能を除き、すべての Citrix ADC 機能をサポートします。

> - GSLB か
> - Citrix Gateway とその機能
> - Telco 機能
>
> スポッティング設定について詳しくは、ストライプ、部分的にストライプ、およびスポットされた構成を参照してください。

長所

アプリケーションの高可用性：自動スケーリングにより、アプリケーションのトラフィック要求を処理するための適切な数の Citrix ADC VPX インスタンスが常に確保されます。これにより、トラフィック要求に関係なく、アプリケーションが常に起動し、実行されていることが保証されます。

スマートなスケーリングの決定とゼロタッチ構成：自動スケーリングはアプリケーションを継続的に監視し、需要に応じて Citrix ADC インスタンスを動的に追加または削除します。一定期間需要が増加すると、インスタンスは自動的に追加されます。一定期間需要が減少すると、インスタンスは自動的に削除されます。Citrix ADC インスタンスの追加と削除は自動的に行われるため、手動でのゼロタッチ構成になります。

自動 **DNS** 管理： Citrix ADM Autoscale 機能は、自動 DNS 管理を提供します。新しい Citrix ADC インスタンスが追加されると、ドメイン名が自動的に更新されます。

正常な接続終了：スケールイン中、Citrix ADC インスタンスは正常に削除され、クライアント接続が失われるのを防ぎます。

コスト管理の向上：自動スケーリングは、必要に応じて Citrix ADC インスタンスを動的に増減します。この方法では、関連するコストを最適化できます。必要なときにのみインスタンスを起動し、不要になったときにインスタンスを終了すると、運用コストが削減されます。したがって、使用したリソースに対してのみお支払いいただきます。

オブザーバビリティ**:** オブザーバビリティは、アプリケーションの稼働状態を監視するアプリケーションの開発/運用担当者にとって重要です。Citrix ADM の AutoScale ダッシュボードでは、しきい値のパラメーター値、AutoScale トリガーのタイムスタンプ、イベント、および Autocale に参加しているインスタンスを視覚化できます。

ライセンスの要件

Citrix Autoscale グループ用に作成された Citrix ADC インスタンスは、Citrix ADC アドバンストライセンスまたはプレミアム ADC ライセンスを使用します。Citrix ADC クラスタリング機能は、アドバンストまたはプレミアム ADC ライセンスに含まれています。

> 注:
>
> ADC クラスタは、ADC Premium ライセンスまたは Advanced ライセンスを使用する ADM 自動スケーリングでのみサポートされます。

次のいずれかの方法を選択して、Citrix ADCitrix ADM によってプロビジョニングされた Citrix ADC のライセンスを取得できます。

- **Citrix ADM** に存在する **ADC** ライセンスを使用する： Autoscale グループの作成時に、プール容量、VPX ライセンス、または仮想 CPU ライセンスを構成します。したがって、Autocale グループに対して新しいインスタンスがプロビジョニングされると、既に設定されているライセンスタイプがプロビジョニングされたインスタンスに自動的に適用されます。

  - プールされた容量: Autocale グループ内のすべてのプロビジョニングされたインスタンスに帯域幅を割り当てます。新しいインスタンスをプロビジョニングするために必要な帯域幅が Citrix ADM で利用可能であることを確認します。詳しくは、「プール容量を構成する」を参照してください。

    Autocale グループの各 ADC インスタンスは、1 つのインスタンス・ライセンスと、指定された帯域幅をプールからチェックアウトします。

  - **VPX** ライセンス： 新しくプロビジョニングされたインスタンスに VPX ライセンスを適用します。新しいインスタンスをプロビジョニングするために、Citrix ADM で必要な数の VPX ライセンスがあることを確認します。

    Citrix ADC VPX インスタンスがプロビジョニングされると、インスタンスは Citrix ADM からライセンスをチェックアウトします。詳しくは、「Citrix ADC VPX チェックインとチェックアウトのライセンス」を参照してください。

  - 仮想 **CPU** ライセンス**:** 新しくプロビジョニングされたインスタンスに仮想 CPU ライセンスを適用します。このライセンスでは、Citrix ADC VPX インスタンスの資格を持つ CPU の数を指定します。新しいインスタンスをプロビジョニングするために必要な数の仮想 CPU が Citrix ADM にあることを確認します。

    Citrix ADC VPX インスタンスがプロビジョニングされると、インスタンスは Citrix ADM から仮想 CPU ライセンスをチェックアウトします。詳しくは、「Citrix ADC 仮想 CPU ライセンス」を参照してください。

  プロビジョニングされたインスタンスが破棄またはプロビジョニング解除されると、適用されたライセンスは自動的に Citrix ADM に返されます。

  消費されたライセンスを監視するには、[ネットワーク] > [ライセンス] ページに移動します。

- **Microsoft Azure** サブスクリプションライセンスの使用**:** Autoscale グループの作成中に、Azure マーケットプレイスで利用可能な Citrix ADC ライセンスを構成します。したがって、Autoscale グループ用に新しいインスタンスがプロビジョニングされると、ライセンスは Azure Marketplace から取得されます。

自動スケーリングでサポートされる **Citrix ADC Azure** 仮想マシンイメージ

最低 3 つの NIC をサポートする Azure 仮想マシンイメージを使用します。自動スケーリング Citrix ADC VPX インスタンスは、プレミアムエディションとアドバンスエディションでのみサポートされます。Azure 仮想マシンイメージタイプについて詳しくは、「仮想マシンの種類とサイズ (Microsoft ドキュメントを参照)」を参照してください。

オートスケーリングの推奨仮想マシンサイズを以下に示します。

- Standard_DS3_v2

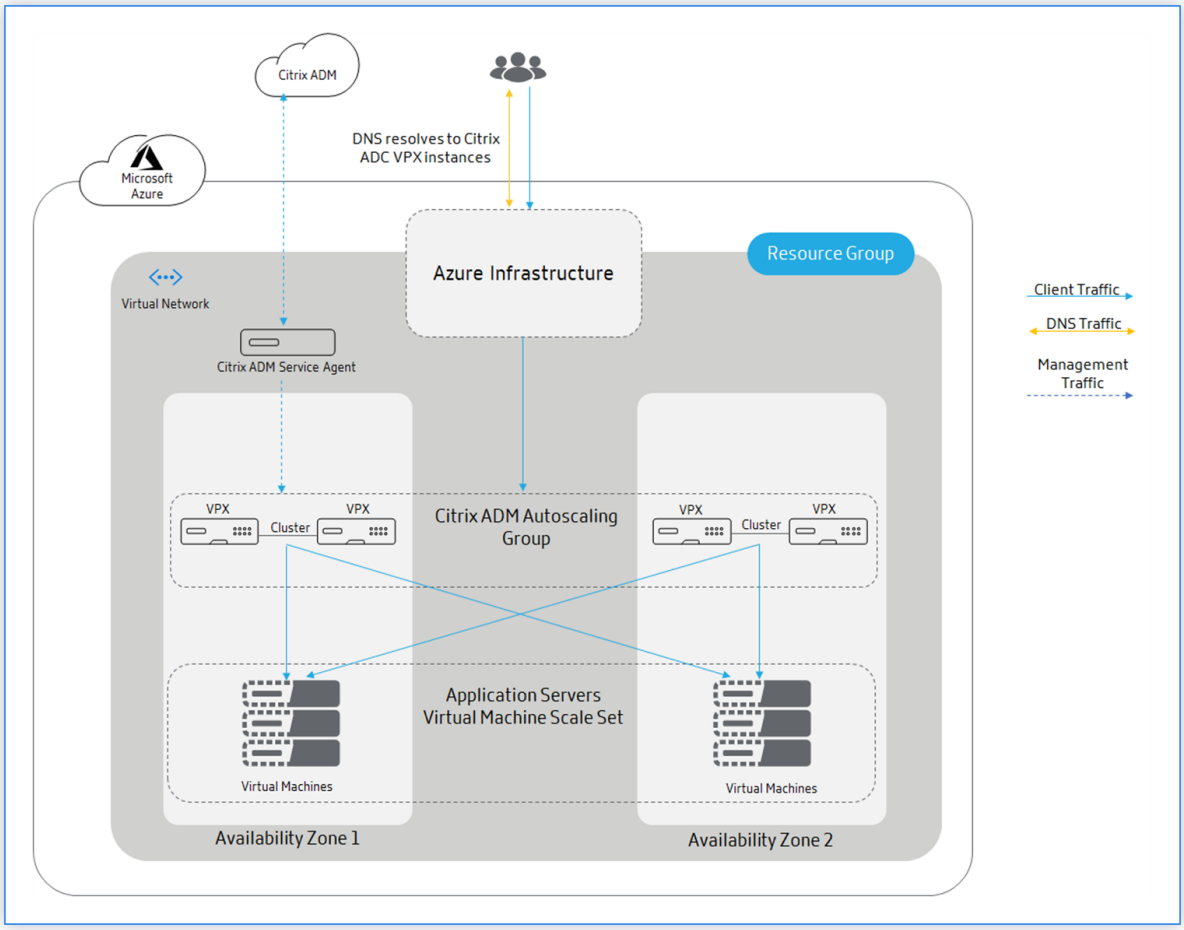
- Standard_B2ms
- Standard_DS4_v2

アーキテクチャ

Citrix ADM は、Azure DNS または Azure ロードバランサー（ALB）を使用してクライアントトラフィックの分散を処理します。

Azure DNS を使用したトラフィックの分散

次の図は、Azure トラフィックマネージャーをトラフィックディストリビューターとして使用して DNS ベースの自動スケーリングがどのように行われるかを示しています。



DNS ベースの自動スケーリングでは、DNS はディストリビューション層として機能します。Azure トラフィックマネージャーは、Microsoft Azure の DNS ベースのロードバランサーです。トラフィックマネージャーは、Citrix ADM 自動スケーリンググループで使用可能な適切な Citrix ADC インスタンスにクライアントトラフィックを転送します。

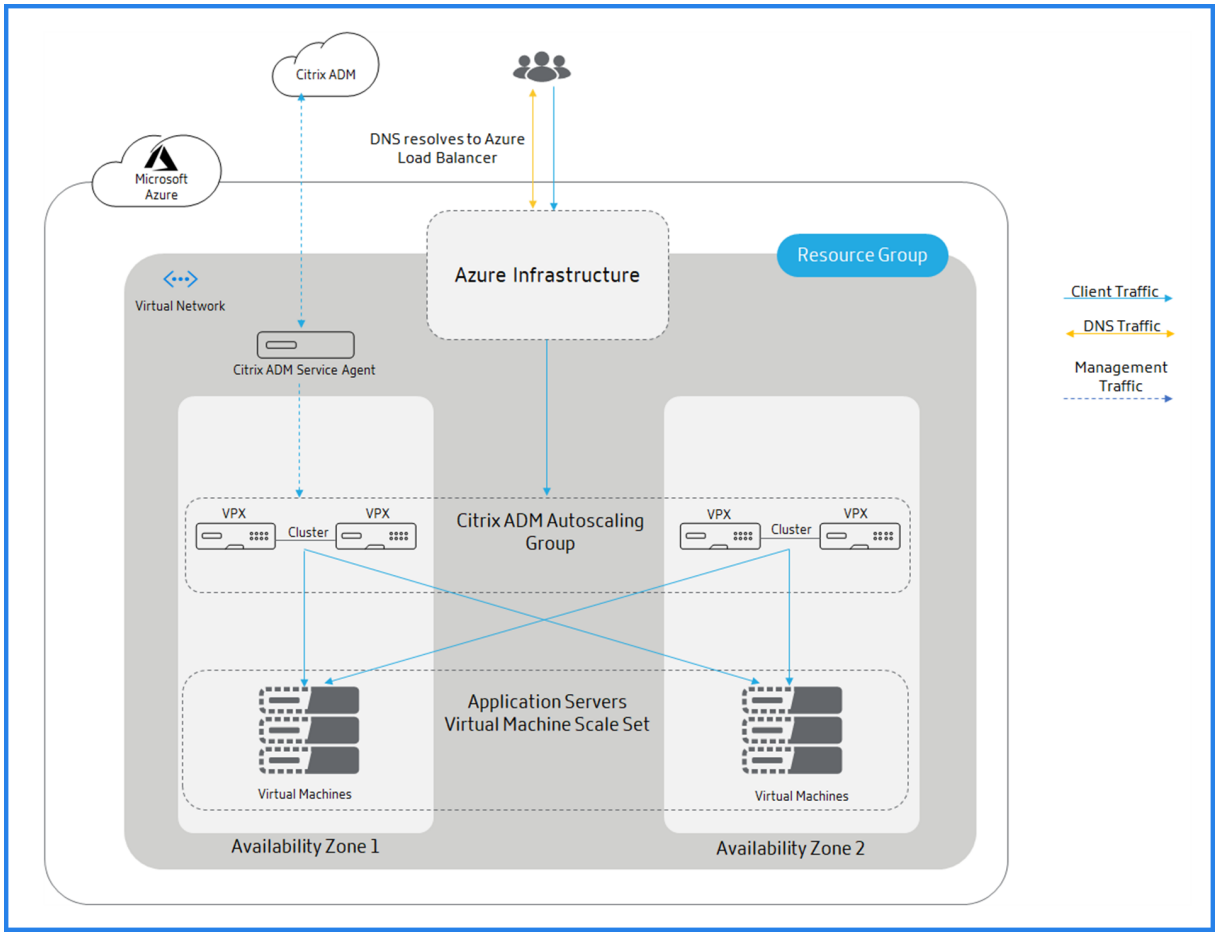
Azure トラフィックマネージャーは、FQDN を Citrix ADC インスタンスの VIP アドレスに解決します。

> 注:
>
> DNS ベースの自動スケーリングでは、Citrix ADM Autoscale グループ内の各 Citrix ADC インスタンスにパブリック IP アドレスが必要です。

Citrix ADM は、クラスターレベルでスケールアウトまたはスケールインアクションをトリガーします。スケールアウトがトリガーされると、登録された仮想マシンがプロビジョニングされ、クラスターに追加されます。同様に、スケールインがトリガーされると、Citrix ADC VPX クラスターからノードが削除され、プロビジョニングが解除されます。

Azure Load Balancer を使用したトラフィックの分散

次の図は、Azure ロードバランサーをトラフィックディストリビューターとして使用して自動スケーリングがどのように行われるかを示しています。



Azure Load Balancer は、クラスターノードへの配布層です。ALB はクライアントトラフィックを管理し、Citrix ADC VPX クラスターに配信します。ALB は、クライアントトラフィックを Citrix ADC VPX クラスターノードに送信します。このクラスターノードは、複数のアベイラビリティーゾーンにまたがって Citrix ADM 自動スケーリンググループで使用できます。

> 注:
>
> パブリック IP アドレスは Azure Load Balancer に割り当てられます。Citrix ADC VPX インスタンスでは、パブリック IP アドレスは必要ありません。

Citrix ADM は、クラスターレベルでスケールアウトまたはスケールインアクションをトリガーします。スケールアウトがトリガーされると、登録された仮想マシンがプロビジョニングされ、クラスターに追加されます。同様に、スケールインがトリガーされると、Citrix ADC VPX クラスターからノードが削除され、プロビジョニングが解除されます。

Citrix ADM Autoscale グループ

Autoscale グループは、Citrix ADC インスタンスのグループで、アプリケーションを単一のエンティティとして負荷分散し、設定されたしきい値パラメータ値に基づいて自動スケーリングをトリガーします。

リソースグループ

リソースグループには、Citrix ADC 自動スケーリングに関連するリソースが含まれます。このリソースグループは、自動スケーリングに必要なリソースを管理するのに役立ちます。詳しくは、「リソースグループの管理」を参照してください。

Azure バックエンド仮想マシンスケールセット

Azure 仮想マシンスケールは、同一の VM インスタンスのコレクションです。VM インスタンスの数は、クライアントのトラフィックに応じて増減できます。このセットは、アプリケーションに高可用性を提供します。詳しくは、「仮想マシンのスケールセット」を参照してください。

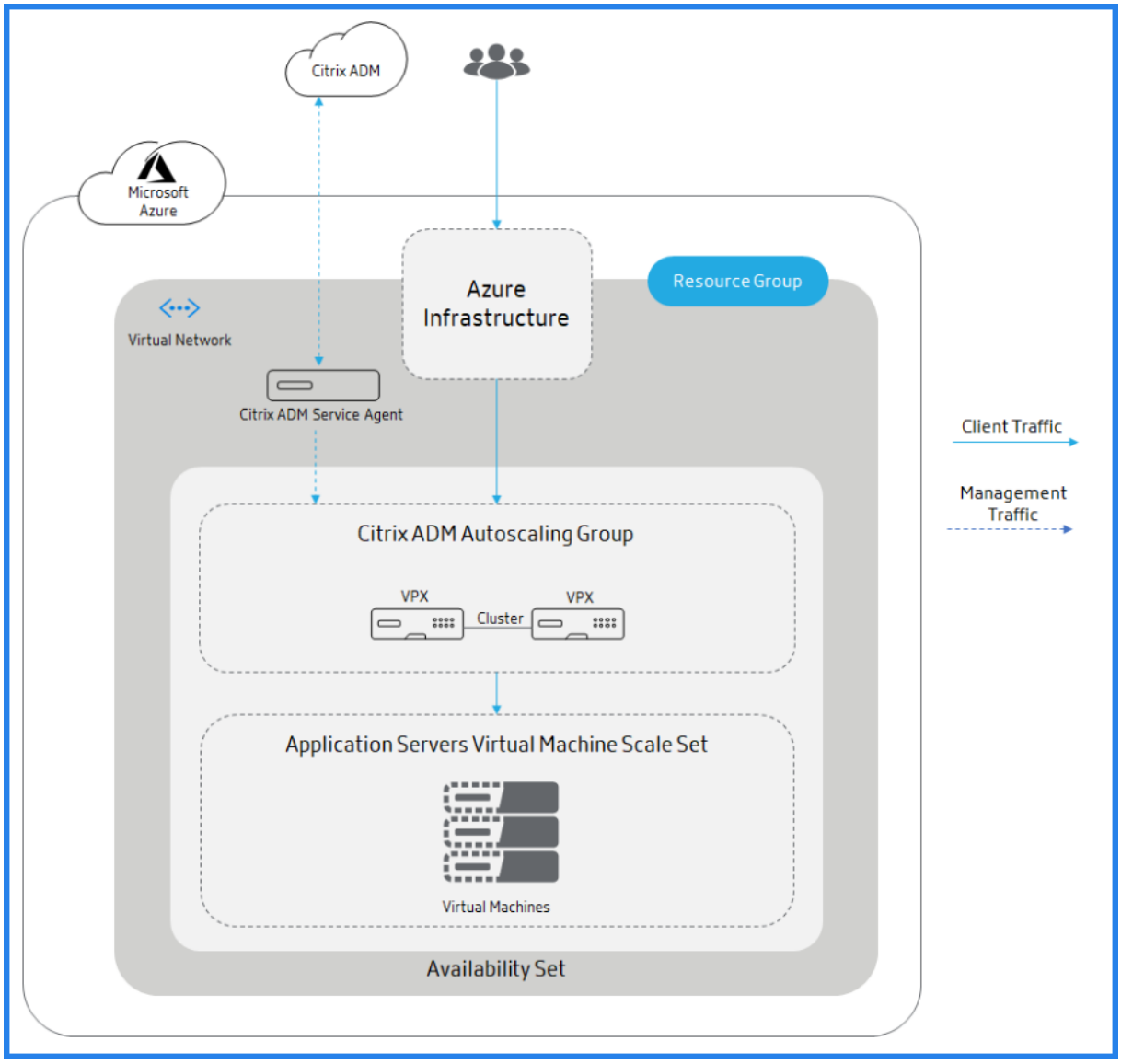
アベイラビリティーゾーン

アベイラビリティーゾーンは、Azure リージョン内の独立した場所です。各リージョンは、複数のアベイラビリティーゾーンで構成されています。各アベイラビリティーゾーンは 1 つのリージョンに属しています。各アベイラビリティーゾーンには、1 つの Citrix ADC VPX クラスターがあります。詳しくは、「Azure のアベイラビリティーゾーン」を参照してください。

可用性セット

可用性セットは、Citrix ADC VPX クラスターとアプリケーションサーバーの論理的なグループです。可用性セットは、クラスター内の複数の分離されたハードウェアノードに ADC インスタンスをデプロイする場合に役立ちます。可用性セットを使用すると、Azure 内でハードウェアまたはソフトウェアの障害が発生した場合に、信頼できる ADM 自動スケーリングを保証できます。詳しくは、「可用性セット」を参照してください。

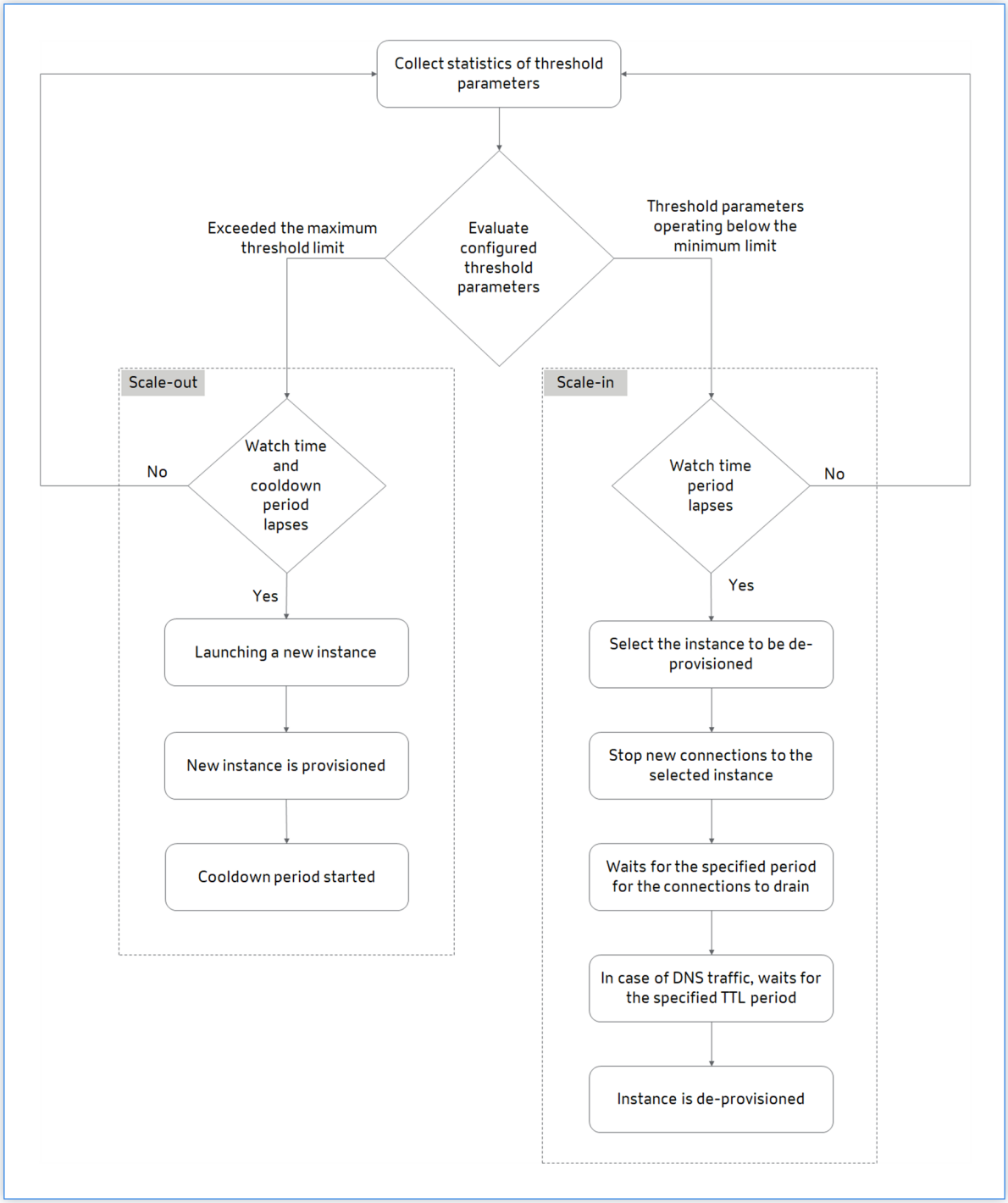
次の図は、可用性セットの自動スケーリングを示しています。



Azure インフラストラクチャ（ALB または Azure トラフィックマネージャ）は、可用性セット内の Citrix ADM 自動スケーリンググループにクライアントトラフィックを送信します。Citrix ADM は、クラスターレベルでスケールアウトまたはスケールインアクションをトリガーします。

オートスケーリングの仕組み

次のフローチャートは、オートスケーリングのワークフローを示しています。



Citrix ADM は、Autoscale プロビジョニングされたクラスターから毎分統計情報（CPU、メモリ、スループット）を収集します。

統計情報は、設定しきい値に対して評価されます。統計情報に応じて、スケールアウトまたはスケールインがトリガーされます。統計情報が最大しきい値を超えると、スケールアウトがトリガーされます。統計情報が最小しきい値を下回ると、スケールインがトリガーされます。

スケールアウトがトリガーされた場合:

1. 新しいノードがプロビジョニングされます。
2. ノードがクラスタに接続され、構成がクラスタから新しいノードに同期されます。
3. ノードは Citrix ADM に登録されています。
4. 新しいノードの IP アドレスは、Azure トラフィックマネージャーで更新されます。

スケールインがトリガーされた場合:

1. 削除するノードが識別されます。
2. 選択したノードへの新しい接続を停止します。
3. 接続がドレインするまで指定した期間待機します。DNS トラフィックでは、指定された存続時間（TTL）期間も待機します。
4. ノードがクラスターから切り離され、Citrix ADM から登録解除され、Microsoft Azure からプロビジョニングが解除されます。

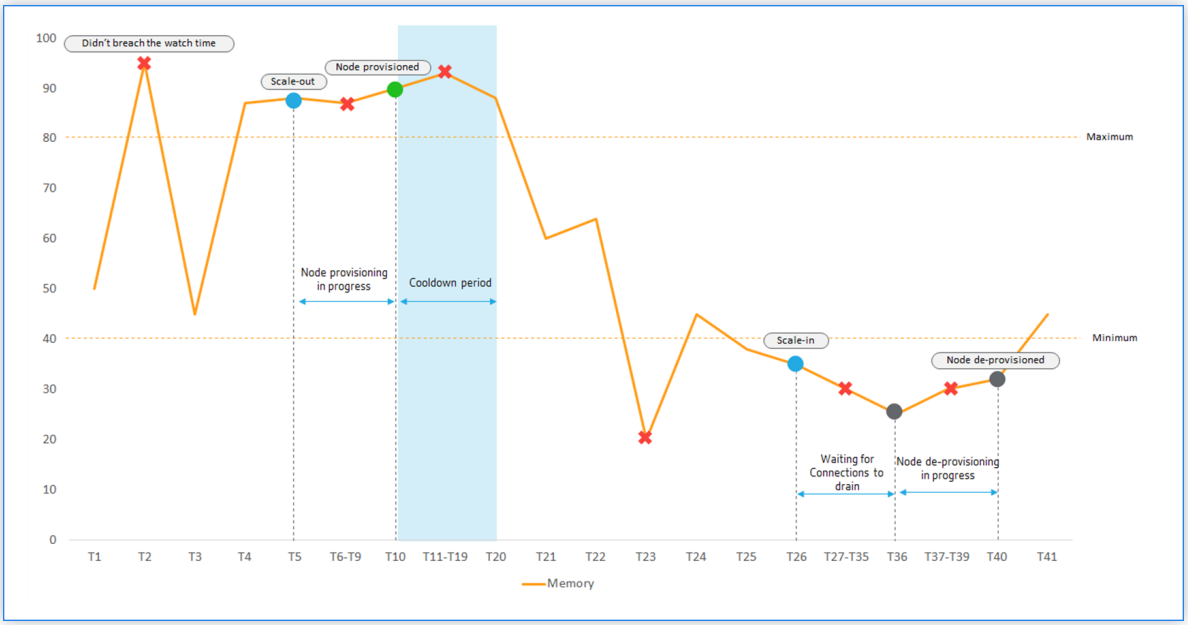
> 注
>
> アプリケーションをデプロイすると、すべてのアベイラビリティーゾーンのクラスターに IP セットが作成されます。次に、ドメインとインスタンスの IP アドレスが Azure トラフィックマネージャーまたは ALB に登録されます。アプリケーションを削除すると、ドメインとインスタンスの IP アドレスが Azure トラフィックマネージャーまたは ALB から登録解除されます。次に、IP セットが削除されます。

オートスケーリングのシナリオの例

次の設定を使用して、単一のアベイラビリティーゾーンに asg_arn という名前の Autoscale グループを作成したとします。

- 選択されたしきい値パラメータ — メモリ使用量。
- メモリに設定されたしきい値の制限:
  - 最小制限:40
  - 最大制限:85
- 総再生時間 — 2 分。
- クールダウン期間 — 10 分。
- プロビジョニング解除中の待機時間（10 分）。
- DNS の存続時間 — 10 秒。

[Autoscale] グループが作成されると、[Autoscale] グループから統計が収集されます。Autoscale ポリシーは、Autoscale イベントが進行中かどうかも評価します。自動スケーリングが進行中の場合は、そのイベントが完了するのを待ってから、統計情報を収集します。



イベントのシーケンス

1. メモリ使用量が **T2** のしきい値制限を超えています。ただし、スケールアウトは指定された総再生時間に対して違反しなかったため、トリガーされません。
2. スケールアウトは、最大しきい値が 2 分（総再生時間）連続的に突破された後、**T5** でトリガーされます。
3. ノードの Provisioning が進行中であるため、**T5-T10** 間の違反に対するアクションは実行されていません。
4. ノードは **T10** でプロビジョニングされ、クラスタに追加されます。クールダウン期間が開始されました。
5. クールダウン期間が原因で、**T10-T20** 間の違反に対する処置は実行されていません。この期間は、Autoscale グループのインスタンスの有機的な増加を保証します。次のスケーリング決定をトリガーする前に、現在のトラフィックが安定し、現在のインスタンスのセットで平均化するのを待機します。
6. メモリ使用量が **T23** の最小しきい値制限を下回っています。ただし、スケールインは指定された総再生時間に対して違反しなかったため、トリガーされません。
7. 最小しきい値が 2 分（総再生時間）連続的に突破された後、スケールインが **T26** でトリガーされます。クラスタ内のノードは、プロビジョニング解除のために識別されます。
8. Citrix ADM が既存の接続を切断するのを待機しているため、**T26-T36** 間の違反に対する処置は実行されていません。DNS ベースの自動スケーリングでは、TTL が有効です。

> 注:
>
> DNS ベースの自動スケーリングの場合、Citrix ADM は指定された TTL（有効期限）期間待機します。次に、ノードのプロビジョニング解除を開始する前に、既存の接続がドレインするのを待機します。

9. ノードのプロビジョニング解除が進行中であるため、**T37-T39** 間の違反に対するアクションは実行されていません。
10. ノードは **T40** でクラスターから削除され、プロビジョニング解除されます。

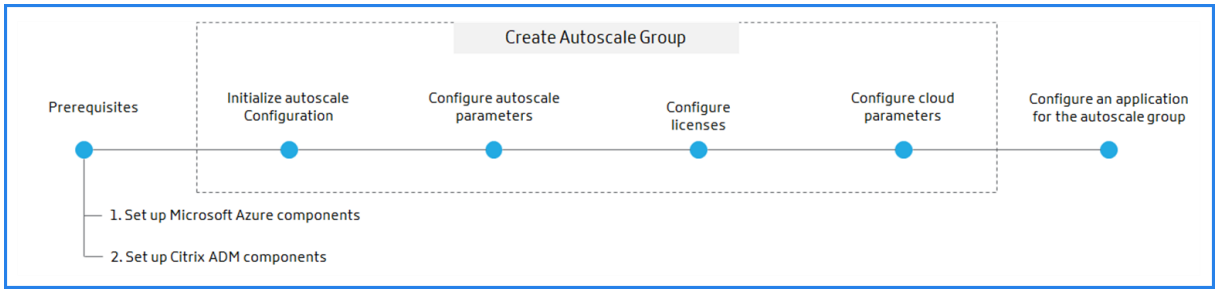
ノードのプロビジョニング解除を開始する前に、選択したノードへのすべての接続がドレインされました。したがって、クールダウン期間は、ノードのプロビジョニング解除後にスキップされます。

構成

May 7, 2021

Citrix ADM は、Microsoft Azure のすべての Citrix ADC VPX クラスターを管理します。Citrix ADM は、クラウドアクセスプロファイルを使用して Azure リソースにアクセスします。

次のフロー図は、Autoscale グループを作成および設定する手順を説明しています。



前提条件

このセクションでは、自動スケーリング Citrix ADC VPX インスタンスを構成する前に、Microsoft Azure および Citrix ADM で完了する必要がある前提条件について説明します。

このドキュメントでは、次のことを前提としています。

- Azure Resource Manager のデプロイモデルをサポートする Microsoft Azure アカウントを持っています。
- Microsoft Azure でリソースグループがあります。

アカウントやその他のタスクの作成方法について詳しくは、「Microsoft Azure ドキュメント」を参照してください。

Microsoft Azure コンポーネントのセットアップ

Citrix ADM で Citrix ADC VPX インスタンスを自動スケーリングする前に、Azure で次のタスクを実行します。

1. 仮想ネットワークを作成する。
2. 「セキュリティグループの作成」を参照してください。

3.「サブネットの作成」を参照してください。

4.「Microsoft Azure で Citrix ADC VPX ライセンスを購読する」を参照してください。

5.「アプリケーションの作成と登録」を参照してください。

仮想ネットワークを作成する

1. Microsoft Azure ポータルにログオンします。
2. [リソースの作成] を選択します。
3. [ネットワーク] を選択し、[仮想ネットワーク] をクリックします。
4. 必要なパラメータを指定します。
   - リソースグループでは、Citrix ADC VPX 製品を展開するリソースグループを指定する必要があります。
   - [**Location**] では、アベイラビリティーゾーンをサポートするロケーションを指定する必要があります。
     - 米国中部
     - 米国東部 2
     - フランス中部
     - 北ヨーロッパ
     - 東南アジア
     - 西ヨーロッパ
     - 米国西部 2

   > 注:
   >
   > アプリケーションサーバーはこのリソースグループに存在します。

5.［作成］をクリックします。

詳しくは、『Microsoft 社のドキュメント』の「Azure 仮想ネットワーク」を参照してください。

セキュリティグループの作成

仮想ネットワーク (VNet) に 3 つのセキュリティグループを作成します。それぞれ 1 つずつ管理、クライアント、およびサーバー接続に使用します。セキュリティグループを作成して、Citrix ADC VPX インスタンスのインバウンドトラフィックとアウトバウンドトラフィックを制御します。Citrix Autoscale グループで制御する着信トラフィックのルールを作成します。規則は、必要に応じていくつでも追加できます。

- 管理： Citrix ADC VPX の管理専用のアカウント内のセキュリティグループ。Citrix ADC は Azure サービスに接続する必要があり、インターネットアクセスが必要です。受信規則は、次の TCP ポートおよび UDP ポートで許可されます。

- TCP: 80、22、443、3008—3011、4001、27000、7279
- UDP: 67、123、161、500、3003、4500、7000

> 注 次のことを確認してください。
>
> セキュリティグループは、Citrix ADM エージェントが VPX にアクセスすることを許可しました。
>
> 27000 および 7279 ポートは、Citrix ADM で開かれます。これらのポートは、Citrix ADM から Citrix ADC ライセンスをチェックアウトするために使用されます。詳しくは、「ポート」を参照してください。

- クライアント： Citrix ADC VPX インスタンスのクライアント側通信専用のアカウント内のセキュリティグループ。通常、インバウンドルールは TCP ポート 80 および 443 で許可されます。また、ADC インスタンスの状態を監視するには、60000 ポートが必要です。
- サーバー： Citrix ADC VPX サーバー側通信専用のアカウント内のセキュリティグループ。

Microsoft Azure でセキュリティグループを作成する方法について詳しくは、「ネットワークセキュリティグループを作成、変更、または削除する」を参照してください。

サブネットの作成

仮想ネットワーク (VNet) に 3 つのサブネットを作成します。各サブネットは管理、クライアント、およびサーバー接続用です。各サブネットについて、VNet で定義されているアドレス範囲を指定します。サブネットを配置するアベイラビリティーゾーンを指定します。

- 管理**:** 仮想ネットワーク (VNet) 内の管理専用のサブネット。Citrix ADC は Azure サービスに接続する必要があり、インターネットアクセスが必要です。
- クライアント**:** クライアント側専用の仮想ネットワーク (VNet) 内のサブネット。通常、Citrix ADC は、インターネットからパブリックサブネット経由でアプリケーションのクライアントトラフィックを受信します。
- サーバー： アプリケーションサーバーがプロビジョニングされるサブネット。すべてのアプリケーションサーバーがこのサブネットに存在し、このサブネットを介して Citrix ADC からのアプリケーショントラフィックを受信します。

> 注
>
> サブネットの作成時に、サブネットに対して適切なセキュリティグループを指定します。

Microsoft Azure でサブネットを作成する方法について詳しくは、「仮想ネットワークサブネットを追加、変更、または削除する」を参照してください。

Microsoft Azure で **Citrix ADC VPX** ライセンスを購読する

1. Microsoft Azure ポータルにログオンします。
2. [リソースの作成] を選択します。
3. マーケットプレイスの検索バーで、`Citrix ADC`を検索して必要な製品バージョンを選択します。

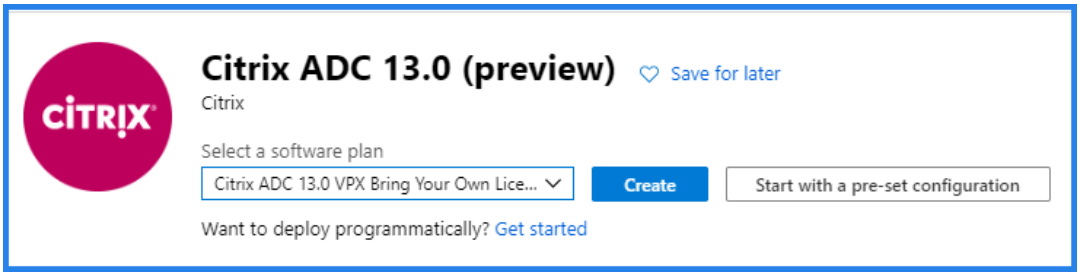
4. **[** ソフトウェアプランの選択] リストで、次のいずれかのライセンスタイプを選択します。

   - 自分のライセンスを持参する
   - 詳細設定
   - Premium

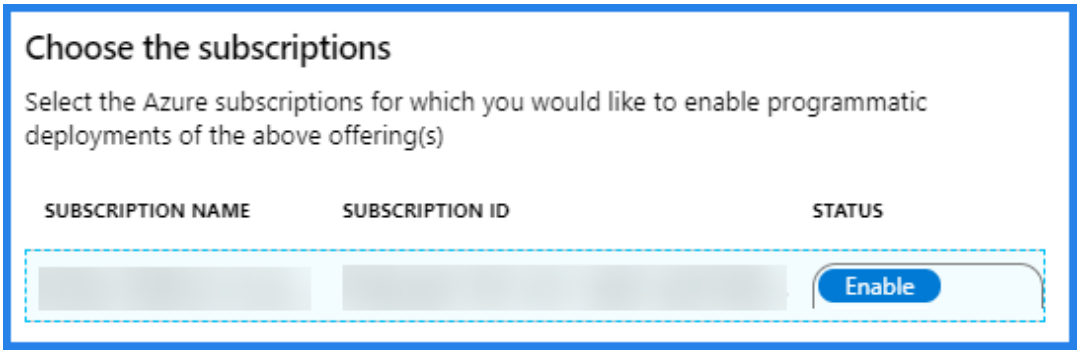
   > 注
   >
   > - ［ライセンスを持ち込む］ オプションを選択すると、Citrix ADCitrix ADC インスタンスの Provisioning 中に、Autoscale グループが Citrix ADM からライセンスをチェックアウトします。
   > - Citrix ADM では、「**Advanced** 」と「Prem **ium** 」は、それぞれ エンタープライズおよび プラチナと同等のライセンスタイプです。

5. 選択した Citrix ADC 製品に対してプログラムによる展開が有効になっていることを確認します。

   a) Bide プログラムで展開したいですか**?** で、[開始] をクリックします。

   b) ［サブスクリプションの選択］ で ［有効にする］ を選択し、選択した Citrix ADC VPX エディションをプログラムで展開します。

   > 重要
   >
   > Azure で Citrix ADC VPX インスタンスを Autoscale するには、プログラムによる展開を有効にする必要があります。

   c) ［保存］ をクリックします。

   d) **[** プログラムによる配置を設定**]** を閉じます。

6. ［作成］ をクリックします。

アプリケーションの作成と登録

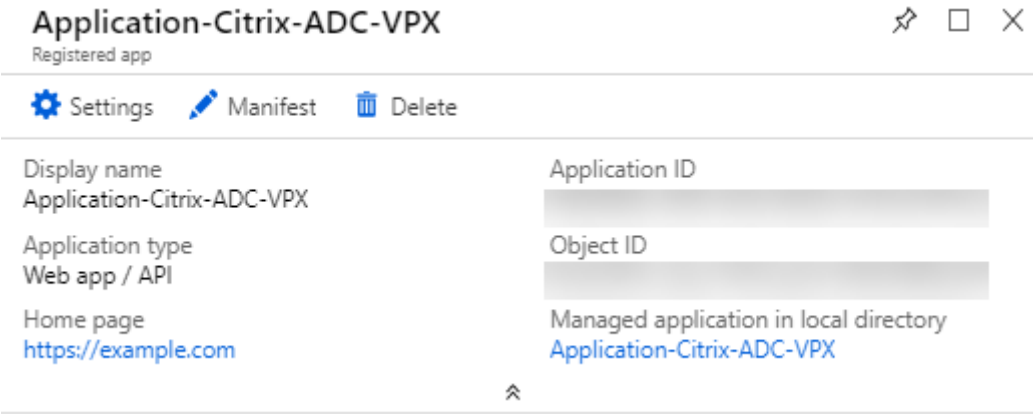
Citrix ADM は、このアプリケーションを使用して、Azure の Citrix ADC VPX インスタンスを Autoscale します。

Azure でアプリケーションを作成して登録するには:

1. Azure ポータルで、[**Azure Active Directory**] を選択します。
   このオプションでは、組織のディレクトリが表示されます。
2. アプリの登録を選択:
   a)「⊠ 名前 | **Name** | marvel⊠」で、アプリケーションの名前を指定します。
   b) リストから アプリケーションの種類を選択します。
   c) [サインオン URL] で、アプリケーションにアクセスするアプリケーション URL を指定します。
3. [作成] をクリックします。

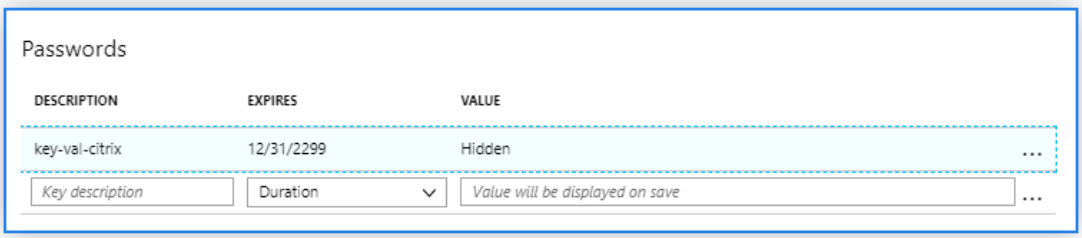
アプリの登録について詳しくは、「Microsoft 社のドキュメント」を参照してください。

Azure は、アプリケーション ID をアプリケーションに割り当てます。以下は、Microsoft Azure に登録されているアプリケーションの例です。



Citrix ADM でクラウドアクセスプロファイルを構成する場合は、次の ID をコピーし、これらの ID を指定します。次の ID を取得する手順については、Microsoft 社のドキュメントを参照してください。

- アプリケーション ID
- ディレクトリ ID
- キー



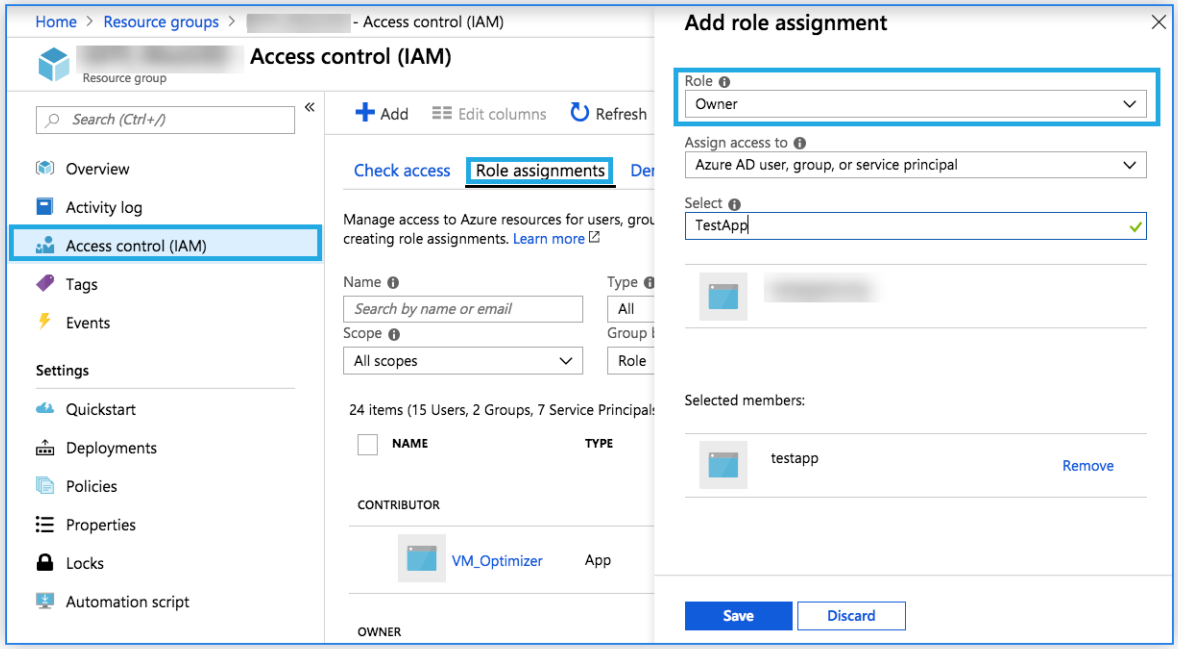
- サブスクリプション ID: ストレージアカウントからサブスクリプション ID をコピーします。

