Citrix Gateway 13.0

Machine translated content

Disclaimer

Contents

Citrix Gateway のリリースノート

March 26, 2020

リリースノートでは、特定のビルドでソフトウェアがどのように変更されたか、およびそのビルドに存在することがわかっている問題について説明します。

リリースノートドキュメントには、次のセクションのすべてまたは一部が含まれています。

- 新機能: ビルドでリリースされた拡張機能やその他の変更。
- 修正された問題: ビルドで修正される問題。
- 既知の問題: ビルドに存在する問題。
- 注: ビルドを使用する際に留意すべき重要な側面。
- 制限事項: ビルドに存在する制限事項。

> 注
>
> - 問題の説明の下の [# XXXXXX] ラベルは、Citrix ADC チームが使用する内部トラッキング ID です。
> - これらのリリースノートには、セキュリティ関連の修正は記載されていません。セキュリティに関する修正とアドバイスの一覧については、Citrix セキュリティ情報を参照してください。

最新のリリースノートのドキュメントを表示するには、リリースノートページを参照してください。

Citrix Gateway について

April 9, 2020

Citrix Gateway は導入が容易で、管理も簡単です。最も一般的な展開構成は、DMZ 内に Citrix Gateway アプライアンスを配置することです。複数の Citrix Gateway アプライアンスをネットワークにインストールすることで、より複雑な展開環境を実現できます。

Citrix Gateway を初めて起動するときは、シリアルコンソール、構成ユーティリティのセットアップウィザード、または動的ホスト構成プロトコル（DHCP）を使用して初期構成を実行できます。MPX アプライアンスでは、アプライアンスの前面パネルにある LCD キーパッドを使用して初期構成を実行できます。IP アドレス、サブネットマスク、デフォルト Gateway IP アドレス、ドメインネームシステム (DNS) アドレスなど、内部ネットワークに固有の基本設定を構成できます。基本的なネットワーク設定を構成したら、認証、承認、ネットワークリソース、仮想サーバー、セッションポリシー、エンドポイントポリシーのオプションなど、Citrix Gateway の操作に固有の設定を構成します。

Citrix Gateway をインストールして構成する前に、このセクションのトピックを参照して、展開を計画してください。導入計画には、アプライアンスのインストール場所の決定、DMZ への複数のアプライアンスのインストール方法の理解、およびライセンス要件が含まれます。Citrix Gateway は、セキュリティで保護されたネットワークで実行されている既存のハードウェアやソフトウェアを変更することなく、あらゆるネットワークインフラストラクチャに

インストールできます。Citrix Gateway は、サーバーロードバランサー、キャッシュエンジン、ファイアウォール、ルーター、IEEE 802.11 ワイヤレスデバイスなど、他のネットワーク製品と連携します。

Citrix Gateway を構成する前に、インストール前のチェックリストに設定を書き込むことができます。

Citrix Gateway アプライアンス	Citrix Gateway アプライアンスおよびアプライアンスのインストール手順について説明します。
インストール前のチェックリスト	ネットワークに Citrix Gateway をインストールする前に確認する計画情報と、完了する必要のあるタスクの一覧を示します。
一般的な展開	ネットワーク DMZ への Citrix Gateway の導入、DMZ のない安全なネットワークへの展開、および負荷分散とフェイルオーバーをサポートする追加のアプライアンスに関する情報を提供します。また、Citrix Virtual Apps and Desktops を使用した Citrix Gateway の展開についても説明します。
ライセンス	アプライアンスへのライセンスのインストールに関する情報を提供します。また、複数の Citrix Gateway アプライアンスへのライセンスのインストールについても説明します。

Citrix Gateway アーキテクチャ

April 9, 2020

Citrix Gateway のコアコンポーネントは次のとおりです。

- 仮想サーバ。Citrix Gateway 仮想サーバーは、ユーザーが利用できるすべての構成済みサービスを代表する内部エンティティです。仮想サーバは、ユーザがこれらのサービスにアクセスするためのアクセスポイントでもあります。1 つのアプライアンスに複数の仮想サーバーを構成して、1 つの Citrix Gateway アプライアンスが異なる認証およびリソースアクセス要件を持つ複数のユーザーコミュニティにサービスを提供できるようにすることができます。
- 認証、認可、アカウンティング。認証、承認、アカウンティングを構成すると、Citrix Gateway または LDAP や RADIUS などの安全なネットワークにある認証サーバーが認識する資格情報を使用して、ユーザーが Citrix Gateway にログオンできるようになります。承認ポリシーは、ユーザーのアクセス許可を定義し、特定のユーザーがアクセスを許可するリソースを決定します。認証と認可の詳細については、認証と承認を参照してください。アカウンティングサーバーは、ユーザーログオンイベント、リソースアクセスインスタンス、操作エ

ラーなど、Citrix Gateway アクティビティに関するデータを保持します。この情報は、Citrix Gateway または外部サーバーに保存されます。アカウンティングの詳細については、「Citrix Gateway での監査の構成」を参照してください。

- ユーザー接続。ユーザーは、次のアクセス方法を使用して Citrix Gateway にログオンできます。
  - Windows 用の Citrix Gateway プラグインは、Windows ベースのコンピュータにインストールされるソフトウェアです。ユーザーは、Windows ベースのコンピューター上の通知領域のアイコンを右クリックしてログオンします。Citrix Gateway プラグインがインストールされていないコンピューターを使用している場合は、Web ブラウザーを使用してログオンし、プラグインをダウンロードしてインストールできます。ユーザーが Citrix Workspace アプリをインストールしている場合、ユーザーは Citrix Workspace アプリから Citrix Gateway プラグインを使用してログオンします。Citrix Workspace アプリと Citrix Gateway プラグインがユーザーデバイスにインストールされている場合、Citrix Workspace アプリは自動的に Citrix Gateway プラグインを追加します。
  - Mac OS X を実行しているユーザーがログオンできるようにする、Mac OS X 用の Citrix Gateway プラグイン。これは、Windows 用の Citrix Gateway プラグインと同じ機能と機能を備えています。Citrix ADC Gatway 10.1、ビルド 120.1316.e をインストールすることで、このプラグインバージョンのエンドポイント分析のサポートを提供できます。
  - Java 用 Citrix Gateway プラグイン。Mac OS X、Linux、およびオプションで、Windows ユーザーが Web ブラウザーを使用してログオンできるようにします。
  - Web Interface または Citrix StoreFront を使用して、サーバーファーム内の公開アプリケーションおよび仮想デスクトップへのユーザー接続を許可する Citrix Workspace アプリ。
  - Citrix Workspace アプリ、Secure Hub、WorxMail、および WorxWeb を使用して、ユーザーが Web アプリケーション、SaaS アプリケーション、iOS および Android モバイルアプリ、および Citrix Endpoint Management でホストされている ShareFile データにアクセスできます。
  - ユーザーは、Citrix Gateway の Web アドレスを使用する Android デバイスから接続できます。ユーザーがアプリを起動すると、接続は Micro VPN を使用してネットワークトラフィックを内部ネットワークにルーティングします。ユーザーが Android デバイスから接続する場合は、Citrix Gateway で DNS 設定を構成する必要があります。詳しくは、「Android デバイスで DNS サフィックスを使用した DNS クエリのサポート」を参照してください。
  - ユーザーは、Citrix Gateway の Web アドレスを使用する iOS デバイスから接続できます。Secure Browse は、グローバルまたはセッションプロファイルで構成します。ユーザーが iOS デバイスでアプリを起動すると、VPN 接続が開始され、Citrix Gateway 経由で接続がルーティングされます。
  - クライアントレスアクセス。ユーザーデバイスにソフトウェアをインストールしなくても、必要なアクセスをユーザーに提供します。

    Citrix Gateway を構成するときに、ポリシーを作成してユーザーのログオン方法を設定できます。セッションおよびエンドポイントの分析ポリシーを作成して、ユーザーのログオンを制限することもできます。

- ネットワークリソース。これには、ファイルサーバー、アプリケーション、Web サイトなど、ユーザーが Citrix Gateway 経由でアクセスするすべてのネットワークサービスが含まれます。
- 仮想アダプタ。Citrix Gateway 仮想アダプタは、IP スプーフィングを必要とするアプリケーションをサポートします。仮想アダプタは、Citrix Gateway プラグインのインストール時にユーザーデバイスにインストールされます。ユーザーが内部ネットワークに接続すると、Citrix Gateway と内部サーバー間の送信接続では、イントラネット IP アドレスが送信元 IP アドレスとして使用されます。Citrix Gateway プラグインは、構成の一部としてサーバーからこの IP アドレスを受け取ります。

  Citrix Gateway で分割トンネリングを有効にすると、すべてのイントラネットトラフィックが仮想アダプタ経由でルーティングされます。イントラネットにバインドされたトラフィックを代行受信する場合、仮想アダプタは A および AAAA レコードタイプ DNS クエリーをインターセプトし、その他すべての DNS クエリーはそのまま残します。内部ネットワークにバインドされていないネットワークトラフィックは、ユーザーデバイスにインストールされているネットワークアダプタを介してルーティングされます。インターネットおよびプライベートローカルエリアネットワーク (LAN) 接続は開いたままであり、接続されたままです。分割トンネリングを無効にすると、すべての接続が仮想アダプタを介してルーティングされます。既存の接続はすべて切断され、ユーザーはセッションを再確立する必要があります。

  イントラネット IP アドレスを構成すると、内部ネットワークへのトラフィックは、仮想アダプタを介してイントラネット IP アドレスでスプーフィングされます。

ユーザー接続の仕組み

March 26, 2020

ユーザーは、リモートロケーションから自分の電子メール、ファイル共有、およびその他のネットワークリソースに接続できます。ユーザーは、次のソフトウェアを使用して内部ネットワークリソースに接続できます。

- Citrix Gateway プラグイン
- Citrix Workspace アプリ
- WorxMail および WorxWeb
- Android と iOS のモバイルデバイス

Citrix Gateway プラグインを使用した接続

Citrix Gateway プラグインを使用すると、次の手順で内部ネットワークのリソースにユーザーがアクセスできます。

1. ユーザーは、Web ブラウザーで Web アドレスを入力して Citrix Gateway に初めて接続します。ログオンページが表示され、ユーザー名とパスワードを入力するよう求められます。外部認証サーバーが構成されている場合、Citrix Gateway はサーバーに接続し、認証サーバーはユーザーの資格情報を確認します。ローカル認証が構成されている場合、Citrix Gateway はユーザー認証を実行します。

2. 事前認証ポリシーを構成する場合、ユーザーが Windows ベースのコンピューターまたは Mac OS X コンピューターの Web ブラウザーで Citrix Gateway の Web アドレスを入力すると、ログオンページが表示される前に、クライアントベースのセキュリティポリシーが設定されているかどうかが Citrix Gateway によって確認されます。セキュリティチェックでは、オペレーティングシステムの更新、ウイルス対策保護、適切に構成されたファイアウォールなど、ユーザーデバイスがセキュリティ関連の条件を満たしていることを確認します。ユーザーデバイスがセキュリティチェックに失敗した場合、Citrix Gateway はユーザーのログオンをブロックします。ログオンできないユーザーは、必要な更新プログラムまたはパッケージをダウンロードし、ユーザーデバイスにインストールする必要があります。ユーザーデバイスが事前認証ポリシーを通過すると、ログオンページが表示され、ユーザーは自分の資格情報を入力できます。Citrix Gateway 10.1、ビルド 120.1316.e をインストールする場合は、Mac OS X コンピューターで高度なエンドポイント分析を使用できます。
3. Citrix Gateway がユーザーの認証に成功すると、VPN トンネルが開始されます。Citrix Gateway では、Windows 用の Citrix Gateway プラグインまたは Mac OS X 用の Citrix Gateway プラグインをダウンロードしてインストールするように求められます。Java 用の Network Gateway プラグインを使用している場合は、ユーザーデバイスも事前に構成されたリソース IP アドレスとポート番号のリストで初期化されます。
4. 認証後のスキャンを構成すると、ユーザーが正常にログオンすると、Citrix Gateway はユーザーデバイス上で必要なクライアントセキュリティポリシーをスキャンします。事前認証ポリシーと同じセキュリティ関連の条件を要求できます。ユーザーデバイスがスキャンに失敗した場合、ポリシーが適用されないか、ユーザーが検疫グループに配置され、ユーザーのネットワークリソースへのアクセスが制限されます。
5. セッションが確立されると、ユーザーは Citrix Gateway のホームページにリダイレクトされ、ユーザーはアクセスするリソースを選択できます。Citrix Gateway に含まれているホームページをアクセスインターフェイスと呼びます。ユーザーが Windows 用の Citrix Gateway プラグインを使用してログオンすると、Windows デスクトップの通知領域にアイコンが表示され、ユーザーが接続されていることを示すメッセージがユーザーに表示されます。また、ユーザーは、Microsoft Outlook を開いたり、電子メールを取得したりするなど、アクセスインターフェイスを使用せずにネットワーク上のリソースにアクセスすることもできます。
6. ユーザー要求が事前認証と認証後の両方のセキュリティチェックに合格した場合、Citrix Gateway は要求されたリソースに接続し、ユーザーデバイスとそのリソース間の安全な接続を開始します。
7. ユーザーは、Windows ベースのコンピューターの通知領域で Citrix Gateway アイコンを右クリックし、[ログオフ] をクリックすると、アクティブなセッションを閉じることができます。セッションは、非アクティブが原因でタイムアウトすることもあります。セッションが閉じられると、トンネルはシャットダウンされ、ユーザは内部リソースにアクセスできなくなります。ユーザーは、ブラウザーで Citrix Gateway の Web アドレスを入力することもできます。ユーザーが Enter キーを押すと、ユーザーがログオフできるアクセスインターフェイスが表示されます。

注：内部ネットワークに Citrix Endpoint Management を展開する場合は、内部ネットワークの外部から接続するユーザーが最初に Citrix Gateway に接続する必要があります。ユーザーが接続を確立すると、ユーザーは Web アプリケーションおよび SaaS アプリケーション、Android および iOS モバイルアプリ、および Citrix Endpoint Management でホストされている ShareFile データにアクセスできます。ユーザーは、クライアントレスアクセスまたは Citrix Workspace アプリまたは Secure Hub を使用して、Citrix Gateway プラグインを使用して接続できます。

Citrix Workspace アプリとの接続

ユーザーは、Citrix Workspace アプリに接続して、Windows ベースのアプリケーションと仮想デスクトップにアクセスできます。ユーザーは、Endpoint Management からアプリケーションにアクセスすることもできます。リモートの場所から接続するには、Citrix Gateway プラグインもデバイスにインストールします。Citrix Workspace アプリは、Citrix Gateway プラグインをプラグインの一覧に自動的に追加します。ユーザーは、Citrix Workspace アプリにログオンするときに、Citrix Gateway プラグインにもログオンできます。また、ユーザーが Citrix Gateway Workspace アプリにログオンするときに、Citrix Gateway プラグインへのシングルサインオンを実行するように Citrix Gateway を構成することもできます。

iOS デバイスと **Android** デバイスとの接続

ユーザーは、Secure Hub を使用して iOS または Android デバイスから接続できます。ユーザーは、Secure Mail を使用して電子メールにアクセスし、WorxWeb を使用して Web サイトに接続できます。

ユーザーがモバイルデバイスから接続する場合、接続は Citrix Gateway を介して内部リソースにアクセスします。ユーザーが iOS に接続する場合は、セッションプロファイルの一部として「Secure Browse」を有効にします。ユーザーが Android で接続する場合、接続は自動的にマイクロ VPN を使用します。さらに、
Secure Mail と WorxWeb は、マイクロ VPN を使用して Citrix Gateway を介して接続を確立します。Citrix Gateway でマイクロ VPN を構成する必要はありません。

一般的な展開

April 9, 2020

組織の内部ネットワーク（またはイントラネット）の境界に Citrix Gateway を展開して、内部ネットワークに存在するサーバー、アプリケーション、およびその他のネットワークリソースへの安全な単一アクセスポイントを提供できます。すべてのリモートユーザーは、内部ネットワーク上のリソースにアクセスする前に、Citrix Gateway に接続する必要があります。

Citrix Gateway は、通常、ネットワーク内の次の場所にインストールされます。

- ネットワーク DMZ で
- DMZ< を持たないセキュアなネットワークの場合

また、Citrix Virtual Apps、Citrix Virtual Desktops、StoreFront、および Citrix Endpoint Management を使用して Citrix Gateway を展開して、ユーザーが Windows、Web、モバイル、SaaS アプリケーションにアクセスできるようにすることもできます。展開環境に Citrix Virtual Apps、StoreFront、デスクトップ 7 が含まれている場合は、シングルホップまたはダブルホップの DMZ 構成で Citrix Gateway を展開できます。ダブルホップ展開は、以前のバージョンの Citrix Virtual Desktops または Citrix Endpoint Management ではサポートされません。

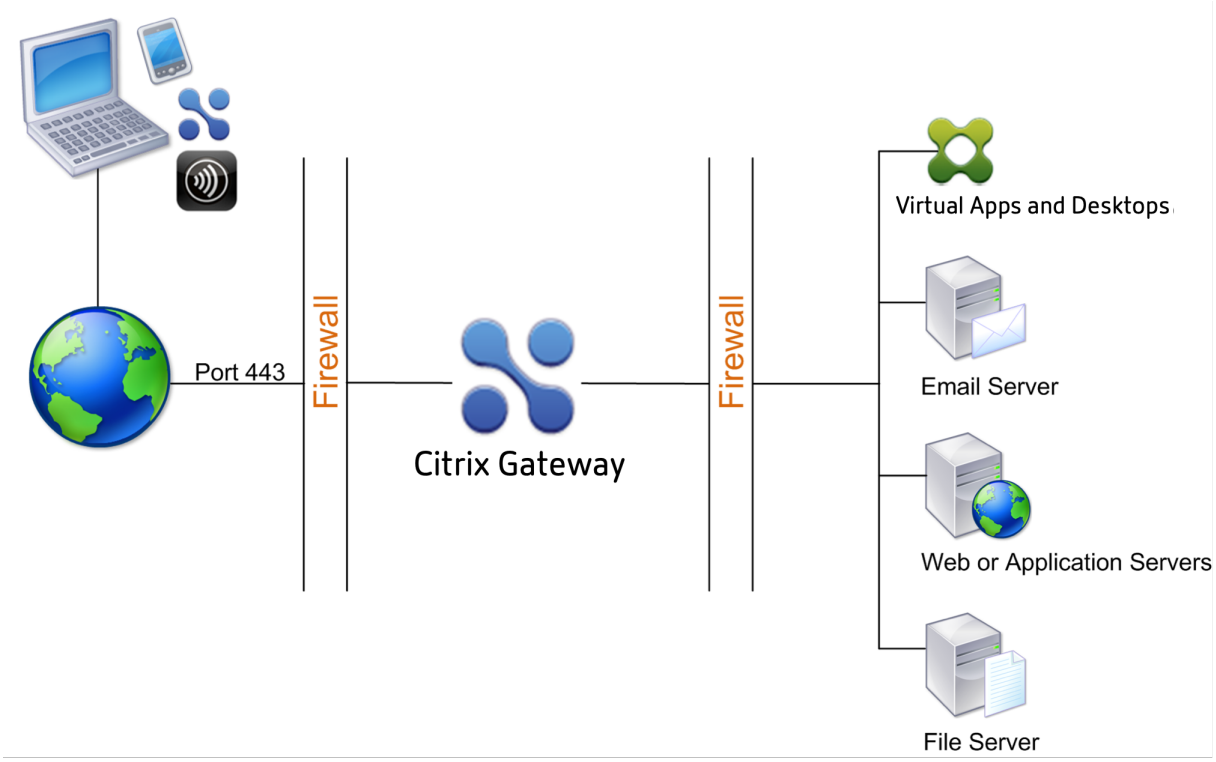
これらの Citrix ソリューションおよびサポートされているその他の Citrix ソリューションを使用して Citrix Gateway インストールを拡張する方法の詳細については、Citrix 製品との統合トピックを参照してください。

DMZ でのデプロイ

March 26, 2020

多くの組織は、DMZ を使用して内部ネットワークを保護します。DMZ は、組織の安全な内部ネットワークとインターネット (または任意の外部ネットワーク) の間にあるサブネットです。DMZ に Citrix Gateway を展開すると、ユーザーは Citrix Gateway プラグインまたは Citrix Workspace アプリを使用して接続します。

図 1: DMZ にデプロイされた Citrix Gateway



前の図に示す構成では、DMZ に Citrix Gateway をインストールし、インターネットと内部ネットワークの両方に接続するように構成します。

DMZ での Citrix Gateway 接続

DMZ に Citrix Gateway を展開する場合、ユーザー接続は最初のファイアウォールを通過して Citrix Gateway に接続する必要があります。デフォルトでは、ユーザー接続はポート 443 で SSL を使用してこの接続を確立します。内部ネットワークへのユーザー接続を許可するには、最初のファイアウォールを介してポート 443 で SSL を許可する必要があります。

Citrix Gateway は、ユーザーデバイスからの SSL 接続を復号化し、ユーザーの代わりに 2 番目のファイアウォールの背後にあるネットワークリソースへの接続を確立します。2 番目のファイアウォールを介して開く必要があるポートは、外部ユーザーにアクセスを許可するネットワークリソースによって異なります。

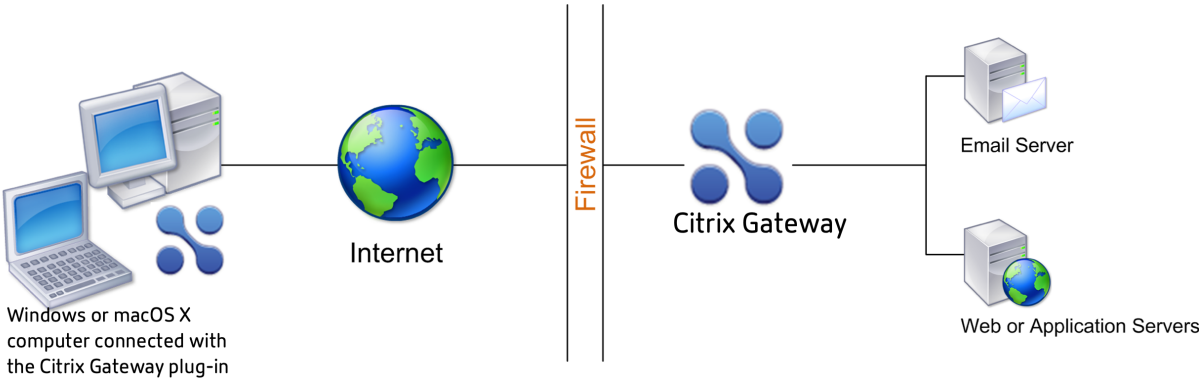
たとえば、外部ユーザに内部ネットワーク内の Web サーバへのアクセスを許可し、このサーバがポート 80 で HTTP 接続をリッスンする場合、ポート 80 で HTTP を 2 番目のファイアウォール経由で許可する必要があります。Citrix Gateway は、外部ユーザーデバイスの代わりに、2 番目のファイアウォールを経由して内部ネットワーク上の HTTP サーバーへの接続を確立します。

セキュリティで保護されたネットワークでの展開

March 26, 2020

Citrix Gateway は、セキュリティで保護されたネットワークにインストールできます。このシナリオでは、1 つのファイアウォールがインターネットとセキュリティで保護されたネットワークの間にあります。Citrix Gateway は、ネットワークリソースへのアクセスを制御するためにファイアウォール内に存在します。

図 1: セキュアなネットワークにデプロイされた Citrix Gateway



Citrix Gateway をセキュリティで保護されたネットワークに展開する場合は、Citrix Gateway 上の 1 つのインターフェイスをインターネットに接続し、もう 1 つのインターフェイスをセキュリティで保護されたネットワークで実行されているサーバーに接続します。Citrix Gateway を安全なネットワークに置くと、ローカルユーザーおよびリモートユーザーにアクセスできるようになります。ただし、この構成にはファイアウォールが 1 つしかないため、では、リモートロケーションから接続するユーザに対する配置の安全性が低下します。Citrix Gateway はインターネットからのトラフィックを傍受しますが、トラフィックはセキュリティで保護されたネットワークに入ってからユーザーを認証します。Citrix Gateway を DMZ に展開すると、ネットワークトラフィックが安全なネットワークに到達する前にユーザーが認証されます。

Citrix Gateway をセキュアなネットワークに展開する場合、Citrix Gateway プラグイン接続はファイアウォールを通過して Citrix Gateway に接続する必要があります。デフォルトでは、ユーザー接続はポート 443 で SSL プロトコルを使用してこの接続を確立します。この接続をサポートするには、ファイアウォールでポート 443 を開く必要があります。

クライアントソフトウェアの要件

March 26, 2020

このセクションでは、Citrix Gateway クライアントソフトウェアのシステム要件について説明します。

Citrix Gateway では、Citrix Gateway プラグインを使用したユーザー接続がサポートされます。ユーザーがプラグインを使用してログオンすると、完全な VPN トンネルが確立されます。Citrix Gateway プラグインを使用すると、ユーザーはアクセスを許可するネットワークリソースに接続して操作できます。

Citrix Gateway でエンドポイントポリシーを構成する場合、ユーザーがログオンすると、Citrix Gateway によってエンドポイント分析プラグインが自動的にダウンロードされ、ユーザーデバイスにインストールされます。

Citrix Gateway プラグインのシステム要件

March 26, 2020

Citrix Gateway プラグインは、クライアントマシンから Citrix Gateway アプライアンスへの安全な接続を確立します。

このプラグインは、Microsoft Windows、macOS X、および Linux オペレーティングシステム用のデスクトップアプリとして配布されます。Web ブラウザで Citrix Gateway アプライアンスのセキュアな URL を認証すると、プラグインがダウンロードされ、マシンに自動的にインストールされます。

プラグインは、Android および iOS デバイス用のモバイルアプリとしてプロビジョニングされます。

注：プラグインをインストールするには、オペレーティングシステムで admin 権限または root 権限が必要です。

デスクトップアプリケーションとしての Citrix Gateway プラグインは、以下のオペレーティングシステムと Web ブラウザーでサポートされています。

オペレーティングシステム	サポートされているブラウザー
macOS X (10.9 以降)	Safari 7.1 以降、Google Chrome Release 30 以降、Mozilla Firefox Release 30 以降
Windows 10 (x86 および x64)	Internet Explorer 11、Google Chrome Release 30 以降、Mozilla Firefox Release 24 以降、Edge Chromium
Windows 8.1	Internet Explorer 11、Google Chrome Release 30 以降、Mozilla Firefox Release 24 以降、Edge Chromium

オペレーティングシステム	サポートされているブラウザー
Windows 8	Internet Explorer 9 および 10、Google Chrome Release 30 以降、Mozilla Firefox Release 24 以降、Edge Chromium
Windows 7	Internet Explorer 9、10、11、Google Chrome Release 30 以降、Mozilla Firefox Release 24 以降、Edge Chromium
Linux、Ubuntu 18.04 LTS、16.04 LTS、14.04 LTS、12.04 LTS. 32 ビットおよび 64 ビット OS がサポートされています。	Mozilla Firefox Release 44 以降、Google Chrome 50 以降

> 重要: Ubuntu 16.04 LTS のバグ（1573408）により、VPN プラグインのインストールが失敗します。同じ場合の回避策は、次のようにリストされます。

コマンドラインインターフェイスを使用して次のコマンドを入力します。

```
sudo dpkg -i nsgclient*.deb
<!--NeedCopy-->
```

必要な依存関係パッケージが見つからない場合、コマンドはそれらを一覧表示し、プラグインのインストールは失敗します。これらの依存関係パッケージは手動でインストールする必要があります。管理者は、コマンドラインインターフェイスを使用して次のコマンドを入力して、不足しているパッケージをインストールできます。

```
apt-get install <dependency package>
<!--NeedCopy-->
```

モバイルアプリとしての Citrix Gateway プラグインは、以下のオペレーティングシステムでサポートされています。

VPN アプリ	サポートされるオペレーティングシステム
Android	Android 4.1 以降
iOS	iOS 8 以降

エンドポイント分析の要件

March 26, 2020

Citrix Gateway がユーザーデバイスにエンドポイント分析プラグインをインストールすると、プラグインによって

ユーザーデバイスがスキャンされ、Citrix Gateway で設定したエンドポイントのセキュリティ要件が確認されます。要件には、オペレーティングシステム、ウイルス対策、Web ブラウザーのバージョンなどの情報が含まれます。

Windows ユーザーがブラウザを使用して Citrix Gateway に初めて接続する場合、ポータルはエンドポイント分析プラグインのインストールを要求します。その後のログオン試行時に、プラグインはアップグレード制御構成をチェックし、クライアントエンドポイント分析プラグインのアップグレードが必要かどうかを判断します。必要であれば、新しい Endpoint Analysis プラグインをダウンロードしてインストールするかどうかを確認するメッセージが表示されます。Windows 用エンドポイント分析プラグインは、Windows 32 ビットアプリケーションとしてインストールされます。インストールまたは使用に特別な権限は必要ありません。

Mac OS X の場合、ユーザーはエンドポイント分析プラグインをインストールする必要があります。Mac OS X 用のプラグインは、32 ビットアプリケーションとしてインストールされます。インストールに特別な権限は必要ありません。その後のログオン試行時に、プラグインのバージョンが一致しない場合、プラグインをダウンロードしてインストールするように求められます。

Endpoint Analysis プラグインを使用するには、ユーザーデバイスに以下のソフトウェアが必要です。

オペレーティングシステム	サポートされているブラウザー
–	–
Mac OS X (10.9 以降)	Safari 7.1 以降、Google Chrome Release 30 以降、Mozilla Firefox Release 30 以降
Windows 10	Internet Explorer 11、Google Chrome Release 30 以降、Mozilla Firefox Release 24 以降、Microsoft Edge はサポートされません。
Windows 8.1	Internet Explorer 11、Google Chrome Release 30 以降、Mozilla Firefox Release 24 以降
Windows 8	Internet Explorer 9 および 10、Google Chrome Release 30 以降、Mozilla Firefox Release 24 以降
Windows 7	Internet Explorer 9 および 10 および 11、Google Chrome Release 30 以降、Mozilla Firefox Release 24 以降
Windows Vista	Internet Explorer 9; Mozilla Firefox Release 9 および 10
Linux; Ubuntu 12.04 LTS、14.04 LTS、16.04 LTS
注: 32 ビットおよび 64 ビット OS がサポートされています。	Mozilla Firefox Release 44 以降、Google Chrome 50 以降

** 注 1: 上記のオペレーティングシステムバリアント ** のすべてのエディションがサポートされています。

注 **2:** Windows エディションでは、すべてのサービスパックと重要な更新プログラムをインストールする必要があります。

** 注 3: Internet Explorer のバージョン ** では、クッキーを有効にする必要があります。最低限必要なバージョンは 7.0 です。

** 注 4:** Mozilla Firefox のバージョンでは、エンドポイント分析はプラグインを有効にする必要があり、最低限必要なバージョンは 3.0 です。

重要: 認証前エンドポイント分析の場合、ユーザーがユーザーデバイスに Endpoint Analysis プラグインをインストールしていない場合、またはスキャンをスキップした場合、ユーザーは Citrix Gateway プラグインを使用し

てログオンできません。認証後のエンドポイント分析の場合、ユーザーはクライアントレスアクセスまたは Citrix Workspace アプリを使用して、スキャンが不要なリソースにアクセスできます。

Citrix 製品との互換性

March 26, 2020

次の表に、Citrix 製品および Citrix Gateway 13.0 と互換性があるバージョンを示します。

> 注： Citrix Gateway の機能は、Citrix ADC VPX で使用できます。

Citrix 製品とサポートされているバージョン

Citrix 製品	リリースバージョン
Citrix SD-WAN	10.2, 11.0
Citrix ADC ADC プラットフォーム	FIPS 準拠のアプライアンスを含む、現在のすべての MPX および VPX モデル。
StoreFront	3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14, 3.15
Web Interface	5.4
Citrix Virtual Apps and Desktops	7.6, 7.12, 7.13, 7.14, 7.15, 7.16, 7.17, 7.18
XenMobile	10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12

> 注： Citrix XenApp 6.5 がサポートされています。

Citrix Workspace アプリ、Citrix モバイル生産性アプリ、およびプラグイン

Citrix Workspace アプリまたはプラグイン	サポートされる最小バージョン
Citrix Gateway プラグイン (macOS X)	3.1.8
Windows 向け Citrix Gateway プラグイン	12.0
iOS 用 Citrix Gateway プラグイン	3.1.4
Android 向け Citrix Gateway プラグイン	2.0.14
Android 向け Citrix Workspace アプリ	3.11
iOS 向け Citrix Workspace アプリ	7.1.3

Citrix Workspace アプリまたはプラグイン	サポートされる最小バージョン
Mac 向け Citrix Workspace アプリ	12.4
Windows 向け Citrix Workspace アプリ	4.4
Linux 向け Citrix Workspace アプリ	13.4
HTML5 向け Citrix Workspace アプリ	2.3
Chrome 用 Citrix Workspace アプリ	2.3
Secure Hub for iOS	10.5
Secure Hub for Android	10.5
Secure Mail for iOS	10.5
SecureWeb for iOS	10.5
Secure Mail for Android	10.5
SecureWeb for Android	10.5

WindowsGateway プラグインでサポートされる **Citrix Gateway** 機能

Citrix Gateway 13.0 ビルド 36.27 以降では、以下の機能がサポートされています。

- デバイスガードのサポート
- n ファクターのサポート
- Opswat v4 のサポート
- SAML のサポート
- AlwaysOn オンサービス

ライセンス

March 26, 2020

Citrix Gateway を展開してユーザー接続をサポートするには、アプライアンスのライセンスを適切に取得する必要があります。

> 重要：受け取ったすべてのライセンスファイルのコピーをローカルに保存しておくことをお勧めします。構成ファイルのバックアップコピーを保存すると、アップロードしたすべてのライセンスファイルもバックアップに含まれます。Citrix Gateway アプライアンスソフトウェアを再インストールする必要があり、構成のバックアップがない場合は、元のライセンスファイルが必要になります。

Citrix Gateway にライセンスをインストールする前に、アプライアンスのホスト名を設定してから、Citrix Gateway

を再起動してください。セットアップウィザードを使用して、ホスト名を構成します。Citrix Gateway のユニバーサルライセンスを生成すると、ホスト名がそのライセンスで使用されます。

Citrix Gateway のライセンスの種類

March 26, 2020

Citrix Gateway にはプラットフォームライセンスが必要です。プラットフォームライセンスでは、ICA プロキシを使用して Citrix Virtual Apps、Citrix Virtual Desktops、または StoreFront への無制限の接続が可能です。Citrix Gateway プラグイン、SmartAccess ログオンポイント、または Secure Hub、WorxWeb、または Secure Mail からの VPN 接続を許可するには、ユニバーサルライセンスも追加する必要があります。Citrix Gateway VPX には、プラットフォームライセンスが付属しています。

プラットフォームライセンスは、以下の Citrix Gateway バージョンでサポートされています。

- Citrix Gateway 13.0
- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1
- NetScaler Gateway 11.0
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10
- Citrix ADC VPX

重要：受け取ったすべてのライセンスファイルのコピーをローカルに保存しておくことをお勧めします。構成ファイルのバックアップコピーを保存すると、アップロードされたすべてのライセンスファイルがバックアップに含まれます。Citrix Gateway アプライアンスソフトウェアを再インストールする必要があり、構成のバックアップがない場合は、元のライセンスファイルが必要です。

プラットフォームライセンス

プラットフォームライセンスでは、Citrix Virtual Apps 上の公開アプリケーションまたは Citrix Virtual Desktops からの仮想デスクトップへの無制限のユーザー接続が可能です。Citrix Workspace アプリを使用した接続では、Citrix Gateway ユニバーサルライセンスは使用されません。これらの接続に必要なのは、プラットフォームライセンスのみです。プラットフォームライセンスは、物理ライセンスと仮想ライセンスにかかわらず、新しい Citrix Gateway のすべての注文とともに電子的に提供されます。保証契約または保守契約の対象となるアプライアンスをすでに所有している場合は、シトリックス Web サイトからプラットフォームライセンスを取得できます。

> 重要：プラットフォームライセンスに基づき、次の数のユニバーサルライセンスが含まれています。
>
> - スタンダードエディション — 500
> - アドバンスドエディション — 1000
> - プレミアム — 無制限

ユニバーサルライセンス

ユニバーサルライセンスでは、同時ユーザーセッションの数は、購入したライセンス数に制限されます。

ユニバーサルライセンスでは、次の機能がサポートされています。

- 完全 VPN トンネル
- マイクロ VPN
- エンドポイント解析
- ポリシーベースの SmartAccess
- Web サイトやファイル共有へのクライアントレスアクセス

Standard エディションのライセンスを購入すると、いつでも 500 の同時セッションを持つことができます。ユーザーがセッションを終了すると、そのライセンスは次のユーザーのために解放されます。複数のコンピューターから Citrix Gateway にログオンするユーザーは、セッションごとにライセンスを占有します。

すべてのライセンスが使用されている場合、ユーザーがセッションを終了するか、セッションを終了するまで、追加の接続を開くことはできません。接続が閉じられると、ライセンスが解放され、新しいユーザーが使用できるようになります。

Citrix Gateway アプライアンスを受け取ると、ライセンスは次の順序で行われます。

- ライセンス認証コード (LAC) が電子メールで送信されます。
- セットアップウィザードを使用して、ホスト名で Citrix Gateway を構成します。
- Citrix のウェブサイトから Citrix Gateway のライセンスを割り当てます。ホスト名を使用して、割り当てプロセス中にライセンスをアプライアンスにバインドします。
- ライセンスファイルは、Citrix Gateway にインストールします。

ユニバーサルライセンスの詳細については、Citrix Gateway ユニバーサルライセンスを参照してください。

プラットフォームまたはユニバーサルライセンスファイルの入手

March 26, 2020

Citrix Gateway をインストールすると、Citrix からプラットフォームまたはユニバーサルライセンスファイルを入手できます。Citrix の Web サイトにログオンして、使用可能なライセンスにアクセスし、ライセンスファイルを生成します。ライセンスファイルが生成されたら、コンピュータにダウンロードします。ライセンスファイルがコ

ンピューター上に存在したら、Citrix Gateway にアップロードします。Citrix ライセンスサーバーについて詳しくは、「Citrix ライセンスシステム」を参照してください。

ライセンスファイルを取得する前に、セットアップウィザードを使用してアプライアンスのホスト名を構成してから、アプライアンスを再起動してください。

重要：ライセンスは Citrix Gateway にインストールする必要があります。アプライアンスは、Citrix ライセンスサーバーからライセンスを取得しません。

ライセンスを取得するには、Citrix ライセンスのアクティブ化、アップグレード、管理Web ページに移動します。このページでは、新しいライセンスを取得し、Citrix ライセンスのライセンス認証、アップグレード、管理を行うことができます。

Citrix Gateway にライセンスをインストールするには

March 26, 2020

ライセンスファイルをコンピューターに正常にダウンロードしたら、Citrix Gateway にライセンスをインストールできます。ライセンスは /nsconfig/license ディレクトリにインストールされます。

セットアップウィザードを使用して Citrix Gateway の初期設定を構成した場合、ウィザードの実行時にライセンスファイルがインストールされます。ライセンスの一部を割り当てた後、後で追加番号を割り当てる場合は、セットアップウィザードを使用せずにライセンスをインストールできます。

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[システム] を展開し、[ライセンス] をクリックします。
2. 詳細ウィンドウで、[ライセンスの管理] をクリックします。
3. [新しいライセンスの追加] をクリックし、[参照] をクリックしてライセンスファイルに移動し、[OK] をクリックします。

   構成ユーティリティに、Citrix Gateway を再起動する必要があるというメッセージが表示されます。[再起動] をクリックします。

最大ユーザー数を設定するには

アプライアンスにライセンスをインストールしたら、アプライアンスに接続できるユーザーの最大数を設定する必要があります。グローバル認証ポリシーの最大ユーザー数を設定します。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ペインの [設定] で、[認証 AAA 設定の変更] をクリックします。

3. [最大ユーザー数] に、ユーザーの合計数を入力し、[OK] をクリックします。

   このフィールドの数字は、ライセンスファイルに含まれるライセンスの数に対応します。この数は、アプライアンスにインストールされているライセンスの合計数以下である必要があります。たとえば、100 のユーザライセンスを含む 1 つのライセンスと 400 のユーザライセンスを含む 2 番目のライセンスをインストールするとします。ライセンスの合計数は 500 です。ログオンできるユーザーの最大数は 500 以下です。500 人のユーザーがログオンしている場合、その数を超えてログオンしようとするユーザーは、ユーザーがログオフするか、セッションを終了するまでアクセスが拒否されます。

ユニバーサルライセンスのインストールの確認

March 26, 2020

続行する前に、ユニバーサルライセンスが正しくインストールされていることを確認してください。

構成ユーティリティを使用してユニバーサルライセンスのインストールを確認するには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[システム] を展開し、[ライセンス] をクリックします。

   ［ライセンス］ペインで、［Citrix Gateway］の横に緑色のチェックマークが表示されます。［許可される Citrix Gateway ユーザーの最大数］フィールドには、アプライアンスでライセンスされた同時ユーザーセッションの数が表示されます。

コマンドラインを使用してユニバーサルライセンスのインストールを確認するには

1. PuTTY などの SSH クライアントを使用して、アプライアンスへのセキュアシェル（SSH）接続を開きます。
2. 管理者の資格情報を使用してアプライアンスにログオンします。
3. コマンドプロンプトで、次のように入力します。show license パラメータ SSL VPN が Yes で、maximum users パラメータがライセンス数に等しい場合、ライセンスは正しくインストールされます。

よくある質問

March 26, 2020

ライセンス

ユニバーサルライセンス **(CCU)** とは何ですか**?**

ユニバーサルライセンスは、Citrix ADC プラットフォームライセンスの上に置かれているアドオンライセンスです。これらのライセンスは、次の場合に必要です。

ICA セッションの保護

1. SmartAccess
2. SmartControl
3. EPA

SSL VPN

1. すべての SSL VPN ユースケース（Unified Gateway、CVPN、RDP プロキシなど）
2. Portal を有効にするには

新しいライセンスポリシーの変更点は何ですか**?**

ユニバーサルライセンスの価格は以下の通りです。

1. 0〜2499 人のユーザー-1 ユーザーあたり 100 ドル
2. 2500 人以上のユーザー-ユーザー 1 人あたり 50 ドル

以前のパッケージは以下の通りです:

1. 標準およびアドバンストには 5 つのユニバーサルライセンスが含まれています
2. プレミアムライセンスには 100 個のユニバーサルライセンスが含まれています。

変更は次のとおりです。

1. 標準には 500 ライセンスが含まれます
2. アドバンストには 1000 のライセンスが含まれます
3. Premium には CCU 要件はありません。つまり、お客様は Premium の CCU を必要としません。

一方、Premium 11.1 以降を購入した場合は、すべてのユースケースでユニバーサルライセンスを使用できます。

ユーザー数	価格
1-10000	$5
10001-20000	$2
20001+	$1.5

新しい価格はいつ購入者に提供されますか**?**

新しいパッケージは、2016 年 9 月 26 日にリリースされた NS 11.1.49.16 ビルドに含まれます。新しい SKU は 2016 年 9 月 19 日に公開されます。

どのようなバージョンの **Citrix ADC** が必要ですか**?**

CCU で新しいパッケージを入手するには、NS 11.1-49.16 以降が必要です。

既存のお客様は、どのようにしてこれを手に入れるのですか**?**

既存のお客様は、新しいパッケージを入手するには、既存の NS バージョンを 11.1.49.xx にアップグレードする必要があります。

お客様がアップグレードを希望しない場合で、SSL VPN に NS を使用することを希望する場合は、次の点を確認してください。

1. Unified Gateway は、アドバンス版またはプレミアム版のみで使用できます。
2. Citrix Virtual Apps and Desktops、プレミアムエディションで CCU を無料で受け取った場合は、SSL VPN 用の CCU を購入するか、11.1.49.xx を実行する NS プレミアムエディションを購入する必要があります。
3. 現時点では、使用シナリオを反映して、オンライン EULA が更新されています。それはここに掲載されます: https://www.citrix.com/buy/licensing/product.html
4. 販売例外プロセスを通じて、同じ価格設定を得ることができます。

Standard エディションを実行しているお客様が **5000** ライセンスを購入する場合、料金はいくらですか**?**

お客様が標準エディションを実行している場合、最初の 500 個のユニバーサルライセンスが無料で入手できます。残りの部分は、1〜10000 ユーザーに対して 5 ドルである新しい価格ごとに課金されます。

同じお客様が戻ってきて、さらに **6000** ライセンスを購入した場合、料金はいくらですか**?**

お客様が再び 6000 ライセンスを購入した場合、6000 ユーザー *1 ユーザーあたり 5 ドル = 30,000 ドルになります。この行を 11,000 ライセンスで使用しても、メリットは得られません。

年間メンテナンスもこの料金に課金されます。

Standard エディションを実行しているお客様が **11000** ライセンスを購入する場合、料金はいくらですか**?**

Standard エディションを実行している場合は、最初の 500 ライセンスが無料で入手できます。残りの場合は、10,500 人のユーザー * 1 ユーザーあたり 2 ドル = 21,000 ドルをお支払いいただきます

他のベンダーはどのように課金されますか**?** また、お客様に伝えるには何が必要ですか**?**

すべての SSL VPN ベンダーは、ユーザセッションライセンスごとに課金されます。Citrix 社は、お客様が Citrix ADC Premium エディションを購入する場合、ユーザーセッションライセンスごとに課金されない唯一の企業です。

お客様が **Citrix Virtual Apps and Desktops**、プレミアムエディションで受け取った **CCU** が **100** 個あり、**Unified Gateway** 用に **100** 個の **CCU** を購入した場合、現在は **200** 個の **CCU** がありますか**?**

はい。彼らは 200 個の CCU を持っています。ただし、SSL VPN のユースケースには 100 個の CCU しか使用できません。ただし、Citrix Virtual Apps and Desktops のユースケースには 200 個の CCU を使用できます。

はじめに

April 9, 2020

Citrix Gateway をインストールする前に、インフラストラクチャを評価し、情報を収集して、組織の特定のニーズを満たすアクセス戦略を計画する必要があります。アクセス戦略を定義するときは、セキュリティへの影響を考慮し、リスク分析を完了する必要があります。また、ユーザーが接続を許可するネットワークを決定し、ユーザー接続を有効にするポリシーを決定する必要もあります。

ユーザーが使用できるリソースの計画に加えて、展開シナリオも計画する必要があります。Citrix Gateway は、次の Citrix 製品で動作します。

- Citrix Endpoint Management
- Citrix Virtual Apps
- Citrix Virtual Desktops
- StoreFront
- Web Interface
- CloudBridge

Citrix Gateway の展開について詳しくは、「一般的な展開」および「Citrix 製品との統合」を参照してください。

アクセス戦略を準備する際には、次の予備的な手順を実行します。

- リソースを特定します。Web、SaaS、モバイルまたは公開アプリケーション、仮想デスクトップ、サービス、リスク分析で定義したデータなど、アクセスを提供するネットワークリソースを一覧表示します。
- アクセスシナリオを作成します。ユーザーがネットワークリソースにアクセスする方法を説明するアクセスシナリオを作成します。アクセスシナリオは、ネットワークへのアクセスに使用される仮想サーバー、エンドポイント分析スキャン結果、認証タイプ、またはその組み合わせによって定義されます。また、ユーザーがネットワークにログオンする方法を定義することもできます。
- クライアント・ソフトウェアを識別します。Citrix Gateway プラグインで完全な VPN アクセスを提供し、ユーザーは Citrix Workspace アプリ、Secure Hub またはクライアントレスアクセスを使用してログオンす

る必要があります。また、Outlook Web App または WorxMail への電子メールアクセスを制限することもできます。これらのアクセスシナリオは、ユーザーがアクセス権を取得したときに実行できるアクションも決定します。たとえば、公開アプリケーションを使用するか、ファイル共有に接続して、ユーザーがドキュメントを変更できるかどうかを指定できます。

- ポリシーをユーザー、グループ、または仮想サーバーに関連付けます。Citrix Gateway で作成するポリシーは、個人またはユーザーのセットが指定した条件を満たしたときに適用されます。作成したアクセスシナリオに基づいて条件を決定します。次に、ユーザーがアクセスできるリソースとそれらのリソースに対してユーザーが実行できるアクションを制御することによって、ネットワークのセキュリティを拡張するポリシーを作成します。ポリシーは、適切なユーザー、グループ、仮想サーバー、またはグローバルに関連付けます。

この項では、アクセス戦略の計画に役立つ次のトピックについて説明します。

- セキュリティの計画には、認証と証明書に関する情報が含まれます。
- 必要なネットワークハードウェアとソフトウェアを定義する前提条件。
- Citrix Gateway を構成する前に、設定を書き留めるために使用できる、インストール前のチェックリスト。

セキュリティの計画

March 26, 2020

Citrix Gateway の展開を計画する際には、証明書と認証と承認に関連する基本的なセキュリティ上の問題を理解する必要があります。

セキュアな証明書管理の設定

デフォルトでは、Citrix Gateway には自己署名の SSL（Secure Sockets Layer）サーバー証明書が含まれており、アプライアンスで SSL ハンドシェイクを完了できます。自己署名証明書は、テストやサンプル展開には適していますが、実稼働環境での使用はお勧めしません。Citrix Gateway を本番環境に展開する前に、認証局（CA）から署名された SSL サーバー証明書をリクエストして受信し、Citrix Gateway にアップロードすることをお勧めします。

Citrix Gateway を SSL ハンドシェイクでクライアントとして動作させる必要のある環境で（別のサーバーとの暗号化された接続を開始する）Citrix Gateway を展開する場合は、信頼されたルート証明書も Citrix Gateway にインストールする必要があります。たとえば、Citrix Virtual Apps および Web Interface を使用して Citrix Gateway を展開する場合、Citrix Gateway から Web Interface への接続を SSL で暗号化できます。この構成では、信頼されたルート証明書を Citrix Gateway にインストールする必要があります。

認証のサポート

Citrix Gateway を構成して、ユーザーを認証し、ユーザーが内部ネットワーク上のネットワークリソースに対して持つアクセス（または承認）のレベルを制御できます。

Citrix Gateway を展開する前に、ネットワーク環境に、次のいずれかの認証タイプをサポートするディレクトリと認証サーバーを配置する必要があります。

- LDAP
- RADIUS
- TACACS+
- 監査およびスマートカードをサポートするクライアント証明書
- RADIUS を使用した RSA 構成
- SAML 認証

環境が前述のリストの認証タイプをサポートしていない場合、またはリモートユーザーの数が少ない場合は、Citrix Gateway でローカルユーザーのリストを作成できます。その後、このローカルリストに対してユーザーを認証するように Citrix Gateway を構成できます。この設定では、ユーザアカウントを別の外部ディレクトリに保存する必要はありません。

Citrix Gateway のデプロイメントを保護する

展開によっては、セキュリティに関する考慮事項が異なる場合があります。Citrix ADC 安全な展開ガイドラインには、セキュリティに関する一般的なガイダンスが記載されています。このガイドラインは、特定のセキュリティ要件に基づいて適切な安全な展開を決定する際に役立ちます。

詳しくは、「Citrix ADC 安全な導入ガイドライン」を参照してください。

前提条件

April 9, 2020

Citrix Gateway の設定を構成する前に、次の前提条件を確認してください。

- Citrix Gateway はネットワークに物理的にインストールされ、ネットワークにアクセスできます。Citrix Gateway は、ファイアウォールの内側にある DMZ または内部ネットワークに展開されます。ダブルホップ DMZ で Citrix Gateway を構成し、サーバーファームへの接続を構成することもできます。DMZ にアプライアンスを展開することをお勧めします。
- Citrix Gateway は、ユーザーがネットワーク上のリソースにアクセスできるように、デフォルト Gateway または内部ネットワークへの静的ルートを使用して構成します。Citrix Gateway は、デフォルトで静的ルートを使用するように構成されています。
- 認証および認可に使用される外部サーバが設定され、実行されています。詳しくは、「認証と承認」を参照してください。
- ネットワークには、適切な Citrix Gateway ユーザー機能を提供するために、名前解決用のドメインネームサーバー（DNS）または Windows インターネットネームサービス（WINS）サーバーがあります。
- Citrix Gateway プラグインを使用してユーザー接続するためのユニバーサルライセンスを Citrix Web サイトからダウンロードし、ライセンスは Citrix Gateway にインストールできます。

- Citrix Gateway には、信頼された証明機関（CA）によって署名された証明書があります。詳しくは、「証明書のインストールと管理」を参照してください。

Citrix Gateway をインストールする前に、インストール前のチェックリストを使用して設定を書き留めます。

インストール前のチェックリスト

April 9, 2020

チェックリストは、Citrix Gateway をインストールする前に完了する必要があるタスクと計画情報の一覧で構成されています。

タスクを完了してメモを作成するときに、各タスクをチェックオフできるようにスペースが用意されています。インストールプロセス中および Citrix Gateway の構成中に入力する必要がある構成値をメモしておくことをお勧めします。

Citrix Gateway のインストールと構成の手順については、Citrix Gateway のインストールを参照してください。

ユーザーデバイス

- ユーザーデバイスが、Citrix Gateway プラグインのシステム要件で説明されているインストールの前提条件を満たしていることを確認します。
- ユーザーが接続するモバイルデバイスを識別します。注意: ユーザーが iOS デバイスに接続する場合は、セッションプロファイルで「Secure Browse」を有効にする必要があります。

Citrix Gateway の基本的なネットワーク接続

アプライアンスの構成を開始する前に、ライセンスと署名付きサーバー証明書を取得することをお勧めします。

- Citrix Gateway のホスト名を特定して書き留めます。注: これは完全修飾ドメイン名 (FQDN) ではありません。FQDN は、仮想サーバーにバインドされている署名付きサーバー証明書に含まれています。
- ユニバーサルライセンスをCitrixから取得します
- 証明書署名要求（CSR）を生成し、認証局（CA）に送信します。CSR を CA に送信する日付を入力します。
- システム IP アドレスとサブネットマスクを書き留めます。
- サブネット IP アドレスとサブネットマスクを書き留めます。
- 管理者パスワードを書き留めます。Citrix Gateway に付属するデフォルトのパスワードは nsroot です。
- ポート番号を書き留めます。これは、Citrix Gateway がセキュアなユーザー接続をリッスンするポートです。デフォルトは TCP ポート 443 です。このポートは、セキュリティで保護されていないネットワーク（インターネット）と DMZ の間のファイアウォール上で開かれている必要があります。
- デフォルト Gateway の IP アドレスを書き留めます。
- DNS サーバの IP アドレスとポート番号を書き留めます。デフォルトのポート番号は 53 です。さらに、DNS サーバーを直接追加する場合は、アプライアンスで ICMP (ping) も構成する必要があります。

- 最初の仮想サーバの IP アドレスとホスト名を書き留めます。
- 2 番目の仮想サーバの IP アドレスとホスト名 (該当する場合) を書き留めます。
- WINS サーバの IP アドレスを書き留めます (該当する場合)。

Citrix Gateway を介してアクセス可能な内部ネットワーク

- ユーザーが Citrix Gateway 経由でアクセスできる内部ネットワークを書き留めます。例：10.10.0.0/24
- ユーザーが Citrix Gateway プラグインを使用して Citrix Gateway 経由で接続するときにアクセスする必要があるすべての内部ネットワークとネットワークセグメントを入力します。

高可用性

Citrix Gateway アプライアンスが 2 つある場合は、1 つの Citrix Gateway が接続を受け入れて管理する高可用性構成でそれらを展開し、2 つ目の Citrix Gateway が最初のアプライアンスを監視します。最初の Citrix Gateway が何らかの理由で接続の受け入れを停止すると、2 番目の Citrix Gateway が引き継ぎ、アクティブな接続の受け入れを開始します。

- Citrix Gateway ソフトウェアのバージョン番号をメモします。
- バージョン番号は、両方の Citrix Gateway アプライアンスで同じである必要があります。
- 管理者パスワード（nsroot）を書き留めます。パスワードは、両方のアプライアンスで同じである必要があります。
- プライマリ Citrix Gateway の IP アドレスと ID を書き留めます。最大 ID 番号は 64 です。
- セカンダリ Citrix Gateway の IP アドレスと ID を書き留めます。
- ユニバーサルライセンスを取得し、両方のアプライアンスにインストールします。
- 両方のアプライアンスに同じユニバーサルライセンスをインストールする必要があります。
- RPC ノードのパスワードを書き留めます。

認証と承認

Citrix Gateway では、さまざまな種類の認証と承認がサポートされており、さまざまな組み合わせで使用できます。認証と認可の詳細については、認証と承認を参照してください。

LDAP 認証

環境に LDAP サーバーが含まれている場合は、LDAP を使用して認証できます。

- LDAP サーバの IP アドレスとポートを書き留めます。

  LDAP サーバへのセキュアでない接続を許可する場合、デフォルトはポート 389 です。SSL を使用して LDAP サーバーへの接続を暗号化する場合、デフォルトはポート 636 です。

- セキュリティの種類を書き留めます。

セキュリティは、暗号化の有無にかかわらず設定できます。

- 管理者のバインド DN を書き留めます。

  LDAP サーバーで認証が必要な場合は、LDAP ディレクトリへのクエリを実行するときに Citrix Gateway が認証に使用する管理者 DN を入力します。たとえば、cn = 管理者、cn = ユーザー、dc = エース、dc = com などです。

- 管理者パスワードを書き留めます。

  これは、管理者のバインド DN に関連付けられたパスワードです。

- ベース DN を書き留めます。

  ユーザーを検索する DN（またはディレクトリレベル）です。たとえば、ou=users,dc=ace,dc=com です。

- サーバーのログオン名属性を書き留めます。

  ユーザーのログオン名を指定する LDAP ディレクトリの人物オブジェクト属性を入力します。既定値は sAMAccountName です。Active Directory を使用していない場合、この設定に共通する値は cn または uid です。
  LDAP ディレクトリ設定の詳細については、「LDAP 認証の構成」を参照してください。

- グループ属性を書き留めます。
  ユーザーが属するグループを指定する LDAP ディレクトリ個人オブジェクト属性を入力します。デフォルトは memberOf です。この属性により、Citrix Gateway は、ユーザーが属するディレクトリグループを識別できます。

- サブアトリビュート名を書き留めます。

RADIUS 認証および認可

環境に RADIUS サーバが含まれている場合は、認証に RADIUS を使用できます。
RADIUS 認証には、RSA SecurID、セーフワード、およびゲマルトプロティバ製品が含まれます。

- プライマリ RADIUS サーバの IP アドレスとポートを書き留めます。デフォルトのポートは 1812 です。
- プライマリ RADIUS サーバシークレット（共有シークレット）を書き留めます。
- セカンダリ RADIUS サーバの IP アドレスとポートを書き留めます。デフォルトのポートは 1812 です。
- セカンダリ RADIUS サーバシークレット（共有シークレット）を書き留めます。
- パスワードエンコードのタイプ（PAP、CHAP、MS-CHAP v1、MSCHAP v2）を書き留めます。

SAML 認証

セキュリティーアサーションマークアップ言語 (SAML) は、ID プロバイダー (IdP) とサービスプロバイダーの間で認証と承認を交換するための XML ベースの標準です。

- セキュアな IdP 証明書を取得して Citrix Gateway にインストールします。

- リダイレクト URL を書き留めます。
- ユーザフィールドを書き留めます。
- 署名証明書の名前を書き留めます。
- SAML 発行者名を書き留めます。
- デフォルトの認証グループを書き留めます。

ファイアウォールを介したポートのオープン（シングルホップ **DMZ**）

組織が単一の DMZ で内部ネットワークを保護し、DMZ に Citrix Gateway を展開する場合は、ファイアウォールを介して次のポートを開きます。ダブルホップ DMZ 展開に 2 つの Citrix Gateway アプライアンスをインストールする場合は、ファイアウォールで適切なポートを開くを参照してください。

セキュリティで保護されていないネットワークと **DMZ** 間のファイアウォール

- インターネットと Citrix Gateway の間のファイアウォールで TCP/SSL ポート（デフォルト 443）を開きます。ユーザーデバイスはこのポートで Citrix Gateway に接続します。

セキュリティで保護されたネットワーク間のファイアウォール

- DMZ とセキュリティで保護されたネットワーク間のファイアウォールで 1 つ以上の適切なポートを開きます。Citrix Gateway は、1 つ以上の認証サーバー、またはこれらのポート上の保護されたネットワーク内の Citrix Virtual Apps and Desktops を実行しているコンピューターに接続します。
- 認証ポートを書き留めます。

  Citrix Gateway 構成に適したポートのみを開きます。

  - LDAP 接続の場合、デフォルトは TCP ポート 389 です。
  - RADIUS 接続の場合、デフォルトは UDP ポート 1812 です。Citrix Virtual Apps and Desktops のポートをメモします。
- Citrix Virtual Apps and Desktops で Citrix Gateway を使用している場合は、TCP ポート 1494 を開きます。セッション画面の保持を有効にする場合は、1494 ではなく TCP ポート 2598 を開きます。これらのポートは両方とも開いたままにしておくことをお勧めします。

Citrix Virtual Desktops、**Citrix Virtual Apps**、**Web Interface**、または **StoreFront**

Citrix Gateway を展開して、Web Interface または StoreFront 経由で Citrix Virtual Apps and Desktops にアクセスできるようにする場合は、以下のタスクを実行します。この展開では、Citrix Gateway プラグインは必要ありません。ユーザーは、Web ブラウザーと Citrix Receiver のみを使用して、Citrix Gateway 経由で公開アプリケーションおよびデスクトップにアクセスします。

- Web Interface または StoreFront を実行しているサーバーの FQDN または IP アドレスを書き留めます。

- Secure Ticket Authority（STA）を実行しているサーバの FQDN または IP アドレスを書き留めます（Web Interface の場合のみ）。

Citrix Endpoint Management

内部ネットワークに Citrix Endpoint Management を展開する場合は、以下のタスクを実行します。ユーザーがインターネットなどの外部ネットワークから Endpoint Management に接続する場合、ユーザーはモバイル、Web、SaaS アプリケーションにアクセスする前に Citrix Gateway に接続する必要があります。

- Endpoint Management の FQDN または IP アドレスを書き留めます。
- ユーザーがアクセスできるウェブ、SaaS、モバイル iOS または Android アプリケーションを特定します。

Citrix Virtual Apps を使用したダブルホップ DMZ 展開

ダブルホップ DMZ 構成で 2 つの Citrix Gateway アプライアンスを展開して、Citrix Virtual Apps を実行しているサーバーへのアクセスをサポートする場合は、以下のタスクを実行します。

最初の DMZ での Citrix Gateway

最初の DMZ は、内部ネットワークの最も外側のエッジ (インターネットまたは安全でないネットワークに最も近い) にある DMZ です。クライアントは、DMZ とインターネットを分離するファイアウォールを介して最初の DMZ の Citrix Gateway に接続します。最初の DMZ に Citrix Gateway をインストールする前に、この情報を収集してください。

- この Citrix Gateway のチェックリストの「Citrix Gateway の基本的なネットワーク接続」セクションの項目に入力します。

  これらの項目を完了すると、インターフェイス 0 はこの Citrix Gateway をインターネットに接続し、インターフェイス 1 はこの Citrix Gateway を 2 番目の DMZ の Citrix Gateway に接続します。

- プライマリアプライアンスで 2 番目の DMZ アプライアンス情報を設定します。

  ダブルホップ DMZ の最初のホップとして Citrix Gateway を構成するには、最初の DMZ のアプライアンス上の 2 番目の DMZ で Citrix Gateway のホスト名または IP アドレスを指定する必要があります。最初のホップでアプライアンス上で Citrix Gateway プロキシーをいつ構成するかを指定したら、Citrix Gateway にグローバルにバインドするか、仮想サーバーにバインドします。

- アプライアンス間の接続プロトコルとポートをメモします。

  二重 DMZ の最初のホップとして Citrix Gateway を構成するには、接続プロトコルと 2 番目の DMZ の Citrix Gateway が接続をリッスンするポートを指定する必要があります。接続プロトコルとポートは SSL を使用する SOCKS (デフォルトのポート 443) です。プロトコルとポートは、最初の DMZ と 2 番目の DMZ を分離するファイアウォールを介して開かれている必要があります。

2 番目の **DMZ** の **Citrix Gateway**

2 番目の DMZ は、内部のセキュアなネットワークに最も近い DMZ です。2 番目の DMZ に展開された Citrix Gateway は、ICA トラフィックのプロキシとして機能し、外部ユーザーデバイスと内部ネットワーク上のサーバー間で 2 番目の DMZ を通過します。

- この Citrix Gateway のチェックリストの「Citrix Gateway の基本的なネットワーク接続」セクションのタスクを完了します。

  これらの項目を完了すると、インターフェイス 0 がこの Citrix Gateway を最初の DMZ の Citrix Gateway に接続することに注意してください。インターフェイス 1 は、この Citrix Gateway をセキュリティ保護されたネットワークに接続します。

アップグレードしています

March 26, 2020

Citrix Gateway にあるソフトウェアは、新しいリリースが利用可能になったときにアップグレードできます。あなたは、Citrix のウェブサイト上で更新を確認することができます. 新しいリリースにアップグレードできるのは、アップデートがリリースされたときに Citrix Gateway ライセンスが Subscription Advantage プログラムに登録されている場合のみです。Subscription Advantage はいつでも更新できます。詳細については、シトリックスサポートWeb サイトを参照してください。

Citrix Gateway の最新のメンテナンスリリースについては、Citrix Knowledge Centerを参照してください。

ソフトウェアの更新を確認するには

1. シトリックスの Web サイトにアクセスします。
2. [My Account] をクリックしてログオンします。
3. ［ダウンロード］をクリックします。
4. ［ダウンロードの検索］で Citrix Gateway を選択します。
5. [ダウンロードの種類を選択] で、[製品ソフトウェア] を選択し、[検索] をクリックします。
   仮想アプライアンスを選択して、Citrix ADC VPX をダウンロードすることもできます。この場合、対象のハイパーバイザーを選択するためのページが開きます。
6. ［Citrix Gateway ページで［Citrix ADC Gateway］または［Access Gateway］を展開します。
7. ダウンロードするアプライアンスソフトウェアのバージョンをクリックします。
8. ダウンロードするバージョンのアプライアンスソフトウェアページで、仮想アプライアンスを選択し、ダウンロードをクリックします。
9. 画面の指示に従ってソフトウェアをダウンロードしてください。

ソフトウェアをコンピュータにダウンロードしたら、アップグレードウィザードまたはコマンドプロンプトを使用してソフトウェアをインストールできます。

アップグレードウィザードを使用して **Citrix Gateway** をアップグレードするには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[システム] をクリックします。
2. 詳細ウィンドウで、[アップグレードウィザード] をクリックします。
3. [**Next**] をクリックして、ウィザードの指示に従います。

コマンドプロンプトを使用して **Citrix Gateway** をアップグレードするには

1. ソフトウェアを Citrix Gateway にアップロードするには、WinSCP などのセキュアな FTP クライアントを使用してアプライアンスに接続します。
2. ソフトウェアをコンピュータからアプライアンスの /var/nsinstall ディレクトリにコピーします。
3. PuTTY などのセキュアシェル（SSH）クライアントを使用して、アプライアンスへの SSH 接続を開きます。
4. Citrix Gateway にログオンします。
5. コマンドプロンプトで、次のコマンドを実行します: `shell`
6. nsinstall ディレクトリに移動するには、コマンド・プロンプトで次のように入力します。`cd /var/nsinstall`
7. ディレクトリの内容を表示するには、次のように入力します。`ls`
8. ソフトウェアを解凍するには、tar —xvzf ビルド _X_XX.tgz と入力します。

   ここで、build_X_XX.tgz は、アップグレードするビルドの名前です。
9. インストールを開始するには、コマンドプロンプトで次のように入力します。`./installns`
10. インストールが完了したら、Citrix Gateway を再起動します。

Citrix Gateway の再起動後、インストールが正常に完了したことを確認するには、構成ユーティリティーを起動します。アプライアンスの Citrix Gateway のバージョンが右上隅に表示されます。

システムのインストール

April 9, 2020

Citrix Gateway アプライアンスを受け取ったら、アプライアンスを開梱し、サイトとラックを準備します。アプライアンスを設置する場所が環境基準を満たしており、指示に従ってサーバラックが設置されていることを確認したら、ハードウェアを取り付けます。アプライアンスをマウントしたら、ネットワーク、電源、および初期設定に使用するコンソール端末に接続します。アプライアンスの電源を入れたら、初期構成を実行し、管理およびネットワーク IP アドレスを割り当てます。インストール手順に記載されている注意事項と警告を必ず守ってください。

Citrix ADC VPX 仮想アプライアンスをインストールする場合は、まず仮想アプライアンスのイメージを取得し、Hypervisor または他の仮想マシンモニターにインストールする必要があります。

Citrix Gateway アプライアンスを構成する前に、設定を書き留めておくことができるように、Citrix Gateway のインストール前のチェックリストトピックを使用することをお勧めします。このチェックリストには、Citrix Gateway とアプライアンスのインストールに関する情報が含まれています。

Citrix Gateway の構成

March 26, 2020

Citrix Gateway で基本ネットワーク設定を構成したら、ユーザーがセキュリティで保護されたネットワーク上のネットワークリソースに接続できるように詳細設定を構成します。これらの設定には、次のものがあります。

- 仮想サーバ。Citrix Gateway で複数の仮想サーバーを構成できるため、実装する必要のあるユーザーシナリオに応じて異なるポリシーを作成できます。各仮想サーバには、独自の IP アドレス、証明書、およびポリシーセットがあります。たとえば、仮想サーバーを構成し、グループのメンバシップと仮想サーバーにバインドするポリシーに応じて、内部ネットワークのネットワークリソースにユーザーを制限できます。仮想サーバーを作成するには、次の方法を使用します。
  - クイック構成ウィザード
  - Citrix Gateway ウィザード
  - 構成ユーティリティ
- 高可用性。ネットワークに 2 つの Citrix Gateway アプライアンスを展開するときに、高可用性を構成できます。プライマリアプライアンスに障害が発生した場合、セカンダリアプライアンスはユーザーセッションに影響を与えずに引き継ぐことができます。
- 証明書。証明書を使用して、Citrix Gateway へのユーザー接続をセキュリティで保護できます。証明書署名要求 (CSR) を作成するときは、証明書に完全修飾ドメイン名を追加します。証明書を仮想サーバーにバインドできます。
- 認証。Citrix Gateway では、ローカル LDAP、RADIUS、SAML、クライアント証明書、TACACS+ など、複数の認証タイプがサポートされています。さらに、カスケード認証と 2 要素認証を構成できます。
  注: 認証に RSA、Safeword、または Gemalto Protiva を使用している場合は、RADIUS を使用してこれらのタイプを構成します。
- ユーザー接続。セッションプロファイルを使用して、ユーザー接続を構成できます。プロファイル内では、ユーザーがログオンできるプラグインと、ユーザーが必要とする制限事項を決定できます。次に、1 つのプロファイルでポリシーを作成できます。セッション・ポリシーは、ユーザー、グループ、仮想サーバーにバインドできます。
- ホームページ。デフォルトのアクセスインタフェースをホームページとして使用することも、カスタムホームページを作成することもできます。ユーザーが Citrix Gateway に正常にログオンすると、ホームページが表示されます。
- エンドポイント解析。Citrix Gateway では、ユーザーのログオン時にユーザーデバイスにソフトウェア、ファイル、レジストリエントリ、プロセス、およびオペレーティングシステムがないかチェックするポリシーを構成できます。エンドポイント分析では、ユーザーデバイスに必要なソフトウェアが必要とされるため、ネッ

トワークのセキュリティを強化できます。

構成ユーティリティの使用

April 9, 2020

構成ユーティリティでは、ほとんどの Citrix Gateway 設定を構成できます。構成ユーティリティにアクセスするには、Web ブラウザを使用します。

構成ユーティリティにログオンするには

1. Web ブラウザで、Citrix Gateway のシステム IP アドレスを入力します（`http://192.168.100.1`など）。
   注：Citrix Gateway には、デフォルトの IP アドレス
   192.168.100.1 とサブネットマスク
   255.255.0.0 が事前構成されています。
2. [ユーザー名] と [パスワード] に「nsroot」と入力します。
3. ［展開の種類］で Citrix Gateway を選択し、［ログイン］をクリックします。

構成ユーティリティに初めてログオンすると、デフォルトで [ホーム] タブにダッシュボードが開きます。［ホーム］タブでは、クイック構成ウィザードを使用して、仮想サーバー、認証、証明書、および Citrix Endpoint Management の設定を構成できます。クイック構成ウィザードでは、StoreFront または Web Interface 設定を構成することもできます。

Citrix Gateway の構成について詳しくは、以下を参照してください。

- 「セットアップウィザードを使用した初期設定の構成」を参照してください。
- Configuring Settings with the Quick Configuration Wizard
- 「Citrix Gateway ウィザードを使用した設定の構成」を参照してください。

Citrix Gateway のポリシーとプロファイル

March 26, 2020

Citrix Gateway のポリシーとプロファイルを使用すると、特定のシナリオまたは条件下で構成設定を管理および実装できます。個々のポリシーでは、指定した一連の条件が満たされたときに有効になる構成設定を規定または定義します。各ポリシーには一意の名前があり、ポリシーにバインドされたプロファイルを持つことができます。

Citrix Gateway でのポリシーの詳細については、以下のトピックを参照してください。

ポリシーのしくみ

April 9, 2020

ポリシーは、ブール条件と、プロファイルと呼ばれる設定の集まりで構成されます。条件は実行時に評価され、ポリシーを適用する必要があるかどうかを判断します。

プロファイルとは、特定のパラメータを使用した設定の集まりです。プロファイルには任意の名前を付けることができ、複数のポリシーで再利用できます。プロファイル内で複数の設定を構成できますが、ポリシーごとに含めることができるプロファイルは 1 つだけです。

ポリシーを、設定した条件とプロファイルを使用して、仮想サーバ、グループ、ユーザー、またはグローバルにバインドできます。ポリシーは、管理する構成設定のタイプによって参照されます。たとえば、セッションポリシーでは、ユーザーのログオン方法やユーザーのログオン状態を維持できる時間を制御できます。

Citrix Virtual Apps で Citrix Gateway を使用している場合、Citrix Gateway のポリシー名がフィルターとして Citrix Virtual Apps に送信されます。Citrix Virtual Apps および SmartAccess と連携するように Citrix Gateway を構成する場合は、Citrix Virtual Apps で次の設定を構成します。

- アプライアンス上で構成されている仮想サーバーの名前。この名前は、Citrix Gateway ファーム名として Citrix Virtual Apps に送信されます。
- 事前認証またはセッションポリシーの名前は、フィルタ名として送信されます。

Citrix Endpoint Management と連携するように Citrix Gateway を設定する方法の詳細については、「Citrix Endpoint Management 環境の設定の構成」を参照してください。

Citrix Virtual Apps and Desktops で機能する Citrix Gateway 構成について詳しくは、「Web Interface を使用した Citrix Virtual Apps および Citrix Virtual Desktops リソースへのアクセス」および「Citrix Endpoint Management または StoreFront との統合」を参照してください。

事前認証ポリシーの詳細については、エンドポイントポリシーの設定を参照してください。

ポリシーの優先順位の設定

March 26, 2020

ポリシーは、ポリシーがバインドされている順序で優先順位付けされ、評価されます。

ポリシープライオリティは、次の 2 つの方法で決定します。

- ポリシーがバインドされるレベル（グローバル、仮想サーバ、グループ、またはユーザー）。ポリシーレベルは、次のように上位から下位にランク付けされます。
  - ユーザー（最も高い優先度）
  - グループ

  - 仮想サーバ
  - グローバル（最も低い優先度）
- ポリシーがバインドされているレベルに関係なく、数値優先順位が優先されます。グローバルにバインドされたポリシーの優先順位番号が 1 で、ユーザーにバインドされた別のポリシーの優先順位番号が 2 の場合、グローバルポリシーが優先されます。プライオリティ番号が小さいほど、ポリシーの優先順位が高くなります。

条件付きポリシーの設定

March 26, 2020

ポリシーを設定する場合、任意のブール式を使用して、ポリシーが適用される条件を表すことができます。条件付きポリシーを設定する場合、次のような、使用可能な任意のシステム式を使用できます。

- クライアントセキュリティストリング
- ネットワーク情報
- HTTP ヘッダーとクッキー
- 時間帯
- クライアント証明書の値

SmartAccess のセッションポリシーなど、ユーザーデバイスが特定の条件を満たしている場合にのみ適用するポリシーを作成することもできます。

条件付きポリシーを設定するもう 1 つの例は、ユーザーの認証ポリシーを変更することです。たとえば、自宅のコンピュータやモバイルデバイスから Micro VPN を使用するなど、内部ネットワークの外部から Citrix Gateway プラグインを使用して接続しているユーザーは、LDAP を使用して認証され、ワイドエリアネットワーク（WAN）経由で接続しているユーザーは認証されるように要求できます。を使用して、RADIUS を使用します。

注：ポリシー規則がセッションプロファイルのセキュリティ設定の一部として構成されている場合、エンドポイント分析結果に基づくポリシー条件は使用できません。

Citrix Gateway でのポリシーの作成

March 26, 2020

構成ユーティリティを使用してポリシーを作成できます。ポリシーを作成したら、適切なレベル (ユーザー、グループ、仮想サーバー、またはグローバル) にポリシーをバインドします。ポリシーをこれらのレベルの 1 つにバインドすると、ポリシー条件が満たされていれば、ユーザーはプロファイル内で設定を受け取ります。各ポリシーとプロファイルには一意の名前があります。

展開の一部として Citrix Endpoint Management または StoreFront を使用している場合は、クイック構成ウィザードを使用してこの展開の設定を構成できます。ウィザードの詳細については、Configuring Settings with the

Quick Configuration Wizardを参照してください。

システム式の設定

March 26, 2020

システム式は、ポリシーが適用される条件を指定します。たとえば、事前認証ポリシーの式は、ユーザーがログオンしているときに適用されます。セッションポリシーの式は、ユーザーが認証され、Citrix Gateway にログオンした後に評価され、適用されます。

Citrix Gateway では、次の式を使用できます。

- Citrix Gateway への接続を確立するときにユーザーが使用できるオブジェクトを制限する一般的な式
- ユーザーデバイスにインストールして実行する必要があるソフトウェア、ファイル、プロセス、またはレジストリ値を定義するクライアントセキュリティ式
- ネットワーク設定に基づいてアクセスを制限するネットワークベースの式

Citrix Gateway は、Citrix ADC アプライアンスとして使用することもできます。アプライアンス上の一部の式は、Citrix ADC により適用可能です。一般的な式とネットワークベースの式は、Citrix ADC で一般的に使用され、一般的に Citrix Gateway では使用されません。Citrix Gateway では、クライアントセキュリティ式を使用して、正しいアイテムがユーザーデバイスにインストールされているかどうかを判断します。

クライアントセキュリティ式の設定

式はポリシーのコンポーネントです。式は、要求または応答に対して評価される単一の条件を表します。次のような条件をチェックする単純な式のセキュリティ文字列を作成できます。

- サービスパックを含むユーザーデバイスのオペレーティングシステム
- ウイルス対策ソフトウェアのバージョンとウイルス定義
- ファイル
- プロセス
- レジストリ値
- ユーザー証明書

単純な式と複合式を作成する

March 26, 2020

単純な式は、単一の条件をチェックします。単純な式の例を次に示します。

REQ.HTTP.URL == `HTTP://www.mycompany.com`

複合式は、複数の条件をチェックします。複合式を作成するには、論理演算子 && と	. シンボルを使用して、評価の順序で式をグループ化できます。

複合式は次のように分類できます。

- 名前の付いた式。独立したエンティティとして、名前付き式は他のポリシーで再利用でき、ポリシーの一部になります。名前付き式は、設定ユーティリティのシステムレベルで設定します。定義済みの名前付き式をポリシーで使用することも、独自の式を作成することもできます。
- インライン式。インライン式は、ポリシーに固有のポリシー内で構築する式です。

名前付き式を作成するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[AppExpert] を展開し、[式] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [ポリシー式の作成] ダイアログボックスの [式名] に、式の名前を入力します。
4. 式を作成するには、[追加] をクリックします。
5. 次のいずれかを行います:
   a) [よく使用する式] で、一覧から式を選択し、[OK] をクリックし、[作成] をクリックして、[閉じる] をクリックします。
   b) [式を作成] で、式文字列のパラメータを選択し、[OK] をクリックし、[作成] をクリックして、[閉じる] をクリックします。

カスタム式の追加

March 26, 2020

ポリシーを作成する場合は、ポリシーの設定中にカスタム式を作成できます。たとえば、ユーザーが Citrix Gateway プラグインを使用してログオンしたり、セッションの制限時間を設定したり、Windows でシングルサインオンを許可したりするためのセッションプロファイルを作成するとします。セッションプロファイルを作成したら、[セッションポリシーの作成] ダイアログボックスで式を作成できます。次の例は、プロセスおよびウイルス対策アプリケーションをチェックする式を示しています。

クライアント. アプリケーション. プロセス (ccapp.exe) は存在する-頻繁な 5 &&& クライアント. アプリケーション.AV (シマンテック) . バージョン ==14.20.0.29-新鮮さ 5 &&&ns_true

ポリシー式での演算子と演算子の使用

March 26, 2020

演算子は、1 つまたは複数のオブジェクト (オペランドを操作する演算、ブール演算、リレーショナルなど) を識別する記号です。このトピックの最初のセクションでは、使用できる演算子を定義し、定義を示します。2 番目のセクションでは、メソッド、URL、クエリなどの特定の修飾子で使用できる演算子を示します。

演算子と定義

このセクションでは、ポリシー式を作成するときに使用できる演算子を定義し、その演算子について説明します。

- ==,! =, 等式, 次数

これらの演算子は、完全一致をテストします。大文字と小文字が区別されます（’‘cmd.exe” は “cMd.exe” ‘と等しくありません)。これらの演算子は、正確な構文を満たす特定の文字列を許可するが、他の文字列を除外する権限を作成する場合に便利です。

- GT

この演算子は、数値比較に使用されます。これは、URL とクエリ文字列の長さに使用されます。

- CONTAINS, NOTCONTAINS

これらの演算子は、指定された修飾子に対してチェックを実行し、指定された文字列が修飾子に含まれているかどうかを判断します。これらの演算子では、大文字と小文字は区別されません。

- EXISTS, NOTEXISTS

これらの演算子は、特定の修飾子の存在をチェックします。たとえば、これらの演算子を HTTP ヘッダーに適用して、特定の HTTP ヘッダーが存在するか、または URL クエリが存在するかを判断できます。

- CONTENTS

この演算子は、修飾子が存在し、内容があるかどうか（つまり、値に関係なく、ヘッダーが存在し、それに関連付けられた値があるかどうか）をチェックします。

修飾子、演算子、オペランド、アクションおよび例

このセクションでは、演算子とオペランドに使用できるパラメータを示します。各項目は修飾子で始まり、関連する演算子とオペランドがリストされ、式が実行するアクションが記述され、例が示されます。

- 方法

演算子:EQ、NEQ
オペランド: 必須:
- 標準 HTTP メソッド

- サポートされているメソッド
- GET, HEAD, POST, PUT, DELETE OPTIONS, TRACE, CONNECT
アクション: 設定されたメソッドへの着信要求メソッドを検証します。
例: メソッド EQ GET

URL

-

演算子:EQ, NEQ
オペランド: 必須:URL (形式:/[プレフィックス] [*] [. サフィックス])
アクション: 設定された URL で着信 URL を確認します。
例:
URL EQ/Foo*.asp
URL EQ /foo*
URL EQ /*.asp
URL EQ /foo.asp

-

演算子:CONTAINS、NOTCONTAINS
オペランド: 必須: 任意の文字列 (引用符で囲む)
アクション: 構成されたパターンの有無について、着信 URL を検証します。(URL および URL クエリを含む)。
例:URL は 'ZZZ' を含み

- URL LEN

演算子:GT
オペランド: 必須: 長さ (整数値)
処理: 着信 URL の長さと設定された長さを比較します。(URL および URL クエリを含む)。
例:URLLEN GT 60

- URL QUERY

演算子:CONTAINS、NOTCONTAINS
オペランド: 必須: 任意の文字列 (引用符で囲む)。
オプション: 長さおよびオフセット
処理: 着信 URL クエリーで、構成されたパターンが存在するかどうかを
検証します。
CONTENTS と同様に使用されます。
オプションが指定されていない場合は、パターンの後の URL クエリ全体が使用されます。
オプションが存在する場合、パターンの後のクエリの長さのみが使用されます。
オフセットは、パターンの検索を開始する位置を示すために使用されます。
例: URLQUERY CONTAINS 'ZZZ'

- URL QUERY LEN

演算子:GT
オペランド: 必須: 長さ (整数値)
処理: 着信 URL クエリの長さと設定された長さを比較します。
例：URLQUERYLN GT 60

- URL TOKENS

演算子:EQ, NEQ
オペランド: 必須:URL トークン (サポートされている URL トークン =, +,%,! 、&、?)。
アクション: 着信 URL を比較して、設定されたトークンの存在を確認します。疑問符の前にバックスラッシュ（\）を入力する必要があります。
例：URLTOKENS EQ '% , +, &, \?'