アプリケーションへのロールのアクセス許可の割り当て

Citrix ADM は、サービスとしてのアプリケーションの原則を使用して、Microsoft Azure の Citrix ADC インスタンスを AutoScale します。この権限は、選択したリソースグループにのみ適用されます。

登録済みアプリケーションにロールのアクセス許可を割り当てるには、Microsoft Azure サブスクリプションの所有者である必要があります。

1. Azure ポータルで、[リソースグループ] を選択します。
2. ロール権限を割り当てるリソースグループを選択します。
3. [アクセス制御 **(IAM)**] を選択します。
4. [役割の割り当て] で、[追加] をクリックします。
5.「ロール」リストから「所有者」を選択します。
6. Citrix ADC インスタンスの自動スケーリング用に登録されているアプリケーションを選択します。
7.［保存］をクリックします。



Citrix ADM コンポーネントのセットアップ

Citrix ADCitrix ADM で Citrix ADC VPX インスタンスを自動スケーリングする前に、Azure で次のタスクを実行します。

1. Azure でのエージェントのプロビジョニング

2. サイトの作成
3. Citrix ADM サービスエージェントにサイトを接続する

Azure での **Citrix ADM** エージェントのプロビジョニング

Citrix ADM サービスエージェントは、Citrix ADM とデータセンターまたはクラウドで検出されたインスタンスの間の仲介として機能します。

1. [ネットワーク**] > [**エージェント**]** に移動します。
2. [プロビジョニング] をクリックします。
3. [**Microsoft Azure**] を選択し、[次へ] をクリックします。
4. 「プロビジョニングパラメータ」タブで、次の項目を指定します。
    - 名前：Citrix ADM エージェント名を指定します。
    - サイト：エージェントと ADC VPX インスタンスをプロビジョニングするために作成したサイトを選択します。
    - クラウドアクセスプロファイル -リストからクラウドアクセスプロファイルを選択します。
    - アベイラビリティーゾーン -AutoScale グループを作成するゾーンを選択します。選択したクラウドアクセスプロファイルに応じて、そのプロファイルに固有のアベイラビリティーゾーンが設定されます。
    - セキュリティグループ -セキュリティグループは、Citrix ADC エージェントのインバウンドおよびアウトバウンドトラフィックを制御します。制御する着信トラフィックと発信トラフィックの両方のルールを作成します。
    - [**Subnet**]：エージェントをプロビジョニングする管理サブネットを選択します。
    - タグ -AutoScale グループタグのキーと値のペアを入力します。タグは、大文字と小文字を区別するキーと値のペアで構成されます。これらのタグを使用すると、Autoscale グループを簡単に整理して識別できます。タグは、Azure と Citrix ADM の両方に適用されます。
5. ［完了］をクリックします。

または、Azure マーケットプレイスから Citrix ADM エージェントをインストールすることもできます。詳しくは、「Microsoft Azure への Citrix ADM エージェントのインストール」を参照してください。

サイトの作成

Citrix ADM でサイトを作成し、Microsoft Azure リソースグループに関連付けられた VNet の詳細を追加します。

1. Citrix ADM で、［ネットワーク］>［サイト］に移動します。
2. ［追加］をクリックします。
3. **[** クラウドを選択**]** ペインで、

a) サイトの種類として [データセンター] を選択します。

b) [種類] リストから [**Azure**] を選択します。

c) [**Azure** から **VNet** をフェッチする] チェックボックスをオンにします。

このオプションを使用すると、Microsoft Azure アカウントから既存の VNet 情報を取得できます。

d)［次へ］をクリックします。

4. **[** リージョンの選択**]** ペインで、

a) [クラウドアクセスプロファイル] で、Microsoft Azure アカウント用に作成されたプロファイルを選択します。プロファイルがない場合は、プロファイルを作成します。

b) クラウドアクセスプロファイルを作成するには、[追加] をクリックします。

c)［名前］で、Citrix ADM で Azure アカウントを識別する名前を指定します。

d) [テナント **Active Directory ID /**テナント **ID**] で、テナントの Active Directory ID または Microsoft Azure のアカウントを指定します。

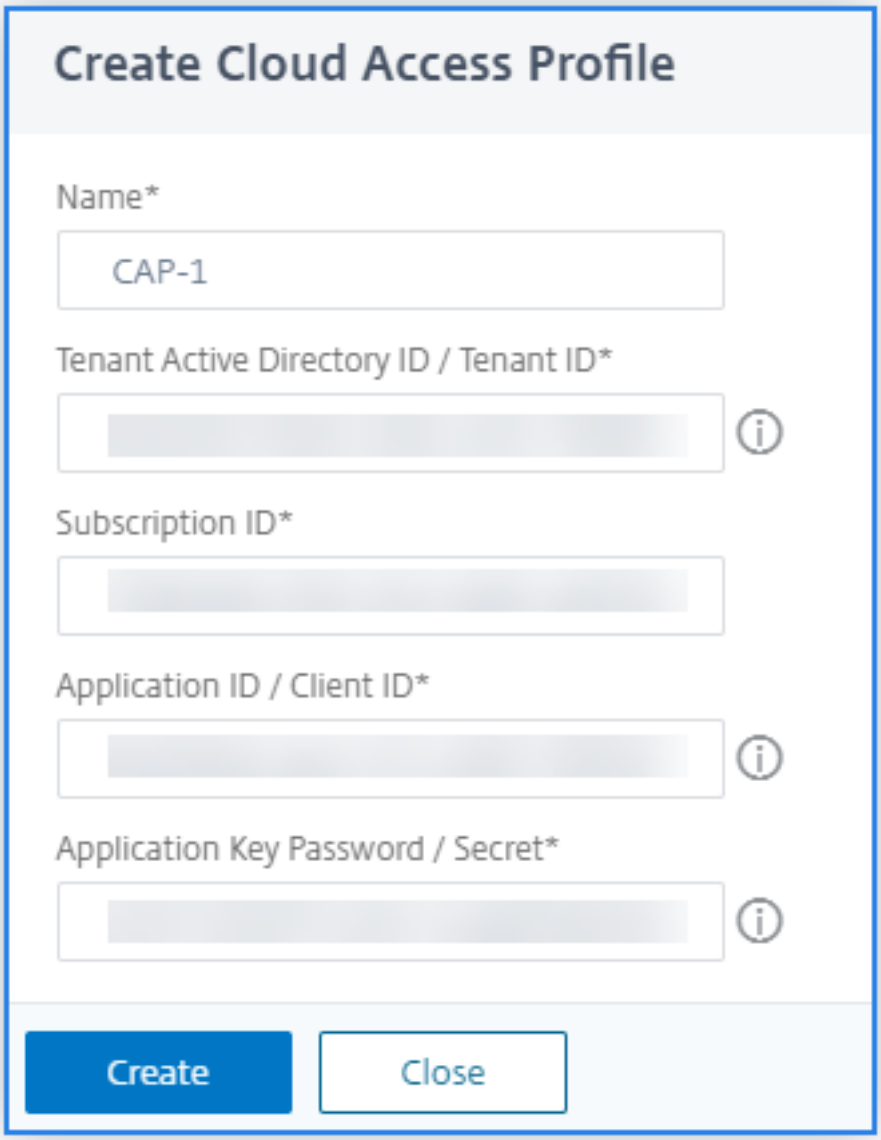
e) サブスクリプション **ID** を指定します。

f) アプリケーション **ID** またはクライアント **ID** を指定します。

g) アプリケーションキーのパスワード**/**シークレットを指定します。

h)［作成］をクリックします。

詳しくは、「アプリケーションの作成と登録」および「Azure アプリケーションへのクラウドアクセスプロファイルのマッピング」を参照してください。



i) **VNet** で、管理する Citrix ADC VPX インスタンスを含む仮想ネットワークを選択します。

j) サイト名を指定します。

k) ［完了］をクリックします。

Azure アプリケーションへのクラウドアクセスプロファイルのマッピング

Citrix ADM 用語	**Microsoft Azure** 用語
テナント Active Directory ID /テナント ID	ディレクトリ ID

Citrix ADM 用語	**Microsoft Azure** 用語
サブスクリプション ID	サブスクリプション ID
アプリケーション ID /クライアント ID	アプリケーション ID
アプリケーションキーのパスワード/シークレット	キーまたは証明書またはクライアントシークレット

Citrix ADM サービスエージェントにサイトを接続する

1. Citrix ADM で、［ネットワーク］>［エージェント］に移動します。
2. サイトをアタッチするエージェントを選択します。
3. [サイトの添付] をクリックします。
4. リストからアタッチするサイトを選択します。
5. ［保存］をクリックします。

手順 **1**：**Citrix ADM** で **Autoscale** 構成を初期化する

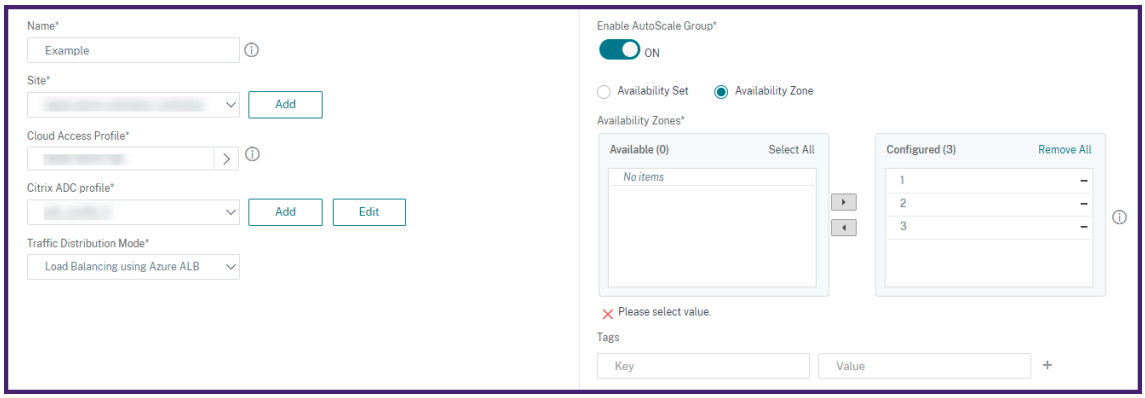
1. Citrix ADM で、［ネットワーク］>［**Autoscale** グループ］に移動します。
2. [追加] をクリックして、Autoscale グループを作成します。

   [AutoScale グループの作成] ページが表示されます。
3. [**Microsoft Azure**] を選択し、[次へ] をクリックします。
4. 「基本パラメータ」に、次の詳細を入力します。
   - 名前： Autoscale グループの名前を入力します。
   - サイト： Microsoft Azure で Citrix ADC VPX インスタンスを Autoscale するために作成したサイトを選択します。サイトを作成していない場合は、[追加] をクリックしてサイトを作成します。
   - エージェント：プロビジョニングされたインスタンスを管理する Citrix ADM エージェントを選択します。
   - クラウドアクセスプロファイル：クラウドアクセスプロファイルを選択します。クラウドアクセスプロファイルを追加または編集することもできます。
   - デバイスプロファイル：リストからデバイスプロファイルを選択します。Citrix ADC VPX インスタンスにログオンする必要がある場合、Citrix ADM はデバイスプロファイルを使用します。

     > 注：

> 選択したデバイスプロファイルがMicrosoft Azure のパスワードルールに準拠していることを確認します。

- トラフィック分散モード**:** 既定のトラフィック 分散モードとして、**[Azure LB** を使用した負荷分散] オプションが選択されます。また、トラフィック分散に **Azure DNS** モードを使用して DNS を選択することもできます。
- **Autoscale** グループを有効にする**:** ASG グループのステータスを有効または無効にします。このオプションはデフォルトで有効になっています。このオプションを無効にすると、自動スケーリングはトリガーされません。
- 可用性セットまたはアベイラビリティーゾーン**:** Autoscale グループを作成する可用性セットまたはアベイラビリティーゾーンを選択します。選択したクラウドアクセスプロファイルに応じて、アベイラビリティーゾーンがリストに表示されます。
- タグ: Autoscale グループタグのキーと値のペアを入力します。タグは、大文字と小文字を区別するキーと値のペアで構成されます。これらのタグを使用すると、Autoscale グループを簡単に整理して識別できます。タグは、Microsoft Azure と Citrix ADM の両方に適用されます。



5. [次へ] をクリックします。

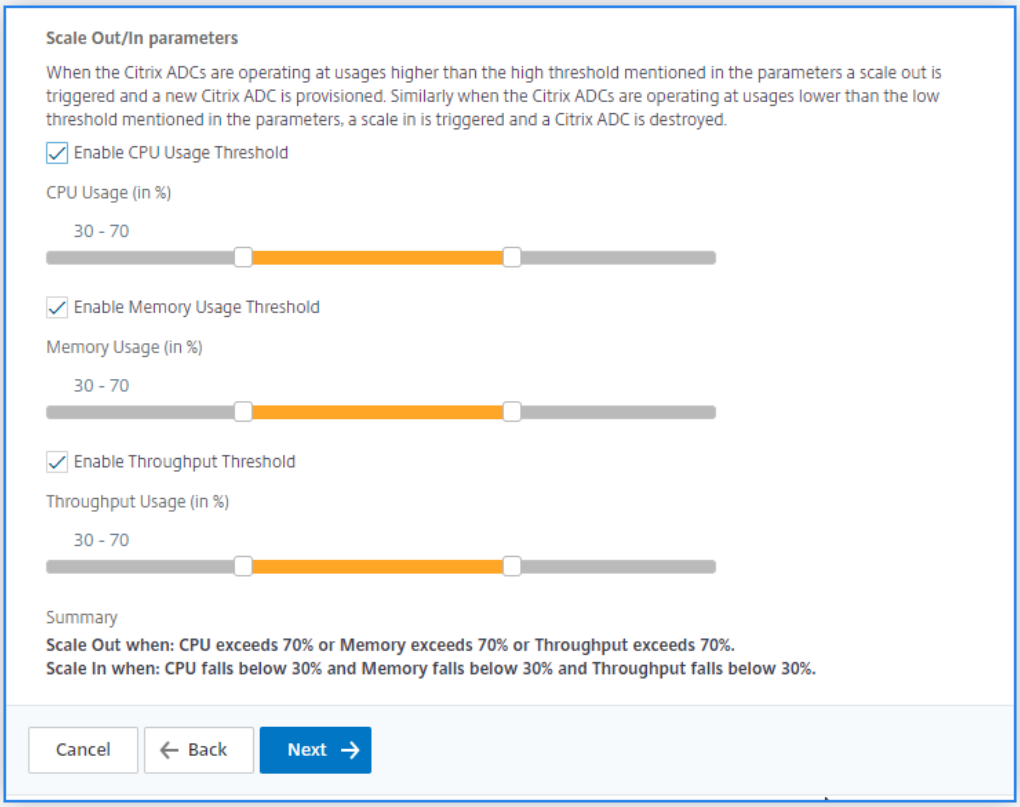
手順 **2: Autoscale** パラメータを構成する

1. [**Autoscale** パラメータ] タブで、次の詳細を入力します。
2. スケールアウトまたはスケールインをトリガーするために値を監視する必要がある次のしきい値パラメータを 1 つ以上選択します。
   - **CPU** 使用率しきい値の有効化**:** CPU 使用率に基づいてメトリックを監視します。
   - メモリ使用量のしきい値の有効化**:** メモリ使用量に基づいてメトリックを監視します。
   - スループットのしきい値の有効化**:** スループットに基づいてメトリックを監視します。

     > 注
     >
     > - デフォルトの最小しきい値制限は 30 で、最大しきい値制限は 70 です。ただし、制限を変更

するには変更します。

- 最小しきい値制限は、最大しきい値制限の半分以下である必要があります。
- モニタリング用に複数のしきい値パラメータを選択できます。しきい値パラメータの少なくとも 1 つが最大しきい値を超えている場合、スケールアウトがトリガーされます。ただし、スケールインがトリガーされるのは、すべてのしきい値パラメータが通常のしきい値を下回っている場合だけです。



- スケールアウトを高速化するためにスペアノードを保持**:** このオプションは、スケールアウトを高速化するのに役立ちます。ADM は、スケールアウトアクションが発生する前に予備ノードをプロビジョニングし、シャットダウンします。AutoScale グループに対してスケールアウトアクションが発生すると、ADM は、すでにプロビジョニングされているスペアノードを起動します。その結果、スケールアウトにかかる時間が短縮されます。
- 最小インスタンス**:** この Autoscale グループにプロビジョニングする必要があるインスタンスの最小数を選択します。

  デフォルトの最小インスタンス数は、選択したゾーンの数と同じです。最小インスタンスは、指定されたゾーン数の倍数でのみ増分できます。

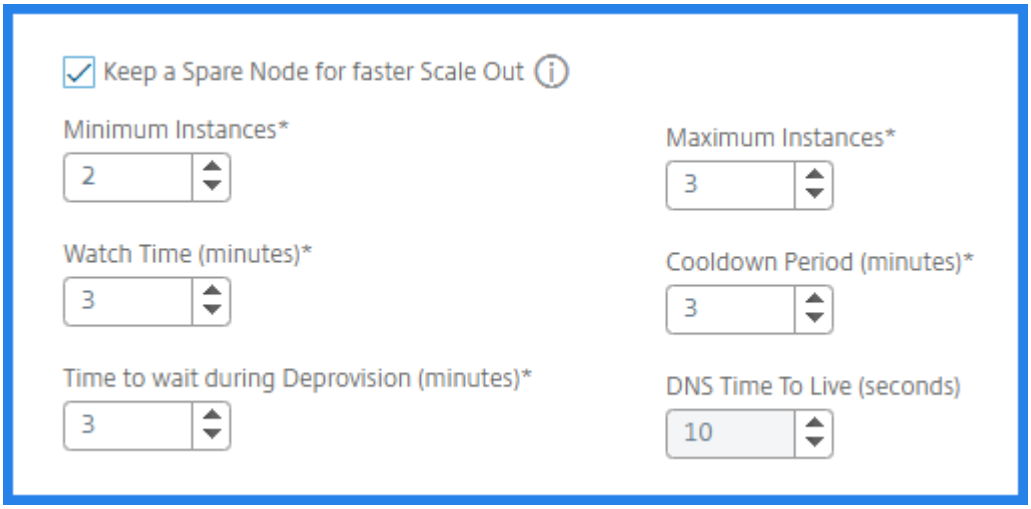
  たとえば、アベイラビリティーゾーンの数が 4 の場合、最小インスタンスはデフォルトで 4 です。最小インスタンスを 8、12、16 増やすことができます。

- インスタンスの最大数**:** この Autoscale グループにプロビジョニングする必要があるインスタンスの最大数を選択します。

  インスタンスの最大数は、最小インスタンスの値以上である必要があります。インスタンスの最大数は、アベイラビリティーゾーンの数に 32 を掛けた数を超えることはできません。

  インスタンスの最大数 = アベイラビリティーゾーンの数 * 32

- 総再生時間（分）: 総再生時間を選択します。スケーリングが発生するために、スケールパラメータのしきい値を超える必要のある時間。この指定された時間内に収集されたすべてのサンプルでしきい値を超えると、スケーリングが行われます。
- クールダウン期間（分）: クールダウン期間を選択します。スケールアウト時のクールダウン期間は、スケールアウトが発生した後に統計の評価を停止する必要がある時間です。この期間は、Autoscale グループのインスタンスの有機的な増加を保証します。次のスケーリング決定をトリガーする前に、現在のトラフィックが安定し、現在のインスタンスのセットで平均化するのを待機します。
- プロビジョニング解除中の待機時間（分）: ドレイン接続のタイムアウト時間を選択します。スケールインアクション中、インスタンスはプロビジョニングを解除するように識別されます。Citrix ADM は、指定された時間が経過するまで、指定されたインスタンスが新しい接続を処理することを制限し、プロビジョニングを解除します。この期間では、このインスタンスへの既存の接続をプロビジョニング解除する前にドレインアウトできます。
- **DNS** 存続時間（秒）: 時間（秒）を選択します。この期間では、ルータがパケットを廃棄する前に、ネットワーク内にパケットが存在するように設定されます。このパラメーターは、Microsoft Azure トラフィックマネージャーを使用して、トラフィック分散モードが DNS である場合にのみ適用されます。



3. ［次へ］をクリックします。

手順 **3**: **Citrix ADC** インスタンスを **Provisioning** するためのライセンスを構成する

次のいずれかのモードを選択して、AutoScale グループの一部である Citrix ADC インスタンスにライセンスを付与します。

- **Citrix ADM** 使用：Citrix ADC インスタンスの Provisioning 中に、Autoscale グループは Citrix ADM からライセンスをチェックアウトします。
- **Microsoft Azure** の使用：［クラウドから割り当て］オプションでは、Azure マーケットプレイスで利用可能な Citrix 製品ライセンスが使用されます。Citrix ADC インスタンスの Provisioning 時に、Autoscale グループはマーケットプレイスのライセンスを使用します。

  Azure Marketplace のライセンスを使用する場合は、[プロビジョニングパラメータ] タブで製品またはライセンスを指定します。

詳しくは、「ライセンス要件」を参照してください。

Citrix ADM ライセンスを使用する

このオプションを使用するには、［Azure でのライセンスソフトウェアの持ち込み］プランで Citrix ADC 製品をサブスクライブしていることを確認します。Microsoft Azure で Citrix ADC VPX ライセンスを購読するを参照してください。

1. [ライセンス] タブで、[**ADM** から割り当て] を選択します。
2. [ライセンスの種類] で、リストから次のいずれかのオプションを選択します。
   - 帯域幅ライセンス**:** [帯域幅ライセンスタイプ] リストから、次のいずれかのオプションを選択できます。
     - プール容量**:** Autoscale グループ内のすべての新しいインスタンスに割り当てる容量を指定します。

       共通プールから、Autoscale グループの各 ADC インスタンスは 1 つのインスタンス・ライセンスをチェックアウトし、帯域幅が指定されている分だけチェックアウトします。
     - **VPX** ライセンス： Citrix ADC VPX インスタンスがプロビジョニングされると、インスタンスは Citrix ADM からライセンスをチェックアウトします。
   - 仮想 **CPU** ライセンス：プロビジョニングされた Citrix ADC VPX インスタンスは、Autoscale グループで実行されている CPU の数に応じてライセンスをチェックアウトします。

   > 注：
   >
   > プロビジョニングされたインスタンスが削除または破棄されると、適用されたライセンスは Citrix ADM ライセンスプールに戻ります。これらのライセンスは、次回の Autoscale 時に新しいインスタンスをプロビジョニングするために再利用することができます。
3. [ライセンスエディション] で、ライセンスエディションを選択します。Autoscale グループは、指定されたエディションを使用してインスタンスをプロビジョニングします。
4. ［次へ］をクリックします。

ステップ **4:** クラウドパラメータを設定する

1.「プロビジョニングパラメータ」タブで、次の詳細を入力します。

   - リソースグループ： Citrix ADC インスタンスを展開するリソースグループを選択します。
   - 製品/ライセンス：プロビジョニングする Citrix ADC 製品バージョンを選択します。選択したタイプに対してプログラムによるアクセスが有効になっていることを確認します。詳しくは、「Microsoft Azure で Citrix ADC VPX ライセンスを購読する」を参照してください。
   - **Azure VM** サイズ**:** リストから必要な仮想マシンのサイズを選択します。

     > 注**:**
     >
     > 選択した Azure VM サイズに、最低 3 つの NIC があることを確認します。詳しくは、「自動スケーリングでサポートされる Azure 仮想イメージ」を参照してください。

   - **ADC** のクラウドアクセスプロファイル： Citrix ADM は、このプロファイルを使用して Azure アカウントにログインし、ADC インスタンスをプロビジョニングまたはプロビジョニング解除します。また、Azure LB または Azure DNS も構成します。
   - イメージ：必要な Citrix ADC バージョンイメージを選択します。［新規追加］をクリックして、Citrix ADC イメージを追加します。
   - セキュリティグループ：セキュリティグループは、Citrix ADC VPX インスタンスのインバウンドトラフィックとアウトバウンドトラフィックを制御します。管理、クライアント、およびサーバーのトラフィックのセキュリティグループを選択します。管理、クライアント、およびサーバーのセキュリティグループについて詳しくは、「セキュリティグループ」を参照してください。
   - サブネット： Citrix ADC サブネットを Autoscale するには、管理、クライアント、サーバーサブネットなど、3 つの別々のサブネットが必要です。サブネットには、自動スケーリングに必要なエンティティが含まれています。選択について詳しくはサブネットを参照してください。

2. [完了] をクリックします。

手順 **5: Autoscale** グループのアプリケーションを構成する

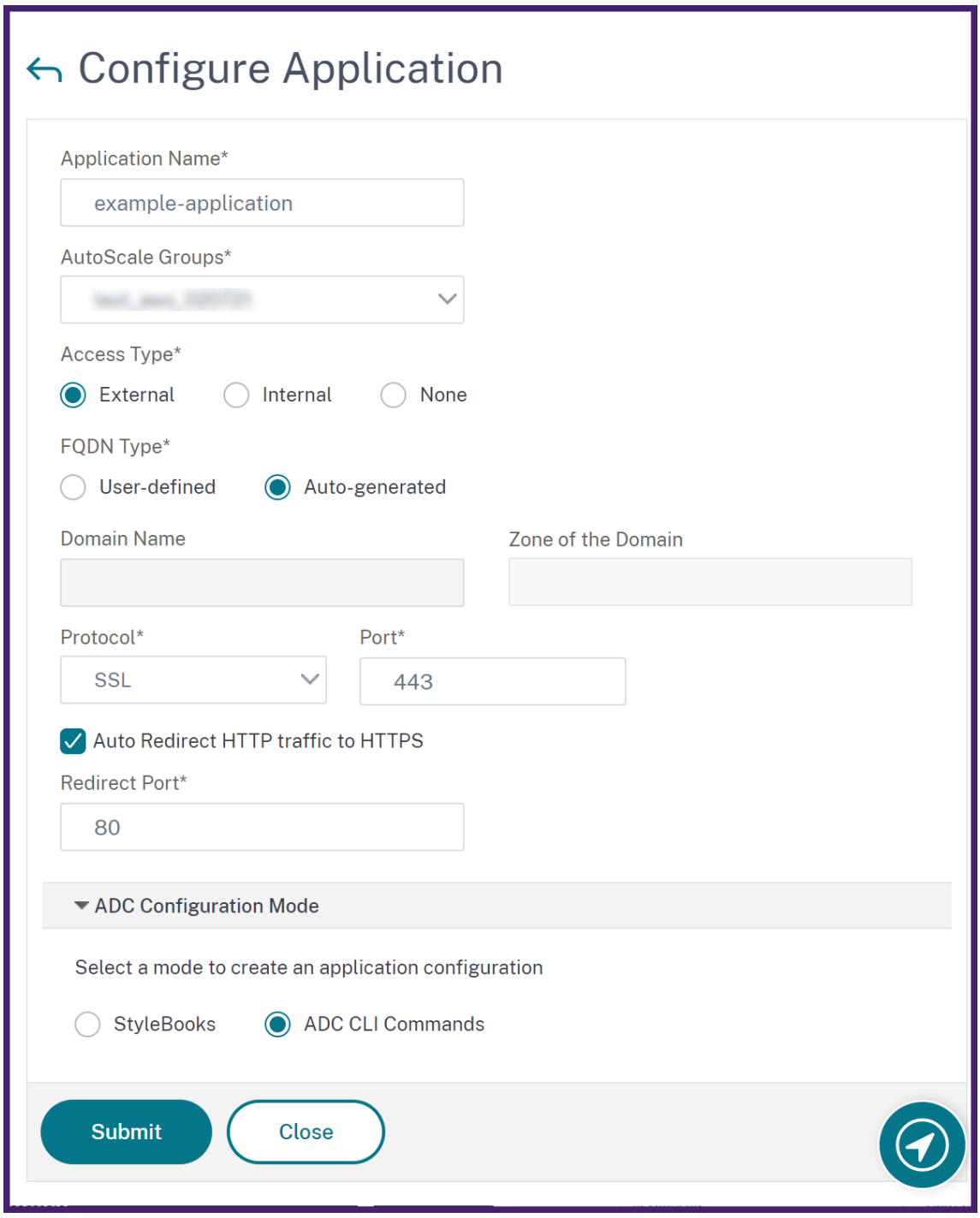
1. Citrix ADM で、［ネットワーク］>［**AutoScale** グループ］に移動します。
2. 作成した Autoscale グループを選択し、[設定] をクリックします。
3.「アプリケーションの構成」で、次の詳細を指定します。

   - アプリケーション名 -アプリケーションの名前を指定します。
   - アクセスタイプ -ADM Auto Scaling ソリューションは外部アプリケーションと内部アプリケーションの両方に使用できます。必要なアプリケーションアクセスタイプを選択します。
   - **FQDN** タイプ -ドメイン名とゾーン名を割り当てるモードを選択します。

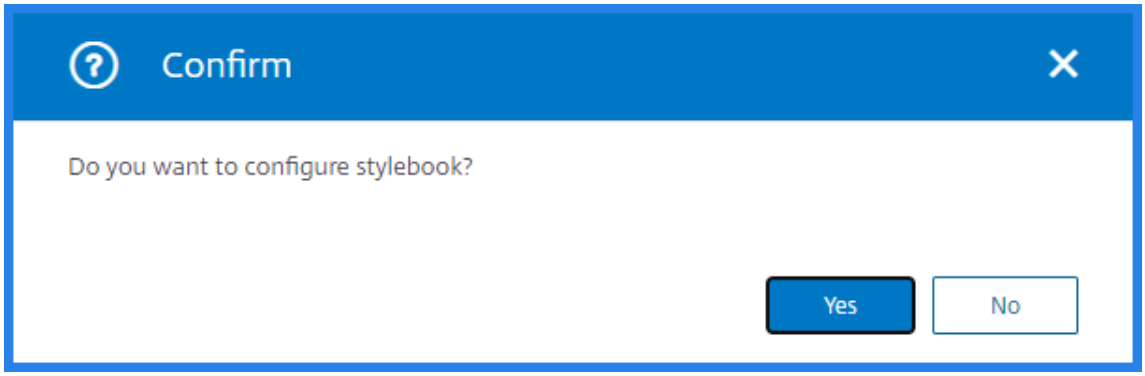
手動で指定する場合は、[ユーザー定義] を選択します。ドメイン名とゾーン名を自動的に割り当てるには、[自動生成] を選択します。

- ドメイン名 -アプリケーションのドメイン名を指定します。このオプションは、[ユーザー定義 FQDN タイプ] を選択した場合にのみ適用されます。
- **[** ドメインのゾーン]: リストからアプリケーションのゾーン名を選択します。このオプションは、[ユーザー定義 FQDN タイプ] を選択した場合にのみ適用されます。

  このドメイン名とゾーン名は、Azure の仮想サーバーにリダイレクトされます。たとえば、`app.example.com`でアプリケーションをホストする場合、`app`はドメイン名、`example.com`はゾーン名です。
- **Protocol**： リストからプロトコルタイプを選択します。設定されたアプリケーションは、選択したプロトコルタイプに応じてトラフィックを受信します。
- [ポート]: ポート値を指定します。指定されたポートは、アプリケーションと Autosale グループ間の通信を確立するために使用されます。

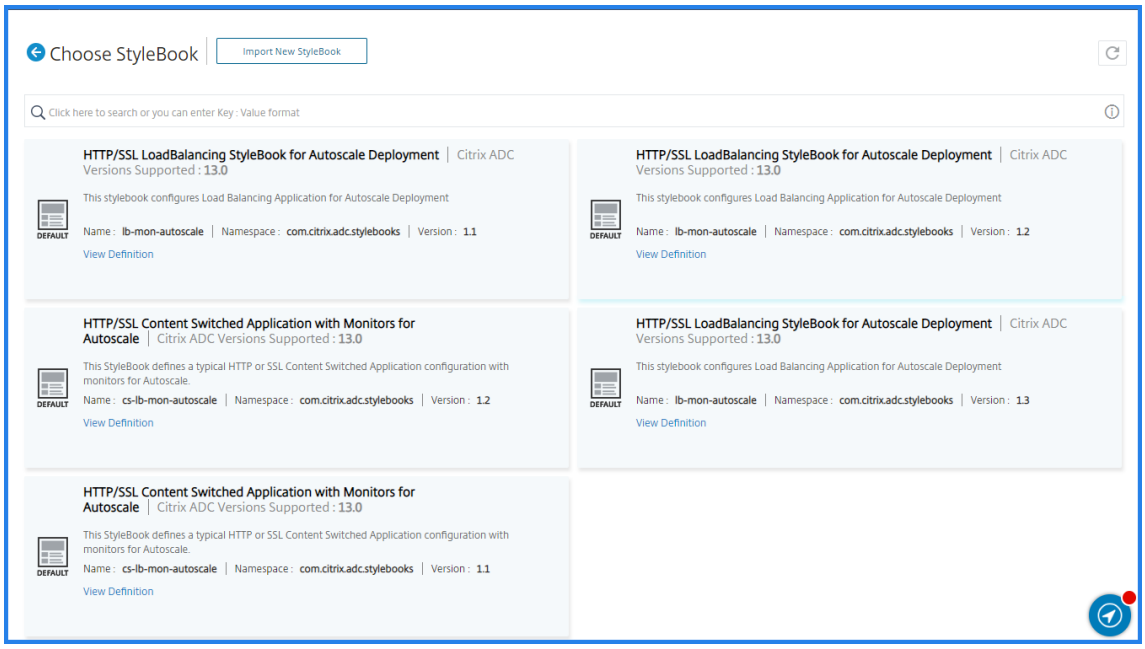


StyleBooks を使用してアプリケーションを構成する場合は、確認ウィンドウで [はい] を選択します。



> メモ今後次の詳細を変更する場合は
>
> 、アプリケーションのアクセスタイプを変更します。
>
> - FQDN タイプ
> - ドメイン名
> - ドメインのゾーン

4. 選択した Autoscale グループの構成を展開する必要な StyleBook を選択します。



StyleBook をインポートする場合は、「新しい **StyleBook** をインポート」をクリックします。

5. すべてのパラメータの値を指定します。

   構成パラメータは、選択した StyleBook にあらかじめ定義されています。

6. [アプリケーションサーバーグループタイプ **CLOUD**] チェックボックスをオンにして、仮想マシンのスケールセットで使用可能なアプリケーションサーバーを指定します。

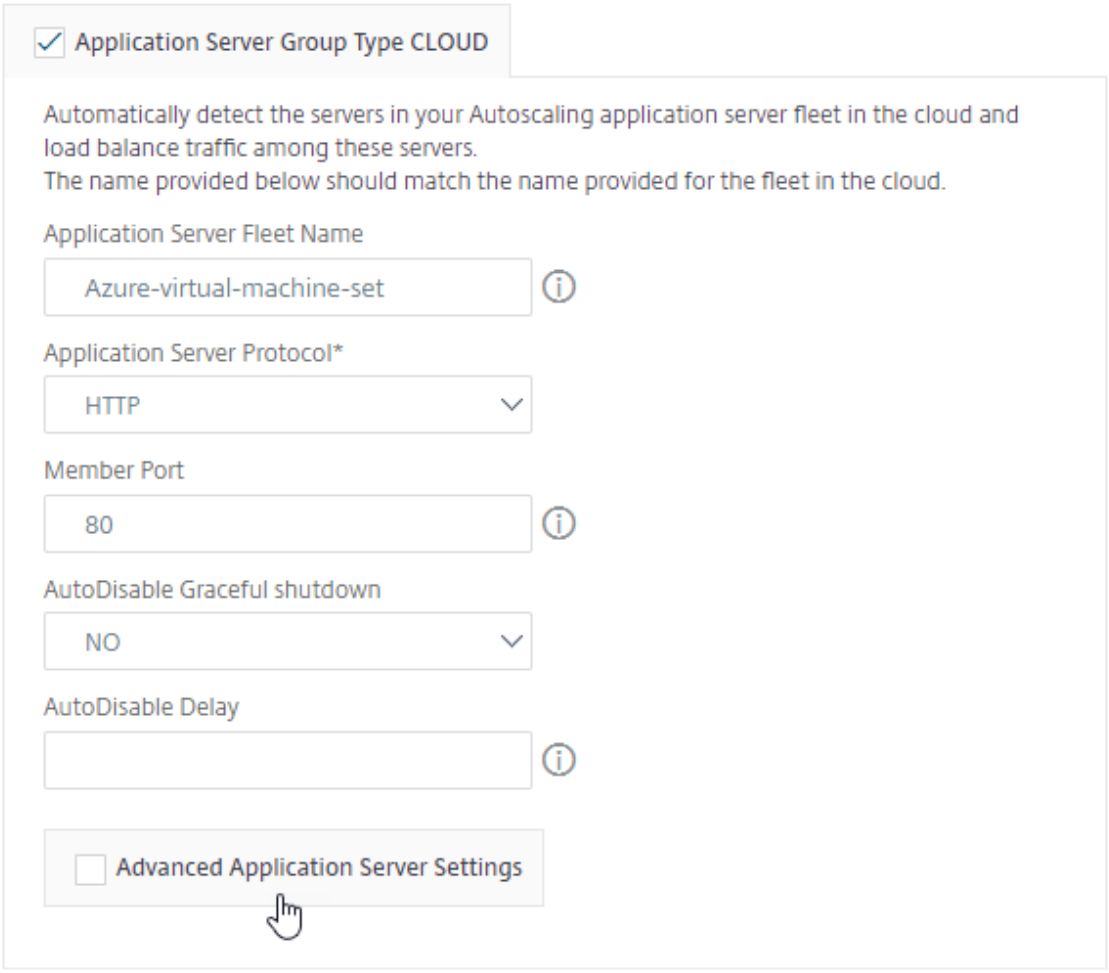
   a) [アプリケーションサーバーフリート名] で、仮想マシンのスケールセットの **AutoScale** 設定名を指定します。

b) リストから アプリケーションサーバープロトコルを選択します。

c)「メンバー・ポート」で、アプリケーション・サーバーのポート値を指定します。

> 注:
>
> ［自動無効グレースフルシャットダウン］が［いいえ］に設定され、［**AutoDisable** 遅延］フィールドが空白になっていることを確認してください。

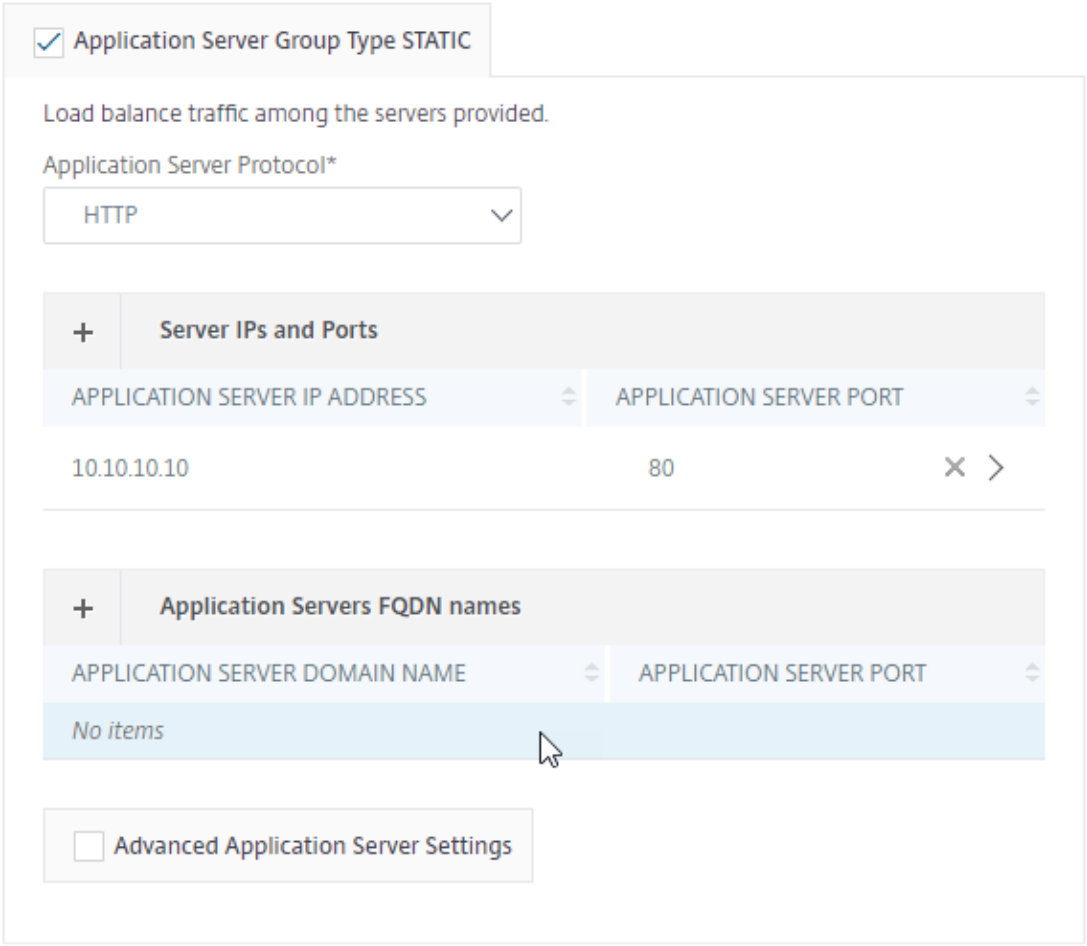
d) アプリケーションサーバーの詳細設定を指定する場合は、「アプリケーションサーバー の詳細設定」チェックボックスをオンにします。次に、[アプリケーションサーバーの詳細設定] に表示されている必要な値を指定します。



7. 仮想ネットワークにスタンドアロンのアプリケーションサーバーがある場合は、「アプリケーションサーバーグループタイプ **STATIC** 」チェックボックスをオンにします。

a) リストから アプリケーションサーバープロトコルを選択します。

b)「サーバーの **IP** とポート」で、「**+** 」をクリックしてアプリケーションサーバーの IP アドレス、ポート、および重みを追加し、「作成」をクリックします。



8. ［作成］をクリックします。

Autoscale グループ構成の変更

Autoscale グループ構成を変更したり、Autoscale グループを削除したりできます。変更できるのは、次の Autoscale グループパラメータのみです。

- しきい値パラメータの最大値と最小値
- 最小および最大インスタンス値
- 排水接続期間の値
- クールダウン期間の値
- ウォッチの継続時間の値

Autoscale グループは、作成後に削除することもできます。

Autoscale グループを削除すると、すべてのドメインと IP アドレスが DNS から登録解除され、クラスターノードのプロビジョニングが解除されます。

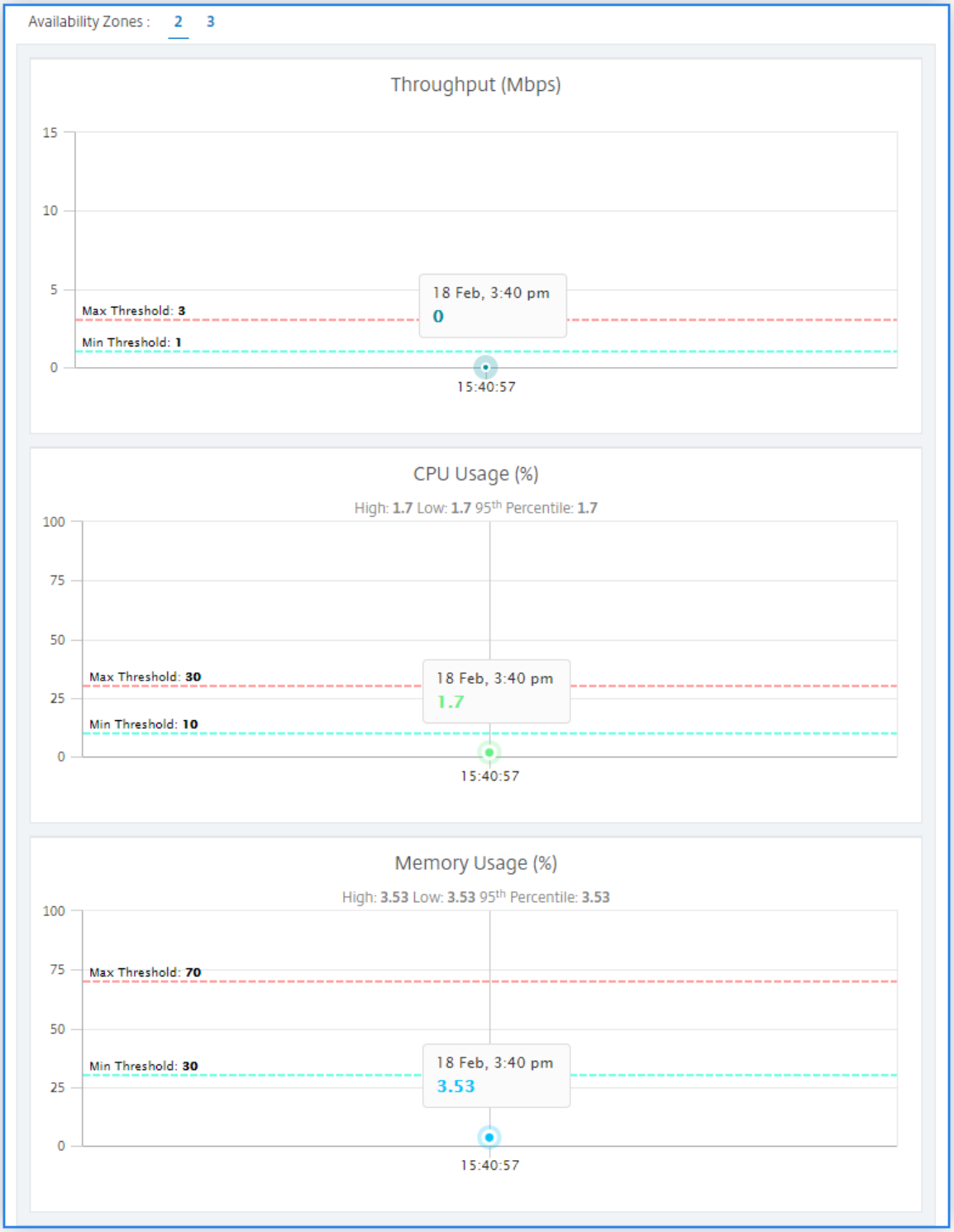
ダッシュボード

May 7, 2021

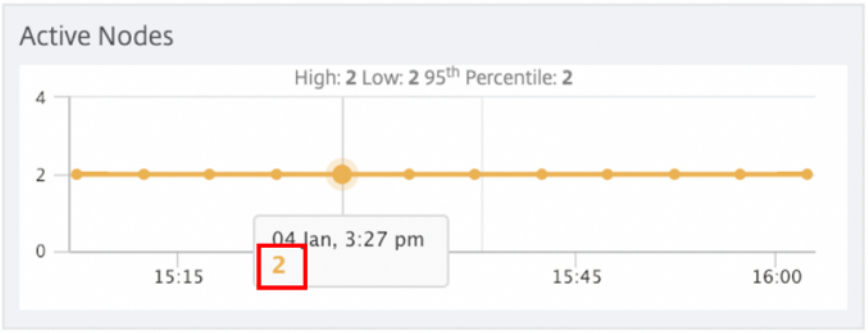
1. Citrix ADM で、［ネットワーク］**>**［グループの **Autoscale**］に移動します。
2. Autoscale グループを選択し、[ダッシュボード] をクリックします。