- VERSION

演算子:EQ, NEQ
オペランド: 必須: 標準 HTTP バージョン。有効な HTTP バージョン文字列 HTTP/1.0、HTTP/1.1
アクション: 着信リクエストの HTTP バージョンと、設定された HTTP バージョンを比較します。
例：VERSION EQ HTTP/1.1

Header

-

演算子:EXISTS、NOTEXISTS
オペランド: なし
処理: 受信要求で HTTP ヘッダーの存在を検査します。
例：Header Cookie EXISTS

-

演算子:CONTAINS、NOTCONTAINS
オペランド: 必須: 任意の文字列 (引用符で囲む)。
オプション: 長さおよびオフセット
処理: 着信要求で、特定のヘッダーに構成されたパターンが存在するかどうかを検証します。CONTENTS と同様に使用されます。オプションが指定されていない場合は、パターンの後の HTTP ヘッダー値全体が使用されます。オプションが存在する場合、パターンの後のヘッダーの長さのみが使用されます。オフセットは、パターンの検索を開始する位置を示すために使用されます。
例：Header Cookie CONTAINS "&sid"

-

演算子:CONTENTS
オペランド: オプション: 長さおよびオフセット
処理:HTTP ヘッダーの内容を使用します。オプションを指定しない場合は、HTTP ヘッダー値全体が使用されます。オプションが存在する場合、オフセットから始まるヘッダーの長さのみが使用されます。
例：Header User-Agent CONTENTS

- SOURCEIP

オペレータ:EQ, NEQ
オペランド: 必須:IP アドレス
オプション: サブネットマスク
アクション: 着信要求の送信元 IP アドレスを、設定された IP アドレスと照合して検証します。オプションのサブネットマスクが指定されている場合、着信要求は、設定された IP アドレスおよびサブネットマスクに対して検証されます。
例: Sourceip EQ 192.168.100.0 -netmask 255.255.255.0

- DESTIP

オペレータ:EQ, NEQ
オペランド: 必須:IP アドレス
オプション: サブネットマスク
アクション: 着信要求の宛先 IP アドレスを、設定された IP アドレスと照合して検証します。オプションのサブネットマスクが指定されている場合、着信要求は、設定された IP アドレスおよびサブネットマスクに対して検証されます。
例: Sourceip EQ 192.168.100.0 -netmask 255.255.255.0

- SOURCEPORT

オペレータ:EQ, NEQ
オペランド: 必須: ポート番号
オプション: ポート範囲
アクション: 着信要求の送信元ポート番号を、設定されたポート番号と照合して検証します。
例: SOURCEPORT EQ 10-20

- DESTPORT

オペレータ: EQ、NEQ
オペランド: 必須: ポート番号
オプション: ポート範囲
アクション: 着信要求の宛先ポート番号を、設定されたポート番号と照合して検証します。
例: DESTPORT NEQ 80

- CLIENT.SSL.VERSION

演算子:EQ, NEQ
オペランド: 必須:SSL バージョン
アクション: セキュアな接続で使用されている SSL または TLS バージョンのバージョンを確認します。
例: CLIENT.SSL.VERSION EQ SSLV3

- CLIENT.CIPHER.TYPE

演算子:EQ, NEQ
オペランド: 必須: クライアント暗号タイプ

アクション: 使用されている暗号の種類 (エクスポートまたは非エクスポート) をチェックします。
例：CLIENT.CIPHER.TYPE EQ EXPORT

- CLIENT.CIPHER.BITS

演算子：EQ、NEQ、GE、LE、GT、LT
オペランド：必須：クライアント暗号ビット
アクション：使用されている暗号の鍵強度をチェックします。
例：CLIENT.CIPHER.BITS GE 40

- CLIENT.CERT

演算子：EXISTS、NOTEXISTS
オペランド：none
アクション：クライアントが SSL ハンドシェイク中に有効な証明書を送信したかどうかを確認します。
例：CLIENT.CERT EXISTS

- CLIENT.CERT.VERSION

オペレータ:EQ, NEQ, GE, LE, GT, LT
オペランド: クライアント証明書バージョン
アクション: クライアント証明書のバージョンを確認します。
例：CLIENT.CERT.VERSION EQ 2

- CLIENT.CERT.SERIALNUMBER

オペレータ:EQ, NEQ
オペランド: 必須: クライアント証明書のシリアル番号
アクション: クライアント証明書のシリアル番号を確認します。シリアル番号は文字列として扱われます。
例：CLIENT.CERT.SER IALNUMBER EQ 2343323

- CLIENT.CERT.SIGALGO

演算子:EQ, NEQ
オペランド: 必須: クライアント証明書の署名アルゴリズム。
アクション: クライアント証明書で使用されている署名アルゴリズムをチェックします。
例：CLIENT.CERT.SIGALGO EQ md5WithRSAEncryption

- CLIENT.CERT.SUBJECT

演算子:CONTAINS、NOTCONTAINS
オペランド: 必須: クライアント証明書のサブジェクト
オプション: 長さ、オフセット
アクション: クライアント証明書のサブジェクトフィールドをチェックします。
例：CLIENT.CERT.SUBJECT CONTAINS CN= Access_Gateway

- CLIENT.CERT.ISSUER

演算子:CONTAINS、NOTCONTAINS
オペランド: 必須: クライアント証明書発行者
オプション: 長さ、オフセット
アクション: クライアント証明書の発行者フィールドをチェックします。
例：CLIENT.CERT.ISSUER CONTAINS O=VeriSign

- CLIENT.CERT.VALIDFROM

演算子:EQ, NEQ, GE, LE, GT, LT
オペランド: 必須: 日付
処理: クライアント証明書が有効である日付を確認します。
有効な日付フォーマットは、1994 年 11 月 5 日（
火）08:12:31（グリニッジ標準時
）火曜日、11 月 9 日～94 日午前 8 時 12 分 31 秒（グリニッジ標準時）火曜日、11 月 14 日午前 8 時 12 分 31 秒（火）です。

- CLIENT.CERT.VALIDTO

演算子:EQ, NEQ, GE, LE, GT, LT
オペランド: 必須: 日付
処理: クライアント証明書が有効になるまでの日付をチェックします。
有効な日付フォーマットは、次のとおりです。
Tue, 05 Nov 1994 08:12:31 GMT
Tuesday, 05-Nov-94 08:12:31 GMT
Tue Nov 14 08:12:31 1994
Example: CLIENT.CERT.VALIDTO GE ‘Tue Nov 14 08:12:31 1994’

Citrix Gateway の構成設定の表示

March 26, 2020

Citrix Gateway の構成を変更すると、その変更はログファイルに保存されます。いくつかのタイプの構成設定を表示できます。

- 保存された設定。Citrix Gateway に保存した設定を確認できます。
- 実行構成。仮想サーバーや認証ポリシーなど、Citrix Gateway に保存した構成として保存していないアクティブな設定を表示できます。
- 実行構成と保存構成の比較。Citrix Gateway で実行中および保存済みの構成を並べて比較できます。

Citrix Gateway の構成設定をクリアすることもできます。

重要：Citrix Gateway の設定をクリアすると、証明書、仮想サーバー、ポリシーが削除されます。構成をクリアしないことをお勧めします。

Citrix Gateway 構成の保存

March 26, 2020

Citrix Gateway の現在の構成をネットワーク上のコンピューターに保存したり、現在の実行構成を表示したり、保存済み構成と実行構成を比較したりできます。

Citrix Gateway 上に構成を保存するには

1. 構成ユーティリティの詳細ペインの上にある [保存] アイコンをクリックし、[はい] をクリックします。

Citrix Gateway で構成ファイルを表示および保存するには

保存された構成は、仮想サーバー、ポリシー、IP アドレス、ユーザー、グループ、証明書の設定など、Citrix Gateway のログファイルに保存される設定です。

Citrix Gateway で設定を構成するときに、その設定をコンピューター上のファイルに保存できます。Citrix Gateway ソフトウェアを再インストールする必要がある場合や、誤って一部の設定を削除した場合は、このファイルを使用して構成を復元できます。設定を復元する必要がある場合は、ファイルを Citrix Gateway にコピーし、コマンドラインインターフェイスまたは WinSCP などのプログラムを使用してアプライアンスを再起動してファイルを Citrix Gateway にコピーします。

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[診断] をクリックします。
2. 詳細ペインの [構成の表示] で、[保存された構成] をクリックします。
3. [保存された構成] ダイアログボックスで、[出力テキストをファイルに保存] をクリックし、ファイルに名前を付け、[保存] をクリックします。
   注：ns.conf というファイル名でファイルを保存することをお勧めします。

現在の実行構成を表示するには

Citrix Gateway に加えた変更を、保存する手間をかけずに実行構成と呼びます。これらの設定は Citrix Gateway で有効ですが、アプライアンスには保存されません。ポリシー、仮想サーバ、ユーザ、グループなどの追加設定を構成した場合は、実行構成でこれらの設定を表示できます。

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[診断] をクリックします。
2. 詳細ペインの [構成の表示] で、[実行構成] をクリックします。

保存された構成と実行構成を比較するには

アプライアンスに保存されている設定を確認し、それらの設定を実行構成と比較できます。実行構成を保存するか、構成を変更するかを選択できます。

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[診断] をクリックします。
2. 詳細ペインの [構成の表示] で、[保存済み v/s 実行中] をクリックします。

Citrix Gateway 構成のクリア

March 26, 2020

Citrix Gateway の構成設定をクリアできます。次の 3 つのレベルのうち、クリアする設定を選択できます。

重要：Citrix Gateway の構成設定をクリアする前に、構成を保存することをお勧めします。

- 基本。システム IP アドレス、デフォルト Gateway、マッピングされた IP アドレス、サブネット IP アドレス、DNS 設定、ネットワーク設定、高可用性設定、管理パスワード、機能およびモード設定を除き、アプライアンス上のすべての設定をクリアします。
- [拡張]: システム IP アドレス、マッピング IP アドレス、サブネット IP アドレス、DNS 設定、および高可用性定義を除くすべての設定をクリアします。
- フル。アプライアンスへのネットワーク接続を維持するために必要なシステム IP（NSIP）アドレスとデフォルトルートを除く、工場出荷時の設定に構成を復元します。

構成のすべてまたは一部をクリアすると、機能設定は工場出荷時のデフォルト設定に設定されます。

構成をクリアしても、証明書やライセンスなど、Citrix Gateway に保存されているファイルは削除されません。ファイル ns.conf は変更されません。構成をクリアする前に構成を保存する場合は、まず構成をコンピュータに保存します。構成を保存すると、Citrix Gateway で ns.conf ファイルを復元できます。アプライアンスにファイルを復元して Citrix Gateway を再起動すると、ns.conf の構成設定が復元されます。

rc.conf などの設定ファイルへの変更は元に戻りません。

高可用性ペアを使用している場合、両方の Citrix Gateway アプライアンスが同じように変更されます。たとえば、1 つのアプライアンスの基本設定をクリアすると、変更内容が 2 番目のアプライアンスに伝播されます。

Citrix Gateway の構成設定をクリアするには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[診断] をクリックします。
2. 詳細ペインの [メンテナンス] で、[構成のクリア] をクリックします。
3. [構成レベル] で、クリアするレベルを選択し、[実行] をクリックします。

ウィザードを使用した **Citrix Gateway** の構成

April 9, 2020

Citrix Gateway には、アプライアンスの設定に使用できる次の 6 つのウィザードがあります。

- Citrix Gateway アプライアンスに初めてログオンすると、初回セットアップウィザードが表示されます。
- セットアップウィザードでは、Citrix Gateway の基本設定を初めて構成できます。
- Citrix Endpoint Management の統合構成は、Citrix Gateway と Citrix Endpoint Management 環境を構成するのに役立ちます。
- クイック構成ウィザードでは、Citrix Endpoint Management、StoreFront、および Web Interface への接続に関する正しいポリシー、式、および設定を構成できます。
- Citrix Gateway ウィザードでは、Citrix Gateway 固有の設定を構成できます。
- 公開アプリケーションウィザードでは、Citrix Workspace アプリを使用してユーザー接続の設定を構成できます。

初回セットアップウィザードの仕組み

Citrix Gateway アプライアンスの初期設定のインストールと構成が完了したら、構成ユーティリティに初めてログオンするときに、次の条件が満たされない場合は初回セットアップウィザードが表示されます。

- アプライアンスにライセンスがインストールされていません。
- サブネットまたはマッピング IP アドレスを設定していません。
- アプライアンスのデフォルト IP アドレスが 192.168.100.1 の場合。

セットアップウィザードの仕組み

セットアップウィザードを使用して、アプライアンスで次の初期設定を構成します。

- システム IP アドレスとサブネットマスク
- マッピングされた IP アドレスとサブネットマスク
- ホスト名
- デフォルトゲートウェイ
- ライセンス

注: セットアップウィザードを実行する前に、Citrix の Web サイトからライセンスをダウンロードしてください。詳細については、「
Citrix Gateway のライセンス」を参照してください。

統合 **Citrix Endpoint Management** 構成の仕組み

Citrix Endpoint Management MDM を使用して Citrix Gateway を展開すると、アプリケーションのスケーリング、高可用性の確保、およびセキュリティの維持が可能です。Citrix Endpoint Management 構成を使用するには、

バージョン 10.1、ビルド 120.1316.e をインストールする必要があります。

統合 Citrix Endpoint Management 構成では、次のものが作成されます。

- デバイスマネージャ用のロードバランシングサーバ。
- メールフィルタリング機能を備えた Microsoft Exchange 用のサーバーの負荷分散。
- ShareFile 用のサーバーの負荷分散。

統合 Citrix Endpoint Management 構成での設定の作成について詳しくは、「Citrix Endpoint Management 環境の設定の構成」を参照してください。

クイック構成ウィザードの仕組み

クイック構成ウィザードでは、Citrix Gateway で複数の仮想サーバーを構成できます。仮想サーバーを追加、編集、削除できます。

クイック構成ウィザードでは、次の展開をシームレスに構成できます。

- Citrix Virtual Apps and Desktops への Web Interface 接続。Secure Ticket Authority（STA）の複数のインスタンスを構成できます。
- Citrix Endpoint Management のみ
- StoreFront のみ
- Citrix Endpoint Management と StoreFront の併用

クイック構成ウィザードでは、アプライアンスで次の設定を構成できます。

- 仮想サーバ名、IP アドレス、およびポート
- 非セキュアポートからセキュアポートへのリダイレクション
- LDAP サーバー
- RADIUS サーバー
- 証明書
- DNS サーバー
- Citrix Endpoint Management と Citrix Virtual Apps and Desktops

Citrix Gateway は、Citrix Endpoint Management へのユーザー接続を直接サポートします。これにより、ユーザーは ShareFile へのアクセスに加えて、自分の Web、SaaS、およびモバイルアプリケーションにアクセスできるようになります。StoreFront の設定を構成して、ユーザーが Windows ベースのアプリケーションおよび仮想デスクトップにアクセスできるようにすることもできます。

クイック構成ウィザードを実行すると、Citrix Endpoint Management、StoreFront および Web Interface の設定に基づいて、次のポリシーが作成されます。

- セッションポリシー（Receiver、Receiver for Web、Citrix Gateway プラグイン、およびプログラムネイバーフッドエージェントのポリシーとプロファイルなど）
- クライアントレスアクセス
- LDAP および RADIUS 認証

Citrix Gateway ウィザードの仕組み

Citrix Gateway ウィザードを使用して、アプライアンスで次の設定を構成します。

- 仮想サーバー
- 証明書
- ネームサービスプロバイダ
- 認証
- 承認
- ポートのリダイレクト
- クライアントレスアクセス
- SharePoint のクライアントレス・アクセス

公開アプリケーションウィザードの仕組み

公開アプリケーションウィザードを使用して、内部ネットワーク内の Citrix Virtual Apps and Desktops を実行しているサーバーに接続するように Citrix Gateway を構成します。公開アプリケーションウィザードでは、次の操作を実行できます。

- サーバファームに接続する仮想サーバを選択します。
- Web Interface または StoreFront のユーザー接続、シングルサインオン、および Secure Ticket Authority の設定を構成します。
- SmartAccess のセッションポリシーを作成または選択します。

ウィザード内では、ユーザー接続用のセッションポリシー式を作成することもできます。サーバーファームに接続するように Citrix Gateway を構成する方法の詳細については、「Web Interface を使用した公開アプリケーションおよび Virtual Desktops へのアクセスの提供」を参照してください。

初回セットアップウィザードを使用した **Citrix Gateway** の構成

March 26, 2020

Citrix Gateway（物理アプライアンスまたは VPX 仮想アプライアンス）を初めて構成するには、アプライアンスと同じネットワーク上に構成された管理コンピューターが必要です。

アプライアンスの管理 IP アドレスとして、Citrix Gateway IP（NSIP）アドレスと、サーバーが接続できるサブネット IP（SNIP）アドレスを割り当てる必要があります。Citrix Gateway と SNIP アドレスの両方に適用されるサブネットマスクを割り当てます。タイムゾーンも設定する必要があります。ホスト名を割り当てる場合は、NSIP アドレスの代わりに名前を指定してアプライアンスにアクセスできます。

初回セットアップウィザードには、2 つのセクションがあります。最初のセクションでは、Citrix Gateway アプライアンスの基本的なシステム設定を構成します。

- NSIP アドレス、SNIP アドレス、サブネット・マスク
- アプライアンスのホスト名
- DNS サーバー
- タイムゾーン
- 管理者パスワード

2 番目のセクションでは、ライセンスをインストールします。DNS サーバーのアドレスを指定すると、ローカルコンピューターからアプライアンスにライセンスをアップロードする代わりに、ハードウェアシリアル番号 (HSN) またはライセンスアクティベーションコード (LAC) を使用してライセンスを割り当てることができます。

注：ライセンスをローカルコンピュータに保存することをお勧めします。

これらの設定の構成が完了すると、Citrix Gateway からアプライアンスの再起動を求めるメッセージが表示されます。アプライアンスに再度ログオンすると、他のウィザードと構成ユーティリティを使用して追加設定を構成できます。

Configuring Settings with the Quick Configuration Wizard

April 9, 2020

Citrix Gateway で、クイック構成ウィザードを使用して、Citrix Endpoint Management、StoreFront、または Web Interface との通信を有効にするための設定を構成できます。構成が完了すると、ウィザードによって、Citrix Gateway、Endpoint Management、StoreFront、または Web Interface 間の通信に関する適切なポリシーが作成されます。これらのポリシーには、認証、セッション、およびクライアントレスアクセスポリシーが含まれます。ウィザードが完了すると、ポリシーが仮想サーバにバインドされます。

クイック構成ウィザードを完了すると、Citrix Gateway は Endpoint Management または StoreFront と通信でき、ユーザーは Windows ベースのアプリケーション、仮想デスクトップ、Web、SaaS、およびモバイルアプリケーションにアクセスできます。ユーザーは Endpoint Management に直接接続できます。

ウィザードでは、次の設定を構成します。

- 仮想サーバ名、IP アドレス、およびポート
- 非セキュアポートからセキュアポートへのリダイレクション
- 証明書
- LDAP サーバー
- RADIUS サーバー
- 認証用のクライアント証明書 (2 要素認証のみ)
- Endpoint Management、StoreFront、または Web Interface

クイック構成ウィザードは、LDAP、RADIUS、およびクライアント証明書の認証をサポートします。ウィザードで 2 要素認証を構成するには、次のガイドラインに従います。

- プライマリ認証タイプとして LDAP を選択した場合は、セカンダリ認証タイプとして RADIUS を設定できます。
- プライマリ認証タイプとして RADIUS を選択した場合は、セカンダリ認証タイプとして LDAP を設定できます。
- プライマリ認証タイプとしてクライアント証明書を選択した場合は、セカンダリ認証タイプとして LDAP または RADIUS を設定できます。

クイック構成ウィザードを使用して複数の LDAP 認証ポリシーを作成することはできません。たとえば、[サーバーログオン名の属性] フィールドで sAMAccountName を使用するポリシーと、[サーバーログオン名の属性] フィールドでユーザープリンシパル名 (UPN) を使用する LDAP ポリシーを構成するとします。これらの個別のポリシーを構成するには、Citrix Gateway 構成ユーティリティを使用して認証ポリシーを作成します。詳しくは、「LDAP 認証の構成」を参照してください。

簡易構成ウィザードでは、以下の方法を使用して、Citrix Gateway の証明書を構成できます。

- アプライアンスにインストールされている証明書を選択します。
- 証明書と秘密キーをインストールします。
- テスト証明書を選択します。
  注: テスト証明書を使用する場合は、証明書に含まれる完全修飾ドメイン名 (FQDN) を追加する必要があります。

クイック構成ウィザードは、次の 2 つの方法のいずれかで開くことができます。

- Citrix Gateway のログオンページで、［展開の種類］で［Citrix Gateway］を選択すると、［ホーム］タブが表示されます。[展開の種類] で他のオプションを選択すると、[ホーム] は表示されません。
- Citrix Gateway の詳細ペインの［Citrix Gateway の作成/監視］リンクから選択します。Citrix ADC 機能を有効にするライセンスをインストールすると、このリンクが表示されます。Citrix Gateway のみのアプライアンスのライセンスを取得した場合、リンクは表示されません。

ウィザードを最初に実行した後、ウィザードを再度実行して、追加の仮想サーバーと設定を作成できます。

重要: クイック構成ウィザードを使用して追加の Citrix Gateway 仮想サーバーを構成する場合は、一意の IP アドレスを使用する必要があります。既存の仮想サーバーで使用されている IP アドレスと同じ IP アドレスを使用することはできません。たとえば、IP アドレスが 192.168.10.5 で、ポート番号が 80 の仮想サーバーがあるとします。ポート番号 443 の IP アドレス 192.168.10.5 の 2 番目の仮想サーバーを作成するのには、クイック構成ウィザードを実行します。構成を保存しようとすると、エラーが発生します。

クイック構成ウィザードで設定を構成するには

1. 構成ユーティリティで、次のいずれかの操作を行います。
   a) アプライアンスに Citrix Gateway のみのライセンスが付与されている場合は、［ホーム］タブをクリックします。
   b) アプライアンスに Citrix ADC 機能を含めるライセンスが付与されている場合は、［構成］タブのナビゲーションペインで［Citrix Gateway］をクリックし、詳細ペインの［はじめに］で［エンタープライズ

ストア用の Citrix Gateway の構成］をクリックします。

2. ダッシュボードで、［新しい Citrix Gateway の作成］をクリックします。
3. Citrix Gateway の設定で、以下を構成します。
   a) [名前] に、仮想サーバーの名前を入力します。
   b) [IP アドレス] に、仮想サーバーの IP アドレスを入力します。
   c) ［Port］ボックスにポート番号を入力します。デフォルトのポート番号は 443 です。
   d) ポート 80 からポート 443 へのユーザー接続を許可するには、[ポート 80 からセキュアポートへ要求をリダイレクト] を選択します。
4. ［続行］をクリックします。
5. [証明書] ページで、次のいずれかの操作を行います。
   a) [証明書の選択] をクリックし、[証明書] で証明書を選択します。
   b) [証明書のインストール] をクリックし、[証明書の選択] で [キーの選択] の [参照] をクリックして、証明書と秘密キーに移動します。
   c) [テスト証明書の使用] をクリックし、[証明書 FQDN] に、テスト証明書に含まれる完全修飾ドメイン名 (FQDN) を入力します。
6. ［続行］をクリックします。
7. [認証設定] で、次の操作を行います。
   a) [プライマリ認証] で、[LDAP]、[RADIUS]、または [証明書] を選択します。
   b) 認証サーバーを選択するか、前の手順で選択した認証タイプの設定を構成します。[Cert] を選択した場合は、クライアント証明書を選択するか、新しいクライアント証明書をインストールします。
   c) [セカンダリ認証] で、認証の種類を選択し、認証サーバーの設定を構成します。
8. ［続行］をクリックします。

ネットワークと認証の設定が完了したら、Citrix Endpoint Management または Citrix Virtual Apps and Desktops（StoreFront または Web Interface）の設定を構成できます。

エンタープライズストア設定の構成

Citrix Gateway では、Web、SaaS、モバイルアプリケーションおよび ShareFile へのユーザーアクセスは、Endpoint Management 経由でのみサポートされます。StoreFront または Web Interface も展開すると、ユーザーは Windows ベースのアプリと仮想デスクトップにアクセスできます。次のオプションの設定を構成できます。

- Endpoint Management のみ
- StoreFront のみ
- Endpoint Management と StoreFront の併用
- Web Interface のみ

前の手順で [続行] をクリックすると、展開シナリオの設定を構成できます。次の手順は、Citrix の統合設定ページで開始します。

仮想サーバーを作成した後、クイック構成ウィザードで仮想サーバーを編集しても、Citrix Endpoint Management または Citrix Virtual Apps and Desktops の設定は変更できません。

たとえば、Citrix Enterprise Store の設定を構成する前に仮想サーバーの構成をキャンセルすると、設定を行わずに Web インターフェイスが自動的に選択されます。この状況が発生した場合、Web Interface を構成するために仮想サーバーの詳細を編集することはできますが、Citrix Endpoint Management に切り替えることはできません。切り替えるには、新しい仮想サーバを作成する必要があります。構成中はウィザードをキャンセルしないでください。Web Interface 仮想サーバーが必要ない場合は、クイック構成ウィザードを使用して削除できます。

StoreFront のみの設定を構成するには

1. ［Citrix Virtual Apps and Desktops］をクリックします。
2. [展開の種類] で、[StoreFront] を選択します。
3. StoreFront サーバーの完全修飾ドメイン名（FQDN）に、StoreFront サーバーの完全修飾ドメイン名（FQDN）を入力します。
4. Receiver for Web パスで、デフォルトのパスをそのまま使用するか、独自のパスを入力します。
5. セキュアなユーザー接続の場合は、[HTTPS] を選択します。
6.「シングルサインオンドメイン」で、StoreFront のドメインを入力します。
7. StoreFront を展開し、Citrix Virtual Apps または Citrix Virtual Desktops から公開アプリケーションへのアクセスを許可する場合は、STA URL に、Secure Ticket Authority（STA）を実行しているサーバーの完全な IP アドレスまたは FQDN を入力します。
8. ［完了］をクリックします。

ユーザーが Citrix Gateway 経由で StoreFront に接続すると、ユーザーは Receiver for Web または Receiver からアプリやデスクトップを起動できます。

Endpoint Management のみの設定を構成するには

1. ［Citrix Endpoint Management］をクリックします。
2. [App Controller FQDN] に、Endpoint Management の FQDN を入力します。
3. ［完了］をクリックします。

Web Interface 設定を構成するには

1. クイック構成ウィザードで、［Citrix Virtual Apps and Desktops］をクリックします。
2. [展開の種類] で [Web Interface] を選択し、次の構成を行います。
   a) ［Citrix Virtual Apps サイトの URL］に、Web Interface の完全な IP アドレスまたは FQDN を入力します。
   b) Citrix Virtual Apps サービスサイトの URL に、PNAgent パスを含む Web Interface の完全な IP アドレスまたは FQDN を入力します。既定のパスを入力することも、独自のパスを入力することもできます。
   c)「シングル・サインオン・ドメイン」で、使用するドメインを入力します。
   d) [STA URL] に、STA を実行しているサーバーの完全な IP アドレスまたは FQDN を入力します。
3. ［完了］をクリックします。

Citrix Gateway ウィザードを使用した設定の構成

April 9, 2020

セットアップウィザードを実行した後、Citrix Gateway ウィザードを実行して Citrix Gateway に追加の設定を構成できます。Citrix Gateway ウィザードは、構成ユーティリティから実行します。

Citrix Gateway には、テスト証明書が付属しています。認証局（CA）からの署名付き証明書がない場合は、Citrix Gateway ウィザードを使用してテスト証明書を使用できます。署名付き証明書を受け取ったら、テスト証明書を削除し、署名付き証明書をインストールできます。Citrix Gateway を公開する前に、署名付き証明書を取得することをお勧めします。

注：証明書署名リクエスト（CSR）は、Citrix Gateway ウィザードから作成できます。Citrix Gateway ウィザードを使用して CSR を作成する場合は、ウィザードを終了し、CA から署名付き証明書を受け取ったときにウィザードを再度開始する必要があります。証明書について詳しくは、「
証明書のインストールと管理」を参照してください。

仮想サーバーを構成するときに、Citrix Gateway ウィザードでインターネットプロトコルバージョン 6（IPv6）のユーザー接続を構成できます。ユーザー接続の IPv6 の使用について詳しくは、ユーザ接続用の IPv6 の設定を参照してください。

Citrix Gateway ウィザードを起動するには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］をクリックします。
2. 詳細ペインの [はじめに] で、[Citrix Gateway ウィザード] をクリックします。
3. ［Next］をクリックして、ウィザードの指示に従います。

Citrix Gateway でのホスト名および完全修飾ドメイン DN の構成

March 26, 2020

ホスト名は、ライセンスファイルに関連付けられた Citrix Gateway アプライアンスの名前です。ホスト名はアプライアンスに固有で、ユニバーサルライセンスをダウンロードするときに使用されます。ホスト名は、セットアップウィザードを実行して Citrix Gateway を初めて構成するときに定義します。

完全修飾ドメイン名 (FQDN) は、仮想サーバーにバインドされる署名付き証明書に含まれます。Citrix Gateway で FQDN を構成しないでください。1 つのアプライアンスは、証明書を使用して Citrix Gateway で構成された各仮想サーバーに、一意の FQDN を割り当てることができます。

証明書の詳細を表示すると、証明書の FQDN を検索できます。FQDN は、証明書のサブジェクトフィールドにあります。

証明書の **FQDN** を表示するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[SSL] を展開し、[証明書] をクリックします。
2. 詳細ペインで証明書を選択し、[操作]、[詳細] の順にクリックします。
3. [証明書の詳細] ダイアログボックスで、[件名] をクリックします。証明書の FQDN が一覧に表示されます。

証明書のインストールと管理

March 26, 2020

Citrix Gateway では、証明書を使用して安全な接続を作成し、ユーザーを認証します。

セキュアな接続を確立するには、接続の一方の端にサーバー証明書が必要です。サーバー証明書を発行した認証局 (CA) のルート証明書は、接続のもう一方の端に必要です。

- サーバー証明書。サーバー証明書は、サーバーの ID を証明します。Citrix Gateway では、この種類のデジタル証明書が必要です。
- ルート証明書。ルート証明書は、サーバー証明書に署名した CA を識別します。ルート証明書は CA に属します。ユーザーデバイスでは、サーバー証明書を検証するために、このタイプのデジタル証明書が必要です。

ユーザーデバイス上の Web ブラウザとの安全な接続を確立すると、サーバーはその証明書をデバイスに送信します。

ユーザーデバイスがサーバー証明書を受信すると、Internet Explorer などの Web ブラウザは、証明書を発行した CA と、その CA がユーザーデバイスによって信頼されているかどうかを確認します。CA が信頼されていない場合、またはテスト証明書の場合、Web ブラウザは、証明書を受け入れるか拒否するかをユーザに求めます（サイトへのアクセスを効果的に許可または拒否します）。

Citrix Gateway では、次の 3 種類の証明書がサポートされています。

- 仮想サーバーにバインドされ、サーバーファームへの接続にも使用できるテスト証明書。Citrix Gateway には、テスト証明書がプリインストールされています。
- CA によって署名され、秘密キーとペアになっている PEM または DER 形式の証明書。
- 証明書と秘密キーを格納または転送するために使用される PKCS #12 形式の証明書。PKCS #12 証明書は通常、既存の Windows 証明書から PFX ファイルとしてエクスポートされ、Citrix Gateway にインストールされます。

Thawte や VeriSign など、信頼された CA によって署名された証明書を使用することをお勧めします。

証明書署名要求の作成

April 9, 2020

SSL または TLS を使用してセキュアな通信を提供するには、Citrix Gateway でサーバー証明書が必要です。証明書を Citrix Gateway にアップロードする前に、証明書署名リクエスト（CSR）と秘密キーを生成する必要があります。Citrix Gateway ウィザードまたは構成ユーティリティに含まれている証明書要求の作成を使用して、CSR を作成します。証明書要求の作成は、署名のために認証局（CA）に電子メールで送信される.csr ファイルと、アプライアンスに残る秘密キーを作成します。CA は証明書に署名し、指定した電子メールアドレスで返却します。署名付き証明書を受け取ったら、Citrix Gateway にインストールできます。CA から証明書を受け取ったら、証明書を秘密キーとペアにします。

重要：Citrix Gateway ウィザードを使用して CSR を作成する場合は、ウィザードを終了し、署名付き証明書が CA から送信されるまで待つ必要があります。証明書を受け取ったら、Citrix Gateway ウィザードを再度実行して設定を作成し、証明書をインストールできます。Citrix Gateway ウィザードの詳細については、「Citrix Gateway ウィザードを使用した設定の構成」を参照してください。

Citrix Gateway ウィザードを使用して **CSR** を作成するには

1. 構成ユーティリティで、[構成] タブをクリックし、ナビゲーションペインで [Citrix ADC Gateway] をクリックします。
2. 詳細ペインの [はじめに] で、[Citrix ADC Gateway ウィザード] をクリックします。
3. [サーバー証明書の指定] ページが表示されるまで、ウィザードの指示に従います。
4. [証明書署名要求の作成] をクリックし、フィールドに入力します。
   注：完全修飾ドメイン名（FQDN）は、Citrix Gateway のホスト名と同じである必要はありません。FQDN は、ユーザーログオンに使用されます。
5. [作成] をクリックして証明書をコンピュータに保存し、[閉じる] をクリックします。
6. 設定を保存せずに Citrix Gateway ウィザードを終了します。

Citrix ADC GUI を使用して **CSR** を作成するには

CitrixCitrix Gateway ウィザードを実行せずに、Citrix ADC GUI を使用して CSR を作成することもできます。

1. [トラフィック 管理] > [**SSL] > [SSL** ファイル] に移動し、[証明書署名要求 **(CSR)** の作成] を選択します。
2. 証明書の設定を完了し、[作成] をクリックします。

証明書と秘密キーを作成したら、Thawte や VeriSign などの証明書を CA に電子メールで送信します。

Citrix Gateway への署名付き証明書のインストール

March 26, 2020

認証局（CA）から署名付き証明書を受け取ったら、アプライアンスの秘密キーとペアリングし、Citrix Gateway に証明書をインストールします。

署名付き証明書と秘密キーをペアリングするには

1. WinSCP などのセキュアシェル（SSH）プログラムを使用して、証明書を Citrix Gateway のフォルダ nsconfig/ssl にコピーします。
2. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[SSL] を展開し、[証明書] をクリックします。
3. 詳細ペインで、[Install] をクリックします。
4. [証明書とキーのペア名] に、証明書の名前を入力します。
5.「証明書ファイル名」で、「参照」のドロップダウン・ボックスを選択し、「アプライアンス」をクリックします。
6. 証明書に移動し、[選択]、[開く] の順にクリックします。
7.「秘密鍵ファイル名」で、「参照」のドロップダウン・ボックスを選択し、「アプライアンス」をクリックします。秘密キーの名前は、証明書署名要求 (CSR) と同じ名前です。秘密鍵は、Citrix Gateway の\ nsconfig\ ssl ディレクトリにあります。
8. 秘密キーを選択し、[開く] をクリックします。
9. 証明書が PEM 形式の場合は、[パスワード] に秘密キーのパスワードを入力します。
10. 証明書の有効期限が切れたときの通知を構成する場合は、[有効期限が切れたときに通知] を選択します。
11. [通知期間] に日数を入力し、[作成]、[閉じる] の順にクリックします。

証明書と秘密キーを仮想サーバーにバインドするには

証明書と秘密キーのペアを作成してリンクしたら、仮想サーバーにバインドします。

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、仮想サーバーをクリックし、[開く] をクリックします。
3. [証明書] タブの [使用可能] で証明書を選択し、[追加] をクリックし、[OK] をクリックします。

仮想サーバーからテスト証明書をバインド解除するには

署名付き証明書をインストールした後、仮想サーバーにバインドされているテスト証明書のバインドを解除します。構成ユーティリティーを使用して、テスト証明書のバインドを解除できます。

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、仮想サーバーをクリックし、[開く] をクリックします。
3. [証明書] タブの [構成済み] で、テスト証明書を選択し、[削除] をクリックします。

中間証明書の構成

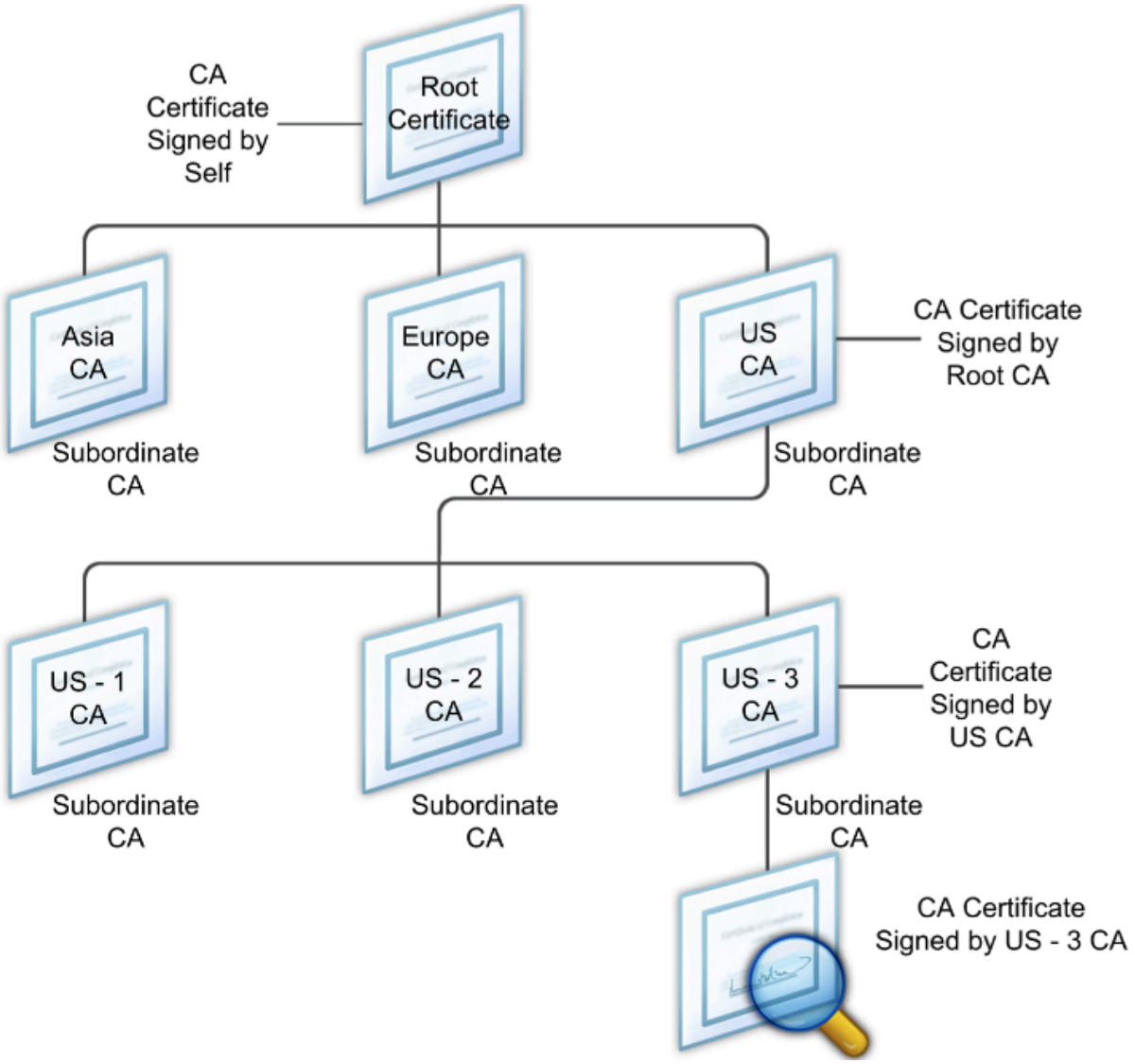
March 26, 2020

中間証明書は、Citrix Gateway（サーバー証明書）とルート証明書（通常はユーザーデバイスにインストールされます）の間にある証明書です。中間証明書はチェーンの一部です。

組織によっては、組織単位間の地理的分離の問題を解決するために、または組織の異なるセクションに異なる発行ポリシーを適用するために、証明書を発行する責任を委任します。

証明書を発行する責任は、下位の証明機関 (CA) を設定することで委任できます。CA は、独自の証明書に署名することも (自己署名付き)、別の CA によって署名することもできます。X.509 標準には、CA の階層を設定するためのモデルが含まれています。このモデルでは、次の図に示すように、ルート CA は階層の最上位にあり、CA による自己署名証明書です。ルート CA に直接従属する CA には、ルート CA によって署名された CA 証明書があります。階層内の下位 CA の下位 CA には、下位 CA によって署名された CA 証明書があります。

図 1: 一般的なデジタル証明書チェーンの階層構造を示す X.509 モデル



サーバ証明書が自己署名証明書を持つ CA によって署名されている場合、証明書チェーンは、エンドエンティティ証明書とルート CA の 2 つの証明書で構成されます。ユーザーまたはサーバー証明書が中間 CA によって署名されてい

る場合、証明書チェーンは長くなります。

次の図は、最初の 2 つの要素が、エンドエンティティ証明書（この場合は gwy01.company.com）と中間 CA の証明書をこの順序で示しています。中間 CA の証明書の後には、その CA の証明書が続きます。この一覧は、リストの最後の証明書がルート CA の証明書になるまで続きます。チェーン内の各証明書は、前の証明書の ID を証明します。

図 2：一般的なデジタル証明書チェーン

中間証明書をインストールするには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[SSL] を展開し、[証明書] をクリックします。
2. 詳細ペインで、[Install] をクリックします。
3. [証明書とキーのペア名] に、証明書の名前を入力します。
4. [詳細] の [証明書ファイル名] で、[参照] (アプライアンス) をクリックし、ドロップダウンボックスで [ローカル] または [アプライアンス] を選択します。
5. コンピュータ（ローカル）または Citrix Gateway（アプライアンス）上の証明書に移動します。
6.「証明書の形式」で「PEM」を選択します。
7. [インストール] をクリックし、[閉じる] をクリックします。

Citrix Gateway に中間証明書をインストールする場合、秘密鍵やパスワードを指定する必要はありません。

証明書がアプライアンスにインストールされたら、証明書をサーバー証明書にリンクする必要があります。

中間証明書をサーバー証明書にリンクするには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[SSL] を展開し、[証明書] をクリックします。
2. 詳細ウィンドウで、サーバー証明書を選択し、[操作] で [リンク] をクリックします。
3. [CA 証明書名] の横にある一覧から中間証明書を選択し、[OK] をクリックします。

認証にデバイス証明書を使用する

October 22, 2021

Citrix Gateway では、デバイス ID を証明書の秘密キーにバインドできるデバイス証明書チェックがサポートされています。デバイス証明書チェックは、従来の EPA ポリシーまたは高度な EPA ポリシーの一部として設定できます。従来の EPA ポリシーでは、デバイス証明書は事前認証 EPA に対してだけ設定できます。

Citrix Gateway に 2 つ以上のデバイス証明書をインストールする場合、ユーザーが Citrix Gateway へのログオンを開始するとき、またはエンドポイント分析スキャンを実行する前に、正しい証明書を選択する必要があります。

デバイス証明書を作成するときは、X.509 証明書である必要があります。

> 重要**:** Windows では、デフォルトで、デバイス証明書にアクセスするための管理者権限が義務されています。管理者以外のユーザのデバイス証明書チェックを追加するには、VPN プラグインをインストールする必要があります。VPN プラグインのバージョンは、デバイス上の EPA プラグインと同じバージョンである必要があります。

デバイス証明書の作成の詳細については、以下を参照してください。

- Active Directory 証明書サービス (AD CS) のネットワークデバイス登録サービス (NDES)を参照してください。
- Microsoft System Center web サイトの構成マネージャー用の PKI 証明書の展開手順の例:Windows Server 2008 証明機関を参照してください。
- DCE/RPC および Active Directory 証明書プロファイルペイロードを使用して、Microsoft Certificate Authority から証明書を要求する方法をアップルのサポートウェブサイトでご確認ください。
- iPad/iPhone の証明書発行「ディレクトリサービスチームに問い合わせる Microsoft サポートブログ」を参照してください。
- ネットワークデバイス登録サービスの設定を参照してください。

従来の **EPA** ポリシーの仮想サーバーでデバイス証明書を有効にしてバインドするには

デバイス証明書を作成したら、Citrix Gateway への既存の証明書のインポートとインストールの手順に従って Citrix Gateway に証明書をインストールします。証明書をインストールした後、証明書を仮想サーバーにバインドします。

1. 構成ユーティリティで、[**Citrix Gateway**] **>** [****** 仮想サーバー] ****** に移動します。
2. 詳細ウィンドウで、仮想サーバーをクリックし、[編集**]** をクリックします。
3. 仮想サーバーの詳細ウィンドウで、鉛筆アイコンをクリックし、[詳細] を展開します。
4. [デバイス証明書を有効にする**]** を選択します。
5. 表示される選択ダイアログで、[**Add**] を選択し、有効にするデバイス証明書をクリックします。選択したデバイス証明書の隣にあるプラス記号のアイコンをクリックし、[**OK**] をクリックします。

> 注: 高度な EPA ポリシーの仮想サーバー上でデバイス証明書を有効化およびバインドする方法については、EPA コンポーネントとしての nFactor でのデバイス証明書を参照してください。

既存の証明書のインポートとインストール

April 9, 2020

既存の証明書は、インターネットインフォメーションサービス（IIS）を実行している Windows ベースのコンピュータから、または Secure Gateway を実行しているコンピュータからインポートできます。

証明書をエクスポートするときは、秘密キーもエクスポートしてください。場合によっては、秘密キーをエクスポートできないため、Citrix Gateway に証明書をインストールできないことがあります。このような場合は、証明書署名要求 (CSR) を使用して新しい証明書を作成します。詳しくは、「証明書署名要求の作成」を参照してください。

証明書と秘密キーを Windows からエクスポートすると、コンピューターによって個人情報交換 (.pfx) ファイルが作成されます。このファイルは、PKCS #12 証明書として Citrix Gateway にインストールされます。

Secure Gateway を Citrix Gateway Gateway に置き換える場合は、証明書と秘密鍵を Secure Gateway からエクスポートできます。Secure Gateway から Citrix Gateway Gateway へのインプレース移行を行う場合は、アプリケーションとアプライアンスの完全修飾ドメイン名（FQDN）が同じである必要があります。Secure Gateway から証明書をエクスポートすると、すぐに Secure Gateway を破棄し、Citrix Gateway に証明書をインストールしてから、構成をテストします。FQDN が同じであれば、ネットワーク上で Secure Gateway と Citrix Gateway を同時に実行することはできません。

Windows Server 2003 または Windows Server 2008 を使用している場合は、Microsoft Management Console を使用して証明書をエクスポートできます。詳細については、Windows オンラインヘルプを参照してください。

他のすべてのオプションのデフォルト値をそのまま使用し、パスワードを定義して、.pfx ファイルをコンピューターに保存します。証明書をエクスポートしたら、Citrix Gateway にインストールします。

証明書と秘密キーを **Citrix Gateway** にインストールするには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］をクリックします。
2. 詳細ペインの [はじめに] で、[Citrix Gateway ウィザード] をクリックします。
3. [次へ] をクリックし、既存の仮想サーバーを選択して、[次へ] をクリックします。
4. [証明書オプション] で、[PKCS #12 (.pfx) ファイルをインストールする] を選択します。
5. [PKCS #12 ファイル名] で、[参照] をクリックし、証明書に移動し、[選択] をクリックします。
6. [パスワード] に、秘密キーのパスワードを入力します。

   これは、証明書を PEM 形式に変換するときに使用したパスワードです。
7. ［次へ］をクリックして、他の設定を変更せずに Citrix Gateway ウィザードを終了します。

証明書が Citrix Gateway にインストールされると、証明書は構成ユーティリティの［SSL］>［証明書］ノードに表示されます。

秘密キーを作成するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[SSL] をクリックします。
2. 詳細ペインの [SSL キー] で、[RSA キーの作成] をクリックします。
3. [Key Filename] にプライベートキーの名前を入力するか、[Browse] をクリックして既存のファイルに移動します。
4. [キーサイズ (ビット)] に、秘密キーのサイズを入力します。
5. [公衆指数] で、[F4] または [3] を選択します。

   RSA キーの公開指数値。これは暗号アルゴリズムの一部であり、RSA キーの作成に必要です。値は F4 (16 進数:0x10001) または 3 (16 進数:0x3) です。デフォルトは F4 です。
6. [キー形式] で、[PEM] または [DER] を選択します。証明書には PEM 形式をお勧めします。
7. [PEM エンコーディングアルゴリズム] で、[DES] または [DES3] を選択します。
8. [PEM パスフレーズ] および [パスフレーズの検証] にパスワードを入力し、[作成]、[閉じる] の順にクリックします。

   注: パスフレーズを割り当てるには、[
   Key Format] が PEM である必要があり、エンコードアルゴリズムを選択する必要があります。

構成ユーティリティで DSA 秘密キーを作成するには、[DSA キーの作成] をクリックします。上記の同じ手順に従って DSA 秘密キーを作成します。

証明書を **PFX** 形式から **PEM** 形式に変換する

March 26, 2020

SSL 証明書は、SSL 負荷分散仮想サーバーおよび Citrix Gateway 仮想サーバーに使用されます。PEM 証明書は Base64 でエンコードされた ASCII ファイルです。PEM 証明書は、テキストエディタ/メモ帳で開くことができ、それらには「—–BEGIN CERTIFICATE—–」および「—–END CERTIFICATE—–」ステートメントが含まれていることがわかります。

セキュアで信頼できるアクセスのためには、Citrix Gateway サーバーに SSL サーバー証明書をインストールする必要があります。アップロードされた証明書ファイルには、次の特性が必要です。

- サーバー証明書は、エンドユーザーが信頼する証明機関 (CA) によって発行されている必要があります。最良の結果を得るには、ベリサイン、Thawte、ジオトラストなどの商用 CA を使用してください。
- 証明書は、プライバシー拡張メール (PEM) 形式である必要があります。これは、バイナリ識別符号化規則 (DER) 形式の Base64 エンコーディングであるテキストベースの形式です。
- 証明書ファイルに秘密キーを含める必要があり、秘密キーを暗号化しないでください。PEM ファイルを使用するためにパスワードは必要ありません。

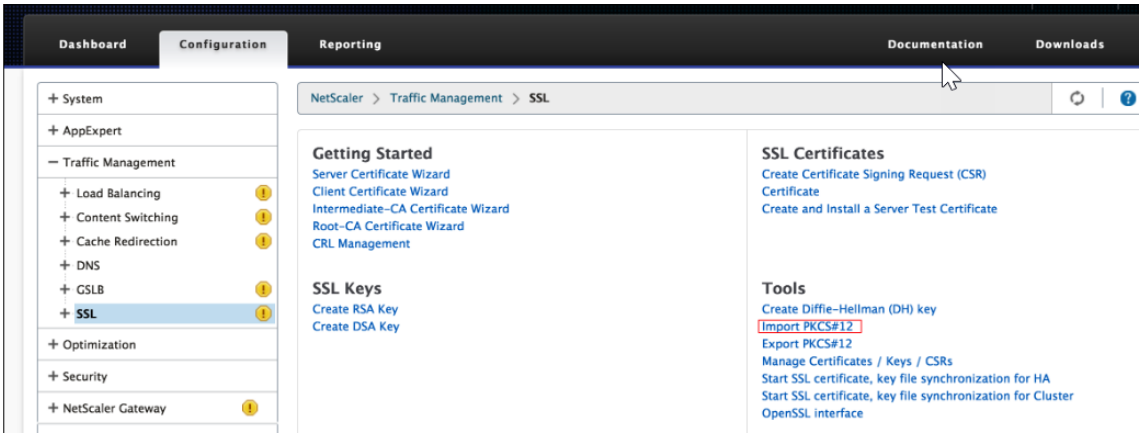
- 必要な中間証明書も PEM ファイルの末尾に追加する必要があります。

PFX 証明書を PEM 形式に変換して Citrix Gateway で使用するには、次のいずれかの手順を実行します。

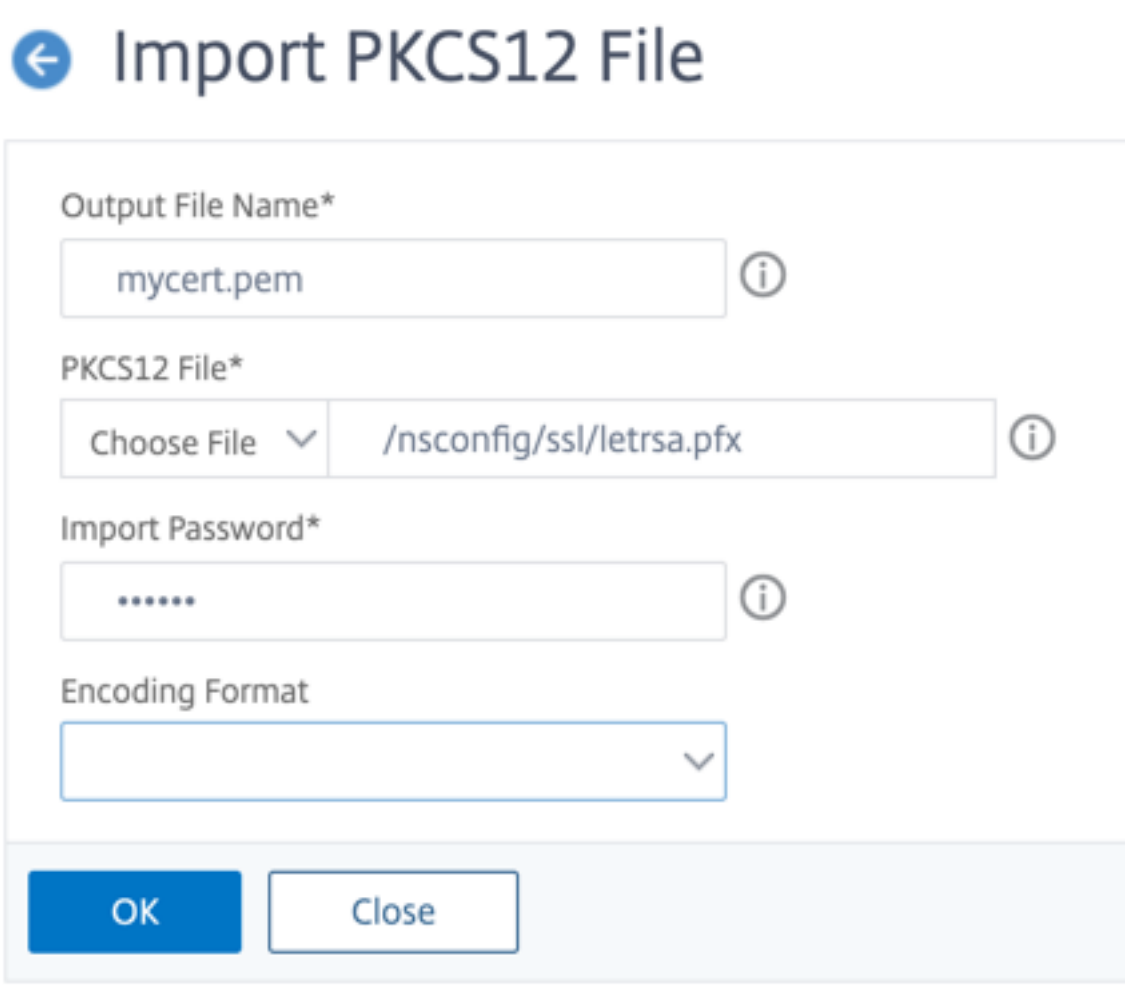
Citrix Gateway ウィザード

Citrix Gateway ウィザードを使用して PFX 証明書を PEM 形式に変換するには、以下の手順を実行します。

1. 「トラフィック管理」に移動し、「SSL」ノードを選択します。
2. [PKCS #12 のインポート] リンクをクリックします。

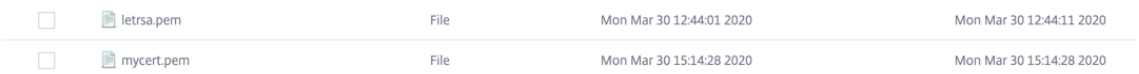


3. PEM 証明書のファイル名を [出力ファイル名] フィールドに指定します。
4. [参照] をクリックし、PEM 形式に変換する PFX 証明書を選択します。一部のユーザーは、証明書を/ncsonfig/SSL ディレクトリにアップロードし、そこから使用することを好みます。PFX 証明書が Citrix Gateway に保存されている場合は、［アプライアンス］オプションを選択し、ワークステーションに保存されている場合は［ローカル］を使用します。



5. 「インポート・パスワード」を指定します。
6. [OK] をクリックします。
7. ファイルがエンコードされている場合は、エンコード形式として DES または 3DES を選択します。
8. [PEM パスフレーズ] と [PEM パスフレーズの確認] を指定します。
9. [証明書/キー/ CSR の管理] リンクをクリックして、変換された PEM 証明書ファイルを表示します。

10. 変換された PEM ファイルと共に、アップロードされた PFX ファイルを表示できます。



11. [SSL] ノードを展開します。
12.「証明書」ノードを選択します。
13.［Install］をクリックします。
14. 証明書のインストールウィザードで、証明書とキーのペア名を指定します。
15. 証明書ファイル名と秘密キーファイル名の両方の PEM ファイルを参照します。
16. パスワードを指定します。
17.［Install］をクリックします。

オープン **SSL** ユーティリティ

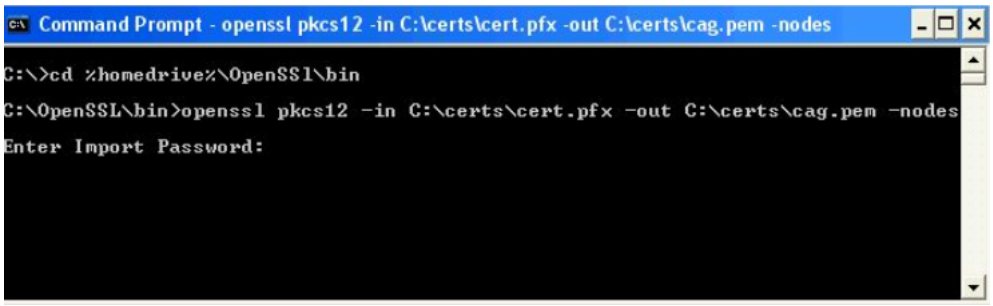
インターネットインフォメーションサービス (IIS) 証明書ウィザードを使用して Windows サーバーに証明書を要求してインストールした場合は、その証明書を秘密キーとともに個人情報交換 (PFX) ファイルにエクスポートできます。この証明書を Citrix Gateway にインポートするには、PFX ファイルを暗号化されていない PEM 形式に変換する必要があります。

オープンソースユーティリティ OpenSSL を使用して、PFX から PEM への変換を実行できます。オープン SSL の Win32 ディストリビューションをダウンロードします。

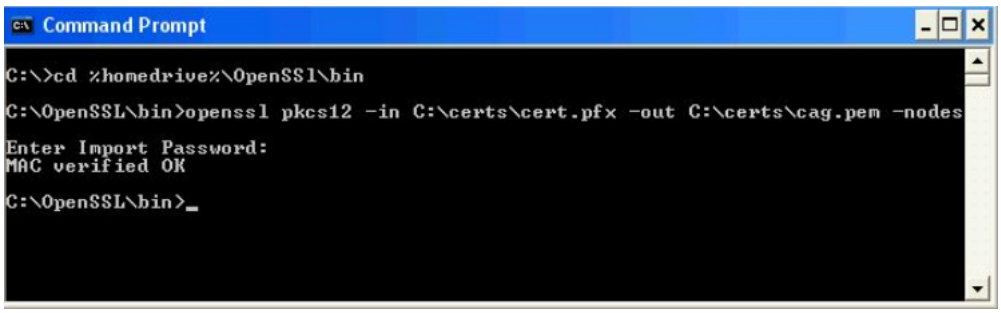
OpenSSL を使用する場合は、C++ の再配布可能ファイルが必要になることもあります。Microsoft Visual C++ 2008 再頒布可能パッケージ (x86) からダウンロードします。

PFX ファイルを PEM ファイルに変換するには、Windows マシンで次の手順を実行します。

1. ダウンロードして、Win32 OpenSSL からパッケージをインストールします。
2. c:\certs フォルダを作成し、c:\certs フォルダに yourcert.pfx ファイルをコピーします。
3. コマンドプロンプトを開き、OpenSSL\bin directory: %homedrive%\OpenSSL\bin に変更します。
4. 次のコマンドを実行して、PFX ファイルを暗号化されていない PEM ファイルに変換します (すべて 1 行で)。
   openssl pkcs12-in c:\certs\yourcert.pfx-out c:\certs\cag.pem —nodes



5. インポートパスワードの入力を求められたら、証明書を PFX ファイルにエクスポートするときに使用したパスワードを入力します。MAC が確認済みであることを示すメッセージが表示されます。



6. Citrix Gateway 管理ポータルまたは HTTPS ポート 9001 をブラウザに指定します。`https://netscaler-gateway-server:9001`
7. root としてログオンします。デフォルトのパスワードは rootadmin です。
8. ページ上部の [メンテナンス] リンクをクリックします。
9. [秘密鍵 + 証明書 (.pem) のアップロード] フィールドの横にある [参照] ボタンをクリックします。c:\certs\cag.pem ファイルを参照し、[アップロード] をクリックします。
10. 新しい SSL 証明書を適用するには、Citrix Gateway を再起動します。

証明書失効リスト

March 26, 2020

認証局 (CA) は時折、証明書失効リスト (CRL) を発行します。CRL には、信頼できなくなった証明書に関する情報が含まれています。たとえば、アンが XYZ 社を離れるとします。同社は、アンの証明書を CRL に配置して、そのキーでメッセージに署名できないようにすることができます。

同様に、秘密キーが侵害された場合、または証明書の有効期限が切れて新しい証明書が使用されている場合に、証明書を取り消すことができます。公開キーを信頼する前に、証明書が CRL に表示されていないことを確認してください。

Citrix Gateway では、次の 2 つの CRL タイプがサポートされています。

- 失効した、または有効でなくなった証明書を一覧表示する CRL
- オンライン証明書ステータス・プロトコル（OSCP)。X.509 証明書の失効ステータスを取得するために使用されるインターネット・プロトコル

CRL を追加するには

Citrix Gateway アプライアンスで CRL を構成する前に、CRL ファイルがアプライアンス上にローカルに保存されていることを確認してください。高可用性セットアップの場合、CRL ファイルは両方の Citrix Gateway アプライアンスに存在し、ファイルへのディレクトリパスは両方のアプライアンスで同じである必要があります。

CRL を更新する必要がある場合は、次のパラメータを使用できます。

- CRL 名: Citrix ADC に追加される CRL の名前。最大 31 文字です。
- CRL ファイル: Citrix ADC に追加される CRL ファイルの名前です。デフォルトでは、/var/netscaler/ssl ディレクトリ内の CRL ファイルが検索されます。最大 63 文字です。
- URL: 最大 127 文字
- ベース DN: 最大 127 文字
- バインド DN: 最大 127 文字
- パスワード: 最大 31 文字
- 日: 最大 31 日

1. 構成ユーティリティの [構成] タブで、[SSL] を展開し、[CRL] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [Add CRL] ダイアログボックスで、次の値を指定します。
    - CRL 名
    - CRL ファイル
    - フォーマット (オプション)
    - CA 証明書（オプション）
4. [**Create**] をクリックしてから、[**Close**] をクリックします。CRL 詳細ペインで、構成した CRL を選択し、画面の下部に表示される設定が正しいことを確認します。

構成ユーティリティで **LDAP** または **HTTP** を使用して **CRL** 自動リフレッシュを構成するには

CRL は、CA によって定期的に、または場合によっては特定の証明書が失効した直後に生成および発行されます。Citrix Gateway アプライアンスで CRL を定期的に更新して、無効な証明書で接続しようとするクライアントから保護することをお勧めします。

Citrix Gateway アプライアンスは、Web ロケーションまたは LDAP ディレクトリから CRL を更新できます。更新パラメータと Web の場所または LDAP サーバーを指定する場合、コマンドの実行時にローカルハードディスクドライブに CRL が存在する必要はありません。最初の更新では、CRL File パラメーターで指定されたパスに、ローカルハードディスクドライブにコピーが格納されます。CRL を保存するためのデフォルトのパスは /var/netscaler/sl です。

CRL リフレッシュパラメータ

- **CRL** 名

Citrix Gateway で更新される **CRL** の名前。

```
1 **CRL 自 動 更 新 の 有 効 化 **
```

CRL 自動更新を有効または無効にします。


```
**CA 証 明 書 **
```

CRL を発行した **CA** の証明書。この **CA** 証明書は、アプライアンスにインストールする必要があります。**Citrix ADC** は、証明書がインストールされている **CA** からのみ **CRL** を更新できます。

```
** 方 法 **
```

Web サーバ（**HTTP**）または **LDAP** サーバから **CRL** リフレッシュを取得するプロトコル。指定可能な値**:HTTP**、**LDAP**。デフォルトは **HTTP** です。

```
** ス コ ー プ **
```

LDAP サーバーでの検索操作の範囲。指定したスコープが
Base の場合、検索はベース DN と同じレベルになります。指定されたスコープが「
One」の場合、検索はベース DN の 1 レベル下まで拡張されます。

- サーバー **IP**

CRL の取得元となる **LDAP** サーバの **IP** アドレス。**IPv6 IP** アドレスを使用するには、**[IPv6]** を選択します。

```
** ポ ー ト **
```

LDAP または **HTTP** サーバーが通信するポート番号。

```
**URL**
```

CRL の取得元となる **Web** ロケーションの **URL**。

```
** ベ ー ス  DN**
```

LDAP サーバが CRL 属性を検索するために使用するベース DN。
注：LDAP サーバーで CRL を検索するには、CA 証明書の発行元名ではなくベース DN 属性を使用することをお勧めします。Issuer-Name フィールドが LDAP ディレクトリ構造の DN と正確に一致しない場合があります。

- バインド **DN**

LDAP リポジトリ内の **CRL** オブジェクトにアクセスするために使用されるバインド **DN** 属性。バインド **DN** アトリビュートは、**LDAP** サーバの管理者クレデンシャルです。**LDAP** サーバへの不正アクセスを制限するには、このパラメータを設定します。

```
1  **パスワード**
```

LDAP リポジトリ内の **CRL** オブジェクトへのアクセスに使用する管理者パスワード。これは、**LDAP** リポジトリへのアクセスが制限されている場合、つまり匿名アクセスが許可されていない場合に必要です。

```
1  **間隔**
```

CRL リフレッシュを実行する間隔。**CRL** を瞬時に更新する場合は、間隔を **NOW** として指定します。可能な値：**MONTHLY**、**DAILY**、**WEEKLY**、**NOW**、**NONE**。

```
1  **日**
```

CRL 更新を実行する日。間隔が **DAILY** に設定されている場合、このオプションは使用できません。

```
1  **時間**
```

CRL 更新を実行する時刻を **24** 時間形式で指定します。

```
1  **バイナリ**
```

LDAP ベースの CRL 取得モードをバイナリに設定します。指定可能な値: はい、いいえ。デフォルト： NO。

1. ナビゲーションウィンドウで、[SSL] を展開し、[CRL] をクリックします。
2. 更新パラメータを更新する設定済みの CRL を選択し、[Open] をクリックします。
3. [CRL 自動更新を有効にする] オプションを選択します。
4. 「CRL 自動リフレッシュ・パラメータ」グループで、次のパラメータの値を指定します。
   注意: アスタリスク（*）は必須パラメータを示します。
   - 方法
   - バイナリ
   - Scope
   - Server IP
   - Port*
   - URL
   - Base DN*

- Bind DN
- Password
- Interval
- Day(s)
- Time

5. ［作成］をクリックします。[CRL] ペインで、構成した CRL を選択し、画面の下部に表示される設定が正しいことを確認します。

OCSP による証明書ステータスのモニタリング

March 26, 2020

オンライン証明書状態プロトコル (OCSP) は、クライアントの SSL 証明書の状態を決定するために使用されるインターネットプロトコルです。Citrix Gateway は、RFC 2560 で定義されている OCSP をサポートしています。OCSP には、タイムリーな情報という点で、証明書失効リスト (CRL) よりも大きな利点があります。クライアント証明書の最新の失効ステータスは、多額の金銭や価値の高い株式取引を含む取引で特に役立ちます。また、使用するシステムリソースとネットワークリソースも少なくなります。Citrix Gateway の OCSP 実装には、リクエストのバッチ処理とレスポンスのキャッシュが含まれます。

Citrix Gateway の **OCSP** 実装

Citrix Gateway アプライアンスでの OCSP 検証は、SSL ハンドシェイク中に Citrix Gateway がクライアント証明書を受信したときに開始されます。証明書を検証するために、Citrix Gateway は OCSP リクエストを作成し、そのリクエストを OCSP レスポンダーに転送します。そのためには、Citrix Gateway がクライアント証明書から OCSP レスポンダーの URL を抽出するか、ローカルに構成された URL を使用します。Citrix Gateway がサーバーからの応答を評価し、トランザクションを許可するか拒否するかを決定するまで、トランザクションは中断状態になります。サーバーからの応答が構成された時間を超えて遅延し、他の応答者が構成されていない場合、Citrix Gateway では、OCSP チェックをオプションまたは必須のどちらに設定したかに応じて、トランザクションが許可されるか、エラーが表示されます。Citrix Gateway は、OCSP リクエストのバッチ処理と OCSP レスポンダーのキャッシュをサポートし、OCSP レスポンダーの負荷を軽減し、応答を高速化します。

OCSP 要求のバッチ処理

Citrix Gateway はクライアント証明書を受信するたびに、OCSP レスポンダーに要求を送信します。OCSP レスポンダーの過負荷を回避するために、Citrix Gateway では、同じリクエストで複数のクライアント証明書の状態を問い合わせることができます。要求のバッチ処理が効率的に機能するためには、バッチの形成を待っている間に単一の証明書の処理が遅れることがないように、タイムアウトを定義する必要があります。

OCSP 応答キャッシュ

OCSP レスポンダから受信した応答をキャッシュすると、ユーザへの応答が高速になり、OCSP レスポンダの負荷が軽減されます。クライアント証明書の失効ステータスを OCSP レスポンダーから受信すると、Citrix Gateway は事前に定義された時間だけ応答をローカルにキャッシュします。SSL ハンドシェイク中にクライアント証明書を受信すると、Citrix Gateway はまずローカルキャッシュにこの証明書のエントリを確認します。（キャッシュのタイムアウト制限内で）有効なエントリが見つかった場合、エントリが評価され、クライアント証明書が受け入れられるか拒否されます。証明書が見つからない場合、Citrix Gateway は OCSP レスポンダーにリクエストを送信し、そのレスポンスをローカルキャッシュに保存します。

OCSP 証明書ステータスの設定

March 26, 2020

オンライン証明書状態プロトコル (OCSP) の構成には、OCSP 応答側の追加、OCSP 応答側の認証局 (CA) からの署名付き証明書へのバインド、および証明書と秘密キーのセキュアソケットレイヤー (SSL) 仮想サーバーへのバインドが含まれます。すでに設定した OCSP レスポンダーに別の証明書と秘密キーをバインドする必要がある場合は、まずレスポンダーのバインドを解除してから、レスポンダーを別の証明書にバインドする必要があります。

OCSP を設定するには

1. [構成] タブのナビゲーションウィンドウで [SSL] を展開し、[OCSP レスポンダー] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前] に、プロファイルの名前を入力します。
4. [URL] に、OCSP レスポンダの Web アドレスを入力します。

   このフィールドは必須です。Web アドレスは 32 文字以下にする必要があります。
5. OCSP レスポンスをキャッシュするには、［キャッシュ］をクリックし、［タイムアウト］に Citrix Gateway がレスポンスを保持する分数を入力します。
6. [要求のバッチ処理] で、[有効化] をクリックします。
7.「バッチ処理の遅延」で、OCSP 要求のグループのバッチ処理に許可される時間をミリ秒単位で指定します。

   値の範囲は 0 ～10000 です。デフォルトは 1 です。
8. [時間スキュー時に生成] に、アプライアンスが応答を確認または受け入れる必要がある場合に Citrix Gateway が使用できる時間を入力します。
9. OCSP レスポンダによる署名チェックを無効にするには、[応答の検証] で [応答の信頼性] を選択します。

   応答を信頼できるようにする場合は、手順 8 と手順 9 をスキップします。

10. [証明書] で、OCSP 応答の署名に使用する証明書を選択します。

    証明書が選択されていない場合、OCSP レスポンダがバインドされている CA を使用して応答を検証します。

11. [要求タイムアウト] に、OCSP 応答を待機するミリ秒数を入力します。

    この時間には、バッチ処理遅延時間が含まれます。値の範囲は 0 ～120000 です。デフォルトは 2000 です。

12. [署名証明書] で、OCSP 要求の署名に使用する証明書と秘密キーを選択します。証明書と秘密キーを指定しない場合、要求は署名されません。

13. 1 回だけ使用される番号（nonce）拡張子を有効にするには、[Nonce] を選択します。

14. クライアント証明書を使用するには、[クライアント証明書の挿入] をクリックします。

15. ［Create］をクリックしてから、［Close］をクリックします。

Citrix Gateway 構成のテスト

March 26, 2020

Citrix Gateway で初期設定を構成したら、アプライアンスに接続して設定をテストできます。

Citrix Gateway の設定をテストするには、ローカルユーザーアカウントを作成します。次に、仮想サーバーの IP アドレスまたはアプライアンスの完全修飾ドメイン名（FQDN）のいずれかを使用して、Web ブラウザを開き、Web アドレスを入力します。たとえば、アドレスバーに`https://my.company.com`または`https://192.168.96.183`と入力します。

ログオン画面で、前に作成したユーザーアカウントのユーザー名とパスワードを入力します。ログオンすると、Citrix Gateway プラグインをダウンロードしてインストールするように求められます。

Citrix Gateway プラグインをインストールして接続すると、アクセスインターフェイスが表示されます。アクセスインターフェイスは、Citrix Gateway のデフォルトのホームページです。

構成ユーティリティを使用した新しいユーザーアカウントの作成

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] > [ユーザー管理] の順に展開し、[AAA ユーザー] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [ユーザー名] に、ユーザー名を入力します。
4. ローカル認証を使用する場合は、[外部認証] チェックボックスをオフにします。LDAP や RADIUS などの外部認証タイプを使用したユーザの認証がデフォルトです。このチェックボックスをオフにすると、Citrix Gateway はユーザーを認証します。
5. [パスワード] と [パスワードの確認] で、ユーザーのパスワードを入力し、[作成] をクリックし、[閉じる] をクリックします。

構成ユーティリティを使用してユーザーを追加する場合、次のポリシーをユーザーにバインドできます。

- 承認
- トラフィック、セッション、監査
- ブックマーク
- イントラネットアプリケーション
- イントラネット IP アドレス

テストユーザーアカウントでのログオンで問題が発生した場合は、次の点を確認してください。

- 証明書の警告が表示された場合は、テスト証明書または無効な証明書が Citrix Gateway にインストールされます。認証局（CA）によって署名された証明書がアプライアンスにインストールされている場合は、ユーザーデバイスに対応するルート証明書があることを確認してください。
- CA 署名付き証明書を使用した場合は、署名付き証明書署名要求 (CSR) を使用してサイト証明書を正しく生成したことと、CSR に入力された識別名 (DN) データが正確であることを確認します。問題は、ホスト名が、署名付き証明書の IP アドレスと一致しないこともあります。構成済み証明書の共通名が、構成済みの仮想サーバーの IP アドレス情報に対応していることを確認します。
- ログオン画面が表示されない場合や、他のエラーメッセージが表示された場合は、セットアッププロセスを確認し、すべての手順を正しく実行し、すべてのパラメータを正確に入力したことを確認します。

仮想サーバーの作成

March 26, 2020

仮想サーバーは、ユーザーがログオンするアクセスポイントです。各仮想サーバには、独自の IP アドレス、証明書、およびポリシーセットがあります。仮想サーバは、着信トラフィックを受け入れる IP アドレス、ポート、およびプロトコルの組み合わせで構成されます。仮想サーバーには、ユーザーがアプライアンスにログオンするときの接続設定が含まれます。仮想サーバーでは、次の設定を構成できます。

- 証明書
- 認証
- ポリシー
- ブックマーク
- アドレスプール (IP プールまたはイントラネット IP とも呼ばれます)
- Citrix Gateway を使用したダブルホップ DMZ 展開
- Secure Ticket Authority
- SmartAccess ICA プロキシセッション転送

Citrix Gateway ウィザードを実行すると、ウィザード中に仮想サーバーを作成できます。追加の仮想サーバは、次の方法で構成できます。

- 仮想サーバノードから。このノードは、構成ユーティリティのナビゲーション区画にあります。構成ユーティリティを使用して、仮想サーバーを追加、編集、および削除できます。

- クイック構成ウィザードを使用します。Citrix Endpoint Management、StoreFront または Web Interface を環境内に展開する場合は、クイック構成ウィザードを使用して、仮想サーバーと展開に必要なすべてのポリシーを作成できます。

ユーザーがログオンして RADIUS などの特定の認証タイプを使用できるようにするには、仮想サーバーを構成し、サーバーに一意の IP アドレスを割り当てます。ユーザーがログオンすると、仮想サーバーに送信され、RADIUS 資格情報の入力が求められます。

また、ユーザーが Citrix Gateway にログオンする方法を構成することもできます。セッションポリシーを使用して、ユーザーソフトウェアの種類、アクセス方法、およびログオン後にユーザーに表示されるホームページを構成できます。