選択したモニタリングパラメータのグラフを表示できます。右側のパネルには、自動スケーリングをトリガーするイベントが表示されます。左側のパネルには、ゾーンごとのクラスタ内のアクティブなノード、アクティブなノードのグラフ、およびイベントが表示されます。

次の図は、サンプルのダッシュボードを示しています。

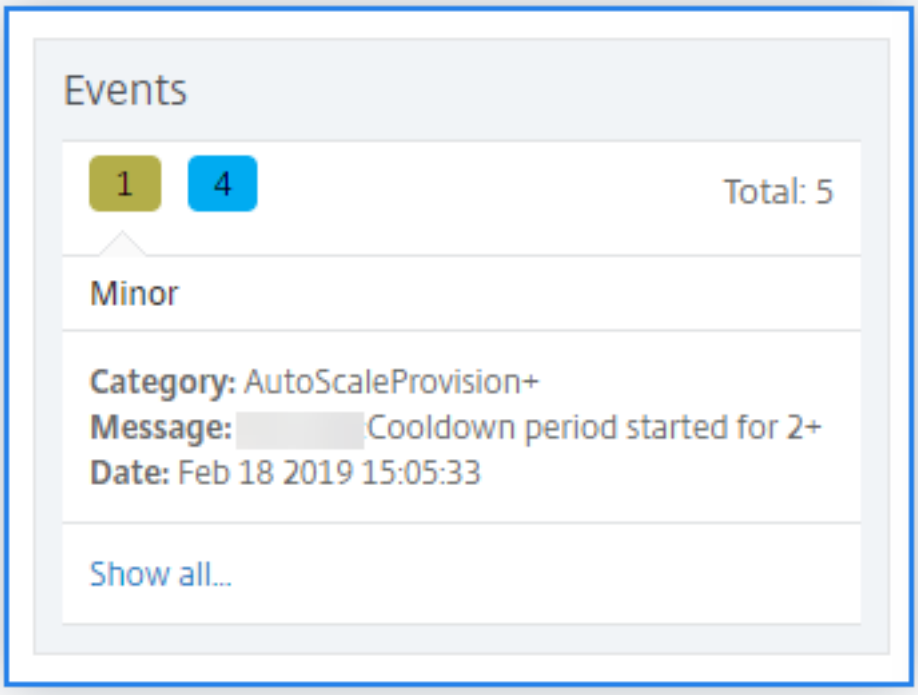


次の図は、アクティブなノードのグラフを示しています。タイムスタンプの下の数字は、アクティブノードの数を示します。アベイラビリティーゾーンに含まれるアクティブなノードの数は、いつでも表示できます。

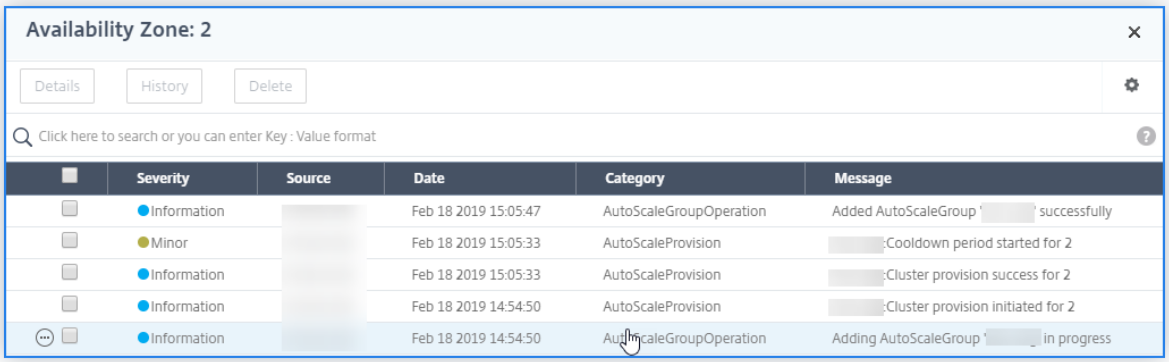


イベント

ダッシュボードの [イベント] タブには、選択した Autoscale グループのイベントの合計数が表示されます。また、最新のイベントの簡単なメッセージも表示されます。



イベントの詳細を表示するには、[すべて表示] をクリックします。



Azure 用語集

May 7, 2021

Citrix ADM で必要な Azure の用語の一覧を次に示します。

用語	定義
Azure ロードバランサー	Azure ロードバランサーは、ネットワーク内の Citrix ADC VPX インスタンス間で着信トラフィックを分散するリソースです。トラフィックは、ロードバランサーセット内に定義された仮想マシンに分配されます。ロードバランサーには、外部ロードバランサー、インターネットに接続するロードバランサー、または内部ロードバランサーがあります。
トラフィックマネージャ	Azure トラフィックマネージャーは、Microsoft Azure の DNS ベースのロードバランサーです。ネットワーク内の目的の Citrix ADC VPX インスタンスに着信トラフィックを送信します。
Azure Resource Manager (ARM)	ARM は、Azure のサービスの新しい管理フレームワークです。Azure Load Balancer は、ARM ベースの API およびツールを使用して管理されます。
バックエンド・アドレス・プール	これらの IP アドレスは、負荷が分散される仮想マシン NIC に関連付けられます。
BLOB	バイナリラージオブジェクト — Azure ストレージに格納できるファイルまたはイメージなどの任意のバイナリオブジェクト。

用語	定義
フロントエンド IP 構成	Azure ロードバランサーには、1 つ以上のフロントエンド IP アドレス (仮想 IP (VIP) とも呼ばれます) を含めることができます。これらの IP アドレスがトラフィックの入口として使用されます。
インスタンスレベルのパブリック IP（ILPIP）	ILPIP は、クラウドサービスではなく、仮想マシンまたはロールインスタンスに直接割り当てることができるパブリック IP アドレスです。この IP は、クラウドサービスに割り当てられている VIP (仮想 IP) の代わりには使用されません。むしろ、仮想マシンまたはロールインスタンスに直接接続するために使用できる追加の IP アドレスです。
インバウンド NAT ルール	これらのルールは、ロードバランサーのパブリックポートを、バックエンドアドレスプール内の特定の仮想マシンのポートにマッピングします。
IP コンフィグ	これは、個々の NIC に関連付けられた IP アドレスのペア（パブリック IP とプライベート IP）です。IP-Config では、パブリック IP アドレスが NULL の場合があります。各 NIC には、最大 255 個の IP 構成を関連付けることができます。
ロードバランシングのルール	特定のフロントエンド IP とポートの組み合わせを、バックエンド IP アドレスとポートの組み合わせのセットにマップする規則プロパティ。ロードバランサーリソースの単一の定義で、複数のロードバランシングルールを定義できます。各ルールは、仮想マシンに関連付けられたフロントエンド IP とポート、バックエンド IP とポートの組み合わせを反映します。
ネットワークセキュリティグループ（NSG）	NSG には、仮想ネットワーク内の仮想マシンインスタンスへのネットワークトラフィックを許可または拒否するアクセスコントロールリスト (ACL) ルールのリストが含まれています。NSG は、サブネット、またはそのサブネット内の個々の仮想マシンインスタンスに関連付けることができます。

用語	定義
プライベート IP アドレス	このアドレスは、Azure 仮想ネットワーク内の通信に使用される IP アドレスです。また、VPN Gateway を使用してネットワークを Azure に拡張する場合のオンプレミスネットワークです。プライベート IP アドレスにより、Azure リソースは他のリソースと通信できます。仮想ネットワークまたはオンプレミスネットワークでの通信は、VPN Gateway または ExpressRoute 回線を介して行われます。この通信には、インターネットで到達可能な IP アドレスは必要ありません。 Azure Resource Manager デプロイモデルでは、プライベート IP アドレスが Azure の仮想マシン、内部ロードバランサ (ILB)、およびアプリケーションゲートウェイに関連付けられます。
プローブ	バックエンドアドレスプール内の仮想マシンインスタンスの可用性をチェックするために使用されるヘルスプローブ。
パブリック IP アドレス (PIP)	PIP は、インターネットとの通信に使用されます。これには、仮想マシン、内部ロードバランサ (ILB)、VPN ゲートウェイ、および Azure のアプリケーションゲートウェイに関連付けられた Azure の一般向けサービスが含まれます。
リージョン	国境を越えない地理内のエリア。1 つ以上のデータセンターが含まれています。価格設定、地域サービスおよびタイプは、リージョンレベルで公開されます。リージョンは通常、リージョナルペアから遠く離れた別のリージョンとペアになります。リージョンペアは、ディザスタリカバリや高可用性シナリオのメカニズムとしても使用されます。ロケーションとも呼ばれます。
リソースグループ	リソースマネージャのコンテナは、アプリケーションに関連するリソースを保持します。リソースグループには、アプリケーションのすべてのリソースを含めることも、論理的にグループ化されたリソースのみを含めることもできます。

用語	定義
ストレージアカウント	Azure ストレージアカウントを使用すると、Azure Storage 内の Azure BLOB、キュー、テーブル、およびファイルサービスにアクセスできます。ストレージアカウントは、Azure ストレージデータオブジェクトに一意の名前空間を提供します。
仮想マシン	オペレーティングシステムを実行する物理コンピュータのソフトウェア実装。同じハードウェア上で複数の仮想マシンを同時に実行できます。Azure では、仮想マシンはさまざまなサイズで利用できます。
仮想ネットワーク	Azure 仮想ネットワークは、クラウド内の独自のネットワークを表現したものです。これは、論理的に分離され、Azure クラウドのサブスクリプション専用です。このネットワーク内の IP アドレスブロック、DNS 設定、セキュリティポリシー、およびルートテーブルを制御できます。

Google クラウドでの Citrix ADC VPX インスタンスのプロビジョニング

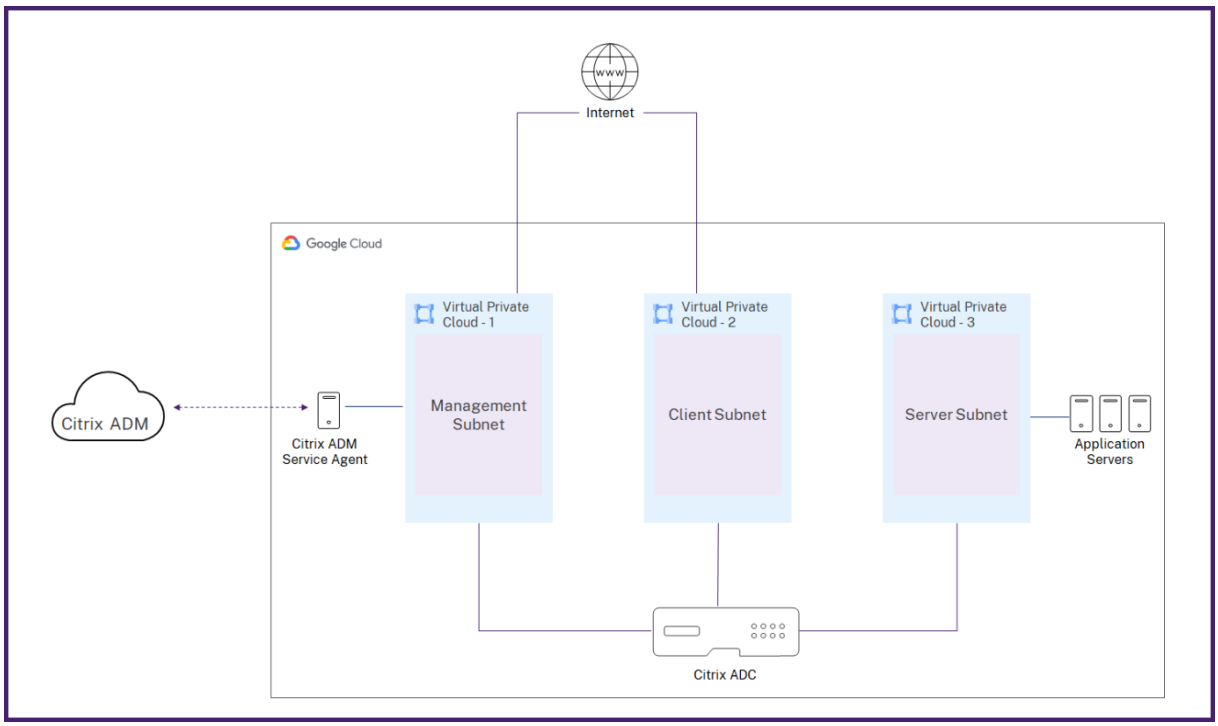
May 7, 2021

Google Cloud でホストされるアプリケーションやサービスは、安全なトラフィック管理とネットワークリソースの効率的な最適化に加え、クラウドのメリットも必要です。Google Cloud にプロビジョニングされた Citrix ADC VPX インスタンスは、安全なトラフィック管理、リソース消費の最適化、ウェブアプリケーションの所有コストの削減を実現します。

Citrix ADM を使用すると、Google Cloud での ADC VPX インスタンスの展開、セットアップ、管理を自動化できます。ADM を使用して Citrix ADC VPX インスタンスをプロビジョニングすると、クラウドの柔軟性と柔軟性と Citrix ADC 制御機能が組み合わされます。

Citrix ADM 展開アーキテクチャ

次の画像は、Citrix ADM と Google クラウドを接続して Google クラウドで Citrix ADC VPX インスタンスをプロビジョニングする方法の概要を示しています。



Google Cloud で Citrix ADC VPX インスタンスをプロビジョニングおよび管理するには、3 つの仮想プライベートクラウド（VPC）ネットワークが必要です。VPC ネットワークには、サブネットとファイアウォールが含まれています。ファイアウォールには、サブネットへの着信トラフィックと発信トラフィックを制御するルールがあります。

Citrix ADM サービスエージェントは、Citrix ADC VPX インスタンスのプロビジョニングと管理に役立ちます。

前提条件

このセクションでは、Citrix ADC VPX インスタンスをプロビジョニングする前に、Google Cloud および Citrix ADM で完了する必要がある前提条件について説明します。

このドキュメントでは、Google Cloud アカウントを所有していることを前提としています。アカウントの作成方法の詳細については、「Google クラウドドキュメント」を参照してください。

Google クラウドコンポーネントを設定する

Citrix ADM で Citrix ADC VPX インスタンスをプロビジョニングする前に、Google Cloud で次のタスクを実行します。

1. API の有効化
2. サービスアカウントの作成
3. VPC ネットワークを作成する
4. ファイアウォールの作成
5. Google クラウドで Citrix ADC VPX ライセンスを購読する

API の有効化

Citrix ADM では、Google Cloud で必要なリソースを展開およびプロビジョニングするには、プログラムによるアクセスが必要です。そのため、Google クラウドプロジェクトで次の API を有効にします。

- Compute Engine API
- クラウド DNS API

Google クラウドで API を有効にする方法の詳細については、「API の有効化」を参照してください。

サービスアカウントの作成

ADM は、サービスアカウントを使用して Google クラウドリソースにアクセスします。サービスアカウントを作成するには、次の手順を実行します。

1. Google クラウドアカウントにログインします。
2. [**IAM** と管理] **>** [サービスアカウント] に移動します。
3. [**+** サービスアカウントの作成] をクリックします。

   2 つのサービスアカウントを作成し、1 つのサービスアカウントを ADM に使用します。また、ADC インスタンスには別のものが使用されます。サービスアカウントを作成するには、次の手順を実行します。

   a) 名前、ID、および説明を指定し、[作成] をクリックします。

   b) 次の定義済みロールを割り当てます。

   - ADM に必要な IAM ロール

   ```
   roles/iam.serviceAccountUser
   roles/compute.instanceAdmin.v1
   roles/compute.networkAdmin
   roles/dns.admin
   <!--NeedCopy-->
   ```

   - ADM によって作成される ADC インスタンスに必要な IAM ロール:

   ```
   roles/compute.instanceAdmin.v1
   roles/compute.networkAdmin
   <!--NeedCopy-->
   ```

   これらのロールにより、サービスアカウントが Google Cloud リソースにアクセスできるようになります。

   c) [完了] をクリックします。

VPC ネットワークを作成する

VPC ネットワークに、管理、クライアント、およびサーバー接続用の 3 つのサブネットを作成します。カスタムオプションを選択して、サブネットを作成します。各サブネットのアドレス範囲を指定します。サブネットを配置するリージョンを指定します。

- 管理**:** 管理 VPC ネットワーク内の管理専用のサブネット。Citrix ADC は、Google クラウドサービスに連絡する必要があり、インターネットアクセスが必要です。
- クライアント**:** クライアント側専用のクライアント VPC ネットワーク内のサブネット。通常、Citrix ADC は、インターネットからパブリックサブネット経由でアプリケーションのクライアントトラフィックを受信します。
- サーバー: アプリケーションサーバーがプロビジョニングされるサブネット。すべてのアプリケーションサーバーがこのサブネットに存在し、このサブネットを介して Citrix ADC からのアプリケーショントラフィックを受信します。Google Cloud でサブネットを作成する方法の詳細については、「VPC ネットワークの概要」を参照してください。

ファイアウォールの作成

ファイアウォールには、Citrix ADC VPX インスタンスのインバウンドトラフィックとアウトバウンドトラフィックを制御するルールがあります。規則は、必要に応じていくつでも追加できます。Citrix ADC インスタンスを AutoScale するには、3 つのファイアウォールを作成する必要があります。

- 管理：ファイアウォールは、Citrix ADC VPX の管理専用です。Citrix ADC は、Google クラウドサービスに連絡する必要があり、インターネットアクセスが必要です。受信規則は、次の TCP ポートおよび UDP ポートで許可されます。
  - TCP: 80、22、443、3008—3011、4001、27000、7279
  - UDP: 67、123、161、500、3003、4500、7000

  > 注:
  >
  > ファイアウォールにより、Citrix ADM エージェントが VPX にアクセスできることを確認してください。

- クライアント：ファイアウォールは、Citrix ADC VPX インスタンスのクライアント側通信専用です。通常、受信規則は TCP ポート 80、22、および 443 で許可されます。
- サーバー：ファイアウォールは、Citrix ADC VPX サーバー側通信専用です。Google Cloud でファイアウォールを作成する方法の詳細については、「VPC ファイアウォールルールの概要」を参照してください。

Google クラウドで **Citrix ADC VPX** ライセンスを購読する

1. Google クラウドポータルにログオンします。
2. マーケットプレイスで、Citrix ADC を検索し、必要な製品バージョンを選択します。
3. 次のいずれかのライセンスタイプを選択します。

- カスタマーライセンス取得済み
- Enterprise
- Platinum

> 注:
>
> ［カスタマーライセンス］オプションを選択した場合、AutoScale グループは Citrix ADC インスタンスのプロビジョニング中に Citrix ADM からライセンスをチェックアウトします。

Citrix ADM コンポーネントのセットアップ

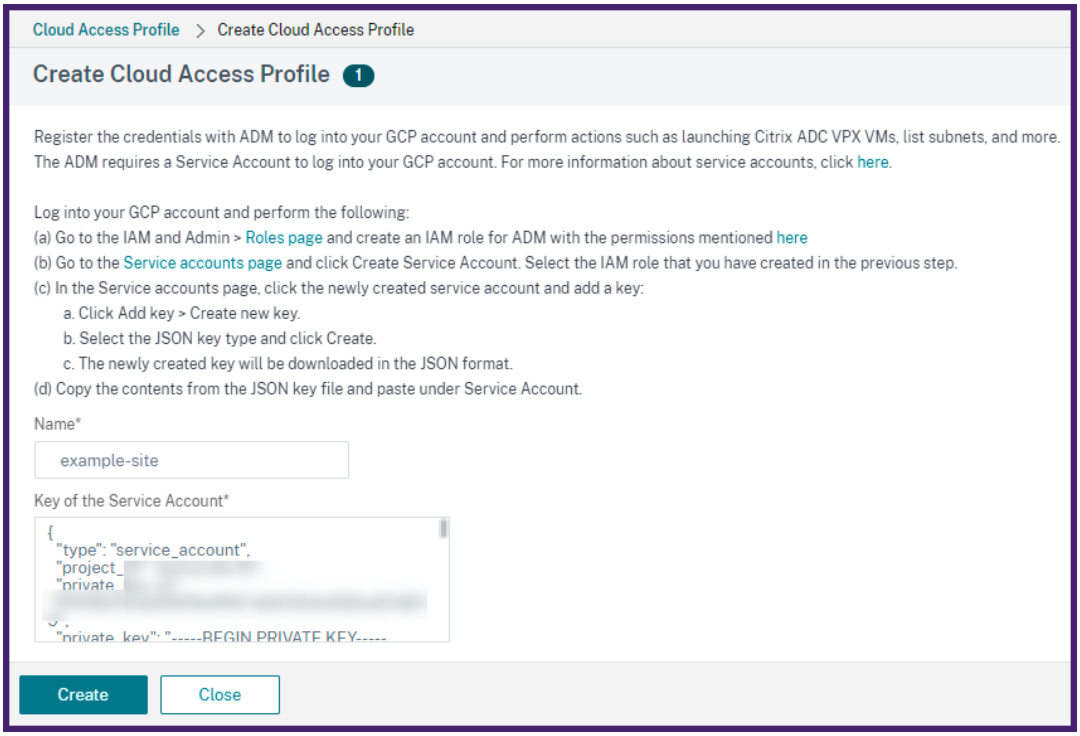
Citrix ADM で Citrix ADC VPX インスタンスをプロビジョニングする前に、Citrix ADM で次のタスクを実行します。

1. サイトを作成する。
2. Google クラウドでの Citrix ADM エージェントのプロビジョニング。
3. Citrix ADM サービスエージェントにサイトを接続する。

サイトの作成

Citrix ADM でサイトを作成し、Google クラウドに関連付けられた VNet の詳細を追加します。

1. Citrix ADM で、［ネットワーク］**>**［サイト］に移動します。
2. ［追加］をクリックします。
3. **[** クラウドを選択**]** ペインで、
   a) [サイトタイプ] として [データセンター] を選択します。
   b) [種類] リストから [**Google** クラウド] を選択します。
   c) [**Google** クラウドからリージョンを取得する] チェックボックスをオンにします。
      このオプションは、Google クラウドアカウントから既存のリージョン情報を取得するのに役立ちます。
   d) ［次へ］をクリックします。
4. **[** リージョンの選択**]** ペインで、
   a) [クラウドアクセスプロファイル] で、Google Cloud アカウント用に作成したプロファイルを選択します。プロファイルがない場合は、プロファイルを作成します。
   b) クラウドアクセスプロファイルを作成するには、[追加] をクリックします。
   c) ［名前］で、Citrix ADM で Google クラウドアカウントを識別する名前を指定します。
   d) [サービスアカウントのキー] で、Google Cloud で作成されたサービスアカウント JSON を指定します。



e) ［作成］をクリックします。

詳しくは、「サービスアカウントの作成」を参照してください。

f) [リージョン] で、管理する Citrix ADC VPX インスタンスを含む VPC ネットワークを含むリージョンを選択します。

g) サイト名を指定します。

h) ［完了］をクリックします。

Google クラウドでの **Citrix ADM** エージェントのプロビジョニング

Citrix ADM サービスエージェントは、Citrix ADM とデータセンターまたはクラウドで検出されたインスタンスの間の仲介として機能します。

1. [ネットワーク**] > [**エージェント**]** に移動します。
2. [プロビジョニング] をクリックします。
3. [**Google** クラウド] を選択し、[次へ] をクリックします。
4. 「プロビジョニングパラメータ」タブで、次の項目を指定します。
   - 名前：Citrix ADM エージェント名を指定します。
   - サイト：エージェントと ADC VPX インスタンスをプロビジョニングするために作成したサイトを選択します。
   - クラウドアクセスプロファイル -リストからクラウドアクセスプロファイルを選択します。

- **[** ゾーン**]: AutoScale** グループを作成するゾーンを選択します。選択したクラウドアクセスプロファイルに応じて、そのプロファイルのゾーンが入力されます。
- [ネットワーク]-AutoScale グループを作成する VPC ネットワークを選択します。
- [**Subnet**]: エージェントをプロビジョニングする管理サブネットを選択します。
- タグ -AutoScale グループタグのキーと値のペアを入力します。タグは、大文字と小文字を区別するキーと値のペアで構成されます。これらのタグを使用すると、Autoscale グループを簡単に整理して識別できます。タグは Google クラウドと Citrix ADM の両方に適用されます。

5. ［完了］をクリックします。

または、Google クラウドマーケットプレイスから Citrix ADM エージェントをインストールすることもできます。詳しくは、「Google クラウドへの Citrix ADM エージェントのインストール」を参照してください。

Citrix ADM サービスエージェントにサイトを接続する

1. Citrix ADM で、［ネットワーク］**>**［エージェント］に移動します。
2. サイトをアタッチするエージェントを選択します。
3. [サイトの添付] をクリックします。
4. リストからアタッチするサイトを選択します。
5. ［保存］をクリックします。

構成タスク

Google Cloud でスタンドアロン ADC VPX インスタンスをプロビジョニングするには、次の手順を実行します。

1. Citrix ADM で、［ネットワーク］**>**［インスタンス］**>**［**Citrix ADC**］の順に移動します。
2. [プロビジョニング] をクリックします。
3. [**Google** クラウド] を選択し、[次へ] をクリックします。インスタンスをプロビジョニングするために必要なパラメータを指定します。
4. 基本パラメータ、ライセンス、およびプロビジョニングパラメータを指定します。

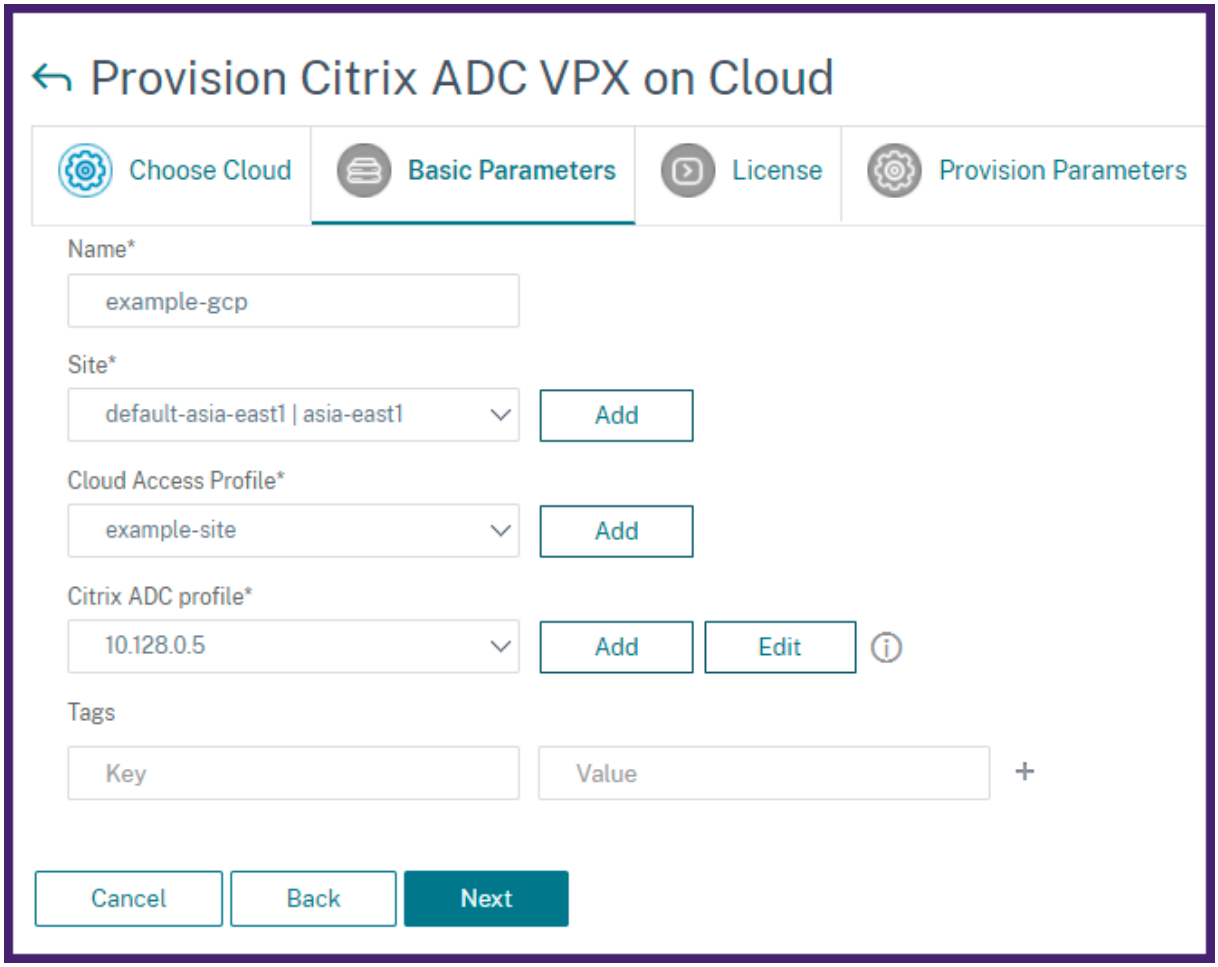
基本パラメータの設定

1. [基本パラメータ] タブで、次の項目を指定します。
   - 名前: ADC VPX インスタンスの名前を指定します。
   - [サイト]: 前に作成したサイトを選択します。
   - エージェント: Citrix ADC VPX インスタンスを管理するために作成されるエージェントを選択します。

- クラウドアクセスプロファイル -サイト作成時に作成されたクラウドアクセスプロファイルを選択します。
- **Citrix ADC** プロファイル：認証を提供するプロファイルを選択します。

  Citrix ADC VPX インスタンスにログオンする必要がある場合、Citrix ADM はデバイスプロファイルを使用します。

2. ［次へ］をクリックします。



ライセンスの設定

ライセンスを ADC インスタンスに適用するには、次のいずれかのモードを選択します。

- **Citrix ADM** を使用する：プロビジョニングするインスタンスは、Citrix ADM からライセンスをチェックアウトします。
- **Google** クラウドの使用：［クラウドから割り当て］オプションでは、Google クラウドマーケットプレイスで利用可能な Citrix 製品ライセンスが使用されます。プロビジョニングするインスタンスは、マーケットプレイスのライセンスを使用します。

Google Cloud Marketplace のライセンスを使用する場合は、[プロビジョニングパラメータ] タブで製品またはライセンスを指定します。

詳しくは、「ライセンス要件」を参照してください。

Citrix ADM ライセンスを使用する

このオプションを使用するには、[Google **Cloud** にライセンスソフトウェアを使用する] プランで Citrix ADC 製品をサブスクライブしていることを確認します。Google クラウドで Citrix ADC VPX ライセンスを購読するを参照してください。

1. [ライセンス] タブで、[**ADM** から割り当て] を選択します。
2. [ライセンスの種類] で、リストから次のいずれかのオプションを選択します。
   - 帯域幅ライセンス**:** [帯域幅ライセンスタイプ] リストから、次のいずれかのオプションを選択できます。
     - プールされた容量**:** インスタンスに割り当てる容量を指定します。

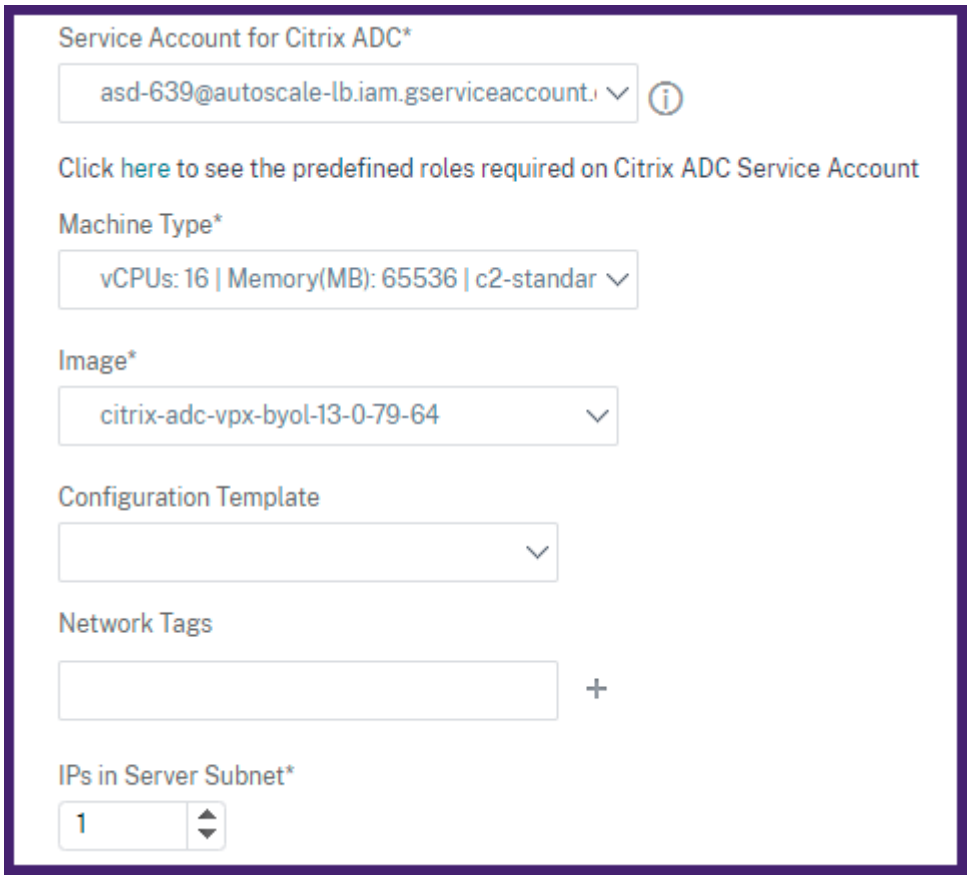
       ADC インスタンスは、共通プールから 1 つのインスタンス・ライセンスをチェックアウトし、指定された帯域幅だけを指定します。
     - **VPX** ライセンス： Citrix ADC VPX インスタンスがプロビジョニングされると、インスタンスは Citrix ADM からライセンスをチェックアウトします。
   - 仮想 **CPU** ライセンス：プロビジョニングされた Citrix ADC VPX インスタンスは、インスタンスで実行されている CPU の数に応じてライセンスをチェックアウトします。

   > 注:
   >
   > プロビジョニングされたインスタンスが削除または破棄されると、適用されたライセンスは Citrix ADM ライセンスプールに戻ります。これらのライセンスは、新しいインスタンスをプロビジョニングするために再利用することができます。
3. [ライセンスエディション] で、ライセンスエディションを選択します。ADM は、指定されたエディションを使用してインスタンスをプロビジョニングします。
4. [次へ] をクリックします。

プロビジョニングパラメータの構成

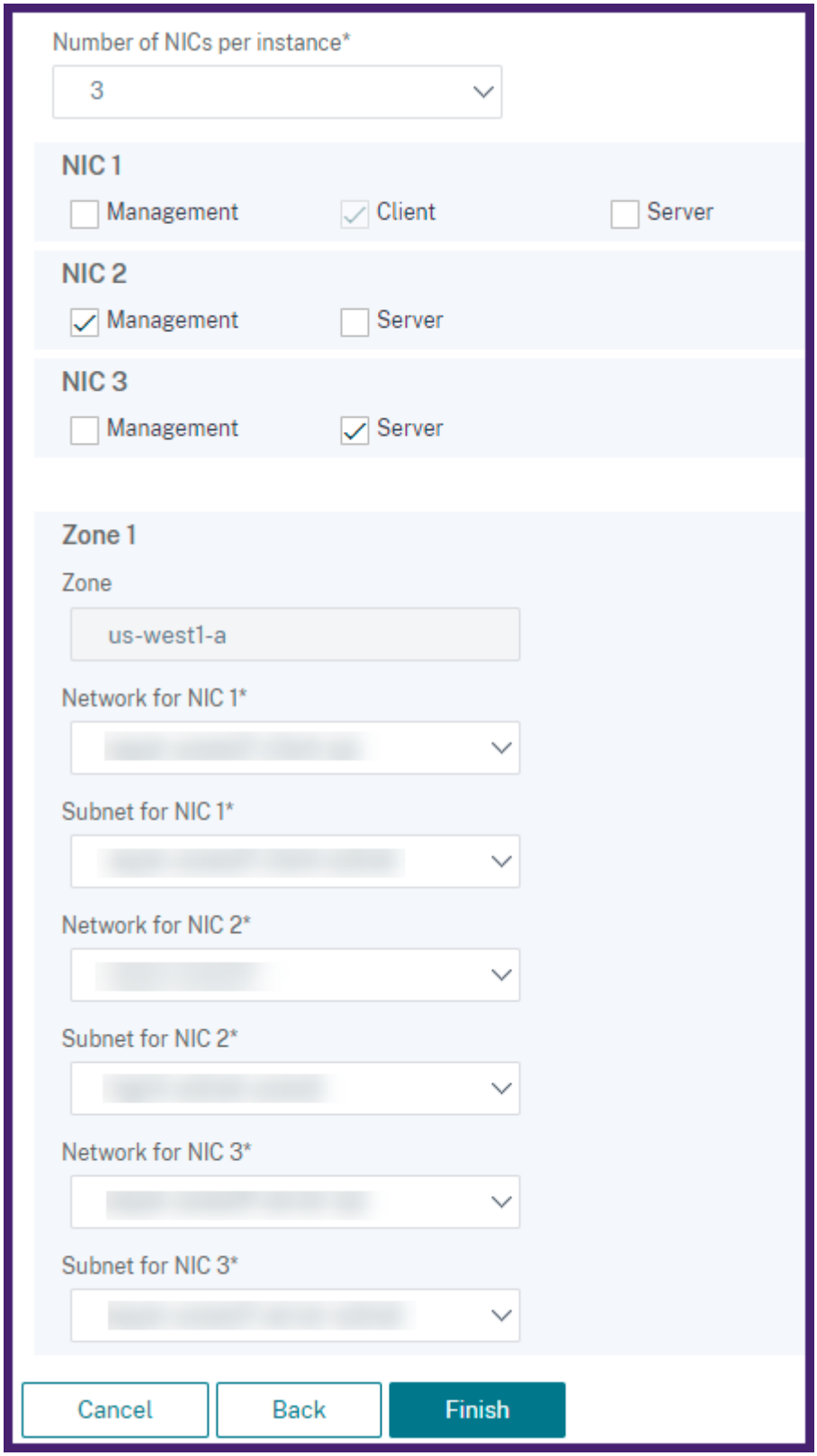
1. 「プロビジョニングパラメータ」タブで、次の項目を指定します。
   - **ADC** サービスアカウント: Google クラウドで作成したサービスアカウントを選択します。ADM は、サービスアカウントを使用して Google クラウドリソースにアクセスします。
   - 製品**/**ライセンス： プロビジョニングする Citrix ADC 製品のバージョンを選択します。詳細については、「Google Cloud で Citrix ADC VPX ライセンスを購読する」を参照してください。
   - マシンタイプ: リストから必要なマシンタイプを選択します。

- イメージ：必要な Citrix ADC バージョンイメージを選択します。［新規追加］をクリックして、Citrix ADC イメージを追加します。
- 「構成テンプレート」— ADC インスタンスへのデプロイに使用する設定テンプレートを選択します。
- [インスタンスごとのサーバーサブネット内の **IP**] — サーバーサブネット内に各インスタンスが持つことができる SNIP アドレスの数を指定します。



このタブでは、必要な NIC を指定および構成することもできます。各 NIC には、専用のファイアウォールとサブネットが含まれています。

詳しくは、「VPC ネットワークを作成する」および「ファイアウォールの作成」を参照してください。



2. ［完了］をクリックします。

プロビジョニングされた **Citrix ADC VPX** インスタンスの表示

Citrix ADM で表示するには:

1. Citrix ADM で、［ネットワーク］>［インスタンス］**>**［**Citrix ADC**］に移動します。
2. ［**Citrix ADC VPX** ］タブを選択します。

   Google クラウドでプロビジョニングされた Citrix ADC VPX インスタンスは、ここに記載されています。

Google クラウドで表示するには:

1. Google クラウドポータルにログオンします。
2. プロビジョニングされた Citrix ADC VPX インスタンスを表示する［リソース］タブに移動します。

> 注:
>
> Citrix ADC VPX インスタンスの名前は、Citrix ADM でインスタンスをプロビジョニングするときに指定した名前と同じです。

Citrix ADM を使用した **Google** クラウドでの **Citrix ADC VPX** の自動スケーリング

May 7, 2021

自動スケーリングは、実際の使用状況に応じて自動的にリソースを追加または削除するクラウドコンピューティング方法です。自動スケーリングは、変動するクライアント要求や処理ジョブ数を満たすために、サイトまたはアプリケーションがオンデマンドのリソース割り当てを必要とする場合に便利です。

Web アプリケーションやサービスの需要は大きく異なる場合があります。トラフィックのニーズに応じて適切な数の Citrix ADC インスタンスを維持することが重要です。Google Cloud のネットワークリソースは、需要に応じて増減できます。したがって、パフォーマンスを損なうことなく、コストの最適化を提供します。
Citrix Application Delivery Management（ADM）オートスケーリングでは、リソースの消費量が変動するため、Citrix ADC インスタンスの正確な数が維持されます。Citrix ADM は、変動するリソース消費量に基づいてトラフィックフローを決定し、Citrix ADC インスタンスを動的にスケールアウトまたはスケールインします。したがって、適切な数の Citrix ADC インスタンスを維持するための柔軟性を提供します。

Citrix ADM は、Citrix ADC インスタンスのリソース使用率を監視し、設定されたしきい値と照合します。設定されたリソースの 1 つが指定されたしきい値を超えると、スケールアウトアクションがトリガーされます。

Citrix ADM は、構成されているすべてのリソースの使用量が通常のしきい値を下回った場合にのみ、スケールインアクションをトリガーします。

> 重要:
>
> 自動スケーリングは、クラスターノード上でスポット設定を必要とする以下の機能を除き、すべての Citrix ADC 機能をサポートします。

> - GSLB か
> - Citrix Gateway とその機能
> - Telco 機能
>
> スポッティング設定について詳しくは、ストライプ、部分的にストライプ、およびスポットされた構成を参照してください。

長所

アプリケーションの高可用性：自動スケーリングにより、アプリケーションのトラフィック要求を処理するための適切な数の Citrix ADC VPX インスタンスが常に確保されます。これにより、トラフィック要求に関係なく、アプリケーションが常に起動し、実行されていることが保証されます。

スマートなスケーリングの決定とゼロタッチ構成：自動スケーリングはアプリケーションを継続的に監視し、需要に応じて Citrix ADC インスタンスを動的に追加または削除します。一定期間需要が増加すると、インスタンスは自動的に追加されます。一定期間需要が減少すると、インスタンスは自動的に削除されます。Citrix ADC インスタンスの追加と削除は自動的に行われるため、手動でのゼロタッチ構成になります。

自動 **DNS** 管理： Citrix ADM Autoscale 機能は、自動 DNS 管理を提供します。新しい Citrix ADC インスタンスが追加されると、ドメイン名が自動的に更新されます。

正常な接続終了：スケールイン中、Citrix ADC インスタンスは正常に削除され、クライアント接続が失われるのを防ぎます。

コスト管理の向上：自動スケーリングは、必要に応じて Citrix ADC インスタンスを動的に増減します。この方法では、関連するコストを最適化できます。必要なときにのみインスタンスを起動し、不要になったときにインスタンスを終了すると、運用コストが削減されます。したがって、使用したリソースに対してのみお支払いいただきます。

オブザーバビリティ**:** オブザーバビリティは、アプリケーションの稼働状態を監視するアプリケーションの開発/運用担当者にとって重要です。Citrix ADM の AutoScale ダッシュボードでは、しきい値のパラメーター値、AutoScale トリガーのタイムスタンプ、イベント、および Autocale に参加しているインスタンスを視覚化できます。

ライセンスの要件

Citrix Autoscale グループ用に作成された Citrix ADC インスタンスは、Citrix ADC アドバンストライセンスまたはプレミアム ADC ライセンスを使用します。Citrix ADC クラスタリング機能は、アドバンストまたはプレミアム ADC ライセンスに含まれています。

次のいずれかの方法を選択して、Citrix ADCCitrix ADM によってプロビジョニングされた Citrix ADC のライセンスを取得できます。

- **Citrix ADM** に存在する **ADC** ライセンスを使用する：AutoScale グループの作成時に、プール容量、VPX ライセンス、または仮想 CPU ライセンスを構成します。したがって、Autocale グループに対して新しいインスタンスがプロビジョニングされると、既に設定されているライセンスタイプがプロビジョニングされたインスタンスに自動的に適用されます。

- プールされた容量: Autocale グループ内のすべてのプロビジョニングされたインスタンスに帯域幅を割り当てます。新しいインスタンスをプロビジョニングするために必要な帯域幅が Citrix ADM で利用可能であることを確認します。詳しくは、「プール容量を構成する」を参照してください。

  Autocale グループの各 ADC インスタンスは、1 つのインスタンス・ライセンスと、指定された帯域幅をプールからチェックアウトします。

- **VPX** ライセンス: 新しくプロビジョニングされたインスタンスに VPX ライセンスを適用します。新しいインスタンスをプロビジョニングするために、Citrix ADM で必要な数の VPX ライセンスがあることを確認します。

  Citrix ADC VPX インスタンスがプロビジョニングされると、インスタンスは Citrix ADM からライセンスをチェックアウトします。詳細については、「Citrix ADC VPX チェックインおよびチェックアウトライセンス」を参照してください。

- 仮想 CPU ライセンス: 新しくプロビジョニングされたインスタンスに仮想 CPU ライセンスを適用します。このライセンスでは、Citrix ADC VPX インスタンスの資格を持つ CPU の数を指定します。新しいインスタンスをプロビジョニングするために必要な数の仮想 CPU が Citrix ADM にあることを確認します。

Citrix ADC VPX インスタンスがプロビジョニングされると、インスタンスは Citrix ADM から仮想 CPU ライセンスをチェックアウトします。詳細については、「Citrix ADC 仮想 CPU ライセンス」を参照してください。

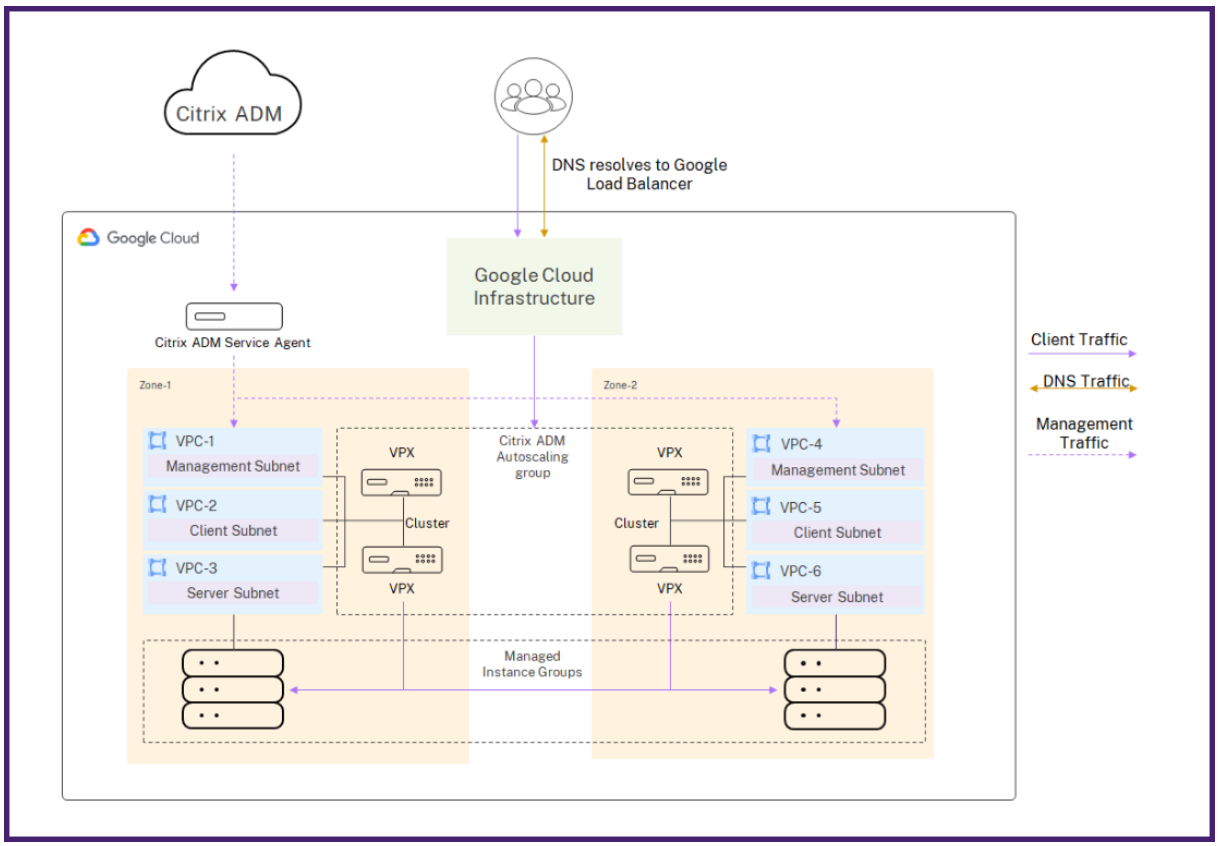
プロビジョニングされたインスタンスが破棄またはプロビジョニング解除されると、適用されたライセンスは自動的に Citrix ADM に返されます。

消費されたライセンスを監視するには、[ネットワーク**] > [**ライセンス**]** ページに移動します。

- **Google Cloud** サブスクリプションライセンスの使用: AutoScale グループの作成時に、Google マーケットプレイスで利用可能な Citrix ADC ライセンスを構成します。そのため、Autosale グループに対して新しいインスタンスがプロビジョニングされると、ライセンスは Google Marketplace から取得されます。

アーキテクチャ

Citrix ADM は、Google ネットワークロードバランサーを使用してクライアントトラフィックの分散を処理します。次の図は、トラフィックディストリビュータとして Google ネットワークロードバランサーを使用して自動スケーリングがどのように行われるかを示しています。



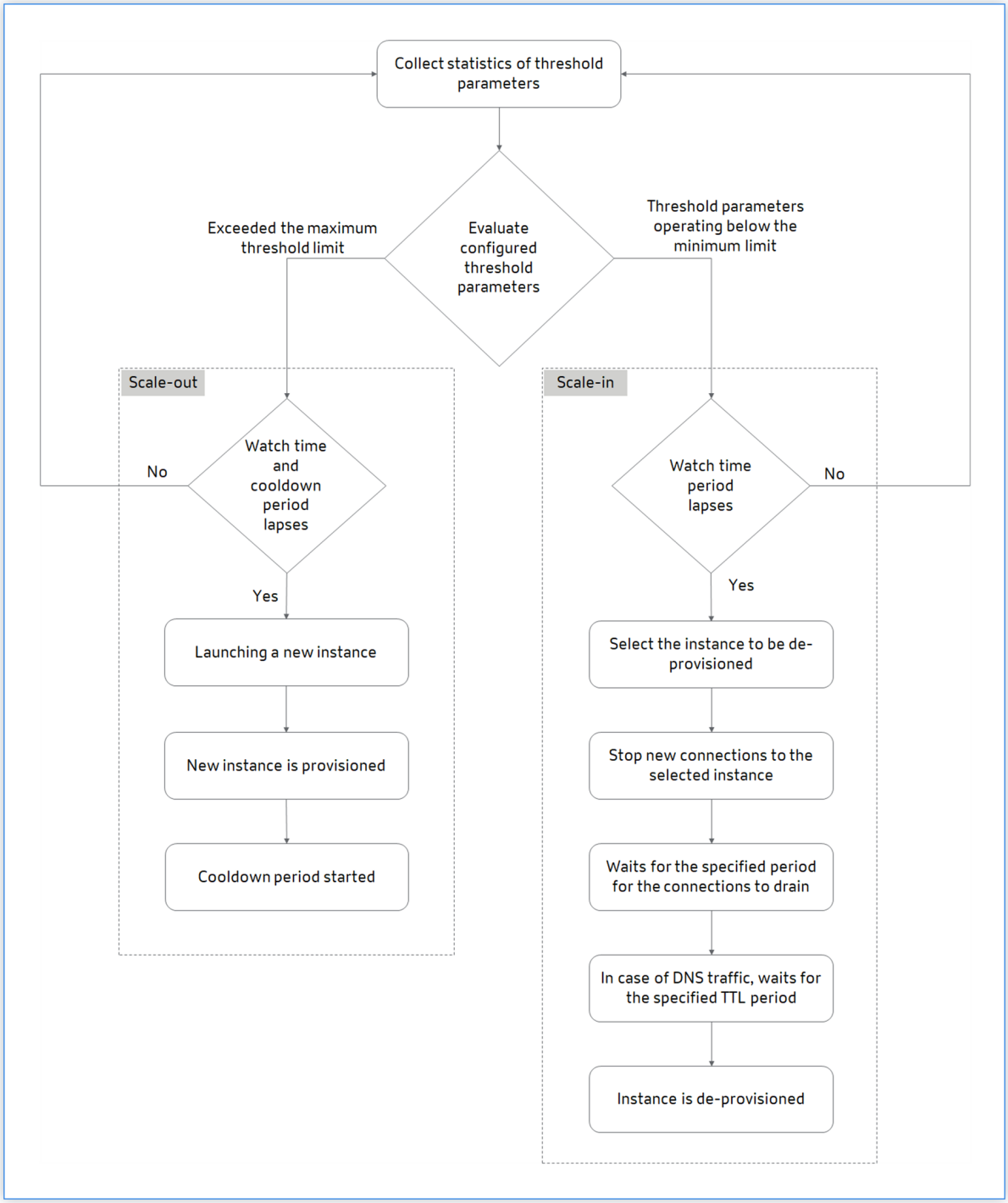
Google ネットワークロードバランサーは、クラスターノードへの分散層です。ネットワークロードバランサーは、クライアントトラフィックを管理し、Citrix ADC VPX クラスタに配信します。ネットワークロードバランサーは、クライアントトラフィックを Citrix ADC VPX クラスタノードに送信します。このクラスタノードは、複数のゾーンにまたがる Citrix ADM 自動スケーリンググループで使用できます。

Citrix ADM は、クラスターレベルでスケールアウトまたはスケールインアクションをトリガーします。スケールアウトがトリガーされると、登録された仮想マシンがプロビジョニングされ、クラスターに追加されます。同様に、スケールインがトリガーされると、Citrix ADC VPX クラスターからノードが削除され、プロビジョニングが解除されます。

Citrix ADMAutoScale グループは、単一のエンティティとしてアプリケーションを負荷分散し、構成されたしきい値パラメータ値に基づいて自動スケーリングをトリガーする Citrix ADC インスタンスのグループです。

オートスケーリングの仕組み

次のフローチャートは、オートスケーリングのワークフローを示しています。



Citrix ADM は、Autoscale プロビジョニングされたクラスターから毎分統計情報（CPU、メモリ、スループット）を収集します。

統計情報は、設定しきい値に対して評価されます。統計情報に応じて、スケールアウトまたはスケールインがトリガーされます。統計情報が最大しきい値を超えると、スケールアウトがトリガーされます。統計情報が最小しきい値を下回ると、スケールインがトリガーされます。

スケールアウトがトリガーされた場合:

1. 新しいノードがプロビジョニングされます。
2. ノードがクラスタに接続され、構成がクラスタから新しいノードに同期されます。
3. ノードは Citrix ADM に登録されています。
4. 新しいノードの IP アドレスが Google ネットワークロードバランサーで更新されます。

スケールインがトリガーされた場合:

1. 削除するノードが識別されます。
2. 選択したノードへの新しい接続を停止します。
3. ノードがクラスタから切り離され、Citrix ADM から登録解除され、Google Cloud からプロビジョニング解除されます。

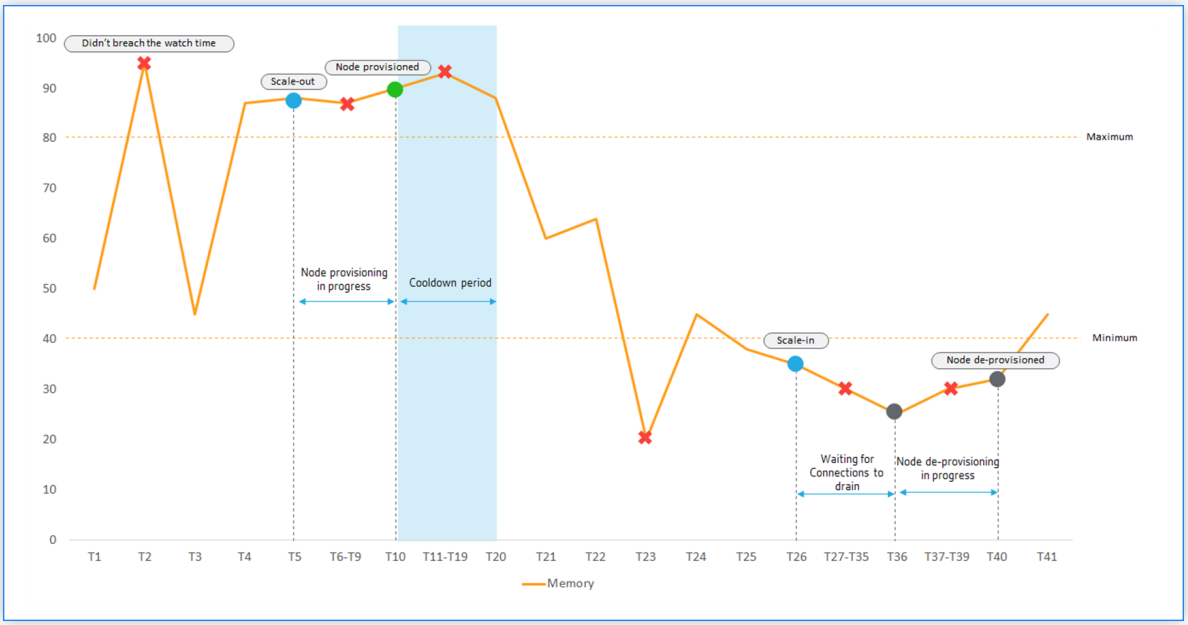
> 注
>
> アプリケーションをデプロイすると、すべてのアベイラビリティーゾーンのクラスターに IP セットが作成されます。次に、ドメインとインスタンスの IP アドレスが Google ネットワークロードバランサーに登録されます。アプリケーションを削除すると、ドメインとインスタンスの IP アドレスは Google ネットワークロードバランサーから登録解除されます。次に、IP セットが削除されます。

オートスケーリングのシナリオの例

次の設定を使用して、単一のアベイラビリティーゾーンに asg_arn という名前の Autoscale グループを作成したとします。

- 選択されたしきい値パラメータ — メモリ使用量。
- メモリに設定されたしきい値の制限:
  - 最小制限:40
  - 最大制限:85
- 総再生時間 — 2 分。
- クールダウン期間 — 10 分。
- プロビジョニング解除中の待機時間（10 分）。
- DNS の存続時間 — 10 秒。

[Autoscale] グループが作成されると、[Autoscale] グループから統計が収集されます。Autoscale ポリシーは、Autoscale イベントが進行中かどうかも評価します。自動スケーリングが進行中の場合は、そのイベントが完了するのを待ってから、統計情報を収集します。



イベントのシーケンス

1. メモリ使用量が **T2** のしきい値制限を超えています。ただし、スケールアウトは指定された総再生時間に対して違反しなかったため、トリガーされません。
2. スケールアウトは、最大しきい値が 2 分（総再生時間）連続的に突破された後、**T5** でトリガーされます。
3. ノードの Provisioning が進行中であるため、**T5-T10** 間の違反に対するアクションは実行されていません。
4. ノードは **T10** でプロビジョニングされ、クラスタに追加されます。クールダウン期間が開始されました。
5. クールダウン期間が原因で、**T10-T20** 間の違反に対する処置は実行されていません。この期間は、Autoscale グループのインスタンスの有機的な増加を保証します。次のスケーリング決定をトリガーする前に、現在のトラフィックが安定し、現在のインスタンスのセットで平均化するのを待機します。
6. メモリ使用量が **T23** の最小しきい値制限を下回っています。ただし、スケールインは指定された総再生時間に対して違反しなかったため、トリガーされません。
7. 最小しきい値が 2 分（総再生時間）連続的に突破された後、スケールインが **T26** でトリガーされます。クラスタ内のノードは、プロビジョニング解除のために識別されます。
8. Citrix ADM が既存の接続を切断するのを待機しているため、**T26-T36** 間の違反に対する処置は実行されていません。DNS ベースの自動スケーリングでは、TTL が有効です。

> 注:
>
> DNS ベースの自動スケーリングの場合、Citrix ADM は指定された TTL（有効期限）期間待機します。次に、ノードのプロビジョニング解除を開始する前に、既存の接続がドレインするのを待機します。

9. ノードのプロビジョニング解除が進行中であるため、**T37-T39** 間の違反に対するアクションは実行されていません。
10. ノードは **T40** でクラスターから削除され、プロビジョニング解除されます。

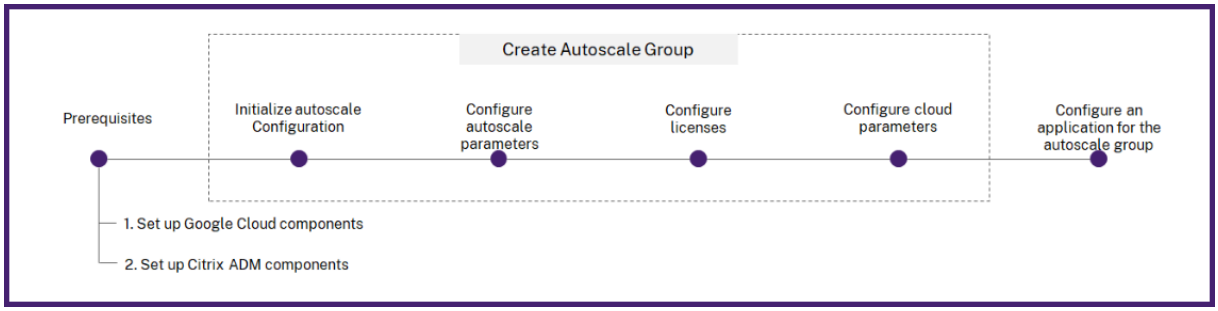
ノードのプロビジョニング解除を開始する前に、選択したノードへのすべての接続がドレインされました。したがって、クールダウン期間は、ノードのプロビジョニング解除後にスキップされます。

構成

May 7, 2021

Citrix ADM は、Google クラウド内のすべての Citrix ADC VPX クラスタを管理します。Citrix ADM は、クラウドアクセスプロファイルを使用して Google Cloud リソースにアクセスします。

次のフロー図は、Autoscale グループを作成および設定する手順を説明しています。



前提条件

このセクションでは、Citrix ADC VPX インスタンスを AutoScale する前に、Google Cloud および Citrix ADM で完了する必要がある前提条件について説明します。

このドキュメントでは、Google Cloud アカウントを所有していることを前提としています。アカウントの作成方法の詳細については、「Google クラウドドキュメント」を参照してください。

Google クラウドコンポーネントを設定する

Citrix ADM で Citrix ADC VPX インスタンスをプロビジョニングする前に、Google Cloud で次のタスクを実行します。

1. API の有効化
2. サービスアカウントの作成
3. VPC ネットワークを作成する
4. ファイアウォールの作成

API の有効化

Citrix ADM では、Google Cloud で必要なリソースを展開およびプロビジョニングするには、プログラムによるアクセスが必要です。そのため、Google クラウドプロジェクトで次の API を有効にします。

- Compute Engine API
- クラウド DNS API

Google クラウドで API を有効にする方法の詳細については、「API の有効化」を参照してください。

サービスアカウントの作成

ADM は、サービスアカウントを使用して Google クラウドリソースにアクセスします。サービスアカウントを作成するには、次の手順を実行します。

1. Google クラウドアカウントにログインします。
2. [**IAM** と管理] **>** [サービスアカウント] に移動します。
3. [**+** サービスアカウントの作成] をクリックします。

   2 つのサービスアカウントを作成し、1 つのサービスアカウントを ADM に使用します。また、ADC インスタンスには別のものが使用されます。サービスアカウントを作成するには、次の手順を実行します。

   a) 名前、ID、および説明を指定し、[作成] をクリックします。

   b) 次の定義済みロールを割り当てます。

   - ADM に必要な IAM ロール

   ```
   roles/iam.serviceAccountUser
   roles/compute.instanceAdmin.v1
   roles/compute.networkAdmin
   roles/dns.admin
   <!--NeedCopy-->
   ```

   - ADM によって作成される ADC インスタンスに必要な IAM ロール:

   ```
   roles/compute.instanceAdmin.v1
   roles/compute.networkAdmin
   <!--NeedCopy-->
   ```

   これらのロールにより、サービスアカウントが Google Cloud リソースにアクセスできるようになります。

   c) [完了] をクリックします。

サービスアカウントを作成したら、そのアカウントにキーを追加します。

1. キーを追加するサービスアカウントを選択します。

2. [キーを追加] **>** [新しいキーを作成] を選択します。
3. JSON キータイプを選択し、[作成] をクリックします。

VPC ネットワークを作成する

VPC ネットワークに、管理、クライアント、およびサーバー接続用の 3 つのサブネットを作成します。カスタムオプションを選択して、サブネットを作成します。各サブネットのアドレス範囲を指定します。サブネットを配置するリージョンを指定します。

- 管理**:** 管理 VPC ネットワーク内の管理専用のサブネット。Citrix ADC は、Google クラウドサービスに連絡する必要があり、インターネットアクセスが必要です。
- クライアント**:** クライアント側専用のクライアント VPC ネットワーク内のサブネット。通常、Citrix ADC は、インターネットからパブリックサブネット経由でアプリケーションのクライアントトラフィックを受信します。
- サーバー: アプリケーションサーバーがプロビジョニングされるサブネット。すべてのアプリケーションサーバーがこのサブネットに存在し、このサブネットを介して Citrix ADC からのアプリケーショントラフィックを受信します。Google Cloud でサブネットを作成する方法の詳細については、「VPC ネットワークの概要」を参照してください。

ファイアウォールの作成

ファイアウォールには、Citrix ADC VPX インスタンスのインバウンドトラフィックとアウトバウンドトラフィックを制御するルールがあります。規則は、必要に応じていくつでも追加できます。Citrix ADC インスタンスを AutoScale するには、3 つのファイアウォールを作成する必要があります。

- 管理: ファイアウォールは、Citrix ADC VPX の管理専用です。Citrix ADC は、Google クラウドサービスに連絡する必要があり、インターネットアクセスが必要です。受信規則は、次の TCP ポートおよび UDP ポートで許可されます。
  - TCP: 80、22、443、3008—3011、4001、27000、7279
  - UDP: 67、123、161、500、3003、4500、7000

  このサブネットからのインターネットアクセスを許可するようにクラウド NAT を設定します。詳しくは、「クラウド NAT の使用」を参照してください。

  > 注:
  >
  > ファイアウォールにより、Citrix ADM エージェントが VPX にアクセスできることを確認してください。

- クライアント: ファイアウォールは、Citrix ADC VPX インスタンスのクライアント側通信専用です。通常、インバウンドルールは TCP ポート 80 および 443 で許可されます。また、ADC インスタンスの状態を監視するには、60000 ポートが必要です。
- サーバー: ファイアウォールは、Citrix ADC VPX サーバー側通信専用です。Google Cloud でファイアウォールを作成する方法の詳細については、「VPC ファイアウォールルールの概要」を参照してください。

Citrix ADM コンポーネントのセットアップ

Citrix ADM で Citrix ADC VPX インスタンスをプロビジョニングする前に、Citrix ADM で次のタスクを実行します。

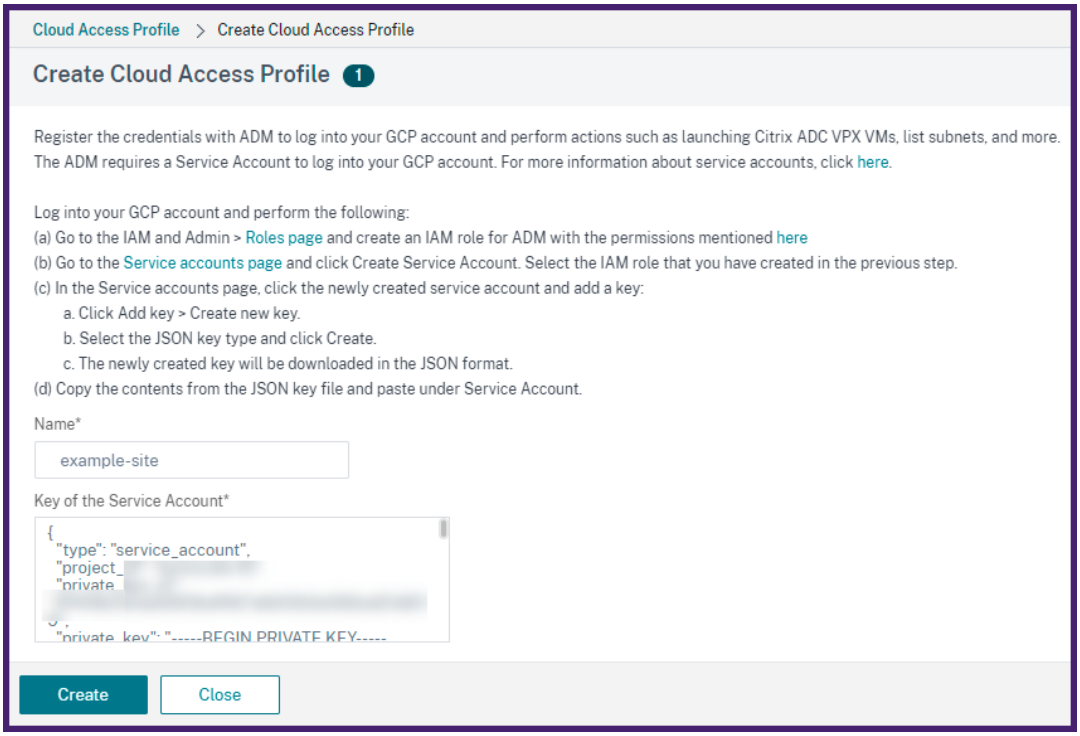
1. サイトを作成する。
2. Google クラウドでの Citrix ADM エージェントのプロビジョニング。
3. Citrix ADM サービスエージェントにサイトを接続する。

サイトの作成

Citrix ADM でサイトを作成し、Google クラウドに関連付けられたクライアント VPC の詳細を追加します。

1. Citrix ADM で、［ネットワーク］**>**［サイト］に移動します。
2. ［追加］をクリックします。
3. **[** クラウドを選択**]** ペインで、
   a) [サイトタイプ] として [データセンター] を選択します。
   b) [種類] リストから [**Google** クラウド] を選択します。
   c) [**Google** クラウドからリージョンを取得する] チェックボックスをオンにします。

      このオプションは、Google クラウドアカウントから既存のリージョン情報を取得するのに役立ちます。
   d) ［次へ］をクリックします。
4. **[** リージョンの選択**]** ペインで、
   a) [クラウドアクセスプロファイル] で、Google Cloud アカウント用に作成したプロファイルを選択します。プロファイルがない場合は、プロファイルを作成します。
   b) クラウドアクセスプロファイルを作成するには、[追加] をクリックします。
   c) ［名前］で、Citrix ADM で Google クラウドアカウントを識別する名前を指定します。
   d) [サービスアカウントのキー] で、Google Cloud で作成されたサービスアカウント JSON を指定します。



e) ［作成］をクリックします。

詳しくは、「サービスアカウントの作成」を参照してください。

f) [リージョン] で、管理する Citrix ADC VPX インスタンスを含む VPC ネットワークを含むリージョンを選択します。

g) サイト名を指定します。

h) ［完了］をクリックします。

Google クラウドでの **Citrix ADM** エージェントのプロビジョニング

Citrix ADM サービスエージェントは、Citrix ADM とデータセンターまたはクラウドで検出されたインスタンスの間の仲介として機能します。

1. [ネットワーク**] > [**エージェント**]** に移動します。
2. [プロビジョニング] をクリックします。
3. [**Google** クラウド] を選択し、[次へ] をクリックします。
4. 「プロビジョニングパラメータ」タブで、次の項目を指定します。
   - 名前：Citrix ADM エージェント名を指定します。
   - サイト：エージェントと ADC VPX インスタンスをプロビジョニングするために作成したサイトを選択します。
   - クラウドアクセスプロファイル -リストからクラウドアクセスプロファイルを選択します。

- **[** ゾーン**]: AutoScale** グループを作成するゾーンを選択します。選択したクラウドアクセスプロファイルに応じて、そのプロファイルのゾーンが入力されます。
- [ネットワーク]-AutoScale グループを作成する VPC ネットワークを選択します。
- [**Subnet**]: エージェントをプロビジョニングする管理サブネットを選択します。
- ラベル -AutoScale グループラベルのキーと値のペアを入力します。タグは、大文字と小文字を区別するキーと値のペアで構成されます。これらのラベルを使用すると、AutoScale グループを容易に整理して識別できます。ラベルは Google クラウドと Citrix ADM の両方に適用されます。

5. [完了] をクリックします。

または、Google クラウドから Citrix ADM エージェントをインストールすることもできます。詳しくは、「Google クラウドへの Citrix ADM エージェントのインストール」を参照してください。

Citrix ADM サービスエージェントにサイトを接続する

1. Citrix ADM で、[ネットワーク] **>** [エージェント] に移動します。
2. サイトをアタッチするエージェントを選択します。
3. [サイトの添付] をクリックします。
4. リストからアタッチするサイトを選択します。
5. [保存] をクリックします。

手順 **1-Citrix ADM** で **AutoScale** 構成を初期化する

1. Citrix ADM で、[ネットワーク] **>** [**AutoScale** グループ] に移動します。
2. [追加] をクリックして、Autoscale グループを作成します。

   [AutoScale グループの作成] ページが表示されます。
3. [**Google** クラウド] を選択し、[次へ] をクリックします。
4. 「基本パラメータ」に、次の詳細を入力します。
   - [名前]: [AutoScale] グループの名前を入力します。
   - サイト: Google Cloud 上の Citrix ADC VPX インスタンスを AutoScale するために作成したサイトを選択します。サイトを作成していない場合は、[追加] をクリックしてサイトを作成します。
   - エージェント: プロビジョニングされたインスタンスを管理する Citrix ADM エージェントを選択します。
   - クラウドアクセスプロファイル: クラウドアクセスプロファイルを選択します。クラウドアクセスプロファイルを追加または編集することもできます。

- **Citrix ADC** プロファイル：リストからデバイスプロファイルを選択します。Citrix ADC VPX インスタンスにログオンする必要がある場合、Citrix ADM はデバイスプロファイルを使用します。
- トラフィック分散モード: Google クラウドは、Google ネットワークロードバランサーを使用した負荷分散の 1 つのトラフィック分散のみをサポートしています。
- **AutoScale** グループを有効にする: ASG グループのステータスを有効または無効にします。このオプションはデフォルトで有効になっています。このオプションを無効にすると、自動スケーリングはトリガーされません。
- ゾーン: 自動尺度グループを作成するリージョンを選択します。選択したクラウドアクセスプロファイルに応じて、リージョンがリストに表示されます。
- ラベル: AutoScale グループラベルのキーと値のペアを入力します。タグは、大文字と小文字を区別するキーと値のペアで構成されます。これらのラベルを使用すると、AutoScale グループを容易に整理して識別できます。ラベルは Google クラウドと Citrix ADM の両方に適用されます。

5. ［次へ］をクリックします。

手順 **2: Autoscale** パラメータを構成する

[自動尺度パラメータ] タブで、次の詳細を入力します。

1. スケールアウトまたはスケールインをトリガーするために値を監視する必要がある次のしきい値パラメータを 1 つ以上選択します。
   - **CPU** 使用率のしきい値の有効化: CPU 使用率に基づいてメトリックを監視します。
   - メモリ使用量のしきい値の有効化：メモリ使用量に基づいてメトリックを監視します。
   - スループットしきい値の有効化: スループットに基づいてメトリックスを監視します。

     > 注
     >
     > - デフォルトの最小しきい値制限は 30 で、最大しきい値制限は 70 です。ただし、制限を変更するには変更します。
     > - 最小しきい値制限は、最大しきい値制限の半分以下である必要があります。
     > - モニタリング用に複数のしきい値パラメータを選択できます。しきい値パラメータの少なくとも 1 つが最大しきい値を超えている場合、スケールアウトがトリガーされます。ただし、スケールインがトリガーされるのは、すべてのしきい値パラメータが通常のしきい値を下回っている場合だけです。

   - 最小インスタンス: この AutoScale グループにプロビジョニングする必要があるインスタンスの最小数を選択します。

     デフォルトの最小インスタンス数は、選択したゾーンの数と同じです。最小インスタンスは、指定されたゾーン数の倍数でのみ増分できます。

たとえば、ゾーンの数が 4 の場合、最小インスタンスはデフォルトで 4 になります。最小インスタンスを 8、12、16 増やすことができます。

- インスタンスの最大数: この AutoScale グループにプロビジョニングする必要があるインスタンスの最大数を選択します。

  インスタンスの最大数は、最小インスタンスの値以上である必要があります。インスタンスの最大数は、ゾーンの数に 32 を乗じた数を超えることはできません。

  インスタンスの最大数 = ゾーン数 * 32

- [総再生時間 **(**分**)**]: 総再生時間を選択します。スケーリングが発生するために、スケールパラメータのしきい値を超える必要のある時間。この指定された時間内に収集されたすべてのサンプルでしきい値を超えると、スケーリングが行われます。

- クールダウン期間 **(**分**)**: クールダウン期間を選択します。スケールアウト時のクールダウン期間は、スケールアウトが発生した後に統計の評価を停止する必要がある時間です。この期間は、Autoscale グループのインスタンスの有機的な増加を保証します。次のスケーリング決定をトリガーする前に、現在のトラフィックが安定し、現在のインスタンスのセットで平均化するのを待機します。

- プロビジョニング解除中の待機時間 **(**分**)**: ドレイン接続のタイムアウト期間を選択します。スケールインアクション中、インスタンスはプロビジョニングを解除するように識別されます。Citrix ADM は、指定された時間が経過するまで、指定されたインスタンスが新しい接続を処理することを制限し、プロビジョニングを解除します。この期間では、このインスタンスへの既存の接続をプロビジョニング解除する前にドレインアウトできます。

2. ［次へ］をクリックします。

手順 **3-**ライセンスの設定

Citrix ADM は、必要なバージョンとライセンスを使用して ADC インスタンスをプロビジョニングします。ADC イメージは、カスタマーライセンス（BYOL）または Google Cloud からライセンスを取得できます。

ライセンスを ADC インスタンスに適用するには、次のいずれかのモードを選択します。

- **Citrix ADM** から割り当て：プロビジョニングするインスタンスは、Citrix ADM からライセンスをチェックアウトします。

- **Google** クラウドから割り当て：［クラウドから割り当て］オプションでは、Google クラウドで利用可能な Citrix 製品ライセンスが使用されます。プロビジョニングするインスタンスは、Google Cloud のライセンスを使用します。

  Google Cloud のライセンスを使用する場合は、[プロビジョニングパラメータ] タブで製品またはライセンスを指定します。

詳しくは、「ライセンス要件」を参照してください。

Citrix ADM からライセンスを割り当てる

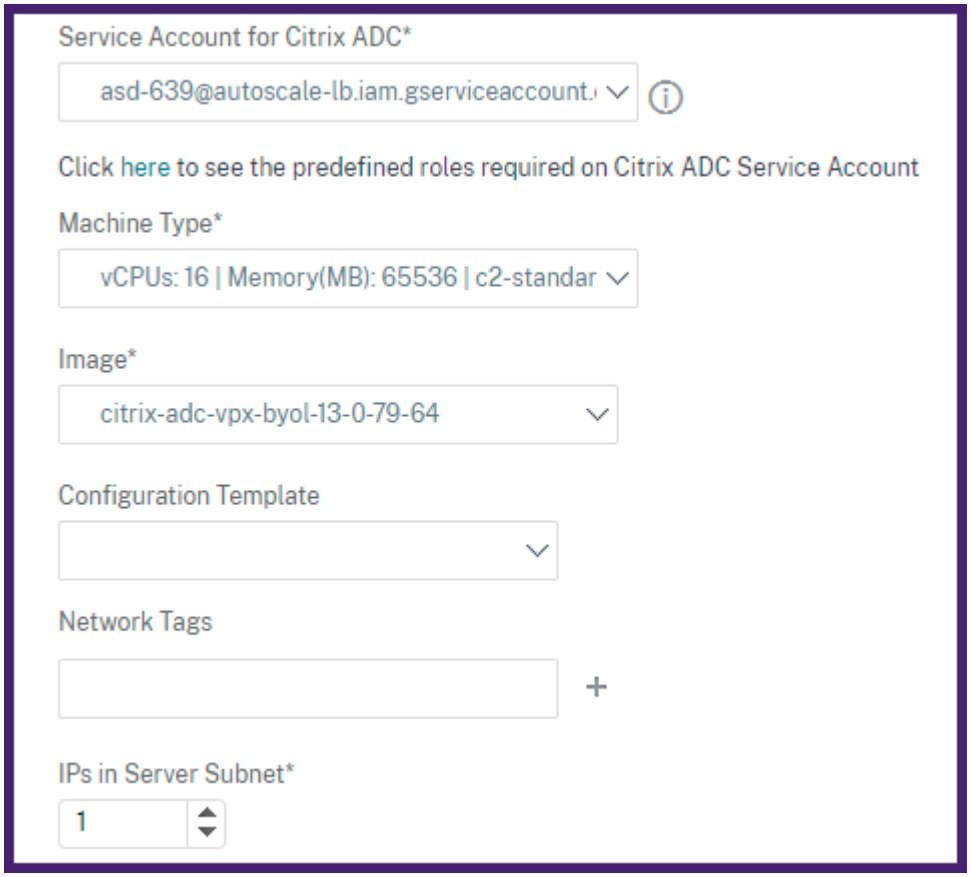
1. [ライセンス] タブで、[**ADM** から割り当て] を選択します。
2. [ライセンスの種類] で、リストから次のいずれかのオプションを選択します。
   - 帯域幅ライセンス**:** [帯域幅ライセンスタイプ] リストから、次のいずれかのオプションを選択できます。
     - プールされた容量**:** インスタンスに割り当てる容量を指定します。

       ADC インスタンスは、共通プールから 1 つのインスタンス・ライセンスをチェックアウトし、指定された帯域幅だけを指定します。
     - **VPX** ライセンス： Citrix ADC VPX インスタンスがプロビジョニングされると、インスタンスは Citrix ADM からライセンスをチェックアウトします。
   - 仮想 **CPU** ライセンス：プロビジョニングされた Citrix ADC VPX インスタンスは、インスタンスで実行されている CPU の数に応じてライセンスをチェックアウトします。

   > 注:
   >
   > プロビジョニングされたインスタンスが削除または破棄されると、適用されたライセンスは Citrix ADM ライセンスプールに戻ります。これらのライセンスは、新しいインスタンスをプロビジョニングするために再利用することができます。
3. [ライセンスエディション] で、ライセンスエディションを選択します。ADM は、指定されたエディションを使用してインスタンスをプロビジョニングします。
4. [次へ] をクリックします。

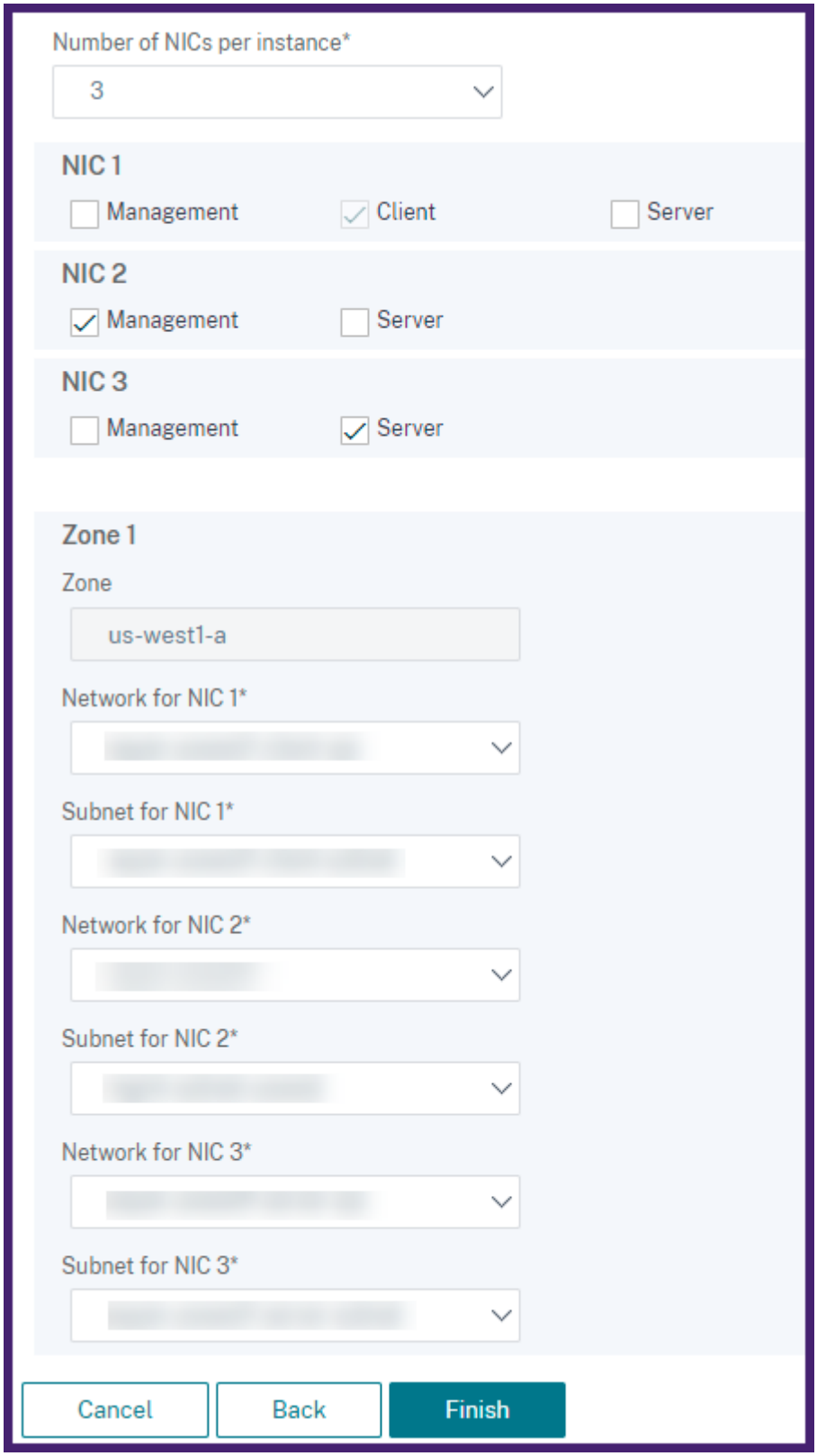
ステップ **4:** プロビジョニングパラメーターの設定

1. 「プロビジョニングパラメータ」タブで、次の項目を指定します。
   - **ADC** サービスアカウント: Google クラウドで作成したサービスアカウントを選択します。ADM は、サービスアカウントを使用して Google クラウドリソースにアクセスします。
   - 製品**/**ライセンス： プロビジョニングする Citrix ADC 製品のバージョンを選択します。詳細については、「Google Cloud で Citrix ADC VPX ライセンスを購読する」を参照してください。
   - マシンタイプ: リストから必要なマシンタイプを選択します。
   - イメージ： 必要な Citrix ADC バージョンイメージを選択します。[新規追加] をクリックして、Citrix ADC イメージを追加します。
   - 「構成テンプレート」— ADC インスタンスへのデプロイに使用する設定テンプレートを選択します。
   - [インスタンスごとのサーバーサブネット内の **IP**] — サーバーサブネット内に各インスタンスが持つことができる SNIP アドレスの数を指定します。