追加の仮想サーバーを作成するには

April 9, 2020

構成ユーティリティまたはクイック構成ウィザードのナビゲーションウィンドウにある仮想サーバーノードを使用して、仮想サーバーの追加、変更、有効化、無効化、および削除を行うことができます。クイック構成ウィザードを使用した仮想サーバの構成の詳細については、
Configuring Settings with the Quick Configuration Wizardを参照してください。

構成ユーティリティを使用して仮想サーバーを作成するには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. 必要な設定を構成し、[作成]、[閉じる] の順にクリックします。

仮想サーバでの接続タイプの設定

March 26, 2020

仮想サーバーを作成および構成するときに、次の接続オプションを構成できます。

- Citrix Workspace アプリとの接続は、SmartAccess、エンドポイント分析、またはネットワーク層トンネリング機能を使用しない、Citrix Virtual Apps and Desktops にのみ行えます。
- Citrix Gateway プラグインと SmartAccess との接続。これにより、SmartAccess、エンドポイント分析、ネットワーク層トンネリング機能を使用できます。
- モバイルデバイスから Citrix Gateway へのマイクロ VPN 接続を確立する Secure Hub との接続。

- 複数のデバイスからユーザーが ICA セッション・プロトコルを介して行われる並列接続。複数のユニバーサルライセンスを使用できないように、接続は単一のセッションに移行されます。

ユーザソフトウェアを使用せずにユーザがログオンできるようにするには、クライアントレスアクセスポリシーを設定して、それを仮想サーバにバインドします。

仮想サーバー上で基本接続または **SmartAccess** 接続を構成するには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前] に、仮想サーバーの名前を入力します。
4. [IP アドレス] と [ポート] に、仮想サーバーの IP アドレスとポート番号を入力します。
5. 次のいずれかを行います:
   - ICA 接続のみを許可するには、[基本モード] をクリックします。
   - Secure Hub、Citrix Gateway プラグイン、および SmartAccess を使用したユーザーのログオンを許可するには、［SmartAccess モード］をクリックします。
   - SmartAccess が複数のユーザー接続の ICA プロキシセッションを管理できるようにするには、［ICA プロキシセッションの移行］をクリックします。
6. 仮想サーバーのその他の設定を構成し、[作成]、[閉じる] の順にクリックします。

ワイルドカード仮想サーバに対するリッスンポリシーの設定

March 26, 2020

Citrix Gateway 仮想サーバーを構成して、仮想サーバーが特定の仮想ローカルエリアネットワーク（VLAN）をリッスンする機能を制限できます。指定された VLAN 上のトラフィックを処理するように制限するリッスンポリシーを使用して、ワイルドカード仮想サーバを作成できます。

構成パラメータは次のとおりです。

パラメーター	説明
名前	仮想サーバーの名前。この名前は必須であり、仮想サーバーを作成した後は変更できません。名前は 127 文字以内で、最初の文字は数字または文字でなければなりません。また、アット記号 (@)、アンダースコア (_)、ダッシュ (-)、ピリオド (.)、コロン (:)、シャープ記号 (#)、スペースも使用できます。
IP	仮想サーバの IP アドレス。VLAN にバインドされたワイルドカード仮想サーバの場合、値は常に * です。

パラメーター	説明
種類	サービスの動作。選択肢は、HTTP、SSL、FTP、TCP、SSL_TCP、UDP、SSL_ ブリッジ、NNTP、DNS、任意の、SIP-UDP、DNS-TCP、および RTSP です。
ポート	仮想サーバーがユーザー接続をリッスンするポート。ポート番号は 0 ～65535 である必要があります。VLAN にバインドされたワイルドカード仮想サーバの場合、値は通常 * です。
リッスン優先度	リッスンポリシーに割り当てられているプライオリティ。プライオリティは逆の順序で評価されます。番号が小さいほど、リッスンポリシーに割り当てられるプライオリティが高くなります。
リッスンポリシールール	仮想サーバがリッスンする VLAN の識別に使用するポリシールール。ルールは、CLIENT.VLAN.ID.EQ (<ipaddressat>) です。<ipaddressat>では、VLAN に割り当てられた ID 番号を置き換えます。

リッスンポリシーを使用してワイルドカード仮想サーバーを作成するには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前] に、仮想サーバーの名前を入力します。
4. 「プロトコル」で、プロトコルを選択します。
5. [IP アドレス] に、仮想サーバーの IP アドレスを入力します。
6. [ポート] に、仮想サーバーのポートを入力します。
7. [詳細設定] タブの [リッスンポリシー] の [リッスンの優先度] に、リッスンポリシーの優先度を入力します。
8. [リッスンポリシールール] の横にある [設定] をクリックします。
9. [式を作成] ダイアログボックスで、[追加] をクリックして式を設定し、[OK] をクリックします。
10. ［Create］をクリックしてから、［Close］をクリックします。

Citrix Gateway での IP アドレスの構成

March 26, 2020

構成ユーティリティおよびユーザー接続にログオンするように IP アドレスを構成できます。Citrix Gateway は、管

理アクセス用にデフォルトの IP アドレス 192.168.100.1 とサブネットマスク 255.0.0 で構成されます。デフォルトの IP アドレスは、システム IP（NSIP）アドレスにユーザーが構成した値が存在しないときに使用されます。

- NSIP アドレス。アプライアンスへのすべての管理関連アクセスに使用される Citrix Gateway の管理 IP アドレス。Citrix Gateway では、NSIP アドレスも認証に使用されます。
- デフォルト **Gateway**。セキュリティで保護されたネットワークの外部から Citrix Gateway にトラフィックを転送するルーター。
- サブネット **IP**（**SNIP**）アドレス。セカンダリネットワーク上のサーバと通信することにより、ユーザーデバイスを表す IP アドレス。これは、マッピング IP（MIP）アドレスに似ています。

SNIP アドレスは 1024 ～64000 のポートを使用します。

Citrix Gateway で **IP** アドレスを使用する方法

Citrix Gateway は、発生している機能に基づいて、IP アドレスからのトラフィックをソースします。以下のリストでは、一般的なガイドラインとして、Citrix Gateway がそれぞれの IP アドレスを使用する方法について説明します。

- 認証。Citrix Gateway は、SNIP アドレスを使用します。
- ホームページからのファイル転送。Citrix Gateway は、SNIP アドレスを使用します。
- **DNS** クエリと **WINS** クエリ。Citrix Gateway は、MIP アドレスまたは SNIP アドレスのいずれかを使用します。
- セキュアなネットワーク内のリソースへのネットワークトラフィック。Citrix Gateway では、Citrix Gateway の構成に応じて、MIP アドレス、SNIP アドレス、または IP プールが使用されます。
- **ICA** プロキシ設定。Citrix Gateway は、MIP アドレスまたは SNIP アドレスを使用します。

マッピングされた **IP** アドレスの変更または削除

March 26, 2020

Citrix Gateway では、1 つのマッピングされた IP アドレスがサポートされます。アプライアンスで 1 つのマッピング IP アドレスを設定した場合、アドレスを変更または削除することはできません。マッピング IP アドレスを変更する必要がある場合は、最初に新しいマッピング IP アドレスを作成してから、元のマッピング IP アドレスを削除します。

設定ユーティリティの [セットアップウィザード] または [ネットワーク] ノードを使用して、マップされた IP アドレスを追加構成できます。

新しいマッピング **IP** アドレスを作成するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] > [ネットワーク] を展開し、[IP] をクリックします。

2. 詳細ウィンドウで、[追加] をクリックします。
3. [IP の作成] ダイアログボックスの [IP アドレス] に IP アドレスを入力します。
4. [ネットマスク] に、サブネットマスクを入力します。
5. [IP タイプ] で [マップ済み IP] を選択し、[作成] をクリックします。

マッピング **IP** アドレスを削除するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] > [ネットワーク] を展開し、[IP] をクリックします。
2. 詳細ウィンドウで、マッピングアドレスをクリックし、[削除] をクリックします。

サブネット **IP** アドレスの設定

March 26, 2020

サブネット IP アドレスにより、ユーザーは別のサブネット上にある外部ホストから Citrix Gateway に接続できます。サブネット IP アドレスを追加すると、対応するルートエントリがルートテーブル内に作成されます。サブネットごとに作成されるエントリは 1 つだけです。ルートエントリは、サブネットで最初に追加された IP アドレスに対応します。

システム IP アドレスとマッピングされた IP アドレスとは異なり、Citrix Gateway の初期構成時にサブネット IP アドレスを指定する必要はありません。

マッピングされた IP アドレスとサブネット IP アドレスは、1024 ～64000 のポートを使用します。

サブネット **IP** アドレスを追加するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] > [ネットワーク] を展開し、[IP] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [IP の作成] ダイアログボックスの [IP アドレス] に IP アドレスを入力します。
4. [ネットマスク] に、サブネットマスクを入力します。
5. [IP タイプ] で、[サブネット IP] を選択し、[閉じる]、[作成] の順にクリックします。

ユーザ接続用の **IPv6** の設定

March 26, 2020

インターネットプロトコルバージョン 6（IPv6）を使用して、ユーザー接続をリッスンするように Citrix Gateway を構成できます。次のいずれかの設定を構成する場合は、[IPv6] チェックボックスをオンにして、ダイアログボックスに IPv6 アドレスを入力します。

- グローバル設定-公開アプリケーション-ICA プロキシ
- グローバル認証-Radius
- グローバル認証-LDAP
- グローバル認証-TACACS
- セッションプロファイル-公開アプリケーション-ICA プロキシ
- Citrix Gateway 仮想サーバー
- 認証サーバの作成-Radius
- 認証サーバーの作成-LDAP
- 認証サーバの作成-TACACS
- 監査サーバーの作成
- 高可用性のセットアップ
- 高可用性を実現するためのルートモニタのバインド/バインド解除
- 仮想サーバ（負荷分散）

IPv6 アドレスでリッスンするように Citrix Gateway 仮想サーバーを構成すると、ユーザーは Citrix Workspace アプリでのみ接続できます。Citrix Gateway プラグインを使用したユーザー接続は、IPv6 ではサポートされていません。

Citrix Gateway で IPv6 を構成するには、次のガイドラインを使用できます。

- Citrix Virtual Apps Web Interface. ユーザー接続用に IPv6 を構成し、IPv6 を使用するマップされた IP アドレスがある場合、Citrix Virtual Apps および Web Interface サーバーでも IPv6 を使用できます。Web Interface は、Citrix Gateway の背後にインストールする必要があります。ユーザーが Citrix Gateway 経由で接続すると、IPv6 アドレスは IPv4 に変換されます。接続が戻ると、IPv4 アドレスは IPv6 に変換されます。
- 仮想サーバ。Citrix Gateway ウィザードを実行するときに、仮想サーバーの IPv6 を構成できます。Citrix Gateway ウィザードの［仮想サーバー］ページで［IPv6］をクリックし、IP アドレスを入力します。Citrix Gateway ウィザードでは、仮想サーバーの IPv6 アドレスの構成のみを使用できます。
- その他。ICA プロキシ、認証、監査、高可用性用に IPv6 を構成するには、ダイアログボックスの「IPv6」チェックボックスを選択し、IP アドレスを入力します。

セキュリティで保護されたネットワークにある **DNS** サーバーの解決

April 9, 2020

DNS サーバーがファイアウォールの背後にあるセキュリティで保護されたネットワークにあり、ファイアウォールが ICMP トラフィックをブロックしている場合、ファイアウォールが要求をブロックしているため、サーバーへの接

続をテストできません。この問題を解決するには、次の手順を実行します。

- 既知の完全修飾ドメイン名 (FQDN) に解決するカスタム DNS モニターを使用して DNS サービスを作成する。
- Citrix Gateway で直接アドレス指定できない DNS 仮想サーバーを作成する。
- サービスを仮想サーバーにバインドする。

注:

- DNS 仮想サーバーと DNS サービスを構成するのは、DNS サーバーがファイアウォールの内側にある場合だけです。
- Citrix ADC 負荷分散ライセンスをアプライアンスにインストールすると、［仮想サーバーとサービス］ノードはナビゲーションペインに表示されません。この手順を実行するには、[負荷分散] を展開し、[仮想サーバー] をクリックします。

DNS サービスと **DNS** モニターを構成するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[仮想サーバーとサービス] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前] ボックスに、サービスの名前を入力します。
4. [プロトコル] で、[DNS] を選択します。
5. [IP アドレス] に、DNS サーバーの IP アドレスを入力します。
6. [Port］ボックスにポート番号を入力します。
7. [サービス] タブで、[追加] をクリックします。
8. [モニター] タブの [使用可能] で、[dns]、[追加]、[作成]、[閉じる] の順にクリックします。
9. [仮想サーバーの作成 (負荷分散)] ダイアログボックスで、[作成] をクリックし、[閉じる] をクリックします。

次に、DNS 仮想サーバーを構成するにはの手順を使用して DNS 仮想サーバーを作成し、DNS サービスを仮想サーバーにバインドします。

DNS サービスを **DNS** 仮想サーバーにバインドするには

1. [仮想サービス (負荷分散) の構成] ダイアログボックスの [サービス] タブで、[追加] をクリックし、DNS サービスを選択し、[作成] をクリックして [閉じる] をクリックします。

DNS 仮想サーバの構成

March 26, 2020

DNS 仮想サーバーを構成するには、名前と IP アドレスを指定します。Citrix Gateway 仮想サーバーと同様に、DNS 仮想サーバーに IP アドレスを割り当てる必要があります。ただし、ユーザデバイスがすべての内部アドレスを解決で

きるように、この IP アドレスはターゲットネットワークの内部側にある必要があります。DNS ポートも指定する必要があります。

注：アプライアンスに Citrix ADC 負荷分散ライセンスをインストールすると、[
仮想サーバーとサービス］ノードはナビゲーションペインに表示されません。この機能は、負荷分散仮想サーバーを使用して構成できます。詳しくは、Citrix eDocs の「Citrix ADC」のトピックを参照してください。

DNS 仮想サーバーを構成するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[仮想サーバーとサービス] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前] に、仮想サーバーの名前を入力します。
4. [IP アドレス] に、DNS サーバーの IP アドレスを入力します。
5. [ポート] に、DNS サーバーがリッスンするポートを入力します。
6. [プロトコル] で [DNS] を選択し、[作成] をクリックします。

最後に、展開環境のニーズに応じて、次の 2 つの方法のいずれかを使用して、DNS 仮想サーバーを Citrix Gateway に関連付けます。

- サーバーを Citrix Gateway にグローバルにバインドします。
- DNS 仮想サーバーを仮想サーバーごとにバインドします。

DNS 仮想サーバをグローバルに展開すると、すべてのユーザがそれにアクセスできます。次に、DNS 仮想サーバーを仮想サーバーにバインドすることで、ユーザーを制限できます。

ネームサービスプロバイダの設定

March 26, 2020

Citrix Gateway では、ネームサービスプロバイダーを使用して Web アドレスを IP アドレスに変換します。

Citrix Gateway ウィザードを実行すると、DNS サーバーまたは WINS サーバーを構成できます。構成ユーティリティを使用して、追加の DNS サーバーまたは WINS サーバーを構成することもできます。

DNS サーバーを **Citrix Gateway** に追加するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [ネットワーク構成] タブで、[追加] をクリックします。

4. [ネームサーバーの挿入] ダイアログボックスの [IP アドレス] に DNS サーバーの IP アドレスを入力し、[作成] をクリックし、[閉じる] をクリックします。
5. 構成ユーティリティで [OK] をクリックします。

WINS サーバーを **Citrix Gateway** に追加するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [ネットワークの構成] タブの [WINS サーバーの IP] に WINS サーバーの IP アドレスを入力し、[OK] をクリックします。

次に、DNS 仮想サーバー名と IP アドレスを指定します。Citrix Gateway 仮想サーバーと同様に、IP アドレスを仮想サーバーに割り当てる必要があります。ただし、ユーザデバイスがすべての内部アドレスを適切に解決できるように、この IP アドレスはターゲットネットワークの内部側にある必要があります。DNS ポートも指定する必要があります。

DNS サーバーと WINS サーバーを名前解決用に構成する場合は、Citrix Gateway ウィザードを使用して、最初に名前検索を実行するサーバーを選択できます。

名前ルックアップの優先順位を指定するには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］をクリックします。
2. 詳細ペインの [はじめに] で、[Citrix Gateway ウィザード] をクリックします。
3. [ネームサービスプロバイダ] ページが表示されるまで、[次へ] をクリックして現在の設定を受け入れます。
4. [名前ルックアップの優先度] で、[WINS] または [DNS] を選択し、ウィザードの最後に進みます。

サーバ起動接続の構成

March 26, 2020

IP アドレスが有効な状態で Citrix Gateway にログオンする各ユーザーについて、DNS サフィックスがユーザー名に追加され、DNS アドレスレコードがアプライアンスの DNS キャッシュに追加されます。この手法は、ユーザーの IP アドレスではなく、DNS 名をユーザーに提供するのに役立ちます。

ユーザーのセッションに IP アドレスを割り当てると、内部ネットワークからユーザーのデバイスに接続することができます。たとえば、リモートデスクトップまたは仮想ネットワークコンピューティング（VNC）クライアントで接続しているユーザーは、ユーザーデバイスにアクセスして問題のアプリケーションを診断できます。また、内部ネットワーク IP アドレスを持つ 2 人の Citrix Gateway ユーザーがリモートでログオンし、Citrix Gateway を介して相互に通信することもできます。アプライアンス上でログオンしているユーザーの内部ネットワーク IP アドレスを検出できるようにすることで、この通信に役立ちます。

リモートユーザーは、以下の ping コマンドを使用して、その時点で Citrix Gateway にログオンできるユーザーの内部ネットワーク IP アドレスを検出できます。

ピング・アンド・ドロップ
サーバーは、次の方法でユーザーデバイスへの接続を開始できます。
- TCP または UDP 接続。接続は、内部ネットワークの外部システムから、または Citrix Gateway にログオンしている別のコンピューターから発信できます。これらの接続には、Citrix Gateway にログオンした各ユーザーデバイスに割り当てられた内部ネットワーク IP アドレスが使用されます。Citrix Gateway がサポートするサーバー起動接続の種類を以下に説明します。
TCP または UDP サーバーが開始する接続の場合、サーバーはユーザーデバイスの IP アドレスとポートに関する事前知識を持ち、接続を行います。Citrix Gateway は、この接続を傍受します。
次に、ユーザーデバイスがサーバーへの初期接続を確立し、サーバーは最初に構成されたポートから既知または派生したポート上のユーザーデバイスに接続します。
このシナリオでは、ユーザーデバイスは、サーバーへの初期接続を行い、ポートと IP アドレスは、この情報が埋め込まれているアプリケーション固有のプロトコルを使用してサーバーと交換します。これにより、Citrix Gateway は、アクティブな FTP 接続などのアプリケーションをサポートできるようになります。
- ポートコマンド.. これは、アクティブな FTP および特定の Voice over IP プロトコルで使用されます。
- プラグイン間の接続。Citrix Gateway は、内部ネットワーク IP アドレスを使用してプラグイン間の接続をサポートします。
このタイプの接続では、同じ Citrix Gateway を使用する 2 つの Citrix Gateway ユーザーデバイスが相互に接続を開始できます。この種類の例として、Office Communicator や Yahoo! などのインスタントメッセージングアプリケーションを使用します。メッセンジャー。
ユーザーが Citrix Gateway をログオフし、ログオフ要求がアプライアンスに届かなかった場合、ユーザーは任意のデバイスを使用して再度ログオンし、前のセッションを新しいセッションに置き換えることができます。この機能は、ユーザごとに 1 つの IP アドレスが割り当てられる配置で役立ちます。
ユーザーが Citrix Gateway に初めてログオンすると、セッションが作成され、IP アドレスが割り当てられます。ユーザーがログオフしても、ログオフ要求が失われたり、ユーザーデバイスがクリーンログオフを実行できなかった場合、セッションはシステム上で維持されます。ユーザーが同じデバイスまたは別のデバイスから再度ログオンしようとすると、認証に成功した後、ログオンの転送ダイアログボックスが表示されます。ユーザーがログオンを転送すると、Citrix Gateway 上の前のセッションが閉じられ、新しいセッションが作成されます。ログオンの転送は、ログオフ後の 2 分間しかアクティブになりません。複数のデバイスから同時にログオンを試みると、最後のログオン試行によって元のセッションが置き換えられます。

Citrix Gateway でのルーティングの構成

March 26, 2020

内部ネットワークリソースへのアクセスを提供するには、Citrix Gateway が内部で安全なネットワークにデータをルーティングできる必要があります。デフォルトでは、Citrix Gateway は静的ルートを使用します。

Citrix Gateway がデータをルーティングできるネットワークは、Citrix Gateway のルーティングテーブルと Citrix Gateway に指定したデフォルト Gateway の構成によって決まります。

Citrix Gateway のルーティングテーブルには、ユーザーがアクセスする必要のある内部ネットワークリソースにデータをルーティングするために必要なルートが含まれている必要があります。

Citrix Gateway では、次のルーティングプロトコルがサポートされています。

- Routing Information Protocol (RIP v1 および v2)
- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGF)

スタティックルートの設定

別のホストまたはネットワークとの通信を設定するときに、動的ルーティングを使用しない場合は、Citrix Gateway から新しい宛先への静的ルートを構成する必要があります。

スタティックルートを設定するには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[システム] > [ネットワーク] > [詳細設定] を展開し、[ルート] をクリックします。
2. 詳細ウィンドウの [基本] タブで、[追加] をクリックします。
3. ルートの設定を構成し、[Create] をクリックします。

スタティックルートをテストするには

1. 構成ユーティリティのナビゲーションウィンドウで、[システム] を展開し、[診断] をクリックします。
2. 詳細ペインの [ユーティリティ] で、[Ping] をクリックします。
3. [パラメータ] の [ホスト名] に、デバイスの名前を入力します。
4. [詳細設定] の [送信元 IP アドレス] にデバイスの IP アドレスを入力し、[実行] をクリックします。

   他のデバイスとの通信に成功した場合は、同じ数のパケットが送信および受信され、パケットが失われなかったことを示すメッセージが表示されます。

   他のデバイスと通信していない場合、ステータスメッセージには、パケットが受信されず、すべてのパケットが失われたことが示されます。この通信不足を修正するには、手順を繰り返してスタティックルートを追加します。

テストを停止するには、[Ping] ダイアログボックスで [停止] をクリックし、[閉じる] をクリックします。

自動ネゴシエーションの設定

March 26, 2020

デフォルトでは、アプライアンスはオートネゴシエーションを使用するように構成されています。このオートネゴシエーションでは、Citrix Gateway はネットワークトラフィックを両方向に送信し、適切なアダプタ速度を決定します。デフォルト設定の「
自動ネゴシエーション」のままにすると、Citrix Gateway は全二重操作を使用します。ネットワークアダプタは双方向で同時にデータを送信できます。

自動ネゴシエーションを無効にすると、Citrix Gateway は半二重操作を使用します。半二重操作では、アダプターは 2 つのノード間で両方向にデータを送信できますが、アダプターは一度に使用できるのは一方または他方のみです。

初めてインストールする場合は、アプライアンスに接続されているポートに対して自動ネゴシエーションを使用するように Citrix Gateway を構成することをお勧めします。最初にログオンして Citrix Gateway を構成したら、自動ネゴシエーションを無効にできます。自動ネゴシエーションをグローバルに設定することはできません。各インターフェイスの設定を有効または無効にする必要があります。

自動ネゴシエーションを有効または無効にするには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[システム] > [ネットワーク] を展開し、[インターフェイス] をクリックします。
2. 詳細ペインでインターフェイスを選択し、[開く] をクリックします。
3. [インターフェイスの設定] ダイアログボックスで、次のいずれかの操作を行います。
    - 自動ネゴシエーションを有効にするには、[自動ネゴシエーション] の横にある [はい] をクリックし、[OK] をクリックします。
    - 自動ネゴシエーションを無効にするには、[自動ネゴシエーション] の横にある [いいえ] をクリックし、[OK] をクリックします。

認証と承認

March 26, 2020

Citrix Gateway では、Citrix Gateway のユーザー認証を幅広くカスタマイズできる柔軟な認証設計を採用しています。業界標準の認証サーバーを使用し、サーバーを使用してユーザーを認証するように Citrix Gateway を構成できます。Citrix Gateway では、クライアント証明書に存在する属性に基づく認証もサポートされます。Citrix Gateway 認証は、ユーザー認証に単一のソースを使用する単純な認証手順と、複数の認証タイプに依存するより複雑なカスケード認証手順に対応するように設計されています。

Citrix Gateway 認証には、ローカルユーザーおよびグループを作成するためのローカル認証が組み込まれています。この設計では、構成する認証手順を制御するポリシーの使用を中心としています。作成するポリシーは、Citrix

Gateway のグローバルサーバーレベルまたは仮想サーバーレベルで適用でき、ユーザーのソースネットワークに基づいて条件付きで認証サーバーパラメーターを設定できます。

ポリシーはグローバルにバインドされるか、仮想サーバーにバインドされるため、ポリシーに優先順位を割り当てて、認証の一部として複数の認証サーバーのカスケードを作成することもできます。

Citrix Gateway には、次の認証タイプがサポートされています。

- Local
- Lightweight Directory Access Protocol (LDAP)
- RADIUS
- SAML
- TACACS+
- クライアント証明書認証 (スマートカード認証を含む)

Citrix Gateway は、RSA セキュリティ ID、ゲマルトプロティバ、およびセーフワードもサポートしています。RADIUS サーバを使用して、これらのタイプの認証を設定します。

認証により、ユーザーは Citrix Gateway にログオンして内部ネットワークに接続できますが、認証によって、ユーザーがアクセスできる安全なネットワーク内のリソースが定義されます。認可は、LDAP ポリシーおよび RADIUS ポリシーを使用して設定します。

デフォルトのグローバル認証タイプの設定

March 26, 2020

Citrix Gateway をインストールして Citrix Gateway ウィザードを実行すると、ウィザード内で認証を構成しました。この認証ポリシーは、Citrix Gateway のグローバルレベルに自動的にバインドされます。Citrix Gateway ウィザードで設定する認証タイプは、デフォルトの認証タイプです。デフォルトの認証タイプを変更するには、Citrix Gateway ウィザードを再度実行するか、構成ユーティリティでグローバル認証設定を変更します。

認証の種類を追加する必要がある場合は、Citrix Gateway で認証ポリシーを構成し、構成ユーティリティを使用してポリシーを Citrix Gateway にバインドできます。認証をグローバルに設定する場合は、認証のタイプを定義し、設定を構成し、認証できる最大ユーザ数を設定します。

ポリシーを設定してバインドしたら、プライオリティを設定して、どの認証タイプが優先されるかを定義できます。たとえば、LDAP および RADIUS 認証ポリシーを設定します。LDAP ポリシーのプライオリティ番号が 10 で、RADIUS ポリシーのプライオリティ番号が 15 の場合、各ポリシーをバインドする場所に関係なく、LDAP ポリシーが優先されます。これをカスケード認証と呼びます。

ログオンページは、Citrix Gateway のインメモリキャッシュから配信するか、Citrix Gateway で実行されている HTTP サーバーから配信するかを選択できます。メモリ内キャッシュからログオンページを配信する場合、Citrix Gateway からのログオンページの配信は、HTTP サーバーからの送信よりも大幅に高速です。メモリ内キャッシュ

からログオンページを配信することを選択すると、多数のユーザーが同時にログオンするときの待機時間が短縮されます。キャッシュからのログオンページの配信は、グローバル認証ポリシーの一部としてのみ構成できます。

また、認証用の特定の IP アドレスであるネットワークアドレス変換 (NAT) IP アドレスを構成することもできます。この IP アドレスは認証で一意であり、Citrix Gateway のサブネット、マッピングされた IP アドレスまたは仮想 IP アドレスではありません。これはオプションの設定です。

注：Citrix Gateway ウィザードを使用して SAML 認証を構成することはできません。

クイック構成ウィザードを使用して、LDAP、RADIUS、およびクライアント証明書の認証を構成できます。ウィザードを実行すると、Citrix Gateway で構成されている既存の LDAP サーバーまたは RADIUS サーバーから選択できます。LDAP または RADIUS の設定を構成することもできます。2 要素認証を使用する場合は、プライマリ認証タイプとして LDAP を使用することをお勧めします。

認証をグローバルに設定するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [認証設定の変更] をクリックします。
3. [最大ユーザー数] に、この認証の種類を使用して認証できるユーザーの数を入力します。
4. [NAT IP アドレス] に、認証に使用する一意の IP アドレスを入力します。
5. [静的キャッシュを有効にする] を選択して、ログオンページを高速に配信します。
6. 認証が失敗した場合にユーザーにメッセージを提供するには、[拡張認証フィードバックを有効にする] を選択します。ユーザーが受け取るメッセージには、パスワードのエラー、アカウントの無効化またはロック済み、またはユーザーが見つからなかったなどがあります。
7.「デフォルトの認証タイプ」で、認証タイプを選択します。
8. 認証の種類の設定を構成し、[OK] をクリックします。

認可なしの認証の設定

April 9, 2020

承認は、ユーザーが Citrix Gateway 経由で接続できるリソースを定義します。認可ポリシーを構成するには、式を使用し、ポリシーを許可または拒否するように設定します。Citrix Gateway では、認証のみを使用するように構成できます。

承認なしで認証を構成すると、Citrix Gateway はグループ承認チェックを実行しません。ユーザーまたはグループに対して構成するポリシーは、ユーザーに割り当てられます。

認可の設定の詳細については、認可の設定を参照してください。

認可の設定

March 26, 2020

承認は、ユーザーが Citrix Gateway にログオンするときにアクセスできるネットワークリソースを指定します。認可のデフォルト設定では、すべてのネットワークリソースへのアクセスを拒否します。デフォルトのグローバル設定を使用し、承認ポリシーを作成して、ユーザーがアクセスできるネットワークリソースを定義することをお勧めします。

Citrix Gateway で承認を構成するには、承認ポリシーと式を使用します。承認ポリシーを作成したら、アプライアンスで構成したユーザーまたはグループにそのポリシーをバインドできます。

認可ポリシーの設定

March 26, 2020

認可ポリシーを設定するときに、内部ネットワークのネットワークリソースへのアクセスを許可または拒否するように設定できます。たとえば、ユーザが 10.3.3.0 ネットワークにアクセスできるようにするには、次の式を使用します。

REQ.IP.DESTIP==10.3.0.0 -netmask 255.255.0.0

承認ポリシーは、ユーザーとグループに適用されます。ユーザーが認証されると、Citrix Gateway は、RADIUS、LDAP、または TACACS+ サーバーからユーザーのグループ情報を取得して、グループ承認チェックを実行します。ユーザーがグループ情報を使用できる場合、Citrix Gateway はそのグループに許可されているネットワークリソースをチェックします。

ユーザーがアクセスできるリソースを制御するには、承認ポリシーを作成する必要があります。認可ポリシーを作成する必要がない場合は、デフォルトのグローバル認可を設定できます。

ファイルパスへのアクセスを拒否する式を認可ポリシー内に作成した場合、ルートディレクトリではなく、サブディレクトリパスのみを使用できます。たとえば、「\\ ルートディレクトリ\\ dir1\\ dir2」ではなく、fs.path に「\\ dir1\\ dir2」が含まれているを使用します。この例で 2 番目のバージョンを使用すると、ポリシーは失敗します。

認可ポリシーを設定したら、次のタスクに示すように、それをユーザーまたはグループにバインドします。

デフォルトでは、認可ポリシーは、最初に仮想サーバにバインドしたポリシーに対して検証され、次にグローバルにバインドされたポリシーに対して検証されます。ポリシーをグローバルにバインドし、ユーザー、グループ、または仮想サーバにバインドするポリシーよりもグローバルポリシーを優先させる場合は、ポリシーのプライオリティ番号を変更できます。プライオリティ番号はゼロから始まります。プライオリティ番号が小さいほど、ポリシーの優先順位が高くなります。

たとえば、グローバルポリシーの優先順位番号が 1 で、ユーザの優先順位が 2 の場合、グローバル認証ポリシーが最初に適用されます。

> 重要:
>
> - 従来の認可ポリシーは、TCP トラフィックにだけ適用されます。
> - 高度な認可ポリシーは、すべてのタイプのトラフィック（TCP/UDP/ICMP/DNS）に適用できます。
>   - UDP/ICMP/DNS トラフィックにポリシーを適用するには、ポリシーが UDP_REQUEST、ICMP_REQUEST、DNS_REQUEST の各タイプでバインドされている必要があります。
>   - バインディング中、「タイプ」が明示的に言及されていないか、「タイプ」が REQUEST に設定されている場合、動作は以前のビルドから変更されません。つまり、これらのポリシーは、TCP トラフィックにのみ適用されます。

高度な承認ポリシーの詳細については、「https://support.citrix.com/article/CTX232237」を参照してください。

GUI を使用して認可ポリシーを設定するには

1. **Citrix Gateway >** ［ポリシー］ **>** ［認証］に移動します。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. 「アクション」で、「許可」または「拒否」を選択します。
5. [式] で、[式エディタ] をクリックします。
6. 式の構成を開始するには、[選択] をクリックして必要な要素を選択します。
7. 式が完成したら、[完了] をクリックします。
8. ［作成］をクリックします。

GUI を使用して認可ポリシーをユーザーにバインドするには

1. **Citrix Gateway >** ［ユーザー管理］に移動します。
2. [**AAA** ユーザ] をクリックします。
3. 詳細ペインでユーザーを選択し、[編集] をクリックします。
4. [詳細設定] で、[承認ポリシー] をクリックします。
5. 「ポリシー・バインディング」ページで、ポリシーを選択するか、ポリシーを作成します。
6. [優先度] で、優先度番号を設定します。
7. 「タイプ」で要求タイプを選択し、「**OK**」をクリックします。

GUI を使用して認可ポリシーをグループにバインドするには

1. **Citrix Gateway >** ［ユーザー管理］に移動します。
2. [**AAA** グループ] をクリックします。
3. 詳細ペインでグループを選択し、[編集] をクリックします。
4. [詳細設定] で、[承認ポリシー] をクリックします。
5. 「ポリシー・バインディング」ページで、ポリシーを選択するか、ポリシーを作成します。

6. [優先度] で、優先度番号を設定します。
7.「タイプ」で要求タイプを選択し、「**OK**」をクリックします。

デフォルトのグローバル認可の設定

March 26, 2020

ユーザが内部ネットワーク上でアクセスできるリソースを定義するには、デフォルトのグローバル認可を設定します。グローバル認可を設定するには、内部ネットワーク上のネットワークリソースへのアクセスをグローバルに許可または拒否します。

作成したグローバル認可アクションは、直接またはグループを通じて、認可ポリシーが関連付けられていないすべてのユーザに適用されます。ユーザまたはグループの認可ポリシーは、常にグローバル認可アクションよりも優先されます。デフォルトの認可アクションが Deny に設定されている場合は、すべてのユーザまたはグループに認可ポリシーを適用して、それらのユーザまたはグループがネットワークリソースにアクセスできるようにする必要があります。この要件は、セキュリティを向上させるのに役立ちます。

デフォルトのグローバル認可を設定するには、次の手順を実行します。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [セキュリティ] タブの [既定の承認操作] の横にある [許可] または [拒否] を選択し、[OK] をクリックします。

認証の無効化

March 26, 2020

デプロイメントで認証が不要な場合は、無効にすることができます。認証を必要としない各仮想サーバーの認証を無効にできます。

重要：慎重に認証を無効にすることをお勧めします。外部認証サーバーを使用していない場合は、Citrix Gateway でユーザーの認証を許可するローカルユーザーとグループを作成します。認証を無効にすると、Citrix Gateway への接続を制御および監視する認証、承認、およびアカウンティング機能の使用が停止します。ユーザーが Citrix Gateway に接続するために Web アドレスを入力しても、ログオンページは表示されません。

認証を無効にするには

1. 構成ユーティリティのナビゲーションペインで、［Citrix Gateway］を展開し、［仮想サーバー］をクリックします。

2. 詳細ウィンドウで、仮想サーバーをクリックし、[開く] をクリックします。
3. [認証] タブの [ユーザー認証] で、[認証を有効にする] をクリックしてオフにします。

特定の時間に対する認証の設定

March 26, 2020

通常の勤務時間などの特定の時間にユーザが内部ネットワークへのアクセスを許可するように、認証ポリシーを設定できます。ユーザーが別の時間にログオンしようとすると、ログオンは拒否されます。

ユーザーが Citrix Gateway にログオンするタイミングを制限するには、認証ポリシー内で式を作成し、仮想サーバーまたはグローバルにバインドします。

時刻、日付、または曜日の認証を構成するには

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］>［ポリシー］>［認証］の順に展開します。
2. [認証] で、認証の種類を選択します。
3. 詳細ペインで、[ポリシー] タブをクリックし、認証ポリシーを選択して [開く] をクリックします。
4. [認証ポリシーの構成] ダイアログボックスの [式] で、[任意の式に一致] の横にある [追加] をクリックします。
5. [式の追加] ダイアログボックスの [式の種類] で、[日付/時刻] を選択します。
6.「修飾子」で、次のいずれかを選択します。
    - ユーザーがログオンできない時間を構成する時間。
    - ユーザーがログオンできない日付を構成するには、[DATE] をクリックします。
    - DAYOFWEEK を使用して、ユーザーがログオンできない日を設定します。
7.「演算子」で、値を選択します。
8. [値] で、テキストボックスの横のカレンダーをクリックし、日、日付、または時刻を選択します。
9. [OK] を 2 回クリックし、[閉じる] をクリックして [OK] をクリックします。

認証ポリシーのしくみ

March 26, 2020

ユーザーが Citrix Gateway にログオンすると、ユーザーが作成したポリシーに従って認証されます。ポリシーは、認証タイプを定義します。単一の認証ポリシーは、単純な認証のニーズに使用でき、通常はグローバルレベルでバインドされます。デフォルトの認証タイプ（ローカル）を使用することもできます。ローカル認証を構成する場合は、Citrix Gateway でユーザーとグループも構成する必要があります。

複数の認証ポリシーを構成し、それらをバインドして、詳細な認証手順と仮想サーバーを作成できます。たとえば、複数のポリシーを設定することで、カスケード認証と 2 要素認証を設定できます。また、認証ポリシーの優先順位を

設定して、Citrix Gateway がユーザーの資格情報をチェックするサーバーと順序を決定することもできます。認証ポリシーには、式とアクションが含まれます。たとえば、式を True value に設定した場合、ユーザーがログオンすると、アクションによってユーザーログオンが true と評価され、ユーザーはネットワークリソースにアクセスできます。

認証ポリシーを作成したら、グローバルレベルまたは仮想サーバのいずれかでポリシーをバインドします。少なくとも 1 つの認証ポリシーを仮想サーバーにバインドする場合、グローバル認証の種類が仮想サーバーにバインドされているポリシーよりも優先順位が高い場合を除き、ユーザーが仮想サーバーにログオンするときに、グローバルレベルにバインドした認証ポリシーは使用されません。

ユーザーが Citrix Gateway にログオンすると、認証は次の順序で評価されます。

- 仮想サーバで、バインドされた認証ポリシーがあるかどうかがチェックされます。
- 認証ポリシーが仮想サーバーにバインドされていない場合、Citrix Gateway はグローバル認証ポリシーをチェックします。
- 認証ポリシーが仮想サーバーまたはグローバルにバインドされていない場合、ユーザーはデフォルトの認証タイプを使用して認証されます。

LDAP および RADIUS 認証ポリシーを設定し、2 要素認証用にポリシーをグローバルにバインドする場合は、設定ユーティリティでポリシーを選択し、ポリシーがプライマリ認証タイプかセカンダリ認証タイプかを選択できます。グループ抽出ポリシーを設定することもできます。

認証プロファイルの設定

April 9, 2020

Citrix Gateway ウィザードまたは構成ユーティリティを使用して、認証プロファイルを作成できます。プロファイルには、認証ポリシーのすべての設定が含まれます。プロファイルは、認証ポリシーを作成するときに構成します。

Citrix Gateway ウィザードでは、選択した認証タイプを使用して認証を構成できます。ウィザードの実行後に追加の認証ポリシーを構成する場合は、構成ユーティリティを使用できます。Citrix Gateway ウィザードの詳細については、「Citrix Gateway ウィザードを使用した設定の構成」を参照してください。

構成ユーティリティを使用して認証ポリシーを作成するには

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］ > ［ポリシー］ > ［認証］の順に展開します。
2. ナビゲーションウィンドウの [認証] で、認証の種類を選択します。
3. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
4. 外部認証タイプを使用している場合は、[サーバー] の横にある [新規] をクリックします。
5. [認証サーバーの作成] ダイアログボックスで、認証の種類の設定を構成し、[作成]、[閉じる] の順にクリックします。

6. [認証ポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [True value] を選択し、[式の追加] をクリックし、[作成] をクリックして、[閉じる] をクリックします。
   注意: 認証タイプを選択して認証プロファイルを保存する場合、認証タイプは変更できません。別の認証タイプを使用するには、新しいポリシーを作成する必要があります。

構成ユーティリティを使用して認証ポリシーを変更するには

認証サーバの IP アドレスや式など、設定された認証ポリシーおよびプロファイルを変更できます。

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］>［ポリシー］>［認証］の順に展開します。
2. ナビゲーションウィンドウの [認証] で、認証の種類を選択します。
3. 詳細ペインの [サーバー] タブで、サーバーを選択し、[開く] をクリックします。

認証ポリシーを削除するには

ネットワークから認証サーバーを変更または削除した場合は、Citrix Gateway から対応する認証ポリシーを削除します。

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］>［ポリシー］>［認証］の順に展開します。
2. ナビゲーションウィンドウの [認証] で、認証の種類を選択します。
3. 詳細ペインの [ポリシー] タブでポリシーを選択し、[削除] をクリックします。

認証ポリシーのバインド

March 26, 2020

認証ポリシーを設定したら、ポリシーをグローバルにバインドするか、仮想サーバにバインドします。いずれかの設定ユーティリティーを使用して、認証ポリシーをバインドできます。

構成ユーティリティを使用して認証ポリシーをグローバルにバインドするには、次の手順を実行します。

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］>［ポリシー］>［認証］の順に展開します。
2. 認証タイプをクリックします。
3. 詳細ウィンドウの [ポリシー] タブで、サーバーをクリックし、[操作] で [グローバルバインド] をクリックします。
4. [プライマリ] タブまたは [セカンダリ] タブの [詳細] で、[ポリシーの挿入] をクリックします。
5. [ポリシー名] でポリシーを選択し、[OK] をクリックします。

   注：ポリシーを選択すると、Citrix Gateway によって式が True の値に自動的に設定されます。

構成ユーティリティを使用してグローバル認証ポリシーをバインド解除するには、次の手順を実行します。

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］>［ポリシー］>［認証］の順に展開します。
2. [ポリシー] タブの [操作] で、[グローバルバインド] をクリックします。
3. [認証ポリシーをグローバルにバインド/バインド解除] ダイアログボックスの [プライマリ] タブまたは [セカンダリ] タブの [ポリシー名] でポリシーを選択し、[ポリシーのバインド解除] をクリックして、[OK] をクリックします。

認証ポリシーの優先順位の設定

March 26, 2020

デフォルトでは、認証ポリシーは、最初に仮想サーバにバインドしたポリシーに対して検証され、次にグローバルにバインドされたポリシーに対して検証されます。認証ポリシーをグローバルにバインドし、仮想サーバにバインドするポリシーよりもグローバルポリシーを優先させる場合は、ポリシーのプライオリティ番号を変更できます。プライオリティ番号はゼロから始まります。プライオリティ番号が小さいほど、認証ポリシーの優先順位が高くなります。

たとえば、グローバルポリシーのプライオリティ番号が 1 で、仮想サーバのプライオリティが 2 の場合、グローバル認証ポリシーが最初に適用されます。

グローバル認証ポリシーの優先順位を設定または変更するには

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］>［ポリシー］>［認証］の順に展開します。
2. [ポリシー] タブの [操作] で、[グローバルバインド] をクリックします。
3. [認証グローバルポリシーのバインド/バインド解除] ダイアログボックスの [プライマリ] タブまたは [セカンダリ] タブで、[優先度] に番号を入力し、[OK] をクリックします。

仮想サーバにバインドされた認証ポリシーの優先順位を変更するには

仮想サーバーにバインドされている認証ポリシーを変更することもできます。

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 仮想サーバを選択し、[開く] をクリックします。
3. [認証] タブをクリックし、[プライマリ] または [セカンダリ] を選択します。
4. ポリシーを選択し、[優先度] に優先度の番号を入力し、[OK] をクリックします。

ローカルユーザの構成

March 26, 2020

Citrix Gateway でローカルにユーザーアカウントを作成して、認証サーバー上のユーザーを補完することができます。たとえば、社外のコンサルタントや来訪者などの一時的なユーザー用のアカウントを、認証サーバー上ではなく Access Gateway 上にローカルに作成します。

ローカル認証を使用している場合は、ユーザーを作成し、Citrix Gateway で作成したグループに追加します。ユーザーとグループを構成したら、承認およびセッションポリシーを適用し、ブックマークを作成し、アプリケーションを指定し、ユーザーがアクセスできるファイル共有とサーバーの IP アドレスを指定できます。

ローカルユーザーを作成するには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］>［ユーザー管理］の順に展開し、［AAA ユーザー］をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [ユーザー名] に、ユーザー名を入力します。
4. ローカル認証を使用している場合は、[外部認証] をオフにします。
   注意:LDAP や RADIUS などの
   外部認証サーバーに対してユーザーが認証されるようにするには、「外部認証」を選択します。このチェックボックスをオフにすると、Citrix Gateway がローカルユーザーデータベースに対して認証されます。
5. [パスワード] と [パスワードの確認] で、ユーザーのパスワードを入力し、[作成] をクリックし、[閉じる] をクリックします。

ユーザパスワードを変更するには

ローカルユーザーの作成後、ユーザーのパスワードを変更したり、外部認証サーバーに対して認証されるようにユーザーアカウントを構成したりできます。

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］>［ユーザー管理］の順に展開し、［AAA ユーザー］をクリックします。
2. 詳細ペインでユーザーを選択し、[開く] をクリックします。
3. [パスワード] と [パスワードの確認] に、ユーザーの新しいパスワードを入力し、[OK] をクリックします。

ユーザーの認証方法を変更するには

ローカル認証用に構成されているユーザーがいる場合は、認証を外部認証サーバに変更できます。これを行うには、外部認証を有効にします。

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］>［ユーザー管理］の順に展開し、［AAA ユーザー］をクリックします。
2. 詳細ペインでユーザーを選択し、[開く] をクリックします。
3. [外部認証] を選択し、[OK] をクリックします。

ユーザーを削除するには

Citrix Gateway からユーザーを削除することもできます。

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］>［ユーザー管理］の順に展開し、［AAA ユーザー］をクリックします。
2. 詳細ペインでユーザーを選択し、[削除] をクリックします。

Citrix Gateway からユーザーを削除すると、関連するすべてのポリシーもユーザープロファイルから削除されます。

グループの構成

March 26, 2020

Citrix Gateway では、ローカルグループであり、ローカル認証でユーザーを認証できるグループを作成できます。認証に外部サーバーを使用している場合、Citrix Gateway のグループは、内部ネットワークの認証サーバーで構成されたグループと一致するように構成されます。ユーザーがログオンして認証されると、グループ名が認証サーバー上のグループと一致する場合、ユーザーは Citrix Gateway 上のグループの設定を継承します。

グループを構成したら、承認ポリシーとセッションポリシーの適用、ブックマークの作成、アプリケーションの指定、ユーザーがアクセスできるファイル共有とサーバーの IP アドレスの指定を行うことができます。

ローカル認証を使用している場合は、ユーザーを作成し、Citrix Gateway で構成されたグループに追加します。ユーザーは、そのグループの設定を継承します。

重要: ユーザーが Active Directory グループのメンバーである場合、Citrix Gateway 上のグループの名前は Active Directory グループと同じである必要があります。

新しいグループを作成するには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］>［ユーザー管理］の順に展開し、［AAA グループ］をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [グループ名] にグループの名前を入力し、[作成] をクリックし、[閉じる] をクリックします。

グループを削除するには

Citrix Gateway からユーザーグループを削除することもできます。

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］>［ユーザー管理］の順に展開し、［AAA グループ］をクリックします。
2. 詳細ペインでグループを選択し、[削除] をクリックします。

グループへのユーザーの追加

March 26, 2020

ユーザーをグループに追加するには、グループの作成時または後で追加できます。複数のグループにユーザーを追加して、ユーザーはそれらのグループにバインドされているポリシーと設定を継承できます。

ユーザーをグループに追加するには、次の手順に従います。

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］> ［ユーザー管理］の順に展開し、［AAA グループ］をクリックします。
2. 詳細ウィンドウで、グループを選択し、[開く] をクリックします。
3. [ユーザー] タブの [使用可能なユーザー] で、ユーザーを選択し、[追加] をクリックして [OK] をクリックします。

グループを使用したポリシーの設定

March 26, 2020

グループを構成したら、[グループ] ダイアログボックスを使用して、ユーザーアクセスを指定するポリシーと設定を適用できます。ローカル認証を使用している場合は、ユーザーを作成し、Citrix Gateway で構成されたグループに追加します。ユーザーは、そのグループの設定を継承します。

[グループ] ダイアログボックスで、ユーザーのグループに対して次のポリシーまたは設定を構成できます。

- ユーザー
- 承認ポリシー
- 監査ポリシー
- セッション・ポリシー
- トラフィックポリシー
- ブックマーク
- イントラネットアプリケーション
- イントラネット IP アドレス

構成では、複数のグループに属するユーザーがいる場合があります。さらに、各グループには、異なるパラメータが設定された 1 つ以上のバインドされたセッションポリシーがある場合があります。複数のグループに属するユーザーは、そのユーザーが属するすべてのグループに割り当てられたセッションポリシーを継承します。どのセッションポリシー評価が他方よりも優先されるかを確認するには、セッションポリシーの優先度を設定する必要があります。

たとえば、グループ 1 がホームページ www.homepage1.com で構成されたセッションポリシーにバインドされているとします。グループ 2 は、ホームページ www.homepage2.com で構成されたセッションポリシーにバインドされます。これらのポリシーが、優先順位番号のないグループまたは優先順位番号が同じグループにバインドされて

いる場合、両方のグループに属するユーザーに表示されるホームページは、最初に処理されるポリシーによって異なります。ホーム・ページ www.homepage1.com のセッション・ポリシーの優先順位を低く設定すると、両方のグループに属するユーザーが常にホーム・ページ www.homepage1.com を受け取ることができます。

セッション・ポリシーに優先順位番号が割り当てられていないか、同じ優先順位番号が割り当てられていない場合、優先順位は次の順序で評価されます。

- ユーザー
- グループ
- 仮想サーバ
- グローバル

ポリシーがプライオリティ番号なしで同じレベルにバインドされている場合、またはポリシーが同じプライオリティ番号を持つ場合、評価の順序はポリシーバインド順序に従って行われます。最初にレベルにバインドされたポリシーは、後でバインドされたポリシーよりも優先されます。

LDAP 認証の構成

April 9, 2020

1 つ以上の LDAP サーバーを使用してユーザーアクセスを認証するように Citrix Gateway を構成できます。

LDAP 認証には、Active Directory、LDAP サーバー、および Citrix Gateway で同じグループ名が必要です。グループ名は、大文字小文字の使い分けを含め、一字一句正確に一致させる必要があります。

既定では、LDAP 認証は、セキュアソケットレイヤー (SSL) またはトランスポート層セキュリティ (TLS) を使用してセキュリティで保護されています。セキュア LDAP 接続には 2 つのタイプがあります。1 つのタイプの場合、LDAP サーバは、LDAP サーバがクリア LDAP 接続を受け入れるために使用するポートとは別のポートで SSL または TLS 接続を受け入れます。ユーザーが SSL 接続または TLS 接続を確立すると、LDAP トラフィックは接続を介して送信できます。

LDAP 接続のポート番号は次のとおりです。

- セキュリティで保護されていない LDAP 接続の場合は 389
- 安全な LDAP 接続用の 636
- Microsoft のセキュリティで保護されていない LDAP 接続の場合 3268
- Microsoft の LDAP 接続のセキュリティで保護された 3269

2 番目のタイプのセキュア LDAP 接続では、StartTLS コマンドを使用し、ポート番号 389 を使用します。Citrix Gateway でポート番号 389 または 3268 を構成すると、サーバーは StartTLS を使用して接続を試みます。他のポート番号を使用する場合、サーバーは SSL または TLS を使用して接続を試みます。サーバーが StartTLS、SSL、または TLS を使用できない場合、接続は失敗します。

LDAP サーバーのルートディレクトリを指定すると、Citrix Gateway はすべてのサブディレクトリを検索してユー

ザー属性を検索します。大きなディレクトリでは、この方法はパフォーマンスに影響を与える可能性があります。このため、特定の組織単位（OU）を使用することをお勧めします。

次の表に、LDAP サーバーのユーザー属性フィールドの例を示します。

LDAP サーバー	ユーザー属性	大文字と小文字を区別する
Microsoft Active Directory Server	sAMAccountName	いいえ
Novell eDirectory	ou	はい
IBM Directory Server	uid	はい
Lotus Domino	CN	はい
Sun ONE Directory（旧 iPlanet）	uid または cn	はい

次の表に、ベース DN の例を示します。

LDAP サーバー	ベース DN
Microsoft Active Directory Server	DC=citrix,DC=local
Novell eDirectory	ou=users,ou=dev
IBM Directory Server	cn=users
Lotus Domino	OU=City,O=Citrix, C=US
Sun ONE Directory（旧 iPlanet）	ou=People,dc=citrix,dc=com

次の表に、バインド DN の例を示します。

LDAP サーバー	Bind DN
Microsoft Active Directory Server	CN=Administrator, CN=Users, DC=citrix, DC=local
Novell eDirectory	cn=admin, o=citrix
IBM Directory Server	LDAP_dn
Lotus Domino	CN=Notes Administrator, O=Citrix, C=US
Sun ONE Directory（旧 iPlanet）	uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot

注：LDAP サーバ設定の詳細については、
LDAP ディレクトリ内の属性の決定を参照してください。

構成ユーティリティを使用して **LDAP** 認証を構成するには

March 26, 2020

1. **Citrix Gateway** > ［ポリシー］ > ［認証］ に移動します。
2. [**LDAP**] をクリックします。
3. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
4. [名前**]** に、ポリシーの名前を入力します。
5. [サーバー] の横にある [新規] をクリックします。
6. [名前**]** に、サーバーの名前を入力します。
7. [サーバー] の [**IP** アドレス**]** と **[**ポート] に、LDAP サーバーの IP アドレスとポート番号を入力します。
8. [種類] で、[Active Directory] の場合は [**AD**]、[Novell ディレクトリサービス] の場合は [**NDS**] を選択します。
9. [接続の設定**]** で、次の操作を行います。
   a) [ベース **DN (**ユーザーの場所**)**] に、ユーザーが配置されるベース DN を入力します。ベース DN は、選択したディレクトリ（AD または NDS）の下にあるユーザーを検索します。

      ベース DN は、ユーザー名を削除し、ユーザーが配置されているグループを指定することによって、バインド DN から取得されます。基本識別名の構文の例を次に示します。

      ```
      ou=users,dc=ace,dc=com
      cn=Users,dc=ace,dc=com
      <!--NeedCopy-->
      ```

   b) [管理者バインド **DN**] に、LDAP ディレクトリへのクエリの管理者バインド DN を入力します。バインド DN の構文の例を次に示します。

      ```
      domain/user name
      ou=administrator,dc=ace,dc=com
      user@domain.name (for Active Directory)
      cn=Administrator,cn=Users,dc=ace,dc=com
      <!--NeedCopy-->
      ```

      Active Directory の場合は、cn= グループ名として指定されたグループ名が必要です。Citrix Gateway で定義するグループ名と LDAP サーバー上のグループ名は同一である必要があります。

他の LDAP ディレクトリの場合、グループ名は必須ではないか、必要に応じて ou=groupname として指定されます。

Citrix Gateway は、管理者の資格情報を使用して LDAP サーバーにバインドし、ユーザーを検索します。ユーザーを見つけた後、Citrix Gateway は管理者の資格情報をアンバインドし、ユーザーの資格情報で再バインドします。

c) [管理者パスワード] と [管理者パスワードの確認] に、LDAP サーバーの管理者パスワードを入力します。

10. 追加の LDAP 設定を自動的に取得するには、[属性の取得] をクリックします。

    [属性の取得] をクリックすると、[その他の設定] の下のフィールドが自動的に入力されます。この手順を無視する場合は、手順 12 および 13 に進みます。それ以外の場合は、手順 14 に進みます。

11. ［その他の設定］ の ［サーバーのログオン名の属性］ に、構成する LDAP サーバーのログオン名を Citrix Gateway が検索する属性を入力します。デフォルトは「samAccountName」です。

12. 「検索フィルタ」に、単一または複数のアクティブなディレクトリ・グループに関連付けられているユーザーを検索する値を入力します。

    たとえば、「memberOf=CN=GatewayAccess,OU=Groups,DC=Users,DC=lab」などです。

    > 注:
    >
    > 上記の例を使用すると、Citrix Gateway のアクセスを特定の AD グループのメンバーのみに制限できます。

13. [グループ属性] で、Active Directory のデフォルトの memberOf のままにするか、使用している LDAP サーバーの種類の属性に属性を変更します。この属性により、Citrix Gateway は承認中にユーザーに関連付けられたグループを取得できます。

14. [セキュリティの種類] で、セキュリティの種類を選択し、[作成] をクリックします。

15. ユーザーが LDAP パスワードを変更できるようにするには、[パスワード の変更を許可] を選択します。

    注:

    - セキュリティタイプとして **PLAINTEXT** を選択した場合、ユーザーにパスワードの変更を許可することはできません。
    - セキュリティのために **PLAINTEXT** または **TLS** を選択した場合は、ポート番号 389 を使用します。**SSL** を選択した場合は、ポート番号 636 を使用します。

LDAP ディレクトリ内の属性の決定

March 26, 2020

Citrix Gateway で認証設定を構成できるように、LDAP ディレクトリ属性を決定する際にサポートが必要な場合は、Softerra の無料の LDAP ブラウザーで簡単に検索できます。

LDAP ブラウザはからダウンロードできますLDAP アドミニストレーター Web サイト。ブラウザをインストールしたら、次の属性を設定します。

- LDAP サーバーのホスト名または IP アドレス。
- LDAP サーバーのポート。デフォルトは 389 です。
- ベース DN フィールド。空白のままにできます。LDAP ブラウザーから提供される情報は、Citrix Gateway でこの設定を構成するために必要なベース DN を特定するのに役立ちます。
- 匿名バインドチェックでは、LDAP サーバに接続するためにユーザクレデンシャルが必要かどうかを判断します。LDAP サーバーでクレデンシャルが必要な場合は、チェックボックスをオフのままにします。

設定が完了すると、LDAP ブラウザは左ペインにプロファイル名を表示し、LDAP サーバに接続します。

LDAP グループ抽出の設定

April 9, 2020

2 要素認証を使用している場合は、プライマリ認証ソースとセカンダリ認証ソースの両方から抽出されたグループが連結されます。認可ポリシーは、プライマリまたはセカンダリ認証サーバから抽出されたグループに適用できます。

LDAP サーバーから取得したグループ名は、Citrix Gateway でローカルに作成されたグループ名と比較されます。2 つのグループ名が一致する場合、ローカルグループのプロパティは LDAP サーバから取得したグループに適用されます。

ユーザーが複数の LDAP グループに属している場合、Citrix Gateway は、ユーザーが属するすべてのグループからユーザー情報を抽出します。ユーザーが Citrix Gateway 上の 2 つのグループのメンバーであり、各グループにバインドされたセッションポリシーがある場合、ユーザーは両方のグループからセッションポリシーを継承します。ユーザーが正しいセッションポリシーを受け取るようにするには、セッションポリシーの優先順位を設定します。

Citrix Gateway 認証で動作する LDAP グループメンバーシップ属性の詳細については、以下を参照してください。

- LDAP グループ抽出のユーザーオブジェクトからの直接の動作
- LDAP グループ抽出がグループオブジェクトから間接的に機能する方法

LDAP グループ抽出のユーザーオブジェクトからの直接の動作

March 26, 2020

グループオブジェクトからグループメンバーシップを評価する LDAP サーバーは、Citrix Gateway 認証で動作します。

一部の LDAP サーバーでは、Active Directory (memberOf 属性を使用) や IBM eDirectory (groupMembership 属性を使用) など、オブジェクトが属するグループに関する情報をユーザーオブジェクトに含めることができます。ユーザーのグループメンバーシップは、IBM ディレクトリサーバー (ibm-allGroups を使用) や Sun ONE ディレクトリサーバー (nsRole を使用) などのユーザーオブジェクトの属性にすることができます。これらのタイプの LDAP サーバーはいずれも、Citrix Gateway グループ抽出で動作します。

たとえば、IBM Directory Server では、静的、動的、ネストされたグループを含むすべてのグループ・メンバーシップは、ibm-allGroups 属性を使用して返すことができます。Sun ONE では、管理、フィルタリング、ネストを含むすべてのロールが nsRole 属性を使用して計算されます。

LDAP グループ抽出がグループオブジェクトから間接的に機能する方法

March 26, 2020

グループオブジェクトからのグループメンバーシップを間接的に評価する LDAP サーバーは、Citrix Gateway 認証では機能しません。

Lotus Domino などの一部の LDAP サーバーでは、グループオブジェクトにユーザーに関する情報のみを含めることができます。これらの LDAP サーバーでは、ユーザーオブジェクトにグループに関する情報を格納できないため、Citrix Gateway グループ抽出では機能しません。このタイプの LDAP サーバでは、グループのメンバー・リストでユーザーを検索することにより、グループ・メンバーシップ検索が実行されます。

LDAP 認可グループのアトリビュートフィールド

March 26, 2020

次の表に、LDAP グループ属性フィールドの例を示します。

LDAP サーバ	LDAP 属性
Microsoft Active Directory Server	memberOf
Novell eDirectory	groupMembership
IBM Directory Server	ibm-allGroups
Sun ONE Directory（旧 iPlanet）	nsRole

LDAP 認可を設定するには

March 26, 2020

認証ポリシーで LDAP 認可を設定するには、グループアトリビュート名とサブアトリビュートを設定します。

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］ > ［ポリシー］ > ［認証］の順に展開します。
2. [認証] で、認証の種類をクリックします。
3. 詳細ウィンドウで、[追加] をクリックします。
4. [名前] に、ポリシーの名前を入力します。
5. [サーバー] の横にある [新規] をクリックします。
6. [名前] に、サーバーの名前を入力します。
7. [サーバー] に、LDAP サーバーの IP アドレスとポートを入力します。
8. [グループ属性] に memberOf と入力します。
9. [サブ属性] の [名前] に CN と入力し、[作成] をクリックします。
10. [認証ポリシーの作成] ダイアログボックスで、[名前付き式] の横にある式を選択し、[式の追加]、[作成]、[閉じる] の順にクリックします。

LDAP ネストされたグループ抽出の設定

March 26, 2020

Citrix Gateway では、LDAP グループに対してクエリを実行し、認証サーバー上で構成した上位グループからグループとユーザー情報を抽出できます。たとえば、group1 を作成し、そのグループ内に group2 と group3 を作成したとします。ユーザーが group3 に属している場合、Citrix Gateway は、ネストされたすべての上位グループ（group2、group1）から指定されたレベルまでの情報を抽出します。

認証ポリシーを使用して、LDAP ネストされたグループ抽出を設定できます。クエリを実行すると、Citrix Gateway は、最大ネストレベルに達するまで、または使用可能なすべてのグループを検索するまでグループを検索します。

LDAP ネストされたグループ抽出を構成するには

1. 構成ユーティリティーのナビゲーションペインで、[Citrix Gateway]、[ポリシー]、[認証/承認]、[認証]、[認証］の順に展開し、［LDAP］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [サーバー] の横にある [新規] をクリックします。
5. [名前] に、サーバーの名前を入力します。
6. LDAP サーバの設定を構成します。
7. [ネストされたグループの抽出] を展開し、[有効にする] をクリックします。

8. [最大ネストレベル] に、Citrix Gateway がチェックするレベル数を入力します。
9. [グループ名識別子] に、LDAP サーバー上のグループ名を一意に識別する LDAP 属性名 (sAMAccountName など) を入力します。
10. [グループ検索属性] に、任意のグループの親グループ (memberOf など) を決定するために検索応答で取得する LDAP 属性名を入力します。
11. [グループ検索サブ属性] に、グループの親グループを決定するために、[グループ検索属性] の一部として検索する LDAP サブ属性名を入力します。たとえば、「CN」と入力します。
12. [グループ検索フィルタ] で、クエリ文字列を入力します。たとえば、フィルタは (& (サムアカウント名 = テスト) (オブジェクトクラス =*)) になります。
13. [Create] をクリックしてから、[Close] をクリックします。
14. [認証ポリシーの作成] ダイアログボックスで、[名前付き式] の横にある式を選択し、[式の追加]、[作成]、[閉じる] の順にクリックします。

複数のドメインに対する **LDAP** グループ抽出の設定

March 26, 2020

認証用のドメインが複数あり、StoreFront または Web Interface を使用している場合は、グループ抽出を使用して正しいドメイン名を Web Interface に送信するように Citrix Gateway を構成できます。

Active Directory では、ネットワーク内の各ドメインに対してグループを作成する必要があります。グループを作成したら、そのグループと指定したドメインに属するユーザーを追加します。Active Directory でグループを構成したら、Citrix Gateway 上の複数のドメインに対して LDAP グループの抽出を構成します。

複数のドメインのグループ抽出用に Citrix Gateway を構成するには、ネットワーク上のドメイン数と同じ数のセッションおよび認証ポリシーを作成する必要があります。たとえば、Sampa と Child という 2 つのドメインがあるとします。各ドメインは、1 つのセッションポリシーと 1 つの認証ポリシーを受け取ります。

ポリシーを作成したら、Citrix Gateway でグループを作成し、そのグループにセッションポリシーをバインドします。次に、仮想サーバーに認証ポリシーをバインドします。

StoreFront を複数のドメインに展開する場合は、ドメイン間に信頼関係が必要です。

複数のドメインに Citrix Endpoint Management または Web Interface を展開する場合、ドメインは相互に信頼する必要はありません。

グループ抽出のセッションポリシーの作成

March 26, 2020

グループ抽出のセッションポリシーを作成する最初の手順は、2 つのセッションプロファイルを作成し、次のパラメータを設定することです。

- ICA プロキシを有効にします。
- Web Interface Web アドレスを追加します。
- Windows ドメインを追加します。
- プロファイルをセッションポリシーに追加し、式を true に設定します。

グループ抽出用のセッションプロファイルを作成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウで、[プロファイル] タブをクリックし、[追加] をクリックします。
3. [名前] に、プロファイルの名前を入力します。たとえば、「Sampa」と入力します。
4. [公開アプリケーション] タブで、次の操作を行います。
   a) ICA プロキシの横にある「グローバルオーバーライド」をクリックし、「オン」を選択します。
   b) Web Interface アドレス] の横の [グローバル上書き] をクリックし、Web Interface Web アドレスを入力します。
   c) [シングルサインオンドメイン] の横にある [グローバル上書き] をクリックし、Windows ドメインの名前を入力して [作成] をクリックします。
5. [名前] で、最初のドメインの名前をクリアし、2 番目のドメインの名前を入力します ([子] など)。
6. [シングルサインオンドメイン] の横にある最初の Windows ドメインの名前を消去し、2 番目のドメインの名前を入力し、[作成]、[閉じる] の順にクリックします。

セッションプロファイルを作成したら、2 つのセッションポリシーを作成します。各セッションポリシーでは、プロファイルの 1 つを使用します。

セッションポリシーを作成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4.「要求プロファイル」で、最初のドメインのプロファイルを選択します。
5. [名前付き式] の横にある [全般] をクリックし、[True value] を選択し、[式の追加] をクリックして、[作成] をクリックします。
6. [名前] で、名前を 2 番目のドメインに変更します。
7. [要求プロファイル] で、2 番目のドメインのプロファイルを選択し、[作成]、[閉じる] の順にクリックします。

複数のドメインの **LDAP** 認証ポリシーの作成

March 26, 2020

Citrix Gateway でセッションポリシーを作成したら、ほぼ同じ LDAP 認証ポリシーを作成します。認証ポリシーを設定する場合、重要なフィールドは
Search Filter です。このフィールドには、Active Directory で作成したグループの名前を入力する必要があります。

最初に認証プロファイルを作成してから、認証ポリシーを作成します。

複数のドメイングループ抽出の認証プロファイルを作成するには

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］>［ポリシー］>［認証］の順に展開します。
2. ナビゲーションペインで［LADP］をクリックします。
3. 詳細ウィンドウで、[サーバー] タブをクリックし、[追加] をクリックします。
4. [名前] に、最初のドメインの名前を入力します (例:Sampa)。
5. LDAP サーバの設定を構成し、[Create] をクリックします。
6. ステップ 3、4、5 を繰り返して 2 番目のドメインの認証プロファイルを設定し、[Close] をクリックします。

プロファイルを作成して保存したら、認証ポリシーを作成します。

複数のドメイングループ抽出の認証ポリシーを作成するには

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］>［ポリシー］>［認証］の順に展開します。
2. 詳細ウィンドウで、[ポリシー] タブをクリックし、[追加] をクリックします。
3. [名前] に、最初のドメインの名前を入力します。
4.「認証タイプ」で「LDAP」を選択します。
5.「サーバー」で、最初のドメインの認証プロファイルを選択します。
6. [名前付き式] の横にある [全般] をクリックし、[True value] を選択し、[式の追加] をクリックして、[作成] をクリックします。
7. [名前] に、2 番目のドメインの名前を入力します。
8. [サーバー] で、2 番目のドメインの認証プロファイルを選択し、[作成]、[閉じる] の順にクリックします。

複数のドメインの **LDAP** グループ抽出のためのグループとバインディングポリシーの作成

March 26, 2020

認証ポリシーを作成したら、Citrix Gateway にグループを作成します。グループを作成したら、認証ポリシーを仮想サーバーにバインドします。

Citrix Gateway でグループを作成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、[Citrix Gateway] > [ユーザー管理] の順に展開し、[AAA グループ] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [グループ名] に、最初の Active Directory グループの名前を入力します。
   重要：複数のドメインからグループを抽出するために Citrix Gateway でグループを作成する場合、グループ名は Active Directory で定義したグループと同じである必要があります。グループ名も大文字と小文字が区別され、大文字と小文字は Active Directory で入力した大文字と小文字と一致する必要があります。
4. [ポリシー] タブで、[セッション] をクリックし、[ポリシーの挿入] をクリックします。
5. [ポリシー名] でポリシーをダブルクリックし、[作成] をクリックします。

認証ポリシーを仮想サーバーにバインドするには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 構成ユーティリティのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
3. 詳細ウィンドウで、仮想サーバーをクリックし、[開く] をクリックします。
4. [認証] タブで [プライマリ] をクリックし、[ポリシー名] の [ポリシーの挿入] をダブルクリックして、最初の認証ポリシーを選択します。
5. [ポリシー名] の [ポリシーの挿入] をクリックし、2 番目の認証ポリシーをダブルクリックして、[OK] をクリックします。

クライアント証明書認証の構成

March 26, 2020

Citrix Gateway 仮想サーバーにログオンするユーザーを、クライアント証明書の属性に基づいて認証することもできます。クライアント証明書認証は、2 要素認証を提供するために、LDAP や RADIUS などのほかの種類の認証と一緒に使用することもできます。

クライアント側の証明書の属性でユーザーを認証するには、仮想サーバー上のクライアント認証が有効になっており、クライアント証明書を要求するように構成されている必要があります。さらに、Citrix Gateway 上でルート証明書をその仮想サーバーにバインドする必要があります。

ユーザーが Citrix Gateway 仮想サーバーにログオンすると、認証後、証明書の指定されたフィールドからユーザー名情報が抽出されます。通常、このフィールドは Subject:CN です。ユーザー名の抽出に成功すると、ユーザーの認証が完了します。SSL（Secure Sockets Layer）ハンドシェイク時に有効な証明書が提供されなかったりユーザー名の抽出に失敗したりすると、認証に失敗します。

クライアント証明書に基づいて認証するには、既定の認証の種類としてクライアント証明書を指定します。また、「証明書アクション」を作成して、クライアントの SSL 証明書に基づいた認証時の動作を定義することもできます。

クライアント証明書をデフォルトの認証タイプとして構成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [認証設定の変更] をクリックします。
3. [最大ユーザー数] に、クライアント証明書を使用して認証できるユーザーの数を入力します。
4. 「デフォルトの認証タイプ」で、「Cert」を選択します。
5. 「ユーザー名フィールド」で、ユーザー名を保持する証明書フィールドの種類を選択します。
6. [グループ名フィールド] で、グループ名を保持する証明書フィールドのタイプを選択します。
7. [既定の承認グループ] に、既定のグループの名前を入力し、[OK] をクリックします。

クライアント証明書からのユーザー名の抽出

Citrix Gateway でクライアント証明書による認証を有効にすると、クライアント証明書の属性に基づいてユーザーが認証されます。認証が正常に完了すると、証明書からユーザー名またはユーザーのユーザーおよびグループ名が抽出され、そのユーザーに指定されたポリシーが適用されます。

クライアント証明書認証ポリシーの構成およびバインド

March 26, 2020

クライアント証明書認証ポリシーを作成し、仮想サーバーにバインドできます。このポリシーを使用して、特定のグループまたはユーザーへのアクセスを制限できます。このポリシーは、グローバルポリシーよりも優先されます。

クライアント証明書の認証ポリシーを構成するには、次の手順を実行します。

1. 構成ユーティリティの［構成］タブで、［**Citrix Gateway**］**>**［ポリシー］**>**［認証］の順に展開します。
2. ナビゲーションウィンドウの [認証] で、[**CERT**] をクリックします。
3. 詳細ウィンドウで、[追加] をクリックします。
4. [**Name**] フィールドに、ポリシーの名前を入力します。
5. [サーバー] の横にある [新規] をクリックします。
6. [名前**]** に、プロファイルの名前を入力します。
7. [**2** 係数] の横の [**OFF**] を選択します。
8. [ユーザー名] フィールドと [グループ名] フィールドで値を選択し、[作成] をクリックします。
   注：クライアント証明書をデフォルトの認証タイプとして設定した場合は、ポリシーに使用したものと同じ名前を使用します。デフォルトの認証タイプの [

User Name] フィールドと [
Group Name] フィールドに入力した場合は、プロファイルにも同じ値を使用します。

9. [認証ポリシーの作成] ダイアログボックスで、[名前付き式] の横にある式を選択し、[式の 追加]、[作成]、[閉じる] の順にクリックします。

クライアント証明書ポリシーを仮想サーバにバインドするには、次の手順を実行します。

クライアント証明書の認証ポリシーを構成したら、それを仮想サーバーにバインドできます。

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[**Citrix Gateway**] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、仮想サーバーをクリックし、[開く] をクリックします。
3. **Citrix Gateway** 仮想サーバーの構成］ダイアログボックスで、［認証］タブをクリックします。
4. [プライマリ] または [セカンダリ] をクリックします。
5. [詳細] の [ポリシーの挿入] をクリックします。
6. [ポリシー名] でポリシーを選択し、[**OK**] をクリックします。

クライアント証明書を要求するように仮想サーバーを構成するには、次の手順を実行します。

認証にクライアント証明書を使用する場合は、SSL ハンドシェイク中にクライアント証明書が要求されるように仮想サーバーを構成する必要があります。

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[**Citrix Gateway**] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、[仮想サーバー] をクリックし、[開く] をクリックします。
3. [証明書] タブで、[**SSL** パラメーター] をクリックします。
4. [その他] の [クライアント認証] をクリックします。
5. [クライアント証明書] で、[オプション] または [必須] を選択し、[OK] を 2 回クリックします。同じ仮想サーバー上で他の認証タイプを許可し、クライアント証明書を使用する必要がない場合は、[オプション] を選択します。

> 注
>
> - コールバック URL の詳細については、Citrix Gateway のインポートを参照してください。
> - 証明書について詳しくは、「証明書のインストール、リンク、および更新」を参照してください。

2 要素クライアント証明書認証の設定

March 26, 2020

最初にユーザーを認証するようにクライアント証明書を構成し、次に LDAP や RADIUS などのセカンダリ認証タイプを使用してログオンするようにユーザーに要求できます。このシナリオでは、クライアント証明書が最初にユーザーを認証します。その後、ユーザー名とパスワードを入力できるログオンページが表示されます。SSL (セキュアソケットレイヤー) ハンドシェイクが完了すると、ログオンシーケンスは、次の 2 つのパスのいずれかを使用できます。

- ユーザー名もグループも証明書から抽出されません。ログオンページが表示され、有効なログオン資格情報の入力を求めるプロンプトが表示されます。Citrix Gateway は、通常のパスワード認証の場合と同様にユーザー資格情報を認証します。
- クライアント証明書からユーザー名とグループ名が抽出されます。ユーザー名のみが抽出されると、ログオン名が存在するユーザーにはログオンページが表示され、ユーザーは名前を変更できません。パスワードフィールドのみが空白です。

認証の第 2 ラウンド中に Citrix Gateway が抽出するグループ情報は、Citrix Gateway が証明書から抽出したグループ情報（存在する場合）に追加されます。

スマートカード認証の構成

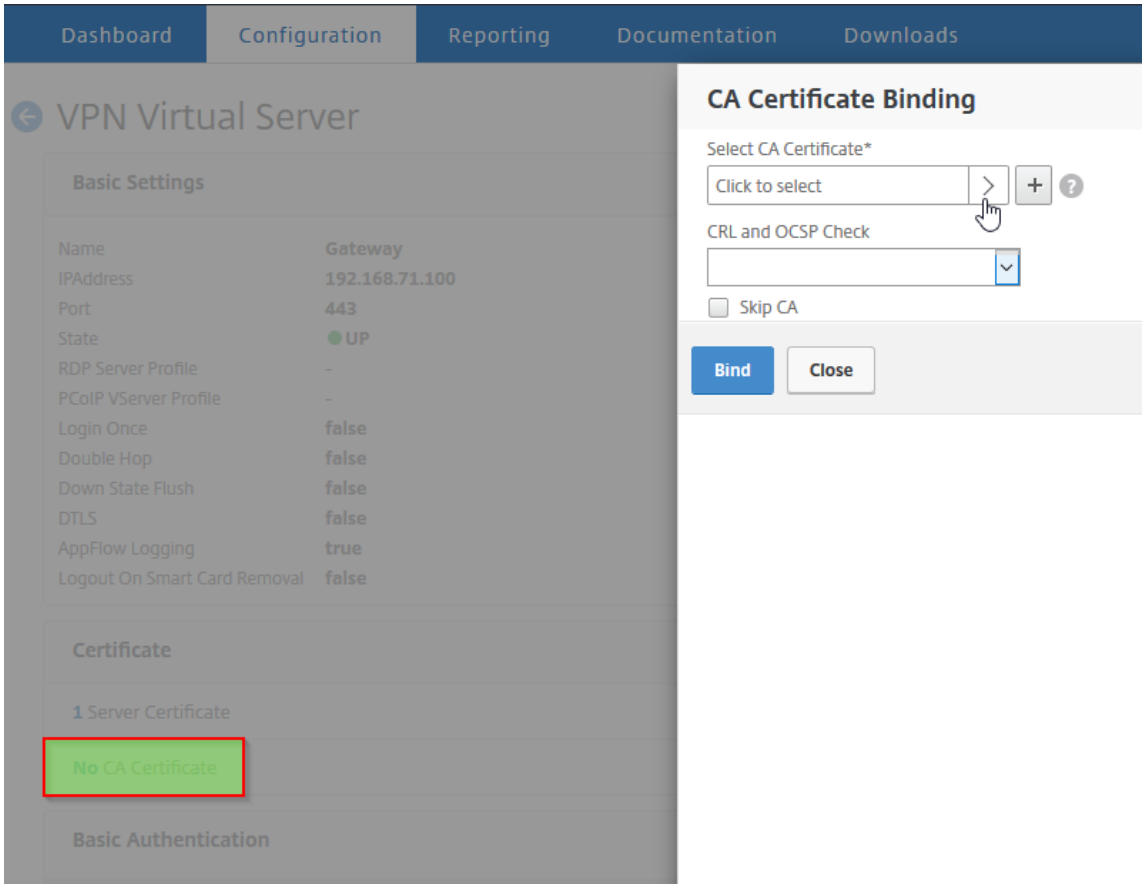
April 9, 2020

暗号化スマートカードを使用してユーザーを認証するように、Citrix Gateway を構成できます。

Citrix Gateway で動作するようにスマートカードを構成するには、次の操作を行う必要があります。

- 証明書認証ポリシーを作成します。詳しくは、「クライアント証明書認証の構成」を参照してください。
- 認証ポリシーを仮想サーバーにバインドします。
- クライアント証明書を発行する認証局（CA）のルート証明書を Citrix Gateway に追加します。詳しくは、「Citrix Gateway にルート証明書をインストールするには」を参照してください。

  重要: スマートカード認証用にルート証明書を仮想サーバーに追加する場合は、次の図に示すように、**[CA** 証明書の選択] ドロップダウンボックスから証明書を選択する必要があります。
  図 1: スマートカード認証用のルート証明書の追加



クライアント証明書を作成したら、フラッシュと呼ばれる証明書をスマートカードに書き込むことができます。この手順を完了すると、スマートカードをテストできます。

スマートカードパススルー認証用に Web Interface を構成する場合、次のいずれかの条件が存在する場合、Web Interface へのシングル・サインオンは失敗します。