このタブでは、必要な NIC を指定および構成することもできます。各 NIC には、専用のファイアウォールとサブネットが含まれています。

詳しくは、「VPC ネットワークを作成する」および「ファイアウォールの作成」を参照してください。



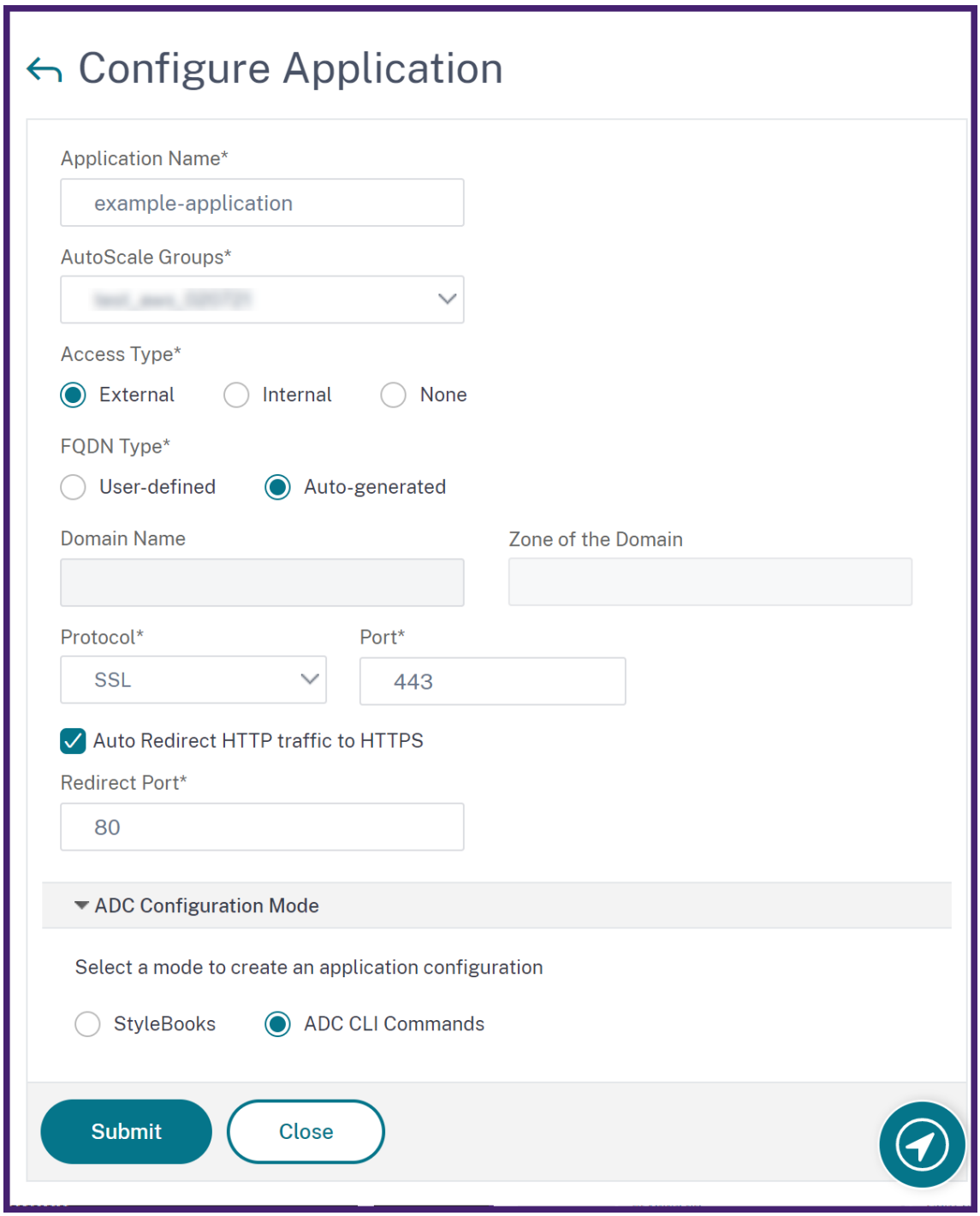
2. ［完了］をクリックします。

手順 **5: Autoscale** グループのアプリケーションを構成する

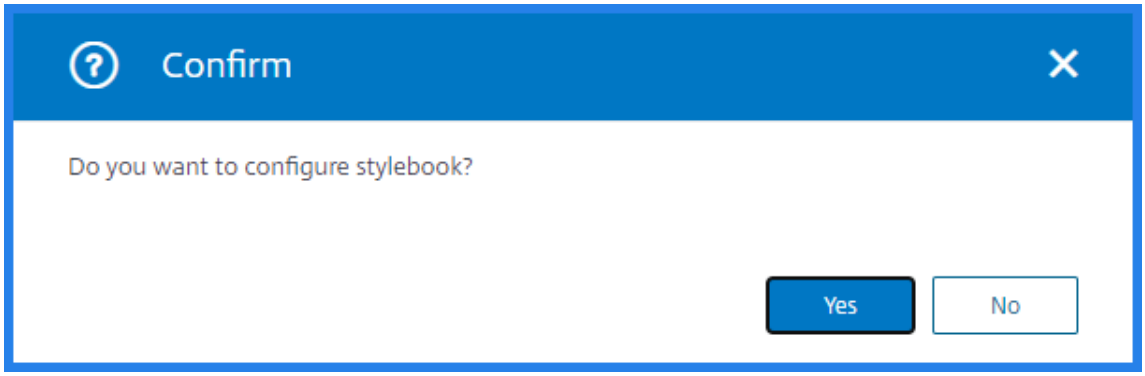
1. Citrix ADM で、［ネットワーク］>［**AutoScale** グループ］に移動します。
2. 作成した Autoscale グループを選択し、[設定] をクリックします。
3.「アプリケーションの構成」で、次の詳細を指定します。
    - アプリケーション名 -アプリケーションの名前を指定します。
    - アクセスタイプ -ADM Auto Scaling ソリューションは外部アプリケーションと内部アプリケーションの両方に使用できます。必要なアプリケーションアクセスタイプを選択します。
    - **FQDN** タイプ -ドメイン名とゾーン名を割り当てるモードを選択します。

      手動で指定する場合は、[ユーザー定義] を選択します。ドメイン名とゾーン名を自動的に割り当てるには、[自動生成] を選択します。
    - ドメイン名 -アプリケーションのドメイン名を指定します。このオプションは、[ユーザー定義 FQDN タイプ] を選択した場合にのみ適用されます。
    - **[** ドメインのゾーン]: リストからアプリケーションのゾーン名を選択します。このオプションは、[ユーザー定義 FQDN タイプ] を選択した場合にのみ適用されます。

      このドメインとゾーン名は、Google Cloud の仮想サーバーにリダイレクトされます。たとえば、`app.example.com`でアプリケーションをホストする場合、`app`はドメイン名、`example.com`はゾーン名です。
    - **Protocol**： リストからプロトコルタイプを選択します。設定されたアプリケーションは、選択したプロトコルタイプに応じてトラフィックを受信します。
    - [ポート]: ポート値を指定します。指定されたポートは、アプリケーションと Autosale グループ間の通信を確立するために使用されます。

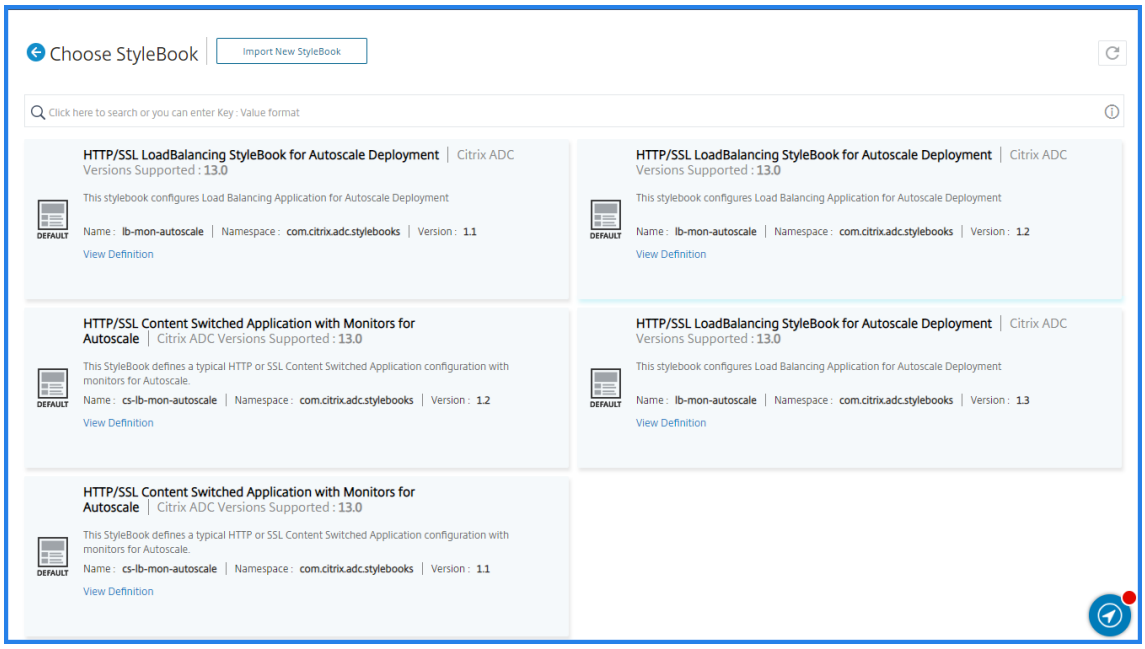


StyleBooks を使用してアプリケーションを構成する場合は、確認ウィンドウで [はい] を選択します。



> メモ今後次の詳細を変更する場合は
>
> 、アプリケーションのアクセスタイプを変更します。
>
> - FQDN タイプ
> - ドメイン名
> - ドメインのゾーン

4. 選択した Autoscale グループの構成を展開する必要な StyleBook を選択します。



StyleBook をインポートする場合は、「新しい **StyleBook** をインポート」をクリックします。

5. すべてのパラメータの値を指定します。

   構成パラメータは、選択した StyleBook にあらかじめ定義されています。

6. [アプリケーションサーバーグループタイプ **CLOUD**] チェックボックスをオンにして、仮想マシンのスケールセットで使用可能なアプリケーションサーバーを指定します。

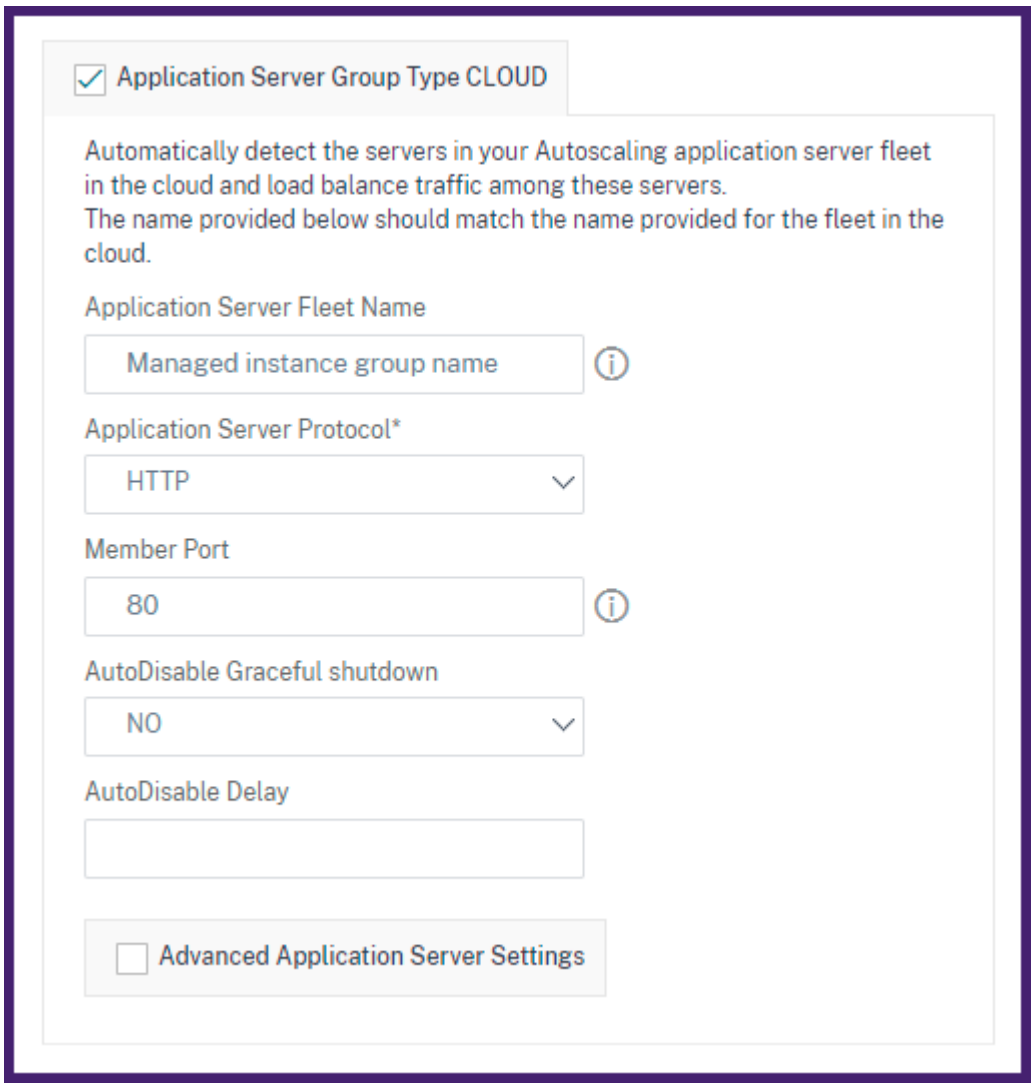
   a) [アプリケーションサーバーフリート名] で、仮想マシンのスケールセットの **AutoScale** 設定名を指定します。

b) リストから アプリケーションサーバープロトコルを選択します。

c)「メンバー・ポート」で、アプリケーション・サーバーのポート値を指定します。

> 注:
>
> ［自動無効グレースフルシャットダウン］が［いいえ］に設定され、［**AutoDisable** 遅延］フィールドが空白になっていることを確認してください。

d) アプリケーションサーバーの詳細設定を指定する場合は、「アプリケーションサーバー の詳細設定」チェックボックスをオンにします。次に、[アプリケーションサーバーの詳細設定] に表示されている必要な値を指定します。

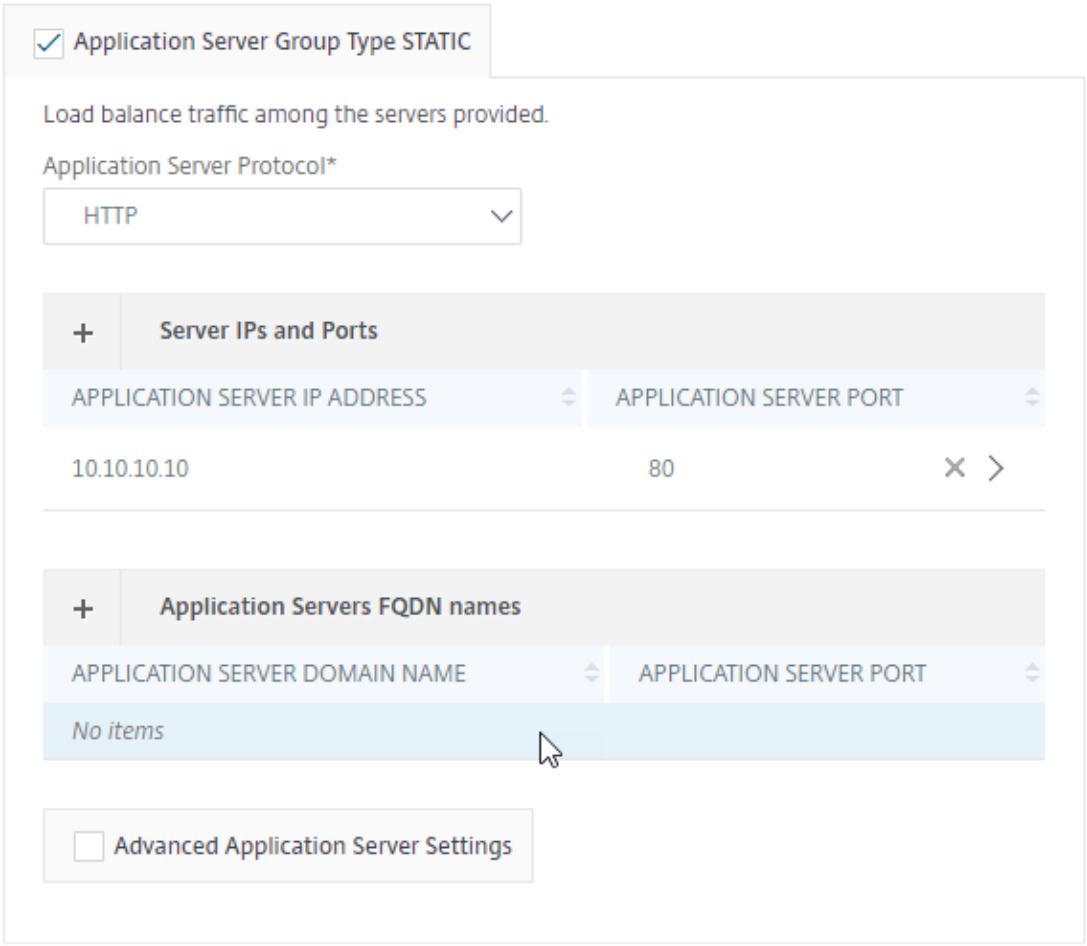


7. 仮想ネットワークにスタンドアロンのアプリケーションサーバーがある場合は、「アプリケーションサーバーグループタイプ **STATIC** 」チェックボックスをオンにします。

a) リストから アプリケーションサーバープロトコルを選択します。

b)「サーバーの **IP** とポート」で、「**+** 」をクリックしてアプリケーションサーバーの IP アドレス、ポート、

および重みを追加し、「作成」をクリックします。



8. ［作成］をクリックします。

Autoscale グループ構成の変更

Autoscale グループ構成を変更したり、Autoscale グループを削除したりできます。変更できるのは、次の Autoscale グループパラメータのみです。

- しきい値パラメータの最大値と最小値
- 最小および最大インスタンス値
- 排水接続期間の値
- クールダウン期間の値
- ウォッチの継続時間の値

Autoscale グループは、作成後に削除することもできます。

Autoscale グループを削除すると、すべてのドメインと IP アドレスが DNS から登録解除され、クラスターノードのプロビジョニングが解除されます。

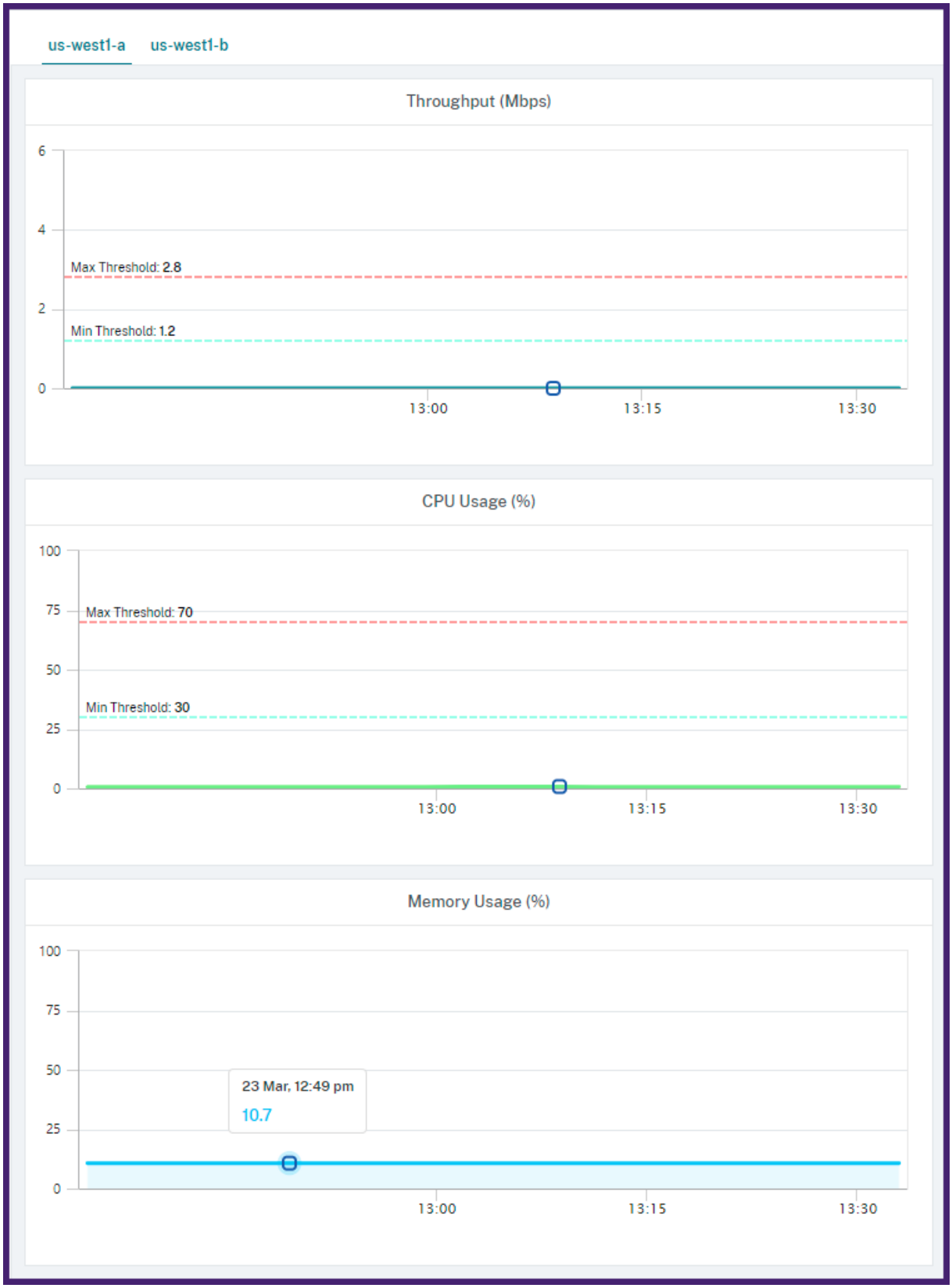
ダッシュボード

May 7, 2021

選択したモニタリングパラメータのグラフを表示できます。右側のパネルには、自動スケーリングをトリガーするイベントが表示されます。左側のパネルには、ゾーンごとのクラスタ内のアクティブなノード、アクティブなノードのグラフ、およびイベントが表示されます。

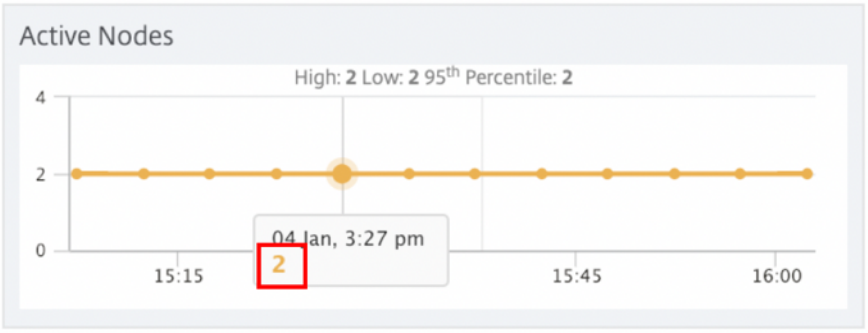
1. Citrix ADM で、［ネットワーク］**>**［グループの **Autoscale**］に移動します。
2. [Autoscale] グループを選択し、[ダッシュボード] をクリックします。

次の図に、ダッシュボードの例を示します。



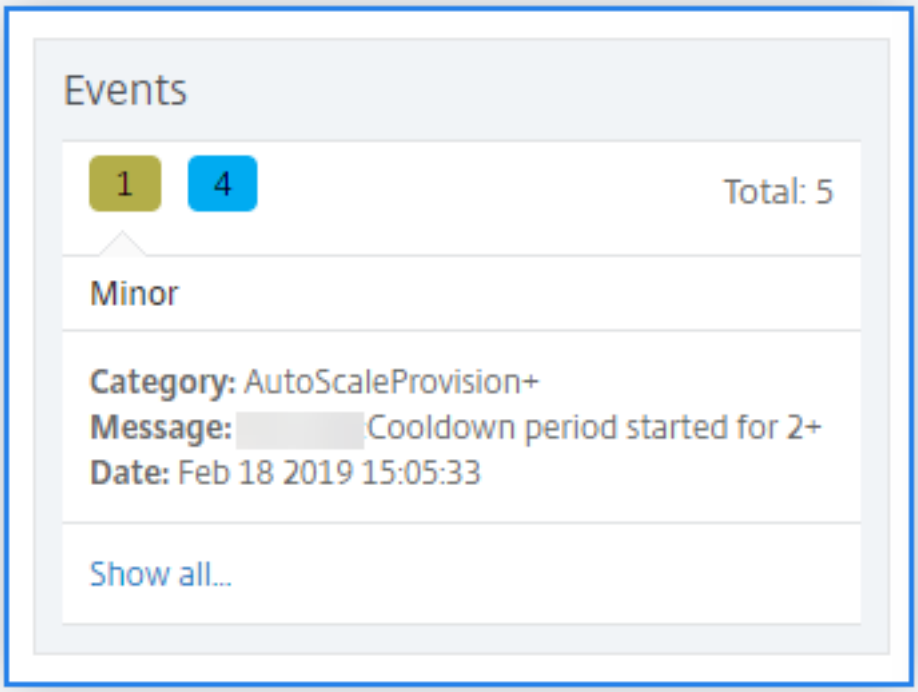
次の図は、アクティブなノードのグラフを示しています。タイムスタンプの下の数字は、アクティブノードの数を示

します。ゾーンの一部であるアクティブノードの数は、いつでも表示できます。

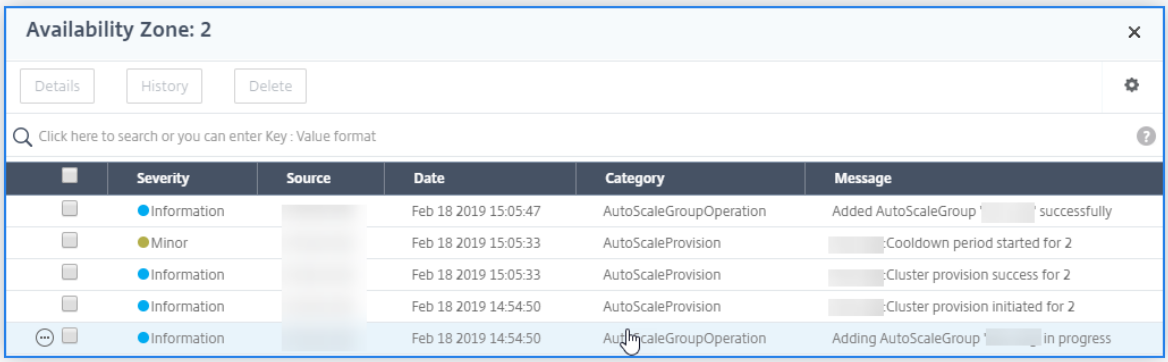


イベント

ダッシュボードの [イベント] タブには、選択した Autoscale グループのイベントの合計数が表示されます。また、最新のイベントの簡単なメッセージも表示されます。



イベントの詳細を表示するには、[すべて表示] をクリックします。



ハイブリッドおよびマルチクラウド環境向けの **Citrix ADC** グローバル負荷分散

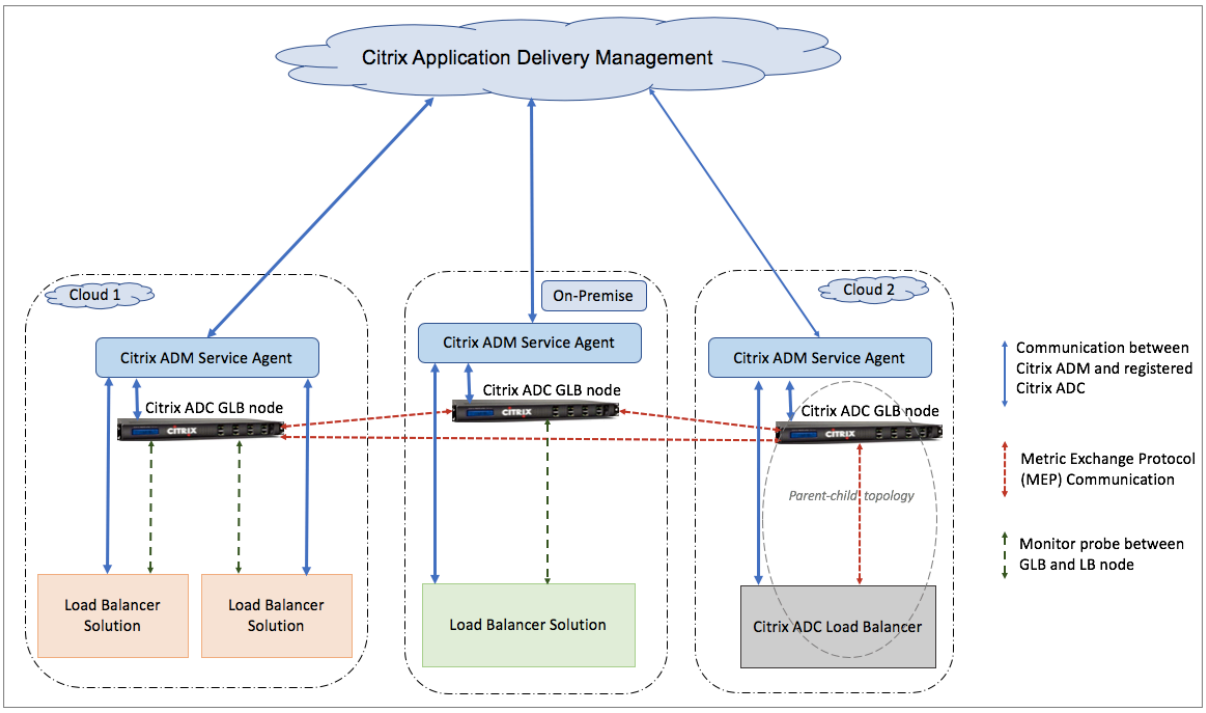
May 7, 2021

Citrix ADC ハイブリッドおよびマルチクラウドグローバル負荷分散（GLB）ソリューションを使用すると、ハイブリッドクラウド、複数のクラウド、オンプレミス展開の複数のデータセンターにアプリケーショントラフィックを分散できます。Citrix ADC ハイブリッドおよびマルチクラウド GLB ソリューションは、既存のセットアップを変更することなく、ハイブリッドまたはマルチクラウドの負荷分散設定を管理するのに役立ちます。また、オンプレミスのセットアップがある場合は、クラウドに完全に移行する前に、Citrix ADC ハイブリッドおよびマルチクラウド GLB ソリューションを使用して、クラウド内のサービスの一部をテストできます。たとえば、トラフィックのごく一部だけをクラウドにルーティングし、ほとんどのトラフィックをオンプレミスで処理できます。また、Citrix ADC ハイブリッドおよびマルチクラウド GLB ソリューションでは、単一の統合コンソールから、地理的な場所にまたがる Citrix ADC インスタンスを管理および監視できます。

ハイブリッドおよびマルチクラウドアーキテクチャは、「ベンダーロックイン」を回避し、パートナーと顧客のニーズを満たすために異なるインフラストラクチャを使用することによって、エンタープライズ全体のパフォーマンスを改善することもできます。複数のクラウドアーキテクチャを使用すると、使用した分だけ支払う必要があるため、インフラストラクチャのコストをより効率的に管理できます。また、インフラストラクチャをオンデマンドで使用できるため、アプリケーションの拡張性も向上します。また、クラウド間ですばやく切り替えて、各プロバイダーの最高のサービスを活用することもできます。

Citrix ADC ハイブリッドおよびマルチクラウド **GLB** ソリューションのアーキテクチャ

次の図は、Citrix ADC ハイブリッドおよびマルチクラウド GLB 機能のアーキテクチャを示しています。



Citrix ADC GLB ノードは、DNS の名前解決を処理します。これらの GLB ノードのいずれも、クライアントの場所から DNS 要求を受信できます。DNS 要求を受信する GLB ノードは、設定された負荷分散方式によって選択されたロードバランサーの仮想サーバーの IP アドレスを返します。メトリック（サイト、ネットワーク、および永続性メトリック）は、独自の Citrix プロトコルであるメトリック交換プロトコル（MEP）を使用して GLB ノード間で交換されます。MEP プロトコルの詳細については、「メトリック交換プロトコルの構成」を参照してください。

GLB ノードで構成されたモニターは、同じデータセンター内の負荷分散仮想サーバーのヘルスステータスを監視します。親子トポロジでは、GLB ノードと Citrix ADC ノード間のメトリックは MEP を使用して交換されます。ただし、GLB ノードと Citrix ADC LB ノード間のモニタープローブの構成は、親子トポロジではオプションです。

Citrix Application Delivery Management（ADM）サービスエージェントは、Citrix 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します。Citrix ADM サービスエージェントとそのインストール方法の詳細については、「はじめに」を参照してください。

> 注 このドキュメントでは、次の前提条件を示します。

- 既存の負荷分散設定がある場合は、起動して実行されています。
- SNIP アドレスまたは GLB サイトの IP アドレスは、Citrix ADC GLB ノードごとに構成されます。この IP アドレスは、他のデータセンターとメトリックスを交換するときに、データセンターのソース IP アドレスとして使用されます。
- ADNS または ADNS-TCP サービスは、各 Citrix ADC GLB インスタンス上で構成され、DNS トラフィックを受信します。
- 必要なファイアウォールとセキュリティグループは、クラウドサービスプロバイダーで設定されます。

> セキュリティグループの設定
>
> クラウドサービスプロバイダーで、必要なファイアウォール/セキュリティグループの構成を設定する必要があります。AWS セキュリティ機能の詳細については、「AWS ドキュメント」を参照してください。Microsoft Azure ネットワークセキュリティグループの詳細については、Microsoft Azure ドキュメントを参照してください。
>
> さらに、GLB ノードでは、MEP トラフィック交換用に ADNS サービス/DNS サーバーの IP アドレスのポート 53、GSLB サイト IP アドレスのポート 3009 を開く必要があります。負荷分散ノードで、アプリケーショントラフィックを受信するための適切なポートを開く必要があります。たとえば、HTTP トラフィックを受信するためにポート 80 を開き、HTTPS トラフィックを受信するためにポート 443 を開く必要があります。Citrix ADM サービスエージェントと Citrix ADM 間の NITRO 通信用にポート 443 を開きます。
>
> ダイナミックラウンドトリップ時間 GLB 方式の場合、設定されている LDNS プローブタイプに応じて UDP プローブと TCP プローブを許可するようにポート 53 を開く必要があります。UDP または TCP プローブは、SNIP の 1 つを使用して開始されるため、この設定は、サーバー側のサブネットにバインドされたセキュリティグループに対して実行する必要があります。

Citrix ADC ハイブリッドおよびマルチクラウド **GLB** ソリューションの機能

このセクションでは、Citrix ADC ハイブリッドおよびマルチクラウド GLB ソリューションの機能の一部について説明します。

他の負荷分散ソリューションとの互換性

Citrix ADC ハイブリッドおよびマルチクラウド GLB ソリューションは、Citrix ADC ロードバランサ、Nginx、HAProxy、およびその他のサードパーティロードバランサーなど、さまざまな負荷分散ソリューションをサポートします。

> 注:
>
> Citrix ADC 以外の負荷分散ソリューションは、近接ベースおよび非メトリックベースの GLB 方式が使用され、親子トポロジが構成されていない場合にのみサポートされます。

GLB メソッド

Citrix ADC ハイブリッドおよびマルチクラウド GLB ソリューションは、次の GLB 方式をサポートしています。

- メトリックベースの GLB メソッド。メトリックベースの GLB メソッドは、メトリック交換プロトコルを介して他の Citrix ADC ノードからメトリックを収集します。
  - 最小接続: クライアント要求は、アクティブな接続数が最も少ないロードバランサーにルーティングされます。
  - 最小帯域幅: クライアント要求は、現在最も少ない量のトラフィックを処理しているロードバランサーにルーティングされます。

  - [最小パケット]: クライアント要求は、過去 14 秒間で最も少ないパケットを受信したロードバランサーにルーティングされます。
- 非メトリックベースの GLB メソッド
  - ラウンドロビン: クライアントリクエストは、ロードバランサーのリストの上部にあるロードバランサーの IP アドレスにルーティングされます。その後、そのロードバランサーはリストの一番下に移動します。
  - ソース IP ハッシュ: このメソッドは、クライアント IP アドレスのハッシュ値を使用してロードバランサーを選択します。
- 近接ベースの GLB メソッド
  - 静的近接: クライアントリクエストは、クライアント IP アドレスに最も近いロードバランサーにルーティングされます。
  - ラウンドトリップ時間 (RTT): この方法では、RTT 値 (クライアントのローカル DNS サーバーとデータセンター間の接続の遅延時間) を使用して、最もパフォーマンスの高いロードバランサーの IP アドレスを選択します。

ロードバランシング方式の詳細については、「負荷分散アルゴリズム」を参照してください。

GLB トポロジ

Citrix ADC ハイブリッドおよびマルチクラウド GLB ソリューションは、アクティブ/パッシブトポロジと親子トポロジをサポートします。

- アクティブ/パッシブトポロジ：障害点からの保護により、災害復旧を実現し、アプリケーションの継続的な可用性を確保します。プライマリデータセンターがダウンすると、パッシブデータセンターは運用可能になります。GSLB アクティブ/パッシブトポロジの詳細については、災害復旧のための GSLB の設定を参照してください。
- 親子トポロジ：メトリックベースの GLB メソッドを使用して GLB ノードと LB ノードを構成し、LB ノードが別の Citrix ADC インスタンスに展開されている場合に使用できます。親子トポロジでは、LB ノード（子サイト）は Citrix ADC アプライアンスである必要があります。親サイトと子サイト間のメトリックの交換はメトリック交換プロトコル（MEP）を介して行われます。

親子トポロジの詳細については、MEP プロトコルを使用した親子トポロジの配置を参照してください。

IPv6 サポート

Citrix ADC ハイブリッドおよびマルチクラウド GLB ソリューションは、IPv6 もサポートしています。

監視

Citrix ADC ハイブリッドおよびマルチクラウド GLB ソリューションは、セキュリティで保護された接続を有効にするオプション付きの組み込みモニターをサポートします。ただし、LB 構成と GLB 構成が同じ Citrix ADC インスタンス上にある場合、または親子トポロジを使用する場合は、モニターの構成はオプションです。

永続性

Citrix ADC ハイブリッドおよびマルチクラウド GLB ソリューションでは、次の機能がサポートされています。

- ソース IP ベースの永続性セッション。これにより、設定されたタイムアウトウィンドウ内に到達した場合に、同じクライアントからの複数の要求が同じサービスに送信されます。クライアントが別の要求を送信する前にタイムアウト値が期限切れになると、セッションは破棄され、構成された負荷分散アルゴリズムを使用して、クライアントの次の要求のための新しいサーバーが選択されます。
- スピルオーバーパーシステンス。プライマリへの負荷がしきい値を下回った後も、バックアップ仮想サーバは受信した要求を処理し続けます。詳しくは、「スピルオーバーの設定」を参照してください。
- サイト永続性。GLB ノードは、クライアント要求を処理するデータセンターを選択し、その後のすべての DNS 要求に対して、選択したデータセンターの IP アドレスを転送するようにします。構成された永続性が DOWN のサイトに適用される場合、GLB ノードは GLB メソッドを使用して新しいサイトを選択し、新しいサイトは、クライアントからの後続の要求に対して永続的になります。

Citrix ADM スタイルブックを使用した構成

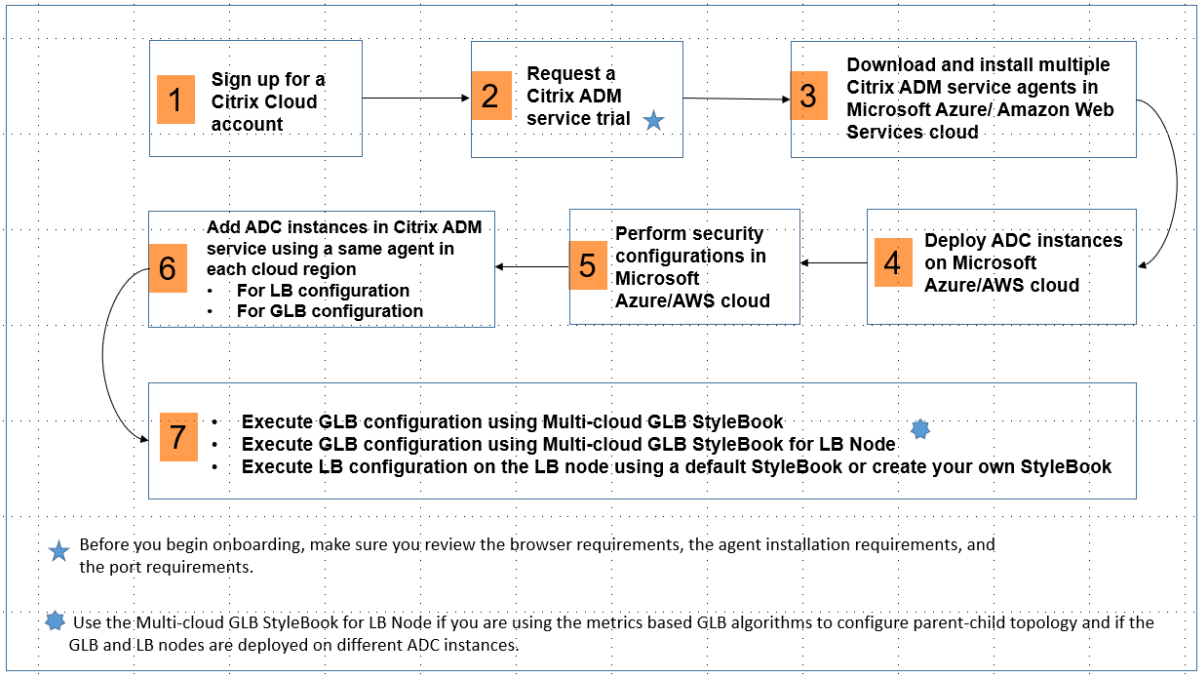
Citrix ADM でデフォルトのマルチクラウド GLB StyleBook を使用して、Citrix ADC インスタンスをハイブリッドおよびマルチクラウド GLB 構成で構成できます。

デフォルトのマルチクラウド GLB StyleBook for LB Node StyleBook を使用して、アプリケーショントラフィックを処理する親子トポロジの子サイトである Citrix ADC 負荷分散ノードを構成できます。この StyleBook は、親子トポロジの場合に LB ノードを設定する場合のみ使用してください。ただし、各 LB ノードは、この StyleBook を使用して個別に設定する必要があります。

Citrix ADC ハイブリッドおよびマルチクラウド **GLB** ソリューション構成のワークフロー

Citrix ADM で出荷されたマルチクラウド GLB StyleBook を使用して、Citrix ADC インスタンスをハイブリッドおよびマルチクラウド GLB 構成で構成できます。

次の図は、Citrix ADC ハイブリッドおよびマルチクラウド GLB ソリューションを構成するためのワークフローを示しています。ワークフロー図の手順については、図の後で詳しく説明します。



クラウド管理者として次のタスクを実行します。

1. Citrix Cloud アカウントにサインアップします。

   Citrix ADM の使用を開始するには、Citrix Cloud の会社アカウントを作成するか、社内のユーザーが作成した既存のアカウントに参加します。

2. Citrix Cloud にログオンしたら、［**Citrix** アプリケーション配信の管理］タイルの［管理］をクリックして、ADM サービスを初めてセットアップします。

3. 複数の Citrix ADM サービスエージェントをダウンロードしてインストールします。

   Citrix ADM サービスエージェントをネットワーク環境にインストールして構成し、データセンターまたはクラウド内の Citrix ADM と管理インスタンス間の通信を有効にする必要があります。各リージョンにエージェントをインストールすると、管理対象インスタンスで LB および GLB 構成を構成できます。LB および GLB 設定は、1 つのエージェントを共有できます。上記の 3 つのタスクの詳細については、「はじめに」を参照してください。

4. Microsoft Azure/AWS クラウド/オンプレミスのデータセンターにロードバランサーをデプロイします。

   クラウドとオンプレミスにデプロイするロードバランサーの種類に応じて、それに応じてプロビジョニングします。たとえば、Microsoft Azure Resource Manager（ARM）ポータル、Amazon Web Services（AWS）仮想プライベートクラウド、オンプレミスのデータセンターで Citrix ADC VPX インスタンスをプロビジョニングできます。仮想マシンを作成し、他のリソースを構成して、スタンドアロンモードで LB または GLB ノードとして機能するように Citrix ADC インスタンスを構成します。Citrix ADC VPX インスタンスを展開する方法の詳細については、次のドキュメントを参照してください。

   - AWS AMI 用の Citrix ADC VPX の起動。

- Azure Resource Manager でスタンドアロンモードで Citrix ADC VPX を構成する。

5. セキュリティ設定を実行します。

   ARM または AWS でネットワークセキュリティグループとネットワーク ACL を設定して、インスタンスとサブネットのインバウンドトラフィックとアウトバウンドトラフィックを制御します。

6. Citrix ADM に Citrix ADC インスタンスを追加します。

   Citrix ADC インスタンスは、Citrix ADM から検出、管理、監視するネットワークアプライアンスまたは仮想アプライアンスです。これらのインスタンスを管理および監視するには、サービスにインスタンスを追加し、LB（LB 用の Citrix ADC を使用している場合）と GLB インスタンスの両方を登録する必要があります。Citrix ADCitrix ADM で Citrix ADC インスタンスを追加する方法の詳細については、「はじめに」を参照してください。

7. デフォルトの Citrix ADM StyleBooks を使用して、GLB および LB 構成を実装します。

   - マルチクラウド **GLB StyleBook** を使用して、選択した GLB Citrix ADC インスタンスで GLB 構成を実行します。
   - ロードバランシング設定を実装します。（マネージドインスタンスで既に LB 設定がある場合は、この手順を省略できます）。

   Citrix ADC インスタンスでロードバランサーを構成するには、次の 2 つの方法のいずれかを使用します。

   - アプリケーションの負荷分散のためにインスタンスを手動で設定します。インスタンスを手動で設定する方法の詳細については、「基本的な負荷分散のセットアップ」を参照してください。
   - StyleBooks を使用してください。Citrix ADM StyleBooks（HTTPS/SSL 負荷分散 StyleBook または HTTPS/SSL 負荷分散（モニター付き）StyleBook）のいずれかを使用して、選択した Citrix ADC インスタンスでロードバランサー構成を作成できます。独自の StyleBook を作成することもできます。StyleBook の詳細については、「StyleBook」を参照してください。

8. 次のいずれかの場合に **GLB** 親子トポロジを設定するには、**LB** ノード用のマルチクラウド **GLB StyleBook** を使用します。

   - メトリックベースの GLB アルゴリズム（最小パケット、最小接続、最小帯域幅）を使用して GLB ノードと LB ノードを構成し、LB ノードが別の Citrix ADC インスタンスに展開されている場合。
   - サイトの永続性が必要な場合。

StyleBooks を使用して GLB を構成する

May 7, 2021

マルチクラウド GLB StyleBook を使用して、データセンターでプロビジョニングされる Citrix ADC インスタンスで GLB 構成を構成できます。各データセンターの Citrix ADC GLB インスタンスでサイトの IP アドレスが構成されていることを確認します。

この StyleBook を使用して、後から GLB ノードに追加できる子サイトを受け入れる親サイトを作成することもできます。Citrix ADC インスタンスでマルチクラウド GLB 構成を構成するには

1. [アプリケーション] > [構成] に移動し、[新規作成] をクリックします。
2. [**StyleBook** の選択] ページには、Citrix Application Delivery Management（ADM）で使用できるすべての StyleBook が表示されます。下にスクロールし、[マルチクラウド **GLB StyleBook**] を選択します。

   マルチクラウド GLB StyleBook は、複数のクラウドおよびオンプレミスサイトにデプロイされるアプリケーションの GLB を構成するために使用されます。StyleBook は、この StyleBook で定義されているすべてのパラメータの値を入力できるユーザーインターフェイスページとして表示されます。

   > 注:
   >
   > このドキュメントでは、データセンターとサイトという用語は同じ意味で使用されます。

3. 次のパラメーターを設定します。

   - アプリケーション名。GLB サイトにデプロイされたアプリケーションの名前を入力します。
   - **GLB** アルゴリズム。クライアントにサービスを提供するサイトを選択するためのグローバル負荷分散アルゴリズム（方法）を選択します。ドロップダウンリストボックスで使用できるオプションは、LEASTCONNECTION、LEASTBANDWIDTH、LEASTPACKETS、ROUNDROBIN、STATICPROXIMITY、SOURCEIPHASH、RTT です。
   - 地理データベースファイル GLB アルゴリズムとして STATICPROXIMITY を選択した場合は、静的近接データを含むデータベースファイルの完全パスと名前を入力します。データベースファイルが、指定した場所にあるすべての GLB Citrix ADC インスタンスに存在することを確認します。または、デフォルトのファイルを保持することもできます。
   - プロトコル。ドロップダウンリストボックスから、デプロイされたアプリケーションのアプリケーションプロトコルを選択します。
   - 永続性の設定。仮想サーバーで構成された永続性は、その仮想サーバーで表されるサーバー上の接続の状態を維持します (たとえば、e コマースで使用される接続)。仮想サーバーが選択されると、永続性は負荷分散方式よりも優先されます。持続性構成が DOWN のサービスに適用されている場合、インスタンスは負荷分散方法を使用して新しいサービスを選択し、新しいサービスはクライアントからの後続の要求に対して永続的になります。
   - 持続性タイプ。このアプリケーションに使用する永続性タイプを選択します。たとえば、永続性を SOURCEIP として選択した場合、アプリケーションをホストしているサイトを最初に選択した後、同じクライアントからの後続のすべての要求がそのサイトに送信され、アプリケーションのサービスにアクセスできるようになります。
   - 持続性タイムアウト。持続性タイプとして SOURCEIP を選択した場合は、最後のクライアント要求の後に永続セッションが期限切れになるまでの分数を入力します。指定できる範囲は 2 ～1440 分です。分は秒単位で解決されます。

4. スピルオーバー設定。たとえば、プライマリ仮想サーバの接続制限または帯域幅制限がしきい値に達した場合に、スピルオーバー接続をセカンダリ仮想サーバまたはバックアップ仮想サーバに転送するように、スピルオーバー機能を設定します。

- スピルオーバー方法。ドロップダウンリストボックスから、スピルオーバーの方法を選択します。たとえば、CONNECTION スピルオーバーメソッドは、プライマリサーバ上でアクティブな接続の数を監視します。この方法のスピルオーバーしきい値に達した場合、新しい接続は、バックアップチェーン内の最初の使用可能な仮想サーバに転送されます。HEALTH スピルオーバー方式では、しきい値が設定されたしきい値を下回った場合にスピルオーバーできます。たとえば、70% 未満です。

  > 注:
  >
  > HELATH スピルオーバー方式を除き、Citrix ADC がロードバランサーインスタンスとして使用されている場合にのみ適用できます。

- スピルオーバーしきい値。選択したスピルオーバー方式のしきい値を入力します。
- スピルオーバーの持続性。プライマリへの負荷がしきい値を下回った後も、バックアップ仮想サーバが受信した要求の処理を続行する場合は、スピルオーバー永続性を有効にします。
- スピルオーバー永続タイムアウト。スピルオーバーパーシステンスを有効にする期間を設定します。最小値は 2 分で、最大値は 1440 分です。分は秒単位で解決されます。

5. 永続/スピルオーバーの永続性 **ID**。持続性タイプとして SOURCEIP を選択した場合、またはスピルオーバー永続性が有効な場合は、すべての GLB アプライアンス上で同じドメインを識別する一意の番号を入力します。指定できる範囲は 1 ～65535 です。

   - **GLB** サービスエンドポイントのヘルスチェック（オプション）
   - ヘルスチェックの種類。ドロップダウンリストボックスから、サイト上のアプリケーションを表すロードバランサー VIP アドレスの正常性のチェックに使用するプローブのタイプを選択します。
   - セキュアモード。（オプション）SSL ベースのヘルスチェックが必要な場合に、このパラメータを有効にするには、[**Yes**] を選択します。
   - **HTTP** リクエスト。（任意）ヘルスチェックタイプとして HTTP を選択した場合は、VIP アドレスのプローブに使用する完全な HTTP 要求を入力します。
   - **HTTP** ステータス応答コードのリスト。（任意）ヘルスチェックタイプとして HTTP を選択した場合は、VIP が正常な場合に HTTP 要求への応答で期待される HTTP ステータスコードのリストを入力します。

6. **GLB** ドメイン名。このセクションでは、このアプリケーションに関連付けられている DNS ドメイン名のリストを構成できます。プラスアイコン（**+**）をクリックして、アプリケーションの DNS ドメイン名を作成します。

7. **GLB** サイト. このセクションでは、このアプリケーションが展開されるサイトのリストを構成できます。

   GLB サイトは、GLB 通信の最上位エンティティです。サイトの構成時に指定した情報は、ローカルサイトをリモートサイトにリンクしたり、Citrix Metrics Exchange プロトコル（MEP）を使用して監視データを共有したりするために使用されます。IP アドレスは、GLB Citrix ADC インスタンスが所有し、TCP ポート 3009 を使用します。StyleBook の GLB サイトセクションでは、必要な数の GLB サイトを指定できます。

   プラスアイコン (**+**) をクリックして、サイトを追加します。

   - サイト名。サイトの名前を入力します。

- サイト **IP** アドレス。他のサイトとメトリックスを交換するときに、サイトが送信元 IP アドレスとして使用する IP アドレスを入力します。この IP アドレスは、各サイトの GLB インスタンスで既に設定されているものとします。
- サイトのパブリック **IP** アドレス。（オプション）メトリックの交換に使用されるサイトのパブリック IP アドレスを入力します（そのサイトの IP アドレスが NAT の場合）。

8. 子サイト。プラスアイコン（+）をクリックして、必要な子サイトを構成します。

   - 子サイト名。サイトの名前を入力します。
   - 子サイトの **IP** アドレス。子サイトの IP アドレスを入力します。ここでは、子サイトとして構成されている Citrix ADC ノードのプライベート IP アドレスまたは SNIP を使用します。
   - サイトのパブリック **IP** アドレス。（オプション）メトリックの交換に使用されるサイトのパブリック IP アドレスを入力します（そのサイトの IP アドレスが NAT の場合）。

9. サービスサイトの永続性。サイト上の GLB サービスに使用する永続性のタイプをドロップダウンリストボックスから選択します。

   - [ConnectionProxy] を選択すると、サイト Cookie を挿入した GLB サイトへの接続を作成し、クライアント要求を元のサイトにプロキシし、元の GLB サイトから応答を受信し、応答をクライアントにリレーし、接続を閉じることができます。
   - Cookie を最初に挿入したサイトにリクエストをリダイレクトできるようにするときに`HTTPRedirect`を選択します。永続性の詳細については、「持続的接続の構成」を参照してください。

10. アクティブ **GLB** サービス: このセクションでは、アプリケーションがデプロイされているサイト上のアクティブなサービスのリストを構成できます。

    サービス **IP**。このサイトの GLB サービスの IP アドレスを入力します。

    - サービスのパブリック **IP** アドレス。仮想 IP アドレスがプライベートで、パブリック IP アドレスが NAT になっている場合は、パブリック IP アドレスを指定します。
    - サービスポート。このサイトの GLB サービスのポートを入力します。
    - サービス重量。GLB サービスに割り当てられている重みを入力します。

      > 注:
      >
      > クラウドに送信する必要があるトラフィックの割合、およびオンプレミスで処理する必要があるトラフィックの割合に応じて、サービスに相対的な重みを割り当てることができます。たとえば、クラウドベースの GLB サービスに 3 の重み、オンプレミス GLB サービスに 7 を割り当てた場合、トラフィックの 30% はクラウドに送信され、70% がオンプレミスで処理されます。

    - サイト名。GLB サービスがあるサイトの名前を入力します。
    - サイトプレフィックス。GLB サービスが設定されているサイトのプレフィクスを入力します。これは、サイト永続性が有効で、メソッドが`httpredirect`である場合に適用されます。サイトプレフィクス値は、アプリケーションのすべての GLB サービスで一意である必要があります。

- 最大クライアント接続数。スピルオーバー 持続性設定でスピルオーバー方法として DYNAMIC-CONNECTION を選択した場合は、GLB サービスで設定されている最大クライアント接続数を入力します。値を指定しない場合、デフォルトでは、システムによって構成可能な最大クライアント接続に番号が割り当てられます。

11. パッシブ **GLB** サービス: このセクションでは、アクティブ/パッシブトポロジを使用してアプリケーションが展開されているサイトでパッシブサービスのリストを構成できます。アクティブな GLB サービスに提供した情報と同様に、すべてのバックアップ GLB サービスの情報を入力します。
12. ［ターゲットインスタンス］をクリックし、GLB 構成を展開する各サイトで GLB インスタンスとして構成された Citrix ADC インスタンスを選択します。
13. ［作成］をクリックして、選択した Citrix ADC インスタンスで GLB 構成を作成します。「ドライラン」**(Dry Run**) をクリックして、ターゲットインスタンスに作成されるオブジェクトをチェックすることもできます。作成した StyleBook 構成（設定パック）が、［構成］ページの構成のリストに表示されます。Citrix ADM GUI を使用して、この構成（構成パック）を確認、更新、または削除できます。

StyleBooks を使用して **Citrix ADC LB** ノードで **GLB** を構成する

May 7, 2021

メトリックベースの **GLB** アルゴリズム（最小パケット、最小接続、最小帯域幅）を使用して **GLB** ノードと **LB** ノードを構成し、**LB** ノードが別の **Citrix ADC** インスタンスに展開されている場合は、マルチクラウド **GLB StyleBook for** LB ノードを使用できます。

この StyleBook を使用して、既存の親サイトに追加の子サイトを構成することもできます。この StyleBook は、一度に 1 つの子サイトを構成します。したがって、この StyleBook から子サイトと同じ数の構成（設定パック）を作成します。StyleBook は、子サイトに GLB 設定を適用します。最大 1024 の子サイトを構成できます。

> 注
>
> 親サイトを構成する場合にマルチクラウド GLB StyleBookを使用します。

この StyleBook では、次の前提条件があります。

- SNIP アドレスまたは GLB サイトの IP アドレスが構成されています。
- 必要なファイアウォールとセキュリティグループは、クラウドサービスプロバイダーで設定されます。

LB ノード用のマルチクラウド **GLB StyleBook** を使用した親子トポロジでの子サイトの構成

1. [アプリケーション] > [構成] に移動し、[新規作成] をクリックします。
2. ［**StyleBook** の選択］ページには、Citrix Application Delivery Management（ADM）で使用できるすべての StyleBook が表示されます。下にスクロールし、[マルチクラウド **GLB StyleBook] [LB** ノード**]** を選択します。

StyleBook は、この StyleBook で定義されているすべてのパラメータの値を入力できるユーザーインターフェイスページとして表示されます。

> 注:
>
> このドキュメントでは、データセンターとサイトという用語は同じ意味で使用されます。

3. 次のパラメーターを設定します。

   - アプリケーション名。子サイトを作成する GLB サイトにデプロイされた GLB アプリケーションの名前を入力します。
   - プロトコル。ドロップダウンリストボックスから、デプロイされたアプリケーションのアプリケーションプロトコルを選択します。
   - **LB** ヘルスチェック（オプション）
     - ヘルスチェックの種類。ドロップダウンリストボックスから、サイト上のアプリケーションを表すロードバランサー VIP アドレスの正常性のチェックに使用するプローブのタイプを選択します。
     - セキュアモード。（オプション）SSL ベースのヘルスチェックが必要な場合に、このパラメータを有効にするには、[**Yes**] を選択します。
     - **HTTP** リクエスト。（任意）ヘルスチェックタイプとして HTTP を選択した場合は、VIP アドレスのプローブに使用する完全な HTTP 要求を入力します。
     - **HTTP** ステータス応答コードのリスト。（任意）ヘルスチェックタイプとして HTTP を選択した場合は、VIP が正常な場合に HTTP 要求への応答で期待される HTTP ステータスコードのリストを入力します。

4. 親サイトを構成しています。

   子サイト (LB ノード) を作成する親サイト (GLB ノード) の詳細を指定します。

   - サイト名。親サイトの名前を入力します。
   - サイト **IP** アドレス。他のサイトとメトリックスを交換するときに、親サイトが SourceIP アドレスとして使用する IP アドレスを入力します。この IP アドレスは、各サイトの GLB ノードですでに構成されているものとします。
   - サイトのパブリック **IP** アドレス。（オプション）メトリックの交換に使用される親サイトのパブリック IP アドレスを入力します（そのサイトの IP アドレスが NAT の場合）。

5. 子サイトを構成しています。

   子サイトの詳細を入力します。

   - サイト名。サイトの名前を入力します。
   - サイト **IP** アドレス。子サイトの IP アドレスを入力します。ここでは、子サイトとして構成されている Citrix ADC ノードのプライベート IP アドレスまたは SNIP を使用します。
   - サイトのパブリック **IP** アドレス。（オプション）メトリックの交換に使用される子サイトのパブリック IP アドレスを入力します（そのサイトの IP アドレスが NAT の場合）。

6. アクティブ GLB サービスの設定（任意）

LB 仮想サーバの IP アドレスがパブリック IP アドレスでない場合に限り、アクティブ GLB サービスを設定します。このセクションでは、アプリケーションがデプロイされているサイト上のローカル GLB サービスのリストを構成できます。

- サービス **IP**。このサイトの負荷分散仮想サーバーの IP アドレスを入力します。
- サービスのパブリック **IP** アドレス。仮想 IP アドレスがプライベートで、パブリック IP アドレスが NAT になっている場合は、パブリック IP アドレスを指定します。
- サービスポート。このサイトの GLB サービスのポートを入力します。
- サイト名。GLB サービスがあるサイトの名前を入力します。

7. ［ターゲットインスタンス］をクリックし、GLB 構成を展開する各サイトで GLB インスタンスとして構成された Citrix ADC インスタンスを選択します。
8. ［作成］をクリックして、選択した Citrix ADC インスタンス（LB ノード）に LB 構成を作成します。「ドライラン」**(Dry Run**) をクリックして、ターゲットインスタンスに作成されるオブジェクトをチェックすることもできます。作成した StyleBook 構成が、「構成」ページの構成のリストに表示されます。Citrix ADM GUI を使用して、この構成を確認、更新、または削除できます。

インフラストラクチャ分析

May 7, 2021

ネットワーク管理者の主な目標は、Citrix ADC インスタンスを監視することです。ADC インスタンスは、アプリケーションおよびそれを介してアクセスされるデスクトップの使用状況とパフォーマンスに関する興味深い洞察を提供します。管理者は、ADC インスタンスを監視し、各 ADC インスタンスによって処理されるアプリケーションフローを分析する必要があります。また、管理者は、構成、セットアップ、接続、証明書、およびアプリケーションの使用状況やパフォーマンスにおけるその他の影響に関する可能性のある問題を修復できる必要があります。たとえば、アプリケーショントラフィックパターンの急激な変化は、SSL プロトコルの無効化など、SSL 構成の変更が原因である可能性があります。管理者は、次のことを確実にするために、これらのデータ・ポイント間の相関関係を迅速に特定できる必要があります。

- アプリケーションの可用性が最適な状態にある
- リソースの消費、ハードウェア、容量、構成の変更の問題はありません。
- 未使用の在庫はありません
- 期限切れの証明書はありません

インフラストラクチャ分析機能は、複数のデータソースを関連付けて、インスタンスの状態を定義する測定可能なスコアに定量化することで、データ分析のプロセスを簡素化します。この機能を使用すると、管理者はワンタッチポイントで問題、問題の発生源、および実行可能な修復の可能性を把握できます。

Citrix ADM でのインフラストラクチャ分析

インフラストラクチャ分析機能は、Citrix ADC インスタンスから収集されたすべてのデータを照合し、インスタンスの状態を定義するインスタンススコアに数値化します。インスタンススコアは、表形式またはサークルパックの視覚化として要約されます。Infrastructure Analytics 機能は、インスタンスで問題が発生した、または発生する可能性のある要因を視覚化するのに役立ちます。このビジュアライゼーションは、問題とその再発を防ぐために実行する必要があるアクションを決定するのにも役立ちます。

インスタンススコア

インスタンス・スコアは、ADC インスタンスの健全性を示します。スコアが 100 の場合、問題なく完全に健全なインスタンスを意味します。インスタンススコアは、インスタンス上のさまざまなレベルの潜在的な問題をキャプチャします。これは、インスタンスの健全性を定量化可能な測定値であり、複数の「健全性指標」がスコアに寄与します。

ヘルスインジケータは、インスタンススコアの構成要素です。このスコアは、そのタイムウィンドウで検出されたすべてのインジケータに基づいて、定義済みの「モニタリング期間」に対して定期的に計算されます。現在、Infrastructure Analytics は、インスタンスから収集されたデータに基づいて 1 時間に 1 回インスタンスのスコアを計算します。
インジケータは、インスタンスの次のカテゴリのいずれかに属するアクティビティ（イベントまたは問題）として定義できます。

- システムリソースインジケータ
- クリティカルイベントインジケータ
- SSL 設定インジケータ
- 構成偏差インジケータ

健康指標の説明

- システムリソースインジケータ

  以下は、Citrix ADC インスタンスで発生し、Citrix ADM によって監視される重大なシステムリソースの問題です。

  - 高い **CPU** 使用率。CPU 使用率が、Citrix ADC インスタンスのより高いしきい値を超えました。
  - 高いメモリ使用量。メモリ使用量が Citrix ADC インスタンスでより高いしきい値を超えました。
  - 高いディスク使用率。ディスク使用量が Citrix ADC インスタンスでより高いしきい値を超えました。
  - ディスクエラー。ADC インスタンスがインストールされている Hypervisor のハードディスク 0 またはハードディスク 1 にエラーがあります。
  - 電源障害。電源装置が故障したか、ADC インスタンスから切断されました。
  - **SSL** カードの障害。インスタンスにインストールされている SSL カードが失敗しました。

- フラッシュエラー。Citrix ADC インスタンスでコンパクトフラッシュエラーが発生する。
- **NIC** が廃棄されます。NIC カードによって破棄されたパケットが、Citrix ADC インスタンスのより高いしきい値を超えました。

これらのシステムリソースエラーについて詳しくは、「[インスタンスダッシュボード。]」を参照してください。(/en-us/citrix-application-delivery-management-service/networks/instance-management.html#how-to-use-the-instance-dashboard)

- クリティカルイベントインジケータ

  次のクリティカルイベントは、クリティカル重大度が設定された ADM のイベント管理機能の下にあるイベントによって識別されます。

  - **HA** 同期の失敗。セカンダリサーバで、高可用性の ADC インスタンス間の設定の同期が失敗しました。
  - **HA** ハートビートなし。高可用性の ADC インスタンスのペアにあるプライマリサーバが、セカンダリサーバからハートビートを受信していません。
  - **HA** 不良セカンダリステート。高可用性の ADC インスタンスのペアにあるセカンダリサーバが、ダウン、不明、または Stay セカンダリステートです。
  - **HA** バージョンの不一致。高可用性の ADC インスタンスのペアにインストールされている ADC ソフトウェアイメージのバージョンが一致しません。
  - クラスタ同期の失敗。クラスタモードの ADC インスタンス間の設定の同期が失敗しました。
  - クラスタのバージョンが一致しません。クラスタモードで ADC インスタンスにインストールされている ADC ソフトウェアイメージのバージョンが一致しません。
  - クラスタの伝播に失敗しました。クラスター内のすべてのインスタンスへの構成の伝播に失敗しました。

    > 注:
    >
    > 重要な SNMP イベントのリストを表示するには、イベントの重大度を変更します。重大度レベルを変更する方法について詳しくは、「[Citrix ADC インスタンスで発生するイベントの報告された重大度を変更します。]」を参照してください。(/en-us/citrix-application-delivery-management-service/networks/events/how-to-modify-the-reported-severity-of-events.html)

  Citrix ADM イベントについて詳しくは、「[イベント。]」を参照してください。(/en-us/citrix-application-delivery-management-service/networks/events.html)

- SSL 設定インジケータ
  - キーの強度はお勧めしません。SSL 証明書の重要な強度は、Citrix の標準に従っていません
  - 推奨されない発行者。SSL 証明書の発行元は、Citrix では推奨されません。
  - **SSL** 証明書の有効期限が切れました。ADC インスタンスにインストールされている SSL 証明書の有効期限が切れています。

  - **SSL** 証明書の有効期限が切れています。ADC インスタンスにインストールされた SSL 証明書は、今後の 1 週間以内に期限切れになります。
  - 推奨されていないアルゴリズム。ADC インスタンスにインストールされる SSL 証明書の署名アルゴリズムは、Citrix の標準に準拠していません。

SSL 証明書について詳しくは、「[SSL ダッシュボード。]」を参照してください。(/en-us/citrix-application-delivery-management-service/networks/ssl-certificate-dashboard.html)

- 構成偏差インジケータ
  - 設定ドリフトテンプレート。特定のインスタンスで監査する特定の構成を使用して作成した監査テンプレートから、構成にドリフト（保存されていない変更）があります。
  - 設定ドリフトのデフォルト。デフォルト設定ファイルからの設定にドリフト（保存されていない変更）があります。

構成の偏差の詳細と、監査レポートを実行して構成の偏差を確認する方法については、[監査レポートを表示します。]を参照してください。(/en-us/citrix-application-delivery-management-service/networks/configuration-audit/audit-reports.html)

ADC の容量に関する問題の表示

ADC インスタンスが使用可能な容量の大半を消費した場合、クライアントトラフィックの処理中にパケット廃棄が発生することがあります。この問題は、ADC インスタンスのパフォーマンスが低下します。このような ADC の容量に関する問題を理解することで、ADC の性能を安定させるために、プロアクティブにライセンスを割り当てることができます。

ADC の容量に関する問題を確認するには、

1. [ネットワーク**] > [**インフラストラクチャ分析] に移動します。
2. 容量の問題を表示するインスタンスを展開します。

ADM は、ADC インスタンスから 5 分ごとにこれらのイベントをポーリングし、パケットドロップまたはレート制限カウンタが存在する場合は、その増加を表示します。問題は、次のキャパシティパラメータに分類されます。

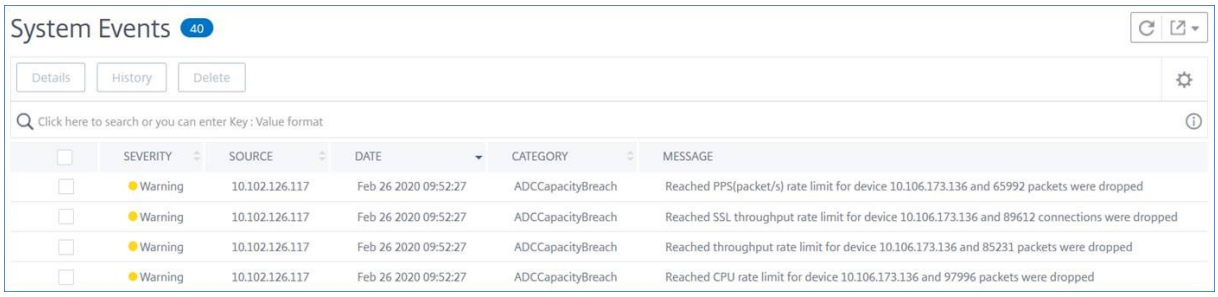
- スループット制限に達しました — スループット制限に達した後、インスタンスでドロップされたパケット数。
- **PE CPU** 制限に達しました -PE CPU 制限に達した後、すべての NIC でドロップされたパケット数。
- **PPS** 制限に達しました — PPS 制限に達した後にインスタンスでドロップされたパケット数。
- **SSL** スループットレート制限 — SSL スループット制限に達した回数。
- **SSL TPS** レート制限 — SSL TPS 制限に達した回数。

ADM は、定義されたキャパシティしきい値に基づいてインスタンススコアを計算します。

- 低しきい値：1 パケットドロップまたはレート制限カウンタ増分
- 高しきい値：10000 パケットのドロップまたはレート制限カウンタ増分

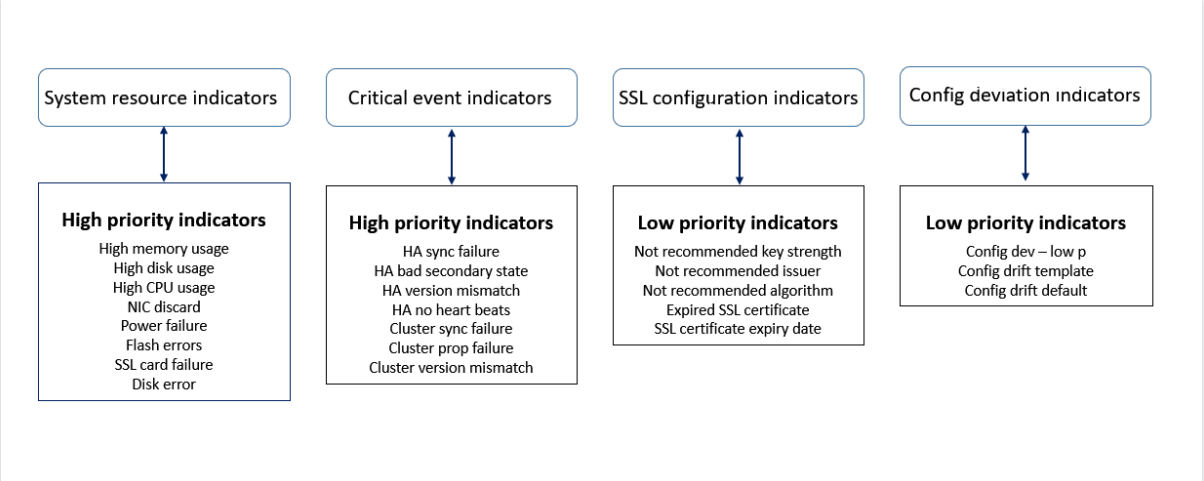
したがって、ADC インスタンスが容量のしきい値に違反すると、インスタンスのスコアが影響を受けます。

パケットがドロップまたはレート制限カウンタが増加すると、ADCCapacityBreach カテゴリの下にイベントが生成されます。これらのイベントを表示するには、「アカウント」>「システム・イベント」に移動します。



健全性指標の値

指標は、その値に基づいて高優先度指標と低優先度指標に分類される。



同じ指標グループ内の健全性指標には、それぞれ異なる重みが割り当てられています。1 つのインジケーターは、別のインジケーターよりもインスタンススコアの低下に大きく寄与する可能性があります。たとえば、メモリ使用量が高いと、ディスク使用量、CPU 使用量、NIC 廃棄量よりもインスタンスのスコアが下がります。インスタンスで検出されたインジケータの数が多い場合は、インスタンスのスコアが小さい方になります。

指標の値は、以下のルールに基づいて計算されます。この指標は、以下の 3 つの方法のいずれかで検出されると言われています。

1. アクティビティに基づきます。たとえば、システムリソースインジケータは、インスタンスに電源障害があるたびにトリガーされ、このインジケータはインスタンススコアの値を減らします。インジケータがクリアされると、ペナルティがクリアされ、インスタンスのスコアが増加します。
2. しきい値違反に基づく。たとえば、NIC カードがパケットを破棄し、しきい値レベルに違反すると、システムリソースインジケータがトリガーされます。
3. しきい値の下限値と上限値の違反に基づきます。ここでは、インジケータは 2 つの方法でトリガできます。

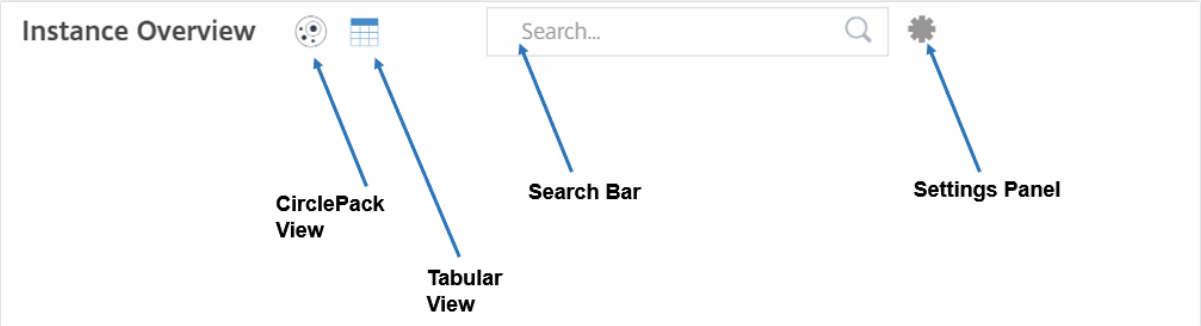
- インジケータの値が低しきい値と高しきい値の間にある場合。この場合、インスタンススコアに部分的なペナルティが課されます。
- 値が上限しきい値を超えると、インスタンススコアにペナルティが課されます。
- 値が低いしきい値を下回った場合、インスタンスコアのペナルティは課されません。

たとえば、CPU 使用率は、使用率が低いしきい値を超えたとき、および値が高いしきい値を超えたときにトリガーされるシステムリソースインジケータです。

インフラストラクチャ分析ダッシュボード

[ネットワーク] > [インフラストラクチャ分析] に移動します。

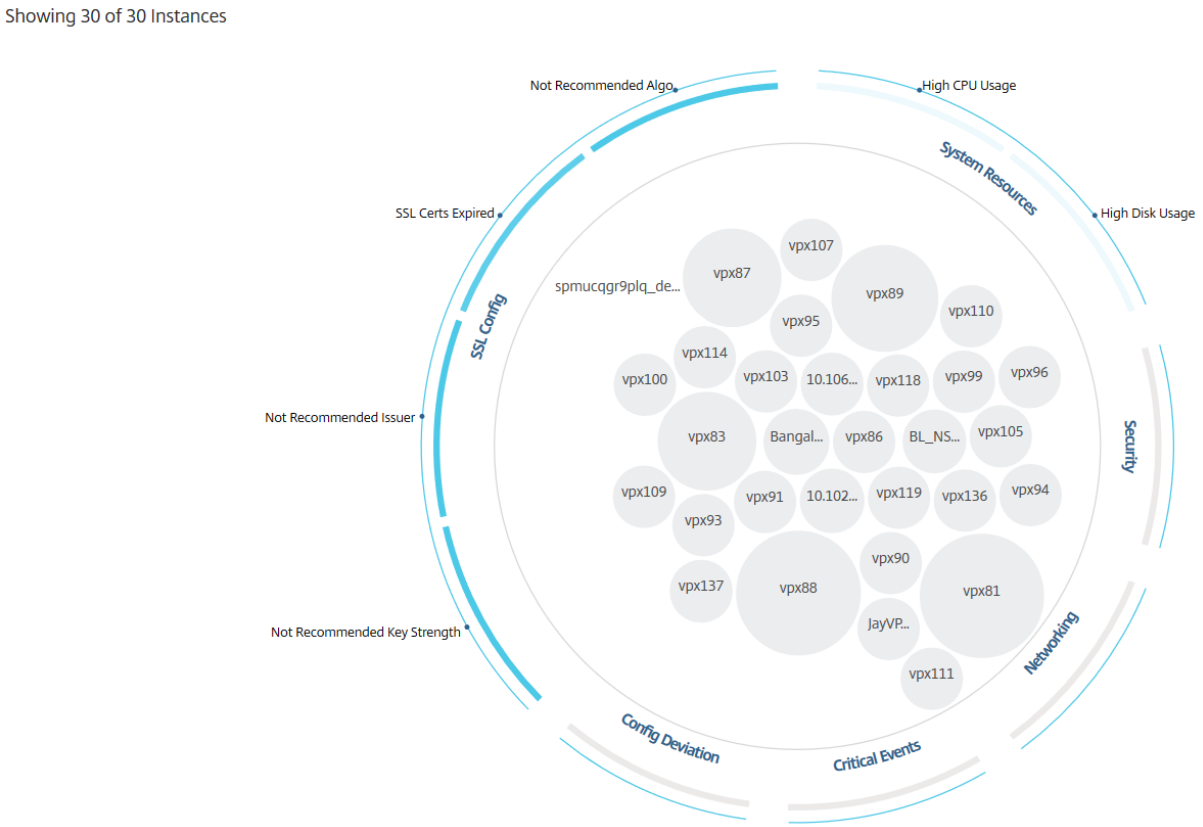
インフラストラクチャ分析は、サークルパック形式または 表形式で表示できます。2 つの形式を切り替えることができます。



- [Tabular] ビューでは、検索バーにホスト名または IP アドレスを入力してインスタンスを検索できます。
- デフォルトでは、[インフラストラクチャ分析] ページの右側に概要パネルが表示されます。
- 設定アイコンをクリックすると、設定パネルが表示されます。
- どちらのビュー形式でも、Summary Panel にはネットワーク内のすべてのインスタンスの詳細が表示されます。

サークル・パックの表示

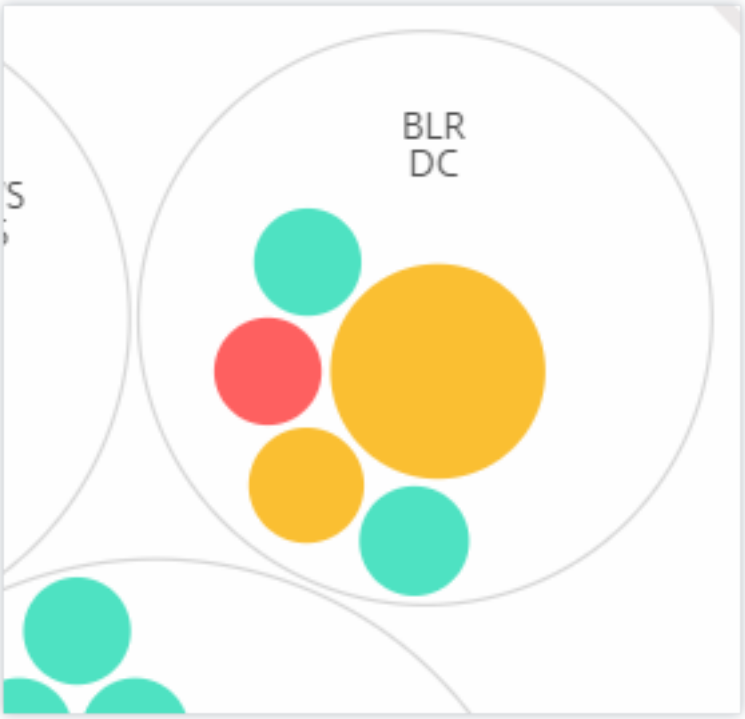
円パッキング図は、インスタンスグループを緊密に整理された円として示しています。小さなインスタンスグループは、同じカテゴリの他のインスタンスグループと同様に色分けされているか、大きなグループ内にネストされている階層を表示することがよくあります。サークルパックは階層データセットを表し、階層内の異なるレベルと、それらが相互にどのように相互作用するかを示します。



インスタンス円

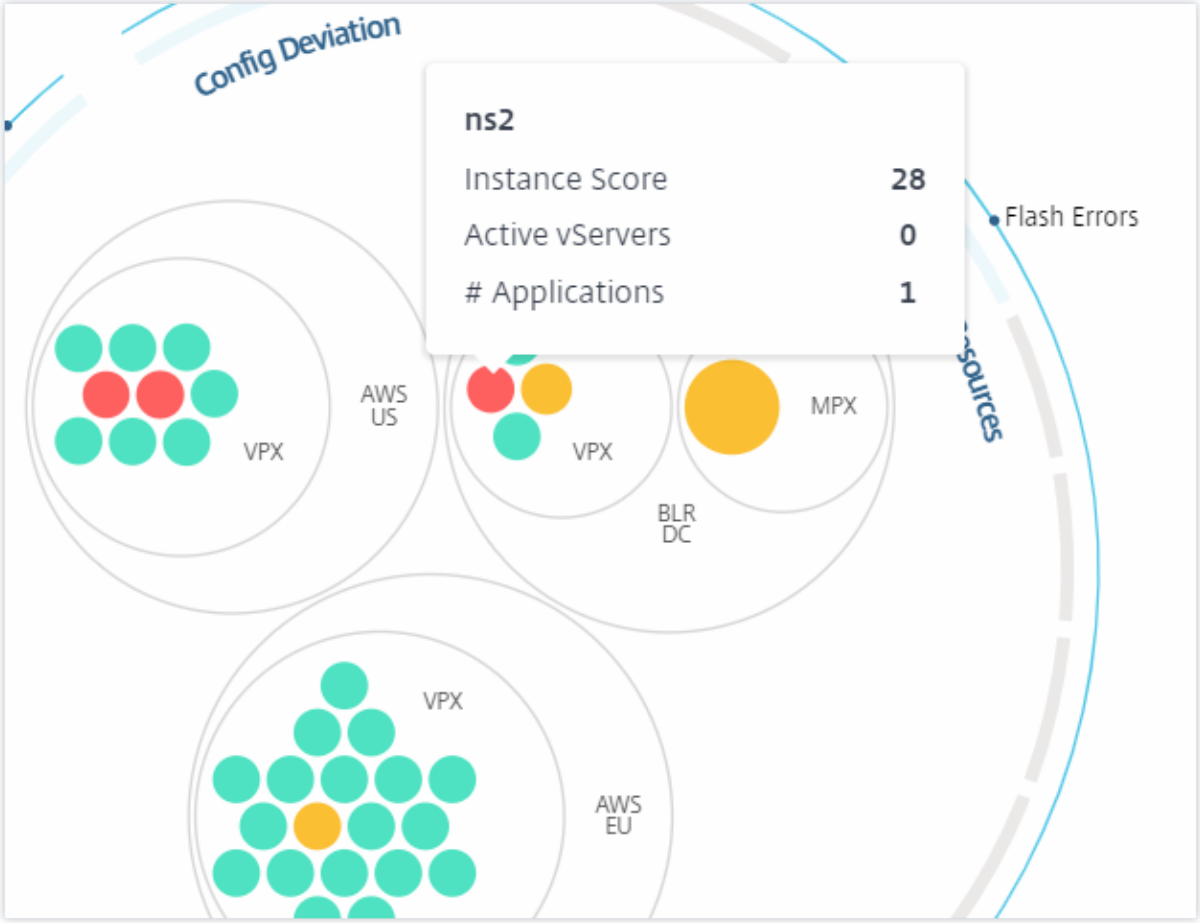
[色]: 各インスタンスは、色付きの円としてサークルパックに表示されます。円の色は、そのインスタンスの状態を示します。

- 緑 -インスタンスのスコアは 100 ～80 です。インスタンスは正常です。
- 黄色 -インスタンスのスコアは 80 ～50 です。いくつかの問題が認識されており、確認が必要です。
- 赤 -インスタンスのスコアが 50 未満です。インスタンスは、そのインスタンスに複数の問題が認識されるため、重要な段階にあります。



サイズ。これらの色付きの円のサイズは、そのインスタンスに構成されている仮想サーバーの数を示します。円が大きいほど、仮想サーバの数が多いことを示します。

各インスタンス円（色付きの円）にマウスポインターを合わせると、概要が表示されます。ホバーツールチップには、インスタンスのホスト名、アクティブな仮想サーバーの数、およびそのインスタンスに構成されているアプリケーション数が表示されます。

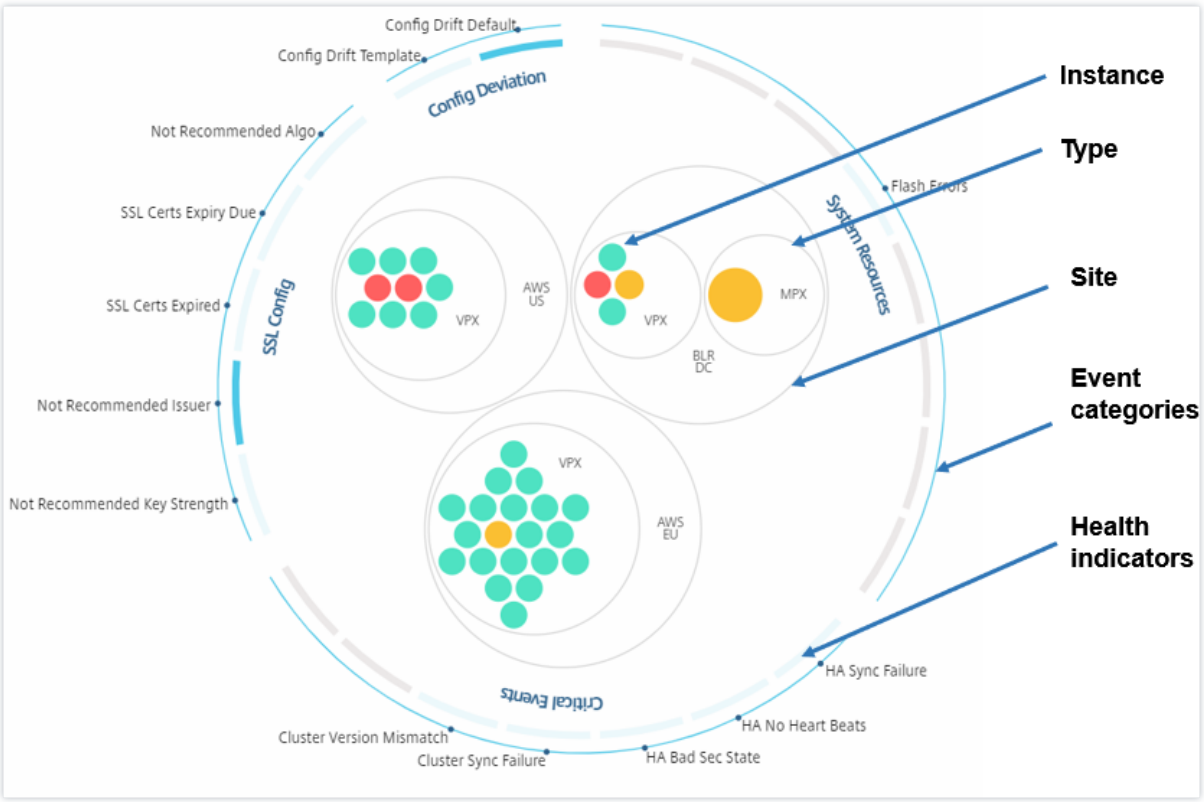


グループ化されたインスタンス円

Circle Pack は、次の基準に基づいてグループ化、ネスト化、または別の円内にパックされたインスタンス円で構成されます。

- それらがデプロイされているサイト
- デプロイされたインスタンスのタイプ（VPX、MPX、SDX、CPX）
- ADC インスタンスの仮想モデルまたは物理モデル
- インスタンスにインストールされている ADC イメージのバージョン

次の図は、Circle Pack を示しています。この Circle Pack では、インスタンスがデプロイされるサイトまたはデータセンター別にグループ化され、次にそのタイプ（VPX、MPX）に基づいてさらにグループ化されます。

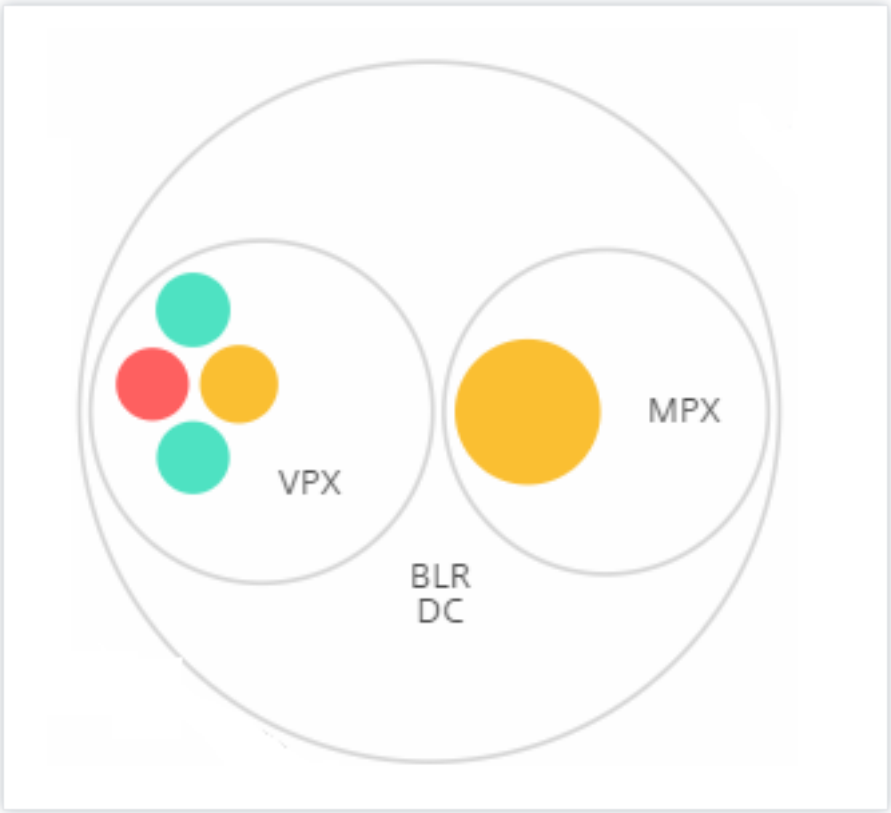


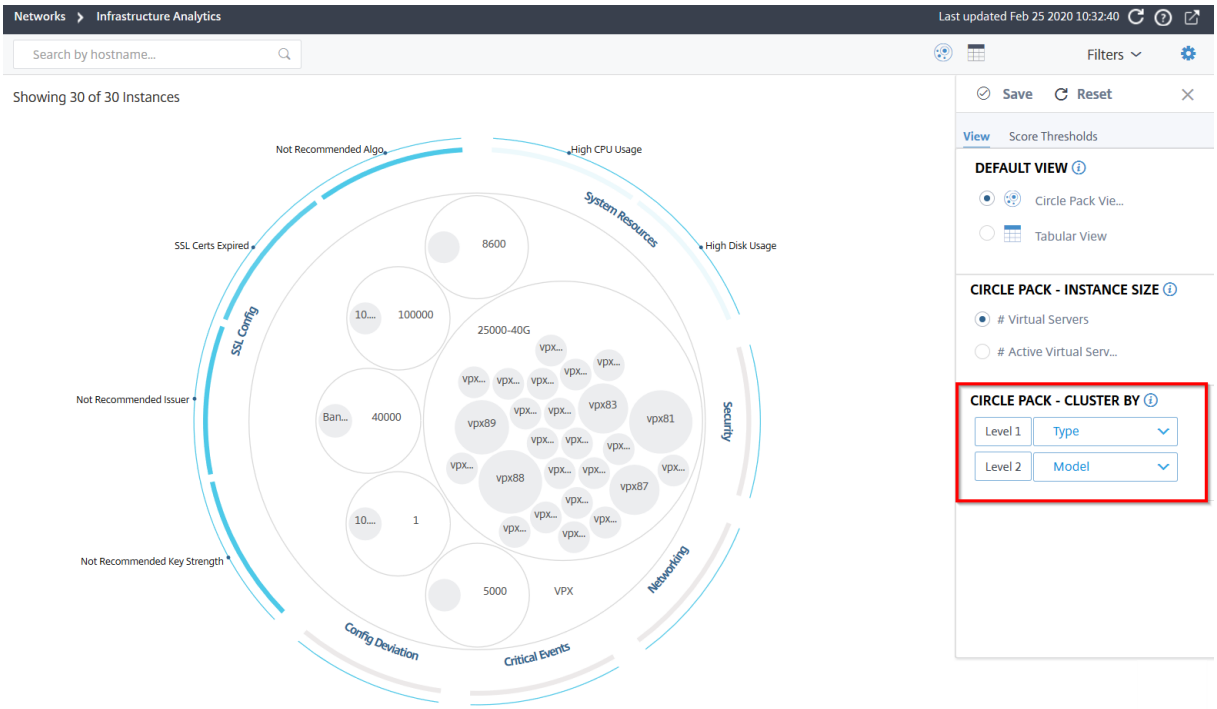
これらのネストされた円はすべて、最も外側の 2 つの円で囲まれています。外側の 2 つの円は、Citrix ADM によって監視されるイベントの 4 つのカテゴリ（システムリソース、クリティカルイベント、SSL 構成、および構成の偏差）と原因となる健全性インジケータを表します。