- [公開アプリケーション] タブでドメインを mydomain ではなく mydomain.com として設定した場合。
- [公開アプリケーション] タブでドメイン名を設定せず、wi-sso-split-upn コマンドを実行する場合は、値を 1 に設定します。この例では、ユーザープリンシパル名には、ドメイン名 “mydomain.com” が含まれています。

スマートカード認証を使用して、ユーザーのログオンプロセスを合理化すると同時に、インフラストラクチャへのユーザーアクセスのセキュリティを強化できます。社内ネットワークへのアクセスは、公開キーのインフラストラクチャを使用した証明書ベースの 2 要素認証によって保護されます。秘密キーは、ハードウェアで保護されるため、スマートカードの外に漏れることはありません。ユーザーは、スマートカードと PIN を使用してさまざまなコーポレートデバイスからデスクトップとアプリケーションにアクセスできるようになります。

スマートカードは、Citrix Virtual Apps and Desktops で提供されるデスクトップとアプリケーションのユーザー認証を StoreFront 経由で行うために使用できます。StoreFront にログオンしているスマートカードユーザーは、Citrix Endpoint Management が提供するアプリケーションにもアクセスできます。ただし、クライアント証明書認証を使用する Endpoint Management Web アプリケーションにアクセスするには、再度認証する必要がありま

す。

詳しくは、StoreFront のドキュメントの「スマートカード認証の構成」を参照してください。

セキュア **ICA** 接続によるスマートカード認証の構成

Citrix Gateway でシングルサインオンが構成されたスマートカードを使用してログオンし、安全な ICA 接続を確立するユーザーは、ログオン時と公開リソースの起動時に、個人識別番号（PIN）の入力を求めるプロンプトが表示されることがあります。この状況は、Web ブラウザーと Citrix Workspace アプリがクライアント証明書を使用するように構成されている同じ仮想サーバーを使用している場合に発生します。Citrix Workspace アプリは、Web ブラウザーとプロセスまたは SSL（セキュア・ソケット・レイヤー）接続を共有しません。したがって、ICA 接続で Citrix Gateway との SSL ハンドシェイクが完了すると、クライアント証明書が 2 回必要です。

ユーザーに 2 番目の PIN プロンプトが表示されないようにするには、次の 2 つの設定を変更する必要があります。

- VPN 仮想サーバ上のクライアント認証を無効にする必要があります。
- SSL 再ネゴシエーションを有効にする必要があります。

仮想サーバを構成したら、Web Interface 5.3 での Citrix Gateway 設定の構成の説明に従って、1 つ以上の STA サーバを仮想サーバにバインドします。

スマートカード認証をテストすることもできます。

クライアント認証を無効にする手順は、次のとおりです。

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. メインの詳細ペインで関連する仮想サーバーを選択し、[編集] をクリックします。
3. [詳細オプション] ウィンドウで、[SSL パラメータ] をクリックします。
4. [クライアント認証] チェックボックスをオフにします。
5. [完了] をクリックします。

SSL 再ネゴシエーションを有効にするには、次の手順を実行します。

1. 設定ユーティリティを使用して、[設定] タブから [トラフィック管理] に移動し、[SSL] をクリックします。
2. メインパネルで、[SSL の詳細設定の変更] をクリックします。
3. [SSL 再ネゴシエーションの拒否] メニューから [いいえ] を選択します。

スマートカード認証をテストするには、次の手順に従います。

1. スマートカードをユーザーデバイスに接続します。
2. Web ブラウザーを開き、Citrix Gateway にログオンします。

共通アクセスカードの設定

March 26, 2020

米国国防総省は、識別と認証に共通のアクセスカードを使用します。

共通アクセスカードを設定するには、次の手順を実行します。

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］>［ポリシー］>［認証］の順に展開します。
2. [サーバー] タブで、[追加] をクリックします。
3. [名前] ボックスに名前を入力します。
4. [認証の種類] で、[証明書] を選択します。
5. [ユーザー名フィールド] に「サブジェクト名: プリンシパル名」と入力し、[作成] をクリックします。
6. [ポリシー] タブで、このサーバを使用するポリシーを作成し、そのポリシーを仮想サーバにバインドします。

RADIUS 認証の構成

March 26, 2020

1 つまたは複数の RADIUS サーバーでユーザーアクセスを認証するように Citrix Gateway を構成できます。RSA SecurID、SafeWord、または Gemalto Protiva 製品を使用している場合、これらの各製品は RADIUS サーバーを使用して構成されます。

構成によっては、ネットワークアクセスサーバの IP アドレス (NAS IP) またはネットワークアクセスサーバ識別子 (NAS ID) の使用が必要になる場合があります。RADIUS 認証サーバーを使用するように Citrix Gateway を構成する場合は、次のガイドラインに従ってください。

- NAS IP の使用を有効にした場合、アプライアンスは、RADIUS 接続の確立に使用される送信元 IP アドレスではなく、構成済みの IP アドレスを RADIUS サーバに送信します。
- NAS ID を構成すると、アプライアンスは RADIUS サーバーにこの識別子を送信します。NAS ID を構成しないと、アプライアンスは RADIUS サーバーにホスト名を送信します。
- NAS IP を有効にすると、アプライアンスは、NAS IP を使用して RADIUS サーバーと通信するように構成された NAS ID を無視します。

ゲマルトプロティバの設定

Protiva は Gemalto が開発した強力な認証プラットフォームで、Gemalto のスマートカード認証の強みを利用しています。Protiva では、ユーザー名、パスワード、および Protiva デバイスが生成するワンタイムパスワードを使用してログオンします。RSA SecurID と同様に、認証要求は Protiva 認証サーバーに送信され、サーバーはパスワードを検証または拒否します。Citrix Gateway で動作するように Gemalto Protiva を構成するには、以下のガイドラインに従ってください。

- Protiva サーバーをインストールします。
- Microsoft IAS RADIUS サーバーに、インターネット認証サーバー (IAS) を拡張する Protiva SAS エージェントソフトウェアをインストールします。IAS サーバーの IP アドレスとポート番号を書き留めておいてください。

- Citrix Gateway で RADIUS 認証プロファイルを構成し、Protiva サーバーの設定を入力します。

セーフワードの設定

SafeWord 製品ラインは、トークンベースのパスコードを使用した安全な認証を提供します。ユーザーがパスコードを入力すると、SafeWord はすぐにパスコードを無効化し、再度使用することはできません。SafeWord サーバーを設定する場合は、次の情報が必要です。

- Citrix Gateway の IP アドレス。これは、RADIUS サーバクライアント設定で設定した IP アドレスと同じ IP アドレスである必要があります。Citrix Gateway は、内部 IP アドレスを使用して RADIUS サーバーと通信します。共有シークレットを構成するときは、内部 IP アドレスを使用します。高可用性を実現するために 2 つのアプライアンスを構成する場合は、仮想内部 IP アドレスを使用します。
- 共有シークレット。
- SafeWord サーバーの IP アドレスとポート。デフォルトのポート番号は 1812 です。

RADIUS 認証を構成するには

March 26, 2020

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］>［ポリシー］>［認証］の順に展開します。
2. [RADIUS] をクリックし、詳細ウィンドウの [ポリシー] タブで [追加] をクリックします。
3. [認証ポリシーの作成] ダイアログボックスの [名前] に、ポリシーの名前を入力します。
4. [名前] に、ポリシーの名前を入力します。
5. [サーバー] の横にある [新規] をクリックします。
6. [認証ポリシーの作成] ダイアログボックスの [名前] に、サーバーの名前を入力します。
7. [サーバー] の [IP アドレス] に、RADIUS サーバーの IP アドレスを入力します。
8. [ポート] に、ポートを入力します。デフォルトは 1812 です。
9. [詳細] の [シークレットキー] と [シークレットキーの確認] に、RADIUS サーバーのシークレットを入力します。
10. [NAS ID] に識別子番号を入力し、[作成] をクリックします。
11. [認証ポリシーの作成] ダイアログボックスで、[名前付き式] の横にある式を選択し、[式の追加]、[作成]、[閉じる] の順にクリックします。

RADIUS 認証プロトコルの選択

March 26, 2020

Citrix Gateway では、次のような複数のプロトコルを使用してユーザー認証を行うように構成された RADIUS の実装がサポートされています。

- パスワード認証プロトコル (PAP)
- Challenge-Handshake Authentication Protocol (CHAP)
- Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP バージョン 1 およびバージョン 2)

Citrix Gateway の展開が RADIUS 認証を使用するように構成されていて、PAP を使用するように RADIUS サーバーが構成されている場合は、強力な共有シークレットを RADIUS サーバーに割り当てることでユーザー認証を強化できます。強力な RADIUS 共有シークレットは、大文字、小文字、数字、句読点のランダムなシーケンスで構成され、少なくとも 22 文字です。可能であれば、ランダムな文字生成プログラムを使用して RADIUS 共有秘密を特定します。

RADIUS トラフィックをさらに保護するには、Citrix Gateway アプライアンスまたは仮想サーバーごとに異なる共有シークレットを割り当てます。RADIUS サーバでクライアントを定義する場合、各クライアントに個別の共有シークレットを割り当てることもできます。その場合は、RADIUS 認証を使用する Citrix Gateway ポリシーを個別に構成する必要があります。

RADIUS ポリシーを作成するときは、ポリシーの一部として Citrix Gateway で共有シークレットを構成します。

IP アドレス抽出の設定

March 26, 2020

RADIUS サーバーから IP アドレスを抽出するように Citrix Gateway を構成できます。ユーザが RADIUS サーバで認証されると、サーバは、ユーザに割り当てられたフレーム IP アドレス（アクセス要求の RADIUS アトリビュート 8 フレーム IP アドレスとも呼ばれる）を返します。IP アドレス抽出のコンポーネントは次のとおりです。

- リモート RADIUS サーバーが、Citrix Gateway にログオンしているユーザーの内部ネットワークからの IP アドレスを提供できるようにします。
- ベンダーでエンコードされたアトリビュートを含め、**ipaddress** タイプを使用する任意の RADIUS アトリビュートを設定できます。

IP アドレス抽出用に RADIUS サーバを設定する場合は、ベンダー ID とアトリビュートタイプを設定します。ベンダー ID とアトリビュートは、RADIUS クライアントと RADIUS サーバ間のアソシエーションを作成するために使用されます。

- RADIUS サーバは、ベンダー識別子（ID）を使用して、RADIUS サーバで設定された IP アドレスのプールからクライアントに IP アドレスを割り当てることができます。ベンダー ID は、内部ネットワークの IP アドレスを提供する RADIUS 応答のアトリビュートです。値 0 は、属性がベンダーエンコードされていないことを示します。
- アトリビュートタイプは、RADIUS 応答のリモート IP アドレスアトリビュートです。最小値は 1 で、最大値は 255 です。

一般的な設定は、RADIUS アトリビュートの フレーム **IP** アドレスを抽出することです。ベンダー ID が 0 に設定されているか、指定されていません。属性タイプは 8 に設定されています。

RADIUS サーバからの IP アドレス抽出を設定するには、次の手順を実行します。

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］>［ポリシー］>［認証］の順に展開します。
2. [RADIUS] をクリックし、詳細ウィンドウの [ポリシー] タブで RADIUS ポリシーを選択し、[開く] をクリックします。
3. [認証ポリシーの構成] ダイアログボックスで、[サーバー] の横にある [変更] をクリックします。
4. [詳細] の [グループベンダー ID] に値を入力します。
5. [グループ属性の種類] に値を入力し、[OK] を 2 回クリックします。

RADIUS グループ抽出の設定

March 26, 2020

RADIUS 許可は、グループ抽出と呼ばれる方法を使用して設定できます。グループ抽出を構成すると、ユーザーを Citrix Gateway に追加するのではなく、RADIUS サーバー上のユーザーを管理できます。

RADIUS 認可を設定するには、認証ポリシーを使用し、グループベンダー ID（ID)、グループアトリビュートタイプ、グループプレフィクス、およびグループセパレータを設定します。ポリシーを構成するときは、式を追加し、ポリシーをグローバルまたは仮想サーバにバインドします。

Windows サーバ 2003 での RADIUS の構成

Windows Server 2003 で RADIUS 認証に Microsoft インターネット認証サービス（IAS）を使用している場合は、Citrix Gateway の構成時に次の情報を提供する必要があります。

- ベンダー ID は、IAS で入力したベンダー固有のコードです。
- 「タイプ」は、ベンダーによって割り当てられた属性番号です。
- 属性名は、IAS で定義した属性名のタイプです。デフォルト名は CTXSUser グループ = です。

IAS が RADIUS サーバーにインストールされていない場合は、コントロールパネルの [プログラムの追加と削除] からインストールできます。詳細については、Windows オンラインヘルプを参照してください。

IAS を構成するには、Microsoft 管理コンソール (MMC) を使用して、IAS 用のスナップインをインストールします。ウィザードに従って、次の設定を選択します。

- ローカルコンピュータを選択します。
- [リモートアクセスポリシー] を選択し、カスタムポリシーを作成します。
- ポリシーの [Windows グループ] を選択します。
- 次のいずれかのプロトコルを選択します。
  - Microsoft Challenge-Handshake Authentication Protocol バージョン 2 (MS-CHAP v2)
  - Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP)

  - Challenge-Handshake Authentication Protocol (CHAP)
  - 暗号化されていない認証（PAP、SPAP）

- 「ベンダー固有の属性」を選択します。

  ベンダー固有の属性は、サーバー上のグループで定義したユーザーと Citrix Gateway のユーザーを一致させる必要があります。この要件を満たすには、ベンダー固有の属性を Citrix Gateway に送信します。[RADIUS] が [Standard] であることを確認します。

- RADIUS のデフォルトは 0 です。この番号は、ベンダーコードに使用します。
- ベンダーが割り当てたアトリビュート番号は 0 です。

  これは、「ユーザー・グループ」属性に割り当てられた番号です。属性は文字列形式です。

- 属性形式に [文字列] を選択します。

  Attribute 値には、属性名とグループが必要です。

  Access Gateway の場合、属性値は CTXSUserGroups= グループ名です。売上と財務など 2 つのグループが定義されている場合、属性値は CTXSUserGroups=sales;finance です。各グループはセミコロンで区切ります。

- [ダイヤルインプロファイルの編集] ダイアログボックスの他のすべてのエントリを削除し、[ベンダー固有] と表示されているエントリを残します。

IAS でリモートアクセスポリシーを構成した後、Citrix Gateway で RADIUS 認証と承認を構成します。

RADIUS 認証を構成するときは、IAS サーバーで構成した設定を使用します。

Windows サーバー **2008** での認証用に **RADIUS** を構成する

Windows Server 2008 では、インターネット認証サービス (IAS) に代わるネットワークポリシーサーバー (NPS) を使用して RADIUS 認証と承認を構成します。サーバーマネージャーを使用して役割として NPS を追加することで、NPS をインストールできます。

NPS をインストールするときに、ネットワークポリシーサービスを選択します。インストール後、[スタート] メニューの [管理サービス] から NPS を起動することで、ネットワークの RADIUS 設定を構成できます。NPS を開くと、Citrix Gateway を RADIUS クライアントとして追加し、サーバーグループを構成します。

RADIUS クライアントを構成するときは、次の設定を選択してください。

- ベンダー名として、[RADIUS 標準] を選択します。
- Citrix Gateway で同じ共有シークレットを構成する必要があるため、共有シークレットを書き留めます。

RADIUS グループには、RADIUS サーバの IP アドレスまたはホスト名が必要です。デフォルト設定は変更しないでください。

RADIUS クライアントとグループを構成したら、次の 2 つのポリシーで設定を行います。

- 接続要求ポリシー: ネットワークサーバーの種類、ネットワークポリシーの条件、ポリシーの設定など、Citrix Gateway 接続の設定を構成します。
- 拡張認証プロトコル (EAP) 認証とベンダー固有の属性を構成するネットワークポリシー。

接続要求ポリシーを構成する場合は、ネットワークサーバーの種類として [未指定] を選択します。次に、条件として [NAS ポートタイプ] を選択し、値として [仮想 (VPN)] を選択して、条件を構成します。

ネットワークポリシーを構成するときは、次の設定を構成する必要があります。

- ネットワークアクセスサーバーの種類として [リモートアクセスサーバー (VPN ダイヤルアップ)] を選択します。
- EAP の [暗号化認証 (CHAP)] と [暗号化されていない認証 (PAP および SPAP)] を選択します。
- ベンダー固有の属性に [RADIUS 標準] を選択します。

  デフォルトの属性番号は 26 です。このアトリビュートは、RADIUS 認可に使用されます。

  Citrix Gateway では、サーバー上のグループで定義されたユーザーと Citrix Gateway 上のユーザーを一致させるために、ベンダー固有の属性が必要です。これは、ベンダー固有の属性を Citrix Gateway に送信することによって行われます。
- 属性形式として [文字列] を選択します。

  Attribute 値には、属性名とグループが必要です。

  Citrix Gateway の場合、属性値は CTXSUserGroups= グループ名です。売上と財務など 2 つのグループが定義されている場合、属性値は CTXSUserGroups=sales;finance です。各グループはセミコロンで区切ります。
- 区切り記号は、セミコロン、コロン、スペース、ピリオドなどのグループを区切るための NPS で使用した区切り記号です。

IAS でリモートアクセスポリシーの構成が完了したら、Citrix Gateway で RADIUS 認証と承認を構成できます。

RADIUS 認可を設定するには

March 26, 2020

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］>［ポリシー］>［認証］の順に展開します。
2. [RADIUS] をクリックします。
3. [ポリシー] タブで、[追加] をクリックします。
4. [名前] に、ポリシーの名前を入力します。
5. サーバーの下 * [+] をクリックします。
6. [名前] に、RADIUS サーバーの名前を入力します。
7. [サーバー] に、RADIUS サーバーの IP アドレスとポートを入力します。

8. [詳細] で、[グループベンダー識別子] と [グループ属性タイプ] の値を入力します。
9. [パスワードのエンコーディング] で、認証プロトコルを選択し、[作成] をクリックします。
10. [認証ポリシーの作成] ダイアログボックスで、[名前付き式] の横にある式を選択し、[式の追加]、[作成]、[閉じる] の順にクリックします。

RADIUS ユーザアカウンティングの設定

March 26, 2020

Citrix Gateway は、ユーザーセッションの開始および停止メッセージを RADIUS アカウンティングサーバーに送信できます。各ユーザセッションに送信されるメッセージには、RFC2866 で定義されたアトリビュートのサブセットが含まれます。表 1 に、サポートされる属性と、それらが送信される RADIUS アカウンティングメッセージ（RAD_START および RAD_STOP）のタイプを示します。表 2 に、Acct-Terminate-Cause 属性に割り当てることができる定義済みの値と、対応する Citrix Gateway イベントを示します。

表 1. サポートされている RADIUS アトリビュート

属性	意味	RAD_START	RAD_STOP
User-Name	セッションに関連付けられたユーザーの名前。	○	○
Session-Id	NetScaler セッション ID。	○	○
Acct-Session-Time	セッション継続時間（秒）。		○
Acct-Terminate-Cause	アカウント解約の理由（下記参照）。		○

表 2. RADIUS 終端の原因

NetScaler のログアウト方法	RADIUS 終了の原因
LOGOUT_SESSN_TIMEDOUT	RAD_TERM_SESSION_TIMEOUT
LOGOUT_SESSN_INITIATEDBYUSER	RAD_TERM_USER_REQUEST
LOGOUT_SESSN_KILLEDBYADMIN	RAD_TERM_ADMIN_RESET
LOGOUT_SESSN_TLOGIN	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_MAXLICRCHD	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_CLISECCHK_FAILED	RAD_TERM_NAS_REQUEST

NetScaler のログアウト方法	RADIUS 終了の原因
LOGOUT_SESSN_PREAUTH_CHANGED	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_COOKIE_MISMATCH	RAD_TERM_NAS_REQUEST
LOGOUT_SESSS_DHT	RAD_TERM_NAS_REQUEST
LOGOUT_SESSS_2FACTOR_FAIL	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_ICALIC	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_INTERNALERR	RAD_TERM_NAS_ERROR
そのほか	RAD_TERM_NAS_ERROR

RADIUS ユーザアカウンティングを設定するには、ポリシーのペアを作成する必要があります。最初のポリシーは、アカウンティングメッセージを送信する RADIUS サーバを指定する RADIUS 認証ポリシーです。2 つ目は、RADIUS アカウンティングポリシーをアクションとして使用するセッションポリシーです。

RADIUS ユーザアカウンティングを設定するには、次の作業を行う必要があります。

1. RADIUS ポリシーを作成し、RADIUS アカウンティングサーバを定義します。アカウンティングサーバは、RADIUS 認証に使用するサーバと同じサーバにできます。
2. RADIUS ユーザアカウンティングサーバを指定するアクションとして RADIUS ポリシーを使用して、セッションポリシーを作成します。
3. セッションポリシーをグローバルにバインドしてすべてのトラフィックに適用するか、Citrix Gateway 仮想サーバーにバインドして、その仮想サーバーを流れるトラフィックにのみ適用します。

RADIUS ポリシーを作成するには

1. 構成ユーティリティーのナビゲーションペインで、［Citrix Gateway］ノードを展開し、［ポリシー］を展開します。
2. [認証] を展開し、[RADIUS] を選択します。
3. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
4. ポリシーの名前を入力します。
5. [Server] メニューからサーバを選択するか、[+] アイコンをクリックしてプロンプトに従って新しい RADIUS サーバを追加します。
6. [式] ペインの [保存されたポリシー式] メニューから [ns_true] を選択します。
7. ［作成］をクリックします。

セッションポリシーを作成するには

RADIUS アカウンティングサーバを指定する RADIUS ポリシーを設定したら、次のように、アクションでこのアカウンティングサーバを適用するセッションポリシーを作成します。

1. 構成ユーティリティーのナビゲーションペインで、[Citrix Gateway] ノードを展開し、[ポリシー] を展開します。
2.「セッション」を選択します。
3. メインの詳細ペインで、[追加] を選択します。
4. ポリシーの名前を入力します。
5. [Action] メニューで [+] アイコンをクリックして、新しいセッションアクションを追加します。
6. セッションアクションの名前を入力します。
7. [クライアントエクスペリエンス] タブをクリックします。
8. [アカウンティングポリシー] メニューで、前に作成した RADIUS ポリシーを選択します。
9. [作成] をクリックします。
10. [式] ペインの [保存されたポリシー式] メニューから [ns_true] を選択します。
11. [作成] をクリックします。

セッションポリシーをグローバルにバインドするには

1. 構成ユーティリティーのナビゲーションペインで、[Citrix Gateway] ノードを展開し、[ポリシー] を展開します。
2.「セッション」を選択します。
3. メインの詳細ペインの [操作] メニューから、[グローバルバインディング] を選択します。
4. [バインド] をクリックします。
5. [ポリシー] ウィンドウで、前に作成したセッションポリシーを選択し、[挿入] をクリックします。
6. [ポリシー] の一覧で、セッションポリシーの [優先度] エントリをクリックし、0 ～64000 の値を入力します。
7. [OK] をクリックします。

セッションポリシーを **Citrix Gateway** 仮想サーバーにバインドするには

1. 構成ユーティリティーのナビゲーションペインで、[Citrix Gateway] ノードを展開し、[仮想サーバー] を選択します。
2. メインの詳細ウィンドウで、仮想サーバーを選択し、[編集] をクリックします。
3. [Policies] ペインで、[+] アイコンをクリックしてポリシーを選択します。
4.「ポリシーの選択」メニューから「セッション」を選択し、「タイプの選択」メニューで「要求」が選択されていることを確認します。
5. [続行] をクリックします。
6. [バインド] をクリックします。
7. [ポリシー] ウィンドウで、前に作成したセッションポリシーを選択し、[挿入] をクリックします。
8. [OK] をクリックします。

SAML 認証の構成

March 26, 2020

セキュリティーアサーションマークアップ言語 (SAML) は、ID プロバイダー (IdP) とサービスプロバイダーの間で認証と承認を交換するための XML ベースの標準です。Citrix Gateway は、SAML 認証をサポートしています。

SAML 認証を構成するときは、次の設定を作成します。

- IdP 証明書名。IdP の秘密鍵に対応する公開鍵です。
- リダイレクト URL。これは、認証 IdP の URL です。認証されていないユーザーは、この URL にリダイレクトされます。
- [ユーザフィールド]: IdP が Subject タグの NameIdentifier タグとは異なる形式でユーザー名を送信する場合、このフィールドを使用してユーザー名を抽出できます。これはオプションの設定です。
- 署名証明書名。これは、IdP への認証要求に署名するために使用される Citrix Gateway サーバーの秘密鍵です。証明書名を設定しない場合、アサーションは署名なしに送信されるか、認証要求は拒否されます。
- SAML 発行者名。この値は、認証要求が送信されるときに使用されます。発行者フィールドには、アサーションが送信される権限を示す一意の名前が必要です。これはオプションのフィールドです。
- デフォルトの認証グループ。これは、ユーザの認証元となる認証サーバ上のグループです。
- 2 つのファクター。この設定では、2 要素認証を有効または無効にします。
- 署名されていないアサーションを拒否します。有効にすると、署名証明書名が構成されていない場合、Citrix Gateway はユーザー認証を拒否します。

Citrix Gateway は、HTTP POST バインディングをサポートしています。このバインディングでは、送信側は、必要な情報を持つフォーム自動投稿を含む 200 OK でユーザーに応答します。具体的には、そのデフォルトフォームには、フォームがリクエストかレスポンスかに応じて、SAMLRequest と SAMLResponse という 2 つの非表示フィールドが含まれている必要があります。フォームには RelayState も含まれています。RelayState は、証明書利用者によって処理されない任意の情報を送信するために送信側によって使用される状態または情報です。証明書利用者は、送信側が RelayState とともにアサーションを取得したときに、送信側が次に何をすべきかを知るように、単に情報を送り返します。RelayState を暗号化または難読化することをお勧めします。

Active Directory フェデレーションサービス 2.0 の構成

フェデレーションサーバーの役割で使用する任意の Windows Server 2008 コンピューターまたは Windows Server 2012 コンピューターで、Active Directory フェデレーションサービス (AD FS) 2.0 を構成できます。Citrix Gateway で動作するように AD FS サーバーを構成する場合は、証明書利用者の信頼ウィザードを使用して、次のパラメーターを構成する必要があります。

Windows Server 2008 パラメーター:

- 証明書利用者の信頼。Citrix Gateway のメタデータファイルの場所（https://vserver.fqdn.com/ns.metadata.xmlなど）を指定します。ここで、vserver.fqdn.com は Citrix Gateway 仮想サーバーの完全修飾ドメイン名（FQDN）です。FQDN は、仮想サーバーにバインドされたサーバー証明書にあります。

- 承認規則。証明書利用者へのアクセスをユーザーに許可または拒否できます。

サーバー 2012 のパラメーター:

- 証明書利用者の信頼。Citrix Gateway のメタデータファイルの場所（https://vserver.fqdn.com/ns.metadata.xmlなど）を指定します。ここで、vserver.fqdn.com は Citrix Gateway 仮想サーバーの完全修飾ドメイン名（FQDN）です。FQDN は、仮想サーバーにバインドされたサーバー証明書にあります。
- AD FS プロファイル。AD FS プロファイルを選択します。
- 証明書。Citrix Gateway は暗号化をサポートしていません。証明書を選択する必要はありません。
- SAML 2.0 WebSSO プロトコルのサポートを有効にします。これにより、SAML 2.0 SSO のサポートが有効になります。Citrix Gateway 仮想サーバーの URL（https:netScaler.virtualServerName.com/cgi/samlauthなど）を指定します。

  この URL は、Citrix Gateway アプライアンス上のアサーションコンシューマーサービスの URL です。これは定数パラメーターであり、Citrix Gateway はこの URL に対する SAML 応答を想定しています。
- 証明書利用者の信頼識別子。「Citrix Gateway」という名前を入力します。これは、証明書利用者を識別する URL です。たとえば、https://netscalerGateway.virtualServerName.com/adfs/services/trust。
- 承認規則。証明書利用者へのアクセスをユーザーに許可または拒否できます。
- 要求ルールを構成します。発行変換規則を使用して LDAP 属性の値を構成し、「要求として LDAP 属性を送信」テンプレートを使用できます。次に、次の情報を含む LDAP 設定を構成します。
  - メールアドレス
  - sAMAccountName
  - ユーザープリンシパル名 (UPN)
  - memberOf
- 証明書の署名。署名検証証明書を指定するには、[中継者のプロパティ] を選択して証明書を追加します。

  署名証明書が 2048 ビット未満の場合は、警告メッセージが表示されます。警告を無視して続行できます。テスト展開を設定している場合は、リレーパーティで証明書失効リスト（CRL）を無効にします。チェックを無効にしないと、AD FS は CRL で証明書の検証を試みます。

  CRL を無効にするには、次のコマンドを実行します。Set-ADFWRelayingPartyTrust - SigningCertificateRevocatonCheck None-TargetName NetScaler

設定を構成したら、中継パーティの信頼ウィザードを完了する前に、証明書利用者のデータを確認します。Citrix Gateway 仮想サーバー証明書は、https://vserver.fqdn.com/cgi/samlauthなどのエンドポイント URL で確認します。

中継パーティの信頼ウィザードでの設定の構成が完了したら、構成された信頼を選択し、プロパティを編集します。次のことを行う必要があります。

- セキュアハッシュアルゴリズムを SHA-1 に設定します。

  注：Citrix では SHA-1 のみがサポートされています。

- 暗号化証明書を削除します。暗号化されたアサーションはサポートされていません。
- 以下を含む要求ルールを編集します。
  - 変換規則の選択
  - 要求ルールの追加
  - 要求規則テンプレートの選択: 要求として LDAP 属性を送信する
  - 名前をつける
  - 属性ストアの選択:Active Directory
  - <Active Directory parameters>LDAP 属性を選択:
  - 「名前 ID」として「外出要求ルール」を選択します。

  注: 属性名 XML タグはサポートされていません。
- シングルサインオフのログアウト URL を設定します。要求ルールは [ログアウト URL の送信] です。カスタムルールは、次のようになります。

```
pre codeblock => issue(Type = "logoutURL", Value = "https://<adfs.fqdn
.com>/adfs/ls/", Properties["http://schemas.xmlsoap.org/ws/2005/05/
identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML
:2.0:attrname-format:unspecified"); <!--NeedCopy-->
```

AD FS の設定を構成したら、AD FS 署名証明書をダウンロードし、Citrix Gateway で証明書キーを作成します。その後、証明書とキーを使用して、Citrix Gateway で SAML 認証を構成できます。

SAML 2 要素認証の設定

SAML の 2 要素認証を設定できます。LDAP 認証を使用して SAML 認証を構成する場合は、次のガイドラインに従ってください。

- SAML がプライマリ認証タイプである場合は、LDAP ポリシーで認証を無効にし、グループ抽出を設定します。次に、LDAP ポリシーをセカンダリ認証タイプとしてバインドします。
- SAML 認証では、パスワードは使用されず、ユーザー名のみが使用されます。また、SAML 認証は、認証が成功した場合にのみユーザーに通知します。SAML 認証が失敗した場合、ユーザーには通知されません。失敗応答は送信されないため、SAML はカスケードの最後のポリシーか、唯一のポリシーである必要があります。
- 不透明な文字列ではなく、実際のユーザー名を構成することをお勧めします。
- SAML をセカンダリ認証タイプとしてバインドすることはできません。

SAML 認証を設定するには

October 22, 2021

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］>［ポリシー］>［認証］の順に展開します。

2. ナビゲーションペインで、[SAML] をクリックします。
3. 詳細ウィンドウで、[追加] をクリックします。
4. [認証ポリシーの作成] ダイアログボックスの [名前] に、ポリシーの名前を入力します。
5. [サーバー] の横にある [新規] をクリックします。
6. [名前] に、サーバープロファイルの名前を入力します。
7.「IdP 証明書名」で証明書を選択するか、「インストール」をクリックします。これは、SAML サーバーまたは IDP サーバーにインストールされた証明書です。

   [インストール] をクリックした場合は、証明書と秘密キーを追加します。詳しくは、「証明書のインストールと管理」を参照してください。
8.「リダイレクト URL」に、認証アイデンティティ・プロバイダ (IdP) の URL を入力します。

   SAML サーバーへのユーザーログオン用の URL です。これは、Citrix Gateway が最初の要求をリダイレクトするサーバーです。
9.「ユーザー・フィールド」に、抽出するユーザー名を入力します。
10.「署名証明書名」で、手順 9 で選択した証明書の秘密キーを選択します。

   これは、AAA 仮想 IP アドレスにバインドされる証明書です。SAML 発行者名は、lb.example.com や ng.example.com など、ユーザーがログオンする完全修飾ドメイン名 (FQDN) です。
11.「SAML 発行者名」に、アプライアンスが初期認証（GET）リクエストを送信する負荷分散または Citrix Gateway 仮想 IP アドレスの FQDN を入力します。
12. [既定の認証グループ] に、グループ名を入力します。
13. 2 ファクタ認証を有効にするには、[2 ファクタ] で [ON] をクリックします。
14. 署名なしアサーションを拒否を無効にします。SAML または IDP サーバーが SAML 応答に署名している場合にのみ、この設定を有効にします。
15. [Create] をクリックしてから、[Close] をクリックします。
16. [認証ポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [全般]、[True value]、[式の追加]、[作成]、[閉じる] の順にクリックします。

SAML 認証を使用して Citrix Gateway にログインする

October 22, 2021

SAML 認証を使用して、Citrix VPN クライアントと Workspace アプリを使用して Citrix Gateway にログインできます。このプラグインは、認証仮想サーバー (nfactor 認証) にバインドされた高度な SAML ポリシーを通じて SAML 認証のみをサポートします。

重要: SAML ポリシーが VPN 仮想サーバー (非 nfactor 認証) に直接バインドされている場合、プラグインは SAML 認証をサポートしません。

サポートされているプラットフォームとアプリ

次の表は、Citrix Gateway へのログイン時に SAML 認証をサポートするプラットフォームとアプリケーションの一覧です。

製品	バージョン
Citrix Gateway	バージョン 12.0 ビルド 41.16 以降
VPN クライアント	バージョン 12.1 は 49.37 以降をビルドします。サポートされているプラットフォーム: Windows 7、Windows 8、Windows 8.1、Windows 10
Workspace アプリのバージョン	Windows: 1808; Mac: 1808

高度な **SAML** ポリシーを使用した **SAML** 認証の構成

高度な SAML ポリシーを使用した SAML 認証の設定の詳細については、「SAML IdP としての Citrix ADC」を参照してください。

SAML 認証の認証の改善

March 26, 2020

この機能は SAML 知識を持つユーザ向けであり、この情報を使用するには、基本的な認証能力が必要です。この情報を使用するには、読者が FIPS を理解している必要があります。

以下の Citrix ADC 機能は、SAML 2.0 仕様と互換性のあるサードパーティのアプリケーション/サーバーで使用できます。

- SAML サービスプロバイダ (SP)
- SAML ID プロバイダー (IdP)

SP と IdP は、クラウドサービス間でシングルサインオン（SSO）を可能にします。SAML SP 機能は、IdP からのユーザーの要求に対処する方法を提供します。IdP は、サードパーティのサービスまたは別の Citrix ADC アプライアンスである可能性があります。SAML IdP 機能は、ユーザーのログオンをアサートし、SP によって消費される要求を提供するために使用されます。

SAML サポートの一部として、IdP モジュールと SP モジュールの両方が、ピアに送信されるデータにデジタル署名します。デジタル署名には、SP からの認証要求、IdP からのアサーション、これらの 2 つのエンティティ間のログア

ウトメッセージが含まれます。デジタル署名は、メッセージの信頼性を検証します。

SAML SP および IdP の現在の実装は、パケットエンジンでシグニチャ計算を行います。これらのモジュールは、SSL 証明書を使用してデータに署名します。FIPS 準拠の Citrix ADC では、SSL 証明書の秘密鍵はパケットエンジンまたはユーザー空間では利用できないため、現在の SAML モジュールは FIPS ハードウェアに対応していません。

このドキュメントでは、シグニチャ計算を FIPS カードにオフロードするメカニズムについて説明します。公開鍵が利用可能であるため、署名の検証はソフトウェアで行われます。

解決策

SAML 機能セットは、署名オフロードに SSL API を使用するように拡張されました。影響を受ける SAML サブ機能の詳細については、docs.citrix.com を参照してください。

1. SAML SP ポストバインディング — 認証リクエストの署名
2. SAML IdP ポストバインディング — アサーション/応答/両方の署名
3. SAML SP シングルログアウトシナリオ — SP によって開始されたモデルでのログアウト要求の署名と IdP によって開始されたモデルでのログアウト応答の署名
4. SAML SP アーティファクトバインディング — アーティファクト解決リクエストの署名
5. SAML SP リダイレクトバインディング — 認証要求の署名
6. SAML IdP リダイレクトバインディング — 応答/アサーション/両方の署名
7. SAML SP 暗号化のサポート — アサーションの復号化

プラットフォーム

API は FIPS プラットフォームにのみオフロードできます。

構成

オフロード設定は、FIPS プラットフォーム上で自動的に実行されます。

ただし、FIPS ハードウェアのユーザー空間では SSL 秘密キーを使用できないため、FIPS ハードウェアで SSL 証明書を作成する際に若干の構成が変更されます。

設定情報は次のとおりです。

- add ssl fipsKey fips-key

  次に、CSR を作成し、CA サーバで使用して証明書を生成する必要があります。その証明書を /nsconfig/sl にコピーできます。ファイルが fips3cert.cer であると仮定しましょう。

- add ssl certKey fips-cert -cert fips3cert.cer -fipsKey fips-key

  次に、SAML SP モジュールの SAML アクションでこの証明書を指定する必要があります。

- set samlAction <name> -samlSigningCertName fips-cert

  同様に、SAML IdP モジュールの samlIdpProfile でこれを使用する必要があります。

- set samlidpprofile fipstest –samlIdpCertName fips-cert

初めて、上記の fips キーはありません。FIPS キーがない場合は、「https://support.citrix.com/servlet/KbServlet/download/95102-665378/NS9000_FIPS_6\[1\]\[1\].1.pdf」の説明に従って作成します。

- create ssl fipskey <fipsKeyName> -modulus <positive_integer> [-exponent (3 | F4)]
- create certreq <reqFileName> -fipskeyName <string>

TACACS+ 認証の設定

April 9, 2020

TACACS+ サーバを認証用に設定できます。RADIUS 認証と同様に、TACACS+ は秘密キー、IP アドレス、およびポート番号を使用します。デフォルトのポート番号は 49 です。

TACACS+ サーバーを使用するように Citrix Gateway を設定するには、サーバーの IP アドレスと TACACS+ シークレットを指定します。ポートを指定する必要があるのは、使用しているサーバのポート番号が、デフォルトのポート番号である 49 以外の場合だけです。

ユーザインターフェイスを使用して TACACS+ 認証を設定するには、次の手順を実行します。

1. 構成ユーティリティの［構成］タブで、［**Citrix Gateway**］**>**［ポリシー］**>**［認証］の順に展開します。
2. [**TACACS**] をクリックします。
3. 詳細ウィンドウで、[追加] をクリックします。
4. [**Name**] フィールドに、ポリシーの名前を入力します。
5. [**Server**] フィールドの横にある [**Add**] をクリックして新しい TACACS サーバを作成するか、[**Edit**] をクリックして既存の TACACS サーバを変更します。
6. [名前] フィールドに、サーバーの名前を入力します。
7. [**IP** アドレス] に IP アドレスを入力します。
8. [ポート] で、デフォルトのポート番号 49 を使用します。
9. [**TACACS** キー] フィールドにキーを入力します。[**TACACS** キーの確認] フィールドに、確認のために同じキーを入力します。
10. [詳細] をクリックします。
11. 「認証」で「**ON**」を選択し、「作成」をクリックします。
12. [認証 **TACACS** ポリシーの作成] ダイアログボックスで、[式] を選択し、[作成] をクリックして、[閉じる] をクリックします。

コマンドラインインターフェイスを使用して TACACS+ 認証を設定するには、次のコマンドを入力します。


```
add authentication tacacsAction <name> [-serverIP <ip_addr|ipv6_addr
    |*>][-serverPort <port>] [-authTimeout <positive_integer>] {
 -tacacsSecret  }

[-authorization ( ON | OFF )] [-accounting ( ON | OFF )][-
    auditFailedCmds ( ON | OFF )] [-groupAttrName <string>][-
    defaultAuthenticationGroup <string>] [-Attribute1 <string>] [-
    Attribute2 <string>] [-Attribute3 <string>] [-Attribute4 <string>]
[-Attribute5 <string>] [-Attribute6 <string>] [-Attribute7 <string>] [-
    Attribute8 <string>] [-Attribute9 <string>] [-Attribute10 <string>]
[-Attribute11 <string>] [-Attribute12 <string>] [-Attribute13 <string>]
     [-Attribute14 <string>] [-Attribute15 <string>] [-Attribute16 <
    string>]
<!--NeedCopy-->
```

Citrix Gateway で TACACS+ サーバー設定を構成したら、ポリシーをバインドしてアクティブにします。ポリシーは、グローバルサーバレベルまたは仮想サーバレベルでバインドできます。認証ポリシーのバインドについて詳しくは、「認証ポリシーのバインド」を参照してください。

基本設定のクリア：**TACACS** 設定をクリアしない

March 26, 2020

概要

この拡張機能では、clear config コマンドの実行時に、RBA（ロールベースアクセス）関連のすべての設定を消去しないことに重点を置いています。

現在の clear config コマンドは、次の 3 つのレベルのいずれかで実行されます。

- Basic
- Extended
- Full

選択したレベルに基づいて、NetScaler 構成がクリアされ、工場出荷時のデフォルトにリセットされます。

使用するコマンドは次のとおりです。

```
clear ns config \[-force\] \<level\>
```

新しいコマンドは、すべての RBA 関連設定の削除を許可/拒否するノブを追加します。

新規コマンド

RBA 構成のクリア機能について説明します。

1. YES/NO ノブ、デフォルト：YES。

   管理者は、RBA 構成を保持するかどうかを決定します。

2. クリア設定の基本レベルのみがサポートされています。

3. 次の設定はクリアされません。

   - Add/bind system user/group.
   - Add cmd policy.
   - TACACS コマンド.(add TACACS action/policy).
   - Bind system global

   注： TACACS 関連の設定（action/policy）は、ポリシーがシステムグローバルにバインドされている場合、またはクリアされている場合、保持されます。

CLI の設定

使用したコマンド

```
clear config [ - force] <level> [-RBAconfig]
```

デフォルトでは、YES に設定され、指定されたレベルに基づいて設定がクリアされます。

—RBAconfig が NO に設定されている場合、RBA 関連の設定は保持されます。以下が含まれます。

- Add /bind system user /group
- Bind system global
- tacacs 関連コマンド (add tacacs action/policy))
- Add cmd policy

多要素認証の設定

March 26, 2020

Citrix Gateway では、次の 2 種類の多要素認証を構成できます。

- 認証の優先度レベルを設定するカスケード認証
- 2 つの種類の認証を使用してユーザーがログオンする必要がある 2 要素認証

複数の認証サーバがある場合は、認証ポリシーのプライオリティを設定できます。設定した優先度レベルによって、認証サーバーがユーザーの資格情報を検証する順序が決まります。プライオリティ番号が小さいポリシーは、番号の大きいポリシーよりも優先されます。

2 つの異なる認証サーバに対してユーザを認証させることができます。たとえば、LDAP 認証ポリシーと RSA 認証ポリシーを設定できます。ユーザーがログオンすると、最初にユーザー名とパスワードで認証されます。次に、個人識別番号 (PIN) と RSA トークンからのコードで認証します。

カスケード認証の設定

March 26, 2020

認証では、ポリシーの優先順位付けを使用して、複数の認証サーバのカスケードを作成できます。カスケードを構成すると、システムは、カスケード・ポリシーで定義されている各認証サーバーを経由して、ユーザーの資格情報を検証します。優先順位付けされた認証ポリシーは、昇順にカスケードされ、1 ～9999 の範囲の優先順位値を持つことができます。これらの優先順位は、グローバルサーバレベルまたは仮想サーバレベルでポリシーをバインドするときに定義します。

認証中に、ユーザーがログオンすると、仮想サーバーが最初にチェックされ、次にグローバル認証ポリシーがチェックされます。ユーザーが仮想サーバとグローバル両方の認証ポリシーに属している場合は、仮想サーバからのポリシーが最初に適用され、次にグローバル認証ポリシーが適用されます。グローバルにバインドされた認証ポリシーをユーザーに受信させる場合は、ポリシーの優先順位を変更します。グローバル認証ポリシーのプライオリティ番号が 1 で、仮想サーバにバインドされた認証ポリシーのプライオリティ番号が 2 の場合、グローバル認証ポリシーが優先されます。たとえば、仮想サーバに 3 つの認証ポリシーをバインドし、各ポリシーの優先順位を設定できます。

ユーザーがプライマリカスケード内のポリシーに対する認証に失敗した場合、またはそのユーザーがプライマリカスケード内のポリシーに対する認証に成功したが、セカンダリカスケード内のポリシーに対する認証に失敗した場合、認証プロセスは停止し、ユーザーはエラーページにリダイレクトされます。

注：複数のポリシーを仮想サーバーまたはグローバルにバインドする場合は、すべての認証ポリシーに一意の優先順位を定義することをお勧めします。

グローバル認証ポリシーの優先順位を設定するには

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］ > ［ポリシー］ > ［認証］の順に展開します。
2. グローバルにバインドされているポリシーを選択し、[アクション] で [グローバルバインディング] をクリックします。
3. [認証グローバルポリシーのバインド/バインド解除] ダイアログボックスの [優先度] で、番号を入力し、[OK] をクリックします。

仮想サーバにバインドされた認証ポリシーの優先順位を変更するには

仮想サーバーにバインドされている認証ポリシーを変更することもできます。

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、仮想サーバーを選択し、[開く] をクリックします。
3. [認証] タブをクリックし、[プライマリ] または [セカンダリ] をクリックします。
4. 認証ポリシーの横の [優先度] に番号を入力し、[OK] をクリックします。

2 要素認証の設定

March 26, 2020

Citrix Gateway は、2 要素認証をサポートしています。通常、Citrix Gateway は、ユーザーの認証時に、構成された認証方法のいずれかを使用してユーザーの認証に成功するとすぐに、認証プロセスを停止します。場合によっては、あるサーバーに対してユーザーを認証する必要がありますが、別のサーバーからグループを抽出する必要があります。たとえば、ネットワークが RADIUS サーバに対してユーザーを認証し、RSA SecurID トークン認証も使用していて、ユーザー・グループがそのサーバに格納されている場合、グループを抽出できるように、そのサーバに対してユーザーを認証する必要がある場合があります。

ユーザーが 2 つの認証タイプを使用して認証され、そのうちの 1 つがクライアント証明書認証の場合、証明書認証ポリシーを 2 番目の認証方法として構成できます。たとえば、プライマリ認証タイプとして LDAP を使用し、セカンダリ認証としてクライアント証明書を使用します。ユーザーは、ユーザー名とパスワードを使用してログオンすると、ネットワークリソースにアクセスできます。

2 要素認証を設定する場合、認証タイプがプライマリまたはセカンダリのどちらであるかを選択します。

2 要素認証を構成するには

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］ > ［ポリシー］ > ［認証］の順に展開します。
2. [ポリシー] タブで、[グローバルバインド] をクリックします。
3. [認証ポリシーをグローバルにバインド/バインド解除] ダイアログボックスで、[プライマリ] をクリックします。
4. [ポリシーの挿入] をクリックします。
5. [ポリシー名] で、認証ポリシーを選択します。
6. [セカンダリ] をクリックし、手順 4 と 5 を繰り返して、[OK] をクリックします。

シングル・サインオンの認証タイプの選択

March 26, 2020

Citrix Gateway でシングルサインオンと 2 要素認証を構成している場合は、シングルサインオンに使用するパスワードを選択できます。たとえば、LDAP がプライマリ認証タイプとして設定され、RADIUS がセカンダリ認証タイプとして設定されているとします。ユーザーがシングルサインオンを必要とするリソースにアクセスすると、デフォルトでユーザー名とプライマリパスワードが送信されます。セッションプロファイル内の Web アプリケーションへのシングルサインオンに使用するパスワードを設定します。

シングルサインオンの認証を構成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウで、[プロファイル] タブをクリックし、次のいずれかの操作を行います。
   - 新しいプロファイルを作成するには、[追加] をクリックします。
   - 既存のプロファイルを修正するには、[開く] をクリックします。
3. [クライアントエクスペリエンス] タブで、[資格情報インデックス] の横にある [グローバルに上書き] をクリックし、[プライマリ] または [セカンダリ] を選択します。
4. これが新しいプロファイルの場合は、[作成] をクリックし、[閉じる] をクリックします。
5. 既存のプロファイルを修正する場合は、[OK] をクリックします。

クライアント証明書および **LDAP 2** 要素認証の設定

March 26, 2020

LDAP でのスマートカード認証を使用するなど、LDAP 認証および承認を伴うセキュアクライアント証明書を使用できます。ユーザーがログオンし、クライアント証明書からユーザー名が抽出されます。クライアント証明書は認証のプライマリ形式で、LDAP はセカンダリ形式です。クライアント証明書の認証は、LDAP 認証ポリシーよりも優先される必要があります。ポリシーの優先順位を設定する場合は、LDAP 認証ポリシーに割り当てる番号よりも小さい番号をクライアント証明書認証ポリシーに割り当てます。

クライアント証明書を使用するには、Windows Server 2008 の証明書サービスなどのエンタープライズ証明機関 (CA) が、Active Directory を実行しているコンピューターで実行されている必要があります。CA を使用してクライアント証明書を作成できます。

LDAP 認証および認可でクライアント証明書を使用するには、SSL (Secure Sockets Layer) を使用するセキュアな証明書である必要があります。LDAP でセキュアなクライアント証明書を使用するには、ユーザーデバイスにクライアント証明書をインストールし、Citrix Gateway に対応するルート証明書をインストールします。

クライアント証明書を設定する前に、次の操作を行います。

- 仮想サーバを作成します。
- LDAP サーバーの LDAP 認証ポリシーを作成します。
- LDAP ポリシーの式を True 値に設定します。

LDAP を使用してクライアント証明書認証を構成するには

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］>［ポリシー］>［認証］の順に展開します。
2. ナビゲーションウィンドウの [認証] で、[証明書] をクリックします。
3. 詳細ウィンドウで、[追加] をクリックします。
4. [名前] に、ポリシーの名前を入力します。
5. [認証の種類] で、[証明書] を選択します。
6. [サーバー] の横にある [新規] をクリックします。
7. [名前] に、サーバーの名前を入力し、[作成] をクリックします。
8. [認証サーバーの作成] ダイアログボックスの [名前] に、サーバーの名前を入力します。
9. [2 係数] の横にある [オン] を選択します。
10. [ユーザー名] フィールドで、[件名:CN] を選択し、[作成] をクリックします。
11. [認証ポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [True value] を選択し、[式の追加] をクリックし、[作成] をクリックして、[閉じる] をクリックします。

証明書認証ポリシーを作成したら、ポリシーを仮想サーバーにバインドします。証明書認証ポリシーをバインドした後、LDAP 認証ポリシーを仮想サーバーにバインドします。

重要: LDAP 認証ポリシーを仮想サーバーにバインドする前に、証明書認証ポリシーを仮想サーバーにバインドする必要があります。

Citrix Gateway にルート証明書をインストールするには

証明書認証ポリシーを作成したら、ルート証明書を CA から Base64 形式でダウンロードしてインストールし、コンピュータに保存します。その後、ルート証明書を Citrix Gateway にアップロードできます。

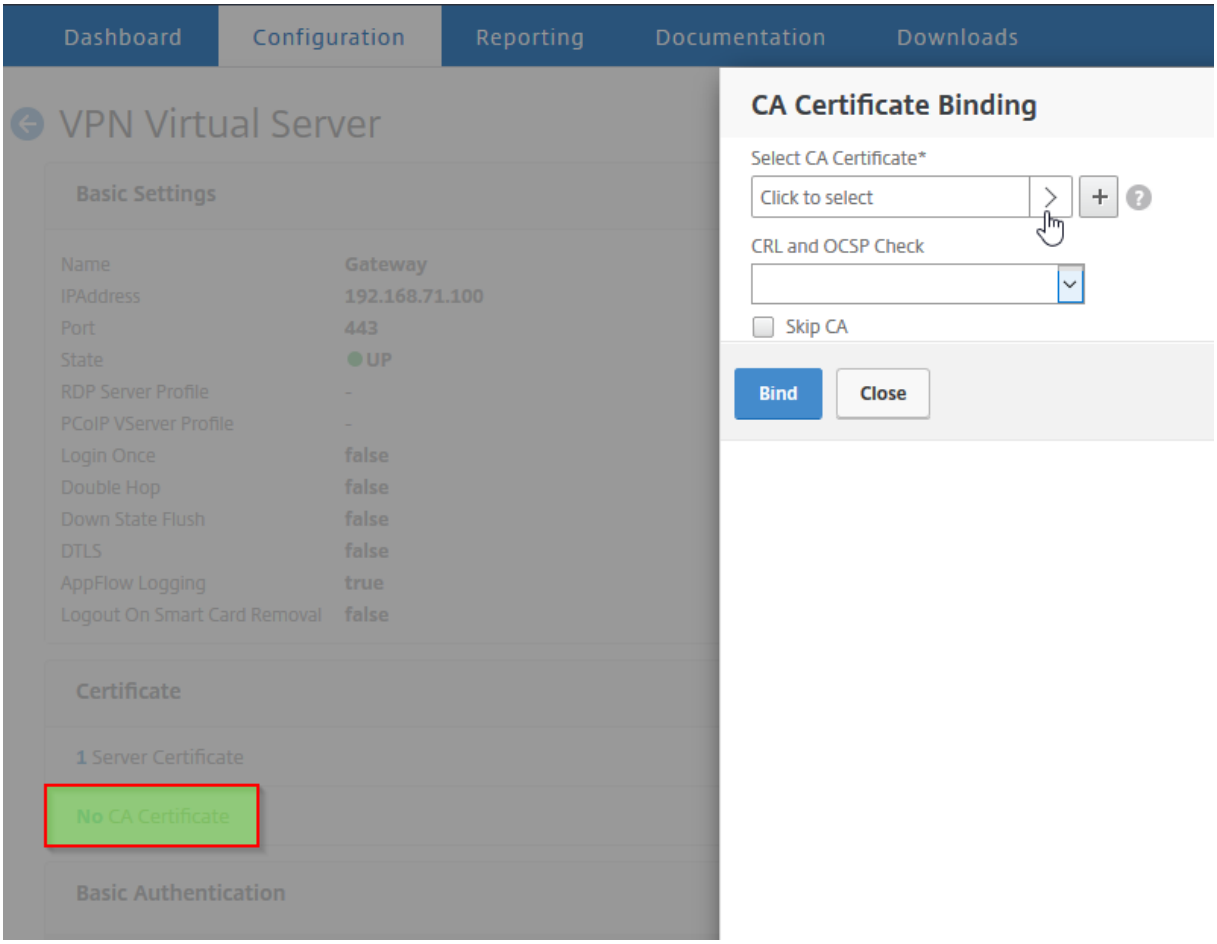
1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[SSL] を展開し、[証明書] をクリックします。
2. 詳細ペインで、［Install］をクリックします。
3. [証明書-キーペア名] に、証明書の名前を入力します。
4.「証明書ファイル名」で「参照」をクリックし、ドロップダウン・ボックスで「アプライアンス」または「ローカル」を選択します。
5. ルート証明書に移動し、[開く]、[インストール] の順にクリックします。

ルート証明書を仮想サーバーに追加するには

Citrix Gateway にルート証明書をインストールしたら、仮想サーバーの証明書ストアに証明書を追加します。

重要: スマートカード認証用にルート証明書を仮想サーバーに追加する場合は、次の図に示すように、**[CA** 証明書の選択] ドロップダウンボックスから証明書を選択する必要があります。

図 1: ルート証明書を CA として追加する



1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、仮想サーバーを選択し、[開く] をクリックします。
3. [証明書] タブの [使用可能] で証明書を選択し、[追加] の横にあるドロップダウンボックスで [CA] をクリックし、[OK] をクリックします。
4. 手順 2 を繰り返します。
5. [証明書] タブで、[SSL パラメーター] をクリックします。
6. [その他] で、[クライアント認証] を選択します。
7. [その他] の [クライアント証明書] の横にある [オプション] を選択し、[OK] を 2 回クリックします。
8. クライアント証明書を構成したら、Citrix Gateway プラグインを使用して Citrix Gateway にログオンして認証をテストします。複数の証明書がインストールされている場合は、正しい証明書を選択するように求める

プロンプトが表示されます。証明書を選択すると、ログオン画面が表示され、証明書から取得した情報が入力されたユーザー名が表示されます。パスワードを入力し、[ログイン] をクリックします。

ログオン画面の [User Name] フィールドに正しいユーザー名が表示されない場合は、LDAP ディレクトリのユーザーアカウントとグループを確認します。Citrix Gateway で定義されているグループは、LDAP ディレクトリ内のグループと同じである必要があります。Active Directory で、ドメインルートレベルでグループを構成します。ドメインルートレベルにない Active Directory グループを作成すると、クライアント証明書の読み取りが不正確になることがあります。

ユーザーとグループがドメインのルートレベルでない場合、Citrix Gateway のログオンページには、Active Directory で構成されているユーザー名が表示されます。たとえば、Active Directory に [ユーザー] というフォルダがあり、証明書には [CN= ユーザー] と表示されます。ログオンページの [ユーザー名] に [ユーザー] と表示されます。

グループとユーザーアカウントをルートドメインレベルに移動しない場合は、Citrix Gateway で証明書認証サーバーを構成するときに、ユーザー名フィールドとグループ名フィールドを空白のままにします。

シングル・サインオンの設定

March 26, 2020

Citrix Gateway は、Windows でのシングルサインオン、Web アプリケーション（SharePoint など）、ファイル共有、Web Interface へのシングル・サインオンをサポートするように構成できます。シングルサインオンは、ユーザーがアクセスインターフェイスのファイル転送ユーティリティまたは通知領域の Citrix Gateway アイコンメニューからアクセスできるファイル共有にも適用されます。

ユーザーがログオンするときにシングル・サインオンを構成すると、ログオン情報をもう一度入力しなくても、自動的に再びログオンします。

Windows でのシングルサインオンの設定

March 26, 2020

ユーザーは、デスクトップから Citrix Gateway プラグインを起動して接続を開きます。ユーザーが Windows にログオンしたときに Citrix Gateway プラグインが自動的に起動するように指定するには、シングルサインオンを有効にします。シングルサインオンを構成すると、ユーザーの Windows ログオン資格情報が Citrix Gateway に渡され、認証が行われます。Citrix Gateway プラグインのシングルサインオンを有効にすると、インストールスクリプトや自動ドライブマッピングなどのユーザーデバイスでの操作が容易になります。

ユーザーデバイスが組織のドメインにログオンしている場合にのみ、シングルサインオンを有効にします。シングルサインオンが有効で、ドメインにないデバイスからユーザーが接続している場合、ユーザーはログオンするように求められます。

シングルサインオンを Windows でグローバルに構成するか、セッションポリシーにアタッチされたセッションプロファイルを使用して構成します。

Windows でシングルサインオンをグローバルに設定するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [クライアントエクスペリエンス] タブで、[Windows でのシングルサインオン] をクリックし、[OK] をクリックします。

セッションポリシーを使用して **Windows** でシングルサインオンを構成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. [クライアントエクスペリエンス] タブで、[Windows でのシングルサインオン] の横にある [グローバルに上書き]、[Windows でのシングルサインオン]、[OK] の順にクリックします。
7. [セッションポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [全般]、[True value]、[式の追加]、[作成]、[閉じる] の順にクリックします。

Web アプリケーションへのシングル・サインオンの構成

March 26, 2020

Web ベース認証を使用する内部ネットワーク内のサーバーにシングルサインオンを提供するように Citrix Gateway を構成できます。シングルサインオンを使用すると、SharePoint サイトや Web Interface などのカスタムホームページにユーザーをリダイレクトできます。また、Citrix Gateway プラグインを使用して、ホームページで構成されたブックマークまたはユーザーが Web ブラウザで入力した Web アドレスからリソースへのシングルサインオンを構成することもできます。

ホームページを SharePoint サイトまたは Web Interface にリダイレクトする場合は、サイトの Web アドレスを指定します。Citrix Gateway または外部認証サーバーによってユーザーが認証されると、ユーザーは指定されたホームページにリダイレクトされます。ユーザクレデンシャルは、Web サーバに透過的に渡されます。Web サーバーが資格情報を受け入れると、ユーザーは自動的にログオンします。Web サーバがクレデンシャルを拒否すると、ユーザ名とパスワードを要求する認証プロンプトが表示されます。

Web アプリケーションへのシングルサインオンは、グローバルに構成することも、セッションポリシーを使用して構成することもできます。

Web アプリケーションへのシングルサインオンをグローバルに設定するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [クライアントエクスペリエンス] タブで、[Web アプリケーションへのシングルサインオン] をクリックし、[OK] をクリックします。

セッションポリシーを使用して Web アプリケーションへのシングルサインオンを構成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ペインの [ポリシー] タブでセッションポリシーを選択し、[開く] をクリックします。
3. [セッションポリシーの構成] ダイアログボックスで、[要求プロファイル] の横にある [変更] をクリックします。
4. [クライアントエクスペリエンス] タブで、[Web アプリケーションへのシングルサインオン] の横にある [グローバル上書き]、[Web アプリケーションへのシングルサインオン]、[OK] の順にクリックします。

Web アプリケーションへのシングルサインオン用の HTTP ポートを定義するには

シングルサインオンは、宛先ポートが HTTP ポートと見なされるネットワークトラフィックに対してのみ試行されます。HTTP トラフィックにポート 80 以外のポートを使用するアプリケーションへのシングルサインオンを許可するには、Citrix Gateway で 1 つ以上のポート番号を追加します。複数のポートを有効にできます。ポートはグローバルに設定されます。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [ネットワークの構成] タブで、[詳細設定] をクリックします。
4. [HTTP ポート] にポート番号を入力し、[追加] をクリックし、[OK] を 2 回クリックします。

   追加するポートごとにステップ 4 を繰り返すことができます。

注：内部ネットワーク内の Web アプリケーションがパブリック IP アドレスを使用している場合、シングルサインオンは機能しません。シングルサインオンを有効にするには、クライアントレスアクセスまたは Citrix Gateway プラグインがユーザーデバイス接続に使用されるかどうかに関係なく、グローバルポリシー設定の一部として分割トンネリングを有効にする必要があります。グローバルレベルで分割トンネリングを有効にできない場合は、プライベートアドレス範囲を使用する仮想サーバを作成します。

LDAP を使用した **Web** アプリケーションへのシングル・サインオンの構成

March 26, 2020

シングルサインオンを構成し、ユーザープリンシパル名 (UPN) を使用して username@domain.com の形式でログオンすると、既定ではシングルサインオンが失敗し、ユーザーは認証を 2 回行う必要があります。ユーザーログオンにこの形式を使用する必要がある場合は、LDAP 認証ポリシーを変更して、この形式のユーザー名を受け入れるようにします。

Web アプリケーションへのシングルサインオンを構成するには

1. 構成ユーティリティの［構成］タブで、［**Citrix Gateway**］**>**［ポリシー］**>**［認証］の順に展開します。
2. 詳細ペインの [ポリシー] タブで、LDAP ポリシーを選択し、[開く] をクリックします。
3. [認証ポリシーの構成] ダイアログボックスで、[サーバー] の横にある [変更] をクリックします。
4. [接続の設定**]** の [ベース DN (ユーザーの場所)] に「DC= ドメイン名, DC=com」と入力します。
5. [管理者バインド **DN**] に「LDAPaccount@domainname.com」と入力します。ドメイン名.com はドメインの名前です。
6. [管理者パスワード**]** と [管理者パスワードの確認] に、パスワードを入力します。
7. [その他の設定**]** の [サーバーログオン名の属性] に「UserPrincipalName」と入力します。
8. [グループ属性**]** に memberOf と入力します。
9.「サブ属性名」に「CN」と入力します。
10. [**SSO** 名の属性**]** に、ユーザーがログオンする形式を入力し、[**OK**] を 2 回クリックします。この値は、[アカウント名] または [ユーザープリンシパル名] のいずれかです。

ドメインへのシングル・サインオンの設定

April 9, 2020

ユーザーが Citrix Virtual Apps を実行しているサーバーに接続し、SmartAccess を使用している場合は、サーバーファームに接続するユーザーのシングルサインオンを構成できます。セッションポリシーとプロファイルを使用して公開アプリケーションへのアクセスを構成する場合は、サーバーファームのドメイン名を使用します。

また、ネットワーク内のファイル共有にシングルサインオンを構成することもできます。

ドメインへのシングルサインオンを構成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ペインの [ポリシー] タブでセッションポリシーを選択し、[開く] をクリックします。

3. [セッションポリシーの構成] ダイアログボックスで、[要求プロファイル] の横にある [変更] をクリックします。
4. [セッションプロファイルの構成] ダイアログボックスの [公開アプリケーション] タブの [シングルサインオンドメイン] で [グローバル上書き] をクリックし、ドメイン名を入力して [OK] を 2 回クリックします。

Citrix Virtual Apps で機能する Citrix Gateway 構成について詳しくは、「Citrix Gateway と Citrix Virtual Apps and Desktops の統合」を参照してください。

Microsoft Exchange 2010 でシングルサインを構成する

March 26, 2020

以下のセクションでは、Citrix Gateway での Microsoft Exchange 2010 のシングルサインオン（SSO）の構成について説明します。Outlook Web アクセス (OWA) 2010 の SSO は、次の条件では動作しません。

- Microsoft Exchange 2010 でフォームベースの認証を使用します。
- 認証、認可、および監査トラフィック管理ポリシーを使用した仮想サーバのロードバランシング。

> 注
>
> この設定は、認証、認可、および監査トラフィック管理ポリシーを持つロードバランシング仮想サーバに対してだけ機能します。クライアントレス VPN を使用した OWA 2010 の SSO では機能しません。

次の手順は、Citrix Gateway で Microsoft Exchange 2010 の SSO を構成する前に考慮する必要がある前提条件です。

- SSO フォームのアクション URL は、OWA 2010 では異なります。トラフィック管理ポリシーを変更する必要があります。
- logon.aspx 要求で PBack クッキーを設定するには、書き換えポリシーが必要です。通常のシナリオでは、クライアントで PBack クッキーを設定し、[送信] をクリックします。
- SSO を使用している場合、logon.aspx への応答が消費され、Citrix Gateway がフォーム要求を生成します。クッキーは、フォーム送信要求に添付されていません。
- OWA サーバーは、フォーム送信要求で PBack クッキーを期待します。書き換えポリシーは、フォーム送信要求に PBack クッキーをアタッチするために必要です。

CLI を使用して、次の操作を実行します

1. 認証、認可、および監査トラフィック管理の設定

```
add tm formSSOAction OWA_Form_SSO_SSOPro -actionURL "/owa/auth.owa
"-userField username -passwdField password -ssoSuccessRule "http.
RES.SET_COOKIE.COOKIE(\"cadata\").VALUE(\"cadata\").LENGTH.GT(70"-
responsesize 15000 -submitMethod POST
```


2. トラフィック管理ポリシーを設定し、ポリシーをバインドする

   - `add tm trafficAction OWA_2010_Prof -appTimeout 1 -SSO ON -formSSO Action OWA_Form_SSO_SSOPro`
   - `add tm trafficPolicy owa2k10_pol "HTTP.REQ.URL.CONTAINS(\"owa/auth/logon.aspx\")"OWA_2010_Prof`
   - `bind tm global -policyName owa2k10_pol -priority 100`

CLI を使用した設定の書き換え

コマンドプロンプトで、次のように入力します。

- `add rewrite action set_pback_cookie insert_after "http.REQ.COOKIE.VALUE(\"OutlookSession\")""\";PBack=0\""-bypassSafetyCheck YES`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")"set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

代替書き換え構成

まれに、Microsoft Outlook が OWA セッションクッキーを発行しない可能性があり、Pback クッキーも挿入されないことがあります。この問題は、上記のコマンドを実行して書き換え構成を実装した後に発生する可能性があります。

このようなシナリオを克服し、回避策として、書き換え設定の代わりに次のコマンドを設定できます。

コマンドプロンプトで、次のように入力します。

- `add rewrite action set_pback_cookie insert_http_header "Cookie"'"PBack=0"'`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")"set_pback_cookie`
- `set rewrite policy set_pback_cookie -action set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

ワンタイムパスワードの使用の設定

April 9, 2020

トークン暗証番号（PIN）やパスコードなどのワンタイムパスワードを使用するように Citrix Gateway を構成できます。ユーザーがパスコードまたは PIN を入力すると、認証サーバーはただちにワンタイムパスワードを無効にし、ユーザーは同じ PIN またはパスワードを再入力できません。

ワンタイムパスワードを使用する製品には、次のものがあります。

- RSA SecurID
- Imprivata OneSign
- SafeWord
- Gemalto Protiva
- Nordic SMS PASSCODE

これらの各製品を使用するには、内部ネットワークの認証サーバを RADIUS を使用するように設定します。詳しくは、「RADIUS 認証の構成」を参照してください。

たとえば、RSA SecurID トークンによって提供される RADIUS でワンタイムパスワードを使用するように Citrix Gateway ateway で認証を構成すると、Citrix Gateway はキャッシュされたパスワードを使用してユーザーの再認証を試みます。この再認証は、Citrix Gateway に変更を加えた場合、または Citrix Gateway プラグインと Citrix Gateway の間の接続が中断されてから復元された場合に発生します。

Citrix Workspace アプリを使用するように接続を構成し、ユーザーが RADIUS または LDAP を使用して Web Interface に接続する場合にも再認証が試行されます。ユーザーがアプリケーションを起動してアプリケーションを使用し、Receiver に戻って別のアプリケーションを起動すると、Citrix Gateway はキャッシュされた情報を使用してユーザーを認証します。

RSA セキュリティ **ID** 認証の設定

April 9, 2020

RSA/ACE サーバを RSA SecureID 認証用に構成する場合は、次の手順を実行する必要があります。

次の情報を使用して RADIUS クライアントを設定します。

- Citrix Gateway アプライアンスの名前を入力します。
- 説明を入力します (必須ではありません)。
- システムの IP アドレスを指定します。
- Citrix Gateway と RADIUS サーバー間の共有シークレットを指定します。
- メーカー/モデルを標準 RADIUS として設定します。

エージェント・ホスト構成では、次の情報が必要です。

- Citrix Gateway の完全修飾ドメイン名（FQDN）を指定します（仮想サーバーにバインドされた証明書に表示されます）。FQDN を指定した後、Tab キーをクリックすると、[ネットワークアドレス] ウィンドウが自動的に表示されます。

FQDN を入力すると、ネットワークアドレスが自動的に表示されます。表示されない場合は、システムの IP アドレスを入力します。

- コミュニケーションサーバを使用して、エージェントタイプを指定します。
- すべてのユーザーまたは Citrix Gateway 経由の認証を許可されたユーザーのセットをインポートするように構成します。

RADIUS サーバのエージェントホストエントリをまだ設定していない場合は、次の情報を含めて作成します。

- RSA サーバの FQDN を指定します。

  FQDN を入力すると、ネットワークアドレスが自動的に表示されます。そうでない場合は、RSA サーバの IP アドレスを入力します。

- エージェントタイプ（RADIUS サーバ）を指定します。

RSA RADIUS サーバの構成の詳細については、製造元のマニュアルを参照してください。

RSA SecurID を構成するには、認証プロファイルとポリシーを作成し、ポリシーをグローバルにバインドするか、仮想サーバにバインドします。RSA SecurID を使用するための RADIUS ポリシーを作成するには、RADIUS 認証の構成を参照してください。

認証ポリシーを作成したら、仮想サーバーまたはグローバルにバインドします。詳しくは、「認証ポリシーのバインド」を参照してください。

RADIUS を使用したパスワードリターンの設定

March 26, 2020

ドメインパスワードは、トークンが RADIUS サーバから生成したワンタイムパスワードに置き換えることができます。ユーザーが Citrix Gateway にログオンすると、トークンから個人識別番号（PIN）とパスコードを入力します。Citrix Gateway が認証情報を検証すると、RADIUS サーバーはユーザーの Windows パスワードを Citrix Gateway に返します。Citrix Gateway はサーバーからの応答を受け入れ、ログオン中にユーザーが入力したパスコードを使用する代わりに、返されたパスワードを使用してシングルサインオンします。RADIUS によるこのパスワード返却機能を使用すると、ユーザーが Windows パスワードを呼び戻す必要なく、シングル・サインオンを構成できます。

ユーザーがパスワードリターンを使用してログオンすると、Citrix Endpoint Management、StoreFront、Web Interface など、内部ネットワークで許可されているすべてのネットワークリソースにアクセスできます。

返されたパスワードを使用してシングルサインオンを有効にするには、Citrix Gateway で「パスワードベンダー識別子」および「パスワード属性の種類」パラメーターを使用して、RADIUS 認証ポリシーを構成します。これらの 2 つのパラメータは、ユーザーの Windows パスワードを Citrix Gateway に返します。

Citrix Gateway は、Imprivata ワンサインをサポートしています. Imprivata OneSign の最低限必要なバージョンは、サービスパック 3 で 4.0 です。Imprivata OneSign の既定のパスワードベンダーの識別子は 398 です。Imprivata OneSign の既定のパスワード属性の種類のコードは 5 です。

RSA、Cisco、Microsoft など、他の RADIUS サーバを使用してパスワードを返すことができます。ベンダー固有のアトリビュート値のペアでユーザシングルサインオンパスワードを返すように RADIUS サーバを設定する必要があります。Citrix Gateway 認証ポリシーでは、これらのサーバーの「パスワードベンダー識別子」および「パスワード属性の種類」パラメーターを追加する必要があります。

ベンダー ID の完全なリストは、インターネット割り当て番号局 (IANA) のウェブサイトを参照してください。たとえば、RSA セキュリティのベンダー識別子は 2197、Microsoft の場合は 311、Cisco Systems の場合は 9 です。ベンダーがサポートするベンダー固有の属性は、ベンダーに確認する必要があります。たとえば、Microsoft では、ベンダー固有の属性の一覧をMicrosoft のベンダー固有の RADIUS アトリビュートに公開しています。

ベンダー固有の属性を選択して、ベンダーの RADIUS サーバ上のユーザーのシングル・サインオン・パスワードを格納できます。RADIUS サーバー上にユーザーパスワードが保存されているベンダー識別子と属性を使用して Citrix Gateway を構成すると、RADIUS サーバーに送信されるアクセス要求パケット内の属性の値が要求されます。RADIUS サーバが access-accept パケット内の対応するアトリビュートと値のペアで応答した場合、使用する RADIUS サーバに関係なく、パスワードのリターンが機能します。

返されたパスワードを使用してシングル・サインオンを構成するには、次の手順に従います。

1. 構成ユーティリティの［構成］タブで、［Citrix Gateway］ > ［ポリシー］ > ［認証］の順に展開します。
2. ナビゲーションペインで、[RADIUS] をクリックします。
3. 詳細ウィンドウで、[追加] をクリックします。
4. [認証ポリシーの作成] ダイアログボックスの [名前] に、ポリシーの名前を入力します。
5. [サーバー] の横にある [新規] をクリックします。
6. [名前] に、サーバーの名前を入力します。
7. RADIUS サーバの設定を構成します。
8. [パスワードベンダー識別子] に、RADIUS サーバーによって返されるベンダー識別子を入力します。この識別子の最小値は 1 である必要があります。
9. [パスワード属性の種類] で、ベンダー固有の AVP コードに RADIUS サーバから返される属性の種類を入力します。値の範囲は 1 ～255 です。
10. [認証ポリシーの作成] ダイアログボックスで、[名前付き式] の横にある式を選択し、[式の追加]、[作成]、[閉じる] の順にクリックします。

Configuring SafeWord Authentication

March 26, 2020

SafeWord 製品ラインは、トークンベースのパスコードを使用して安全な認証を提供するのに役立ちます。ユーザーがパスコードを入力すると、SafeWord によって即座に無効になり、再度使用できなくなります。

Secure Gateway Gateway および Web Interface 展開で Secure Gateway を置き換える場合は、Access Gateway で認証を構成せず、Web Interface で受信 HTTP トラフィックに対して SafeWord 認証を提供し続けることができます。

Access Gateway は、次の製品の SafeWord 認証をサポートしています。

- SafeWord 2008
- SafeWord PremierAccess
- SafeWord for Citrix
- SafeWord RemoteAccess

SafeWord 製品を使用して認証するように Access Gateway を構成するには、次の方法があります。

- SafeWord PremierAccess の一部としてインストールされている RADIUS サーバーを使用するように認証を設定し、認証を処理できるようにします。
- セーフワードリモートアクセス、Citrix 用セーフワードおよびプレミアアクセス 4.0 のコンポーネントであるセーフワード IAS エージェントを使用するように認証を構成します。
- Citrix Web Interface を使用するには、SafeWord Web Interface エージェントをインストールします。認証は Access Gateway 上で構成する必要はなく、Citrix Web Interface で処理できます。この構成では、プレミアアクセス RADIUS サーバーまたはセーフワード IAS エージェントは使用されません。

SafeWord RADIUS サーバを設定する場合は、次の情報が必要です。

- Access Gateway の IP アドレス。RADIUS サーバーでクライアント設定を構成する場合は、Access Gateway の IP アドレスを使用します。
- 共有シークレット。
- SafeWord サーバーの IP アドレスとポート。

Gemalto Protiva 認証の設定

March 26, 2020

Protiva は Gemalto のスマートカード認証の強みを利用するために開発された強力な認証プラットフォームです。Protiva では、ユーザーは Protiva デバイスによって生成されたユーザー名、パスワード、ワンタイムパスワードでログオンします。RSA SecurID と同様に、認証要求は Protiva 認証サーバーに送信され、パスワードは検証または拒否されます。

Gemalto Protiva を Citrix Gateway と連携するように構成するには、以下のガイドラインに従ってください。

- Protiva サーバーをインストールします。
- Microsoft IAS RADIUS サーバーに Protiva インターネット認証サーバー (IAS) エージェントプラグインをインストールします。IAS サーバーの IP アドレスとポート番号を書き留めておいてください。

Gateway 認証の nFactor

October 22, 2021

はじめに

nFactor 認証は、認証に関するまったく新しい可能性セットを可能にします。nFactor を使用する管理者は、仮想サーバーの認証要素を構成するときに、認証、承認、および監査の柔軟性を享受できます。

2 つのポリシーバンクまたは 2 つの要因によって、管理者が制限されなくなりました。政策銀行の数は、さまざまなニーズに合わせて拡張することができます。前述の要因に基づいて、nFactor は認証方法を決定します。動的ログインフォームと失敗時のアクションは、nFactor を使用して可能です。

> 注： nFactor は、Citrix ADC スタンダードエディションではサポートされていません。これは、Citrix ADC アドバンストエディションと Citrix ADC プレミアムエディションでサポートされています。

ユースケース

nFactor 認証は、ユーザプロファイルに基づくダイナミック認証フローを有効にします。場合によっては、これらはユーザーにとって直感的な単純なフローになることがあります。それ以外の場合は、アクティブディレクトリやその他の認証サーバーのセキュリティ保護と組み合わせることができます。Gateway に固有の要件をいくつか次に示します。

1. 動的なユーザ名とパスワードの選択。従来、Citrix クライアント（ブラウザと Receiver を含む）では、最初のパスワードフィールドとしてアクティブディレクトリ（AD）パスワードが使用されていました。2 番目のパスワードは、ワンタイムパスワード (OTP) 用に予約されています。ただし、AD サーバーを保護するには、OTP を最初に検証する必要があります。nFactor は、クライアントの変更を必要とせずにこれを行うことができます。
2. マルチテナント認証エンドポイント。組織によっては、証明書ユーザーおよび証明書以外のユーザーに対して異なる Gateway サーバーを使用します。ユーザーが自分のデバイスを使用してログインする場合、ユーザーのアクセスレベルは、使用するデバイスに応じて Citrix ADC によって異なります。Gateway は、さまざまな認証ニーズに対応できます。
3. グループメンバーシップに基づく認証。一部の組織では、認証要件を決定するために AD サーバーからユーザープロパティを取得します。認証要件は、ユーザーごとに変更することができます。
4. 認証のコファクタです。場合によっては、異なるユーザーセットを認証するために、異なる認証ポリシーのペアが使用されることがあります。ペアポリシーを指定すると、有効な認証が向上します。依存ポリシーは、1 つのフローから作成できます。このようにして、独立した一連のポリシーが独自のフローになり、効率性が向上し、複雑さが軽減されます。

認証応答の処理

Citrix Gateway のコールバック登録は、認証応答を処理します。AAAD（認証デーモン）応答と成功/失敗/エラー/ダイアログコードは、コールバックハンドルに送られます。成功/失敗/エラー/ダイアログコードは、Gateway が適切なアクションを実行するように指示します。

クライアントのサポート

次の表に、構成の詳細を示します。

クライアント	nFactor サポート	認証ポリシーのバインドポイント	EPA
Web ブラウザー	はい	認証	はい
Citrix Workspace アプリ	いいえ	VPN	×
Gateway プラグイン	いいえ	VPN	はい

コマンドライン設定

Gateway 仮想サーバには、属性として指定された認証仮想サーバが必要です。これは、このモデルに必要な唯一の構成です。

```
1 add authnProfile <name-of-profile> -authnVsName <name-of-auth-vserver>
2 <!--NeedCopy-->
```

authnVsName は、認証仮想サーバーの名前です。この仮想サーバーは、高度な認証ポリシーで構成する必要があり、nFactor 認証に使用されます。

```
1 add vpn vserver <name> <serviceType> <IP> <PORT> -authnProfile <name-of
     -profile>
2 set vpn vserver <name> -authnProfile <name-of-profile>
3 <!--NeedCopy-->
```

ここで、authnProfile は以前に作成された認証プロファイルです。

相互運用に関する課題

レガシー Gateway クライアントのほとんどは、rfWeb クライアントに加えて、Gateway から送信された応答に基づいてモデル化されています。たとえば、/vpn/index.html に対する 302 応答は、多くのクライアントで期待されます。また、これらのクライアントは、「pwcount」、「NSC_CERT」などのさまざまな Gateway クッキーに依存しています。

エンドポイント分析（**EPA**）

認証、認可、および監査サブシステムは nFactor の EPA をサポートしていないため、Gateway 仮想サーバが EPA を実行します。EPA の後、ログイン資格情報は、前述の API を使用して認証仮想サーバーに送信されます。認証が完了すると、Gateway は認証後のプロセスを続行し、ユーザセッションを確立します。

設定ミスに関する考慮事項

Gateway クライアントは、ユーザーの資格情報を一度だけ送信します。Gateway は、ログイン要求とともにクライアントから 1 つまたは 2 つのクレデンシャルを取得します。レガシーモードでは、最大 2 つの要素があります。取得したパスワードは、これらの要因に使用されます。ただし、nFactor では、構成できるファクタの数は実質的に無制限です。Gateway クライアントから取得したパスワードは、設定された要素に対して（設定に従って）再利用されます。ワンタイムパスワード (OTP) を複数回再利用しないように注意する必要があります。同様に、管理者は、ある要素で再利用されたパスワードが実際にその要素に適用可能であることを確認する必要があります。

Citrix クライアントの定義

この構成オプションは、Citrix ADC がブラウザクライアントと Receiver などのシッククライアントを判断する際に役立ちます。

管理者は、パターンセット ns_vpn_client_userAgents が提供され、すべての Citrix クライアントのパターンを構成できます。

同様に、「Citrix Receiver」文字列を上記のパッチセットにバインドして、ユーザーエージェントに「Citrix Receiver」を持つすべての Citrix クライアントを無視します。

Gateway の **nFactor** の制限

次の条件が存在する場合、Gateway 認証の nFactor は発生しません。

1. 認証プロファイルは、Citrix Gateway で設定されていません。
2. 高度な認証ポリシーは、認証仮想サーバーにバインドされず、同じ認証仮想サーバーが authnProfile に記載されています。
3. HTTP リクエスト内のユーザーエージェント文字列は、パッチセット ns_vpn_client_useragents で構成されたユーザーエージェントと一致します。

これらの条件が満たされない場合、Gateway にバインドされた従来の認証ポリシーが使用されます。

ユーザーエージェントまたはその一部が前述のパッチセットにバインドされている場合、それらのユーザーエージェントからのリクエストは nFactor フローに参加しません。たとえば、以下のコマンドは、すべてのブラウザの設定を制限します（すべてのブラウザがユーザーエージェント文字列に「Mozilla」が含まれていると仮定します）。

```
bind patset ns_vpn_client_useragents Mozilla
```


LoginSchema

LoginSchema は、ログオンフォームを論理的に表現したものです。XML 言語によって定義されています。loginSchema の構文は、Citrix の共通フォームプロトコル仕様に準拠しています。

LoginSchema は、製品の「ビュー」を定義します。管理者は、フォームのカスタマイズした説明、補助テキストなどを提供できます。これには、フォーム自体のラベルが含まれます。お客様は、特定の時点で提示されたフォームを説明する成功/失敗メッセージを提供できます。

ログインスキーマと **nFactor** の知識が必要です

事前に構築されたログインスキーマファイルは、以下の Citrix ADC の場所/nsconfig/nsconfig/loginschema/LoginSchema/にあります。これらの事前構築された loginSchema ファイルは、一般的なユースケースに対応し、必要に応じて若干のバリエーションに合わせて変更できます。

また、カスタマイズが少ないほとんどの単一要素ユースケースでは、loginSchema (s) 設定は必要ありません。

管理者は、Citrix ADC が要因を検出できるようにする追加の構成オプションについて、ドキュメントを確認することをお勧めします。ユーザーがクレデンシャルを送信すると、管理者は複数のファクタを構成して、認証ファクタを柔軟に選択して処理できます。

LoginSchema を使用しない二要素認証の設定

Citrix ADC は、構成に基づいて二重要素要件を自動的に決定します。ユーザーがこれらの資格情報を提示すると、管理者は仮想サーバーでポリシーの最初のセットを構成できます。各ポリシーに対して、「nextFactor」を「パススルー」として構成できます。「パススルー」とは、Citrix ADC が既存の資格情報を使用してログオンを処理する必要があることを意味します。「パススルー」要素を使用することで、管理者はプログラムで認証フローを駆動できます。詳細については、nFactor 仕様または導入ガイドを参照することをお勧めします。「多要素 (nFactor) 認証」を参照してください。

ユーザー名のパスワードの式

ログイン資格情報を処理するには、管理者は loginSchema を設定する必要があります。loginSchema のカスタマイズが少ない単一ファクタまたは二重ファクタの使用例では、指定された XML 定義は必要ありません。LoginSchema には、ユーザーが提示するユーザー名/パスワードを変更するために使用することができ、このような userExpression と passwdExpression などの他のプロパティがあります。これらは高度なポリシー式であり、ユーザー入力を上書きするために使用することもできます。

nFactor 構成における高レベルの手順

次の図は、nFactor 構成に関連する高レベルの手順を示しています。

GUI の設定

ここでは、次のトピックについて説明します。

- 仮想サーバーの作成
- 認証仮想サーバーの作成
- 認証 CERT プロファイルの作成
- 認証ポリシーの作成
- LDAP 認証サーバーの追加
- LDAP 認証ポリシーの追加
- Radius 認証サーバーを追加する
- Radius 認証ポリシーの追加
- 認証ログインスキーマの作成
- ポリシーラベルの作成

仮想サーバーの作成

1. **Citrix Gateway->** 仮想サーバーに移動します。
2. [追加] ボタンをクリックして、負荷分散仮想サーバーを作成します。

3. 次の情報を入力します。

パラメーター名	パラメータの説明
仮想サーバの名前を入力します。	Citrix Gateway 仮想サーバーの名前。ASCII アルファベットまたはアンダースコア (_) 文字で始まり、ASCII 英数字、アンダースコア、ハッシュ (#)、ピリオド (.)、スペース、コロン (:)、アットマーク (@)、等しい (=)、およびハイフン (-) 文字のみを含める必要があります。仮想サーバの作成後に変更できます。次の要件は、Citrix ADC CLI にのみ適用されます。名前に 1 つ以上のスペースが含まれる場合は、名前を二重引用符または一重引用符で囲みます（「my server」や「my server」など）。
仮想サーバの IP アドレスタイプを入力します。	ドロップダウンメニューから [IP アドレス] または [アドレス指定不可] オプションを選択します。
仮想サーバの IP アドレスを入力します。	インターネットプロトコルアドレス (IP アドレス) は、通信にインターネットプロトコルを使用するコンピュータネットワークに参加している各デバイスに割り当てられる数値ラベルです。
仮想サーバのポート番号を入力します。	ポート番号を入力します。
認証プロファイルを入力します。	仮想サーバー上の認証プロファイルエンティティ。このエンティティを使用して、多要素（nFactor）認証のための認証、承認、および監査仮想サーバーに認証をオフロードできます。
RDP サーバープロファイルを入力します。	仮想サーバーに関連付けられている RDP サーバープロファイルの名前。
「最大ユーザー数」を入力します。	この仮想サーバで許可される同時ユーザー・セッションの最大数。この仮想サーバーにログオンできる実際のユーザー数は、ユーザーライセンスの合計数によって異なります。
最大ログイン試行回数を入力します。	ログオンの最大試行回数。
ログイン失敗タイムアウトを入力します。	ユーザーが最大許容試行回数を超えた場合に、アカウントがロックされる時間（分）。
Windows EPA プラグインのアップグレードを入力します。	Win のプラグインのアップグレード動作を設定するオプション。
Linux EPA プラグインのアップグレードに入ります。	Linux のプラグインのアップグレード動作を設定するオプション。

パラメーター名	パラメータの説明
MAC EPA プラグインのアップグレードに入る	Mac のプラグインのアップグレード動作を設定するオプション。
1 回ログイン	このオプションは、この仮想サーバーのシームレスな SSO を有効/無効にします。
ICA のみ	ON に設定すると、ユーザーが Citrix Workspace アプリまたはブラウザーを使用してログオンし、Wihome パラメーターで指定された Citrix Virtual Apps and Desktops 環境で構成された公開アプリにアクセスできる、基本モードを意味します。ユーザーは Citrix Gateway プラグインを使用して接続できず、エンドポイントスキャンを構成できません。ログインしてアプリにアクセスできるユーザーの数は、このモードでのライセンスによって制限されません。-OFF に設定すると、ユーザーが Citrix Workspace アプリ、ブラウザー、または Citrix Gateway プラグインを使用してログオンできる SmartAccess モードを意味します。管理者は、エンドポイントスキャンをクライアントシステムで実行するように設定し、その結果を使用して公開アプリケーションへのアクセスを制御できます。このモードでは、クライアントは他のクライアントモード（VPN および CVPN）で Gateway に接続できます。ログインしてリソースにアクセスできるユーザの数は、このモードの CCU ライセンスによって制限されます。
認証の有効化	Citrix Gateway に接続するユーザーの認証を要求します。
ダブルホップ	Citrix Gateway アプライアンスをダブルホップ構成で使用します。ダブルホップ展開では、3 つのファイアウォールを使用して DMZ を 2 つのステージに分割することにより、内部ネットワークのセキュリティをさらに強化できます。このような展開では、DMZ に 1 つのアプライアンス、セキュアネットワークに 1 つのアプライアンスを持つことができます。

パラメーター名	パラメータの説明
ダウン状態フラッシュ	仮想サーバーが [DOWN] とマークされている場合は、既存の接続を閉じます。これは、サーバーがタイムアウトした可能性があることを意味します。既存の接続を切断すると、リソースが解放され、場合によっては負荷分散セットアップの回復が高速化されます。[DOWN] とマークされている場合、接続を安全に閉じることができるサーバーでは、この設定を有効にします。トランザクションを完了する必要があるサーバーでは、DOWN 状態フラッシュを有効にしないでください。
DTLS	このオプションは、仮想サーバー上のターンサービスを開始/停止します。
AppFlow ログ	標準の NetFlow または IPFIX 情報（フローの開始と終了のタイムスタンプ、パケットカウント、バイトカウントなど）を含む AppFlow レコードをログに記録します。また、HTTP Web アドレス、HTTP 要求メソッドと応答ステータスコード、サーバーの応答時間、待機時間など、アプリケーションレベルの情報を含むレコードもログに記録します。
ICA プロキシセッションの移行	このオプションは、ユーザーが別のデバイスからログオンしたときに、既存の ICA プロキシセッションを転送するかどうかを決定します。
状態	仮想サーバーの現在の状態 (UP、DOWN、BUSY など)。
デバイス証明書の有効化	EPA の一部としてデバイス証明書チェックがオンかオフかを示します。

4. ページの「サーバー証明書なし」セクションを選択します。
5. [>] をクリックして、サーバー証明書を選択します。
6. SSL 証明書を選択し、[選択] ボタンをクリックします。
7. [バインド] をクリックします。
8. 「使用可能な暗号がありません」という警告が表示された場合は、[**OK**] をクリックします。
9. [続行] ボタンをクリックします。
10. [認証] セクションで、右上の [**+**] アイコンをクリックします。

認証仮想サーバーの作成

1. [セキュリティ**]-> [Citrix ADC AAA]-[**アプリケーショントラフィック**]-[**仮想サーバー**]** に移動します。
2. [追加] をクリックします。
3. 認証仮想サーバーを作成するには、次の基本設定を行います。

   注意**:** 必須フィールドは、設定名の右側に * で示されます。

   a) 新しい認証仮想サーバ の名前を入力します。

   b) **IP** アドレスのタイプを入力します。[IP アドレスの種類] は、[アドレス指定不可] として構成できます。

   c) **IP** アドレスを入力します。IP アドレスはゼロにできます。

   d) 認証仮想サーバの プロトコルの種類を入力します。

   e) 仮想サーバが接続を受け入れる **TCP** ポートを入力します。

   f) 認証仮想サーバによって設定された認証クッキーの ** ドメイン ** を入力します。
4. [**OK**] をクリックします。
5. [サーバー証明書なし] をクリックします。
6. リストから目的のサーバー証明書を選択します。
7. 目的の SSL 証明書を選択し、[**Select**] ボタンをクリックします。

   注：認証仮想サーバーには、バインドされた証明書は必要ありません。
8. サーバー証明書のバインドを設定します。
   - **SNI** 処理に使用される証明書キーをバインドするには、**[SNI** のサーバ証明書] チェックボックスをオンにします。
   - [バインド] ボタンをクリックします。

認証 **CERT** プロファイルの作成

1. セキュリティ**->Citrix ADC AAA-**アプリケーショントラフィック**->** ポリシー**->** 認証**->** 基本ポリシー**->CERT** に移動します。
2. [プロファイル] タブを選択し、[追加] を選択します。
3. 次のフィールドに入力して、認証 CERT プロファイルを作成します。必須フィールドは、設定名の右側に * で示されます。
   - **Name**： クライアント証明書認証サーバ・プロファイルの名前（アクション）。
   - **2** 要素 — この例では、2 要素認証オプションは NOOP です。
   - 「ユーザー名フィールド」**—** ユーザー名を抽出するクライアント証明書フィールドを入力します。「件名」または「発行者」のいずれかに設定する必要があります (両方の二重引用符を含む)。

- グループ名フィールド -グループを抽出するクライアント証明書フィールドを入力します。「件名」または「発行者」のいずれかに設定する必要があります (両方の二重引用符を含む)。
- デフォルトの認証グループ -抽出されたグループに加えて認証が成功したときに選択されるデフォルトのグループです。

4. ［作成］をクリックします。

認証ポリシーの作成

1. セキュリティ**->Citrix ADC AAA-**アプリケーショントラフィック**->** ポリシー**->** 認証**->** 高度なポリシー**->** ポリシーに移動します。
2. [追加] ボタンを選択します。
3. 認証ポリシーを作成するには、次の情報を入力します。必須フィールドは、設定名の右側に * で示されます。

   a)「名前」— アドバンス認証ポリシーの名前を入力します。文字、数字、またはアンダースコア文字 (_) で始まり、文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等しい (=)、コロン (:)、およびアンダースコア文字のみを含める必要があります。認証ポリシーの作成後は変更できません。

   次の要件は、Citrix ADC CLI にのみ適用されます。名前に 1 つ以上のスペースが含まれる場合は、名前を二重引用符または一重引用符で囲みます（「認証ポリシー」や「認証ポリシー」など）。

   b) アクションタイプ -認証アクションのタイプを入力します。

   c) **Action** -ポリシーが一致した場合に実行する認証アクションの名前を入力します。

   d) **[Log Action**]-要求がこのポリシーに一致するときに使用するメッセージログアクションの名前を入力します。

   e)「式」-Citrix ADC の名前付き規則の名前またはデフォルトの構文式を入力します。この規則は、認証サーバーでユーザーを認証するかどうかをポリシーが決定します。

   f)「コメント」— このポリシーに関する情報を保持するコメントを入力します。

4. [作成] をクリックします。

LDAP 認証サーバの追加

1. [セキュリティ**]-> [Citrix ADC AAA]-[**アプリケーショントラフィック**]-> [**ポリシー**]-> [**認証**]-> [**基本ポリシー**]-> [LDAP]** に移動します。
2. LDAP サーバを追加するには、[サーバ] タブを選択し、[追加] ボタンを選択します。

LDAP 認証ポリシーの追加

1. セキュリティ->Citrix ADC AAA-アプリケーショントラフィック-> ポリシー-> 認証-> 高度なポリシー-> ポリシーに移動します。

2. [追加] をクリックして、認証ポリシーを追加します。
3. 認証ポリシーを作成するには、次の情報を入力します。必須フィールドは、設定名の右側に * で示されます。

   a) 名前 -事前認証ポリシーの名前。
   文字、数字、またはアンダースコア文字 (_) で始まり、文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等しい (=)、コロン (:)、およびアンダースコア文字のみを含める必要があります。認証ポリシーの作成後は変更できません。

   次の要件は、Citrix ADC CLI にのみ適用されます。名前に 1 つ以上のスペースが含まれる場合は、名前を二重引用符または一重引用符で囲みます（「認証ポリシー」や「認証ポリシー」など）。

   b) アクションタイプ -認証アクションのタイプ。

   c) **Action** -ポリシーが一致した場合に実行される認証アクションの名前。

   d) **Log Action** -要求がこのポリシーに一致するときに使用するメッセージ・ログ・アクションの名前。

   e) **Expression** -Citrix ADC の名前付きルールの名前、またはデフォルトの構文式。認証サーバーを使用してユーザーを認証するかどうかをポリシーが判断します。

   f) コメント -このポリシーに関する情報を保持するためのコメント。
4. [作成] をクリックします。

RADIUS 認証サーバの追加

1. [セキュリティ**]-> [Citrix ADC AAA]-> [**アプリケーショントラフィック**]-> [**ポリシー**]-> [**認証**]-> [**基本ポリシー**]-> [RADIUS]** に移動します。
2. サーバを追加するには、[サーバ] タブを選択し、[追加] ボタンを選択します。
3. 認証 RADIUS サーバを作成するには、次のように入力します。必須フィールドは、設定名の右側に * で示されます。

   a) RADIUS アクション の名前を入力します。

   b) RADIUS サーバに割り当てられているサーバ名またはサーバの **IP** アドレスを入力します。

   c) RADIUS サーバが接続をリッスンする ポート番号を入力します。

   d) タイムアウト値を数秒で入力します。これは、Citrix ADC アプライアンスが RADIUS サーバーからの応答を待機する値です。

   e) RADIUS サーバーと Citrix ADC アプライアンスの間で共有される 秘密キーを入力します。秘密キーは、Citrix ADC アプライアンスが RADIUS サーバーと通信できるようにするために必要です。

   f) シークレットキーを確認します。
4. [作成] をクリックします。

RADIUS 認証ポリシーの追加

1. セキュリティ**->Citrix ADC AAA-**アプリケーショントラフィック**->** ポリシー**->** 認証**->** 高度なポリシー**->** ポリシーに移動します。
2. [追加] をクリックして、認証ポリシーを作成します。
3. 認証ポリシーを作成するには、次の情報を入力します。必須フィールドは、設定名の右側に * で示されます。

   a) 名前 -事前認証ポリシーの名前。
   文字、数字、またはアンダースコア文字 (_) で始まり、文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等しい (=)、コロン (:)、およびアンダースコア文字のみを含める必要があります。認証ポリシーの作成後は変更できません。

   次の要件は、Citrix ADC CLI にのみ適用されます。名前に 1 つ以上のスペースが含まれる場合は、名前を二重引用符または一重引用符で囲みます（「認証ポリシー」や「認証ポリシー」など）。

   b) アクションタイプ -認証アクションのタイプ。

   c) **Action** -ポリシーが一致した場合に実行される認証アクションの名前。

   d) **Log Action** -要求がこのポリシーに一致するときに使用するメッセージ・ログ・アクションの名前。

   e) **Expression** -Citrix ADC の名前付きルールの名前、またはデフォルトの構文式。認証サーバーを使用してユーザーを認証するかどうかをポリシーが判断します。

   f) コメント -このポリシーに関する情報を保持するためのコメント。
4. [**OK**] をクリックします。
5. 認証ポリシーが表示されていることを確認します。

認証ログインスキーマの作成

1. [セキュリティ**]-> [Citrix ADC AAA]-[**アプリケーショントラフィック**]-[**ログインスキーマ**]** に移動します。
2. [プロファイル] タブを選択し、[追加] ボタンをクリックします。
3. 認証ログイン・スキーマを作成するには、次のフィールドに入力します。

   a)「名前」を入力します。これは新しいログインスキーマの名前です。

   b) 認証スキーマを入力します。これは、ログインページの UI に送信される認証スキーマを読み取るためのファイルの名前です。このファイルには、ログインフォームをレンダリングできるようにするための Citrix フォーム認証プロトコルごとの要素の xml 定義が含まれている必要があります。管理者がユーザーに追加の資格情報を要求せず、以前に取得した資格情報を続行する場合は、引数として「noschema」を指定できます。これは、ユーザー定義のファクタで使用される loginSchemas にのみ適用され、仮想サーバのファクタには適用されません。

   c）ユーザー式を入力します。これは、ログイン中にユーザー名を抽出するための式です。

d）パスワード式を入力する-これはログイン時のパスワード抽出の式です

e）ユーザー・クレデンシャル・インデックスを入力します。これは、ユーザーが入力したユーザー名が、セッションに格納されるインデックスです。

f) パスワードクレデンシャルインデックスを入力します。これは、ユーザーが入力したパスワードがセッションに格納されるインデックスです。

g) 認証強度を入力します。これは現在の認証の重みです。

4. [作成] をクリックします。

   a）ログインスキーマプロファイルが表示されていることを確認します。

ポリシーラベルの作成

ポリシー・ラベルは、特定の要素の認証ポリシーを指定します。各ポリシーラベルは、1 つの要素に対応します。ポリシーラベルは、ユーザーに提示する必要があるログインフォームを指定します。ポリシー・ラベルは、認証ポリシーまたは別の認証ポリシー・ラベルの次の要素としてバインドする必要があります。通常、ポリシーラベルには、特定の認証メカニズムの認証ポリシーが含まれます。ただし、異なる認証メカニズムの認証ポリシーを持つポリシーラベルを使用することもできます。

1. セキュリティ**->Citrix ADC AAA-**アプリケーショントラフィック**->** ポリシー**->** 認証**->** 高度なポリシー**->** ポリシーラベルに移動します。
2. ［追加］をクリックします。
3. 認証ポリシー・ラベルを作成するには、次のフィールドに入力します。

   a) 新しい認証ポリシーラベルの **[Name]** を入力します。

   b) 認証ポリシーラベルに関連付けられた ログインスキーマを入力します。

   c) [続行] をクリックします。

4. ドロップダウンメニューから **[Policy**] を選択します。
5. 目的の 認証ポリシーを選択し、[**Select**] ボタンをクリックします。
6. 次のフィールドに入力します。

   a) ポリシーバインディングの [**Priority**] を入力します。

   b)「**Goto Expression**」を入力します。この式は、現在のポリシー・ルールが TRUE と評価された場合に評価される次のポリシーの優先順位を指定します。

7. 目的の認証ポリシーを選択し、[**Select**] ボタンをクリックします。
8. [バインド] ボタンをクリックします。
9. ［完了］をクリックします。
10. 認証ポリシー・ラベルを確認します。

nFactor 認証用の再キャプチャ設定

Citrix ADC リリース 12.1 ビルド 50.x 以降では、Citrix Gateway は、キャプチャの構成を簡素化する新しいファーストクラスのアクション「captchaAction」をサポートしています。キャプチャは、ファーストクラスのアクションであるように、それは、独自の要因であることができます。nFactor フローのどこにでもキャプチャを挿入できます。

以前は、RfWeb UI の変更を含むカスタム WebAuth ポリシーを記述する必要がありました。キャプチャーアクションが導入されたことで、JavaScript を変更する必要はありません。

> 重要
>
> Captcha がスキーマ内のユーザー名またはパスワードのフィールドと一緒に使用されている場合、Captcha が満たされるまで、送信ボタンは無効になります。

キャプチャの構成

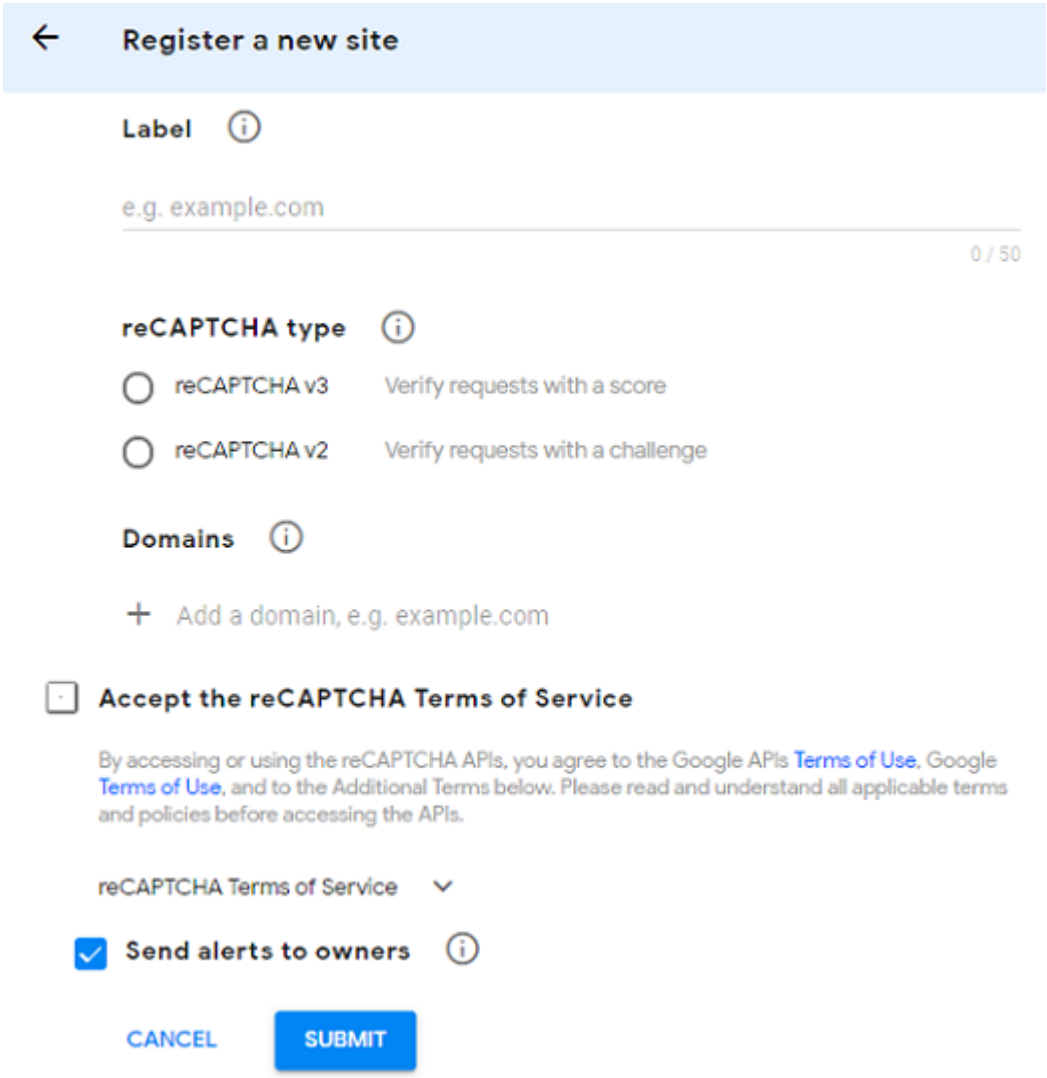
キャプチャの構成には、2 つの部分が含まれます。

1. キャプチャを登録するための Google の構成。
2. ログインフローの一部としてキャプチャを使用する Citrix ADC アプライアンスの構成。

グーグルでキャプチャの設定

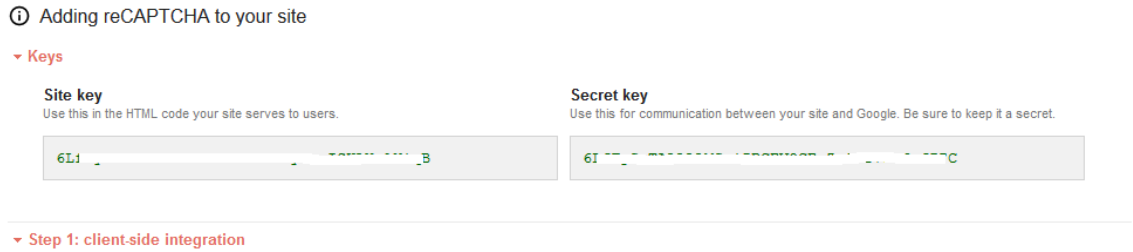
`https://www.google.com/recaptcha/admin##list`でキャプチャのドメインを登録します。

1. このページに移動すると、次の画面が表示されます。



> 注
>
> reCAPTCHA v2 のみを使用してください。目に見えない reCAPTCHA はまだ技術プレビュー中です。

2. ドメインを登録すると、「サイトキー」と「秘密キー」が表示されます。



> 注
>
> セキュリティ上の理由から、「SiteKey」と「SecretKey」はグレー表示になっています。「SecretKey」

> は安全に保管する必要があります。

Citrix ADC アプライアンスでのキャプチャ構成

Citrix ADC アプライアンスのキャプチャ構成は、次の 3 つの部分に分けることができます。

- キャプチャ画面を表示する
- Google サーバーにキャプチャ応答を投稿する
- LDAP 構成は、ユーザーログオンの 2 番目の要素です (オプション)

キャプチャ画面を表示する

ログインフォームのカスタマイズは、SingleAuthCaptcha.xml ログインスキーマを介して行われます。このカスタマイズは、認証仮想サーバーで指定され、ログインフォームをレンダリングするために UI に送信されます。組み込みのログインスキーマである SingleAuthCaptcha.xml は、Citrix ADC アプライアンス上の/nsconfig/loginSchema/ログインスキーマディレクトリにあります。

> 重要
>
> - ユースケースと異なるスキーマに基づいて、既存のスキーマを変更できます。たとえば、Captcha 係数（ユーザー名やパスワードなし）または Captcha との二重認証だけが必要な場合。
> - カスタム変更を実行した場合、またはファイルの名前を変更した場合は、すべての loginSchema を/nsconfig/loginschema ディレクトリから親ディレクトリ/nsconfig/loginschema にコピーすることをお勧めします。

CLI を使用してキャプチャの表示を設定するには

- `add authentication loginSchema singleauthcaptcha -authenticationSchema /nsconfig/loginschema/SingleAuthCaptcha.xml`
- `add authentication loginSchemaPolicy singleauthcaptcha -rule true -action singleauthcaptcha`
- `add authentication vserver auth SSL <IP> <Port>`
- `add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-key-file>`
- `bind ssl vserver auth -certkey vserver-cert`
- `bind authentication vserver auth -policy singleauthcaptcha -priority 5 -gotoPriorityExpression END`

Google サーバーにキャプチャ応答を投稿する

あなたは、ユーザーに表示されなければならないキャプチャを設定した後、管理者は、ブラウザからのキャプチャ応答を確認するために、Google サーバーに構成を追加ポスト。

ブラウザからキャプチャ応答を確認するには

- add authentication captchaAction myrecaptcha -sitekey <sitekey-copied-from-google> -secretkey <secretkey-from-google>
- add authentication policy myrecaptcha -rule **true** -action myrecaptcha
- bind authentication vserver auth -policy myrecaptcha -priority 1

AD 認証が必要な場合は、次のコマンドが必要です。それ以外の場合は、この手順を無視できます。

- add authentication ldapAction ldap-**new** -serverIP x.x.x.x -serverPort 636 -ldapBase "cn=users,dc=aaatm,dc=com"-ldapBindDn adminuser@aaatm.com -ldapBindDnPassword <password> -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName memberof -subAttributeName CN -secType SSL -passwdChange ENABLED -defaultAuthenticationGroup ldapGroup
- add authenticationpolicy ldap-**new** -rule **true** -action ldap-**new**

LDAP 構成は、ユーザーログオンの **2** 番目の要素です **(**オプション**)**

LDAP 認証はキャプチャ後に行われ、2 番目の要素に追加します。

- add authentication policylabel second-factor
- bind authentication policylabel second-factor -policy ldap-**new** -priority 10
- bind authentication vserver auth -policy myrecaptcha -priority 1 -nextFactor second-factor

管理者は、負荷分散仮想サーバーと Citrix Gateway アプライアンスのどちらを使用してアクセスするかに応じて、適切な仮想サーバーを追加する必要があります。ロードバランシング仮想サーバが必要な場合は、管理者が次のコマンドを設定する必要があります。

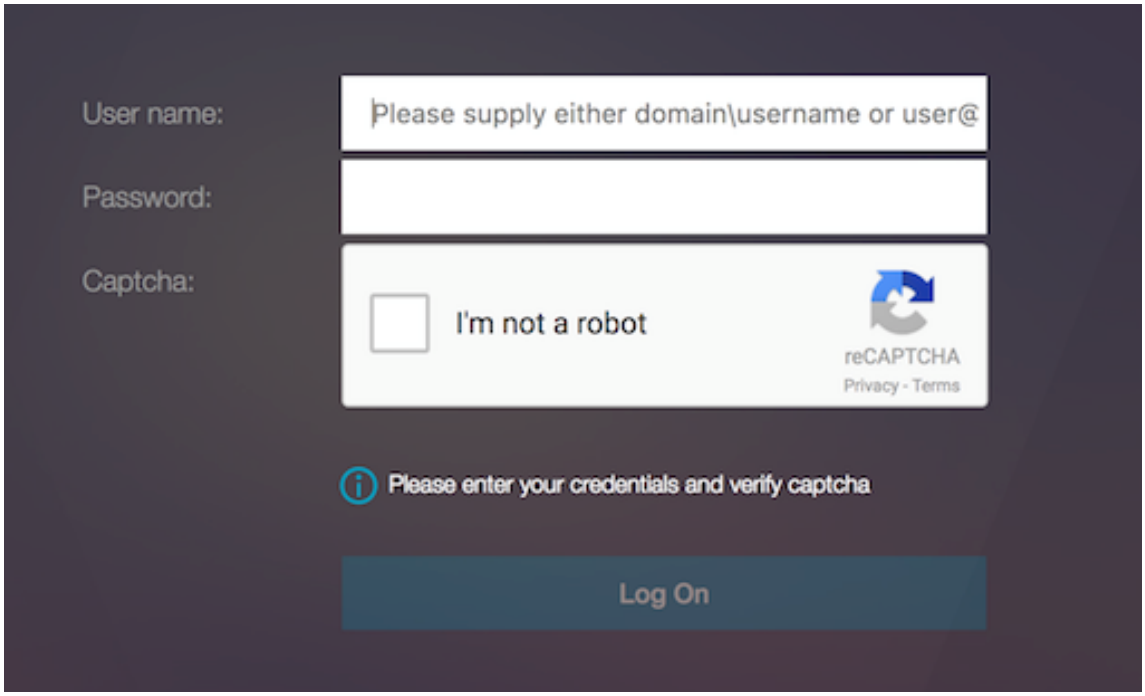
```
1 add lb vserver lbtest HTTP <IP> <Port> -authentication ON -
     authenticationHost nssp.aaatm.com`
2 <!--NeedCopy-->
```

nssp.aaatm.com — 認証仮想サーバーに解決します。

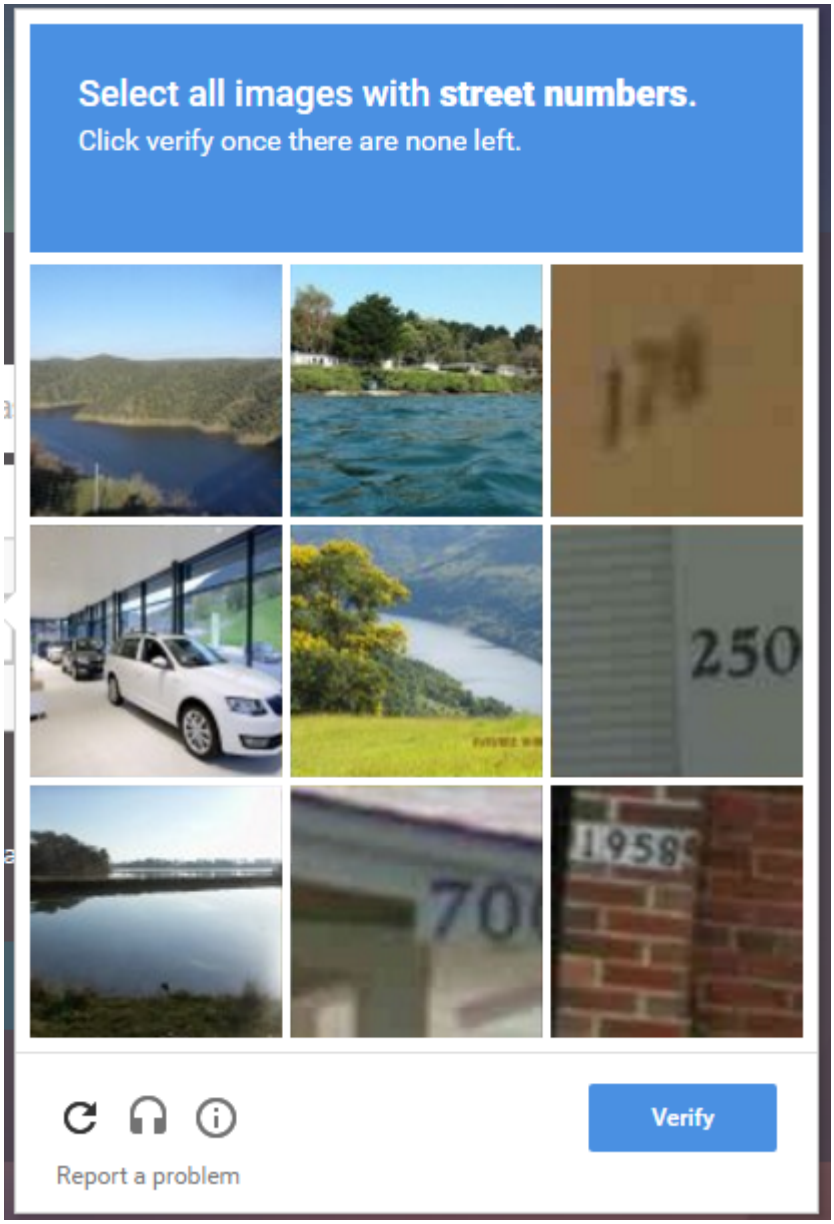
キャプチャのユーザー検証

前のセクションで説明したすべての手順を設定したら、以下に示す UI のスクリーンショットを確認する必要があります。

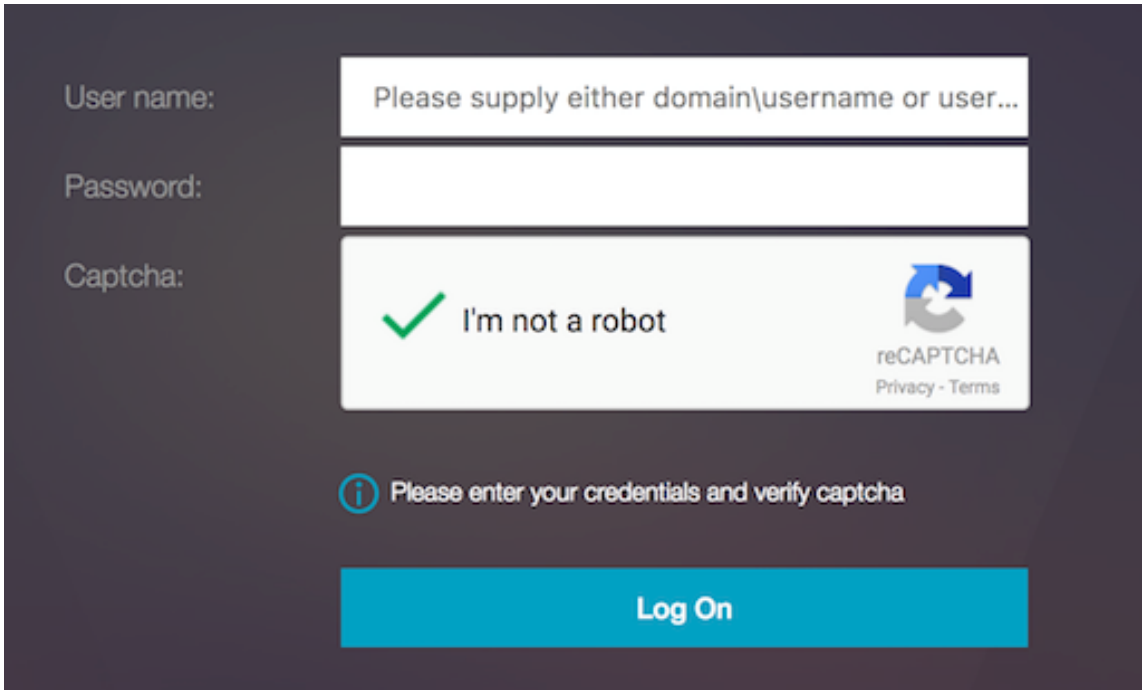
1. 認証仮想サーバーがログインページを読み込むと、ログオン画面が表示されます。ログオンは、キャプチャが完了するまで無効になります。



2. [私はロボットではありません] オプションを選択します。キャプチャウィジェットが表示されます。



3. 完了ページが表示される前に、一連のキャプチャ画像をナビゲートします。
4. AD 資格情報を入力し、[ロボットではありません] チェックボックスをオンにして、[ログオン] をクリックします。認証が成功すると、目的のリソースにリダイレクトされます。



注

- キャプチャが AD 認証で使用されている場合、キャプチャが完了するまで、資格情報の送信ボタンは無効になります。
- キャプチャは、独自の要因で発生します。したがって、AD のような後続の検証は Captcha の ‘nextfactor’ で発生する必要があります。

Unified Gateway Visualizer

March 26, 2020

概要

Unified Gateway Visualizer は、Unified Gateway ウィザードを使用して構成を視覚的に表現します。Unified Gateway Visualizer は、構成の追加と編集、およびバックエンドの問題の診断に使用されます。

Unified Gateway Visualizer には、次の情報が表示されます。
構成	構成
—	-
事前認証ポリシー	認証ポリシー
CS 仮想サーバ	VPN 仮想サーバー
LB 仮想サーバ	XA/XD アプリケーション
ウェブアプリケーション	SaaS アプリ

Unified Gateway の導入により、エンタープライズアプリケーションまたは SaaS アプリケーション、クライアントレスアクセスアプリケーション、Citrix Virtual Apps、およびデスクトップリソースへの 1 つの URL を介してセキュアなリモートアクセスが可能になります。

Unified Gateway の設定

1. メニューから [Unified Gateway] を選択します。

2. 次の画面で、次の情報があることを確認し、[**Get Started**] をクリックします。

```
- Unified Gateway のパブリック IP アドレス。
- オプションのルートCA証明書を持つサーバー証明書チェーン（.PFXまたは.PEM）。
-  LDAP/RADIUS/クライアント証明書ベースの認証の詳細。
-  アプリケーションの詳細（Saasアプリケーションまたは Citrix Virtual Apps and Desktops サーバーの詳細のURL）。
```

3. [続行] ボタンをクリックします。

Unified Gateway 構成の仮想サーバを作成します。

1. 仮想サーバの構成 名を入力します。
2. Unified Gateway 配置のパブリック方向の **Unified Gateway IP** アドレスを入力します。
3. ポート番号を入力します。ポート番号の範囲は 1 ～65535 です。
4. [続行] をクリックします。

サーバー証明書を指定するには、次の情報を入力します。

1. [既存の証明書を使用する] または [証明書のインストール**]** ラジオボタンを選択します。
2. ドロップダウンメニューから サーバー証明書を選択します。
3. [続行] ボタンをクリックします。

認証を指定するには、次の情報を入力します。

1. プルダウンメニューから [プライマリ認証方法] を選択します。
2. [既存のサーバーを使用する**]** または **[**新しいサーバーの追加**]** ラジオボタンを選択します。
3. [続行] ボタンをクリックします。

1. プルダウン・メニューから「ポータル・テーマ」を選択します。
2. [続行] をクリックします。

1. 「**Web** アプリケーション」または「**Citrix Virtual Apps** デスクトップ」ラジオボタンを選択します。
2. [続行] をクリックします。

Web アプリケーションを指定するには、次の情報を入力します。

1. ブックマークのリンクの名前を入力します。
2. VPN URL が表すアプリケーションのタイプを選択します。指定できる値は次のとおりです。

- イントラネットアプリケーション
- クライアントレスアクセス
- SaaS
- この Citrix ADC 上で事前に構成されたアプリケーション

3. このチェックボックスをオンにすると、このアプリケーションに Unified Gateway URL からアクセスできるようになります。
4. ブックマークリンクの URL を入力します。
5. アイコン URL から、アイコンファイルを取得するファイルを選択します。最大長は 255 です。
6. [続行] ボタンをクリックします。

1. ［完了］をクリックします。

1. ［続行］をクリックします。

1. ［完了］をクリックします。

GUI の設定

1. メニューから [Unified Gateway] を選択します。

1. [Unified Gateway ビジュアライザー] アイコンをクリックして、構成済みの Gateway インスタンスにアクセスします。

Unified Gateway のビジュアライザーは、次の図のようになります。

Unified Gateway ビジュアライザーには、事前認証、認証、およびアプリのセクションがあります。vpn 仮想サーバに事前認証ポリシーが設定されている場合は、Unified Gateway ビジュアライザに事前認証が表示されます。

Unified Gateway ビジュアライザーは、ロードバランシングと VPN 仮想サーバーの状態を示すために色分けスキームを使用します。

色彩の色	説明
赤	サーバーがダウンしていることを意味します。
グレー	webapps/Citrix Virtual Apps が設定されていないことを意味します。
緑	仮想サーバーですべてが問題ないことを意味します。
オレンジ	負荷分散仮想サーバーサービスの 1 つを意味します。ダウンしていますが、それでも正常に機能しています。

VPN 仮想サーバの詳細

vpn 仮想サーバの詳細を取得するには、[vpn 仮想サーバ] ノードをクリックします。ポップアップには、C/S ルールやすべてのポリシーなどの詳細が表示されます。

1.（+）アイコンをクリックして、vpn エンティティにポリシーを追加します。

デフォルトでは、次のポリシーがバインドされています。

1. 構成済みのポリシーの詳細を表示するには、目的のノードをクリックします。

VPN 仮想サーバー情報の場合、ポップアップの VPN タイトルは、VPN 仮想サーバーの詳細を示すスライダーに移動するクリック可能なエンティティです。

VPN サーバーの詳細をここに示します。

事前認証ブロック

vpn 仮想サーバに、事前認証ポリシーが関連付けられている場合、Unified Gateway ビジュアライザには PreAuth ブロックが表示されます。[Pre Auth] ブロックはポリシーを表示し、認証前ポリシーを vpn に追加するオプションを提供します。

1. [**+**] をクリックして、事前認証ポリシーを追加します。

事前認証ポリシーが付けられていない場合、このブロックはビューに表示されません。

認証ブロック

Auth ブロックには、プライマリポリシーとセカンダリポリシーが一覧表示されます。Auth ブロックには、ポリシーを追加するためのオプションがあります。

1. [プライマリ] ボックスの一覧の [**+**] をクリックしてプライマリ認証バインドを追加するか、[セカンダリ] ボックスの一覧の [+] をクリックしてセカンダリ認証バインドを追加します。

1. [プライマリ認証方法] ドロップダウンメニューからオプションを選択します。これは必須フィールドです。
2. ラジオボタンを選択して、既存のサーバーを使用するか、新しいサーバーを追加するかを指定します。
3. [**LDAP** ポリシー名**]** ドロップダウンメニューからオプションを選択します。これは必須フィールドです。
4. [セカンダリ認証方法] ドロップダウンメニューからオプションを選択します。これは必須フィールドです。

1. ラジオボタンを選択して、既存のサーバーを使用するか、新しいサーバーを追加するかを指定します。
2. [**RADIUS**] ドロップダウンメニューからオプションを選択します。これは必須フィールドです。
3. ［続行］ をクリックします。

StoreFront の追加

XA/XD の近くにある [**+**] をクリックすると、「XA/XD」アプリが追加されます。

統合ポイントを選択できます。オプションは、StoreFront、WI、または WionNS です。［続行］ をクリックします。

1. StoreFront を構成するには、以下のフィールドに入力します。

フィールド	説明
–	—
StoreFront FQDN	*StoreFront* サーバーの *FQDN* を入力します。最大長: *255* 文字。例: *//storefront.xendt.net*
サイトパス	StoreFront で既に構成されている Receiver for Web サイトへのパスを入力します。
シングル・サインオン・ドメイン	ユーザー認証のデフォルトドメインを入力してください
ストア名	STOREFRONT モニタの名前を入力します。
STORENAME は、StoreFront サーバーの正常性を調べるために StoreFront サービスストア名を定義する引数です。ストオーフロントモニターに適用できます。最大長:31	
Secure Ticket Authority サーバー |*Secure Ticket Authority URL* を入力します。これは通常、配信 *Controller* 上に存在します。
例: *http://sta*|
StoreFront サーバー	StoreFront サーバーの IP アドレスを入力
プロトコル	サーバーで使用されるプロトコルを入力します。
ポート	サーバーが使用するポートを入力します。
負荷分散	StoreFront サーバーの負荷分散構成を入力します。
仮想サーバー *	Unified Gateway 展開のパブリック IP アドレスを入力します。

2. [続行] をクリックします。

SaaS の追加

1. [**+**] をクリックして SaaS アプリを追加すると、[SaaS の追加] ページに移動します。SaaS を設定するには、次のフィールドに入力します。必須の情報が必要なフィールドには、* が付きます。

フィールド	説明
名前 *	ブックマークのリンクの名前を入力します。
アプリケーションの種類	この VPN URL が表すアプリケーションのタイプを入力します。可能な値は次のとおりです。この Citrix ADC 上のイントラネットアプリケーション/クライアントレスアクセス/SaaS/事前構成されたアプリケーション
URL を入力 *	イントラネットアプリケーションの URL を入力します。
ファイルの選択	このリソースを表示するためのアイコンファイルを取得する URL を入力してください。MaxLength = 255

Web アプリケーションの追加

1. [**+**] をクリックして Web アプリを追加すると、[Web アプリの追加] ページに移動します。次のフィールドに入力して、Web アプリケーションを構成します。必須の情報が必要なフィールドには、* が付きます。

フィールド	説明
名前 *	ブックマークのリンクの名前を入力します。
アプリケーションの種類	この VPN URL が表すアプリケーションのタイプを入力します。可能な値は次のとおりです。この Citrix ADC 上のイントラネットアプリケーション/クライアントレスアクセス/SaaS/事前構成されたアプリケーション
URL を入力 *	イントラネットアプリケーションの URL を入力します。
ファイルの選択	このリソースを表示するためのアイコンファイルを取得する URL を入力してください。MaxLength = 255

Unified Gateway の URL からアプリケーションにアクセスできる場合は、アプリケーションをクリックして、ロードバランシングサーバーの詳細にアクセスできます。

(+) をクリックして新しいポリシーを追加できます。ポリシー情報を表示するノードをクリックすると、バインドされたすべてのポリシーを表示できます。

LB にバインドされたサービスの数と、全体的な状態情報も表示されます。さらにクリックすると、すべてのサービスが一覧表示されます。LB に新しいサービスを追加できます。

LB の詳細については、ポップアップのタイトルはクリック可能で、LB 仮想サーバーの詳細ページに表示されます。

モバイル/タブレットデバイスで **RADIUS** 認証と **LDAP** 認証を使用するように **Citrix Gateway** を構成する

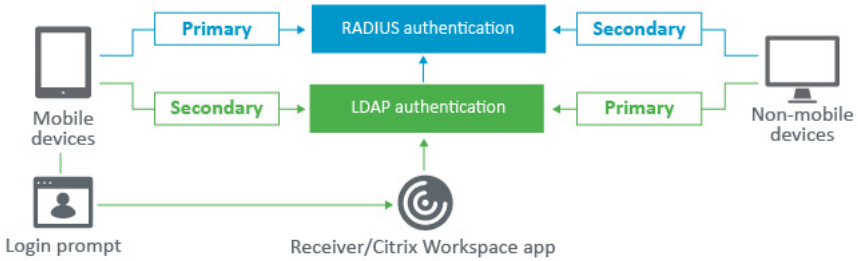
March 26, 2020

このセクションでは、モバイル/タブレットデバイスで RADIUS 認証をプライマリとして使用し、LDAP 認証をセカンダリとして使用するように Citrix Gateway アプライアンスを構成する方法について説明します。

「」セクションで説明した設定では、他のすべての接続で LDAP、2 番目に RADIUS を使用できます。

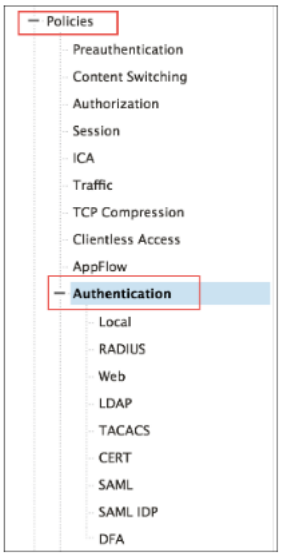
モバイル/タブレットデバイスで使用するために Citrix Workspace アプリで 2 要素認証を構成する場合は、プライマリ認証として RSA SecureID（RADIUS 認証）を追加する必要があります。ただし、Receiver でユーザー名とパ

スワード、パスコードの入力を求めるプロンプトが表示されたら、LDAP を最初に設定し、RADIUS を 2 番目の資格情報として設定します。管理者の観点からは、非モバイル構成と比較して、それは別の構成です。

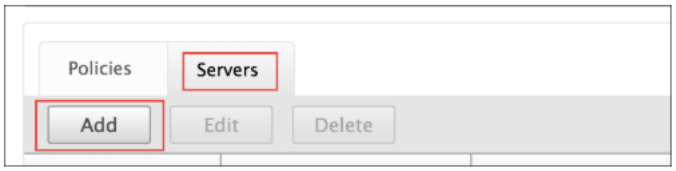


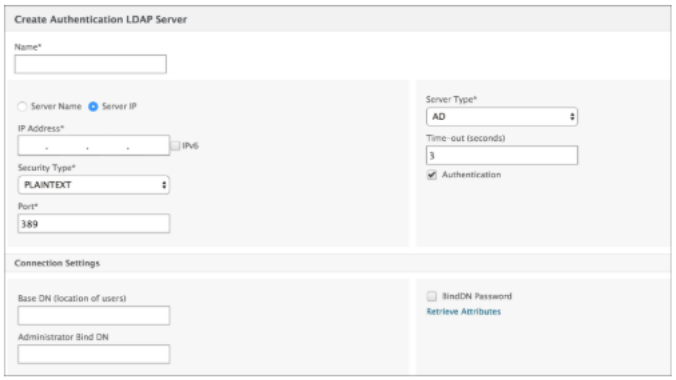
モバイル/タブレットデバイスで RADIUS 認証をプライマリとして使用し、LDAP 認証をセカンダリとして使用するように Citrix Gateway アプライアンスを構成するには、次の手順を実行します。

1. 構成ユーティリティで、Citrix Gateway ／ポリシー／認証を選択し、モバイルデバイスおよび非モバイルデバイス用の LDAP および RSA の認証ポリシーを作成します。これは、ユーザが RADIUS 認証をバイパスできるロジック条件を回避するために必要です。



2. LDAP の [サーバ] タブで [追加] オプションをクリックした後、LDAP サーバの詳細を入力します。



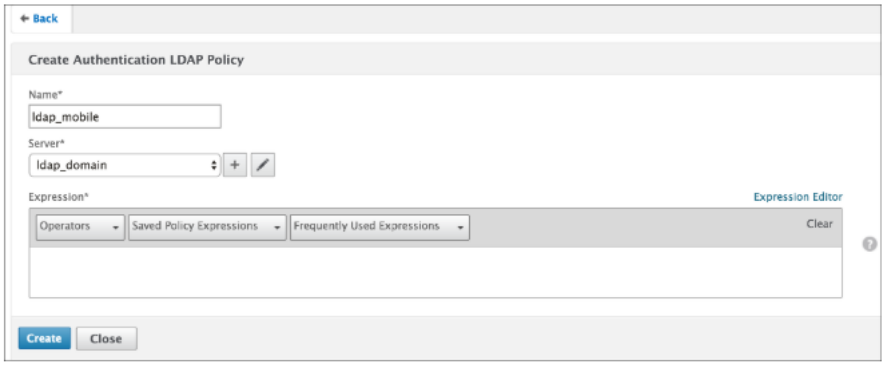


認証サーバーの構成方法の詳細については、「NetScaler で LDAP 認証を構成する方法」の「認証サーバーの作成」を参照してください。

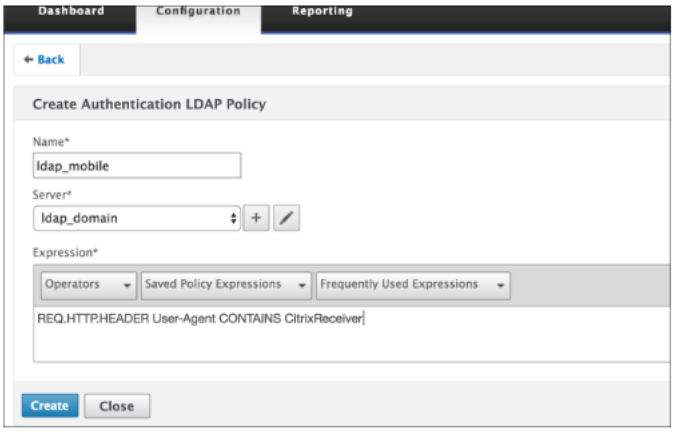
3. 必要な LDAP サーバーを選択して、モバイルデバイスの LDAP ポリシーを作成します。

   このポリシーをモバイルデバイスのみにバインドするには、次の式を使用します。

```
1 `REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver`
```



4. [式エディタ] をクリックしてポリシーを作成します。

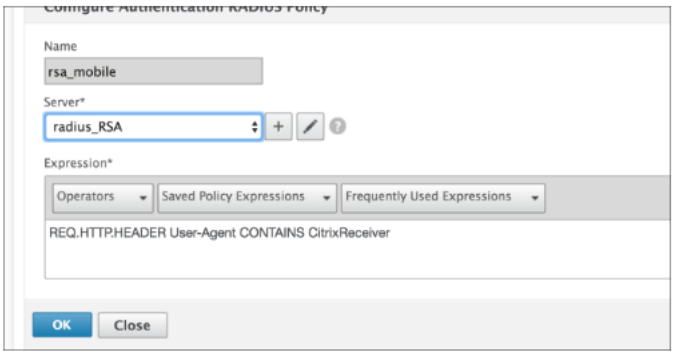


5. モバイルデバイス用の RADIUS ポリシーと RADIUS サーバを作成します。

   (a) ［Citrix Gateway］ > ［ポリシー］ > ［認証］ > ［RADIUS］ から ［RADIUS］ オプションに移動します。[サーバー] タブの [追加] をクリックします。

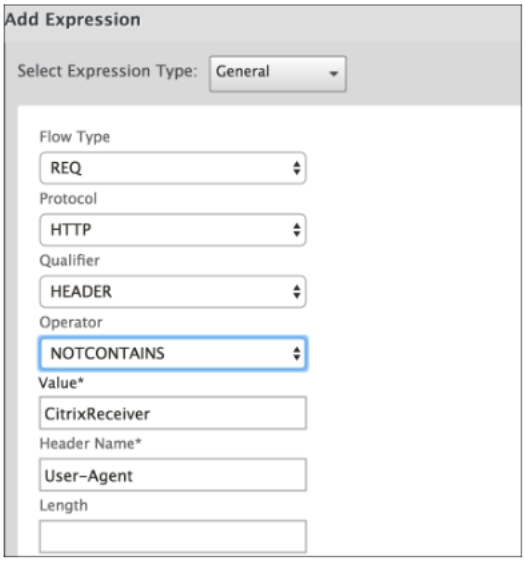
   (b) 必要な情報を追加します。RADIUS 認証のデフォルトポートは 1812 です。

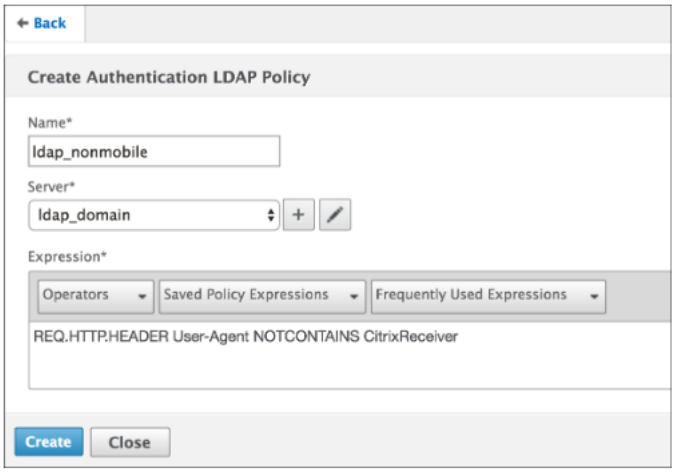
(c) このポリシーをモバイルデバイスのみにバインドするには、次の式を使用します。



6. 同じ手順に従って、非モバイルデバイス用の LDAP ポリシーを作成します。このポリシーをモバイル以外のデバイスにのみバインドするには、次の式を使用します。

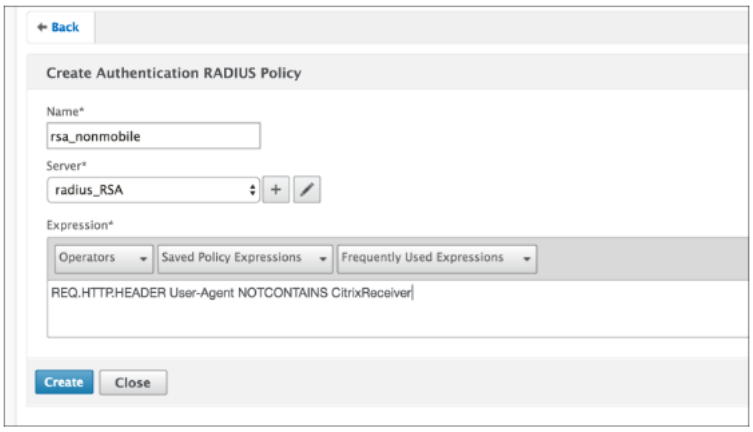
```
`REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver`
```

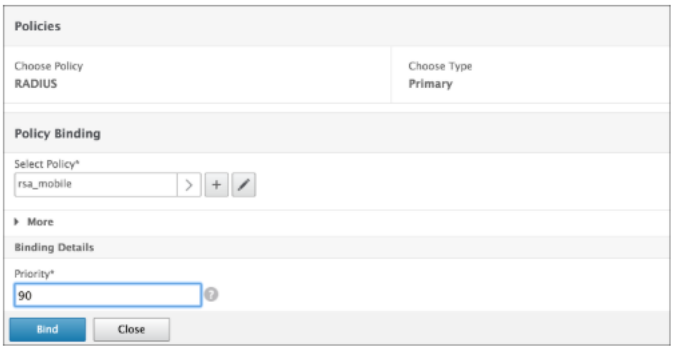


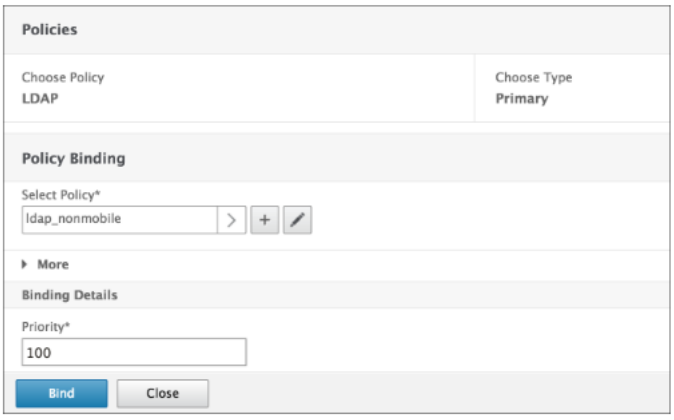
7. モバイルデバイス以外の RADIUS ポリシーを作成します。このポリシーをモバイル以外のデバイスにのみバインドするには、次の式を使用します。

```
`REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver`
```

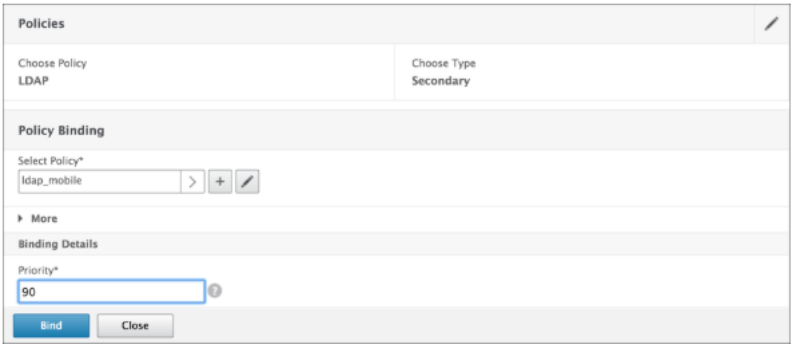



8. Citrix Gateway 仮想サーバーのプロパティに移動し、「認証」タブをクリックします。プライマリ認証ポリシーで、RSA_Mobile ポリシーを最上位プライオリティとして、LDAP_NonMobile ポリシーをセカンダリプライオリティとして追加します。





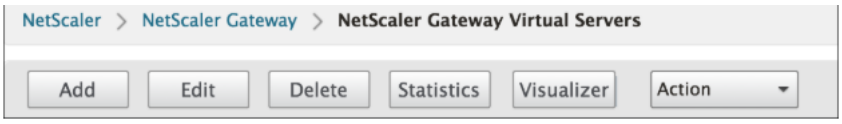
9. セカンダリ認証ポリシーで、LDAP_Mobile ポリシーを最上位プライオリティとして追加し、次に RSA_NonMobile ポリシーをセカンダリプライオリティとして追加します。

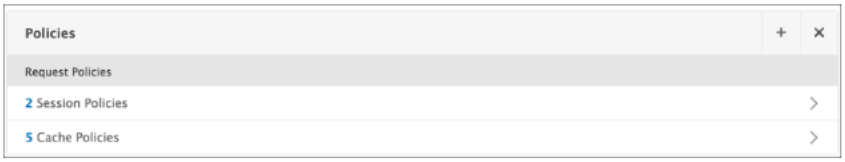


> セッション・ポリシーには、正しい Single Sign-On 資格情報インデックスが必要です。つまり、LDAP 資格情報である必要があります。モバイルデバイスの場合は、[セッションプロファイル] > [クライアントエクスペリエンス] の [資格情報インデックス] を [セカンダリ] に設定する必要があります。これは LDAP です。

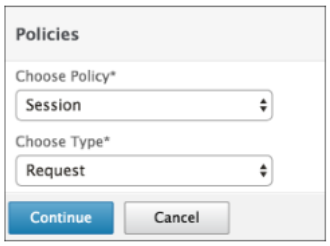
したがって、2 つのセッションポリシーが必要です。1 つはモバイルデバイス用、もう 1 つはモバイルデバイス用です。

(a) モバイルデバイスのセッションポリシーとセッションプロファイルは、次のスクリーンショットに示すように見えます。
セッションポリシーを作成するには、必要な仮想サーバーに移動し、「編集」をクリックし、ポリシー・セクションに移動して「+」記号をクリックします。

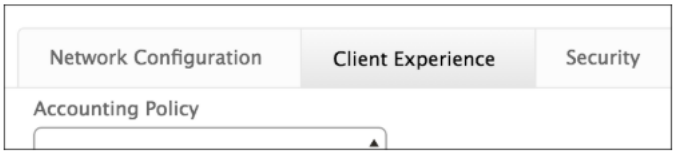


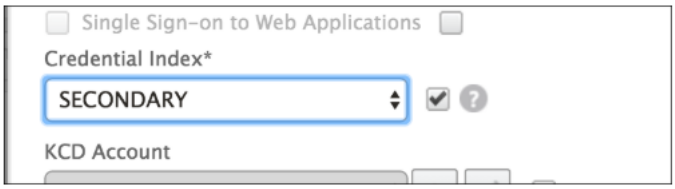


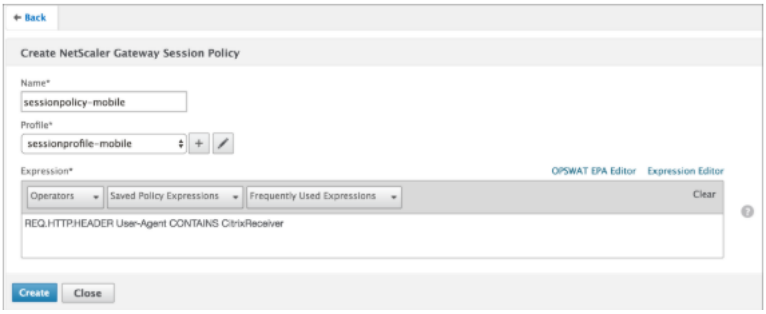
(b) ドロップダウンから [セッション] オプションを選択します。



(c) 目的のセッションポリシー名を入力し、[+] をクリックして新しいプロファイルを作成します。モバイルデバイスの場合は、[セッションプロファイル] > [クライアントエクスペリエンス] の [資格情報インデックス] を [セカンダリ] に設定する必要があります。これは LDAP です。



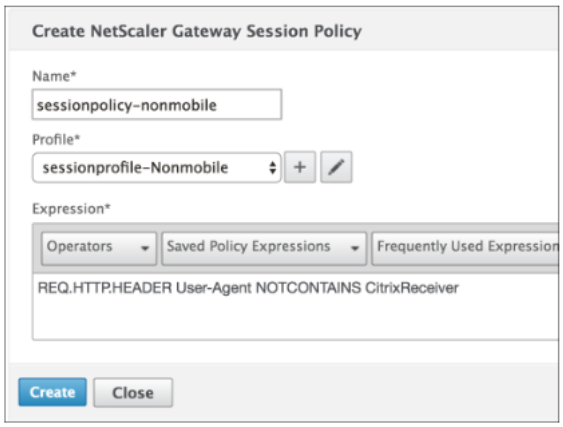




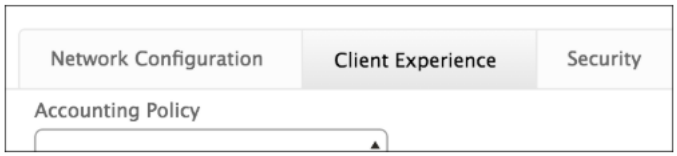
(d) モバイルデバイス以外の場合は、同じ手順に従ってください。[セッションプロファイル] > [クライアントエクスペリエンス] の [資格情報インデックス] を [プライマリ] に設定する必要があります。これは LDAP です。

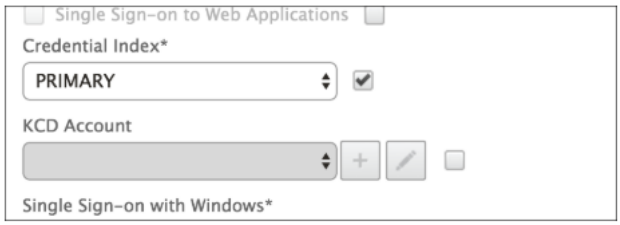
式は次のように変更する必要があります。

```
`REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver`
```

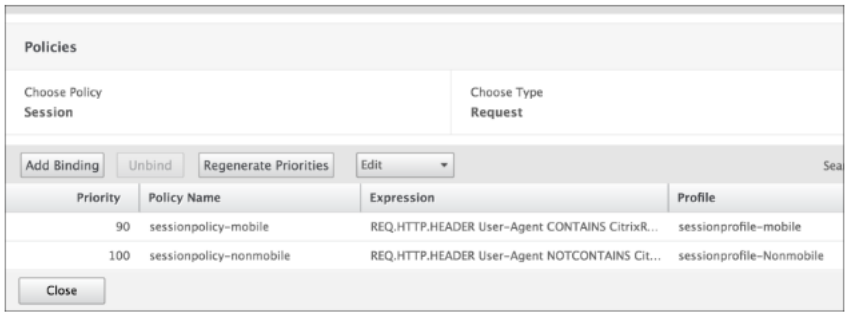


(e) モバイル以外のユーザー用に新しいプロファイルを作成するには、[+] 記号をクリックします。

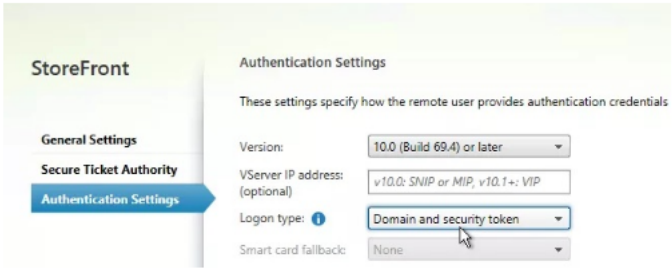


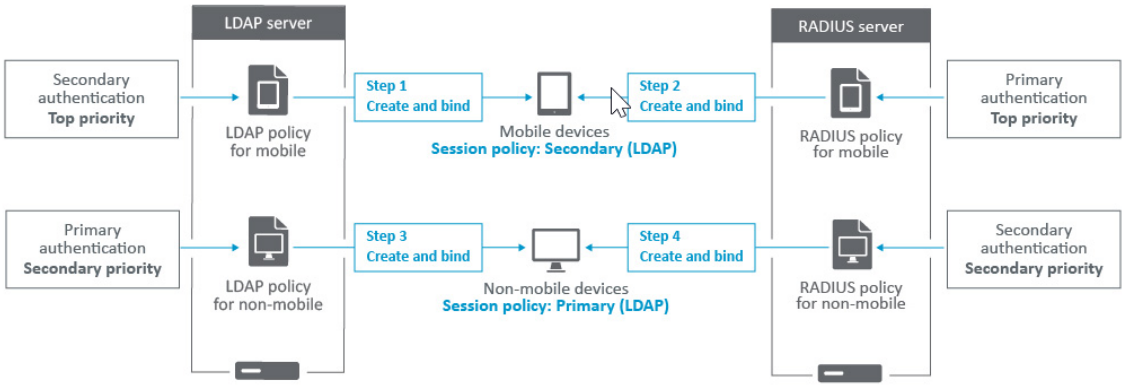


1. 必要な仮想サーバーのポリシーとプロファイルは、次のスクリーンショットのようになります。



2. さらに、StoreFront では、Citrix Gateway 構成で、「ログオンの種類」=「ドメインとセキュリティトークン」を使用するように設定されています。





VPN ユーザエクスペリエンスの設定

April 9, 2020

ユーザーは、以下の方法を使用して、Citrix Gateway 経由で組織のネットワークリソースに接続できます。

- ユーザーデバイスにインストールされているすべての Citrix プラグインを含む Citrix Workspace アプリ。
- Web ブラウザーを使用してアプリケーション、デスクトップ、ShareFile へのユーザー接続を可能にする Web 用 Citrix Workspace アプリ。
- Secure Hub を使用すると、ユーザーは iOS および Android デバイスから Secure Mail、WorxWeb およびモバイルアプリにアクセスできます。
- Windows、Mac OS X、または Linux 用の Citrix Gateway プラグイン。
- iOS と Android のための Citrix Gateway アプリ.
- Java 用の Citrix Gateway プラグイン。
- クライアントレスアクセス。ユーザーソフトウェアをインストールせずに、必要なアクセスをユーザーに提供します。
- Citrix Repeater プラグインとの相互運用性。

ユーザーが Citrix Gateway プラグインをインストールしてから、Citrix XenApp 6.5 から Windows Server 2008（機能パックと機能パック 2 を含む）から Citrix Workspace アプリをインストールすると、Citrix Virtual Desktops 7.0 以降では、Citrix Workspace アプリは自動的に Citrix Gateway プラグインを追加します。ユーザーは、Web ブラウザーまたは Citrix Workspace アプリから Citrix Gateway プラグインを使用して接続できます。

SmartAccess は、エンドポイント分析スキャンの結果に基づいて、ユーザーデバイスに許可されるアクセス方法を自動的に決定します。SmartAccess の詳細については、「SmartAccess 設定」を参照してください。

Citrix Gateway は、iOS および Android モバイルデバイス用の Citrix Endpoint Management Worx アプリをサポートしています. Citrix Gateway には、マイクロ VPN トンネルを確立する iOS モバイルデバイスから Citrix Gateway への接続を可能にする Secure Browse が含まれています。Secure Hub に接続する Android デバイスでは、Micro VPN トンネルが自動的に確立され、Web およびモバイルアプリケーションレベルのセキュアな内部ネットワーク内のリソースへのアクセスを提供します。ユーザーが Worx アプリで Android デバイスから接続する場合は、Citrix Gateway で DNS 設定を構成する必要があります。詳細については、「Android デバイスで DNS サフィックスを使用した DNS クエリのサポート」を参照してください。

Citrix Gateway プラグインでのユーザー接続のしくみ

April 9, 2020

Citrix Gateway は次のように動作します。

- ユーザーが VPN トンネルを介してネットワークリソースにアクセスしようとすると、Citrix Gateway プラグインは組織の内部ネットワーク宛てのネットワークトラフィックをすべて暗号化し、パケットを Citrix

Gateway に転送します。

- Citrix Gateway は SSL トンネルを終了し、プライベートネットワーク宛ての着信トラフィックを受け入れ、トラフィックをプライベートネットワークに転送します。Citrix Gateway は、安全なトンネルを介してリモートコンピュータにトラフィックを送信します。

ユーザーが Web アドレスを入力すると、資格情報の入力とログオンを行うログオンページが表示されます。資格情報が正しい場合、Citrix Gateway はユーザーデバイスとのハンドシェイクを終了します。

ユーザーと Access Gateway の間にプロキシサーバーがある場合は、プロキシサーバーと認証のための資格情報を指定できます。詳しくは、「ユーザ接続のプロキシサポートの有効化」を参照してください。

Citrix Gateway プラグインがユーザーデバイスにインストールされます。最初の接続後、ユーザーが Windows ベースのコンピューターを使用してログオンすると、通知領域のアイコンを使用して接続を確立できます。

セキュアトンネルの確立

March 26, 2020

ユーザーが Citrix Gateway プラグイン、Secure Hub または Citrix Workspace アプリに接続すると、クライアントソフトウェアはポート 443（または Citrix Gateway 上の構成済みポート）を介してセキュアなトンネルを確立し、認証情報を送信します。トンネルが確立されると、Citrix Gateway は Citrix Gateway プラグイン、Secure Hub または Citrix Workspace アプリに構成情報を送信します。アドレスプールを有効にすると、セキュリティ保護対象のネットワークと IP アドレスが記述されます。

セキュアな接続を介したプライベートネットワークトラフィックのトンネリング

Citrix Gateway プラグインが起動し、ユーザーが認証されると、指定されたプライベートネットワーク宛てのネットワークトラフィックがすべてキャプチャされ、セキュアなトンネルを介して Citrix Gateway にリダイレクトされます。Citrix Workspace アプリが Citrix Gateway プラグインをサポートし、ユーザーがログオンしたときにセキュアなトンネルを介して接続を確立する必要があります。

Secure Hub、Secure Mail、および WorxWeb はマイクロ VPN を使用して、iOS および Android モバイルデバイス用のセキュアなトンネルを確立します。

Citrix Gateway は、ユーザーデバイスが接続するすべてのネットワーク接続を受信し、Secure Sockets Layer（SSL）を介して Citrix Gateway に多重化します。この場合、トラフィックは逆多重化され、接続は正しいホストとポートの組み合わせに転送されます。

接続は、単一のアプリケーション、アプリケーションのサブセット、またはイントラネット全体に適用される管理セキュリティポリシーに従います。リモートユーザが VPN 接続を介してアクセスできるリソース（IP アドレスとサブネットペアの範囲）を指定します。

Citrix Gateway プラグインは、定義されたイントラネットアプリケーションの次のプロトコルをインターセプトしてトンネリングします。

- TCP（すべてのポート）
- UDP（すべてのポート）
- ICMP（タイプ 8 および 0-エコー要求/応答）

ユーザーデバイス上のローカルアプリケーションからの接続は、Citrix Gateway に安全にトンネリングされ、ターゲットサーバーへの接続が再確立されます。ターゲットサーバーでは、プライベートネットワーク上のローカル Citrix Gateway からの接続として認識されるため、ユーザーデバイスは非表示になります。これは、逆方向ネットワークアドレス変換 (NAT) とも呼ばれます。IP アドレスを非表示にすると、送信元ロケーションにセキュリティが追加されます。

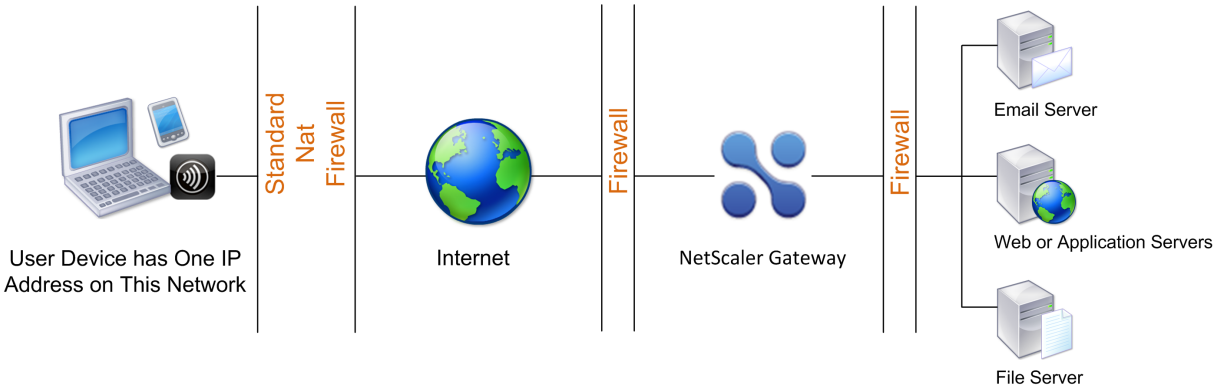
ローカルでは、ユーザーデバイス上で、SYN-ACK、PUSH、ACK、FIN パケットなどの接続関連トラフィックはすべて、Citrix Gateway プラグインによって再作成され、プライベートサーバーから表示されます。