クラスター化されたインスタンス円

Citrix ADM は多くのインスタンスを監視します。これらのインスタンスの監視とメンテナンスを容易にするため、Infrastructure Analytics では 2 つのレベルでインスタンスをクラスター化できます。つまり、インスタンスグループを別のグループ内にネストできます。

たとえば、BLR データセンターには、VPX と MPX の 2 種類の ADC インスタンスが配備されています。まず、ADC インスタンスをタイプ別にグループ化してから、すべてのインスタンスをグループ化するサイト別にグループ化できます。管理しているサイトにデプロイされているインスタンスの種類の数を簡単に特定できるようになりました。

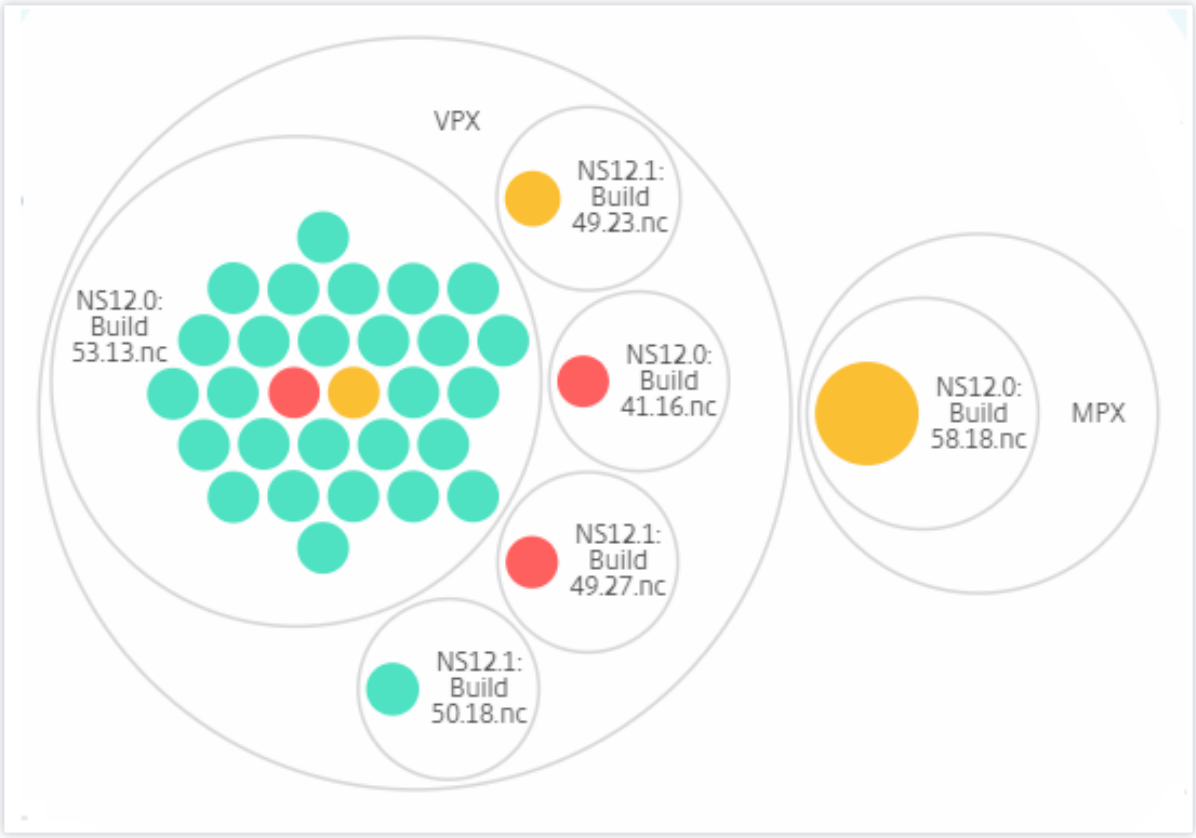




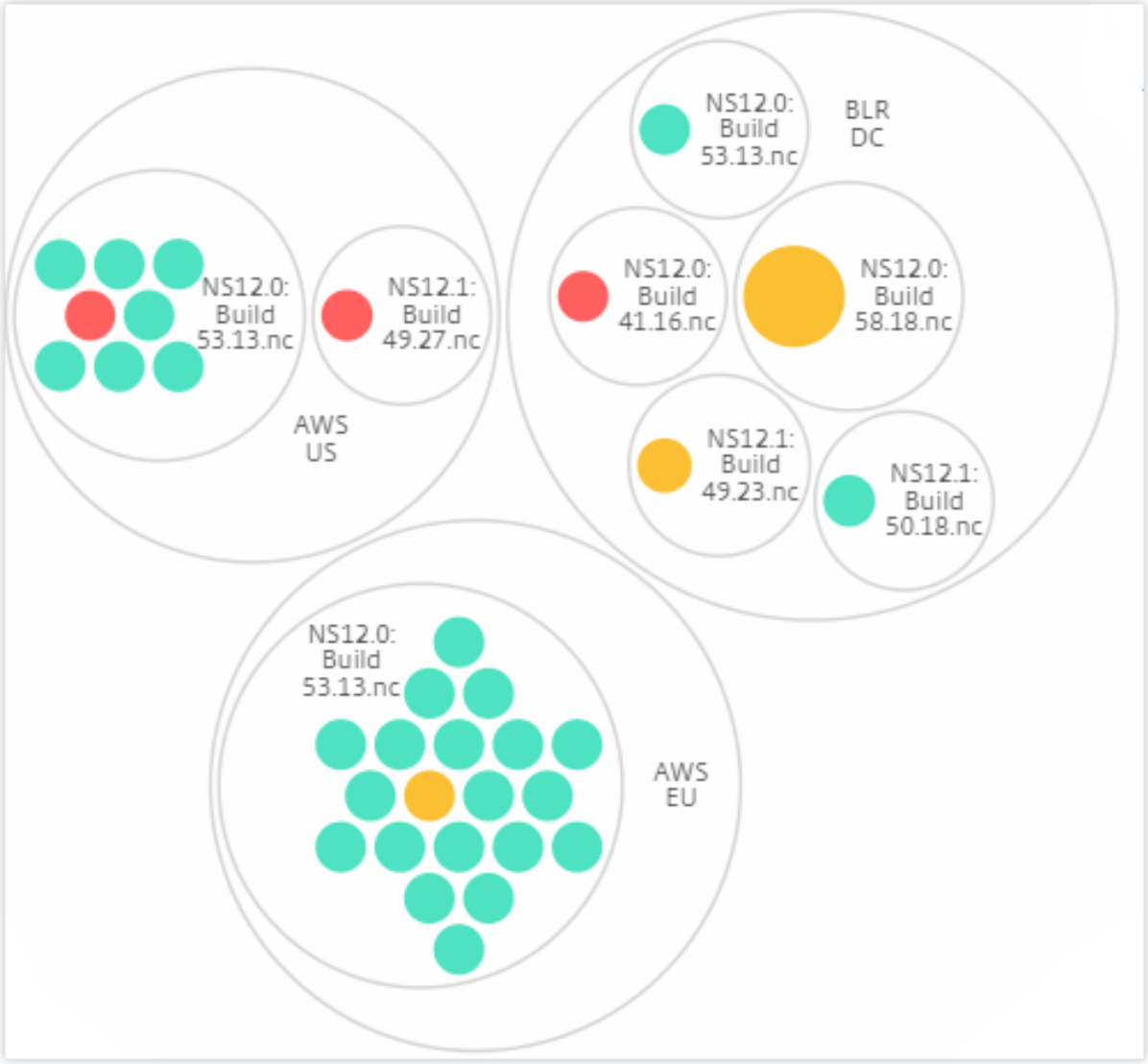
2 レベルクラスタリングのさらにいくつかの例を次に示します。

サイトとモデル**:**

タイプとバージョン**:**

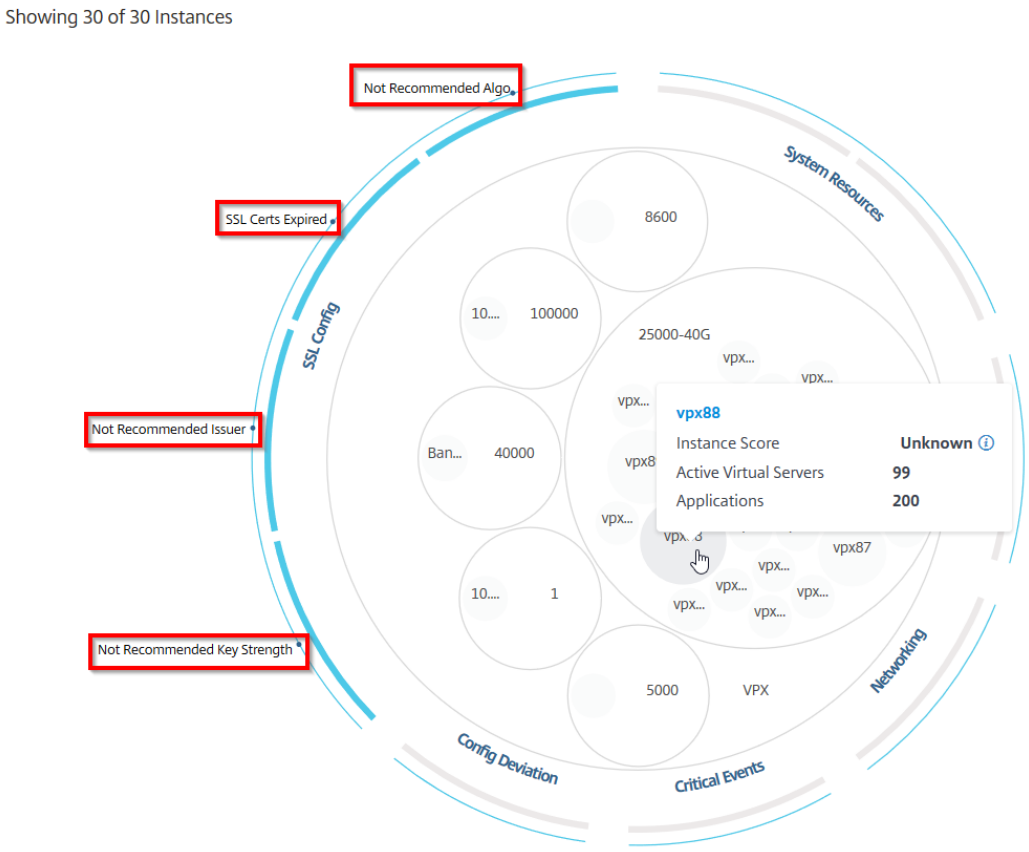


サイトとバージョン**:**



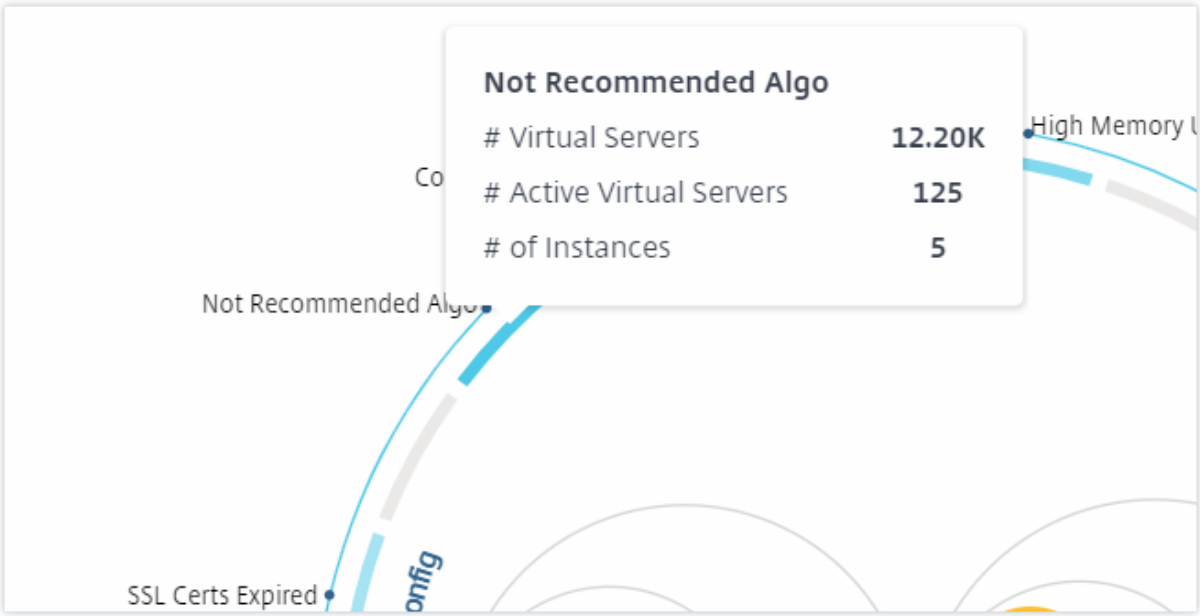
サークルパックの使い方

色付きの円をそれぞれクリックして、そのインスタンスをハイライト表示します。



そのインスタンスで発生したイベントに応じて、それらの健全性インジケータだけが外側の円で強調表示されます。たとえば、次の 2 つのサークルパックの画像は、両方のインスタンスがクリティカル状態にあるにもかかわらず、異なるリスク指標のセットを示しています。

また、健全性インジケータをクリックして、そのリスクインジケータを報告したインスタンスの数に関する詳細を表示することもできます。たとえば、`Not recommended Algo`をクリックすると、そのリスクインジケータのサマリレポートが表示されます。



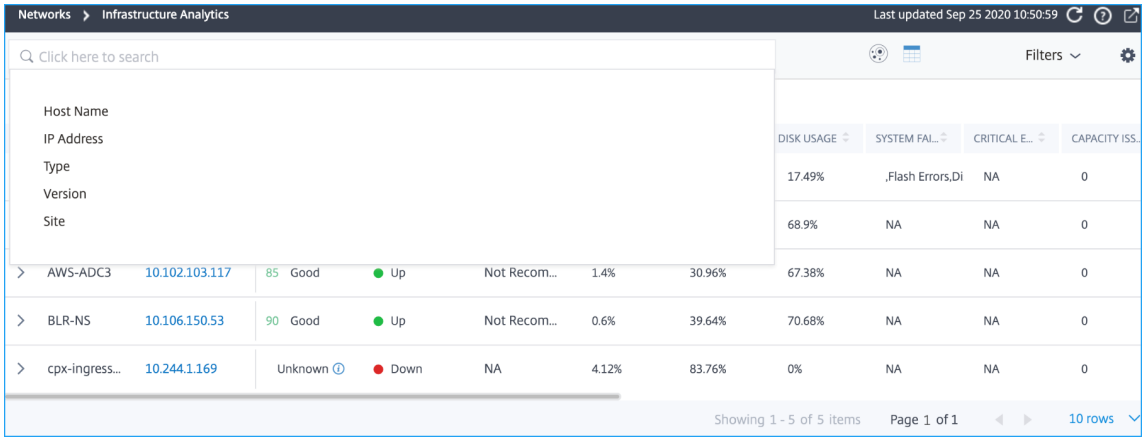
表形式ビュー

表形式ビューには、インスタンスとインスタンスの詳細が表形式で表示されます。詳しくは、「インスタンスの詳細」を参照してください。

検索バー

検索バーにマウスカーソルを置き、次の検索属性を選択して結果をフィルタリングします。

- ホスト名
- IP アドレス
- 種類
- バージョン
- サイト



検索結果は、円ビューとテーブルビューの両方で機能します。

概要パネルの使用方法

Summary Panel を使用すると、レビューやクリティカルな状態が必要なインスタンスに効率的かつ迅速に焦点を当てることができます。パネルは、概要、インスタンス情報、トラフィックプロファイルの 3 つのタブに分かれています。このパネルで行った変更によって、円パックと表形式の両方の表示形式での表示が修正されます。次のセクションでは、これらのタブについて詳しく説明します。以下のセクションの例は、さまざまな選択基準を効率的に使用して、インスタンスによって報告された問題を分析するのに役立ちます。

概要:

[**Overview**] タブでは、ハードウェアエラー、使用状況、期限切れの証明書、およびインスタンスで発生する可能性のある同様のインジケータに基づいてインスタンスを監視できます。ここで監視できるインジケータは次のとおりです。

- CPU 使用率
- メモリ使用率
- ディスク使用率
- システム障害
- クリティカルイベント
- SSL 証明書の有効期限

これらのインジケータの詳細については、「*Citrix ADC* インスタンスの健全性インジケータ」を参照してください。

次の例は、[概要] パネルを操作して、エラーを報告しているインスタンスを分離する方法を示しています。

例 **1:** レビュー状態のインスタンスを表示します。

重大なエラーを報告していないが注意が必要なインスタンスのみを表示するには、[Re **view**] チェックボックスをオンにします。

[**Overview**] パネルのヒストグラムは、高い CPU 使用率、高いメモリ使用率、および高いディスク使用率のイベントに基づいて、インスタンスの集計数を表します。ヒストグラムは、10%、20%、30%、40%、50%、60%、70%、80%、90%、100% で評定されます。いずれかの棒グラフにマウスポインターを合わせます。グラフの下部にある凡例には、使用範囲とその範囲内のインスタンスの数が表示されます。棒グラフをクリックして、その範囲内のすべてのインスタンスを表示することもできます。

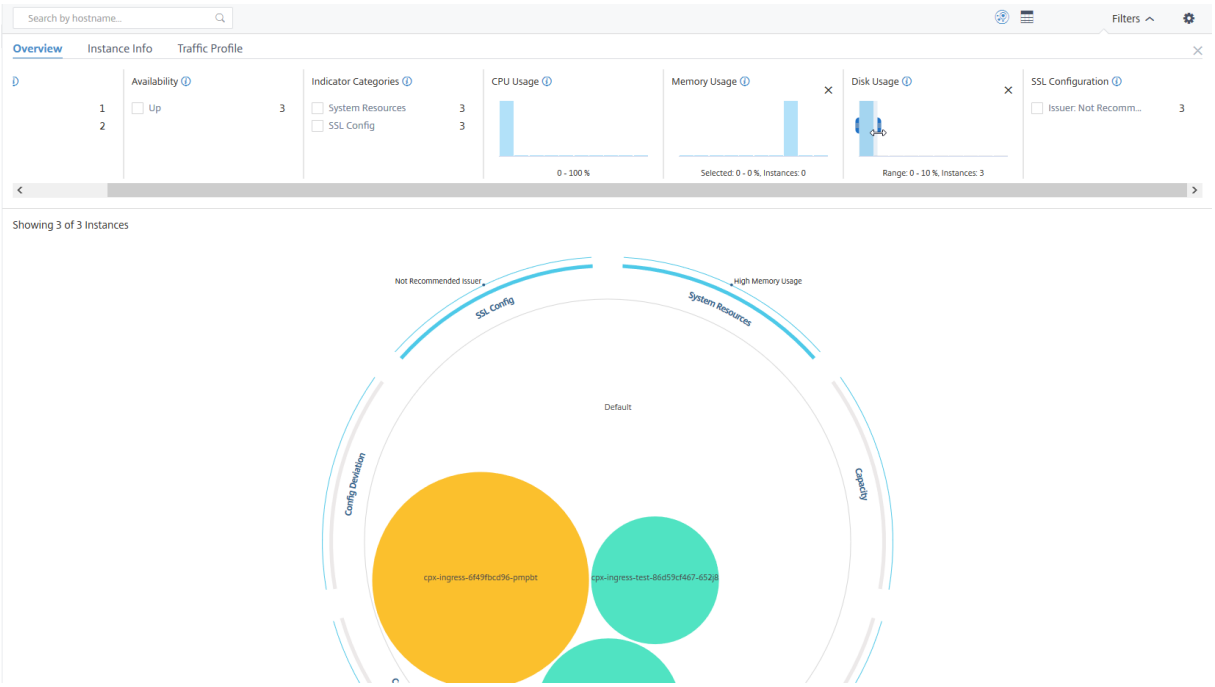
例 **2:** 割り当てられたメモリの **10%** ～**20%** を消費しているインスタンスを表示します。

[メモリ使用量] セクションで、棒グラフをクリックします。凡例には、選択した範囲が 10 ～20% で、その範囲内で動作しているインスタンスが 29 個あることが示されています。

これらのヒストグラムで複数の範囲を選択することもできます。

例 **3:** 複数の範囲のディスク領域を消費しているインスタンスを表示します。

0～10% のディスク領域間でメモリを消費したインスタンスを表示するには、次の図に示すように、マウスポインタを 2 つの範囲にドラッグします。

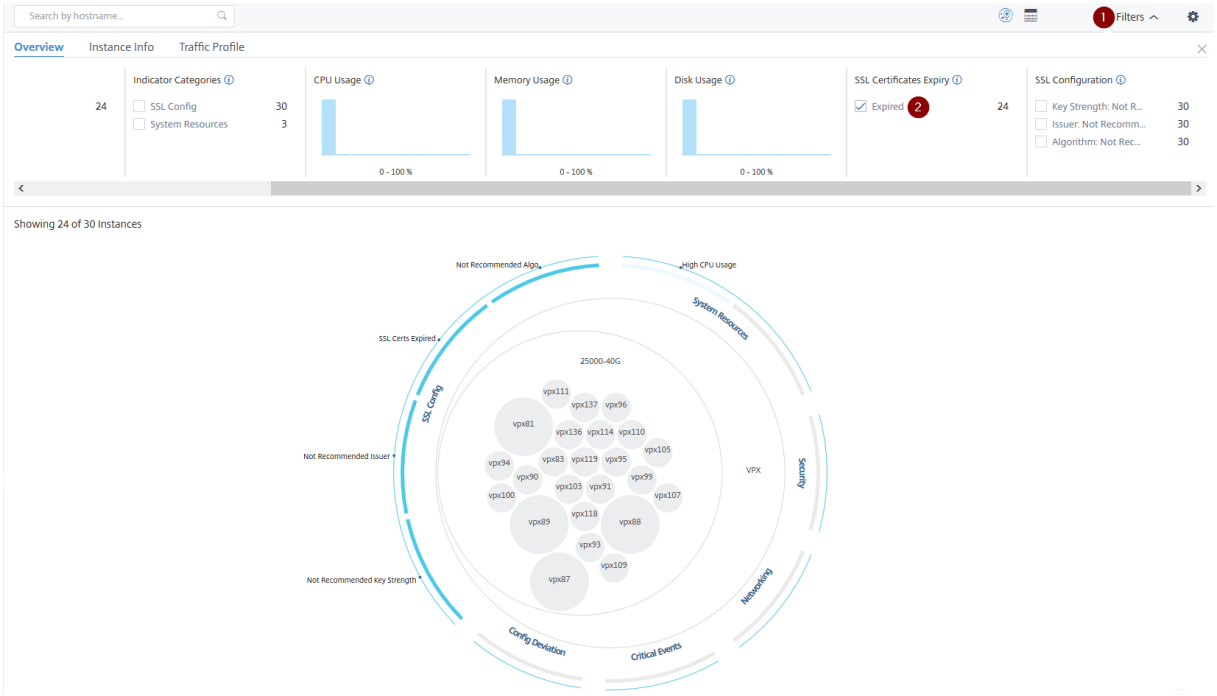


> 注:
>
> [X] をクリックして選択を解除します。「リセット」(**Reset**) をクリックして、複数の選択を削除することもできます。

[**Overview**] パネルの横棒グラフは、SSL 証明書のシステムエラー、重大なイベント、および有効期限ステータスを報告するインスタンスの数を示します。これらのインスタンスを表示するには、チェックボックスをオンにします。

例 **4:** 有効期限が切れた **SSL** 証明書のインスタンスの表示**:**

[**SSL** 証明書の有効期限] セクションで、[**Expired**] チェックボックスをオンにして 3 つのインスタンスを表示します。



1 -[フィルタ] リストをクリックします。

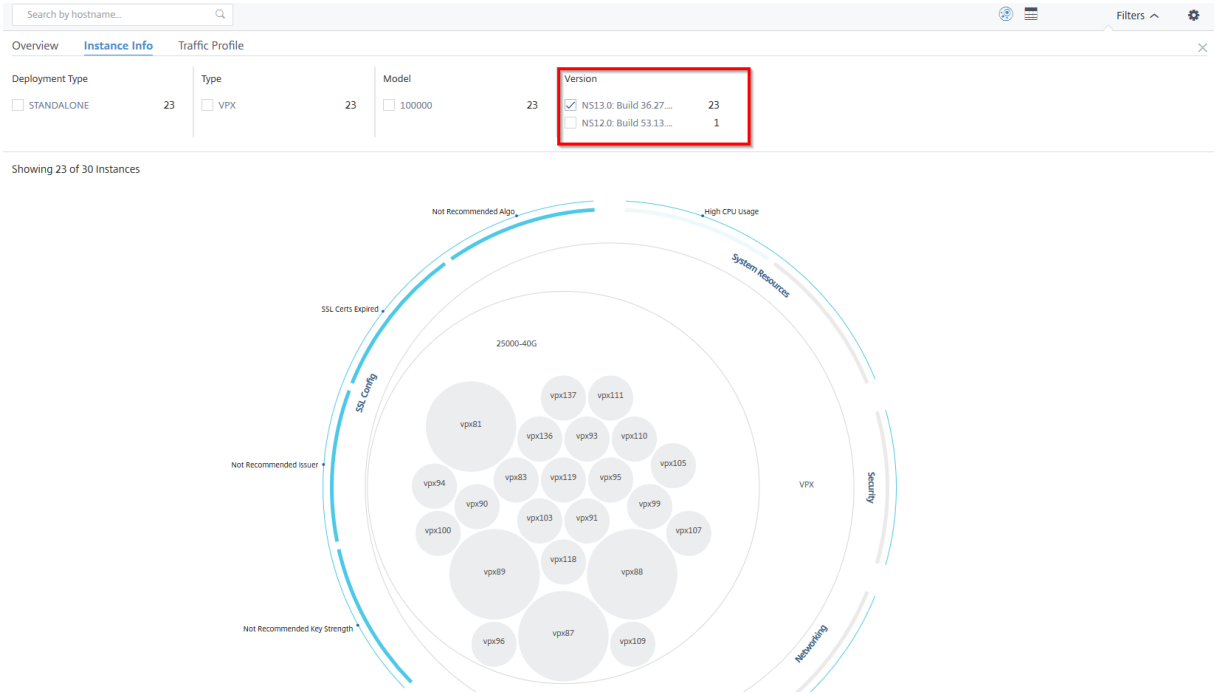
2 -[**SSL** 証明書の有効期限] セクションで、[Exp **ired**] チェックボックスをオンにして、インスタンスを表示します。

インスタンス情報

[**Instance Info**] パネルでは、デプロイのタイプ、インスタンスタイプ、モデル、ソフトウェアのバージョンに基づいてインスタンスを表示できます。複数のチェックボックスをオンにして、選択を絞り込むことができます。

例 **5:** 特定のビルド番号を持つ **ADC VPX** インスタンスの表示**:**

表示するバージョンを選択します。

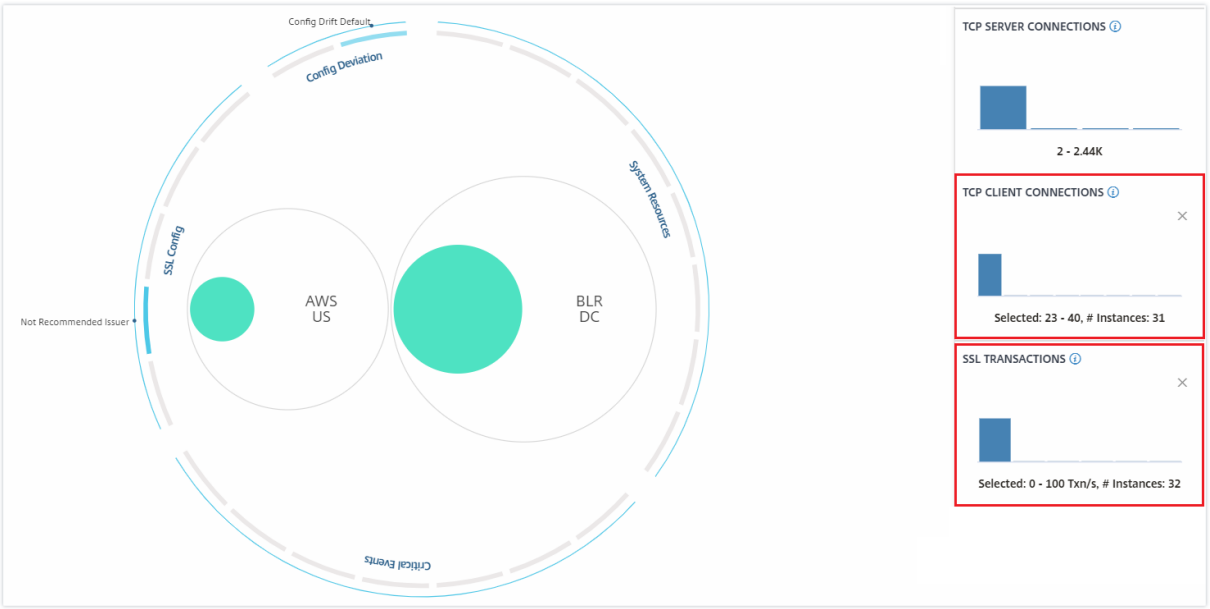


トラフィックプロファイル

[**Traffic]** プロファイルパネルのヒストグラムは、インスタンスでライセンスされたスループット、リクエストの数、接続、およびインスタンスによって処理されたトランザクションに基づいて、インスタンスの集計数を表します。棒グラフを選択して、その範囲のインスタンスを表示します。

例 **6: TCP** 接続をサポートするインスタンスの表示**:**

次の図は、23 ～40 の TCP 接続をサポートし、1 秒あたり最大 100 の SSL トランザクションを処理するインスタンスの数を示しています。

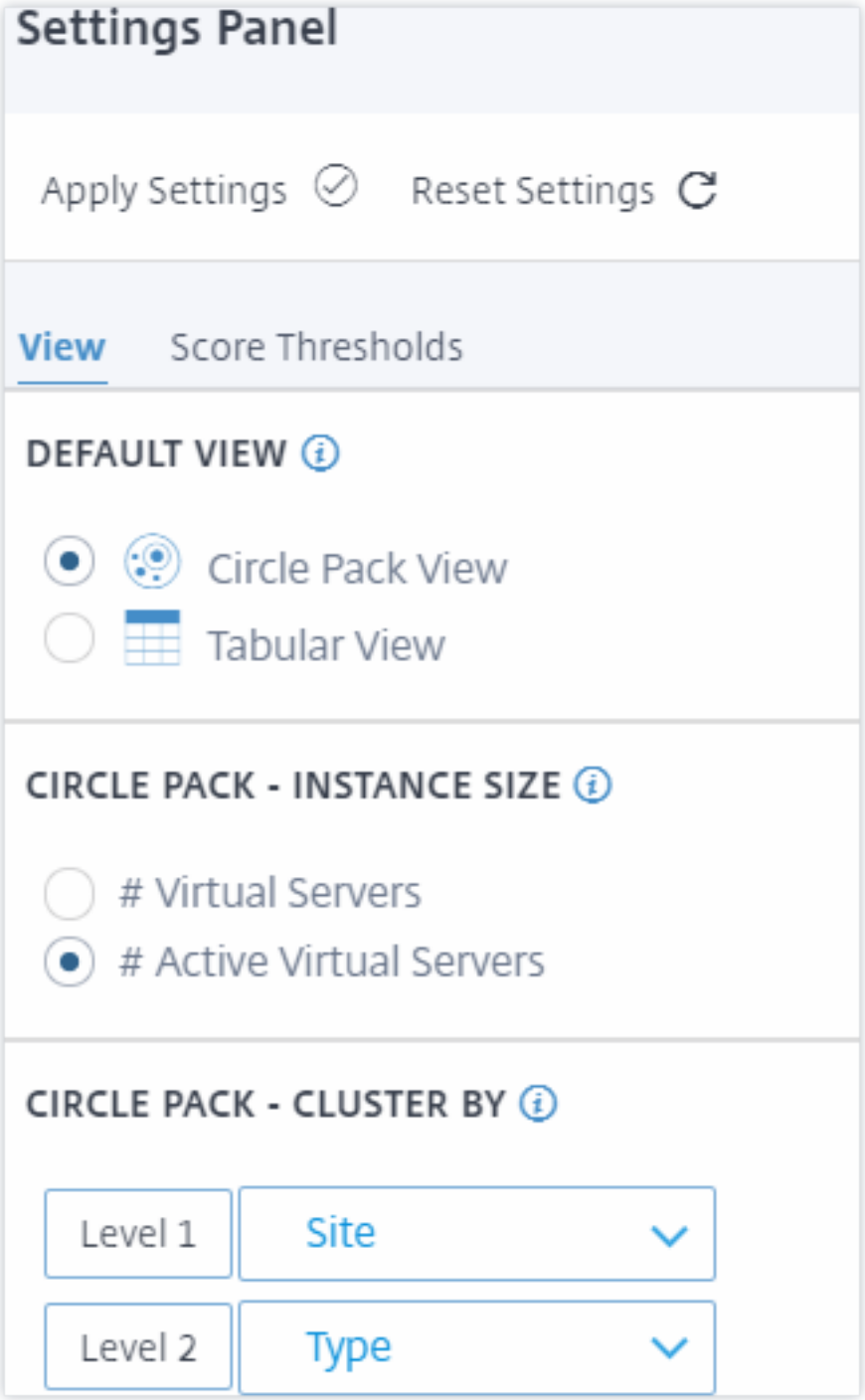


設定パネルの使い方

[設定] パネルでは、インフラストラクチャ分析の既定のビューを設定できます。また、高 CPU 使用率、高ディスク使用率、および高メモリ使用率のしきい値を設定することもできます。設定パネルは、[表示] と [スコアしきい値] の 2 つのタブに分かれています。

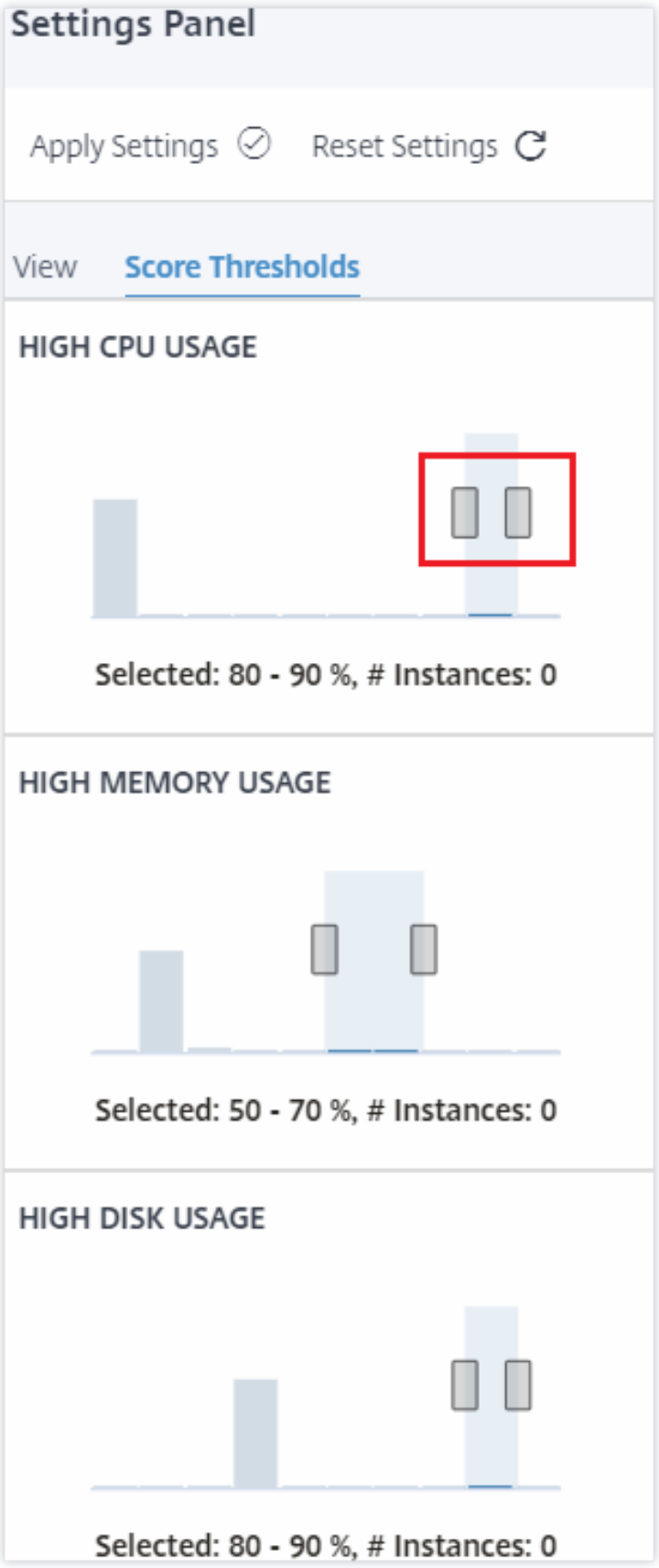
表示

- **[** 既定のビュー**]:** 分析ページのデフォルトのビューとして、「円パック」または「表形式」を選択します。選択した形式は、Citrix ADM でページにアクセスしたときに表示される形式です。
- 円パック**-**インスタンスサイズ。インスタンスサークルのサイズを、仮想サーバーの数またはアクティブな仮想サーバーの数だけにします。
- サークルパック**-**クラスタ **By**. インスタンスサークルの 2 レベルのクラスタリングを決定します。インスタンスのクラスタリングの詳細については、「クラスター化されたインスタンス円」を参照してください。



スコアのしきい値

組織のトラフィック要件に応じて、CPU、メモリ、およびディスクの使用率の高低しきい値および高しきい値を変更できます。各選択ヒストグラムのハンドルをドラッグして、値を設定します。



> 注**:**
>
> [設定の適用] をクリックしてこれらの変更を適用するか、[リセット] をクリックしてすべての変更を削除します。

ダッシュボードでデータを視覚化する方法

Infrastructure Analytics を使用して、ネットワーク管理者は数秒以内に最も注意が必要なインスタンスを特定できるようになりました。これをより詳細に理解するために、私たちは Chris、exampleCommPany のネットワーク管理者について考えてみましょう。

Chris は、組織内に多くの Citrix ADC インスタンスを管理しています。一部のインスタンスは高いトラフィックを処理し、それらを注意深く監視する必要があります。彼は、いくつかの高トラフィックインスタンスが、それらを通過する全トラフィックを処理していないことに気付きました。この削減を分析するには、以前は、さまざまなソースから入ってくる複数のデータレポートを読む必要がありました。Chris は、データを手動で相関させ、どのインスタンスが最適な状態になく、注意が必要かを確かめるために、より多くの時間を費やす必要がありました。Infrastructure Analytics 機能を使用して、すべてのインスタンスの状態を視覚的に確認します。

次の 2 つの例は、Infrastructure Analytics が Chris のメンテナンスアクティビティをどのように支援するかを示しています。

例 **1-SSL** トラフィックを監視するには、次の手順を実行します。

Chris が Circle Pack で、1 つのインスタンスのスコアが低く、そのインスタンスが「Critical」状態になっていることに気付きます。彼はインスタンスをクリックして、問題が何であるかを確認します。インスタンスの概要には、そのインスタンスで SSL カードに障害が発生しているため、そのインスタンスが SSL トラフィックを処理できない（SSL トラフィックが減少した）ことが示されます。Chris はその情報を抽出し、問題をすぐに調査するレポートをチームに送信します。

例 **2-**設定の変更を監視するには、次の手順に従います。

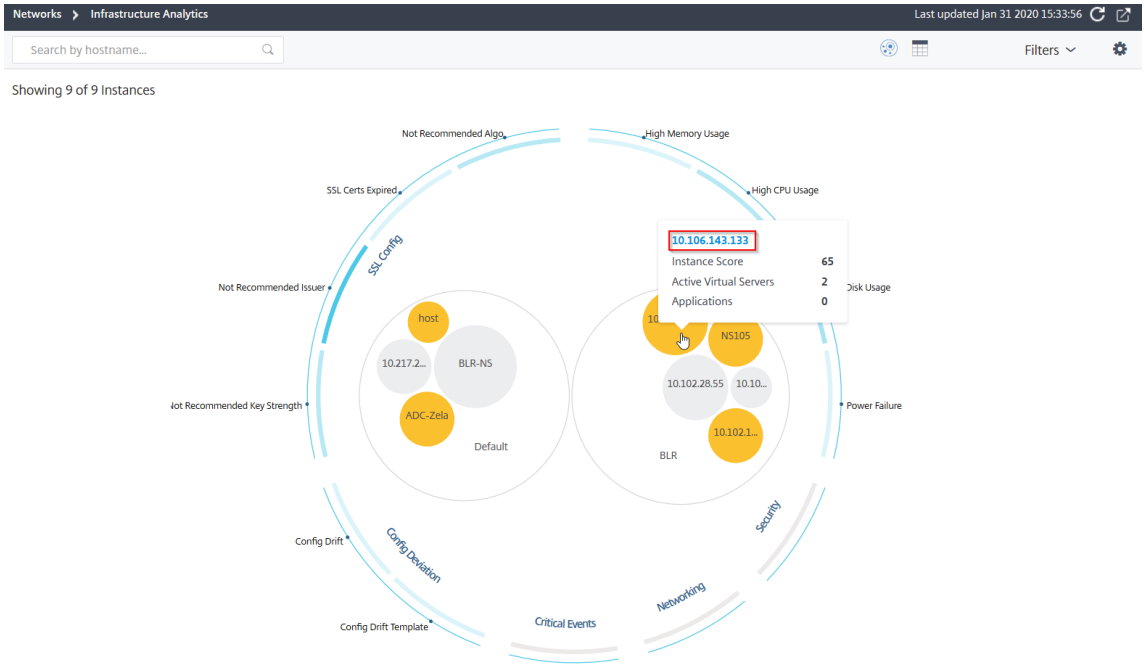
Chris は、別のインスタンスが「Review」状態にあり、最近設定偏差があることに気付きます。設定偏差リスクインジケータをクリックすると、RC4 暗号、SSL v3、TLS 1.0、および TLS 1.1 に関連する設定変更が行われたことがわかります。これは、セキュリティ上の問題が原因である可能性があります。また、このインスタンスの SSL トランザクショントラフィックプロファイルがダウンしていることに気付きます。彼はこのレポートをエクスポートし、さらに問い合わせるために管理者に送信します。

インフラストラクチャ分析でのインスタンスの詳細の表示

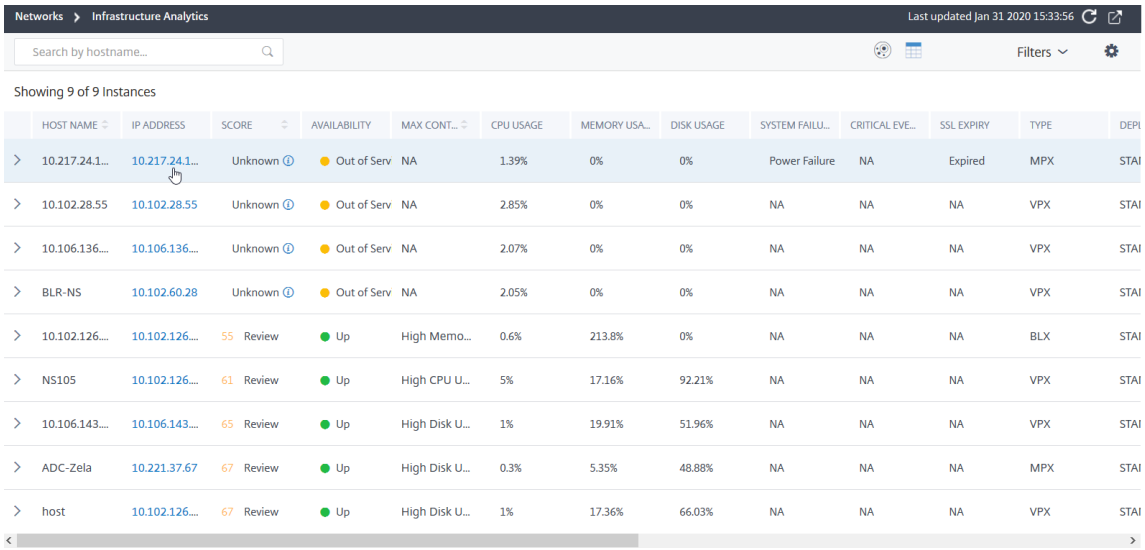
May 7, 2021

1. [ネットワーク] > [インフラストラクチャ分析] に移動します。

2. サークルパックビューをクリックし、IP アドレスを選択します。



テーブルビューから IP アドレスをクリックすることもできます。

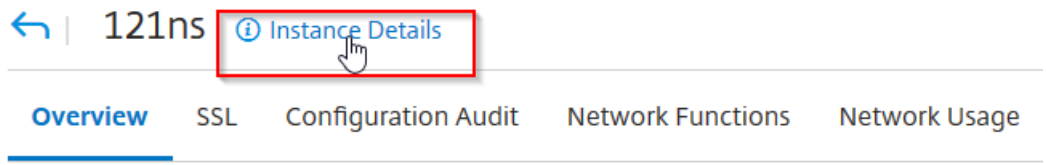


- ホスト名 — ADC インスタンスに割り当てられたホスト名を示します。
- **IP** アドレス：ADC インスタンスの IP アドレスを示します。
- スコア — ADC インスタンスのスコアと、クリティカル、グッド、フェアなどのステータスを示します。
- **Availability**： ADC インスタンスの現在のステータス（**Up**、**Down**、**Out of Service**）を示します。
- 最大寄与度 — ADC インスタンスのエラー数が最大である問題のカテゴリを示します。
- **CPU** 使用率 — インスタンスによって使用されている現在の CPU% を示します。