ファイアウォールとプロキシを介した操作

March 26, 2020

Citrix Gateway プラグインのユーザーは、次の図に示すように、別の組織のファイアウォール内に配置されることがあります。

図 1: 2 つの内部ファイアウォールを介したユーザーデバイスからの接続



NAT ファイアウォールは、Citrix Gateway からユーザーデバイスにセキュアなパケットをルーティングできるテーブルを維持します。回線指向接続の場合、Citrix Gateway はポートマップされたリバース NAT 変換テーブルを維持します。逆 NAT 変換テーブルを使用すると、Citrix Gateway は接続を照合し、パケットを正しいポート番号でユーザーデバイスに返送し、パケットを正しいアプリケーションに戻すことができます。

Citrix Gateway プラグインのアップグレード制御

March 26, 2020

概要

システム管理者は、Citrix ADC プラグインのバージョンが Citrix Gateway のリビジョンと一致しない場合の Citrix ADC プラグインの動作を制御します。新しいオプションは、Mac、Windows、またはオペレーティングシステムのプラグインのアップグレード動作を制御します。

VPN プラグインの場合、Citrix ADC ユーザーインターフェイスの 2 つの場所でアップグレードオプションを設定できます。

- グローバル設定で
- セッション・プロファイル・レベルで

プラグインの動作

Citrix Gateway では、クライアントの種類ごとに、以下の 3 つのオプションを使用してプラグインのアップグレード動作を制御できます。

a.**[** 常に表示**]**

エンドユーザーのプラグインのバージョンが Citrix ADC に同梱されているプラグインと一致しない場合、プラグインは常にアップグレードされます。これはデフォルトの動作です。エンタープライズで複数のプラグインバージョンを実行したくない場合は、このオプションを選択します。

b. エッセンシャル（およびセキュリティ）

プラグインが必要と判断された場合にのみアップグレードされました。次の 2 つの状況においては、アップグレードが必要と判断されます。

- インストールされているプラグインは、現在の Citrix ADC バージョンと互換性がありません。
- インストールされたプラグインは、必要なセキュリティ修正のために更新する必要があります。

プラグインのアップグレード回数を最小限に抑えるが、プラグインのセキュリティ更新プログラムを見逃したくない場合は、このオプションを選択する必要があります。

c.**[** なし**]**

プラグインはアップグレードされません。

VPN プラグインのアップグレードを制御するための **CLI** パラメータ

Citrix Gateway は、Windows および Mac オペレーティングシステム用の 2 種類のプラグイン（EPA と VPN）をサポートしています。セッションレベルで VPN プラグインのアップグレード制御をサポートするために、Citrix Gateway では、WindowsinPluginUpgrade と MacPluginUpgrade という 2 つのセッションプロファイルパラメーターがサポートされています。

これらのパラメータは、グローバル、仮想サーバ、グループ、およびユーザレベルで使用できます。各パラメータには、常に、必須、または絶対に設定できます。これらのパラメータの詳細については、プラグインの動作を参照してください。

EPA プラグインのアップグレードを制御するための CLI パラメータ

Citrix Gateway は、Windows および Mac オペレーティングシステム用の EPA プラグインをサポートしています。仮想サーバーレベルで EPA プラグインのアップグレード制御をサポートするために、Citrix Gateway では、ウィンドウ EPA プラグインアップグレードと macEPA プラグインアップグレードという 2 つの仮想サーバーパラメーターがサポートされています。

パラメーターは、仮想サーバーレベルで使用できます。各パラメータには、常に、必須、または絶対に設定できます。これらのパラメーターの説明については、プラグインの動作を参照してください。

VPN 構成

Windows、Linux、Mac プラグインの VPN 設定については、以下の手順に従ってください。

1. ［Citrix NetScaler> ポリシー］ > ［セッション］ の順に選択します。
2. 目的のセッションポリシーを選択し、[**Edit**] をクリックします。
3. [**+**] アイコンをクリックします。
4. [クライアントエクスペリエンス] タブを選択します。
5. これらのダイアログボックスのオプションは、アップグレードの動作に影響します。
    - 常に
    - 必須
    - なし

> 既定値は [常時] です。

1. 各オプションの右側にあるチェックボックスをオンにします。アップグレード動作を適用する頻度を選択します。

EPA 構成

Windows、Linux、Apple プラグインの EPA 構成については、以下の手順に従ってください。

1. Citrix Gateway > ［仮想サーバー］ の順に選択します。
2. サーバを選択し、[編集] ボタンをクリックします。
3. 鉛筆アイコンをクリックします。
4. [詳細] をクリックします。
5. 表示されるダイアログボックスは、アップグレードの動作に影響します。使用可能なオプションは次のとおりです。
    - 常に
    - 必須
    - なし

要件

- Windows の EPA および VPN プラグインのバージョンは 11.0.0.0 より大きくする必要があります。
- Mac EPA プラグインのバージョンは 3.0.0.31 より大きくなければなりません
- Mac VPN プラグインのバージョンは 3.1.4 (357) より大きくなければなりません。

> 注： Citrix ADC を 11.0 リリースにアップグレードすると、アップグレード制御の構成に関係なく、以前のすべての VPN（および EPA）プラグインが最新バージョンにアップグレードされます。以降のアップグレードでは、上記のアップグレード制御設定を尊重します。

Citrix Gateway で完全な VPN セットアップを構成する

October 22, 2021

このセクションでは、Citrix Gateway アプライアンスで完全な VPN セットアップを構成する方法について説明します。ネットワークに関する考慮事項と、ネットワークの観点から問題を解決するための理想的なアプローチが含まれています。

前提条件

- SSL 証明書：これはインストールされ、VPN 仮想サーバー（VServer）にバインドする必要があります。
  - CTX109260 - NetScaler アプライアンスでパブリック SSL 証明書を生成してインストールする方法
  - CTX122521 - NetScaler アプライアンスのデフォルト証明書を、アプライアンスのホスト名に一致する信頼された CA 証明書に置き換える方法
  - Citrix ドキュメント-SSL ベースの仮想サーバーへの証明書とキーペアのバインド
- 認証プロファイル：これは、Citrix Gateway で作成され、機能する必要があります。
  - 詳細については、Citrix のドキュメントを参照 - 外部ユーザ認証の設定
  - 詳細については、チェックリストを参照してください：AD FS を使用してシングルサインオンを実装および管理する
- ダウンロード Citrix クライアント
- セッションポリシー（完全な VPN 接続を許可する）

ユーザーが Citrix Gateway プラグイン、Secure Hub または Citrix Workspace アプリに接続すると、クライアントソフトウェアはポート 443（または Citrix Gateway 上の構成済みポート）を介してセキュアなトンネルを確立し、認証情報を送信します。トンネルが確立されると、Citrix Gateway は、保護されるネットワークを説明する構成情報を Citrix Gateway プラグイン、Citrix Secure Hub または Citrix Workspace アプリに送信します。イントラネット IP を有効にした場合、この情報には IP アドレスも含まれます。

ユーザデバイス接続を設定するには、ユーザが内部ネットワークでアクセスできるリソースを定義します。ユーザーデバイス接続の設定には、次のものが含まれます。

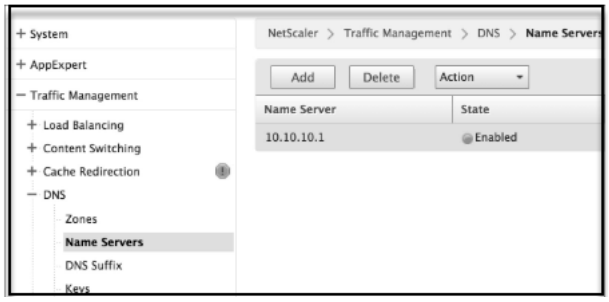
- 分割トンネリング
- ユーザーの IP アドレス (アドレスプール (イントラネット IP) を含む)
- プロキシサーバーを介した接続
- ユーザーがアクセスを許可するドメインの定義
- タイムアウト設定
- シングルサインオン
- Citrix Gateway 経由で接続するユーザーソフトウェア
- モバイルデバイスへのアクセス

ほとんどのユーザーデバイス接続は、セッションポリシーの一部であるプロファイルを使用して構成します。また、認証単位、トラフィック、および認可ポリシーを使用して、ユーザーデバイスの接続設定を定義することもできます。また、イントラネットアプリケーションを使用して構成することもできます。

Citrix Gateway アプライアンスでの完全な VPN セットアップの構成

Citrix Gateway アプライアンスで VPN セットアップを構成するには、以下の手順を実行します。

1. NetScaler 構成ユーティリティから、「トラフィック管理」>「DNS」に移動します。
2. 次のスクリーンショットに示すように、[ネームサーバー] ノードを選択します。DNS ネームサーバがリストされていることを確認します。使用できない場合は、DNS ネームサーバーを追加します。

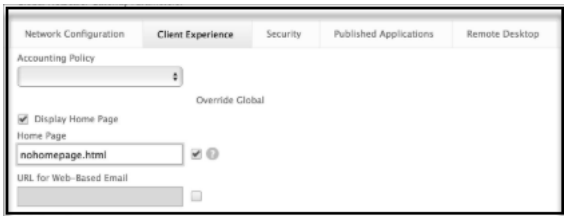


3. Citrix Gateway >［ポリシー］の順に展開します。
4.「セッション」ノードを選択します。
5. Citrix Gateway セッションポリシーとプロファイル］ページの［プロファイル］タブを有効にして、［追加］をクリックします。

> Citrix Gateway セッションプロファイルの構成ダイアログボックスで構成するコンポーネントごとに、各コンポーネントの「グローバルオーバーライド」オプションが選択されていることを確認します。

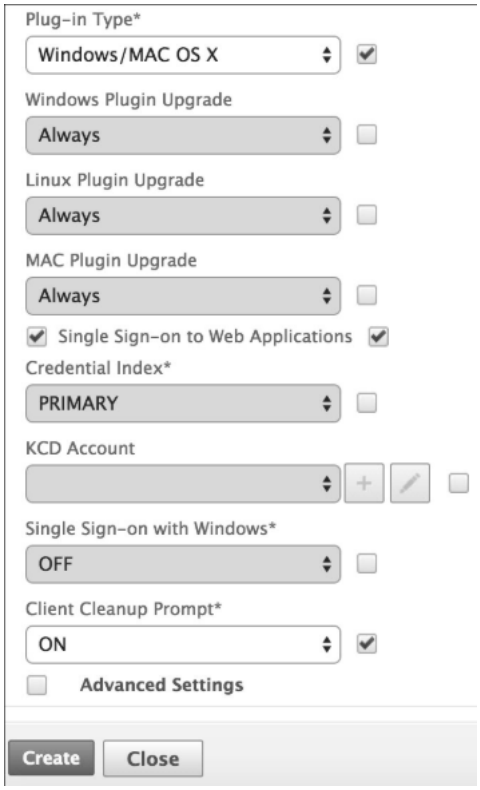
6. [クライアントエクスペリエンス] タブをアクティブにします。
7. ユーザーが VPN にログインするときに URL を表示する場合は、[ホームページ] フィールドにイントラネットポータルの URL を入力します。ホームページパラメータが「nohomepage.html」に設定されている場合、

ホームページは表示されません。プラグインが起動すると、ブラウザインスタンスが起動し、自動的に強制終了されます。

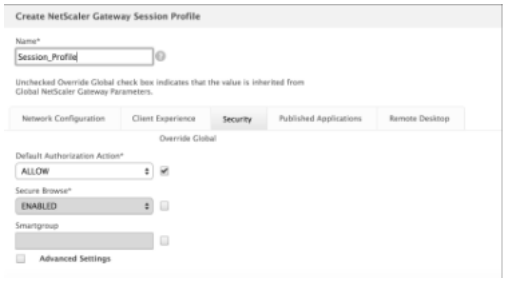


8. [Split Tunnel] リストから目的の設定を選択していることを確認します（この設定の詳細については、上記を参照してください）。
9. FullVPN を使用する場合は、クライアントレスアクセスリストから OFF を選択します。

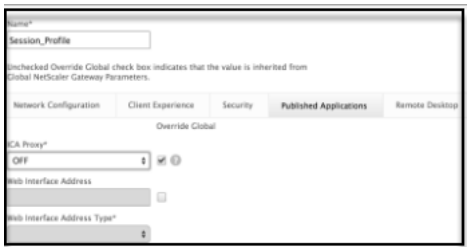
10. プラグインの [タイプ] リストから [Windows/Mac OS X] が選択されていることを確認します。
11. 必要に応じて、「Web アプリケーションへのシングル・サインオン」オプションを選択します。
12. 次のスクリーンショットに示すように、必要に応じて [クライアントクリーンアッププロンプト] オプションが選択されていることを確認します。



13. [セキュリティ] タブをアクティブにします。
14. 次のスクリーンショットに示すように、[既定の承認操作] リストから [ALLOW] が選択されていることを確認します。

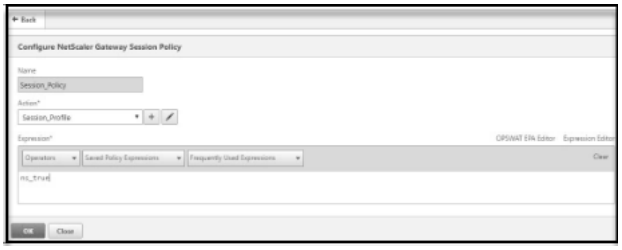


15. [公開アプリケーション] タブをアクティブにします。
16. ［公開アプリケーション］オプションの［ICA プロキシ］リストから［OFF］が選択されていることを確認します。



17. ［作成］をクリックします。

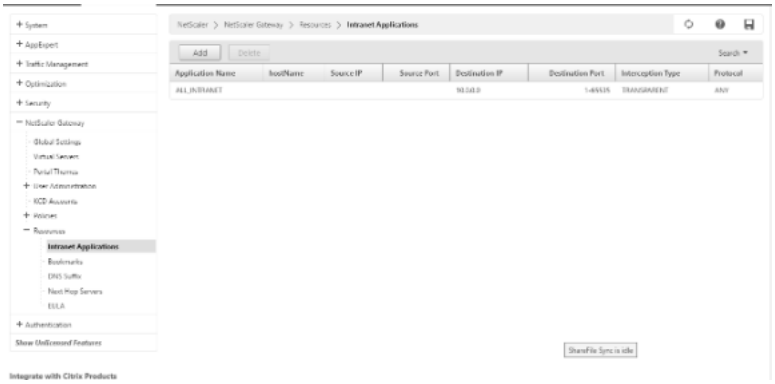
18. ［閉じる］をクリックします。
19. Vserver の Citrix Gateway セッションポリシーとプロファイル］ページの［ポリシー］タブを有効にするか、必要に応じて GROUP/USER レベルでセッションポリシーを有効にします。
20. 次のスクリーンショットに示すように、必要な式または ns_true を使用してセッションポリシーを作成します。



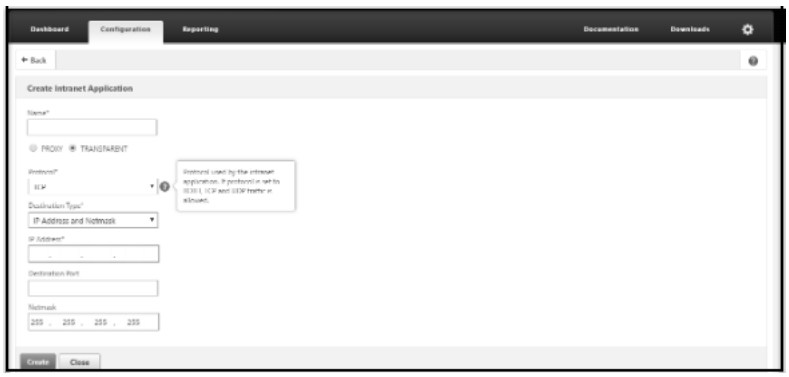
21. セッションポリシーを VPN 仮想サーバーにバインドします。

    Citrix Gateway 仮想サーバー］> ［ポリシー］の順に選択します。ドロップダウンリストから必要なセッションポリシー（この例では Session_Policy）を選択します。

22. 分割トンネルが ON に設定されている場合は、VPN に接続したときにユーザがアクセスできるようにするイントラネットアプリケーションを設定する必要があります。Citrix Gateway > ［リソース］> ［イントラネットアプリケーション］の順に選択します。



23. 新しいイントラネットアプリケーションを作成します。Windows クライアントでの FullVPN の場合は、[透過型] を選択します。許可するプロトコル（TCP、UDP、ANY)、宛先タイプ（IP アドレスとマスク、IP アドレスの範囲、ホスト名）を選択します。



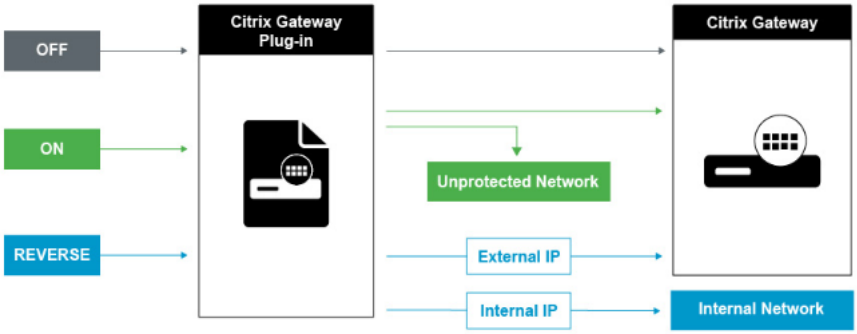
24. 次の式を使用して、iOS および Android 上の Citrix VPN の新しいポリシーを設定します。
25. 次の式を使用して、iOS および Android 上の Citrix VPN の新しいポリシーを設定します。
    REQ.HTTP.HEADER User-Agent CONTAINS CitrixVPN && (REQ.HTTP.HEADER User-Agent CONTAINS NSGiOSplugin || REQ.HTTP.HEADER User-Agent CONTAINS Android)

26. 必要に応じて、USER/GROUP/VSERVER レベルで作成されたイントラネットアプリケーションをバインドします。

    追加パラメータ

    以下に、設定できるパラメータの一部とそれぞれの簡単な説明を示します。

    分割トンネル



分割トンネルオフ

分割トンネルがオフに設定されている場合、Citrix Gateway プラグインはユーザーデバイスからのすべてのネットワークトラフィックをキャプチャし、VPN トンネル経由で Citrix Gateway に送信します。つまり、VPN クライアントは、Citrix Gateway VIP を指すクライアント PC からのデフォルトルートを確立します。つまり、宛先に到達するには、すべてのトラフィックをトンネル経由で送信する必要があります。すべてのトラフィックはトンネルを介して送信されるため、認可ポリシーでは、トラフィックが内部ネットワークリソースへの通過を許可するか、拒否するかを決定する必要があります。

「off」に設定すると、Web サイトへの標準 Web トラフィックを含むすべてのトラフィックがトンネルを通過します。この Web トラフィックを監視および制御することが目的である場合は、NetScaler を使用してこれらの要求を外部プロキシに転送する必要があります。ユーザーデバイスは、内部ネットワークにアクセスするためにプロキシサーバーを介して接続することもできます。
Citrix Gateway は、HTTP、SSL、FTP、および SOCKS プロトコルをサポートしています。ユーザー接続のプロキシサポートを有効にするには、Citrix Gateway でこれらの設定を指定する必要があります。Citrix Gateway のプロキシサーバーが使用する IP アドレスとポートを指定できます。プロキシサーバーは、内部ネットワークへのすべてのそれ以降の接続のためのフォワードプロキシとして使用されます。

詳細については、次のリンクを参照してください。

- ユーザ接続のプロキシサポートの有効化
- 分割トンネル OFF

分割トンネル **ON**

分割トンネリングを有効にすると、Citrix Gateway プラグインが Citrix Gateway に不要なネットワークトラフィックを送信しないようにできます。分割トンネルが有効な場合、Citrix Gateway プラグインは、Citrix Gateway によって保護されたネットワーク（イントラネットアプリケーション）宛てのトラフィックのみを VPN トンネル経由で送信します。Citrix Gateway プラグインは、保護されていないネットワーク宛てのネットワークトラフィックを Citrix Gateway に送信しません。Citrix Gateway プラグインが起動すると、Citrix Gateway からイントラネットアプリケーションのリストを取得し、クライアント PC のイントラネットアプリケーションタブで定義された各サブネットのルートを確立します。Citrix Gateway プラグインは、ユーザーデバイスから送信されたすべてのパケットを調べ、そのパケット内のアドレスをイントラネットアプリケーション（VPN 接続の開始時に作成されたルーティングテーブル）のリストと比較します。パケット内の宛先アドレスがイントラネットアプリケーションのいずれか内にある場合、Citrix Gateway プラグインは VPN トンネルを介して Citrix Gateway にパケットを送信します。宛先アドレスが定義済みのイントラネットアプリケーションにない場合、パケットは暗号化されず、ユーザーデバイスはクライアント PC で最初に定義されたデフォルトのルーティングを使用してパケットを適切にルーティングします。「分割トンネリングを有効にすると、イントラネットアプリケーションは、インターセプトされ、トンネルを介して送信されるネットワークトラフィックを定義します。」

詳細については、次のリンクを参照してください。

- 分割トンネル ON

リバース分割トンネル

Citrix Gateway では、リバース分割トンネリングもサポートされています。リバース分割トンネリングは、Citrix Gateway が傍受しないネットワークトラフィックを定義します。分割トンネリングを逆方向に設定すると、イントラネットアプリケーションは、Citrix Gateway がインターセプトしないネットワークトラフィックを定義します。リバース分割トンネリングを有効にすると、内部 IP アドレス宛てのネットワークトラフィックはすべて VPN トンネルをバイパスし、その他のトラフィックは Citrix Gateway を通過します。リバース分割トンネリングは、すべての非ローカル LAN トラフィックをログに記録するために使用できます。たとえば、ユーザーがホームワイヤレスネットワークを持っていて、Citrix Gateway プラグインを使用してログオンしている場合、Citrix Gateway は、ワイヤレスネットワーク内のプリンターまたは他のデバイス宛てのネットワークトラフィックを傍受しません。

分割トンネリングを設定するには

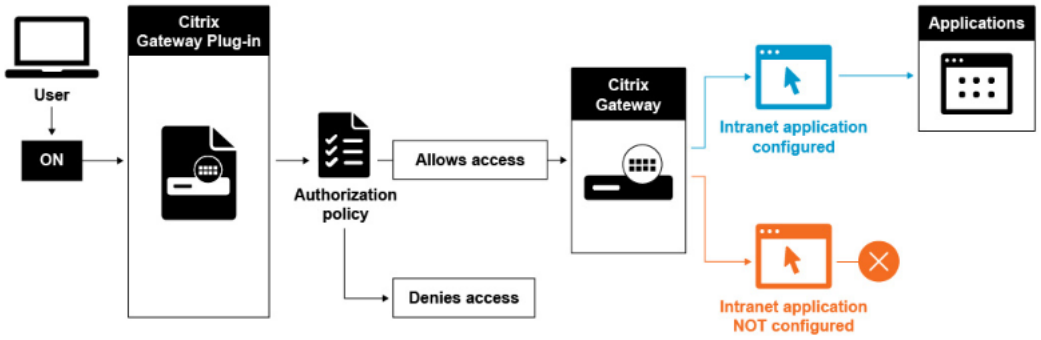
1. 構成ユーティリティから、[構成] タブ > [Citrix Gateway] > [ポリシー] > [セッション] の順に選択します。
2. 詳細ペインの [プロファイル] タブでプロファイルを選択し、[開く] をクリックします。

3. [クライアントエクスペリエンス] タブで、[分割トンネル] の横にある [グローバル上書き] を選択し、オプションを選択して [OK] を 2 回クリックします。

   分割トンネリングおよび認可の設定

   Citrix Gateway の展開を計画するときは、分割トンネリングと、デフォルトの承認アクションと承認ポリシーを考慮することが重要です。

   たとえば、ネットワークリソースへのアクセスを許可する認可ポリシーがあるとします。分割トンネリングが ON に設定されており、イントラネットアプリケーションが Citrix Gateway 経由でネットワークトラフィックを送信するように構成していない。Citrix Gateway にこのような構成がある場合、リソースへのアクセスは許可されますが、ユーザーはリソースにアクセスできません。



認証ポリシーによってネットワークリソースへのアクセスが拒否され、分割トンネリングがオンに設定されていて、イントラネットアプリケーションが Citrix Gateway 経由でネットワークトラフィックをルーティングするように構成されている場合、Citrix Gateway ateway プラグインは Citrix Gateway にトラフィックを送信しますが、リソースへのアクセスは拒否されます。

承認ポリシーの詳細については、以下を参照してください。

- 認可の設定
- 認可ポリシーの設定
- デフォルトのグローバル認可の設定

内部ネットワークリソースへのネットワークアクセスを構成するには

1. 構成ユーティリティで、［構成］タブ > ［Citrix Gateway］ > ［リソース］ > ［イントラネットアプリケーション］の順に選択します。
2. 詳細ウィンドウで、[追加] をクリックします。
3. ネットワークアクセスを許可するためのパラメータを入力し、[作成]、[閉じる] の順にクリックします。

VPN ユーザーのイントラネット IP を設定しない場合、ユーザーは Citrix Gateway VIP にトラフィックを送信し、そこから NetScaler が内部 LAN 上にあるイントラネットアプリケーションリソースに新しいパケットを構築します。この新しいパケットは、SNIP からイントラネットアプリケーションに向かって発信されます。ここから、イントラネットアプリケーションはパケットを取得して処理し、そのパケットの送信元（この場合は SNIP）に返信しよう

とします。SNIP はパケットを取得し、要求を行ったクライアントに応答を返送します。
詳細については、次のリンクを参照してください。

イントラネット IP なし

イントラネット IP が使用されている場合、ユーザーは Citrix Gateway VIP にトラフィックを送信し、そこから NetScaler はクライアント IP をプールから構成された INTRANET IP のいずれかにマップします。NetScaler はイントラネット IP プールを所有するため、内部ネットワークではこれらの範囲を使用しないでください。NetScaler は、DHCP サーバーの場合と同様に、着信 VPN 接続にイントラネット IP を割り当てます。NetScaler は、ユーザーがアクセスする LAN 上にあるイントラネットアプリケーションへの新しいパケットを構築します。この新しいパケットは、イントラネット IP の 1 つからイントラネットアプリケーションに向かって発信されます。ここから、イントラネットアプリケーションはパケットを取得して処理し、そのパケットのソース (INTRANET IP) に返信しようとします。この場合、応答パケットを NetScaler に戻す必要があります。NetScaler では、イントラネット IP が配置されています（NetScaler はイントラネット IP サブネットを所有しています）。このタスクを実行するには、ネットワーク管理者が INTRANET IP へのルートを設定し、SNIP の 1 つを指す必要があります（非対称トラフィックを避けるために、パケットが最初に NetScaler から出るルートを保持する SNIP にトラフィックを戻すことをお勧めします）。

詳細については、次のリンクを参照してください。

イントラネット IP

ネームサービス解決の設定

Citrix Gateway のインストール時に、Citrix Gateway ウィザードを使用して、ネームサービスプロバイダーなどの追加設定を構成できます。ネームサービスプロバイダーは、完全修飾ドメイン名 (FQDN) を IP アドレスに変換します。Citrix Gateway ウィザードでは、DNS サーバーまたは WINS サーバーの構成、DNS 検索の優先度、およびサーバーへの接続を再試行する回数を設定できます。

Citrix Gateway ウィザードを実行すると、その時点で DNS サーバーを追加できます。セッションプロファイルを使用して、追加の DNS サーバーと WINS サーバーを Citrix Gateway に追加できます。その後、ウィザードで最初に使用した名前解決サーバーとは別の名前解決サーバーに接続するようにユーザーとグループに指示できます。

Citrix Gateway で追加の DNS サーバーを構成する前に、名前解決のための DNS サーバーとして機能する仮想サーバーを作成します。

セッションプロファイル内に DNS または WINS サーバーを追加するには

1. 構成ユーティリティで、［構成］タブ > ［Citrix Gateway］ > ［ポリシー］ > ［セッション］ を選択します。
2. 詳細ペインの [プロファイル] タブでプロファイルを選択し、[開く] をクリックします。
3. [ネットワーク構成] タブで、次のいずれかの操作を行います。
   - DNS サーバーを構成するには、[DNS 仮想サーバー] の横にある [グローバル上書き] をクリックし、サーバーを選択して [OK] をクリックします。
   - WINS サーバーを構成するには、[WINS サーバー IP] の横にある [グローバル上書き] をクリックし、IP アドレスを入力して [OK] をクリックします。

ユーザーアクセス方式の選択

March 26, 2020

ユーザー接続を提供するように Citrix Gateway を構成するには、以下のシナリオを使用します。

- Citrix Workspace アプリを使用したユーザー接続。Citrix Workspace アプリは、StoreFront または Web Interface と連携して、サーバーファーム内の公開アプリケーションまたは仮想デスクトップへのアクセスをユーザーに提供します。Citrix Workspace アプリは、ICA ネットワークプロトコルを使用してユーザー接続を確立するソフトウェアです。ユーザーは、ユーザーデバイスに Citrix Workspace アプリをインストールします。ユーザーが Windows ベースまたは Mac ベースのコンピューターに Citrix Workspace アプリをインストールすると、Citrix Workspace アプリは、ユーザー接続用の Citrix Gateway プラグインを含むすべてのプラグインをサブサバイサームします。Citrix Gateway は、Android 向け Citrix Workspace アプリと iOS 向け Citrix Workspace アプリからの接続もサポートしています。ユーザーは、Citrix Endpoint Management、StoreFront、または Web Interface を使用して、仮想デスクトップおよび Windows ベース、Web、モバイル、および SaaS アプリケーションに接続できます。
- Secure Hub とのユーザー接続。ユーザーは、Endpoint Management で設定されたモバイル、Web、および SaaS アプリケーションに接続できます。ユーザーは、モバイルデバイス（Android または iOS）に Secure Hub をインストールします。ユーザーは、Secure Hub にログオンすると、WorxMail と WorxWeb と、Endpoint Management にインストールした他のモバイルアプリをインストールできます。Secure Hub、Secure Mail、および WorxWeb は、マイクロ VPN テクノロジーを使用して Citrix Gateway を介して接続を確立します。
- Citrix Gateway プラグインをスタンドアロンアプリケーションとして使用するユーザー接続。Citrix Gateway プラグインは、ユーザーがユーザーデバイスにダウンロードしてインストールできるソフトウェアです。ユーザーがプラグインを使用してログオンすると、ユーザーはオフィスにいるかのようにセキュリティで保護されたネットワークのリソースにアクセスできます。リソースには、電子メールサーバー、ファイル共有、イントラネット Web サイトが含まれます。
- クライアントレスアクセスを使用したユーザ接続。クライアントレスアクセスにより、ユーザーはユーザーデバイスに Citrix Gateway プラグインや Citrix Workspace アプリなどのソフトウェアをインストールしなくても、必要なアクセスが可能になります。クライアントレスアクセスでは、Outlook Web Access や SharePoint などの限られた Web リソース、Citrix Virtual Apps で公開されたアプリケーション、Citrix Virtual Apps and Desktops からの仮想デスクトップ、アクセスインターフェイスを介してセキュアなネットワーク内のファイル共有に接続できます。ユーザーは、Web ブラウザで Citrix Gateway の Web アドレスを入力して接続し、選択ページでクライアントレスアクセスを選択します。
- 事前認証または認証後のスキャンが失敗した場合のユーザー接続。このシナリオは、アクセスシナリオのフォールバックと呼ばれます。アクセスシナリオのフォールバックでは、ユーザーデバイスが最初のエンドポイント分析スキャンに合格しなかった場合に、Citrix Workspace アプリを使用して、Citrix Gateway プラグインから StoreFront または Web Interface にフォールバックできます。

ユーザーが Citrix Workspace アプリを使用して Citrix Gateway にログオンすると、事前認証スキャンが機能しません。認証後のスキャンは、Citrix Gateway が VPN トンネルを確立するときに機能します。

ユーザーは、以下の方法で Citrix Gateway プラグインをダウンロードしてインストールできます。

- Web ブラウザーを使用して Citrix Gateway に接続する。
- Citrix Gateway 接続を受け入れるように構成された StoreFront への接続。
- グループポリシーオブジェクト (GPO) を使用してプラグインをインストールする。
- Citrix ADC プラグインを Merchandising Server アップロードする。

ユーザーアクセス用の **Citrix Gateway** プラグインの展開

March 26, 2020

Citrix Gateway には、ユーザーアクセス用の次のプラグインが付属しています。

- Windows 向け Citrix Gateway プラグイン
- Citrix Gateway plug-in for Mac
- Citrix Gateway plug-in for Java

ユーザーが Citrix Gateway に初めてログオンすると、Web ページから Citrix Gateway プラグインをダウンロードしてインストールします。ユーザーは、Windows ベースのコンピューターの通知領域にある Citrix Gateway アイコンをクリックしてログオンします。Mac OS X コンピュータでは、ユーザーは [Dock] メニューまたは [アプリケーション] メニューからログオンできます。Citrix Gateway を新しいソフトウェアバージョンにアップグレードすると、ユーザーデバイス上で Citrix Gateway プラグインが自動的に更新されます。

Java 用の Citrix Gateway プラグインは、Java をサポートする任意のユーザーデバイスで使用できます。Java 用の Citrix Gateway プラグインは、ほとんどの TCP ベースのアプリケーションをサポートしますが、Windows 用の Citrix Gateway プラグインまたは Mac OS X 用の Citrix Gateway プラグインの一部の機能のみを提供します。Java 用の Citrix Gateway プラグインを使用すると、ユーザーが定義したネットワークリソースへのアクセスが制限されます。Java プラグインの詳細については、[Java 用 Citrix Gateway プラグインを使用した接続。] を参照してください。(./ng-plugin-select-type/ng-connect-ng-plugin-java-configure-tsk.html)

Citrix Workspace アプリアップデーターを使用した **Citrix Gateway** プラグインの展開

また、Citrix Workspace アプリアップデーターを使用して、Citrix Gateway プラグインを展開することもできます。ユーザーが Citrix Workspace アプリ Updater をインストールすると、ユーザーデバイスにインストールされているすべてのユーザープラグインが Citrix Workspace アプリに自動的に追加されます。ユーザーは、Citrix Workspace アプリを使用して Citrix Gateway プラグインにログオンします。そのためには、Citrix Workspace アプリを開き、Citrix Gateway プラグインを右クリックし、［ログオン］をクリックします。Citrix Gateway アプライアンスを新しいバージョンにアップグレードすると、Citrix Workspace アプリ内の Citrix Gateway プラグインが自動的に新しいバージョンにアップグレードされます。

MSI インストーラーパッケージを使用した Citrix Gateway プラグインの展開

Citrix Gateway プラグインは、Microsoft Active Directory インフラストラクチャまたは標準のサードパーティ製 MSI 展開ツール（Windows サーバーアップデートサービスなど）を使用して展開できます。Windows インストーラーパッケージをサポートするツールを使用する場合は、MSI ファイルをサポートする任意のツールでパッケージを展開できます。次に、展開ツールを使用して、適切なユーザーデバイスにソフトウェアを展開してインストールします。

一元化された展開ツールを使用する利点は次のとおりです。

- セキュリティ要件を遵守する能力。たとえば、管理者以外のユーザーのソフトウェア・インストール権限を有効にせずに、ユーザー・ソフトウェアをインストールできます。
- ソフトウェアのバージョンを管理する。ソフトウェアの更新バージョンをすべてのユーザーに同時に展開できます。
- 拡張性。一元化された導入戦略は、追加のユーザーをサポートするように簡単に拡張できます。
- 優れたユーザーエクスペリエンス。このプロセスにユーザーを関与させることなく、インストール関連の問題を展開、テスト、およびトラブルシューティングできます。

ユーザーソフトウェアのインストールに対する管理制御が優先され、ユーザーデバイスへのアクセスがすぐに使用できる場合は、このオプションをお勧めします。

詳しくは、「Active Directory からの Citrix Gateway プラグインの展開」を参照してください。

展開するソフトウェアプラグインの決定

Citrix Gateway 環境でユーザーデバイス上にソフトウェアプラグインを必要としない場合は、クライアントレスアクセスが提供されていると見なされます。このシナリオでは、ユーザーはネットワークリソースにアクセスするのに Web ブラウザーのみが必要です。ただし、一部の機能では、ユーザーのデバイスにプラグインソフトウェアが必要です。

ユーザー用の Citrix Gateway プラグインの選択

March 26, 2020

Citrix Gateway を構成するときに、ユーザーのログオン方法を選択できます。ユーザーは、次のいずれかのプラグインを使用してログオンできます。

- Windows 向け Citrix Gateway プラグイン
- Citrix Gateway plug-in for Mac OS X
- Citrix Gateway plug-in for Java

構成を完了するには、セッション・ポリシーを作成し、ポリシーをユーザー、グループ、または仮想サーバーにバインドします。また、グローバル設定を構成してプラグインを有効にすることもできます。グローバルプロファイルま

たはセッションプロファイル内で、プラグインの種類として Windows/Mac OS X または Java のいずれかを選択します。ユーザーがログオンすると、グローバルに定義されたプラグインまたはセッションプロファイルとポリシーで定義されたプラグインを受け取ります。プラグインの種類ごとに個別のプロファイルを作成する必要があります。セッションプロファイルでは、「Windows/Mac OS X」または「Java」のいずれかを選択できます。Java 用に Citrix Gateway プラグインを構成する方法については、Java 用 Citrix Gateway プラグインを使用した接続を参照してください。

プラグインをグローバルに設定するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [クライアントエクスペリエンス] タブで、[プラグインの種類] の横にある [Windows/Mac OS X] を選択し、[OK] をクリックします。

セッションプロファイルで **Windows** または **Mac OS X** のプラグインタイプを設定するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 次のいずれかを行います:
   - 新しいセッションポリシーを作成する場合は、詳細ウィンドウで [追加] をクリックします。
   - 既存のポリシーを変更する場合は、ポリシーを選択して [開く] をクリックします。
3. 新しいプロファイルを作成するか、既存のプロファイルを修正します。これを行うには、次のいずれかの操作を行います。
   - [プロファイルの要求] の横にある [新規] をクリックします。
   - [プロファイルの要求] の横にある [変更] をクリックします。
4. [クライアントエクスペリエンス] タブで、[プラグインの種類] の横にある [グローバルにオーバーライド] をクリックし、[Windows/Mac OS X] を選択します。
5. 次のいずれかを行います:
   - 新しいプロファイルを作成する場合は、[Create] をクリックし、ポリシーダイアログボックスで式を設定し、[Create] をクリックして、[Close] をクリックします。
   - 既存のプロファイルを修正する場合は、選択後に [OK] を 2 回クリックします。

Windows 用の **Citrix Gateway** プラグインの傍受モードを設定するには

Windows 用の Citrix Gateway プラグインを構成する場合は、傍受モードを構成して透過モードに設定する必要があります。

1. 構成ユーティリティで、［構成］タブをクリックし、［Citrix Gateway］>［リソース］の順に展開し、［イントラネットアプリケーション］をクリックします。

2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [透明] をクリックします。
5.「プロトコル」で、「ANY」を選択します。
6. [宛先の種類] で、[IP アドレス] と [ネットマスク] を選択します。
7. に IP アドレスを入力します。
8. [ネットマスク] にサブネットマスクを入力し、[作成]、[閉じる] の順にクリックします。

Windows 用の Citrix Gateway プラグインのインストール

March 26, 2020

ユーザーが Citrix Gateway にログオンすると、ユーザーデバイスに Citrix Gateway プラグインをダウンロードしてインストールします。

プラグインをインストールするには、ユーザーがローカル管理者または Administrators グループのメンバーである必要があります。この制限は、初回インストールにのみ適用されます。プラグインのアップグレードには、管理者レベルのアクセスは必要ありません。

ユーザーが Citrix Gateway に接続して使用できるようにするには、次の情報を提供する必要があります。

- Citrix Gateway の Web アドレス（例：https://NetScalerGatewayFQDN/）
- エンドポイントリソースとポリシーを構成している場合、Citrix Gateway プラグインを実行するためのシステム要件

ユーザーデバイスの構成によっては、次の情報も提供する必要があります。

- ユーザーがコンピュータ上でファイアウォールを実行する場合、アクセスを許可したリソースに対応する IP アドレスとの間のトラフィックがファイアウォールによってブロックされないように、ファイアウォール設定を変更する必要がある場合があります。Citrix Gateway プラグインは、Windows XP のインターネット接続ファイアウォールと、Windows XP のサービスパック 2、Windows Vista、Windows 7、Windows 8、または Windows 8.1 の Windows ファイアウォールを自動的に処理します。
- Citrix Gateway 接続を介して FTP にトラフィックを送信するユーザーは、FTP アプリケーションをパッシブ転送するように設定する必要があります。パッシブ転送とは、リモートコンピュータが FTP サーバからリモートコンピュータへのデータ接続を確立するのではなく、FTP サーバへのデータ接続を確立することを意味します。
- 接続全体で X クライアントアプリケーションを実行するユーザーは、XManager などの X サーバーを自分のコンピューターで実行する必要があります。
- Receiver for Windows または Receiver for Mac をインストールするユーザーは、Citrix Gateway プラグインを Receiver から起動するか、Web ブラウザを使用して起動できます。Receiver または Web ブラウザを使用して Citrix Gateway プラグインを使用してログオンする方法についてユーザーに説明します。

ユーザーはファイルやアプリケーションを組織のネットワークに対してローカルであるかのように操作するため、ユーザーを再トレーニングしたり、アプリケーションを構成したりする必要はありません。

セキュリティで保護された接続を初めて確立するには、Web ログオンページを使用して Citrix Gateway にログオンします。Web アドレスの一般的な形式は、https://companyname.comです。ユーザーがログオンすると、Citrix Gateway プラグインをダウンロードしてコンピュータにインストールできます。

Windows 用の **Citrix Gateway** プラグインをインストールするには

1. Web ブラウザで、Citrix Gateway の Web アドレスを入力します。
2. ユーザー名とパスワードを入力し、[ログオン] をクリックします。
3. [ネットワークアクセス] を選択し、[ダウンロード] をクリックします。
4. 指示に従ってプラグインをインストールします。

ダウンロードが完了すると、Citrix Gateway プラグインが接続し、Windows ベースのコンピューターの通知領域にメッセージが表示されます。

ユーザーが Web ブラウザーを使用せずに Citrix Gateway プラグインを使用して接続できるようにする場合は、Windows ベースのコンピューターの通知領域で Citrix Gateway アイコンを右クリックするか、［スタート］メニューからプラグインを起動したときにログオンダイアログボックスを表示するようにプラグインを構成できます。

Windows 用の **Citrix Gateway** プラグインのログオンダイアログボックスを構成するには

ログオンダイアログボックスを使用するように Citrix Gateway プラグインを構成するには、この手順を完了するためにユーザーがログオンする必要があります。

1. Windows ベースのコンピューターの通知領域で Citrix Gateway のアイコンを右クリックし、［Citrix Gateway の構成］をクリックします。
2. [プロファイル] タブをクリックし、[プロファイルの変更] をクリックします。
3. ［オプション］タブで、［Citrix Gateway プラグインを使用してログオンする］をクリックします。
   注：ユーザーが Receiver 内から Citrix Gateway の
   構成］ダイアログボックスを開いた場合、［
   オプション］タブは使用できません。

Active Directory からの **Citrix Gateway** プラグインの展開

March 26, 2020

ユーザーデバイスに Citrix Gateway プラグインをインストールするための管理者権限がない場合は、Active Directory からユーザー用にプラグインを展開できます。

この方法を使用して Citrix Gateway プラグインを展開する場合、インストールプログラムを抽出し、グループポリシーを使用してプログラムを展開できます。このタイプの展開の一般的な手順は次のとおりです。

- MSI パッケージを抽出しています。
- グループポリシーを使用してプラグインを配布する。
- 配布ポイントを作成する。
- グループポリシーオブジェクトを使用して Citrix Gateway プラグインパッケージを割り当てます。
  注：Active Directory からの Citrix Gateway プラグインの配布は、Windows XP、Windows Vista、Windows 7 および Windows 8 でのみサポートされています。

MSI パッケージは、構成ユーティリティまたは Citrix の Web サイトからダウンロードできます。

構成ユーティリティから **Citrix Gateway** プラグインの **MSI** パッケージをダウンロードするには

1. 構成ユーティリティで、[ダウンロード] をクリックします。
2. ［Citrix Gateway プラグイン］で［Windows 用 Citrix Gateway プラグインのダウンロード］をクリックし、nsvpnc_setup.exe ファイルを Windows サーバーに保存します。

   注：[
   ファイルのダウンロード] ダイアログボックスが表示されない場合は、Ctrl キーを押しながら [Citrix Gateway Plugin for Windows
   をダウンロード] リンクをクリックします。
3. コマンドプロンプトで、nsvpnc_setup.exe を保存したフォルダに移動し、次のように入力します。

   setup /c

   これにより、agee.msi ファイルが抽出されます。
4. 解凍したファイルを Windows サーバ上のフォルダに保存します。

ファイルを抽出した後、Windows Server のグループポリシーを使用してファイルを配布します。

配布を開始する前に、グループポリシー管理コンソールを Windows Server 2003、Windows Server 2008、または Windows Server 2012 にインストールします。詳細については、Windows のオンラインヘルプを参照してください。

注：グループポリシーを使用して Citrix Gateway プラグインを公開する場合は、パッケージをユーザーデバイスに割り当てることをお勧めします。MSI パッケージは、デバイスごとにインストールされるように設計されています。

ソフトウェアを配布する前に、Microsoft インターネットセキュリティとアクセラレータ (ISA) サーバーなどの公開サーバー上のネットワーク共有に配布ポイントを作成します。

配布ポイントを作成するには

1. 管理者として公開サーバーにログオンします。

2. フォルダーを作成し、配布パッケージにアクセスする必要があるすべてのアカウントの読み取りアクセス許可を持つネットワーク上で共有します。
3. コマンドプロンプトで、解凍したファイルを保存するフォルダに移動し、「msiexec-a agee.msi」と入力します。
4. ［ネットワークの場所］画面で［変更］をクリックし、Citrix Gateway プラグインの管理インストールを作成する共有フォルダーに移動します。
5. [OK] をクリックし、[インストール] をクリックします。

展開したパッケージをネットワーク共有に配置した後、Windows のグループポリシーオブジェクトにパッケージを割り当てます。

Citrix Gateway プラグインを管理ソフトウェアパッケージとして正常に構成すると、ユーザーデバイスの次回起動時にプラグインが自動的にインストールされます。

> 注：インストールパッケージがコンピュータに割り当てられている場合、ユーザーはコンピュータを再起動する必要があります。

インストールが開始されると、Citrix Gateway プラグインがインストール中であることを示すメッセージが表示されます。

Active Directory を使用した **Citrix Gateway** プラグインのアップグレードと削除

March 26, 2020

Citrix Gateway プラグインの各リリースは、パッチとしてではなく、完全な製品インストールとしてパッケージ化されています。ユーザーがログオンし、Citrix Gateway プラグインが新しいバージョンのプラグインを検出すると、プラグインは自動的にアップグレードされます。また、Active Directory を使用してアップグレードするために Citrix Gateway プラグインを展開することもできます。

これを行うには、Citrix Gateway プラグイン用の新しい配布ポイントを作成します。新しいグループポリシーオブジェクトを作成し、新しいバージョンのプラグインを割り当てます。次に、新しいパッケージと既存のパッケージ間のリンクを作成します。リンクを作成すると、Citrix Gateway プラグインが更新されます。

ユーザーデバイスからの **Citrix Gateway** プラグインの削除

ユーザーデバイスから Citrix Gateway プラグインを削除するには、グループポリシーオブジェクトエディターから割り当てられたパッケージを削除します。

ユーザーデバイスからプラグインを削除すると、プラグインがアンインストール中であることを示すメッセージが表示されます。

Active Directory を使用した **Citrix Gateway** プラグインのインストールのトラブルシューティング

March 26, 2020

ユーザーデバイスの起動時に割り当てられたパッケージのインストールに失敗すると、アプリケーションイベントログに次の警告が表示されることがあります。

ソフトウェアのインストール設定に変更を適用できませんでした。管理者がグループポリシーのログオンの最適化を有効にしているため、ソフトウェアのインストールポリシーアプリケーションは、次のログオンまで遅れています。エラーは次のとおりです。グループポリシーフレームワークは、同期フォアグラウンドポリシーの更新で拡張を呼び出す必要があります。

このエラーは、Windows XP の高速ログオン最適化によって発生します。Windows XP では、グループポリシーオブジェクトの処理を含むすべてのネットワークコンポーネントをオペレーティングシステムが初期化する前にログオンできます。ポリシーによっては、有効にするには複数の再起動が必要になる場合があります。この問題を解決するには、Active Directory で高速ログオン最適化を無効にします。

管理対象ソフトウェアのインストールに関するその他の問題のトラブルシューティングを行うには、グループポリシーを使用して Windows インストーラログを有効にすることをお勧めします。

Java 用 **Citrix Gateway** プラグインを使用した接続

March 26, 2020

Java 用の Citrix Gateway プラグインは、Java をサポートする任意のユーザーデバイスで使用できます。

> 注: Java ランタイム環境（JRE）バージョン 1.4.2 から最新バージョンの JRE まで、次のオペレーティング・システムおよび Web ブラウザが必要です。

- Mac OS X
- Linux
- Windows XP（すべてのバージョン）、Windows Vista、Windows 7、Windows 8
- Internet Explorer
- Firefox
- ウェブブラウザの最新バージョンに Safari 1.2 まで

Java 用の Citrix Gateway プラグインは、ほとんどの TCP ベースのアプリケーションをサポートしますが、Windows 用の Citrix Gateway プラグインまたは Mac OS X 用の Citrix Gateway プラグインの一部の機能のみを提供します。

Java 用 Citrix Gateway プラグインを使用するために、ユーザーデバイスに対する管理者権限は必要ありません。セキュリティ上の理由から、使用するユーザーデバイスに関係なく、特定の仮想サーバー、グループ、またはユーザー

に対してこのプラグインバージョンを使用する必要がある場合があります。

ユーザーデバイスに Citrix Gateway way プラグインをインストールするように Citrix Gateway を構成するには、セッションポリシーを構成し、仮想サーバー、グループ、またはユーザーにバインドします。

ユーザーが Windows 7 を実行しているコンピューターからログオンした場合、Internet Explorer でプロキシサーバーの情報は自動的には設定されません。ユーザーは、Windows 7 を実行しているコンピューターでプロキシサーバーを手動で構成する必要があります。

Java 用に **Citrix Gateway** プラグインを構成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウで、[プロファイル] タブをクリックします。
3. セッションプロファイルを選択し、[開く] をクリックします。
4. [クライアントエクスペリエンス] タブで、[プラグインの種類] の横にある [グローバル上書き] をクリックし、[Java] を選択して [OK] をクリックします。

インターセプションモードを設定するには

セッションポリシーを作成したら、イントラネットアプリケーションを作成して、Citrix Gateway プラグイン for Java でログオンするユーザーの傍受モードを定義します。

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［リソース］の順に展開し、［イントラネットアプリケーション］をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前] ボックスに名前を入力します。
4. [プロキシ] をクリックします。
5. [宛先 IP アドレス] に IP アドレスを入力します。
6. [宛先ポート] に、ポート番号を入力します。
7. [送信元 IP アドレス] に IP アドレスを入力します。
8. [ソースポート] にポート番号を入力し、[作成]、[閉じる] の順にクリックします。

送信元 IP アドレスとポート番号を指定しない場合、Citrix Gateway では IP アドレスに 127.0.0.1、ポートに 0 が自動的に使用されます。

Windows ベースのコンピュータでの **HOSTS** ファイルの更新

ユーザーが Windows Vista、Windows 7、または Windows 8 を実行しているコンピューターで Java 用の Citrix Gateway プラグインを使用してログオンすると、TCP イントラネットアプリケーションのネットワークトラフィックはトンネリングされません。HOSTS ファイルは、Vista および Windows 7 を実行しているコンピューターでは自動的に更新されません。イントラネットアプリケーションを HOSTS ファイルに手動で追加する必要があります。

Windows ベースのコンピュータでは、メモ帳などのテキストエディタで HOSTS ファイルを編集できます。HOSTS ファイルをメモ帳で編集する場合は、管理者としてメモ帳を実行する必要があります。Java 用 Citrix Gateway プラグイン用のイントラネットアプリケーションのマッピングエントリを追加し、ファイルを保存します。

Citrix Gateway プラグインと Citrix Workspace アプリの統合

April 9, 2020

Citrix Gateway は、Citrix Workspace アプリをサポートしています. オーケストレーションされたシステムは、次のコンポーネントで構成されています。

- Windows 向け Citrix Workspace アプリ 3.4 以降
- Mac 向け Citrix Workspace アプリ
- Android 向け Citrix Workspace アプリ
- iOS 向け Citrix Workspace アプリ
- StoreFront 2.1 以降
- アプリケーションコントローラー 2.8 以降または Citrix Endpoint Management 10
- シトリックスの Web サイトでホストされている Citrix アップデートサービス

Citrix 製品との Citrix Gateway の互換性について詳しくは、「Citrix 製品との互換性」を参照してください。

ユーザーがアプライアンスにログオンしたときに、Citrix Gateway プラグインによって Web ブラウザが開き、Citrix Workspace アプリホームページにシングルサインオンできるよう、Citrix Gateway を構成できます。ユーザーは、ホームページから Citrix Workspace アプリをダウンロードできます。

ユーザーが Citrix Workspace アプリでログオンすると、ユーザー接続は次の方法で Citrix Gateway 経由でルーティングできます。

- Endpoint Management へのダイレクト
- StoreFront に直接
- Endpoint Management で MDX モバイルアプリを構成しない場合、StoreFront と Endpoint Management
- Endpoint Management で MDX モバイルアプリを構成する場合は、Endpoint Management から StoreFront へ

注**:** Endpoint Management に直接ルーティングされる接続は、AppController 2.0、AppController 2.5、AppController 2.6、アプリケーションコントローラー 2.8、およびアプリケーションコントローラー 2.9 でのみサポートされます。AppController 1.1 をネットワークに展開している場合、ユーザー接続は StoreFront 経由でルーティングする必要があります。

ユーザー接続と **Citrix Workspace** アプリの仕組み

March 26, 2020

ユーザーは、Citrix Workspace アプリから次のアプリ、デスクトップ、およびデータに接続できます。

- StoreFront および Web Interface で公開された Windows ベースのアプリケーションおよび仮想デスクトップ
- Citrix Endpoint Management を介してアクセスされる ShareFile データ

ユーザーは、次の Citrix Workspace アプリのいずれかを使用してログオンできます。

- Web 向け Citrix Workspace アプリ
- Windows 向け Citrix Workspace アプリ
- Mac 向け Citrix Workspace アプリ
- iOS 向け Citrix Workspace アプリ
- Android 向け Citrix Workspace アプリ

ユーザーは、Web ブラウザーまたはユーザーデバイスの Citrix Workspace アプリのアイコンを使用して、Web 用 Citrix Workspace アプリでログオンできます。

ユーザーが Citrix Workspace アプリの任意のバージョンでログオンすると、アプリケーション、ShareFile データ、およびデスクトップがブラウザまたは Citrix Workspace アプリのウィンドウに表示されます。

Citrix Workspace アプリへの **Citrix Gateway** プラグインの追加

March 26, 2020

ユーザーデバイスに Citrix Workspace アプリをインストールすると、ユーザーは Citrix Workspace アプリを介して Citrix Gateway プラグインを使用してログオンできます。Citrix Gateway プラグインを Merchandising Server アップロードすると、プラグインがユーザーデバイスの Citrix Workspace アプリにダウンロードされてインストールされます。ユーザーが Citrix Workspace アプリを初めてインストールするときに Citrix Gateway プラグインをインストールしている場合、プラグインは自動的に Citrix Workspace アプリに追加されます。

ユーザーデバイスへのプラグインの配信

プラグインをユーザーデバイスに配信するには、Merchandising Server に Citrix Gateway プラグインをアップロードして構成する必要があります。ユーザーが選択すると、プラグインは Merchandising Server からダウンロードおよびインストールされます。

ユーザーが Citrix Gateway プラグインをインストールした後、Citrix Workspace アプリをインストールすると、Citrix Workspace アプリのインストールが完了すると、Citrix Workspace アプリのメニューに Citrix Gateway プラグインが表示されます。

ユーザーが Windows 用の Citrix Workspace アプリを持っている場合、ユーザーは Windows 用の Citrix Workspace アプリアップデーターをインストールできます。これは、プラグインを更新し、Merchandising Server と通信するオプションのコンポーネントです。Citrix Workspace アプリには、Citrix Gateway プラグインを含め、配信可能なすべてのプラグインが含まれています。Windows 用 Citrix Workspace アプリアップデーターの詳細については、Citrix eDocs ライブラリにある Citrix Workspace アプリとプラグインのセクションを参照してください。

Citrix Workspace アプリを使用した **Citrix Gateway** への接続

ユーザーが Windows 用の Citrix Workspace アプリに接続する場合、通知領域で Citrix Workspace アプリのアイコンを右クリックし、［環境設定］をクリックして、［プラグインの状態］をクリックします。Citrix Gateway プラグインがユーザーデバイスにインストールされている場合、ユーザーは Citrix Gateway プラグインを右クリックし、［ログオン］をクリックします。認証が成功すると、Citrix Gateway プラグインは Citrix Gateway への接続を確立し、完全な VPN トンネルを確立します。

ユーザーは、Web ブラウザを使用してログオンすることもできます。ユーザーは、Citrix Gateway の完全修飾ドメイン名（FQDN）を入力し、ログオンします。Citrix Gateway が接続を確立すると、ユーザーは Citrix Workspace アプリの［環境設定］>［プラグインのステータス］パネルで接続を確認できます。

Citrix Gateway の Web アドレスは、Merchandising Server で構成されたメタデータの一部であり、ユーザーはアドレスを変更できません。Citrix Gateway プラグインにより、Citrix Gateway へのログオンが開始されます。ユーザーデバイスにインストールされている Windows 用の Citrix Gateway プラグインのバージョンが Citrix Gateway アプライアンスのバージョンと異なる場合は、ユーザーがログオンしたときにプラグインが自動的にダウングレードまたはアップグレードされます。Mac OS X 用の Citrix Gateway プラグインは自動的にダウングレードされません。以前のバージョンのプラグインを Mac コンピュータにインストールするには、まず Citrix Gateway プラグインをアンインストールしてから、Citrix Gateway から以前のバージョンをダウンロードする必要があります。

Citrix Gateway プラグインのアップグレードまたはダウングレード

Citrix Gateway プラグインのアップグレードまたはダウングレード中に、アプライアンスは正しいバージョンのプラグインを削除、ダウンロード、インストールします。ユーザーは、Citrix Workspace アプリの［環境設定］>［プラグインのステータス］パネルでプラグインのエントリを確認することで、新しいインストールを確認できます。新しくインストールした Citrix Gateway プラグインのバージョンは、Merchandising Server で設定したバージョンとは異なる場合があります。

Citrix Gateway プラグインを **Merchandising Server** に追加する

また、Citrix Gateway プラグインの配信を Merchandising Server で構成することもできます。マーチャンダイジングサーバーでは、Citrix Gateway プラグインの MSI インストールパッケージをアップロードできる Web 構成インターフェイスが提供されます。Merchandising Server では、次の操作を実行できます。

- Citrix Gateway プラグインのバージョンとメタデータを指定します。

- Citrix Gateway アプライアンスの 1 つまたは複数の Web アドレスを構成します。
- オペレーティングシステムまたはその他のパラメータに基づいて特定のルールを関連付けます。

> ユーザーは、Merchandising Server で構成されたサーバーのリストからサーバーを追加または削除することはできませんが、Citrix Workspace アプリのネットワーク設定パネルの構成済みリストから別のサーバーを選択することはできます。

アクセスシナリオのフォールバックまたは負荷分散を使用している場合は、Citrix Gateway の Web アドレスの固定セットを構成し、Merchandising Server デフォルトのアドレスとして指定することができます。ユーザーは、Citrix Workspace アプリのメニューから［ログオン］を選択すると、デフォルトのサーバーに接続します。ユーザーは、Citrix Workspace アプリの［環境設定］>［ネットワーク設定］パネルを使用して、表示されたリストから別のアドレスを選択できます。

ユーザーは、引き続き Web ブラウザーを使用して任意の Citrix Gateway にログオンできます。ユーザーが Web ブラウザーを使用してログオンすると、Citrix Gateway プラグインは自動的に Citrix Gateway のバージョンにアップグレードまたはダウングレードされます。

以下に、Citrix Gateway プラグインを Merchandising Server に追加する一般的な手順を示します。具体的な構成手順については、Citrix eDocs ライブラリの「テクノロジー」セクションの「Merchandising Server」を参照してください。

- Merchandising Server 管理コンソールの [全般] タブで設定を構成します。
- Citrix Gateway プラグインを Merchandising Server に追加します。
- ターゲット・プラットフォームに適したプラグイン・バージョンを選択します。Citrix Gateway プラグインを商品配信に追加ページにプラグインを表示するには、Merchandising Server メインページに追加する必要があります。
- Citrix Gateway プラグインの配信を構成します。
- Citrix Gateway の Web アドレスを識別する場所のわかりやすい名前を使用します。この名前は、Citrix Workspace アプリに表示されます。Citrix Gateway アプライアンスを追加することもできます。
- 認証の種類を指定し、ユーザー名、パスワード、暗証番号（PIN）など、Citrix Workspace アプリのログオンダイアログボックスに表示される特定のラベルをカスタマイズします。
- 配送のルールを追加します。
- [配信へのルールの追加] ページにルールを表示する場合は、ルールを作成する必要があります。
- 配送のスケジュールを設定します。

Citrix Workspace アプリのアイコンの切り離し

March 26, 2020

Citrix Workspace アプリと統合された Citrix Gateway プラグインを使用して Citrix Virtual Apps and Desktops 展開を構成すると、VPN に接続しているユーザーにはプラグインのアイコンが表示されません。Citrix Gateway のプラグインアイコンは、通常、Windows のシステムトレイまたは Mac OS X Finder のメニューバーにあります。このアイコンは、プラグインの設定とコントロールへのインタフェースです。Windows ユーザーの場合、Citrix Workspace アプリと Citrix Gateway プラグインが統合されている場合、Citrix Workspace アプリの［バージョン情報］ダイアログに、Citrix Gateway プラグインのコントロールが表示されます。Mac OS X ユーザーの場合、統合後に使用できる Citrix Gateway プラグインのコントロールはありません。

一部の統合デプロイメントでは、基盤となる機能の統合を維持しながら、プラグインのコントロールを公開する必要がある場合があります。これを行うには、以下の CLI コマンドまたは Citrix ADC 構成ユーティリティータスクを使用して、VPN クライアントのアイコン統合を切り替えます。

コマンドラインを使用したアイコン統合の設定

次のコマンドを使用します:

```
set vpn parameter [-iconWithReceiver (ON/OFF)]

<!--NeedCopy-->
```

構成ユーティリティを使用したアイコン統合の設定

Citrix ADC 構成ユーティリティを使用して、次の操作を行います。

1. ［構成］タブで、Citrix Gateway > ［グローバル設定］に移動します。
2. [グローバル設定の変更] をクリックし、[クライアントエクスペリエンス] タブを選択します。
3. [詳細設定] をクリックします。
4. ［Citrix Workspace アプリで VPN プラグインアイコンを表示する］を選択します。

ICA 接続用の IPv6 の構成

March 26, 2020

Citrix Gateway は、ICA 接続用の IPv6 アドレスをサポートします。IPv6 を使用した Web Interface または StoreFront への接続は、IPv4 接続と同じように機能します。ユーザーが Citrix Gateway の Web アドレスを使用して接続すると、Citrix Gateway は Web Interface または StoreFront への接続をプロキシします。

1 つの DMZ に展開された Citrix Gateway またはダブルホップ DMZ に展開された Citrix Gateway 用に IPv6 を構成できます。

Citrix Gateway で IPv6 を有効にするには、コマンドラインを使用します。次のガイドラインを使用できます。

- アプライアンスで IPv6 を有効にします。
- サブネット IP アドレスを設定します。
- DNS 解決の順序を設定します。
- Web Interface または StoreFront の Web アドレスを設定します。
- Secure Ticket Authority（STA）を Citrix Gateway にバインドします。

デフォルトでは、マッピング IP アドレスは IPv6 アドレスをサポートしません。ユーザー通信を内部ネットワークにルーティングするには、サブネット IP アドレスを作成し、サブネット IP アドレスを使用するように Citrix Gateway を設定する必要があります。

ネットワーク内に複数の IPv6 サブネットを展開する場合は、Citrix Gateway で、ネットワーク上の各サブネットに対して複数の IPv6 サブネット IP アドレスを作成します。ネットワークルーティングは、サブネット IP アドレスを使用して IPv6 パケットをそれぞれのサブネットに送信します。

ICA プロキシ用に IPv6 を構成するには

ICA プロキシ用に IPv6 を構成するには:

1. PuTTY などのセキュアシェル（SSH）接続を使用して、Citrix Gateway にログオンします。
2. コマンドプロンプトで、ns 機能を有効にする IPv6PT と入力します。これにより、IPv6 が有効になります。
3. コマンドプロンプトで、ns モードを有効にする USNIP と入力します。これにより、サブネット IP アドレスの使用が可能になります。
4. コマンドプロンプトで、次のように入力します。**set dns parameter –resolutionOrder AAAA-ThenAQuery AThenAAAAQuery OnlyAAAAQuery OnlyAQuery**
5. コマンドプロンプトで、「**set vpn parameter -wihome** `http://XD_domain/Citrix/StoreWeb`」と入力します。

ここで、<XD_domain> は StoreFront のドメイン名または IP アドレスです。

たとえば、**set vpn parameter -wihome** `http://storefront.domain.com/Citrix/StoreWeb`。

または

set vpn parameter -wihome `http://[1000:2000::3000]/Citrix/StoreWeb`

> IPv6 アドレスを使用してこのパラメータを構成する場合は、IP アドレスを括弧で囲む必要があります。

CitrixCitrix Gateway での Citrix Workspace アプリのホームページの構成

March 26, 2020

Citrix Workspace アプリのホームページは、グローバルに構成することも、セッションプロファイルの一部として構成することもできます。Citrix Workspace Gateway 経由で StoreFront を認識しない Web およびそれ以前のバージョンの Citrix Workspace アプリ用に Citrix Workspace アプリを構成する場合は、2 つのセッションプロファイルを個別に作成する必要があります。Citrix Workspace アプリのホームページには、ユーザーが正常にログオンできるように、各プロファイルの正しい Web アドレスが必要です。

Citrix Gateway を介して StoreFront を認識する Citrix Workspace アプリの場合、Web 用 Citrix Workspace アプリと Citrix Workspace アプリでプロファイルを共有できます。ただし、Web 用 Citrix Workspace アプリ用にセッションプロファイルを構成し、他のすべての Citrix Workspace アプリ用に個別のセッションプロファイルを構成することをお勧めします。

Citrix Workspace アプリのホームページをグローバルに設定するには

Citrix Workspace アプリのホームページをグローバルに設定するには:

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. ［グローバル Citrix Gateway 設定］ダイアログボックスで、［公開アプリケーション］タブをクリックします。
4. Citrix Workspace アプリのホームページで、Citrix Workspace アプリまたは Web ホームページの Citrix Workspace アプリ用の Web アドレスを入力し、「OK」をクリックします。

セッションプロファイルで **Citrix Workspace** アプリのホームページを構成するには

セッションプロファイルで Citrix Workspace アプリのホームページを構成するには:

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［**Citrix Gateway**］**>** ［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウの [プロファイル] タブで、[追加] をクリックします。
3. **Citrix Gateway** セッションプロファイルの作成］ダイアログボックスの［公開アプリケーション］タブで、［**Citrix Receiver** のホームページ］の横にある［グローバル上書き］をクリックします。
4. Citrix Workspace アプリのホームページで、Citrix Workspace アプリまたは Web ホームページの Citrix Workspace アプリの Web アドレスを入力し、「作成」をクリックします。

ログオン・ページへの **Receiver** テーマの適用

March 26, 2020

構成ユーティリティを使用して、Citrix Gateway のログオンページに Receiver テーマを適用できます。Receiver テーマ、デフォルトテーマ、または作成したカスタムテーマを切り替えることができます。この機能は、以下の Citrix Gateway バージョンで使用できます。

- Citrix Gateway 10.1 以降のバージョンです。
- Access Gateway 10、ビルド 71.6014.e
- Access Gateway 10、ビルド 73.5002.e

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. ［グローバル Citrix Gateway 設定］ダイアログボックスで、［クライアントエクスペリエンス］タブをクリックします。
4. [UI テーマ] の横にある [緑の泡] をクリックし、[OK] をクリックします。

   このコマンドは、元のログオンページを Receiver テーマで上書きします。注: 別のテーマを適用した後、キャッシュされたページが表示されないようにブラウザのキャッシュをクリアするようにユーザーに助言します。

ログオン・ページのカスタム・テーマの作成

March 26, 2020

構成ユーティリティを使用して、Citrix Gateway のログオンページのカスタムテーマを作成できます。デフォルトのテーマを使用することも、Citrix Workspace アプリのテーマを使用することもできます。ログオンページにカスタムテーマを適用する場合は、Citrix Gateway コマンドラインを使用してテーマを作成して展開します。次に、構成ユーティリティを使用して、カスタムテーマページを設定します。

カスタムテーマページは、Citrix Gateway のグローバル設定を使用して構成します。

この機能は、以下のバージョンの Citrix Gateway で使用できます。

- Citrix Gateway 10.1
- Access Gateway 10、ビルド 73.5002.e (アプリケーションコントローラーのバージョン 2.5、2.6、または 2.8 でこの機能を使用するには、ビルド 71.6104.e の後にこのビルドをインストールする必要があります)
- Access Gateway 10、ビルド 71.6104.e

コマンドラインを使用してカスタムテーマを作成して展開する

コマンドラインを使用してカスタムテーマを作成して展開するには:

1. Citrix Gateway のコマンドラインにログオンします。

2. コマンドプロンプトで shell と入力します。
3. コマンドプロンプトで mkdir /var/ns_gui_custom; cd /netscaler; tar -cvzf /var/ns_gui_custom/customtheme.tar ns_gui/* と入力します。
4. 構成ユーティリティを使用してカスタムテーマに切り替え、/var/ns_gui_custom/ns_gui/vpn でカスタマイズを変更します。次の操作を実行できます:
   - css/ctx.authentication.css ファイルを編集します。
   - カスタムロゴを /var/ns_gui_custom/ns_gui/vpn/メディアフォルダにコピーします。注**:** WinSCP を使用してファイルを転送できます。
5. 複数の Citrix Gateway アプライアンスがある場合は、すべてのアプライアンスに対して手順 3 と 4 を繰り返します。

ユーザーポータルのカスタマイズ

March 26, 2020

VPN ユーザーにポータルを提供する Citrix Gateway のインストールには、ポータルのテーマを選択してポータルページの外観をカスタマイズするオプションがあります。用意されているテーマのセットから選択するか、テーマをテンプレートとして使用して、カスタマイズまたはブランド化されたポータルを構築できます。構成ユーティリティーを使用して、新しいロゴ、背景画像、カスタム入力ボックスラベル、および CSS ベースのポータルデザインのさまざまな属性を追加することで、テーマを変更できます。組み込みのポータル・テーマには、英語、フランス語、スペイン語、ドイツ語、日本語の 5 つの言語のコンテンツが含まれます。Web ブラウザによって報告されるロケールに応じて、異なるユーザーが異なる言語で提供されます。

VPN ユーザがサインインを許可する前に VPN ユーザに提示されるカスタムのエンドユーザー使用許諾契約（EULA）を作成するオプションがあります。EULA 機能は、ロケール固有のバージョンの EULA をサポートします。EULA は、Web ブラウザで報告されたロケールに基づいてユーザに提示されます。

ポータルテーマと EULA 構成の両方は、VPN 仮想サーバーおよび VPN グローバルレベルで個別にバインドできます。

> 重要： Citrix では、コードの変更が必要なカスタマイズはサポートされておらず、デフォルトのテーマに戻す以外の問題を解決するためのサポートも提供していません。

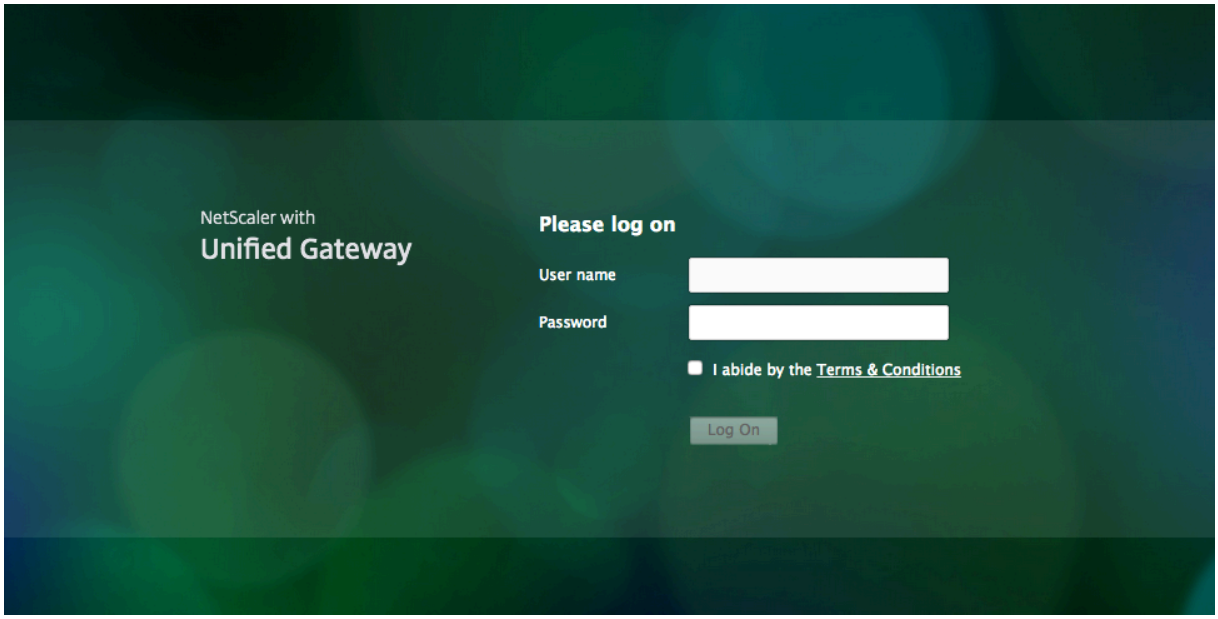
ポータル・テーマの適用

デフォルトでは、VPN ポータルは Caxton テーマを使用するように構成されています。Caxton テーマの名前は Default です。

Caxton Theme

Citrix Gateway には、ポータルに適用できる 2 つのテーマがあります。グリーンバブルと X1 のテーマです。

Greenbubble Theme



X1 Theme

提供されたテーマは、VPN 仮想サーバに直接適用することも、グローバル VPN バインディングとして適用することもできます。

VPN 仮想サーバーへのポータルテーマのバインド

ポータル・テーマは、既存の仮想サーバー上または新しい仮想サーバーの作成時にバインドできます。

コマンドラインを使用してポータル・テーマを既存の **VPN** 仮想サーバーにバインドする

コマンドプロンプトで、「;」と入力します。

```
bind vpn vserver <name> - portaltheme <name>
<!--NeedCopy-->
```

構成ユーティリティーを使用したポータル・テーマの既存の **VPN** 仮想サーバーへのバインド

1. ［構成］タブで［**Citrix Gateway**］に移動し、［仮想サーバー］をクリックします。
2. 仮想サーバーを選択し、[編集] をクリックします。
3. ポータル・テーマがまだ仮想サーバーにバインドされていない場合は、詳細ペインの [詳細設定] の [ポータル・テーマ] をクリックします。それ以外の場合、[ポータルのテーマ] オプションは詳細ペインで既に展開されています。
4. 詳細ペインの [ポータル・テーマ**]** で、**[**ポータル・テーマ なし**]** をクリックして **[**ポータル・テーマ・バインディング] ウィンドウを展開します。
5. [クリックして選択**]** をクリックします。
6. [ポータルテーマ] ウィンドウで、テーマ名をクリックし、[選択] をクリックします。
7. ［バインド］をクリックします。
8. ［完了］をクリックします。

VPN 仮想サーバーを作成する場合は、VPN 仮想サーバーの編集ペインで、上記の手順 3 から開始して、ポータルのテーマをバインドできます。

VPN グローバルへのポータルテーマのバインド

コマンドラインを使用したポータル・テーマの **VPN** グローバル・スコープへのバインド

コマンドプロンプトで、「;」と入力します。

```
bind vpn global portaltheme <name>
<!--NeedCopy-->
```

構成ユーティリティーを使用したポータル・テーマの **VPN** グローバル・スコープへのバインド

1. ［構成］タブで［**Citrix Gateway** に移動します。
2. メインの詳細ペインで、［**Citrix Gateway** ポリシーマネージャー］をクリックします。
3. 「**+**」アイコンをクリックします。

4. 「バインドポイント」リストで、「リソース」を選択します。
5. 「接続タイプ」リストで、「ポータル・テーマ」を選択します。
6. ［続行］をクリックします。
7. 「バインドポイント」画面で、「バインドの追加」をクリックします。
8. [クリックして選択] をクリックします。
9. [ポータルテーマ] ウィンドウで、テーマ名をクリックし、[選択] をクリックします。
10. ［バインド］をクリックします。
11. ［閉じる］をクリックします。
12. [完了] をクリックします。

> ヒント：一連の変更が完了したら、コマンドラインで「save ns config」コマンドを使用するか、構成ユーティリティの保存アイコンをクリックして、変更内容が Citrix ADC 構成ファイルに保存されます。

ポータル・テーマの作成

カスタム・ポータル・デザインを作成するには、提供されているポータル・テーマの 1 つをテンプレートとして使用します。選択したテンプレートテーマのコピーが、指定した名前で作成されます。

在庫ポータル・テーマのカスタム・ポータル・テーマのテンプレートとしての使用

ポータル・テーマを作成するには、構成ユーティリティーまたはコマンド・ラインを使用してテーマ・エンティティーを作成します。ただし、詳細なカスタマイズコントロールは、構成ユーティリティ内でのみ使用できます。

コマンド・ラインを使用したポータル・テーマの作成

コマンドプロンプトで、「;」と入力します。

```
1 add portaltheme <name> basetheme <name>
2 <!--NeedCopy-->
```

構成ユーティリティーを使用したポータル・テーマの作成

1. ［構成］タブで ［**Citrix Gateway**］に移動し、［ポータルのテーマ］をクリックします。
2. メインの詳細ウィンドウで、[追加] をクリックします。
3. テーマの名前を入力し、テンプレートリストからテンプレートを選択し、[**OK**] をクリックします。
4. この時点で、ポータル・テーマ編集ウィンドウの初回ビューが表示されます。［**OK**］をクリックして終了します。

最初のビューを使用して、新しいポータル・テーマのカスタマイズに進むことができます。ただし、ポータル・テーマの編集を続行する前に、インターフェースに関する次のポータル・テーマのカスタマイズセクション、およびインターフェース内のカスタマイズ可能なポータル属性のポップアップの説明をお読みください。

新しいテーマが作成されたら、VPN 仮想サーバーへのポータルテーマのバインドまたはVPN グローバルへのポータルテーマのバインドの説明に従ってバインドできます。新しいテーマは、作成後またはカスタマイズ完了後すぐにバインドできます。

ポータル・テーマのカスタマイズ

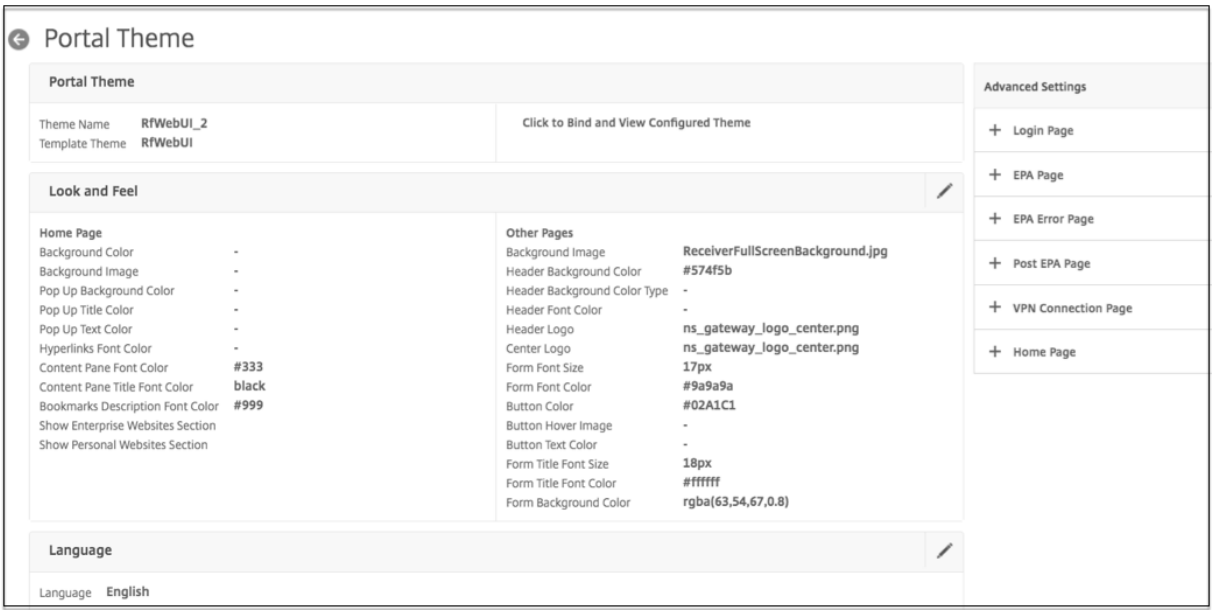
ポータル・テーマをカスタマイズするには、構成ユーティリティーのポータル・テーマ・インターフェースを使用します。最良の結果を得るには、このインタフェースを使用する前に、このインタフェースのさまざまな要素を理解しておく必要があります。

ポータル・テーマ・インタフェースについて

Citrix Gateway 構成ユーティリティで ポータルのテーマインターフェイスを開くには、［構成］タブで ［**Citrix Gateway**］に移動し、［ポータルのテーマ］をクリックします。「ポータル・テーマの作成」の説明に従ってテーマを作成するか、メインの詳細ペインで既存のテーマを選択して「編集」をクリックします。

ポータル・テーマのカスタマイズ・ページには、ポータル・デザインを変更するための 4 つの主要なコンポーネント・ペインがあります。「ポータル・テーマ」ペイン、「ルック・アンド・フィール」ペイン、「詳細設定」ペイン、および「言語」ペインです。

ポータル・テーマ・インタフェース



ページ上部の「ポータル・テーマ」ペインには、編集用にロードされたテーマと、それが基づいているテンプレート・テーマが示されます。ここでの表示オプションを使用すると、ユーザー接続で VPN にアクセスすることなく、カスタマイズ内容を表示できます。表示オプションを使用するには、テーマを VPN 仮想サーバにバインドする必要があります。バインディングは、表示ウィンドウを閉じた後も有効です。

ページの中央にある [ルック **&** フィール] ペインで、ヘッダー、背景色と画像、フォントのプロパティ、ロゴなど、テーマの全般プロパティを構成します。このペインが編集モードの場合、属性凡例を使用して、ポータル・ページで Look & Feel 属性が使用される場所に関するガイダンスを使用できます。

[詳細設定**]** ペインには、個々のポータルページの画面上のコンテンツコントロールが表示されます。編集用にページのコンテンツを読み込むには、一覧表示されているページの 1 つをクリックします。ページコントロールは、他の中央のペインの下に表示されます。ページが変更されていない限り、ポータル・テーマの編集を行っても、[詳細設定**]** ペインでページが折りたたまれたままになります。

[言語] ペインでは、[詳細設定] ペインで編集対象のページを選択したときにロードする言語を選択できます。デフォルトでは、英語のページが読み込まれます。

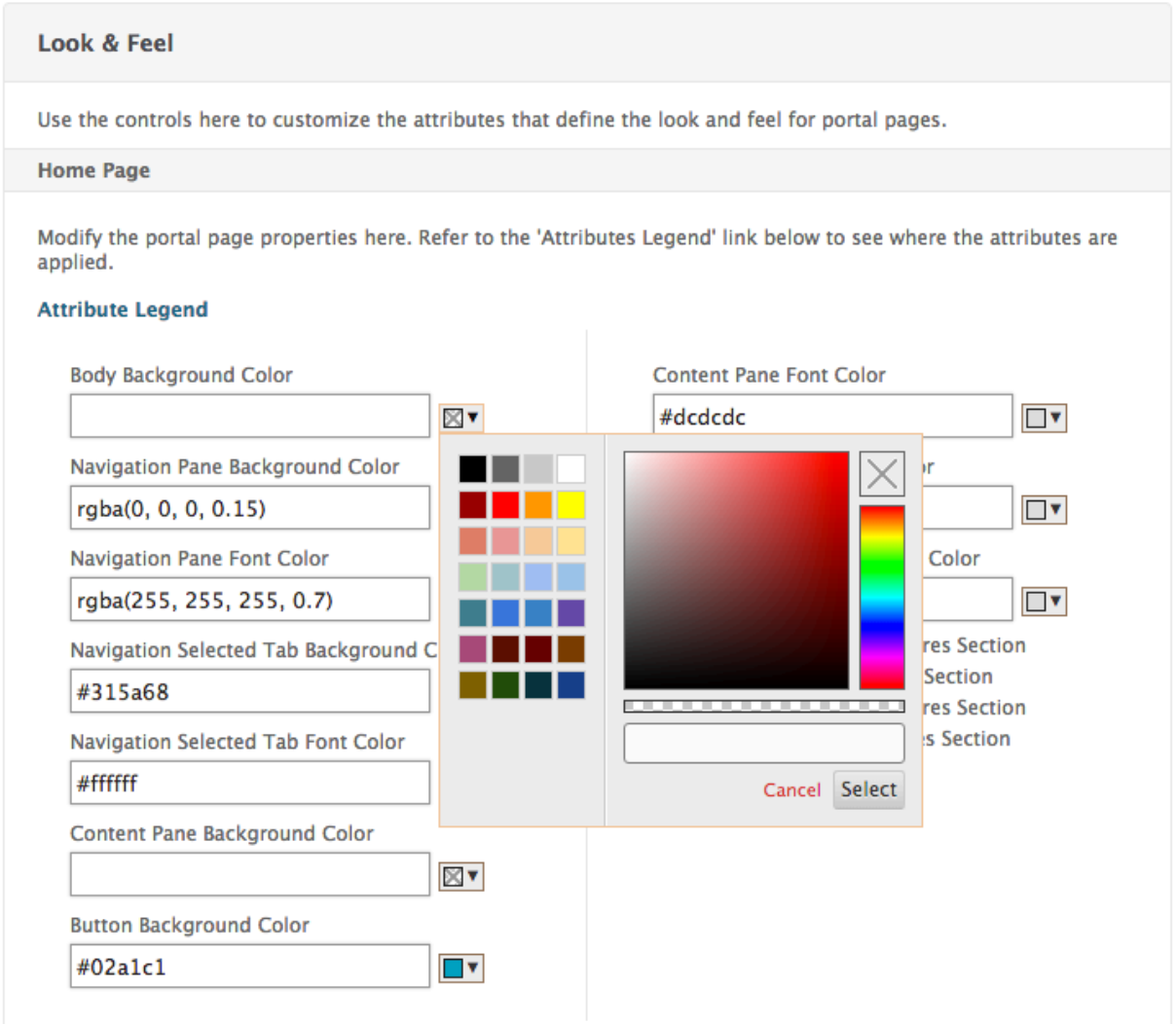
カスタマイズ可能なページ属性のタイプ

ポータル・テーマをカスタマイズする場合、ポータル・テーマ・インタフェースで属性の範囲を変更できます。編集可能なテキストとサポートされている言語に加えて、ポータルのレイアウトのすべてのグラフィック要素をニーズに合わせて調整できます。各ページ要素タイプには、変更する前に考慮すべきパラメータまたは推奨事項があります。

色

ポータルデザインでは、ページの背景、ハイライト、タイトルと本文コンテンツのテキスト、ボタンコントロール、ホバー応答などの属性の色を指定します。カラー属性をカスタマイズするには、選択した項目のカラー値を直接入力するか、付属のカラーピッカーを使用してカラー値を生成します。このインターフェイスでは、有効な HTML カラー値を RGBA 形式、HTML の 16 進数トリプレット形式、および X11 カラー名で入力できます。カラーピッカーは、アトリビュートの入力フィールドの横にあるカラーボックスをクリックすることで、適用可能なカラーアトリビュートに対してアクセスできます。

カラーピッカー



フォント

フォントの色に加えて、一部のページ属性のフォントサイズを変更できます。これらの属性ごとに、ポータルの設計によって決定される各属性で使用できるサイズがメニューに表示されます。

画像

画像の場合、各コントロールで使用できるポップアップの説明に、推奨サイズやその他の要件が表示されます。説明は、ページ上の属性の場所とその機能によって異なります。PNG または JPEG イメージファイル形式を使用できます。アップロードするイメージを選択するには、アイテムのファイル名の下にあるチェックボックスをオンにし、ローカルコンピュータのドライブ上のイメージがある場所を参照します。

ラベル

[詳細設定] セクションで、変更する特定のポータルページのテキストを選択できます。ページの既定の英語のテキストを変更しても、他の言語のテキストは再翻訳されません。代替言語のページコンテンツは利便性のために提供されていますが、カスタマイズについては手動で更新する必要があります。ページの別の言語バージョンを編集するには、開いているポータル・ページの [**X**] アイコンをクリックして、ウィンドウが開いている場合は、まずウィンドウを折

りたたみます。次に、[言語] ペインで 言語を選択し、[**OK**] をクリックします。**[** 詳細設定**]** ウィンドウから開いたすべてのポータルページは、別のページを選択するまで、その言語で表示されます。

> 重要
>
> 高可用性またはクラスター化されたデプロイメントでは、ポータルのテーマが共有構成全体に分散されるのは、プライマリまたは構成コーディネータの Citrix ADC エンティティでそれぞれポータルのテーマが設定されている場合のみです。

古いポータルのカスタマイズに関する注意事項

Citrix Gateway または Access Gateway リリース 11.0 より前のリリースで作成されたカスタムポータル設計を手動で変更したインストールの場合は、カスタマイズインターフェイスで新しいポータルテーマから開始することを強くお勧めします。カスタマイズができない場合は、手動でカスタマイズを適用できますが、その直接サポートは提供されません。

手動でカスタマイズしたポータルを使用する場合は、カスタマイズしたポータルをグローバル・ポータル構成として設定する必要があります。ただし、そうすると、適用されたグローバルポータル構成を VPN 仮想サーバーレベルのポータルテーマのバインドで上書き することはできません。この場合、設定ユーティリティまたはコマンドラインを使用して VPN 仮想サーババインディングを作成しようとすると、エラーが返されます。

また、高可用性とクラスタ構成の場合は、Citrix ADC ファイルシステムの基盤となるファイルが自動的に共有される構成で配布されないため、展開内のすべてのノードで手動でカスタマイズを行う必要があります。

カスタム・ポータル構成の手動作成

Citrix Gateway 11.0 へのアップグレード後にカスタマイズされた古いポータル構成を手動で適用するには、既存のポータルページのコピーを変更し、カスタマイズされたポータルファイルを Citrix ADC ファイルシステムに配置し、**UITHEME** パラメーターとして カスタムを選択する必要があります。

WinSCP またはその他のセキュアコピープログラムを使用して、Citrix ADC ファイルシステムにファイルを転送できます。

1. Citrix Gateway のコマンドラインにログオンします。
2. コマンドプロンプトで **shell** と入力します。
3. コマンドプロンプトで、**mkdir /var/ns_gui_custom; cd /**ネットスケーラ**; tar-cvzf /var/ns_gui_** カスタム**/**カスタムテーマ**.tar.gz ns_gui/*** と入力します。
4. コマンドプロンプトで、**cd /var/netscaler/**ログオン**/**テーマ**/**と入力します。
   - グリーンバブルテーマをカスタマイズする場合は、「**cp-r** グリーンバブルカスタム」と入力して、グリーンバブルテーマのコピーを作成します。
   - 既定のテーマ (Caxton) をカスタマイズする場合は、**cp-r** 既定のカスタムと入力します。
   - X1 テーマをカスタマイズするには、「**cp-r X1** カスタム」と入力します。
5. **/var/netscaler/logon/themes/Custom** の下にコピーされたファイルに必要な変更を加え、テーマを手動でカスタマイズします。

- **css/base.css** に必要な編集を行います。
- カスタムイメージを **/var/ns_gui_custom/ns_gui/vpn/**メディアディレクトリにコピーします。
- **resources/** ディレクトリにあるファイルのラベルを変更します。これらのファイルは、ポータルでサポートされているロケールに対応しています。
- HTML ページまたは javascript ファイルに対する変更も必要な場合は、**/var/ns_gui_custom/ns_gui/**内のファイルに関連するようにできます。

6. カスタマイズの変更がすべて完了したら、プロンプトに次のように入力します。**tar —cvzf /var/ns_gui_custom/customtheme.tar.gz /var/ns_gui_custom/ns_gui/***

> 重要
>
> 前述の手順でテーマディレクトリをコピーする場合は、Citrix ADC シェルインターフェイス内でディレクトリ名の大文字と小文字が区別されるため、コピーしたフォルダ名を「カスタム」と正確に入力する必要があります。ディレクトリ名が正確に入力されていない場合、**UITHEME** 設定が **CUSTOM** に設定されている場合、フォルダは認識されません。

カスタマイズしたテーマを **VPN** グローバルパラメータとして選択

手動でカスタマイズしたポータル構成が完了し、Citrix ADC ファイルシステムにコピーしたら、その構成を Citrix Gateway 構成に適用する必要があります。これは、UITHEME パラメータを CUSTOM に設定することによって実行され、コマンドラインまたは構成ユーティリティを使用して完了できます。

コマンドラインを使用するには、次のコマンドを入力して **UITHEME** パラメータを設定します。

```
1 set vpn parameter UITHEME CUSTOM
2 <!--NeedCopy-->
```

構成ユーティリティーを使用して UITHEME パラメーターを設定するには、以下の手順に従います。

1. ［構成］タブで、**Citrix Gateway >** ［グローバル設定］に移動します。
2. [グローバル設定の変更] をクリックします。
3. [クライアントエクスペリエンス] タブをクリックします。
4. 画面の下部までスクロールし、[**UI** テーマ] リストメニューから [カスタム] を選択します。
5. ［**OK**］をクリックします。

これで、手動でカスタマイズしたポータルが VPN ユーザーに提供されるポータル設計になりました。

使用許諾契約書の作成

VPN ポータルシステムは、ポータル構成にエンドユーザーライセンス契約 (EULA) を適用するオプションを提供します。EULA が VPN グローバルスコープまたは関連する VPN 仮想サーバーのいずれかで Citrix Gateway 構成にバインドされると、VPN ユーザーは VPN への認証を許可する前に、利用規約として EULA に同意する必要があります。

ポータル・テーマと同様に、ユーザーは Web ブラウザーから報告されたロケールに基づいて、言語固有の EULA を提供します。サポートされているどの言語にも一致しないロケールの場合、デフォルトの言語は英語です。EULA ご

とに、サポートされている各言語でカスタムメッセージを入力できます。EULA 構成では、ポータル・テーマの場合と同様に、事前に翻訳されたコンテンツは提供されません。ユーザーの報告されたロケールが、EULA コンテンツが入力されていない言語と一致する場合、VPN ログインページの [利用規約] リンクをクリックすると、空白のページが返されます。

EULA を作成するには、**Citrix Gateway>** グローバル設定 **>EULA** または ****Citrix Gateway>** リソース **>EULA**** の［構成］タブで構成ユーティリティーのいずれかのコントロールを使用します。**[Global Settings]** ペインのコントロールは VPN グローバル EULA バインディングを管理するために使用され、**[Resources] > [EULA**] ノードのコントロールは EULA 設定の一般的な操作に使用されます。VPN 仮想サーバーの EULA バインディングを管理するには、［**Citrix Gateway**］**>** ［仮想サーバー］で **VPN** 仮想サーバーを編集します。一部のコマンドは、EULA エンティティを管理するためのコマンドラインでも使用できます。ただし、完全な EULA 管理コントロールは、構成ユーティリティでのみ使用できます。

コマンドラインを使用した **EULA** エンティティの作成

コマンドプロンプトで、「;」と入力します。

```
1 add vpn eula <name>
2 <!--NeedCopy-->
```

構成ユーティリティを使用した **EULA** エンティティの作成

1. **Citrix Gateway >** ［リソース］**>** ［**EULA**］に移動します。
2. 「追加」**(Add**) をクリックしてエンティティを作成します。
3. エンティティの名前を入力します。
4. 各言語について、関連するタブの下にコンテンツを貼り付けます。テキスト形式または HTML タグを使用して、改行を追加する
 タグなど、コンテンツの書式を設定できます。
5. ［作成］をクリックします。

EULA エンティティが作成されると、そのエンティティは VPN 設定にグローバルにバインドすることも、VPN 仮想サーバーにバインドすることもできます。

コマンドラインを使用して **EULA** を **VPN** グローバルにバインドする

コマンドプロンプトで、「;」と入力します。

```
1 bind vpn global eula <name>
2 <!--NeedCopy-->
```

設定ユーティリティを使用したグローバル **EULA VPN** バインディングの作成

1. ［構成］タブで、**Citrix Gateway >** ［グローバル設定］に移動します。

2. メインの詳細ペインで、[使用許諾契約書の設定] をクリックします。
3. [バインドを追加] をクリックします。
4. [クリックして選択] をクリックします。
5. EULA エンティティを選択し、[選択] をクリックします。
6. [バインド] をクリックします。
7. [閉じる] をクリックします。

コマンドラインを使用して **EULA** を **VPN** 仮想サーバーにバインドする

コマンドプロンプトで、「;」と入力します。

```
bind vpn vserver <name> eula <name>
<!--NeedCopy-->
```

設定ユーティリティを使用した **EULA** を **VPN** 仮想サーバにバインドする

1. [構成] タブで、**Citrix Gateway >** [仮想サーバー] の順に選択します。
2. メインの詳細ペインで、VPN 仮想サーバーを選択し、[**Edit**] をクリックします。
3. ページの右側の [詳細設定] ペインで、[**EULA**] をクリックします。
4. 新しく追加された EULA ペインで、[**EULA** なし] をクリックします。
5. [クリックして選択] をクリックします。
6. EULA エンティティを選択し、[選択] をクリックします。
7. [バインド] をクリックします。
8. [完了] をクリックします。

クライアントレスアクセスの設定

March 26, 2020

クライアントレスアクセスにより、ユーザーは Citrix Gateway プラグインや Receiver などのユーザーソフトウェアをインストールしなくても、必要なアクセスが可能になります。ユーザーは、Web ブラウザを使用して、Outlook Web Access などの Web アプリケーションに接続できます。

クライアントレスアクセスを設定する手順は、次のとおりです。

- グローバルに、またはユーザ、グループ、または仮想サーバにバインドされたセッションポリシーを使用して、クライアントレスアクセスを有効にします。
- Web アドレスのエンコード方式の選択。

特定の仮想サーバに対してのみクライアントレスアクセスを有効にするには、クライアントレスアクセスをグローバルに無効にし、それを有効にするセッションポリシーを作成します。

Citrix Gateway ウィザードを使用してアプライアンスを構成する場合は、ウィザード内でクライアントレスアクセスを構成できます。ウィザードの設定は、グローバルに適用されます。Citrix Gateway ウィザードでは、次のクライアント接続方法を構成できます。

- Citrix Gateway プラグイン。ユーザーは、Citrix Gateway プラグインを使用してのみログオンできます。
- Citrix Gateway プラグインを使用し、アクセスシナリオのフォールバックを許可します。ユーザーは、Citrix Gateway プラグインを使用して Citrix ゲートウェイにログオンします。ユーザーデバイスがエンドポイント分析スキャンに失敗した場合、ユーザーはクライアントレスアクセスを使用してログオンできます。この場合、ユーザーはネットワークリソースへのアクセスが制限されます。
- ユーザーが Web ブラウザとクライアントレスアクセスを使用してログオンできるようにします。ユーザーは、クライアントレスアクセスを使用してのみログオンでき、ネットワークリソースへのアクセスが制限されます。

クライアントレスアクセスの有効化

March 26, 2020

グローバルレベルでクライアントレスアクセスを有効にすると、すべてのユーザがクライアントレスアクセスの設定を受け取ります。Citrix Gateway ウィザード、グローバルポリシー、またはセッションポリシーを使用して、クライアントレスアクセスを有効にできます。

グローバル設定またはセッションプロファイルでは、クライアントレスアクセスには次の設定があります。

- On。クライアントレスアクセスを有効にします。クライアントの選択を無効にし、StoreFront または Web Interface を構成または無効にしない場合、ユーザーはクライアントレスアクセスを使用してログオンします。
- Allow. デフォルトでは、クライアントレスアクセスは有効になっていません。クライアントの選択を無効にし、StoreFront または Web Interface を構成または無効にしない場合、ユーザーは Citrix Gateway プラグインを使用してログオンします。ユーザーのログオン時にエンドポイントの分析が失敗すると、クライアントレスアクセスが可能な選択肢ページが表示されます。
- Off. クライアントレスアクセスはオフになっています。この設定を選択すると、ユーザーはクライアントレスアクセスを使用してログオンできず、クライアントレスアクセスのアイコンが選択肢ページに表示されません。

注：コマンドラインインターフェイスを使用してクライアントレスアクセスを設定する場合、オプションは ON、OFF、または Disabled です。

Citrix Gateway ウィザードを使用してクライアントレスアクセスを有効にしなかった場合は、グローバルに、または構成ユーティリティを使用してセッションポリシーで有効にすることができます。

クライアントレスアクセスをグローバルに有効にするには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。

3. [クライアントエクスペリエンス] タブで、[クライアントレスアクセス] の横にある [ON] を選択し、[OK] をクリックします。

セッションポリシーを使用してクライアントレスアクセスを有効にするには

選択したユーザ、グループ、または仮想サーバだけにクライアントレスアクセスを使用する場合は、クライアントレスアクセスをグローバルに無効にするか、オフにします。次に、セッションポリシーを使用してクライアントレスアクセスを有効にし、ユーザ、グループ、または仮想サーバにバインドします。

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. [クライアントエクスペリエンス] タブで、[クライアントレスアクセス] の横にある [グローバル上書き] をクリックし、[オン] を選択して [作成] をクリックします。
7. [セッションポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [全般]、[True value]、[式の追加]、[作成]、[閉じる] の順にクリックします。
8. ［Create］をクリックしてから、［Close］をクリックします。

クライアントレスアクセスを有効にするセッションポリシーを作成したら、ユーザ、グループ、または仮想サーバにバインドします。

Web アドレスのエンコーディング

March 26, 2020

クライアントレスアクセスを有効にすると、内部 Web アプリケーションのアドレスをエンコードするか、アドレスをクリアテキストのままにするかを選択できます。設定は次のとおりです。

- わかりにくいこれは、標準のエンコーディングメカニズムを使用して、リソースのドメインとプロトコル部分を隠します。
- クリア。Web アドレスはエンコードされず、ユーザーに表示されます。
- 暗号化。ドメインとプロトコルは、セッションキーを使用して暗号化されます。Web アドレスが暗号化されている場合、同じ Web リソースのユーザセッションごとに URL が異なります。ユーザーがエンコードされた Web アドレスをブックマークし、Web ブラウザに保存してからログオフすると、ユーザーがログオンしてブックマークを使用して Web アドレスに再度接続しようとすると、Web アドレスに接続できなくなります。
  注：ユーザーがセッション中に暗号化されたブックマークをアクセスインターフェイスに保存すると、ユーザーがログオンするたびにブックマークが機能します。

この設定は、グローバルに構成することも、セッションポリシーの一部として構成することもできます。セッションポリシーの一部としてエンコーディングを構成する場合は、ユーザー、グループ、または仮想サーバーにバインドできます。

Web アドレスのエンコーディングをグローバルに設定するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [クライアントエクスペリエンス] タブで、[クライアントレスアクセス URL エンコーディング] の横のエンコードレベルを選択し、[OK] をクリックします。

セッションポリシーを作成して **Web** アドレスエンコーディングを設定するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. [クライアントエクスペリエンス] タブで、[クライアントレスアクセス URL エンコーディング] の横にある [グローバル上書き] をクリックし、エンコードレベルを選択して [OK] をクリックします。
7. [セッションポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [全般]、[True value]、[式の追加]、[作成]、[閉じる] の順にクリックします。

クライアントレスアクセスポリシーのしくみ

March 26, 2020

Web アプリケーションへのクライアントレスアクセスを設定するには、ポリシーを作成します。クライアントレスアクセスポリシーの設定は、設定ユーティリティで設定できます。クライアントレスアクセスポリシーは、規則とプロファイルで構成されます。Citrix Gateway に付属する構成済みのクライアントレスアクセスポリシーを使用できます。独自のカスタムクライアントレスアクセスポリシーを作成することもできます。

Citrix Gateway には、以下のポリシーが事前に構成されています。

- Outlook Web Access と Outlook Web App
- SharePoint のユーザー
- その他すべての Web アプリケーション

事前設定されたクライアントレスアクセスポリシーの次の特性に注意してください。

- これらは自動的に設定され、変更することはできません。
- 各ポリシーはグローバルレベルでバインドされます。
- クライアントレスアクセスをグローバルに有効にするか、セッションポリシーを作成しない限り、各ポリシーは適用されません。
- クライアントレスアクセスを有効にしていない場合でも、グローバルバインディングを削除または変更することはできません。

他の Web アプリケーションのサポートは、Citrix Gateway で構成するリライトポリシーのレベルによって異なります。作成したカスタムポリシーをテストして、アプリケーションのすべてのコンポーネントが正常に書き換えられるようにすることをお勧めします。

Receiver for Android、Receiver for iOS、または WorxHome からの接続を許可する場合は、クライアントレスアクセスを有効にする必要があります。iOS デバイスで実行される WorxHome の場合は、セッションプロファイル内で Secure Browse も有効にする必要があります。Secure Browse とクライアントレスアクセスが連携して、iOS デバイスからの接続を許可します。ユーザーが iOS デバイスに接続していない場合、Secure Browse を有効にする必要はありません。

クイック構成ウィザードでは、モバイルデバイスの正しいクライアントレスアクセスポリシーと設定を設定します。クイック構成ウィザードを実行して、StoreFront および Citrix Endpoint Management への接続に適切なポリシーを構成することをお勧めします。

カスタムクライアントレスアクセスポリシーは、グローバルにバインドすることも、仮想サーバにバインドすることもできます。クライアントレスアクセスポリシーを仮想サーバにバインドする場合は、新しいカスタムポリシーを作成してからバインドする必要があります。クライアントレスアクセスにグローバルまたは仮想サーバに対して異なるポリシーを適用するには、カスタムポリシーのプライオリティ番号を変更して、事前設定されたポリシーよりも小さい番号にします。これにより、カスタムポリシーのプライオリティが高くなります。仮想サーバに他のクライアントレスアクセスポリシーがバインドされていない場合は、事前に設定されたグローバルポリシーが優先されます。

注：事前設定されたクライアントレスアクセスポリシーのプライオリティ番号は変更できません。

新しいクライアントレスアクセスポリシーの作成

March 26, 2020

デフォルトのクライアントレスアクセスポリシーと同じ設定を使用し、ポリシーを仮想サーバにバインドする場合は、ポリシーの新しい名前を指定して、デフォルトポリシーをコピーできます。設定ユーティリティを使用して、デフォルトのポリシーをコピーできます。

新しいポリシーを仮想サーバーにバインドした後、ユーザーがログオンしたときにポリシーが最初に実行されるように、ポリシーの優先順位を設定できます。

デフォルト設定を使用して新しいクライアントレスアクセスポリシーを作成するには

1. 構成ユーティリティのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［クライアントレスアクセス］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、既定のポリシーをクリックし、[追加] をクリックします。
3. [名前] にポリシーの新しい名前を入力し、[作成]、[閉じる] の順にクリックします。

クライアントレスアクセスポリシーを仮想サーバにバインドするには

新しいポリシーを作成したら、仮想サーバにバインドします。

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、仮想サーバーを選択し、[開く] をクリックします。
3. Citrix Gateway 仮想サーバーの構成］ダイアログボックスで、［ポリシー］タブをクリックし、［クライアントレス］をクリックします。
4. [ポリシーの挿入] をクリックし、一覧からポリシーを選択して [OK] をクリックします。

クライアントレスアクセスポリシー式の作成と評価

クライアントレスアクセス用の新しいポリシーを作成する場合、ポリシーの独自の式を作成できます。エクスプレッションの作成が完了したら、エクスプレッションの精度を評価できます。

1. 構成ユーティリティのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［クライアントレスアクセス］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、既定のポリシーをクリックし、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイル] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. 書き換え設定を構成し、[作成] をクリックします。
7. [クライアントレスアクセスポリシーの作成] ダイアログボックスの [式] で、[追加] をクリックします。
8. [式の追加] ダイアログボックスで式を作成し、[OK] をクリックします。
9. [クライアントレスアクセスポリシーの作成] ダイアログボックスで、[評価] をクリックし、式が正しいとテストされた場合は、[作成] をクリックします。

Citrix Gateway を使用した高度なクライアントレス **VPN** アクセス

March 26, 2020

クライアントレス VPN（CVPN）は、クライアントマシンで VPN クライアントアプリケーションを使用せずに、Citrix Gateway を介して企業のイントラネットリソースにリモートアクセスを提供する方法を認識します。CVPN

は、クライアント側で Web ブラウザを使用して、企業の Web アプリケーション、ポータル、およびその他のリソースへのリモートアクセスを提供します。
高度な CVPN ソリューションは、CVPN に関する次の制限を排除します。

- 相対 URL は時々識別できません。
- 動的に生成された相対 URL は識別できません。

高度なクライアントレス VPN は、絶対 URL とホスト名を識別し、HTTP 応答/Web ページに存在する相対 URL を書き換える代わりに、新しい一意の方法でそれらを書き換えます。SharePoint では、URL の書き換えに既定のフォルダを使用する必要がなくなり、カスタム SharePoint アクセスがサポートされます。

前提条件

次に、拡張 CVPN を設定するための前提条件を示します。

1. ワイルドカードサーバ証明書 -VPN 仮想サーバにはワイルドカードサーバ証明書が必要です。サーバーがでhttps://vpn.com ホストされている場合、サーバー証明書には、証明書 CN または SAN の一部として (vpn.com および.vpn.com) のエントリが含まれている必要があります (ここで、CN = 共通名、SAN= Subject 代替名)。この証明書をバインドするプロセスは、Citrix Gateway でも変わりません。
2. ワイルドカード **DNS** エントリ -s クライアント (Web ブラウザ) は、高度な CVPN アプリケーションの FQDN を解決する必要があります。Citrix Gateway サーバーのセットアップ中に、vpn.comを解決する DNS エントリを構成していました。'.vpn.com' もvpn.comに解決されるように、'.vpn.com' のサブドメインを設定する必要があります。

高度なクライアントレス **VPN** アクセスの設定

コマンドラインインターフェイスを使用して高度なクライアントレス **VPN** アクセスを設定するには、コマンドプロンプトで次のように入力します。

```
set vpn parameter -clientlessVpnMode ON
set vpn parameter -advancedClientlessVpnMode ENABLED
<!--NeedCopy-->
```

セッションアクションが仮想サーバにバインドされている場合は、そのセッションアクションに対して [Advanced Clientless VPN Mode] オプションも有効にする必要があります。

例:

```
set vpn sessionaction SessionActionName -advancedclientlessvpn ENABLED
<!--NeedCopy-->
```

Citrix ADC GUI を使用して高度なクライアントレス **VPN** アクセスを設定するには:

1. NetScaler の GUI で、「構成」**>**「**Citrix NetScaler>**「グローバル設定」の順に選択します。

2. [グローバル設定**]** ページで、[グローバル設定の変更] をクリックし、[クライアントエクスペリエンス] タブを選択します。
3. [クライアントエクスペリエンス] タブの [クライアントレスアクセス] リストから **[**オン] をクリックします。
4. [クライアントエクスペリエンス] タブの [高度なクライアントレス **VPN** モード] リストから [有効] をクリックします。

   > 注:
   >
   > - セッションアクションが仮想サーバーにバインドされている場合は、［**Citrix Gateway** セッションプロファイルの ****** 設定］ページの［クライアント ****** エクスペリエンス］タブでも、そのセッションアクションの［クライアントレス VPN モード ** の詳細設定］ ** オプションを有効にする必要があります。
   > - [グローバルをオーバーライド] オプションを選択すると、グローバル設定をオーバーライドできます。

> Advanced CVPN 機能は、セッションレベルでも設定できます。

警告

高度な CVPN は、エンタープライズ Web アプリケーションへのアクセスを提供することを目的としています。このようなアプリには、必要なすべての種類のリソース（JavaScript、CSS、画像など）に対して FQDN が 1 つしかありません。内部アプリケーションの完全な FQDN を単一オクテット（cvpn）にエンコードするので、サブドメインの関係を失います。その結果、エンタープライズ WebApp が CORS で設定されるたびに、Advanced CVPN 経由でアクセスする際に問題が発生することがあります。

ユーザーのドメイン・アクセスの構成

March 26, 2020

ユーザがクライアントレスアクセスを使用して接続する場合、ユーザがアクセスを許可するネットワークリソース、ドメイン、および Web サイトを制限できます。Citrix Gateway ウィザードまたはグローバル設定を使用して、ドメインへのアクセスを含めたり除外したりするためのリストを作成できます。

すべてのネットワークリソース、ドメイン、および Web サイトへのアクセスを許可してから、除外リストを作成できます。除外リストには、ユーザーがアクセスできない特定のリソースのセットが記載されています。ユーザーは、除外リストに含まれているドメインにアクセスできません。

また、すべてのネットワークリソース、ドメイン、および Web サイトへのアクセスを拒否し、特定の包含リストを作成することもできます。包含リストには、ユーザーがアクセスできるリソースが挙げられます。ユーザーは、リストに表示されていないドメインにアクセスできません。

注: Citrix Endpoint Management または StoreFront のクライアントレスアクセスポリシーを構成し、ユーザーが Receiver for Web に接続する場合、Receiver for Web がアクセスできるドメインを許可する必要があります。これは、Citrix Gateway が StoreFront および Endpoint Management ネットワークトラフィックを書き換えるために必要です。

Citrix Gateway ウィザードを使用してドメインアクセスを構成するには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］をクリックします。
2. 詳細ペインの [はじめに] で、[Citrix Gateway ウィザード] をクリックします。
3. [次へ] をクリックし、ウィザードの指示に従って、[クライアントレスアクセスの設定] ページを表示します。
4. [クライアントレスアクセス用のドメインの設定] をクリックし、次のいずれかの操作を行います。
    - 除外するドメインの一覧を作成するには、[除外するドメイン] をクリックします。
    - 含まれるドメインの一覧を作成するには、[ドメインの許可] をクリックします。
5. [ドメイン名] にドメイン名を入力し、[追加] をクリックします。
6. 一覧に追加するドメインごとに手順 5 を繰り返し、終了したら [OK] をクリックします。
7. Citrix Gateway ウィザードを使用して、アプライアンスの構成を続行します。

構成ユーティリティを使用してドメイン設定を構成するには

構成ユーティリティのグローバル設定を使用して、ドメイン一覧を作成または変更することもできます。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ペインの [クライアントレスアクセス] で、[クライアントレスアクセス用のドメインの構成] をクリックします。
3. 次のいずれかを行います:
    - 除外するドメインの一覧を作成するには、[除外するドメイン] をクリックします。
    - 含まれるドメインの一覧を作成するには、[ドメインの許可] をクリックします。
4. [ドメイン名] にドメイン名を入力し、[追加] をクリックします。
5. リストに追加するドメインごとに手順 4 を繰り返し、終了したら [OK] をクリックします。

クライアントレスアクセスの構成

March 26, 2020

Citrix Gateway では、1 つまたは複数の SharePoint 2003 または SharePoint 2007 または SharePoint 2013 サイトのコンテンツを書き換えることができます。これにより、ユーザーは Citrix Gateway プラグインを使用せずにコンテンツを利用できるようになります。書き換えプロセスを正常に完了するには、ネットワーク内の各 SharePoint サーバーのホスト名を使用して Citrix Gateway を構成する必要があります。

Citrix Gateway ウィザードまたは構成ユーティリティを使用して、SharePoint サイトのホスト名を構成できます。

Citrix Gateway ウィザードで、ウィザード内を移動して設定を構成します。[クライアントレスアクセスの構成] ページが表示されたら、SharePoint サイトの Web アドレスを入力し、[追加] をクリックします。

Citrix Gateway ウィザードの実行後に初めて Web サイトを追加したり、SharePoint を構成したりするには、構成ユーティリティを使用します。

Citrix ADC GUI を使用して **SharePoint** のクライアントレスアクセスを構成するには

1. **Citrix Gateway** > ［グローバル設定］に移動します。
2. 詳細ウィンドウの [クライアントレスアクセス] で、[**SharePoint** のクライアントレスアクセスの構成] をクリックします。
3. [SharePoint のクライアントレスアクセス] の [SharePoint サーバーのホスト名] に SharePoint サイトのホスト名を入力し、[追加] をクリックします。
4. リストに追加する SharePoint サイトごとに手順 3 を繰り返し、終了したら [**OK**] をクリックします。

SharePoint サイトをホームページとして設定する

March 26, 2020

SharePoint サイトをユーザーのホームページとして設定する場合は、セッションプロファイルを構成し、SharePoint サイトのホスト名を入力します。

SharePoint サイトをホームページとして構成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］ > ［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. [クライアントエクスペリエンス] タブで、[ホームページ] の横にある [グローバルに上書き] をクリックし、SharePoint サイトの名前を入力します。
7. [クライアントレスアクセス] の横にある [グローバル上書き] をクリックし、[オン] を選択して [作成] をクリックします。
8. [セッションポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [全般]、[True value]、[式の追加]、[作成]、[閉じる] の順にクリックします。

セッション・ポリシーを完了したら、ユーザー、グループ、仮想サーバー、またはグローバルにバインドします。ユーザーがログオンすると、SharePoint Web サイトがホームページとして表示されます。

SharePoint 2007 サーバーの名前解決を有効にする

March 26, 2020

SharePoint 2007 サーバーは、応答の一部として構成されたサーバー名をさまざまな URL 内のホスト名として送信します。構成済みの SharePoint サーバー名が完全修飾ドメイン名 (FQDN) でない場合、Citrix Gateway は SharePoint サーバー名を使用して IP アドレスを解決できず、一部のユーザー機能がタイムアウトし、”HTTP: 1.1 Gateway のタイムアウト” というエラーメッセージが表示される。これらの機能には、ファイルのチェックインとチェックアウト、Workspace 表示、およびユーザーがクライアントレスアクセスを使用してログオンしているときの複数のファイルのアップロードなどがあります。

この問題を解決するには、次のいずれかをお試しください。

- 名前解決の前に SharePoint のホスト名が FQDN に変換されるように、Citrix Gateway で DNS サフィックスを構成します。
- すべての SharePoint サーバー名に対して、Citrix Gateway でローカル DNS エントリを構成します。
- FQDN を使用するすべての SharePoint サーバー名を変更します。たとえば、SharePoint.intranet ドメインではなく、

DNS サフィックスを構成するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[DNS] を展開し、[DNS サフィックス] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [DNS サフィックス] で、イントラネットドメイン名をサフィックスとして入力し、[作成]、[閉じる] の順にクリックします。

追加するドメインごとにステップ 3 を繰り返すことができます。

Citrix Gateway 上のすべての SharePoint サーバー名に対してローカル DNS レコードを構成するには

1. 構成ユーティリティのナビゲーションウィンドウで、[DNS] > [レコード] を展開し、[アドレスレコード] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [ホスト名] に、DNS アドレスレコードの SharePoint ホスト名を入力します。
4. [IP アドレス] に SharePoint サーバーの IP アドレスを入力し、[追加]、[作成]、[閉じる] の順にクリックします。

A レコードを追加するホスト名には、CNAME レコードがあってはなりません。また、アプライアンス上に重複する A レコードが存在することもできません。

クライアントレスアクセスパーシステント **Cookie** の有効化

March 26, 2020

パーシステント Cookie は、SharePoint サーバーでホストされている Microsoft Word、Excel、PowerPoint ドキュメントを開いたり編集したりするなど、SharePoint の特定の機能にアクセスするために必要です。

永続的なクッキーはユーザーデバイスに残り、HTTP リクエストごとに送信されます。Citrix Gateway は、永続的な Cookie をユーザーデバイス上のプラグインに送信する前に暗号化し、セッションが存在する限り定期的に Cookie を更新します。セッションが終了すると、クッキーは古くなります。

Citrix Gateway ウィザードでは、管理者は永続的な Cookie をグローバルに有効にできます。セッションポリシーを作成して、ユーザー、グループ、または仮想サーバーごとに永続的な Cookie を有効にすることもできます。

パーシステント Cookie では、次のオプションを使用できます。

- [許可] は、永続的な Cookie を有効にし、ユーザーは SharePoint に保存されている Microsoft ドキュメントを開いて編集できます。
- [拒否] は、永続的な Cookie を無効にし、ユーザーが SharePoint に保存されている Microsoft ドキュメントを開いて編集することはできません。
- Prompt は、セッション中に永続的な Cookie を許可または拒否するようユーザに要求します。

ユーザーが SharePoint に接続しない場合、クライアントレスアクセスには永続的な Cookie は必要ありません。

SharePoint のクライアントレスアクセス用の永続的な **Cookie** の構成

March 26, 2020

SharePoint のクライアントレスアクセス用の永続的な Cookie は、グローバルに、またはセッションポリシーの一部として構成できます。

永続的な **Cookie** をグローバルに設定するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [クライアントエクスペリエンス] タブで、[クライアントレスアクセスパーシステント Cookie] の横にあるオプションを選択し、[OK] をクリックします。

セッションポリシーの一部として永続的な **Cookie** を構成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. [クライアントエクスペリエンス] タブで、[クライアントレスアクセスパーシステント Cookie] の横にある [グローバル上書き] をクリックし、オプションを選択して [作成] をクリックします。
7. [認証ポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [全般]、[True value]、[式の追加]、[作成]、[閉じる] の順にクリックします。

Web Interface を使用したクライアントレスアクセスのユーザ設定の保存

March 26, 2020

ユーザーがクライアントレスアクセスを使用して Web Interface からログオンしてログオフすると、ユーザーが複数回ログオンしたときに Cookie が永続的であっても、Citrix Gateway は前のセッションで設定したクライアント消費 Cookie を転送しません。設定ユーティリティまたはコマンドラインを使用して、Cookie をクライアント Cookie のパターンセットにバインドし、セッション間の Web Interface の設定を保持できます。

構成ユーティリティを使用して **Web Interface** の永続性の **Cookie** をバインドするには

1. 構成ユーティリティの [構成] タブで、[Citrix Gateway] > [ポリシー] を展開し、[クライアントレスアクセス] をクリックします。
2. 右側のウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [クライアントレスアクセスポリシーの作成] ダイアログボックスの [名前] に、ポリシーの名前を入力します。
4. [プロファイル] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. [クライアントクッキー] タブの [クライアントクッキー] で [ns_cvpn_default_client_cookie] を選択し、[変更] をクリックします。
7. [パターンセットを設定] ダイアログボックスの [パターンを指定] 領域の [パターン] で、次のパラメータを入力します。
   - [WIUser] をクリックし、[追加] をクリックします。
   - WING デバイス] をクリックし、[追加] をクリックします。
   - WING セッション] をクリックし、[追加] をクリックします。
8. [OK] をクリックし、[作成] をクリックします。

9. [クライアントレスアクセスポリシーの作成] ダイアログボックスの [式] に true と入力し、[作成] をクリックし、[閉じる] をクリックします。

コマンドラインを使用して **Web Interface** の永続性の **Cookie** をバインドするには

1. PuTTY などのセキュアシェル（SSH）接続を使用して、Citrix Gateway のコマンドラインにログオンします。
2. コマンドプロンプトで shell と入力します。
3. コマンドプロンプトで、次のコマンドを入力します。
    - バインドポリシーパッチセット ns_cvpn_default_client_cookie WIUser と入力し、Enter キーを押します。
    - バインドポリシーパセット ns_cvpn_default_client_cookie WING デバイス、し、ENTER キーを押します。
    - バインドポリシーパセット ns_cvpn_default_client_cookie WING セッションし、Enter キーを押します。

クライアント選択ページの設定

March 26, 2020

複数のログオンオプションをユーザーに提供するように Citrix Gateway を構成できます。クライアント選択ページを構成することにより、ユーザーは、次の選択肢を使用して、1 つの場所からログオンできます。

- Windows 向け Citrix Gateway プラグイン
- Citrix Gateway plug-in for Mac OS X
- Citrix Gateway plug-in for Java
- StoreFront
- Web Interface
- クライアントレスアクセス

ユーザーは、Citrix Gateway または仮想サーバーにバインドされた証明書の Web アドレスを使用して、Citrix Gateway にログオンします。セッションポリシーとプロファイルを作成することで、ユーザーが受け取るログオンの選択肢を決定できます。Citrix Gateway の構成方法に応じて、［クライアントの選択］ページには、以下のログオン選択肢を表すアイコンが 3 つまで表示されます。

- ネットワークアクセス。ユーザーが Web ブラウザーを使用して Citrix Gateway に初めてログオンし、［ネットワークアクセス］を選択すると、ダウンロードページが表示されます。ユーザーが「ダウンロード」をクリックすると、プラグインがユーザーデバイスにダウンロードおよびインストールされます。ダウンロードとインストールが完了すると、アクセスインターフェイスが表示されます。新しいバージョンの Citrix Gateway をインストールしたり、古いバージョンに戻したりすると、Citrix Gateway ateway プラグインがアプライアンス上のバージョンにサイレントでアップグレードまたはダウングレードされます。ユーザーが Mac 用の Citrix Gateway プラグインを使用して接続する場合、ユーザーのログオン時に新しいアプライアンスのバー

ジョンが検出されると、プラグインはサイレントモードでアップグレードされます。このバージョンのプラグインでは、サイレントダウングレードは行われません。

- Web Interface または StoreFront。ユーザーがログオンする Web Interface を選択すると、[Web Interface] ページが表示されます。ユーザーは、公開アプリケーションまたは仮想デスクトップにアクセスできます。ユーザーが StoreFront を選択してログオンすると、Receiver が開き、アプリケーションやデスクトップにアクセスできます。
  注：StoreFront をクライアントとして構成すると、アプリケーションおよびデスクトップはアクセスインターフェイスの左ペインに表示されません。
- クライアントレスアクセス。ユーザがクライアントレスアクセスを選択してログオンすると、アクセスインターフェイスまたはカスタマイズされたホームページが表示されます。アクセスインターフェイスでは、ユーザーはファイル共有、Web サイトに移動し、Outlook Web Access を使用できます。

ユーザーが Java 用の Citrix Gateway プラグインを選択すると、プラグインが起動し、ユーザーがログオンします。選択ページは表示されません。

Secure Browse を使用すると、ユーザーは iOS デバイスから Citrix Gateway 経由で接続できます。Secure Browse を有効にした場合、ユーザーが Secure Hub を使用してログオンすると、Secure Browse はクライアント選択ページを無効にします。

ログオン時のクライアント選択ページの表示

March 26, 2020

クライアント選択オプションを有効にすると、Citrix Gateway への認証に成功すると、1 つの Web ページから Citrix Gateway プラグイン、Web Interface、Receiver またはクライアントレスアクセスを使用してログオンできます。ログオンに成功すると、Web ページにアイコンが表示され、ユーザーは接続を確立する方法を選択できます。また、選択ページに表示されるように、Java 用の Citrix Gateway プラグインを構成することもできます。

エンドポイント分析を使用したり、アクセスシナリオのフォールバックを実装したりすることなく、クライアントの選択を有効にできます。クライアントセキュリティ式を定義しない場合、ユーザーは Citrix Gateway で構成された設定の接続オプションを受け取ります。ユーザーセッションにクライアントセキュリティ式が存在し、ユーザーデバイスがエンドポイント分析スキャンに失敗した場合、Web Interface が設定されている場合、選択ページには Web Interface を使用するオプションのみが表示されます。それ以外の場合、ユーザーはクライアントレスアクセスを使用してログオンできます。

クライアントの選択肢は、グローバルに構成するか、セッションプロファイルとポリシーを使用して構成します。

> 重要：クライアントの選択を構成するときは、検疫グループを構成しないでください。エンドポイント分析スキャンに失敗し、隔離されたユーザーデバイスは、エンドポイントスキャンに合格したユーザーデバイスと同様に扱われます。

クライアント選択オプションをグローバルに有効にするには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [クライアントエクスペリエンス] タブで、[詳細設定] をクリックします。
4. [全般] タブで、[クライアントの選択] をクリックし、[OK] をクリックします。

セッション・ポリシーの一部としてクライアントの選択を有効にするには

また、セッション・ポリシーの一部としてクライアントの選択肢を構成し、ユーザー、グループ、仮想サーバーにバインドすることもできます。

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. [クライアントエクスペリエンス] タブで、[詳細設定] をクリックします。
7. [全般] タブで、[クライアントの選択肢] の横にある [グローバルに上書き]、[クライアントの選択肢]、[OK]、[作成] の順にクリックします。
8. [セッションポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [全般]、[True value]、[式の追加]、[作成]、[閉じる] の順にクリックします。

クライアント選択オプションの構成

March 26, 2020

セッションプロファイルとポリシーを使用してクライアントを選択できるようにするだけでなく、ユーザーソフトウェアの設定を構成する必要があります。たとえば、ユーザーが Citrix Gateway プラグイン、StoreFront または Web Interface、またはクライアントレスアクセスを使用してログオンできるようにする場合です。3 つのオプションとクライアントの選択をすべて有効にする 1 つのセッションプロファイルを作成します。次に、プロファイルをアタッチして True value に設定された式を使用してセッションポリシーを作成します。次に、セッションポリシーを仮想サーバーにバインドします。

セッションポリシーとプロファイルを作成する前に、ユーザーの承認グループを作成する必要があります。

承認グループを作成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、[Citrix Gateway] > [ユーザー管理] の順に展開し、[AAA グループ] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [グループ名] に、グループの名前を入力します。
4. [ユーザー] タブでユーザーを選択し、各ユーザーの [追加] をクリックし、[作成] をクリックして、[閉じる] をクリックします。

次の手順は、Citrix Gateway プラグイン、StoreFront およびクライアントレスアクセスを使用したクライアント選択のセッションプロファイルの例です。

クライアント選択のセッションプロファイルを作成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、[Citrix Gateway] > [ポリシー] の順に展開し、[セッション] をクリックします。
2. 詳細ウィンドウで、[プロファイル] タブをクリックし、[追加] をクリックします。
3. [名前] に、プロファイルの名前を入力します。
4. [クライアントエクスペリエンス] タブで、次の操作を行います。
   a) [ホームページ] の横にある [グローバルに上書き] をクリックし、[ホームページの表示] をオフにします。これにより、アクセスインターフェイスが無効になります。
   b) [クライアントレスアクセス] の横にある [グローバル上書き] をクリックし、[OFF] を選択します。
   c) [プラグインの種類] の横にある [グローバルにオーバーライド] をクリックし、[Windows/Mac OS X] を選択します。
   d) [詳細設定] をクリックし、[クライアント選択肢] の横にある [グローバル上書き] をクリックし、[クライアント選択肢] をクリックします。
5. [セキュリティ] タブの [既定の承認操作] の横にある [グローバルに上書き] をクリックし、[許可] を選択します。
6. [セキュリティ] タブで、[詳細設定] をクリックします。
7. [承認グループ] の [グローバルに上書き] をクリックし、[追加] をクリックしてグループを選択します。
8. [公開アプリケーション] タブで、次の操作を行います。
   a) ICA プロキシの横にある「グローバルオーバーライド」をクリックし、「OFF」を選択します。
   b)「Web Interface アドレス」の横にある「グローバルに上書き」をクリックし、StoreFront の Web アドレス（http://ipAddress/Citrix/など）を入力します。
   c) [Web Interface ポータルモード] の横にある [グローバルに上書き] をクリックし、[コンパクト] を選択します。
   d) [シングルサインオンドメイン] の横にある [グローバル上書き] をクリックし、ドメインの名前を入力します。
9. [Create] をクリックしてから、[Close] をクリックします。

クライアントとして Citrix Gateway プラグインを使用する場合は、[クライアントエクスペリエンス] タブの [プラ

グインの種類］で［Java］を選択します。この選択肢を選択する場合は、イントラネットアプリケーションを構成し、インターセプションモードを [プロキシ] に設定する必要があります。

セッションプロファイルを作成したら、セッションポリシーを作成します。ポリシー内でプロファイルを選択し、式を True value に設定します。

StoreFront をクライアント選択として使用するには、Citrix Gateway で Secure Ticket Authority（STA）も構成する必要があります。STA は仮想サーバにバインドされます。

> 注： StoreFront を実行しているサーバーが使用できない場合、Citrix Virtual Apps 選択肢は選択肢ページに表示されません。

STA サーバをグローバルに構成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ペインの [サーバー] で、[Secure Ticket Authority が使用する STA サーバーのバインド/バインド解除] をクリックします。
3. [STA サーバのバインド/バインド解除] ダイアログ・ボックスで、[追加] をクリックします。
4. [STA サーバーの構成] ダイアログボックスの [URL] に、STA サーバーの Web アドレスを入力し、[作成] をクリックします。
5. 手順 3 と 4 を繰り返して STA サーバを追加し、［OK］をクリックします。

STA を仮想サーバにバインドするには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、仮想サーバーをクリックし、[開く] をクリックします。
3. [公開アプリケーション] タブの [Secure Ticket Authority] の [アクティブ] で、STA サーバーを選択し、[OK] をクリックします。

また、[公開アプリケーション] タブで STA サーバを追加することもできます。

アクセスシナリオフォールバックの設定

March 26, 2020

SmartAccess を使用すると、Citrix Gateway は、エンドポイント分析スキャンの結果に基づいて、ユーザーデバイスに許可されるアクセス方法を自動的に決定できます。アクセスシナリオのフォールバックは、ユーザーデバイスが最初のエンドポイント分析スキャンに合格しなかった場合に、Citrix Workspace アプリを使用して Citrix Gateway プラグインから Web Interface または StoreFront にフォールバックできるようにすることで、この機能をさらに拡張します。

アクセスシナリオのフォールバックを有効にするには、Citrix Gateway へのログオン時に別のアクセス方法をユーザーが受け取るかどうかを決定する認証後のポリシーを構成します。この認証後のポリシーは、グローバルに、またはセッションプロファイルの一部として設定するクライアントセキュリティ式として定義されます。セッションプロファイルを構成すると、プロファイルがセッションポリシーに関連付けられ、ユーザー、グループ、または仮想サーバーにバインドされます。アクセスシナリオのフォールバックを有効にすると、Citrix Gateway はユーザー認証後にエンドポイント分析スキャンを開始します。フォールバック認証後のスキャンの要件を満たさないユーザーデバイスの結果は次のとおりです。

- クライアントの選択が有効になっている場合、ユーザーは Citrix Workspace アプリのみを使用して Web Interface または StoreFront にログオンできます。
- クライアントレスアクセスとクライアントの選択が無効になっている場合、Web Interface または StoreFront のみへのアクセスを提供するグループにユーザーを隔離できます。
- Citrix Gateway でクライアントレスアクセスと Web Interface または StoreFront が有効で、ICA プロキシが無効になっている場合、ユーザーはクライアントレスアクセスに戻ります。
- Web Interface または StoreFront が構成されておらず、クライアントレスアクセスが許可されるように設定されている場合、ユーザーはクライアントレスアクセスに戻ります。

クライアントレスアクセスを無効にすると、アクセスシナリオフォールバック用に次の設定の組み合わせを設定する必要があります。

- フォールバック認証後のスキャンのクライアントセキュリティパラメータを定義します。
- Web Interface のホームページを定義します。
- クライアントの選択を無効にします。
- ユーザーデバイスがクライアントのセキュリティチェックに失敗した場合、ユーザーは隔離グループに配置されます。隔離グループでは、Web Interface または StoreFront および公開アプリケーションのみにアクセスできます。

アクセスシナリオフォールバックのポリシーの作成

October 22, 2021

アクセスシナリオのフォールバック用に Citrix Gateway を構成するには、以下の方法でポリシーとグループを作成する必要があります。

- エンドポイント分析スキャンが失敗した場合にユーザーを配置する隔離グループを作成します。
- エンドポイント分析スキャンが失敗した場合に使用するグローバル Web Interface または StoreFront 設定を作成します。
- グローバル設定を上書きするセッションポリシーを作成し、セッションポリシーをグループにバインドします。
- エンドポイントの分析が失敗した場合に適用されるグローバルクライアントセキュリティポリシーを作成します。

アクセスシナリオフォールバックを設定する場合は、次の注意事項に従ってください。

- クライアントの選択肢またはアクセスシナリオのフォールバックを使用するには、すべてのユーザーに対して Endpoint Analysis プラグインが必要です。エンドポイント分析を実行できない場合、またはスキャン中に [スキャンをスキップ] を選択すると、ユーザーはアクセスを拒否されます。
  注：スキャンをスキップするオプションは、Citrix Gateway 10.1、ビルド 120.1316.e では削除されています
- クライアント選択を有効にすると、ユーザーデバイスがエンドポイント分析スキャンに失敗すると、ユーザーは検疫グループに配置されます。ユーザーは、Citrix Gateway プラグインまたは Citrix Workspace アプリを使用して、Web Interface または StoreFront に引き続きログオンできます。
  注：クライアントの選択を有効にする場合は、隔離グループを作成しないことをお勧めします。エンドポイント分析スキャンに失敗し、隔離されたユーザーデバイスは、エンドポイントスキャンに合格したユーザーデバイスと同様に処理されます。
- エンドポイント分析スキャンが失敗し、ユーザーが検疫グループに入った場合、検疫グループにバインドされたポリシーは、その検疫グループにバインドされたポリシーと同等または低い優先順位を持つユーザーに直接バインドされたポリシーがない場合にのみ有効になります。
- アクセスインターフェイスと Web Interface または StoreFront には、異なる Web アドレスを使用できます。ホームページを構成すると、Citrix Gateway プラグインのアクセスインターフェイスのホームページが優先され、Web Interface ユーザーのホームページが優先されます。StoreFront では、Citrix Workspace アプリのホームページが優先されます。

検疫グループを作成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、[Citrix Gateway] > [ユーザー管理] の順に展開し、[AAA グループ] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [グループ名] にグループの名前を入力し、[作成] をクリックし、[閉じる] をクリックします。
   重要: 検疫グループの名前は、ユーザーが属するドメイングループの名前と一致してはなりません。検疫グループが Active Directory グループ名と一致する場合、ユーザーデバイスがエンドポイント分析のセキュリティスキャンに合格した場合でも、ユーザーは検疫されます。

グループを作成した後、ユーザーデバイスがエンドポイント分析スキャンに失敗した場合に Web Interface にフォールバックするように Citrix Gateway を構成します。

ユーザー接続を隔離するための設定を構成するには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで Citrix Gateway を展開し、[グローバル設定] をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [グローバル Citrix Gateway 設定] ダイアログボックスの [公開アプリケーション] タブで、[ICA プロキシ] の横にある [OFF] を選択します。
4. 「Web Interface アドレス」の横に、StoreFront または Web Interface の Web アドレスを入力します。

5. [シングルサインオンドメイン] の横に Active Directory ドメインの名前を入力し、[OK] をクリックします。

グローバル設定を構成したら、グローバル ICA プロキシ設定を上書きするセッションポリシーを作成し、セッションポリシーを隔離グループにバインドします。

Access シナリオフォールバックのセッションポリシーを作成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [公開アプリケーション] タブの [ICA プロキシ] の横にある [グローバル上書き] をクリックし、[オン] を選択して [作成] をクリックします。
6. [セッションポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [全般]、[True value]、[式の追加]、[作成]、[閉じる] の順にクリックします。

セッションポリシーを作成したら、そのポリシーを隔離グループにバインドします。

セッションポリシーを隔離グループにバインドするには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ユーザー管理］の順に展開し、［AAA グループ］をクリックします。
2. 詳細ペインでグループを選択し、[開く] をクリックします。
3. [セッション] をクリックします。
4. [ポリシー] タブで、[セッション] を選択し、[ポリシーの挿入] をクリックします。
5. [ポリシー名] でポリシーを選択し、[OK] をクリックします。

Citrix Gateway で Web Interface または StoreFront を有効にするセッションポリシーとプロファイルを作成したら、グローバルクライアントセキュリティポリシーを作成します。

グローバルクライアントセキュリティポリシーを作成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [セキュリティ] タブで、[詳細設定] をクリックします。
4. [クライアントセキュリティ] に、式を入力します。システム式の設定の詳細については、システム式の設定および複合クライアントセキュリティ式の設定を参照してください。
5. [隔離グループ] で、グループプロシージャで構成したグループを選択し、[OK] を 2 回クリックします。

Citrix Gateway プラグインの接続を構成する

March 26, 2020

ユーザデバイス接続を設定するには、ユーザが内部ネットワークでアクセスできるリソースを定義します。ユーザーデバイス接続の設定には、次のものが含まれます。

- ユーザーがアクセスを許可するドメインを定義します。
- アドレスプール (イントラネット IP) など、ユーザーの IP アドレスを構成します。
- タイムアウト設定を構成する。
- シングル・サインオンを構成する。
- クライアントインターセプションの設定
- 分割トンネリングの設定。
- プロキシサーバーを介した接続の構成。
- Citrix Gateway 経由で接続するようにユーザーソフトウェアを構成する。
- モバイルデバイスのアクセスを構成します。

ほとんどのユーザーデバイス接続は、セッションポリシーの一部であるプロファイルを使用して構成します。イントラネットアプリケーション、事前認証、およびトラフィックポリシーを使用して、ユーザーデバイスの接続設定を定義することもできます。

注: Windows VPN プラグインと EPA プラグインは、さまざまな操作のためにテレメトリデータを収集します。この機能を無効にするには、クライアントマシンで次の操作を行います。

> レジストリ「HKLM\ ソフトウェア\ Citrix\ セキュアアクセスクライアント\ 無効化 GA」を REG_DWORD の種類を 1 に設定します。

ユーザセッション数の設定

March 26, 2020

グローバルレベルまたは仮想サーバーレベルごとに、特定の時点で Citrix Gateway に接続できるユーザーの最大数を設定できます。アプライアンスに接続するユーザーの数が構成値を超えると、Citrix Gateway でセッションは作成されません。ユーザー数が許可する数を超えた場合、ユーザーにはエラーメッセージが表示されます。

グローバルユーザー制限を設定するには

ユーザ制限をグローバルに設定する場合、制限は、システム上の異なる仮想サーバへのセッションを確立するすべてのユーザに適用されます。ユーザーセッション数が設定した値に達すると、Citrix Gateway 上の仮想サーバー上で新しいセッションを確立することはできません。

Citrix Gateway のデフォルトの認証タイプを設定するときに、グローバルレベルで最大ユーザー数を設定します。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [認証設定の変更] をクリックします。
3. [グローバル認証設定] ダイアログボックスの [最大ユーザー数] にユーザー数を入力し、[OK] をクリックします。

仮想サーバーごとのユーザー制限を設定するには

また、システム上の各仮想サーバーにユーザー制限を適用することもできます。仮想サーバーごとのユーザー制限を構成する場合、制限は、特定の仮想サーバーとのセッションを確立するユーザーにのみ適用されます。他の仮想サーバーとのセッションを確立するユーザーは、この制限の影響を受けません。

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、仮想サーバーをクリックし、[開く] をクリックします。
3. [最大ユーザー数] にユーザー数を入力し、[OK] をクリックします。

タイムアウト設定の構成

March 26, 2020

指定した分数の間、接続にアクティビティがない場合に、強制的に切断されるように Citrix Gateway を構成できます。セッションがタイムアウトする（切断する）1 分前に、セッションが終了することを示すアラートがユーザーに表示されます。セッションが終了すると、ユーザーは再度ログオンする必要があります。

タイムアウトのオプションには、次の **3** つがあります。

- 強制タイムアウト。この設定を有効にすると、ユーザーの操作に関係なくタイムアウト間隔が経過すると、Citrix Gateway でセッションが切断されます。タイムアウト間隔が経過したときに切断が発生するのを防ぐためにユーザーが実行できるアクションはありません。この設定は、Citrix Gateway プラグイン、Citrix Workspace アプリ、Secure Hub または Web ブラウザを使用して接続するユーザーに対して適用されます。デフォルト設定は 30 分です。値を 0 にすると、設定は無効になります。
- セッションタイムアウト。この設定を有効にすると、指定した間隔でネットワークアクティビティが検出されなかった場合、Citrix Gateway はセッションを切断します。この設定は、Citrix Gateway プラグイン、Citrix Workspace アプリ、Citrix Secure Hub または Web ブラウザを使用して接続するユーザーに適用されます。デフォルトのタイムアウト設定は 30 分です。値を 0 にすると、設定は無効になります。
- アイドルセッションのタイムアウト。ユーザーがマウス、キーボード、タッチ操作などの操作が行われなかった場合に、Citrix Gateway プラグインがアイドルセッションを終了するまでの時間。この設定は、Citrix Gateway プラグインを使用して接続するユーザーのみに適用されます。デフォルト設定は 30 分です。値を 0 にすると、設定は無効になります。

> 注**:** Microsoft Outlook などの一部のアプリケーションは、ユーザーの介入なしに、ネットワークトラフィックプローブを自動的に電子メールサーバーに送信します。
> アイドルセッションタイムアウト
> を「セッションタイムアウト」に設定して、ユーザーデバイス上で無人のセッションが適切な時間内にタイムアウトするように構成することをお勧めします。

これらの設定を有効にするには、1 ～65536 の値を入力し、タイムアウト間隔の分数を指定します。これらの設定を複数有効にすると、最初のタイムアウト間隔が経過すると、ユーザーデバイスの接続が閉じます。

タイムアウト設定は、グローバル設定を構成するか、セッションプロファイルを使用して構成します。プロファイルをセッションポリシーに追加すると、ポリシーはユーザー、グループ、または仮想サーバーにバインドされます。タイムアウト設定をグローバルに構成すると、設定がすべてのユーザーセッションに適用されます。

強制タイムアウトの設定

March 26, 2020

強制タイムアウトを設定すると、指定した時間が経過すると、Citrix Gateway プラグインが自動的に切断されます。強制タイムアウトは、グローバルに設定することも、セッションポリシーの一部として設定することもできます。

グローバル強制タイムアウトを構成するには

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [ネットワークの構成] タブで、[詳細設定] をクリックします。
4. [強制タイムアウト (分)] に、ユーザーが接続を維持できる分数を入力します。
5. [強制タイムアウト警告 (分)] に、接続が切断されることをユーザーに警告するまでの時間を分単位で入力し、[**OK**] をクリックします。

セッションポリシー内で強制タイムアウトを構成するには

強制タイムアウトを受け取るユーザーをさらに制御するには、セッションポリシーを作成し、そのポリシーをユーザーまたはグループに適用します。

1. 構成ユーティリティーの 構成タブのナビゲーションペインで、［**Citrix Gateway**］ >［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。

5. [名前] に、プロファイルの名前を入力します。
6. [ネットワーク構成] タブで、[詳細設定] をクリックします。
7. [タイムアウト] の [グローバルに上書き] をクリックし、[強制タイムアウト (分)] にユーザーが接続を維持できる分数を入力します。
8. [強制タイムアウト警告 (分)] の横にある [グローバル上書き] をクリックし、接続が切断されることについてユーザーに警告する時間 (分) を入力します。[**OK**] を 2 回クリックします。
9. [セッションポリシーの作成] ダイアログボックスで、[名前付き式**]** の横にある **[**全般**]**、**[**True value**]、[式の追加 **]、[作成]、[閉じる] の順にクリックします。

セッションまたはアイドルタイムアウトの設定

March 26, 2020

構成ユーティリティを使用して、セッションおよびクライアントのタイムアウト設定をグローバルに設定したり、セッションポリシーを作成したりできます。セッションポリシーとプロファイルを作成するときは、式を True に設定します。

セッションまたはクライアントのアイドルタイムアウトをグローバルに設定するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [クライアントエクスペリエンス] タブで、次のいずれかまたは両方の操作を行います。
   - [セッションタイムアウト (分)] に、分数を入力します。
   - [クライアントアイドルタイムアウト (分)] に分数を入力し、[**OK**] をクリックします。

セッションポリシーを使用してセッションまたはクライアントのアイドルタイムアウト設定を構成するには

1. 構成ユーティリティーの 構成タブのナビゲーションペインで、［**Citrix Gateway**］ >［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. [クライアントエクスペリエンス] タブで、次のいずれかまたは両方の操作を行います。
   - [セッションタイムアウト (分)] の横にある [グローバル上書き] をクリックし、分数を入力して [作成] をクリックします。

- [クライアントアイドルタイムアウト (分)] の横の [グローバル上書き] をクリックし、分数を入力して [作成] をクリックします。

7. [セッションポリシーの作成] ダイアログボックスで、[名前付き式**]** の横にある **[**** 全般]、[**True value**]、[式の追加 **]、[作成]、[閉じる] の順にクリックします。

内部ネットワークリソースへの接続

March 26, 2020

ユーザーが内部ネットワークのリソースにアクセスできるように Citrix Gateway を構成できます。分割トンネリングを無効にすると、ユーザーデバイスからのすべてのネットワークトラフィックが Citrix Gateway に送信され、内部ネットワークリソースへのトラフィックの通過を許可するかどうかが承認ポリシーによって決定されます。分割トンネリングを有効にすると、内部ネットワーク宛てのトラフィックのみがユーザーデバイスによって傍受され、Citrix Gateway に送信されます。Citrix Gateway がインターセプトする IP アドレスを構成するには、イントラネットアプリケーションを使用します。

Windows 用の Citrix Gateway プラグインを使用している場合は、インターセプトモードを透過モードに設定します。Java 用 Citrix Gateway プラグインを使用している場合は、インターセプトモードをプロキシに設定します。インターセプションモードを透過モードに設定すると、以下を使用してネットワークリソースへのアクセスを許可できます。

- 単一の IP アドレスとサブネットマスク
- IP アドレスの範囲

インターセプションモードをプロキシに設定すると、宛先および送信元 IP アドレスおよびポート番号を設定できます。

内部ネットワークリソースへのネットワークアクセスを構成するには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway]、[リソース] の順に展開し、[イントラネットアプリケーション**]** をクリックします。
2. 詳細ウィンドウで、[追加**]** をクリックします。
3. ネットワークアクセスを許可するためのパラメータを入力し、[作成]、[閉じる**]** の順にクリックします。

分割トンネリングの構成

April 9, 2020

分割トンネリングを有効にすると、Citrix Gateway プラグインが Citrix Gateway に不要なネットワークトラフィックを送信しないようにできます。

分割トンネリングを有効にしない場合、Citrix Gateway プラグインはユーザーデバイスからのすべてのネットワークトラフィックをキャプチャし、VPN トンネル経由で Citrix Gateway に送信します。

分割トンネリングを有効にすると、Citrix Gateway プラグインは、VPN トンネルを介して Citrix Gateway によって保護されたネットワーク宛てのトラフィックのみを送信します。Citrix Gateway プラグインは、保護されていないネットワーク宛てのネットワークトラフィックを Citrix Gateway に送信しません。

Citrix Gateway プラグインが起動すると、Citrix Gateway からイントラネットアプリケーションのリストを取得します。Citrix Gateway プラグインは、ユーザーデバイスからネットワーク上で送信されるすべてのパケットを調べ、パケット内のアドレスをイントラネットアプリケーションのリストと比較します。パケット内の宛先アドレスがイントラネットアプリケーションのいずれか内にある場合、Citrix Gateway プラグインは VPN トンネルを介して Citrix Gateway にパケットを送信します。宛先アドレスが定義済みのイントラネットアプリケーションにない場合、パケットは暗号化されず、ユーザーデバイスはパケットを適切にルーティングします。分割トンネリングを有効にすると、イントラネットアプリケーションによってインターセプトされるネットワークトラフィックが定義されます。

> 注：ユーザーが Citrix Workspace アプリを使用してサーバーファーム内の公開アプリケーションに接続する場合、分割トンネリングを構成する必要はありません。

Citrix Gateway では、リバース分割トンネリングもサポートされています。リバース分割トンネリングは、Citrix Gateway が傍受しないネットワークトラフィックを定義します。分割トンネリングを逆方向に設定すると、イントラネットアプリケーションは、Citrix Gateway がインターセプトしないネットワークトラフィックを定義します。リバース分割トンネリングを有効にすると、内部 IP アドレス宛てのネットワークトラフィックはすべて VPN トンネルをバイパスし、その他のトラフィックは Citrix Gateway を通過します。リバース分割トンネリングは、すべての非ローカル LAN トラフィックをログに記録するために使用できます。たとえば、ユーザーがホームワイヤレスネットワークを持っていて、Citrix Gateway プラグインを使用してログオンしている場合、Citrix Gateway は、ワイヤレスネットワーク内のプリンターまたは他のデバイス宛てのネットワークトラフィックを傍受しません。

イントラネットアプリケーションの詳細については、クライアントインターセプションの設定を参照してください。

分割トンネリングは、セッションポリシーの一部として設定します。

分割トンネリングを設定するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで ［**Citrix Gateway** ポリシー］を展開し、［セッション］をクリックします。
2. 詳細ペインの [プロファイル] タブでプロファイルを選択し、[開く**]** をクリックします。
3. [クライアントエクスペリエンス] タブで、[分割トンネル] の横にある [グローバル上書き] を選択し、オプションを選択して [**OK**] を 2 回クリックします。

分割トンネリングおよび認可の設定

Citrix Gateway の展開を計画するときは、分割トンネリングと、デフォルトの承認アクションと承認ポリシーを考慮することが重要です。

たとえば、ネットワークリソースへのアクセスを許可する認可ポリシーがあるとします。分割トンネリングが ON に設定されており、イントラネットアプリケーションが Citrix Gateway 経由でネットワークトラフィックを送信するように構成していない。Citrix Gateway にこのような構成がある場合、リソースへのアクセスは許可されますが、ユーザーはリソースにアクセスできません。

認証ポリシーによってネットワークリソースへのアクセスが拒否され、分割トンネリングが ON に設定されていて、イントラネットアプリケーションが Citrix Gateway 経由でネットワークトラフィックをルーティングするように構成されている場合、Citrix Gateway ateway プラグインは Citrix Gateway にトラフィックを送信しますが、リソースへのアクセスは拒否されます。

クライアントインターセプションの設定

March 26, 2020

イントラネットアプリケーションを使用して、Citrix Gateway 上のユーザー接続の傍受ルールを構成します。デフォルトでは、アプライアンスでシステム IP アドレス、マッピング IP アドレス、またはサブネット IP アドレスを設定すると、これらの IP アドレスに基づいてサブネットルートが作成されます。イントラネットアプリケーションは、これらのルートに基づいて自動的に作成され、仮想サーバーにバインドできます。分割トンネリングを有効にする場合は、クライアントインターセプションが発生するようにイントラネットアプリケーションを定義する必要があります。

構成ユーティリティを使用して、イントラネットアプリケーションを構成できます。イントラネットアプリケーションをユーザー、グループ、または仮想サーバーにバインドできます。

分割トンネリングを有効にし、ユーザーが WorxWeb または WorxMail を使用して接続する場合、クライアント傍受を構成するときに、Citrix Endpoint Management と Exchange サーバーの IP アドレスを追加する必要があります。分割トンネリングを有効にしない場合は、イントラネットアプリケーションで Endpoint Management と Exchange の IP アドレスを構成する必要はありません。

Citrix Gateway プラグイン用のイントラネットアプリケーションの構成

March 26, 2020

リソースへのユーザーアクセス用のイントラネットアプリケーションを作成するには、次の項目を定義します。

- 1 つの IP アドレス
- IP アドレスの範囲
- ホスト名

Citrix Gateway ateway でイントラネットアプリケーションを定義すると、Windows 用の Citrix Gateway プラグインは、リソース宛てのユーザーのトラフィックをインターセプトし、Citrix Gateway 経由でトラフィックを送信します。

イントラネットアプリケーションを構成する場合は、次の点を考慮してください。

- 次の条件が満たされている場合、イントラネットアプリケーションを定義する必要はありません。
  - インターセプションモードが透過モードに設定されている
  - ユーザーが Windows 用の Citrix Gateway プラグインを使用して Citrix Gateway に接続している
  - 分割トンネリングは無効です。
- ユーザーが Java 用 Citrix Gateway プラグインを使用して Citrix Gateway に接続する場合は、イントラネットアプリケーションを定義する必要があります。Citrix Gateway プラグインは、イントラネットアプリケーションで定義されたネットワークリソースへのトラフィックのみをインターセプトします。ユーザーがこのプラグインで接続する場合は、インターセプションモードをプロキシに設定します。

イントラネットアプリケーションを構成するときは、接続に使用するプラグインソフトウェアのタイプに対応する傍受モードを選択する必要があります。

注意: イントラネットアプリケーションは、プロキシインターセプションと透過インターセプションの両方に対して構成できません。Windows 用の Citrix Gateway プラグインと Java 用の Citrix Gateway プラグインの両方で使用されるネットワークリソースを構成するには、2 つのイントラネットアプリケーションポリシーを構成し、そのポリシーをユーザー、グループ、仮想サーバー、または Citrix Gateway グローバルにバインドします。

1 つの **IP** アドレスに対してイントラネットアプリケーションを作成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで ［**Citrix Gateway** リソース］を展開し、［イントラネットアプリケーション］をクリックします。
2. 詳細ウィンドウで、[追加**]** をクリックします。
3. [名前] に、プロファイルの名前を入力します。
4. [イントラネットアプリケーションの作成] ダイアログボックスで、[透明**]** を選択します。
5. [宛先の種類] で、[**IP** アドレス] と [** ネットマスク] を選択します **
6. [プロトコル] で、ネットワークリソースに適用するプロトコルを選択します。
7. [**IP** アドレス**]** に IP アドレスを入力します。
8. [ネットマスク] に「サブネットマスク」と入力し、[作成]、[閉じる**]** の順にクリックします。

IP アドレス範囲を構成するには

Web、電子メール、ファイル共有など、ネットワークに複数のサーバーがある場合は、ネットワークリソースの IP 範囲を含むネットワークリソースを構成できます。この設定により、ユーザーは IP アドレス範囲に含まれるネットワークリソースにアクセスできます。

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで ［**Citrix Gateway** リソース］を展開し、［イントラネットアプリケーション］をクリックします。
2. 詳細ウィンドウで、[** 追加] をクリックします **
3. [名前**]** に、プロファイルの名前を入力します。
4. [プロトコル] で、ネットワークリソースに適用するプロトコルを選択します。

5. [イントラネットアプリケーションの作成] ダイアログボックスで、[透明] を選択します。
6.「宛先の種類」で、「**IP** アドレスの範囲」を選択します
7. [**IP** 開始**]** に開始 IP アドレスを入力し、[IP 終了] に終了 IP アドレスを入力し、[作成]、[** 閉じる] の順にクリックします **

ホスト名のイントラネットアプリケーションを作成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで ［**Citrix Gateway** リソース］を展開し、［イントラネットアプリケーション］をクリックします
2. 詳細ウィンドウで、[** 追加] をクリックします **
3. [名前] に、プロファイルの名前を入力します。
4. [イントラネットアプリケーションの作成] ダイアログボックスで、[透明**]** を選択します。
5.「デスティネーション・タイプ」で、ホスト名を選択します。
6. [プロトコル] で、[**ANY**] を選択し、[作成] をクリックして [閉じる**]** をクリックします。

注意点

1. ワイルドカードホスト名がサポートされています。ホスト名「*.example.com」のイントラネットアプリケーションが構成されている場合、a1.example.com、b2.example.com などはトンネリングされます。
2. ホスト名ベースのイントラネットアプリケーションは、分割トンネリングが **ON** に設定されている場合にのみ機能します。
3. ホスト名ベースのイントラネットアプリケーションは、Windows VPN プラグインでのみサポートされます。

Java 用 **Citrix Gateway** プラグイン用のイントラネットアプリケーションの構成

March 26, 2020

ユーザーが Java 用の Citrix Gateway プラグインを使用して接続する場合は、イントラネットアプリケーションを構成し、傍受モードをプロキシに設定する必要があります。Citrix Gateway プラグインは、プロファイルで指定されたユーザーデバイスのループバック IP アドレスとポート番号を使用して、トラフィックをインターセプトします。

ユーザーが Windows ベースのデバイスから接続している場合、Citrix Gateway プラグインは、アプリケーション HOST 名を設定して、プロファイルで指定されたループバック IP アドレスとポートにアクセスすることで、HOST ファイルの変更を試みます。HOST ファイルを変更するには、ユーザーデバイスに対する管理者権限が必要です。

ユーザーが Windows 以外のデバイスから接続する場合は、イントラネットアプリケーションプロファイルで指定された送信元 IP アドレスとポート値を使用して、アプリケーションを手動で構成する必要があります。

Java 用 **Citrix Gateway** プラグイン用にイントラネットアプリケーションを構成するには

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで ［**Citrix Gateway** リソース］を展開し、［イントラネットアプリケーション］ をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前**]** に、プロファイルの名前を入力します。
4. [プロキシ] をクリックします。
5. [宛先 **IP** アドレス**]** と [宛先ポート] に、宛先 IP アドレスとポートを入力します。
6. [送信元 **IP** アドレス] と [送信元ポート] に、送信元 IP アドレスとポートを入力します。

> 注：送信元 IP アドレスは、ループバック IP アドレス 127.0.0.1 に設定する必要があります。IP アドレスを指定しない場合は、ループバック IP アドレスが使用されます。ポート値を入力しない場合は、宛先ポート値が使用されます。