- メモリ使用量 — インスタンスによって使用されている現在のメモリ% を示します。
- ディスク使用率 — インスタンスによって使用されている現在のディスク% を示します。
- システム障害 — インスタンスシステムのエラーの総数を示します。
- 「クリティカルイベント」— Citrix ADC インスタンスに最大イベントがあるイベントカテゴリを示します。
- **SSL** 有効期限 — ADC インスタンスにインストールされている SSL 証明書の現在のステータスを示します。
- タイプ: VPX、SDX、MPX、CPX などの ADC インスタンスタイプを示します。
- **Deployment** — ADC インスタンスがスタンドアロン・インスタンスまたは HA ペアとしてデプロイされているかどうかを示します。
- モデル — ADC インスタンスのモデル番号を示します。
- バージョン — ADC インスタンスのバージョンとビルド番号を示します。
- スループット — ADC インスタンスからの現在のネットワークスループットを示します。
- **HTTPS** リクエスト/秒 — ADC インスタンスが受信した現在の HTTPS リクエスト/秒を示します。
- **TCP** 接続 — 現在確立されている TCP 接続を示します。
- **SSL** トランザクション — ADC インスタンスによって処理される現在の SSL トランザクションを示します。
- サイト — ADC インスタンスがデプロイされているサイトの名前を示します。

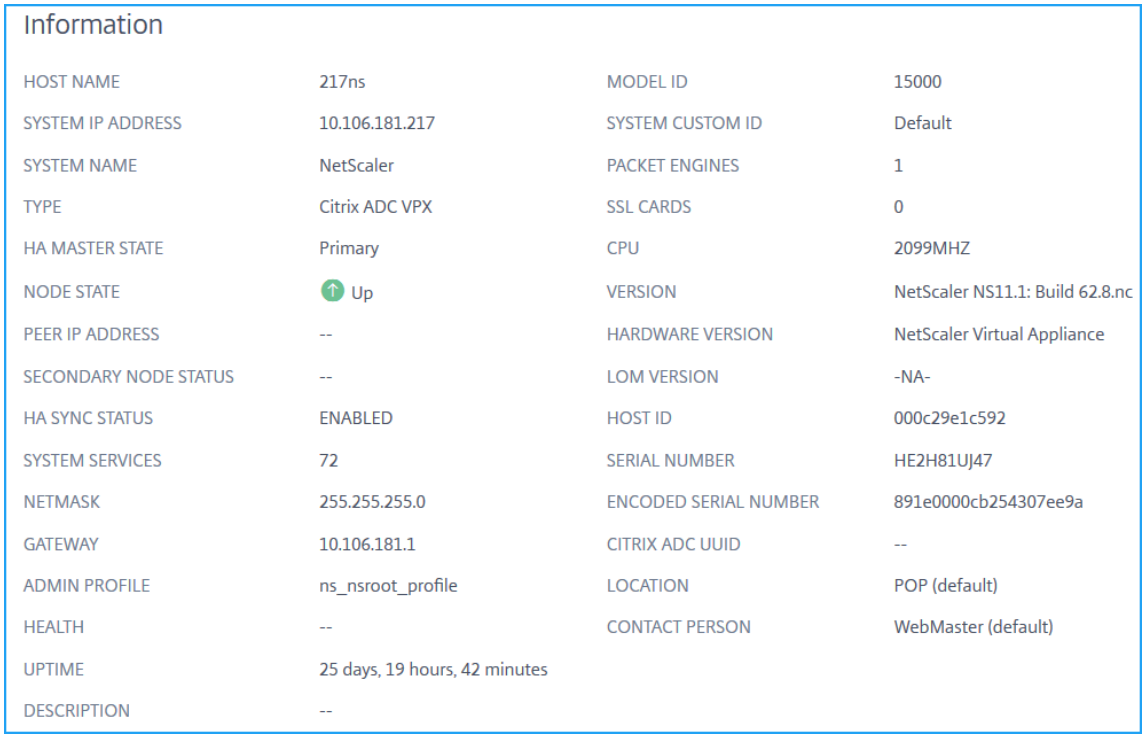
> 注
>
> 5 分ごとに、CPU 使用率、メモリ使用率、ディスク使用率、スループットなどの現在の値が更新されます。

[インスタンスの詳細] をクリックして詳細を表示します。

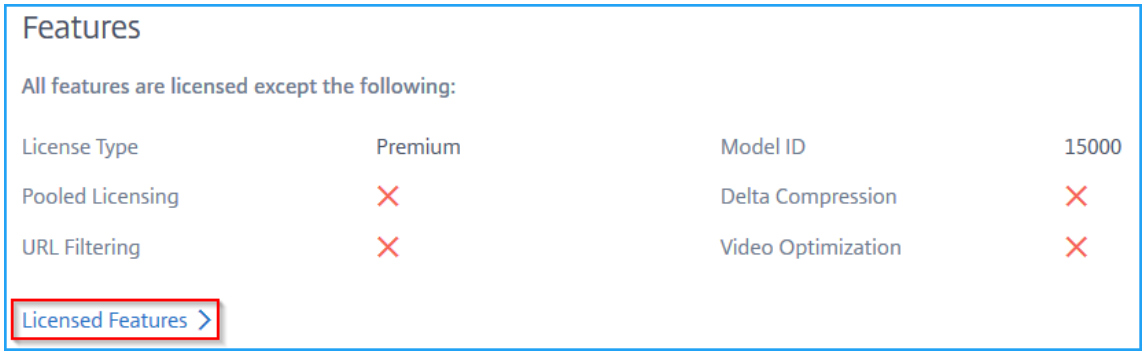


次の詳細が表示されます。

- 情報 -インスタンスタイプ、デプロイタイプ、バージョン、モデルなどのインスタンスの詳細。



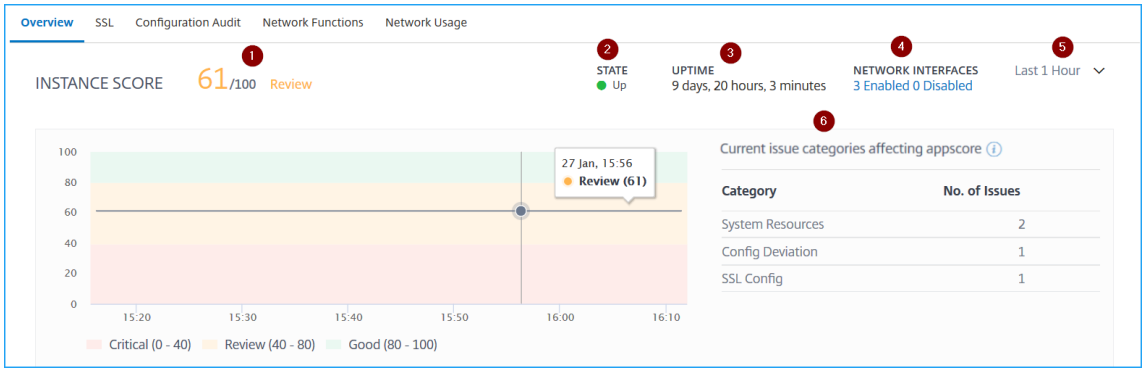
- 機能：デフォルトでは、ライセンスされていない機能が表示されます。ライセンスされた機能を表示するには、[ライセンスされた機能] をクリックします。



- **Modes** — デフォルトでは、インスタンスで無効になっているすべてのモードが表示されます。[**View Enabled Modes**] をクリックして、インスタンスの有効なモードを表示します。

インスタンスダッシュボードにはインスタンスの概要が表示され、次の詳細を確認できます。

- インスタンススコア

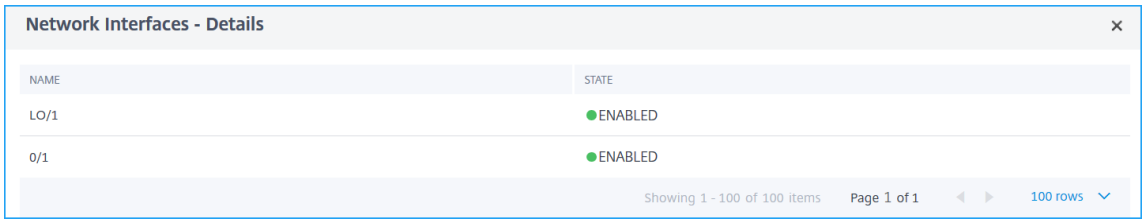


1 — 選択した期間の現在の Citrix ADC インスタンススコアを示します。最終的なスコアは、**100** からペナルティ合計を差し引いたものとして計算されます。グラフには、選択した期間のスコア範囲が表示されます。

2： Citrix ADC インスタンスの現在のステータス（[アップ]、[停止]、[サービス外] など）を示します。

3 — Citrix ADC インスタンスが起動して実行されている期間を示します。

4 — インスタンスに対して有効または無効になっているネットワークインターフェイスの合計を示します。クリックすると、ネットワークインターフェイス名やステータス (有効または無効) などの詳細が表示されます。



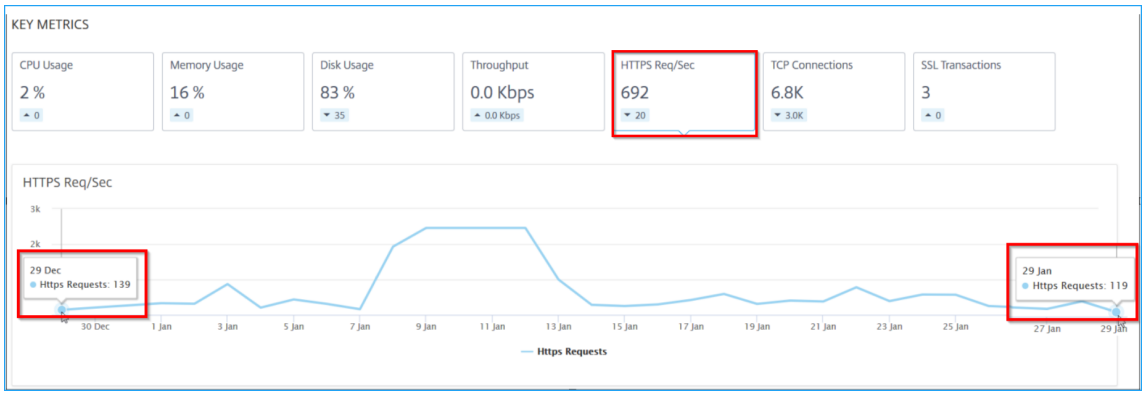
5 — インスタンスの詳細を表示するには、リストから期間を選択します。

6 — ADC インスタンスの問題と問題のカテゴリ合計を表示します。

- 主要メトリック

  各タブをクリックして詳細を表示します。各指標で、選択した時間の平均値と差分値を表示できます。

  次の図は、HTTPS Req/Sec の例で、選択した期間が 1 時間です。値 **692** は、1 か月間の平均の HTTPS 要求/秒、値 **20** は差の値です。グラフでは、最初の値は **139** 、最後の値は **119** です。差の値は **139** ～**119 = 20** です。



  選択した期間について、次のインスタンスメトリックスをグラフ形式で表示できます。

  - **CPU** 使用率 — 選択した期間におけるインスタンスからの平均 CPU%（パケット CPU と管理 CPU の両方で表示）。
  - 「メモリ使用量」— 選択した期間におけるインスタンスからの平均メモリ使用率 (%)。
  - [**Disk Usage**] — 選択した期間におけるインスタンスからの平均ディスク容量%。
  - スループット — 選択した期間にインスタンスによって処理された平均ネットワークスループット。
  - **HTTPS** リクエスト/秒 — 選択した期間にインスタンスが受信した HTTPS リクエストの平均値。
  - **TCP** 接続 — 選択した期間にクライアントとサーバーによって確立された平均 TCP 接続。
  - **SSL** トランザクション — 選択した期間にインスタンスによって処理された平均 SSL トランザクションです。

- 問題

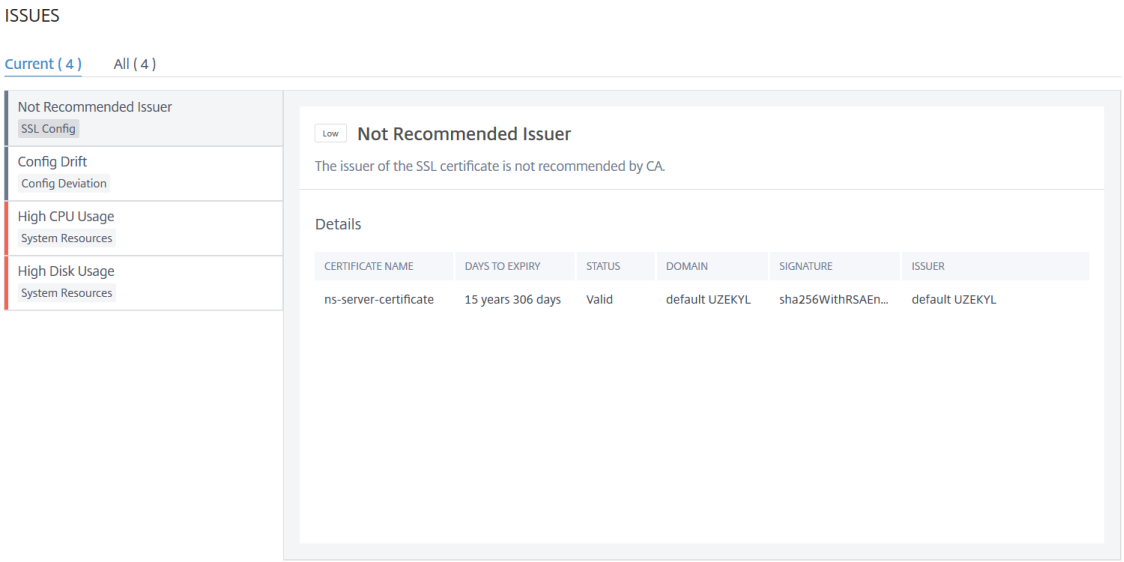
  Citrix ADC インスタンスで発生する次の問題を表示できます。

問題カテゴリ	説明	問題
システムリソース	CPU、メモリ、ディスク使用率など、Citrix ADC システムリソースに関連するすべての問題を表示します。	- 高い CPU 使用率 - 高いメモリ使用量

問題カテゴリ	説明	問題
		- 高いディスク使用率
		- SSL カードの障害
		- 電源障害
		- ディスクエラー
		- フラッシュエラー
		- NIC を破棄します。
SSL 設定	Citrix ADC インスタンスの SSL 構成に関連するすべての問題を表示します。	-SSL 証明書の有効期限が切れました
		- 推奨されない発行者
		- 推奨されていないアルゴリズム
		- 推奨しないキー強度。
設定偏差	Citrix ADC インスタンスで適用された構成ジョブに関連するすべての問題を表示します。	-コンフィグドリフト
		- 実行とテンプレート
クリティカルイベント	高可用性ペアとクラスタで構成された Citrix ADC インスタンスに関連するすべての重要なイベントを表示します。	- クラスタのプロップの障害
		- クラスタ同期の失敗
		- クラスタバージョンの不一致
		- HA 不良セック状態
		- HA ノーヒートビート
		- HA 同期の失敗
		- HA バージョンの不一致

問題カテゴリ	説明	問題
容量の問題	ADC 容量の問題を表示します。ADM は、ADC インスタンスから 5 分ごとにこれらのイベントをポーリングし、パケットドロップまたはレート制限カウンタが存在する場合は、その増加を表示します。問題は、次の容量パラメータに分類されます。	- スループット制限に達しました
		- PE CPU 制限に達しました
		- PPS 制限に達しました
		- SSL スループットレート制限
		- SSL TPS レート制限
ネットワーク	インスタンスで発生する運用上の問題を表示します。	詳しくは、「新しいインジケータによるインフラストラクチャ分析の強化」を参照してください。

各タブをクリックして、問題を分析し、トラブルシューティングします。たとえば、選択した期間について、インスタンスに次のエラーがあるとします。



- [**Current**] タブには、インスタンススコアに現在影響している問題が表示されます。
- [すべて] タブには、選択した期間に検出されたすべてのインフラストラクチャの問題が表示されます。

ADC インスタンスの容量に関する問題の表示

May 7, 2021

ADC インスタンスが使用可能な容量の大半を消費した場合、クライアントトラフィックの処理中にパケット廃棄が発生することがあります。この問題は、ADC インスタンスのパフォーマンスが低下します。このような ADC の容量に関する問題を理解することで、ADC の性能を安定させるために、プロアクティブにライセンスを割り当てることができます。

Circle Pack ビューでは、ADC インスタンスのキャパシティの問題が存在する場合は、その問題を表示できます。

ADC の容量に関する問題を確認するには、

1. [ネットワーク**] > [**インフラストラクチャ分析] に移動します。
2. 円パックビューを選択します。

次の図は、選択したインスタンスにキャパシティの問題が存在することを示しています。

問題は、次のキャパシティパラメータに分類されます。

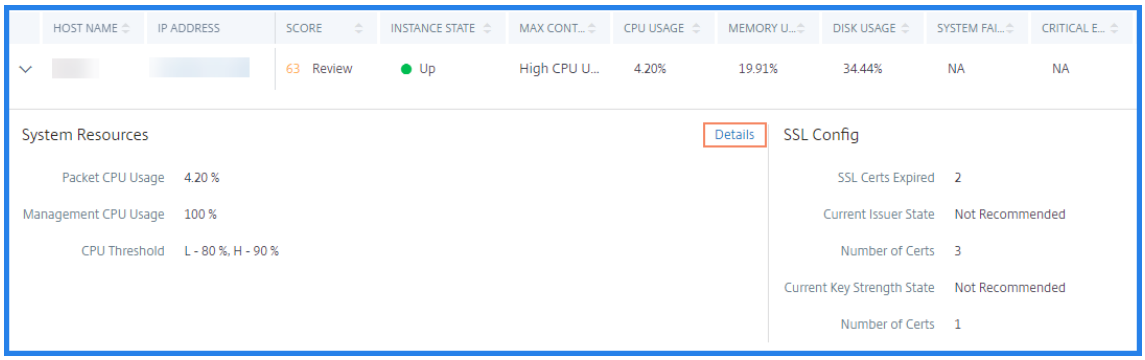
- スループット制限に達しました — スループット制限に達した後、インスタンスでドロップされたパケット数。
- **PE CPU** 制限に達しました -PE CPU 制限に達した後、すべての NIC でドロップされたパケット数。
- **PPS** 制限に達しました — PPS 制限に達した後にインスタンスでドロップされたパケット数。
- **SSL** スループットレート制限 — SSL スループット制限に達した回数。

- **SSL TPS** レート制限 — SSL TPS 制限に達した回数。

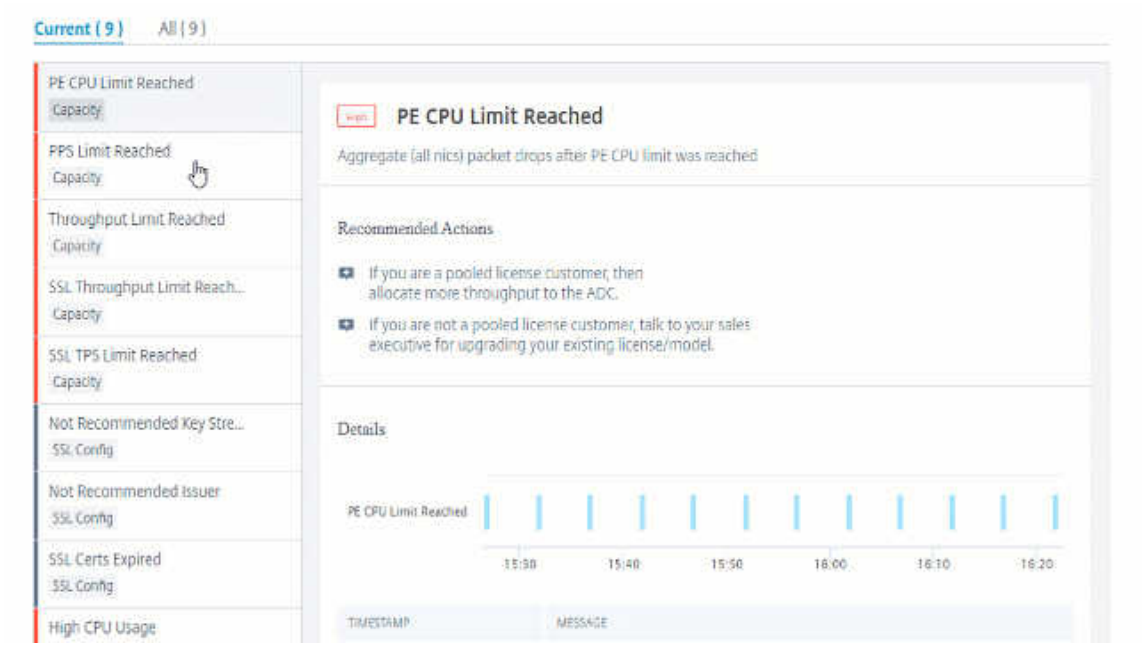
容量の問題を解決するための推奨アクションを表示する

ADM は、容量の問題を解決できるアクションを推奨しています。推奨されるアクションを表示するには、次の手順を実行します。

1. [ネットワーク**] > [**インフラストラクチャ分析] で、表形式のビューを選択します。
2. 容量に問題があるインスタンスを選択し、[**Details**] をクリックします。



3. インスタンスページで、[問題] セクションまでスクロールします。
4. 各問題を選択し、容量の問題を解決するための推奨アクションを表示します。



ADM は、ADC インスタンスから 5 分ごとにこれらのイベントをポーリングし、パケットドロップまたはレート制限カウンタが存在する場合は、その増加を表示します。

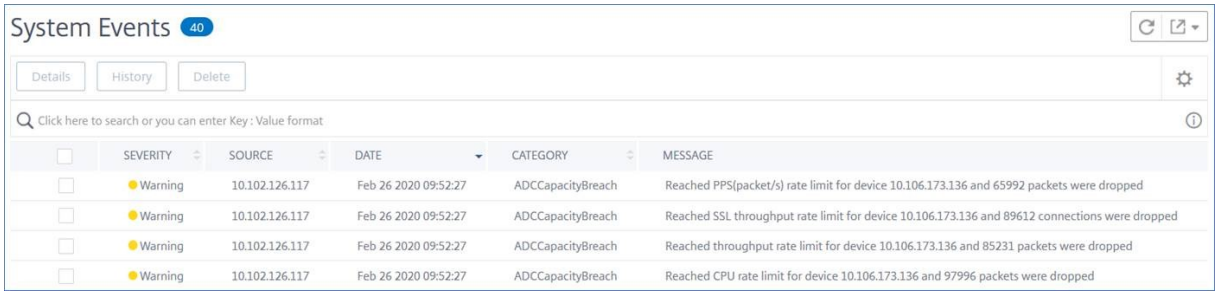
ADM は、定義されたキャパシティしきい値に基づいてインスタンススコアを計算します。

- 低しきい値：1 パケットドロップまたはレート制限カウンタ増分

- 高しきい値：10000 パケットのドロップまたはレート制限カウンタ増分

したがって、ADC インスタンスがキャパシティしきい値を超えると、インスタンスのスコアが影響を受けます。

パケットがドロップまたはレート制限カウンタが増加すると、`ADCCapacityBreach` カテゴリの下にイベントが生成されます。これらのイベントを表示するには、「アカウント」**>**「システム・イベント」に移動します。



新しいインジケータによるインフラストラクチャ分析の強化

May 7, 2021

Citrix **ADM** インフラストラクチャ分析を使用すると、次のことができます。

- Citrix ADC インスタンスで発生する新しい操作上の問題を表示します。
- エラーメッセージを表示し、問題をトラブルシューティングするための推奨事項を確認します。

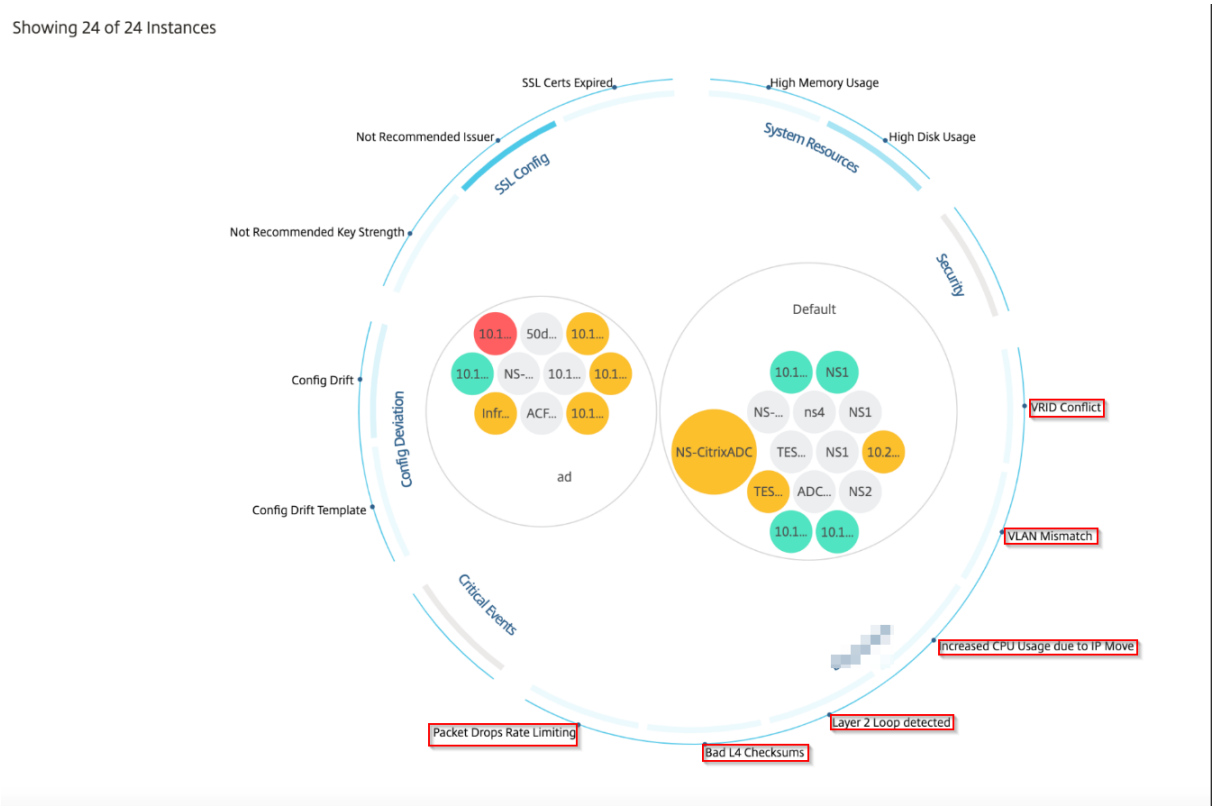
管理者は、問題の根本原因分析をすばやく特定できます。

> 注
>
> ルールインジケータは、次のものではサポートされていません。
>
> - クラスターモードで構成された Citrix ADC インスタンス。
> - 管理パーティションで構成された Citrix ADC インスタンス。

Citrix ADM で、[ネットワーク] > [インフラストラクチャ分析] に移動して、次のインジケータを表示します。

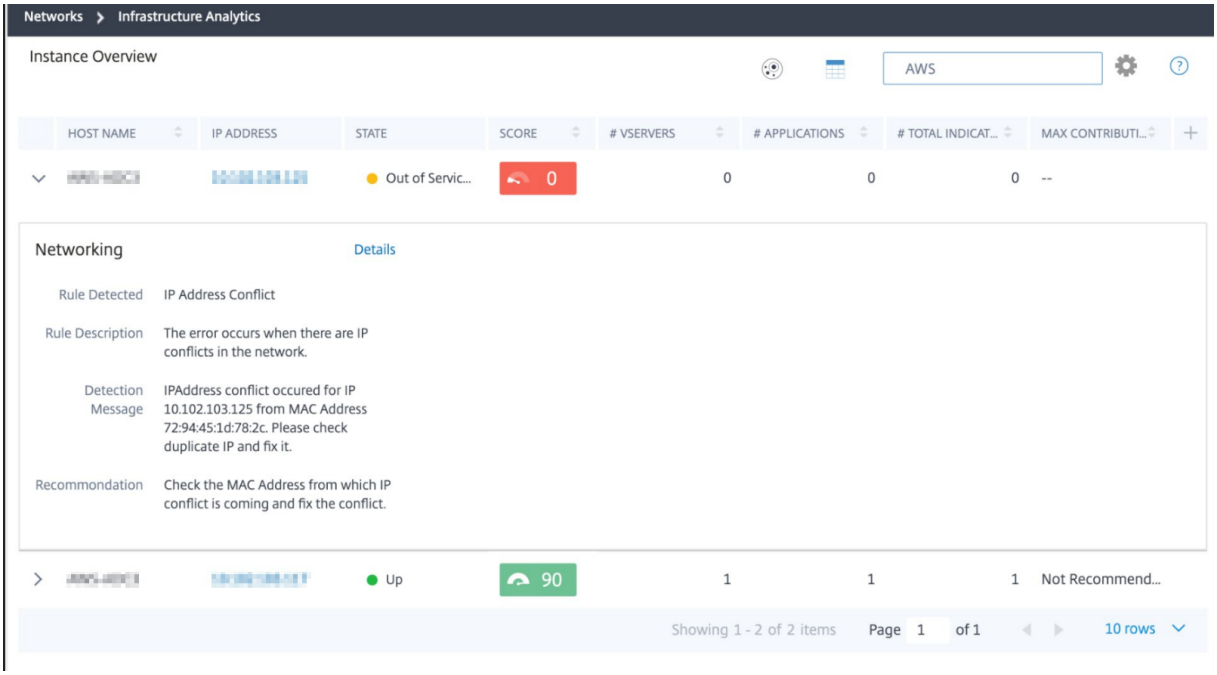
インフラストラクチャ分析のインジケータ名	説明
ポート割り当ての失敗	Citrix ADC が SNIP を使用して新しいサーバー接続と通信するタイミングを検出し、その SNIP で使用可能なポートの総数が枯渇します。推奨されるアクションは、同じサブネットに別の SNIP を追加することです。
セッションのビルダップ	SSL セッションで Citrix ADC メモリが保持されているかどうかを検出します。

インフラストラクチャ分析のインジケータ名	説明
デフォルトのルート設定なし	ルートの非アベイラビリティのためにトラフィックがドロップされるタイミングを検出します。
IP の競合	同じ IP アドレスがネットワーク内の 2 つ以上のインスタンスに設定または適用されているかどうかを検出します。
VRID の競合	指定された VRID に対して断続的なアクセス問題が発生したかどうかを検出します。
VLAN の不一致	IP サブネットにバインドされた VLAN 設定中にエラーが発生したかどうかを検出します。
TCP スモールウィンドウ攻撃	進行中のスモールウィンドウ攻撃の可能性を検出します。ADC はすでにこの攻撃を軽減しているため、このアラートは情報提供のためのものです。
レート制御しきい値	設定されたレート制御しきい値に基づいてパケットがドロップされるタイミングを検出します。
持続性制限	Citrix ADC メモリに最大ヒットが課されるタイミングを検出します。
GSLB サイト名の不一致	サイト名の不一致が原因で GSLB 構成の同期エラーが発生したかどうかを検出します。
不正な **IP** ヘッダー	IPv4 パケットの健全性チェックが失敗したことを検出します。
不正な **L4** チェックサム	TCP パケットのチェックサム検証が失敗したことを検出します。
IP 移動による **CPU** 使用率の向上	多数の Mac を更新する必要があるかどうかを検出します。
過剰なパケットステアリング	非対称の RSS キータイプの使用により、高レベルのソフトウェアパケットステアリングを検出します。
レイヤ **2** ループ	ネットワーク内のレイヤ 2 ループの存在を検出します。
タグ付き **VLAN** の不一致	タグなしインターフェイスでタグ付き VLAN パケットが受信されるタイミングを検出します。



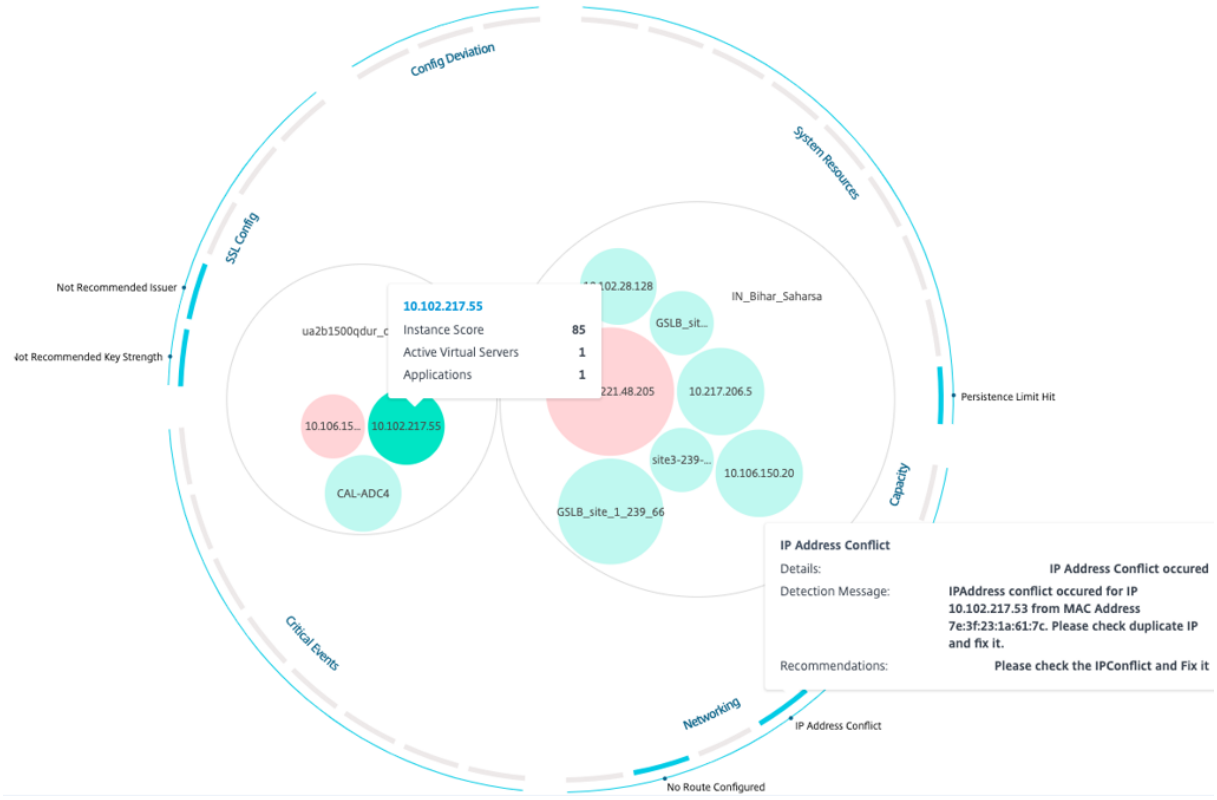
表形式ビュー

Inf **rastructure Analytics** の表形式表示オプションを使用して、異常を表示することもできます。[ネットワーク] > [インフラストラクチャ分析] に移動し、 をクリックしてすべての管理対象インスタンスを表示します。 › をクリックすると、異常の詳細が表示されます。



異常の詳細を表示する

たとえば、ネットワーク内の **IP** アドレスの競合の詳細を表示する場合は、IP アドレスの競合について表示される異常をクリックします。



- **Details** -検出された異常を示します。
- 検出メッセージ -IP アドレスが競合している MAC アドレスを示します。
- 推奨事項 -この IP アドレスの競合を解決するためのトラブルシューティング手順を示します

ハウツー記事

May 7, 2021

Citrix Application Delivery Management（Citrix ADM）「ハウツー記事」は、シンプルで関連性が高く、サービスで利用可能な機能に関する記事を簡単に実装できます。以下の記事では、インスタンス管理、構成管理、イベント管理、アプリケーション管理、StyleBooks、証明書管理など、一般的な Citrix ADM 機能の一部について説明します。

次の表で機能名をクリックすると、その機能の操作方法に関する記事の一覧が表示されます。

トピック		
インスタンス管理	構成管理	証明書管理機能
StyleBook	イベントの管理	

インスタンス管理

グローバルに分散したサイトを監視する方法

Citrix ADC インスタンスの管理パーティションを管理する方法

Citrix ADM にインスタンスを追加する方法

Citrix ADM でインスタンスグループを作成する方法

Citrix ADM で Citrix ADC インスタンスとエンティティをポーリングする方法

Citrix ADM でジオマップ用のサイトを構成する方法

セカンダリ Citrix ADC インスタンスにフェイルオーバーを強制する方法

セカンダリ Citrix ADC インスタンスを強制的にセカンダリ状態にする方法

Citrix ADC MPX または VPX ルートパスワードを変更する方法

Citrix ADC SDX ルートパスワードを変更する方法

構成管理

設定ジョブで SCP (put) コマンドを使用する方法

Citrix ADM を使用して Citrix ADC SDX インスタンスをアップグレードする方法

Citrix ADM 組み込みテンプレートを使用して作成されたジョブをスケジュールする方法

Citrix ADM 組み込みテンプレートを使用して構成されたジョブを再スケジュールする方法

実行構成ジョブを再利用する

Citrix ADM を使用して Citrix ADC インスタンスをアップグレードする方法

Citrix ADM で構成ジョブを作成する方法

Citrix ADM の構成ジョブで変数を使用する方法

構成テンプレートを使用して Citrix ADM で監査テンプレートを作成する方法

Citrix ADM 修正コマンドから構成ジョブを作成する方法

Citrix ADCitrix ADM 上のある Citrix ADC インスタンスから別のインスタンスに、実行および保存された構成コマンドを複製する方法

Citrix ADM で Citrix SD-WAN WO インスタンスの構成ジョブを作成する方法

構成ジョブを使用して、1 つのインスタンスから複数のインスタンスに構成をレプリケートする方法

Citrix ADM でマスター構成テンプレートを使用する方法

証明書管理機能

Citrix ADM でエンタープライズポリシーを構成する方法

Citrix ADM から Citrix ADC インスタンスに SSL 証明書をインストールする方法

Citrix ADM からインストールされた証明書を更新する方法

Citrix ADM を使用して SSL 証明書をリンクおよびリンク解除する方法

Citrix ADM を使用して証明書署名要求 (CSR) を作成する方法

Citrix ADM から SSL 証明書の有効期限の通知を設定する方法

Citrix ADM で SSL ダッシュボードを使用する方法

StyleBook

Citrix ADM でデフォルトのスタイルブックを使用する方法

独自のスタイルブックを作成する方法

Citrix ADM でユーザー定義のスタイルブックを使用する方法

API を使用して StyleBook から設定を作成する方法

StyleBook で定義された仮想サーバーで分析を有効にしてアラームを構成する方法

SSL 証明書と証明書キーファイルを Citrix ADM にアップロードするスタイルブックを作成する方法

ビジネス企業でスタイルブックの Microsoft Skype for Business を使用する方法

ビジネス企業で Microsoft Exchange スタイルブックを使用する方法

企業で Microsoft SharePoint スタイルブックを使用する方法

Microsoft ADFS プロキシスタイルブックを使用する方法

Oracle E-Business StyleBook の使用方法

SSO Office 365 スタイルブックの使用方法

SSOGoogle Apps 使い方 StyleBook

イベントの管理

Citrix ADM でイベントのイベント期間を設定する方法

Citrix ADM を使用してイベントフィルターをスケジュールする方法

Citrix ADM からのイベントに対して繰り返し電子メール通知を設定する方法

Citrix ADM を使用してイベントを抑制する方法

イベントダッシュボードを使用してイベントを監視する方法

Citrix ADM でイベントルールを作成する方法

Citrix ADC インスタンスで発生するイベントの報告された重大度を変更する方法

Citrix ADM でイベントの概要を表示する方法

Citrix ADM で SNMP トラップのイベントの重大度とスキューを表示する方法

Citrix ADM を使用して syslog メッセージをエクスポートする方法

Citrix ADM で Syslog メッセージを抑制する方法

よくあるご質問

May 7, 2021

インストールする必要があるエージェントの数はいくつですか?

エージェントの数は、データセンター内の管理対象インスタンスの数と総スループットによって異なります。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?

サービスに初めてログオンするときは、エージェントを 1 つだけインストールできます。複数のエージェントを追加するには、最初に初期セットアップを完了してから、**[設定]** > [エージェントの設定] に移動します。

組み込みエージェントから外部エージェントに移行できますか

はい、できます。詳しくは、「組み込みエージェントから外部エージェントへの移行」を参照してください。

新しいアクティベーションコードを紛失した場合、どうすれば入手できますか?

初めてオンボーディングする場合は、サービス GUI にアクセスし、[エージェントの設定] 画面に移動し、[アクティベーションコードの生成] をクリックします。

2 番目のエージェントをインストールするときに、新しいアクティベーションコードを生成するには、**[ネットワーク]** > **[エージェント]** > **[アクティベーションコードを生成]** に移動します。

エージェント仮想マシンにログオンするにはどうすればよいですか? デフォルトの認証情報は何ですか?

エージェントがハイパーバイザーまたは Microsoft Azure クラウドにインストールされている場合、ADM サービスエージェントの既定のログオン資格情報は`nsrecover`/`nsroot`で、エージェントのシェルプロンプトが開きます。

エージェントが AWS にインストールされている場合、Citrix ADM サービス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`/`instance id`です。

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リソース要件を教えてください

32 GB RAM、8 仮想 CPU、500 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

HA 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。

プロビジョニング中に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、追加の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 ADM とエンタープライズデータセンターまたはクラウド上のインスタンス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。

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。

間違った値を入力した場合、ネットワーク設定を再実行するにはどうすればよいですか

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

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ます。
- 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ます。

登録は成功しますが、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登録されたら、Citrix ADM にアクセスし、［エージェントの設定］画面に移動します。検出されたエージェントが画面に表示されます。エージェントが正常に動作している場合は、緑色のアイコンが表示されます。実行されていない場合は、赤いアイコンが表示されます。

プロキシサーバーを使用してエージェントを **Citrix ADM** に接続するにはどうすればよいですか?

プロキシサーバーを使用して、エージェントを Citrix ADM サービスに接続できます。エージェントは、すべてのデータをプロキシサーバーに転送し、インターネット経由で Citrix ADM にデータを送信します。

プロキシ・サーバを使用してデータを転送するには、次のスクリプトを使用してエージェント上のプロキシ・サーバの詳細を入力し、スクリプトの指示に従って詳細情報を入力します。proxy_input.py エージェントは、プロキシサーバーを使用して Citrix ADM に接続するときに、この情報を取得します。

ユーザー名とパスワード情報を入力して、プロキシサーバーを認証できます。エージェントがデータを送信すると、プロキシサーバーはユーザー資格情報を認証してから Citrix ADM に転送します。

> 注:
>
> プロキシサーバーは、基本認証のみをサポートしています。

アナリティクスレポートが表示されない

仮想サーバーで Insight を有効にして、アナリティクスレポートを表示します。詳しくは、「アナリティクスの有効化」を参照してください。

Citrix ADM ではどのバージョンの **Citrix ADC** インスタンスがサポートされていますか**?**

管理および監視機能では、10.5 以降を実行している Citrix ADC インスタンスがサポートされています。一部の機能は、特定の Citrix ADC バージョンでのみサポートされています。詳しくは、「システム要件」を参照してください。

Citrix ADM でダッシュボードレポートをエクスポートするにはどうすればよいですか

Citrix **ADM** でダッシュボードのレポートをエクスポートするには、このページの右上にある［エクスポート］アイコンをクリックします。[エクスポート] ページでは、次のいずれかの操作を実行できます。

1. [今すぐエクスポート] タブを選択します。レポートを PDF、JPEG、PNG、または CSV 形式で表示して保存します。
   レポートがシステムにダウンロードされます。
2. レポートを生成およびエクスポートするスケジュールを定期的に設定するには、[レポートのスケジュール] を選択します。レポート生成の繰り返し設定を指定し、レポートのエクスポート先のメールプロファイルを作成します。
   a) 繰り返し -ドロップダウンリストボックスから、[毎日]、[毎週]、または **[**毎月**]** を選択します。

   > 注
   >
   > - [毎週の繰り返し] を選択した場合は、レポートをスケジュールする平日を選択してください。
   > - [毎月の繰り返し] を選択した場合は、レポートをスケジュールするすべての日をカンマで区切って入力します。

   b) [繰り返し時刻]-時刻を 24 時間形式`Hour: Minute`で入力します。
   c) 電子メール -チェックボックスをオンにし、ドロップダウンリストボックスからプロファイルを選択するか、[追加] をクリックして電子メールプロファイルを作成します。
   d) **Slack** -チェックボックスをオンにし、ドロップダウンリストボックスからプロファイルを選択するか、[追加] をクリックして電子メールプロファイルを作成します。

   [スケジュールを有効にする] をクリックしてレポートをスケジュールし、[**OK**] をクリックします。[**Enable Schedule**] チェックボックスをオンにすると、選択したレポートを生成できます。

クライアント側の測定を有効にするにはどのような機能がありますか

クライアント側の測定を有効にすると、ADM は HTML インジェクションを通じて HTML ページのロード時間とレンダリング時間メトリックをキャプチャします。管理者は、これらのメトリックスを使用して、L7 レイテンシーの問題を特定できます。

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