ネームサービス解決の設定

March 26, 2020

Citrix Gateway のインストール時に、Citrix Gateway ウィザードを使用して、ネームサービスプロバイダーなどの追加設定を構成できます。ネームサービスプロバイダーは、完全修飾ドメイン名 (FQDN) を IP アドレスに変換します。Citrix Gateway ウィザードでは、DNS サーバーまたは WINS サーバーの構成、DNS 検索の優先度、およびサーバーへの接続を再試行する回数を設定できます。

Citrix Gateway ウィザードを実行すると、その時点で DNS サーバーを追加できます。セッションプロファイルを使用して、追加の DNS サーバーと WINS サーバーを Citrix Gateway に追加できます。その後、ウィザードで最初に使用した名前解決サーバーとは別の名前解決サーバーに接続するようにユーザーとグループに指示できます。

Citrix Gateway で追加の DNS サーバーを構成する前に、名前解決のための DNS サーバーとして機能する仮想サーバーを作成します。

セッションプロファイル内に **DNS** または **WINS** サーバーを追加するには

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで ［**Citrix Gateway** ポリシー］を展開し、［セッション］ をクリックします。
2. 詳細ペインの [プロファイル] タブでプロファイルを選択し、[開く] をクリックします。
3. [ネットワーク構成] タブで、次のいずれかの操作を行います。
   - DNS サーバーを構成するには、[DNS 仮想サーバー] の横にある [グローバル上書き] をクリックし、サーバーを選択して [**OK]** をクリックします。
   - WINS サーバーを構成するには、[WINS サーバー IP] の横にある [グローバル上書き] をクリックし、IP アドレスを入力して [**OK**] をクリックします。

ユーザ接続のプロキシサポートの有効化

March 26, 2020

ユーザーデバイスは、内部ネットワークにアクセスするためにプロキシサーバーを介して接続できます。Citrix Gateway は、HTTP、SSL、FTP、および SOCKS プロトコルをサポートしています。ユーザー接続のプロキシサポートを有効にするには、Citrix Gateway で設定を指定します。Citrix Gateway のプロキシサーバーが使用する IP アドレスとポートを指定できます。プロキシサーバーは、内部ネットワークへのすべてのそれ以降の接続のためのフォワードプロキシとして使用されます。

ユーザー接続のプロキシサポートを構成するには

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで **Citrix Gateway** を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [クライアントエクスペリエンス] タブで、[詳細設定] をクリックします。
4. [プロキシ**]** タブの **[**プロキシ設定] で、**[**オン**]** を選択します。
5. プロトコルの場合は、IP アドレスとポート番号を入力し、[**OK]** をクリックします。

> 注意： Appliance を選択した場合は、セキュアおよびセキュアでない HTTP 接続のみをサポートするプロキシ・サーバーを構成できます。

Citrix Gateway でプロキシサポートを有効にした後、プロトコルに対応するプロキシサーバーの構成の詳細をユーザーデバイス上で指定します。

プロキシサポートを有効にすると、Citrix Gateway によってプロキシサーバーの詳細がクライアントの Web ブラウザーに送信され、ブラウザーでプロキシ構成が変更されます。ユーザーデバイスが Citrix Gateway に接続すると、ユーザーデバイスはプロキシサーバーと直接通信し、ユーザーのネットワークに接続できます。

Citrix Gateway のすべてのプロトコルを使用するように **1** つのプロキシサーバーを構成するには

Citrix Gateway で使用されるすべてのプロトコルをサポートするように、1 つのプロキシサーバーを構成できます。この設定では、すべてのプロトコルに対して 1 つの IP アドレスとポートの組み合わせを提供します。

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで **Citrix Gateway** を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [クライアントエクスペリエンス] タブで、[詳細設定**]** をクリックします。
4. [プロキシ] タブの [プロキシ設定] で、**[**オン**]** を選択します。
5. プロトコルの場合は、IP アドレスとポート番号を入力します。
6. [すべてのプロトコルに同じプロキシサーバーを使用する] をクリックし、[**OK]** をクリックします。

分割トンネリングを無効にし、すべてのプロキシ設定を On に設定すると、プロキシ設定がユーザデバイスに伝播されます。プロキシ設定が Appliance に設定されている場合、設定はユーザー・デバイスには反映されません。

Citrix Gateway は、ユーザーデバイスの代わりにプロキシサーバーに接続します。プロキシ設定はユーザーのブラウザには反映されないため、ユーザーデバイスとプロキシサーバー間の直接通信はできません。

Citrix Gateway をプロキシサーバーとして構成するには

Citrix Gateway をプロキシサーバーとして構成する場合、サポートされるプロトコルは安全でない安全な HTTP だけです。

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで **Citrix Gateway** を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [クライアントエクスペリエンス] タブで、[詳細設定**]** をクリックします。
4. [プロキシ] タブの [プロキシ設定**]** で、**[** アプライアンス] を選択します。
5. プロトコルの場合は、IP アドレスとポート番号を入力し、[**OK]** をクリックします。

アドレスプールの設定

March 26, 2020

場合によっては、Citrix Gateway プラグインを使用して接続するユーザーに、Citrix Gateway 用の一意の IP アドレスが必要です。たとえば、Samba 環境では、マップされたネットワークドライブに接続する各ユーザーは、異なる IP アドレスから発信されているように見える必要があります。グループのアドレスプール（IP プールとも呼ばれます）を有効にすると、Citrix Gateway で各ユーザーに一意の IP アドレスエイリアスを割り当てることができます。

アドレスプールは、イントラネット IP アドレスを使用して構成します。次のタイプのアプリケーションでは、IP プールから取得される一意の IP アドレスを使用する必要があります。

- ボイスオーバー IP
- アクティブな FTP
- インスタントメッセージ
- セキュアシェル（SSH）
- コンピュータのデスクトップに接続するための仮想ネットワークコンピューティング（VNC）
- クライアントデスクトップに接続するためのリモートデスクトップ (RDP)

Citrix Gateway に接続するユーザーに内部 IP アドレスを割り当てるように Citrix Gateway を構成できます。固定 IP アドレスをユーザに割り当てたり、グループ、仮想サーバ、またはシステムにグローバルに割り当てたりする IP アドレスの範囲を指定できます。

Citrix Gateway では、内部ネットワークの IP アドレスをリモートユーザーに割り当てることができます。リモートユーザは、内部ネットワーク上の IP アドレスでアドレス指定できます。IP アドレスの範囲を使用することを選択し

た場合、システムは要求に応じてその範囲の IP アドレスをリモートユーザに動的に割り当てます。

アドレスプールを設定する場合は、次の点に注意してください。

- 割り当てられた IP アドレスは正しくルーティングされる必要があります。正しいルーティングを行うために、次の点を考慮してください。
  - 分割トンネリングを有効にしない場合は、IP アドレスを Network Address Translation（NAT; ネットワークアドレス変換）デバイス経由でルーティングできることを確認してください。
  - イントラネット IP アドレスを持つユーザー接続によってアクセスされるサーバーには、それらのネットワークに到達するための適切なゲートウェイが構成されている必要があります。
  - ユーザーソフトウェアからのネットワークトラフィックが内部ネットワークにルーティングされるように、Citrix Gateway でゲートウェイまたは静的ルートを構成します。
- IP アドレス範囲を割り当てるときは、連続したサブネットマスクだけを使用できます。範囲のサブセットは、下位レベルのエンティティに割り当てることができます。たとえば、IP アドレス範囲が仮想サーバにバインドされている場合は、範囲のサブセットをグループにバインドします。
- IP アドレス範囲は、バインディングレベル内の複数のエンティティにバインドすることはできません。たとえば、グループにバインドされているアドレス範囲のサブセットを 2 番目のグループにバインドすることはできません。
- Citrix Gateway では、ユーザーセッションでアクティブに使用されている IP アドレスを削除またはバインド解除することはできません。
- 内部ネットワーク IP アドレスは、次の階層を使用してユーザーに割り当てられます。
  - ユーザーの直接バインド
  - グループに割り当てられたアドレスプール
  - 仮想サーバに割り当てられたアドレスプール
  - アドレスのグローバル範囲
- アドレス範囲の割り当てに使用できるのは、連続したサブネットマスクだけです。ただし、割り当てられた範囲のサブセットは、さらに下位レベルのエンティティに割り当てられる場合があります。
  バインドされたグローバルアドレス範囲は、次の範囲にバインドできます。
  - 仮想サーバ
  - グループ
  - ユーザー
- バインドされた仮想サーバアドレス範囲は、次のサブセットにバインドできます。
  - グループ
  - ユーザー

バインドされたグループアドレス範囲は、ユーザーにバインドされたサブセットを持つことができます。

IP アドレスがユーザーに割り当てられると、アドレスプールの範囲がなくなるまで、ユーザーの次回のログオン用にアドレスが予約されます。アドレスが使い果たされると、Citrix Gateway からログオフしたユーザーの IP アドレスを最も長く再利用します。

アドレスを再利用できず、すべてのアドレスがアクティブに使用されている場合、Citrix Gateway はユーザーのログオンを許可しません。この状況を回避するには、他のすべての IP アドレスが使用できない場合に、マッピングされ

た IP アドレスをイントラネット IP アドレスとして使用することを Citrix Gateway に許可します。

イントラネット **IP DNS** 登録

イントラネット IP がクライアントマシンに割り当てられ、VIP トンネルの確立後に、VPN プラグインはそのクライアントマシンがドメインに参加しているかどうかをチェックします。クライアントマシンがドメインに参加しているマシンの場合、VPN プラグインは DNS 登録プロセスを開始し、マシンのホスト名のイントラネットと割り当てられたイントラネット IP アドレスを結び付けます。この登録は、トンネルの確立解除前に元に戻されます。

DSN 登録を成功させるには、次の nsapimgr ノブが設定されていることを確認します。また、権限のある DNS サーバーが「セキュリティで保護されていない」DNS 更新を許可するように設定されていることを確認します。

- **nsapimgr-ys enable_vpn_dns_override=1**：このフラグは、他の構成パラメータとともに NetScaler Gateway VPN クライアントに送信されます。このフラグが設定されていない場合、VPN クライアントが DNS/WINS リクエストをインターセプトすると、対応する GET/DNSHTTP リクエストをトンネル経由で NetScaler Gateway 仮想サーバーに送信し、解決された IP アドレスを取得します。ただし、'enable_vpn_dnstruncate_fix' フラグが設定されている場合、VPN クライアントは DNS/WINS 要求を透過的に NetScaler Gateway 仮想サーバーに転送します。この場合、DNS パケットはそのまま VPN トンネルを介して NetScaler Gateway 仮想サーバーに送信されます。これは、NetScaler Gateway で構成されたネームサーバーから戻ってくる DNS レコードが大きく、UPD 応答パケットに収まらない場合に役立ちます。この場合、クライアントが TCP-DNS を使用するようにフォールバックすると、この TCP-DNS パケットはそのまま NetScaler Gateway サーバーに送信されるため、NetScaler Gateway サーバーは DNS サーバーに対して TCP-DNS クエリを実行します。
- このフラグは、**NetScaler Gateway** サーバー自体によって使用されます。このフラグが設定されている場合、NetScaler Gateway は、「DNS ポート上の TCP 接続」の宛先を NetScaler Gateway で構成された DNS サーバーへの宛先を上書きします（元の着信 TCP-DNS パケットに存在する DNS サーバー IP に送信する代わりに）。UDP DNS 要求の場合、デフォルトでは、設定された DNS サーバを DNS 解決に使用します。

これらのノブの設定の詳細については、https://support.citrix.com/article/CTX200243を参照してください。

アドレスプールの設定

March 26, 2020

設定ユーティリティを使用して、ポリシーをバインドするレベルでアドレスプールを設定します。たとえば、仮想サーバーのアドレスプールを作成する場合は、そのノードでイントラネット IP アドレスを構成します。アドレスプールを設定すると、ポリシーが設定されているエンティティにバインドされます。アドレスプールを作成し、Citrix Gateway でグローバルにバインドすることもできます。

ユーザー、グループ、または仮想サーバーのアドレスプールを構成するには

1. 構成ユーティリティのナビゲーションペインで［**Citrix Gateway**］を展開し、次のいずれかの操作を行います。
   - Citrix Gateway ユーザーの管理］を展開し、［**AAA** ユーザー］をクリックします。
   - **Citrix Gateway** >［ユーザー管理］の順に展開し、［**AAA** グループ］をクリックします。
   - **Citrix Gateway** を展開し、［仮想サーバー］をクリックします。
2. 詳細ウィンドウで、ユーザー、グループ、または仮想サーバーをクリックし、[開く] をクリックします。
3. [イントラネット **IP**] タブの [IP アドレスとネットマスク] に IP アドレスとサブネットマスクを入力し、[追加] をクリックします。
4. プールに追加する IP アドレスごとにステップ 3 を繰り返し、[**OK**] をクリックします。

アドレスプールをグローバルに設定するには

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで **Citrix Gateway** を展開し、［グローバル設定］をクリックします。
2. 詳細ペインの [イントラネット IP] で、すべてのクライアント Citrix Gateway セッションで使用する一意の静的 IP アドレスまたは IP アドレスのプールを割り当てるには、[イントラネット IP] を構成します。
3. [イントラネット **IP** のバインド] ダイアログボックスで、[操作] をクリックし、[挿入] をクリックします。
4. [IP アドレス] と [ネットマスク] に IP アドレスとサブネットマスクを入力し、[追加] をクリックします。
5. プールに追加する各 IP アドレスに対してステップ 3 と 4 を繰り返し、[**OK**] をクリックします。

アドレスプールオプションの定義

March 26, 2020

セッションポリシーまたはグローバル Citrix Gateway 設定を使用して、ユーザーセッション中にイントラネット IP アドレスを割り当てるかどうかを制御できます。アドレスプールオプションを定義すると、イントラネット IP アドレスを Citrix Gateway に割り当てると同時に、特定のユーザーグループのイントラネット IP アドレスを使用できなくなります。

セッションポリシーを使用して、次の 3 つの方法のいずれかを使用してアドレスプールを設定できます。

- Nospillover-イントラネット IP アドレスのアドレスプールを構成すると、プールから使用可能な IP を持つセッションが取得されます。使用可能なすべてのイントラネット IP アドレスを使用したユーザーの場合は、[ログインの転送] ページが表示されます。
- スピルオーバー-アドレスプールを構成し、マップされた IP をイントラネット IP アドレスとして使用する場合、マップされた IP アドレスは、使用可能なすべてのイントラネット IP アドレスを使用したユーザーに使用されます。
- Off：アドレスプールは設定されていません。

> 注：マッピングされた IP アドレスが設定されていない場合は、SNIP が使用されます。

アドレスプールを設定するには

1. 構成ユーティリティーの 構成タブのナビゲーションペインで、[**Citrix Gateway**] > [ポリシー] の順に展開し、[セッション] をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前**]** に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. [ネットワーク構成] タブで、[詳細設定] をクリックします。
7. [イントラネット IP] の横にある [グローバル上書き] をクリックし、オプションを選択します。
8. 手順 9 で「**SPILLOVER** 」を選択した場合は、「Mapped IP」の横にある「グローバル上書き」をクリックし、アプライアンスのホスト名を選択して「**OK**」をクリックし、「作成」をクリックします。
9. [セッションポリシーの作成] ダイアログボックスで、式を作成し、[作成]、[閉じる] の順にクリックします。

転送ログインページの設定

ユーザーがイントラネット IP アドレスを使用できず、Citrix Gateway との別のセッションを確立しようとすると、[ログインの転送] ページが表示されます。[ログインの転送] ページでは、既存の Citrix Gateway セッションを新しいセッションに置き換えることができます。

[ログインの転送] ページは、ログオフ要求が失われた場合や、ユーザーがクリーンログオフを実行しない場合にも使用できます。次に例を示します：

- ユーザーに静的イントラネット IP アドレスが割り当てられ、既存の Citrix Gateway セッションがあります。ユーザが別のデバイスから 2 番目のセッションを確立しようとすると、[Transfer Login] ページが表示され、ユーザはセッションを新しいデバイスに転送できます。
- ユーザーには 5 つのイントラネット IP アドレスが割り当てられ、Citrix Gateway を介して 5 つのセッションが割り当てられます。ユーザが 6 番目のセッションを確立しようとすると、[ログインの転送（Transfer Login）] ページが表示され、既存のセッションを新しいセッションに置き換えることができます。

> 注: ユーザーに > 割り当てられた IP アドレスがなく、[> ログインの転送] ページを使用して新しい > セッションを確立できない場合、ユーザーには > エラーメッセージが表示されます。

[Transfer Login] ページは、アドレスプールを設定し、スピルオーバーを無効にした場合にだけ表示されます。

DNS サフィックスの設定

ユーザーが Citrix Gateway にログオンし、IP アドレスが割り当てられると、ユーザー名と IP アドレスの組み合わせの DNS レコードが Citrix Gateway の DNS キャッシュに追加されます。DNS レコードがキャッシュに追加されるときに、ユーザー名に付加するように DNS サフィックスを構成できます。これにより、ユーザーは DNS 名で参照

できるようになり、IP アドレスよりも覚えやすくなります。ユーザーが Citrix Gateway からログオフすると、レコードは DNS キャッシュから削除されます。

DNS サフィックスを構成するには

1. 構成ユーティリティーの 構成タブのナビゲーションペインで、[**Citrix Gateway**] > [ポリシー] の順に展開し、[セッション] をクリックします。
2. 詳細ペインの [ポリシー] タブでセッションポリシーを選択し、[開く] をクリックします。
3. [プロファイルの要求] の横にある [変更] をクリックします。
4. [ネットワーク構成] タブで、[詳細設定] をクリックします。
5. [イントラネット IP DNS サフィックス] の横の [グローバル上書き] をクリックし、DNS サフィックスを入力して [**OK**] を 3 回クリックします。

VoIP 電話のサポート

April 9, 2020

Citrix Gateway をスタンドアロンアプライアンスとしてインストールし、ユーザーが Citrix Gateway プラグインを使用して接続する場合、Citrix Gateway はボイスオーバー IP（VoIP）ソフトフォンとの双方向通信をサポートします。

音声やビデオなどのリアルタイムアプリケーションは、User Datagram Protocol（UDP; ユーザデータグラムプロトコル）を介して実装されます。Transmission Control Protocol（TCP）は、受信確認および失われたパケットの再送信によって生じる遅延のため、リアルタイムトラフィックには適していません。すべてのパケットを確実に配信するよりも、リアルタイムでパケットを配信することが重要です。ただし、TCP を介したトンネリングテクノロジーでは、このようなリアルタイムパフォーマンスは満たされません。

Citrix Gateway では、次の VoIP ソフトフォンがサポートされています。

- Cisco Softphone
- Avaya IP ソフトフォン

IP PBX とユーザデバイスで実行されているソフトフォンソフトウェアとの間で、セキュアトンネリングがサポートされます。VoIP トラフィックが安全なトンネルを通過できるようにするには、Citrix Gateway プラグインとサポートされているソフトフォンのいずれかを同じユーザーデバイスにインストールする必要があります。VoIP トラフィックがセキュアトンネル経由で送信される場合、次のソフトフォン機能がサポートされます。

- IP ソフトフォンから発信される発信コール
- IP ソフトフォンに発信される着信コール
- 双方向音声トラフィック

VoIP ソフトフォンのサポートは、イントラネット IP アドレスを使用して設定されます。各ユーザーのイントラネット IP アドレスを構成する必要があります。Cisco ソフトフォンコミュニケーションを使用している場合は、イントラ

ネット IP アドレスを設定してユーザにバインドした後、追加の設定は必要ありません。イントラネット IP アドレスの構成の詳細については、アドレスプールの設定を参照してください。

分割トンネリングを有効にする場合は、イントラネットアプリケーションを作成し、Avaya Softphone アプリケーションを指定します。さらに、透過インターセプションを有効にする必要があります。

Java 用 Citrix Gateway プラグインのアプリケーションアクセスの構成

March 26, 2020

アクセスレベルと、セキュアなネットワークでユーザがアクセスを許可するアプリケーションを設定できます。ユーザーが Java 用 Citrix Gateway プラグインを使用してログオンしている場合、［リモートセッション］ダイアログボックスで［アプリケーション］をクリックできます。[イントラネットアプリケーション] ダイアログボックスが表示され、ユーザーがアクセスを許可されているすべてのアプリケーションが一覧表示されます。

ユーザーが Java 用 Citrix Gateway プラグインを使用して接続している場合、ユーザーがアプリケーションにアクセスできるようにする 2 つの方法のうちの 1 つを構成できます。

- HOSTS ファイルの変更方法
- ソース IP とソースポートのメソッド

HOSTS ファイル変更方法を使用したアプリケーションへのアクセス

HOSTS ファイルの変更方法を使用すると、Citrix Gateway プラグインは、HOSTS ファイルで構成するアプリケーションに対応するエントリを追加します。Windows ベースのデバイスでこのファイルを変更するには、管理者としてログオンしているか、管理者権限を持っている必要があります。管理者権限でログオンしていない場合は、HOSTS ファイルを手動で編集し、適切なエントリを追加します。

注:Windows ベースのコンピュータでは、HOSTS ファイルは、次のディレクトリパスにあります。%systemroot%\system32\drivers\etc。Macintosh または Linux コンピュータでは、HOSTS ファイルは /etc/hosts にあります。

たとえば、Telnet を使用してセキュリティで保護されたネットワーク内のコンピュータに接続するとします。リモートコンピュータは、セキュリティで保護されたネットワーク内およびリモートでの作業 (自宅など) に使用します。IP アドレスは、ローカルホストの IP アドレス 127.0.0.1 である必要があります。HOSTS ファイルで、IP アドレスとアプリケーション名を追加します。たとえば、次のようになります。

127.0.0.1

HOSTS ファイルを編集してユーザーデバイスに保存すると、接続をテストします。コマンドプロンプトを開き、Telnet を使用して接続すると、接続をテストできます。ユーザーがセキュリティで保護されたネットワーク内にないユーザーデバイスを使用している場合は、Telnet を起動する前に Citrix Gateway にログオンします。

セキュリティで保護されたネットワーク内のコンピュータに接続するには:

1. コンピュータで使用可能なソフトウェアを使用して Telnet セッションを開始します。
2. コマンドプロンプトから、「telnet を開く」と入力します。

   リモートコンピュータのログオンプロンプトが表示されます。

SourceIP および **SourcePort** メソッドを使用したアプリケーションへのアクセス

ユーザーがセキュリティで保護されたネットワーク内のアプリケーションにアクセスする必要があり、ユーザーデバイスの管理者権限がない場合は、[イントラネットアプリケーション] ダイアログボックスにある送信元 IP アドレスとポート番号を使用して HOSTS ファイルを構成します。

[イントラネットアプリケーション] ダイアログボックスを開き、IP アドレスとポート番号を確認するには

1. ユーザーがプラグインを使用してログオンするときに、[セキュアリモートアクセス] ダイアログボックスで [アプリケーション] をクリックします。
2. 一覧でアプリケーションを見つけ、ソース IP アドレスとソースポート番号をメモします。

IP アドレスとポート番号がある場合は、Telnet セッションを開始して、リモートネットワーク内のコンピュータに接続します。

アクセスインターフェイスの設定

March 26, 2020

Citrix Gateway には、ユーザーがログオンした後に表示される Web ページであるデフォルトのホームページが含まれています。デフォルトのホーム・ページは、アクセス・インタフェースと呼ばれます。Access Interface をホームページとして使用するか、Web Interface をホームページまたはカスタム・ホームページとして構成します。

アクセスインターフェイスには 3 つのパネルがあります。展開環境に Web Interface がある場合、ユーザーはアクセスインターフェイスの左パネルで Receiver にログオンできます。展開環境に StoreFront がある場合、ユーザーは左側のパネルから Receiver にログオンできません。

アクセスインターフェイスは、内部と外部のウェブサイトへのリンクと、内部ネットワークのファイル共有へのリンクを提供するために使用されます。アクセスインタフェースは、次の方法でカスタマイズできます。

- アクセスインターフェイスの変更。
- アクセス・インタフェース・リンクの作成。

ユーザーは、Web サイトやファイル共有に独自のリンクを追加することで、アクセスインタフェースをカスタマイズすることもできます。また、ホームページを使用して、内部ネットワークからデバイスにファイルを転送することもできます。

> 注**:** ユーザーがログオンし、アクセスインターフェイスからファイル共有を開こうとすると、ファイル共有は開かず、「サーバーへの TCP 接続に失敗しました」というエラーメッセージが表示されます。この問題を解決するには、Citrix Gateway システムの IP アドレスから TCP ポート 445 および 139 のファイルサーバーの IP アドレスへのトラフィックを許可するようにファイアウォールを構成します。

アクセス・インタフェースのカスタム・ホームページへの置換

March 26, 2020

グローバル設定またはセッションポリシーとプロファイルのいずれかを使用して、カスタムホームページを構成し、既定のホームページである Access Interface を置き換えることができます。ポリシーを設定したら、ポリシーをユーザー、グループ、仮想サーバ、またはグローバルにバインドできます。カスタムホームページを構成すると、ユーザーのログオン時にアクセスインターフェイスは表示されません。

カスタムホームページをグローバルに設定するには

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで **Citrix Gateway** を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [クライアントエクスペリエンス] タブの [ホームページ] で、[ホームページの表示] をクリックし、カスタムホームページの Web アドレスを入力します。
4. [**OK]** をクリックし、[閉じる**]** をクリックします。

セッションプロファイルでカスタムホームページを構成するには

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで ［**Citrix Gateway** ポリシー］を展開し、［セッション］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加**]** をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規**]** をクリックします。
5. [名前**]** に、プロファイルの名前を入力します。
6. [クライアントエクスペリエンス] タブの [ホームページ] の横にある [グローバルに上書き] をクリックし、[ホームページの表示] をクリックして、ホームページの Web アドレスを入力します。
7. [セッションポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [全般]、[True value]、[式の追加]、[作成]、[閉じる] の順にクリックします。

アクセスインターフェイスの変更

March 26, 2020

Access Interface に依存するのではなく、カスタマイズされたホームページにユーザーを誘導することもできます。これを行うには、Citrix Gateway にホームページをインストールし、新しいホームページを使用するようにセッションポリシーを構成します。

カスタマイズされたホームページをインストールするには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで ［**Citrix Gateway**］をクリックします。
2. 詳細ペインの [アクセスインターフェイスのカスタマイズ] で、[アクセスインターフェイスの **** アップロード] をクリックします。**
3. ネットワーク上のコンピュータ上のファイルからホームページをインストールするには、[ローカルファイル] で [参照] をクリックし、ファイルに移動して [選択**]** をクリックします。
4. Citrix Gateway にインストールされているホームページを使用するには、［リモートパス］で［参照］をクリックし、ファイル を選択して［選択］をクリックします。
5. [アップロード] をクリックし、[閉じる**]** をクリックします。

Web リンクとファイル共有リンクの作成と適用

March 26, 2020

ユーザーが使用できる内部リソースへのリンクのセットが表示されるように、Access Interface を設定できます。これらのリンクを作成するには、まずリンクをリソースとして定義する必要があります。次に、ユーザー、グループ、仮想サーバー、またはグローバルにバインドして、アクセスインターフェイスでアクティブにします。作成したリンクは、[エンタープライズ Web サイト] および [
エンタープライズファイル共有] の下の [Web サイト] ウィンドウと [ファイル共有] ウィンドウに表示されます。ユーザーが独自のリンクを追加すると、これらのリンクは [
個人用 Web サイト] および [個人用ファイル共有] に表示されます。

セッション・ポリシーでアクセス・インタフェース・リンクを作成するには

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで ［**Citrix Gateway** リソース］を展開し、［ポータルのブックマーク］をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前**]** に、ブックマークの名前を入力します。
4. [表示する テキスト**]** に、リンクの説明を入力します。説明が アクセスインターフェイスに表示されます。

5. [ブックマーク] に Web アドレスを入力し、[作成]、[閉じる] の順にクリックします。

クライアントレスアクセスを有効にすると、Web サイトへの要求が Citrix Gateway を通過するようにできます。たとえば、Googleにブックマークを追加したとします。［ブックマークの作成］ダイアログボックスで、Citrix Gateway をリバースプロキシとして使用する］チェックボックスをオンにします。このチェックボックスをオンにすると、Web サイトの要求はユーザーデバイスから Citrix Gateway に送信され、次に Web サイトに送信されます。このチェックボックスをオフにすると、要求はユーザーデバイスから Web サイトに送信されます。このチェックボックスは、クライアントレスアクセスを有効にしている場合にのみ使用できます。

ブックマークをグローバルにバインドするには

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで **Citrix Gateway** を展開し、［グローバル設定］をクリックします。
2. 詳細ペインの [ブックマーク] で、**Citrix Gateway** ポータルページで、アクセス可能にする HTTP アプリケーションおよび Windows ファイル共有アプリケーションへのリンク を作成します。
3. [VPN グローバルバインディング の設定 *] ダイアログボックスで、[追加] をクリックします。
4. [使用可能] で、1 つまたは複数のブックマークを選択し、右矢印をクリックして [構成] の下のブックマークを移動し、**[OK]** をクリックします。

アクセスインターフェイスリンクをバインドするには

アクセス・インタフェース・リンクを次の場所にバインドできます。

- ユーザー
- グループ
- 仮想サーバー

構成を保存すると、ユーザーは [ホーム] タブの [アクセスインターフェイス] でリンクを使用できるようになります。このタブは、ユーザーが正常にログオンした後に最初に表示されるページです。リンクは、タイプに応じて、Web サイトリンク、またはファイル共有リンクとしてページ上に整理されます。

1. 構成ユーティリティのナビゲーションペインで、次のいずれかの操作を行います。
   - **Citrix Gateway** ユーザーの管理］を展開し、［**AAA** ユーザー］をクリックします。
   - **Citrix Gateway** のユーザー管理］を展開し、［**AAA** グループ］をクリックします。
   - **Citrix Gateway** を展開し、［仮想サーバー］をクリックします。
2. 詳細ウィンドウで、次のいずれかの操作を行います。
   - ユーザーを選択し、[開く] をクリックします。
   - グループを選択し、[開く] をクリックします。
   - 仮想サーバを選択し、[開く] をクリックします。
3. ダイアログボックスで、[ブックマーク] タブをクリックします。
4. [使用可能なブックマーク] で、1 つまたは複数のブックマークを選択し、右矢印をクリックして [構成済みブックマーク] の下のブックマークを移動し、**[OK]** をクリックします。

ブックマークでのユーザー名トークンの設定

March 26, 2020

特別なトークン%username% を使用して、ブックマークとファイル共有 URL を設定できます。ユーザーがログオンすると、トークンは各ユーザーのログオン名に置き換えられます。たとえば、\\ EmployeeServer\ %username%\ というフォルダの Jack という名前の従業員のブックマークを作成するとします。ジャックがログオンすると、ファイル共有 URL は\\ 従業員サーバー\ ジャック\ にマップされます。ブックマークにユーザー名トークンを設定する場合は、次の状況に留意してください。

- 1 つの認証タイプを使用している場合は、トークン%username% がユーザー名に置き換えられます。
- 2 要素認証を使用している場合、%username% トークンの代わりに、プライマリ認証タイプのユーザー名が使用されます。
- クライアント証明書認証を使用している場合は、クライアント証明書認証プロファイルのユーザー名フィールドを使用して、%username% トークンの置き換えが行われます。

トラフィックポリシーの仕組み

March 26, 2020

トラフィックポリシーでは、ユーザ接続に対して次の設定を構成できます。

- 信頼できないネットワークからアクセスされる機密アプリケーションのタイムアウトを短くする。
- 一部のアプリケーションで TCP を使用するようにネットワークトラフィックを切り替える。[TCP] を選択した場合は、特定のアプリケーションに対してシングルサインオンを有効または無効にする必要があります。
- Citrix Gateway プラグインのトラフィックに他の HTTP 機能を使用する状況を特定します。
- ファイルタイプの関連付けで使用されるファイル拡張子を定義します。

トラフィックポリシーの作成

April 9, 2020

トラフィックポリシーを設定するには、プロファイルを作成し、次のパラメータを設定します。

- プロトコル (HTTP または TCP)
- アプリケーションのタイムアウト
- Web アプリケーションへのシングル・サインオン
- フォームのシングルサインオン
- ファイルタイプの関連付け
- リピータプラグイン

- Kerberos 制約付き委任 (KCD) アカウント

トラフィックポリシーを作成したら、ポリシーを仮想サーバ、ユーザ、グループ、またはグローバルにバインドできます。

たとえば、Web アプリケーション PeopleSoft 人事管理が内部ネットワークのサーバーにインストールされているとします。このアプリケーションのトラフィックポリシーを作成して、宛先 IP アドレスと宛先ポートを定義し、ユーザーがアプリケーションにログオンしたままにできる時間（15 分など）を設定できます。

アプリケーションへの HTTP 圧縮などの他の機能を設定する場合は、トラフィックポリシーを使用して設定を構成できます。ポリシーを作成するときは、アクションの HTTP パラメータを使用します。式で、アプリケーションを実行しているサーバーの宛先アドレスを作成します。

トラフィックポリシーを設定するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［トラフィック］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [トラフィックポリシーの作成] ダイアログボックスの [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. [プロトコル] で、[HTTP] または [TCP] を選択します。

   > 注**:** プロトコルとして [TCP] を選択した場合、シングルサインオンは構成できず、[プロファイル] ダイアログボックスで設定が無効になります。

7. [AppTimeout (分)] に、分数を入力します。この設定により、ユーザーが Web アプリケーションにログオンしたままにできる時間が制限されます。
8. Web アプリケーションへのシングル・サインオンを有効にするには、「シングル・サインオン」で「ON」を選択します。

   注：フォームベースのシングルサインオンを使用する場合は、トラフィックプロファイル内で設定を構成できます。詳しくは、「
   フォームベースのシングル・サインオンの設定」を参照してください。
9. ファイル・タイプの関連付けを指定するには、「ファイル・タイプの関連付け」で「ON」を選択します。
10. リピータプラグインを使用してネットワークトラフィックを最適化するには、[ブランチリピータ] で [ON] を選択し、[作成] をクリックして [閉じる] をクリックします。
11. アプライアンスで KCD を構成する場合は、[KCD アカウント] でアカウントを選択します。

    アプライアンスでの KCD の設定の詳細については、「NetScaler アプライアンスでの Kerberos 制約付き委任の構成」を参照してください。

12. [Create Traffic Policy] ダイアログボックスで、式を作成または追加し、[Create] をクリックし、[Close] をクリックします。

フォームベースのシングル・サインオンの設定

April 9, 2020

フォームベースのシングルサインオンにより、ユーザーはネットワーク内のすべての保護されたアプリケーションに一度ログオンできます。Citrix Gateway でフォームベースのシングルサインオンを構成すると、ユーザーはパスワードを再入力しなくても、HTML フォームベースのログオンを必要とする Web アプリケーションにアクセスできます。シングルサインオンを使用しない場合、ユーザーは各アプリケーションにアクセスするために個別にログオンする必要があります。

フォームのシングルサインオンプロファイルを作成したら、フォームシングルサインオンプロファイルを含むトラフィックプロファイルとポリシーを作成します。詳しくは、「トラフィックポリシーの作成」を参照してください。

フォームベースのシングルサインオンを構成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［トラフィック］をクリックします。
2. 詳細ウィンドウで、[フォーム SSO プロファイル] タブをクリックし、[追加] をクリックします。
3. [名前] に、プロファイルの名前を入力します。
4. [アクション URL] に、完成したフォームの送信先の URL を入力します。

   > 注： URL は、ルート相対 URL です。

5. [ユーザー名フィールド] に、ユーザー名フィールドの属性の名前を入力します。
6. 「パスワード・フィールド」に、パスワード・フィールドの属性の名前を入力します。
7. [SSO 成功規則] で、ポリシーによって呼び出されたときにこのプロファイルが実行するアクションを記述する式を作成します。このフィールドの下にある [接頭辞]、[追加]、および [演算子] ボタンを使用して式を作成することもできます。

   このルールは、シングルサインオンが成功したかどうかをチェックします。
8. [名前値のペア] に、ユーザー名フィールドの値を入力し、続けてアンパサンド (&)、パスワードフィールドの値を入力します。

   値の名前は、アンパサンド (&) で区切ります。たとえば、名前 1 = 値 1、名前 2 = 値 2 です。
9. [レスポンスサイズ] に、レスポンスサイズ全体を許可するバイト数を入力します。フォームを抽出するために解析する応答のバイト数を入力します。

10.「抽出」で、名前と値のペアが静的か動的かを選択します。既定の設定は [動的] です。
11. [送信方法] で、ログオン資格情報をログオンサーバーに送信するためにシングルサインオンフォームで使用する HTTP 方法を選択します。デフォルトは Get です。
12.［Create］をクリックしてから、［Close］をクリックします。

SAML シングルサインオンの設定

March 26, 2020

シングルサインオン (SSO) 用の SAML 1.1 または SAML 2.0 プロファイルを作成できます。ユーザーは、シングルサインオン用の SAML プロトコルをサポートする Web アプリケーションに接続できます。Citrix Gateway は、SAML Web アプリケーションのアイデンティティプロバイダー（IdP）シングルサインオンをサポートしています。

SAML シングルサインオンを構成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［トラフィック］をクリックします。
2. 詳細ペインで、[SAML SSO プロファイル] タブをクリックします。
3. 詳細ウィンドウで、[追加] をクリックします。
4. [名前] に、プロファイルの名前を入力します。
5.「署名証明書名」に、X.509 証明書の名前を入力します。
6. [ACS URL] に、ID プロバイダーまたはサービスプロバイダーのアサーションコンシューマサービスを入力します。アサーションコンシューマーサービス URL（ACS URL）は、ユーザに SSO 機能を提供します。
7. [リレー状態規則] で、[保存されたポリシー式] と [頻繁に使用する式] からポリシーの式を作成します。「演算子」(Operator) リストからを選択し、式の評価方法を定義します。式をテストするには、[評価] をクリックします。
8. [パスワードの送信] で [ON] または [OFF] を選択します。
9. [発行者名] に、SAML アプリケーションの ID を入力します。
10.［Create］をクリックしてから、［Close］をクリックします。

トラフィックポリシーのバインディング

March 26, 2020

トラフィックポリシーは、仮想サーバー、グループ、ユーザー、および Citrix Gateway Global にバインドできます。設定ユーティリティを使用して、トラフィックポリシーをバインドできます。

設定ユーティリティを使用してトラフィックポリシーをグローバルにバインドするには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［トラフィック］をクリックします。
2. 詳細ペインでポリシーを選択し、[操作] で [グローバルバインド] をクリックします。
3. [トラフィックポリシーのバインド/バインド解除] ダイアログボックスの [詳細] で、[ポリシーの挿入] をクリックします。
4. [ポリシー名] でポリシーを選択し、[OK] をクリックします。

トラフィックポリシーの削除

March 26, 2020

どちらの構成ユーティリティーを使用して、Citrix Gateway からトラフィックポリシーを削除できます。設定ユーティリティを使用してトラフィックポリシーを削除し、ポリシーをユーザ、グループ、または仮想サーバレベルにバインドする場合は、まずポリシーをバインド解除する必要があります。その後、ポリシーを削除できます。

設定ユーティリティを使用してトラフィックポリシーをバインド解除するには

1. 構成ユーティリティのナビゲーションペインで、次のいずれかの操作を行います。
   - Citrix Gateway を展開し、［仮想サーバー］をクリックします。
   - Citrix Gateway >［ユーザー管理］の順に展開し、［AAA グループ］をクリックします。
   - Citrix Gateway >［ユーザー管理］の順に展開し、［AAA ユーザー］をクリックします。
2. 詳細ウィンドウで、仮想サーバー、グループ、またはユーザーを選択し、[開く] をクリックします。
3. Citrix Gateway 仮想サーバーの構成]、［AAA グループの構成]、または［AAA ユーザーの構成］ダイアログボックスで、［ポリシー］タブをクリックします。
4. [トラフィック] をクリックし、ポリシーを選択して [ポリシーのバインド解除] をクリックします。
5. [OK] をクリックし、[閉じる] をクリックします。

トラフィックポリシーがバインド解除されたら、ポリシーを削除できます。

設定ユーティリティを使用してトラフィックポリシーを削除するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［トラフィック］をクリックします。
2. 詳細ペインの [ポリシー] タブで、トラフィックポリシーを選択し、[削除] をクリックします。

セッションポリシーの設定

March 26, 2020

セッションポリシーは、ユーザー、グループ、仮想サーバー、およびグローバルに適用される式と設定の集合です。

セッションポリシーを使用して、ユーザー接続の設定を構成します。Windows 用の Citrix Gateway プラグインや Mac 用の Citrix Gateway プラグインなど、ユーザーがログオンするソフトウェアの設定を定義できます。また、ユーザーが Citrix Workspace アプリまたは Secure Hub を使用してログオンするように設定することもできます。セッションポリシーは、ユーザーが認証された後に評価され、適用されます。

セッションポリシーは、次の規則に従って適用されます。

- セッションポリシーは常に設定のグローバル設定を上書きします。
- セッション・ポリシーを使用して設定されていない属性またはパラメータは、仮想サーバに対して確立されたポリシーに設定されます。
- セッションポリシーまたは仮想サーバによって設定されないその他のアトリビュートは、グローバル構成によって設定されます。

> 重要: 次の手順は、セッション・ポリシーの作成に関する一般的なガイドラインです。クライアントレスアクセスや公開アプリケーションへのアクセスなど、さまざまな設定のセッションポリシーを設定するための具体的な手順があります。手順には、特定の設定を構成するための指示が含まれている場合があります。ただし、その設定は、セッションプロファイルとポリシーに含まれる多くの設定の 1 つになることがあります。この手順では、セッションプロファイル内に設定を作成し、そのプロファイルをセッションポリシーに適用するように指示されます。新しいセッションポリシーを作成しなくても、プロファイルおよびポリシー内の設定を変更できます。さらに、グローバルレベルですべての設定を作成し、グローバル設定を上書きするセッションポリシーを作成することもできます。

ネットワークに Citrix Endpoint Management または StoreFront を展開する場合は、クイック構成ウィザードを使用してセッションポリシーとプロファイルを構成することをお勧めします。ウィザードを実行するときに、配置の設定を定義します。次に、必要な認証、セッション、およびクライアントレスアクセスポリシーが作成されます。

セッションポリシーを作成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. セッションプロファイルの設定を完了し、[Create] をクリックします。
7. [セッションプロファイルの作成] ダイアログボックスで、ポリシーの式を追加し、[作成]、[閉じる] の順にクリックします。

注意: 式で「
True value」を選択すると、ポリシーがバインドされているレベルに常に適用されます。

セッション・プロファイルの作成

April 9, 2020

セッションプロファイルには、ユーザー接続の設定が含まれます。

セッションプロファイルは、ユーザーデバイスがポリシー式の条件を満たす場合にユーザーセッションに適用されるアクションを指定します。プロファイルは、セッションポリシーで使用されます。設定ユーティリティーを使用して、セッションポリシーとは別にセッションプロファイルを作成し、そのプロファイルを複数のポリシーに使用できます。ポリシーで使用できるプロファイルは 1 つだけです。

セッションプロファイルでのユーザ接続のネットワーク設定の構成

セッションプロファイルの [ネットワーク構成] タブを使用して、ユーザー接続の次のネットワーク設定を構成できます。

- DNS サーバー
- WINS サーバの IP アドレス
- イントラネット IP アドレスとして使用できるマップされた IP アドレス
- アドレスプールのスピルオーバー設定 (イントラネット IP アドレス)
- イントラネット IP DNS サフィックス
- HTTP ポート
- 強制タイムアウト設定

セッションプロファイルでの接続設定の構成

セッションプロファイルの [クライアントエクスペリエンス] タブを使用して、次の接続設定を構成できます。

- アクセスインターフェイスまたはカスタマイズされたホームページ
- Web ベースの電子メールの Web アドレス (Outlook Web Access など)
- プラグインの種類（Windows の場合は Citrix Gateway プラグイン、Mac OS X の場合は Citrix Gateway プラグイン、Java の場合は Citrix Gateway プラグイン）
- 分割トンネリング
- セッションおよびアイドルタイムアウトの設定
- クライアントレスアクセス
- クライアントレスアクセス URL エンコーディング
- プラグインの種類 (Windows、Mac、または Java)
- Web アプリケーションへのシングル・サインオン

- 認証用のクレデンシャルインデックス
- Windows でのシングルサインオン
- クライアントのクリーンアップ動作
- ログオンスクリプト
- クライアントのデバッグ設定
- 分割 DNS
- プライベートネットワーク IP アドレスおよびローカル LAN アクセスへのアクセス
- クライアントの選択
- プロキシ設定

ユーザー接続の設定の詳細については、Citrix Gateway プラグインの接続を構成するを参照してください。

セッションプロファイルでのセキュリティ設定の構成

セッションプロファイルの [セキュリティ] タブを使用して、次のセキュリティ設定を構成できます。

- デフォルトの承認アクション（許可または拒否）
- iOS デバイスからの接続の Secure Browse
- 隔離グループ
- 承認グループ

Citrix Gateway での認証の構成の詳細については、「認可の設定」を参照してください。

セッションプロファイルでの **Citrix Virtual Apps and Desktops** 設定の構成

セッションプロファイルの［公開アプリケーション］タブを使用して、Citrix Virtual Apps and Desktops を実行しているサーバーへの接続について次の設定を構成できます。

- ICA プロキシ。Citrix Workspace アプリを使用したクライアント接続です。
- Web Interface のアドレス
- Web Interface ポータルモード
- サーバー・ファーム・ドメインへのシングル・サインオン
- Citrix Workspace アプリのホームページ
- アカウントサービスアドレス

サーバーファーム内の公開アプリケーションに接続するための設定を構成する方法については、Web Interface を使用した公開アプリケーションおよび Virtual Desktops へのアクセスの提供を参照してください。

セッション・プロファイルは、セッション・ポリシーとは独立して作成できます。ポリシーを作成するときに、ポリシーにアタッチするプロファイルを選択できます。

構成ユーティリティを使用してセッションプロファイルを作成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウで、[プロファイル] タブをクリックし、[追加] をクリックします。
3. プロファイルの設定を構成し、[作成]、[閉じる] の順にクリックします。

プロファイルを作成したら、それをセッションポリシーに含めることができます。

構成ユーティリティを使用してセッションポリシーにプロファイルを追加するには

1. 構成ユーティリティのナビゲーションペインで、[Access Gateway] > [ポリシー] を展開し、[セッション] をクリックします。
2. [ポリシー] タブで、次のいずれかの操作を行います。
   - [Add] をクリックして、新しいセッションポリシーを作成します。
   - ポリシーを選択し、[Open] をクリックします。
3.「要求プロファイル」で、リストからプロファイルを選択します。
4. セッションポリシーの構成を完了し、次のいずれかの操作を行います。
   a) [Create] をクリックし、[Close] をクリックしてポリシーを作成します。
   b) [OK] をクリックし、[閉じる] をクリックしてポリシーを変更します。

セッションポリシーのバインド

March 26, 2020

セッション・ポリシーを作成したら、ユーザー、グループ、仮想サーバー、またはグローバルにバインドします。セッションポリシーは次の順序で階層として適用されます。

- ユーザー
- グループ
- 仮想サーバー
- グローバル

構成ユーティリティを使用してセッションポリシーをバインドするには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで [Citrix Gateway] を展開し、次のいずれかの操作を行います。
   a) [仮想サーバー] をクリックします。
   b) [ユーザ管理] を展開し、[AAA グループ] をクリックします。
   c) [ユーザ管理] を展開し、[AAA ユーザ] をクリックします。
2. 手順 1 で選択した内容に応じて、次のいずれかのダイアログボックスの [Policies] タブをクリックします。

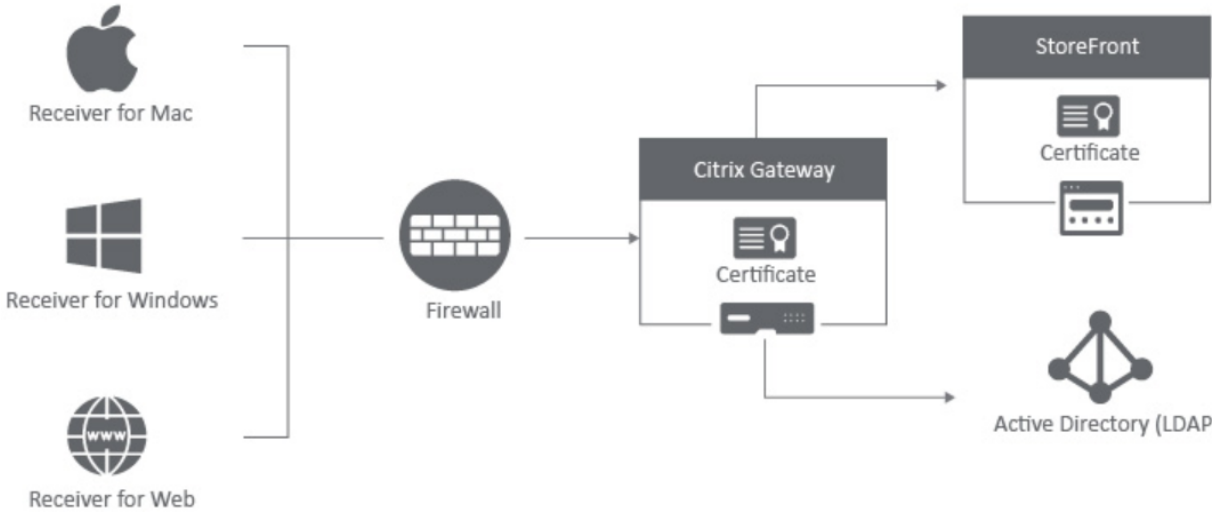
- Citrix Gateway 仮想サーバーの作成
- AAA グループの設定
- AAA ユーザの設定

3. セッションポリシーを追加するには、[セッション] をクリックします。
4. [ポリシーの挿入] をクリックし、セッションポリシーを選択して [OK] をクリックします。

StoreFront の Citrix Gateway セッションポリシーの構成

October 22, 2021

この記事では、Citrix Workspace アプリまたは Web ブラウザを使用しているユーザーに対して、StoreFront を使用した Citrix Gateway ドメインのみの認証を構成する方法について説明します。

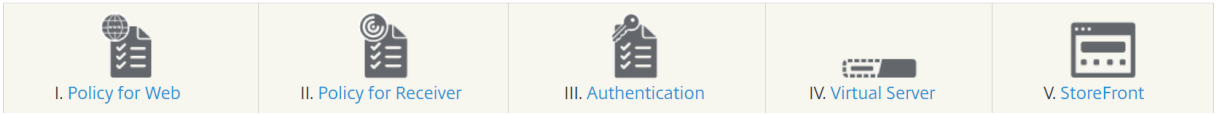


最小要件

- Citrix StoreFront 2.x または 3.0
- Citrix ADC 10.5 以降
- Windows 4.x 向け Citrix Workspace アプリ
- Mac 11.8 向け Citrix Workspace アプリ
- Web ブラウザー（Web 向け Citrix Workspace アプリ）
- 「CTX108876-Citrix ADC アプライアンスで LDAP 認証を構成する方法」で説明されているように、Citrix ADC アプライアンス上で構成された認証
- StoreFront サーバーと Citrix Gateway 用に構成された SSL 証明書。次のトピックの詳細については、StoreFront のドキュメントを参照してください。

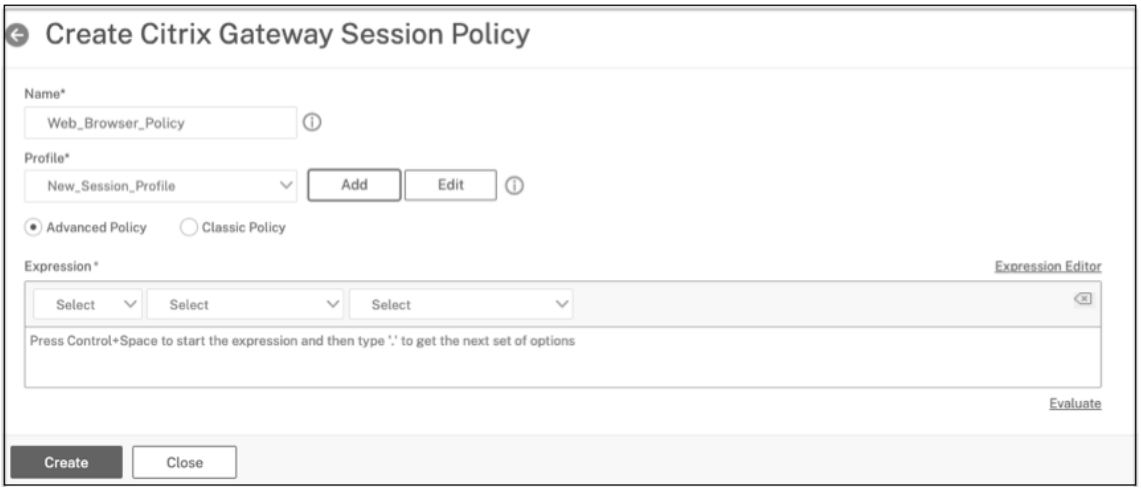
- StoreFront 2.6 のインストールとセットアップ
  - Windows 2012 Server 証明書
  - SSL バインドをサイトに追加するには
  - Citrix ADC アプライアンス 10.5 用の証明書のインストールと管理

StoreFront での **Citrix Gateway** の構成

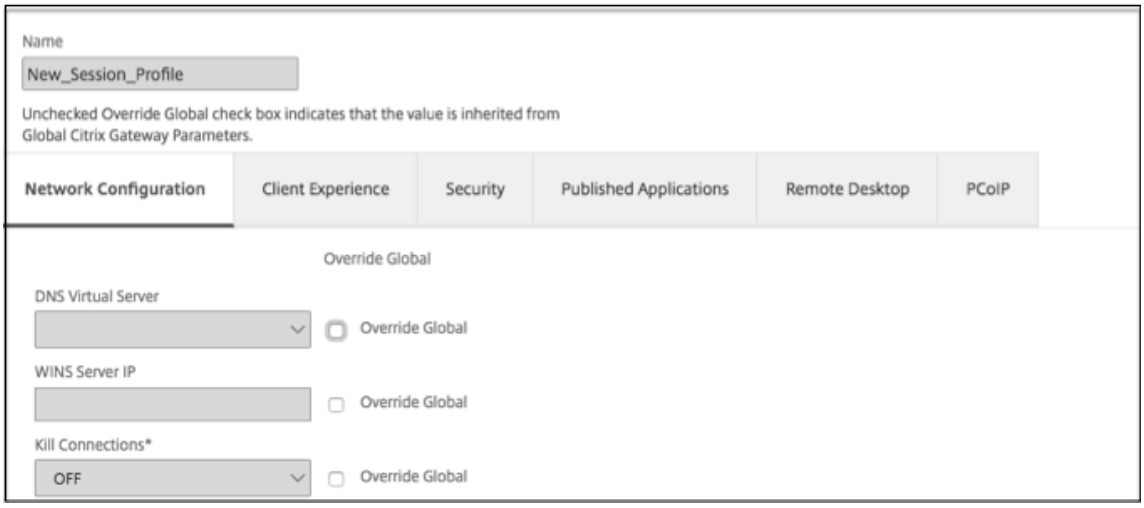


Web ブラウザベースのアクセス用のセッションポリシーを作成する

1. セッションポリシーを作成するには、[**Citrix Gateway**] **>** [ポリシー] **>** [セッション] の順に選択します。
2. [セッションポリシー] フィールドで、[追加] をクリックします。
3. [名前] フィールドに、セッション・ポリシーの名前を入力します。たとえば、Web_ ブラウザ _ ポリシーなどです。
4. + 記号の付いたボックスをクリックします。



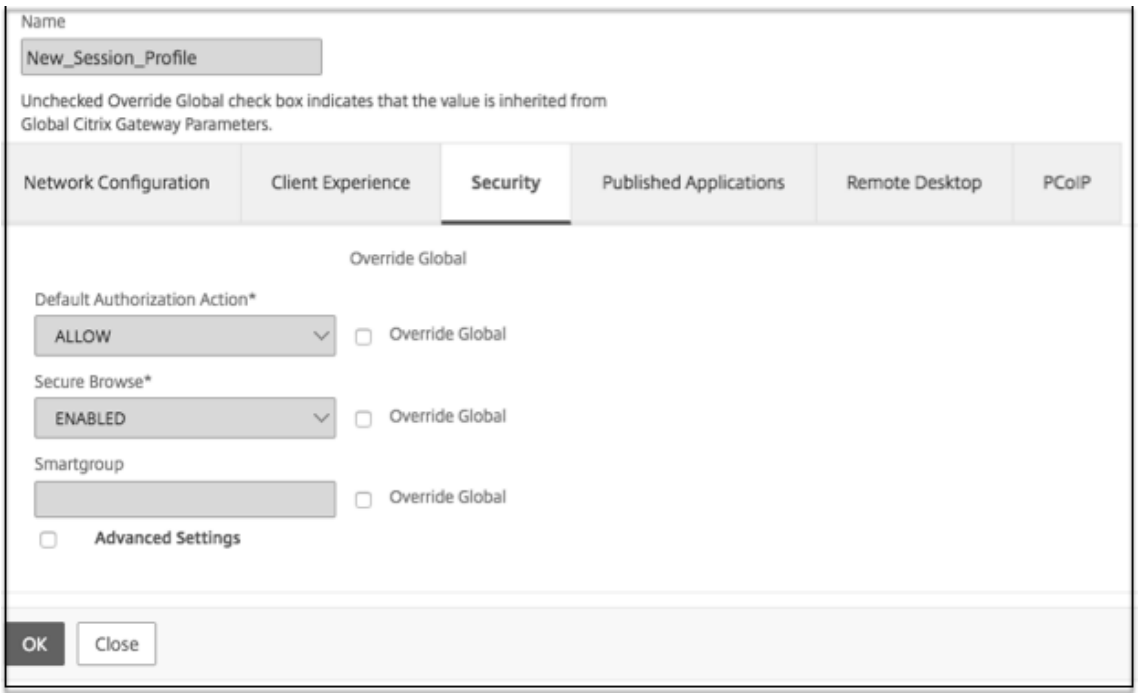
5. **Citrix Gateway** セッションプロファイルの設定] ウィンドウで、新しいセッションプロファイルの名前を入力します。



6. [クライアントエクスペリエンス] タブで、次の設定を有効にします。

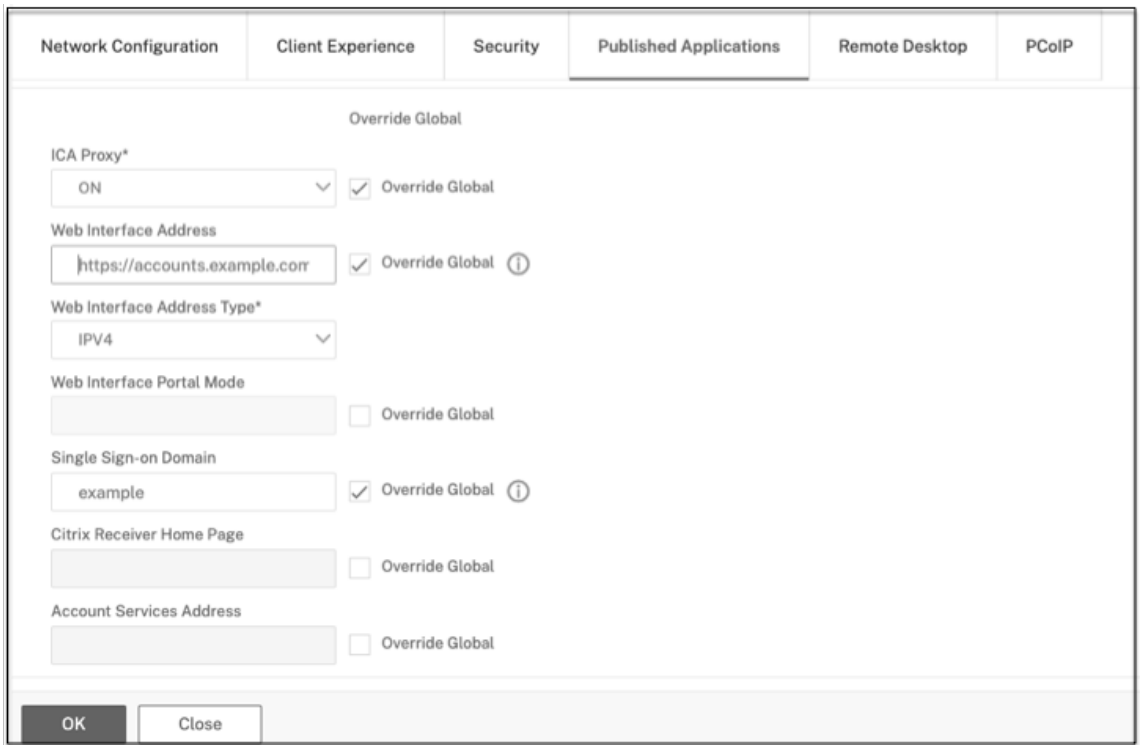
   - クライアントレスアクセス: **On** に設定
   - **Web** アプリケーションへのシングルサインオン: チェックボックスをオンにします。
   - プラグインの種類: **Windows/MAC OS X** に設定

7. [セキュリティ] タブで、[既定の承認操作] を有効にし、[許可] に設定します。



8. [公開アプリケーション] タブで、次の設定を有効にします。

   - **ICA** プロキシ：ON に設定します。
   - **Web Interface** アドレス：StoreFront サーバーの FQDN の後に Web ストアへのパスが続きます
   - シングル・サインオン・ドメイン -ドメインの NetBIOS 名

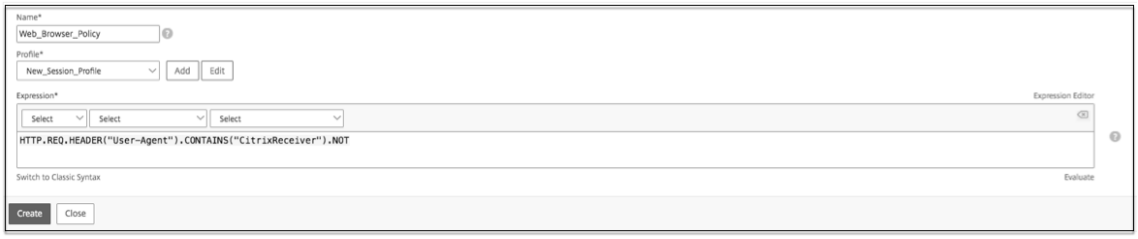


9. [作成] をクリックします。
10. クラシックポリシー式を使用している場合は、[式] フィールドに次の情報を追加し、[作成] をクリックします。

```
1 REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

11. 詳細ポリシー式を使用している場合は、[式] フィールドに次の情報を追加し、[作成] をクリックします。

```
1 HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

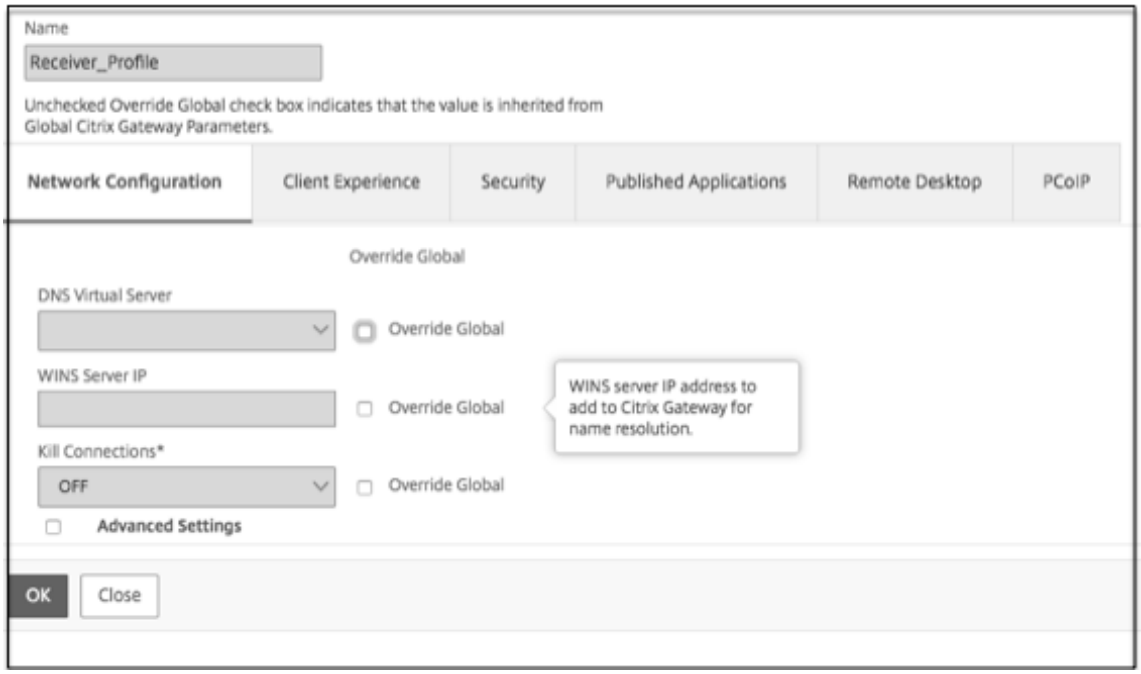


このポリシーは、Citrix ADC が Web ブラウザベースの接続と Citrix Workspace アプリベースの接続を区別するために必要です。このポリシーは、Web ブラウザベースの接続に適用されます。

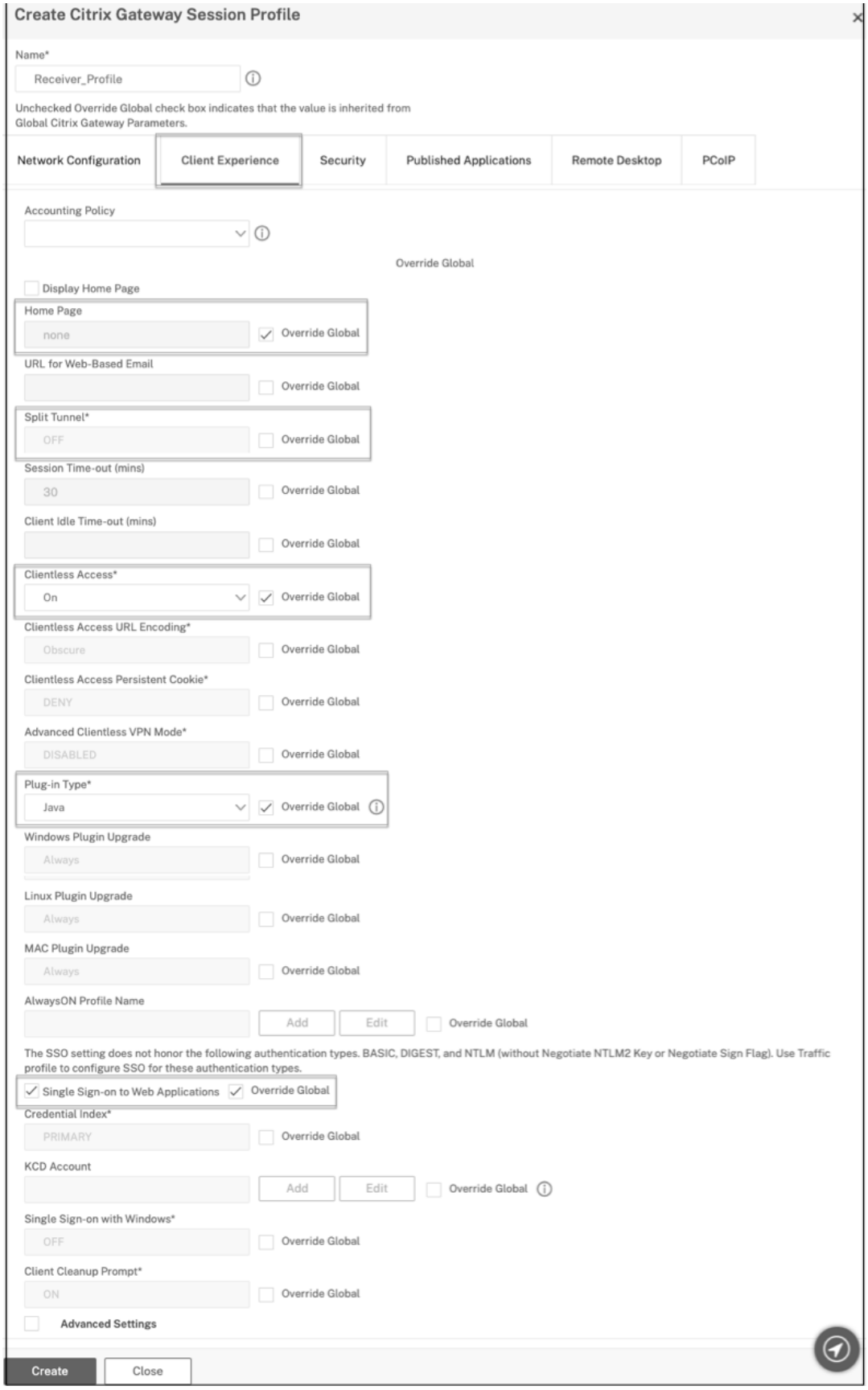
Windows または **Mac** 用の **Citrix Workspace** アプリ、および **Citrix Gateway** 上のモバイルデバイスのセッションポリシーを作成する

1. **Citrix Gateway >** ［ポリシー］ **>** ［セッション］に移動します。
2. [セッションポリシー] フィールドで、[追加] をクリックします。
3. ［名前］フィールドに、セッション・ポリシーの名前を入力します。たとえば、Receiver_Policy
4. + 記号の付いたボックスをクリックします。

5. **Citrix Gateway** セッションプロファイルの設定］ウィンドウで、新しいセッションプロファイルの名前を入力します。

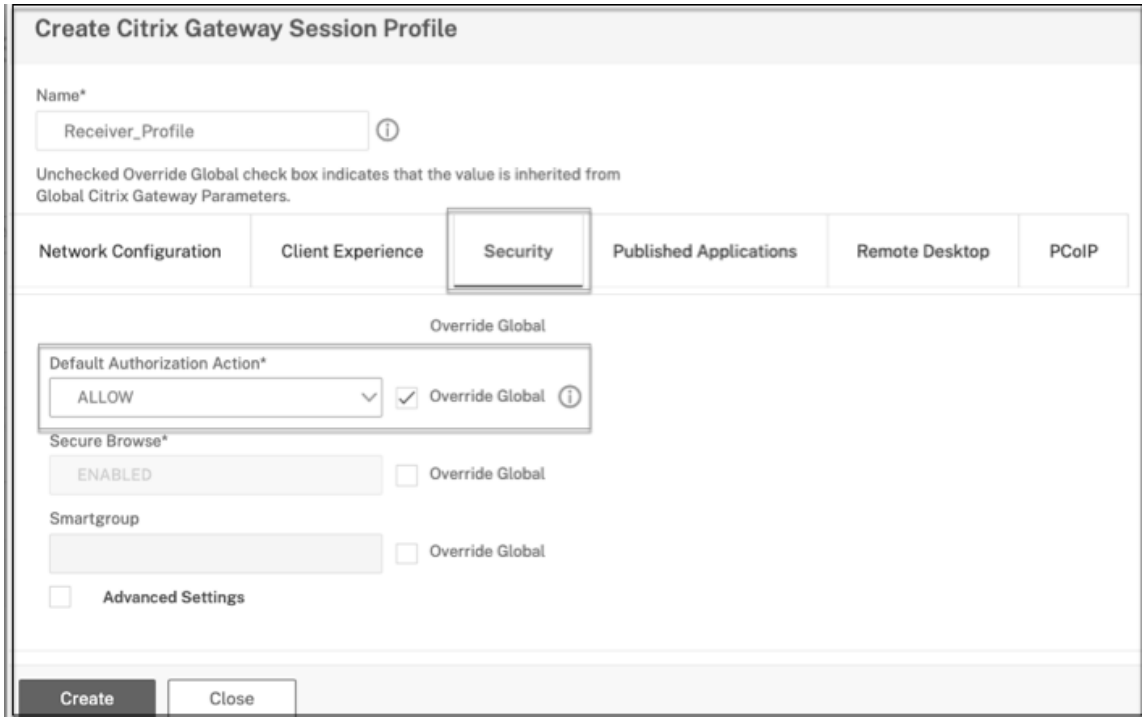


6. [クライアントエクスペリエンス] タブで、次の設定を有効にします。



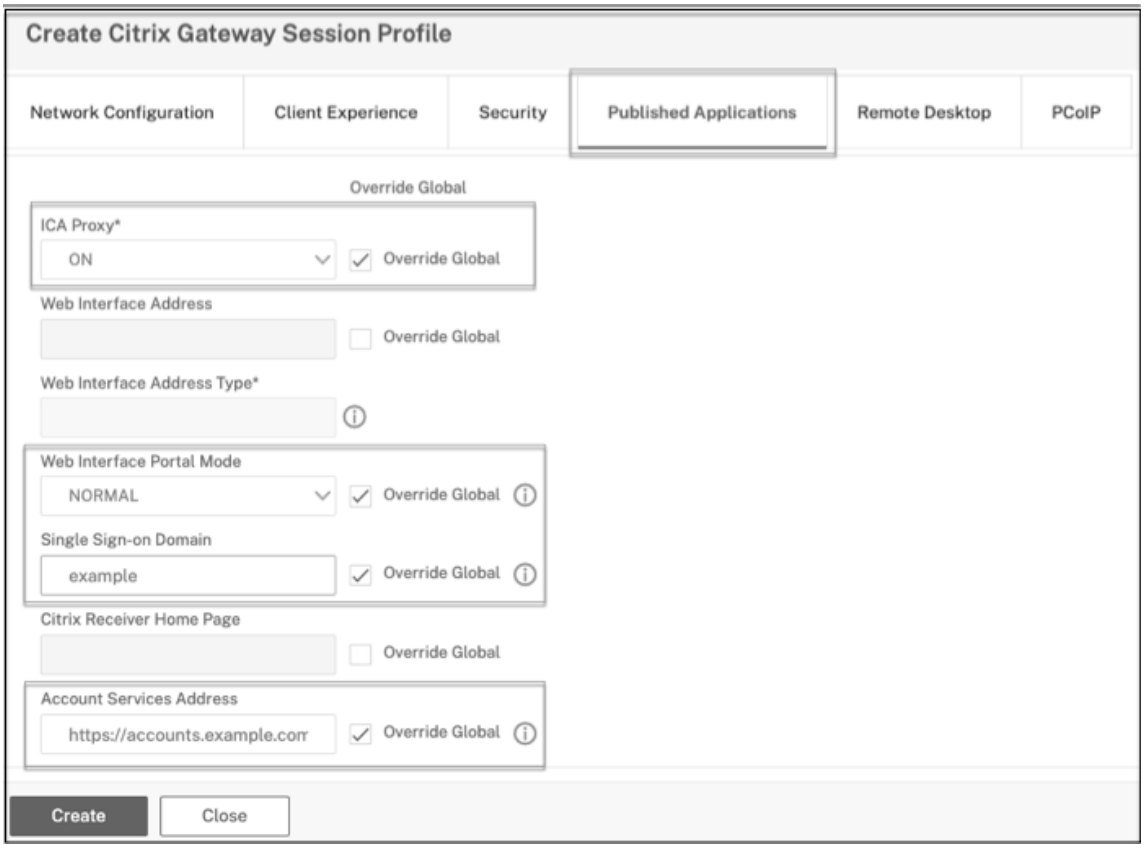
- ホームページ: 「なし」に設定
- 分割トンネル: **OFF** に設定
- クライアントレスアクセス: **[**オン**]** に設定
- **Web** アプリケーションへのシングル・サインオン: チェック・ボックスを選択します。
- プラグインの種類: **Java** に設定

7. [セキュリティ] タブで、[既定の承認操作] を [許可] に設定します。



8. [公開アプリケーション] タブで、次の設定を有効にします。

- **ICA** プロキシ: ON に設定します。
- **Web Interface** アドレス: StoreFront サーバーの FQDN に続いてストアへのパス
- シングル・サインオン・ドメイン: ドメインの NetBIOS 名
- アカウント・サービス所在地**:** アカウント・サービスの所在地を入力します。最後のバックスラッシュは重要です。



9. [作成] をクリックします。
10. クラシックポリシー式を使用している場合は、[式] フィールドに次の情報を追加し、[作成] をクリックします。

```
1 REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
```

11. 詳細ポリシー式を使用している場合は、[式] フィールドに次の情報を追加し、[作成] をクリックします。

```
1 HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
```


このポリシーは、Citrix ADC が Web ブラウザベースの接続と Citrix Workspace アプリベースの接続を区別するために必要です。このポリシーは、Citrix Workspace アプリベースの接続に適用されます。

Citrix ADC アプライアンスで認証を構成する

Citrix ADC アプライアンスでの LDAP 認証の構成については、LDAP 認証の構成を参照してください。

Citrix Gateway 仮想サーバーを作成し、セッションポリシーをバインドする

1. [**Citrix Gateway**] **>** [仮想サーバー] に移動し、[追加] をクリックして新しい仮想サーバーを追加します。
2. 仮想サーバーが作成されたら、会社の要件に基づいて特定のセッションポリシーを仮想サーバーにバインドします。

StoreFront の認証を構成する

1. StoreFront 上の Citrix Gateway からのパススルー認証を有効にします。詳しくは、「認証サービスの構成」を参照してください。

   StoreFront は、認証コールバックサービスの Citrix Gateway 仮想サーバーのバインドされた証明書（ルート証明書または中間証明書）の発行元を信頼する必要があります。

2. Citrix Gateway を StoreFront に追加します。詳しくは、「Citrix Gateway 接続の追加」を参照してください。

   ゲートウェイ URL は、ユーザが Web ブラウザのアドレスバーに入力する内容と正確に一致する必要があります。

3. StoreFront ストアでリモートアクセスを有効にします。詳しくは、「Citrix Gateway を介したストアへのリモートアクセスの管理」を参照してください。

エンタープライズブックマークの高度なポリシーサポート

March 26, 2020

エンタープライズブックマーク (VPN URL) を高度なポリシーとして設定できるようになりました。

VPN URL を高度なポリシーとして設定する

VPN URL を高度なポリシーとして設定するには、次のタスクを実行する必要があります。

- VPN URL アクションを作成する
- VPN URL ポリシーの作成）
- ポリシーをバインドポイントにバインドする

VPN URL アクションを作成する

コマンドプロンプトで、次のコマンドを入力します。

```
1 add vpn urlAction <name> -linkName <string> -actualURL <string> [-
    vServerName <string>] [-clientlessAccess ( ON | OFF )] [-comment <
    string>] [-iconURL <URL>] [-ssotype <ssotype>] [-applicationtype <
    applicationtype>] [-samlSSOProfile <string>]
```

VPN URL アクションを作成する

コマンドプロンプトで、次のコマンドを入力します。

```
1 add vpn urlAction <name> -linkName <string> -actualURL <string> [-
    vServerName <string>] [-clientlessAccess ( ON | OFF )] [-comment <
    string>] [-iconURL <URL>] [-ssotype <ssotype>] [-applicationtype <
    applicationtype>] [-samlSSOProfile <string>]
```

VPN URL アクションを作成する

コマンドプロンプトで、次のコマンドを入力します。

```
1 add vpn urlAction <name> -linkName <string> -actualURL <string> [-
    vServerName <string>] [-clientlessAccess ( ON | OFF )] [-comment <
    string>] [-iconURL <URL>] [-ssotype <ssotype>] [-applicationtype <
    applicationtype>] [-samlSSOProfile <string>]
```


VPN URL アクションに対する以下の操作がサポートされています

- **add**

```
add vpn urlAction <name> -linkName <string> -actualURL <string> [-
    vServerName <string>] [-clientlessAccess ( ON | OFF )] [-
    comment <string>] [-iconURL <URL>] [-ssotype <ssotype>] [-
    applicationtype <applicationtype>] [-samlSSOProfile <string>]
```

- **set**

```
set vpn urlAction <name> [-vServerName <string>] [-
    clientlessAccess ( ON | OFF )] [-comment <string>] [-iconURL <
    URL>] [-ssotype <ssotype>] [-applicationtype <applicationtype>]
     [-samlSSOProfile <string>]
```

- **unset**

```
unset vpn urlAction <name> [-vServerName] [-clientlessAccess] [-
    comment] [-iconURL] [-ssotype] [-applicationtype] [-
    samlSSOProfile]
```

- **show**

```
show vpn urlAction [<name>]
```

- **remove**

```
remove vpn urlAction <name>
```

- **rename**

```
rename vpn urlAction <name>@ <newName>@
```

Following operations for VPN URL policy are supported

- **add**

```
add vpn urlPolicy <name> -rule <expression> -action <string> [-
    comment <string>] [-logAction <string>]
```

- **set**

```
set vpn urlPolicy <name> [-rule <expression>] [-action <string>]
    [-comment <string>] [-logAction <string>]
```


- **unset**

```
unset vpn urlPolicy <name> [-comment] [-logAction]
```

- **show**

```
show vpn urlPolicy [<name>]
```

- **remove**

```
remove vpn urlPolicy <name>
```

- **rename**

```
rename vpn urlpolicy <name>@ <newName>@
```

- **stat**

```
stat vpn urlpolicy [<name>] [-detail] [-fullValues] [-ntimes <
    positive_integer>] [-logFile <input_filename>] [-clearstats (
    basic | full )]
```

- **bind**

```
bind vpn vserver <vserver name> -policy <string> -priority <
    positive_integer> [-gotoPriorityExpression <expression>]
bind vpn global -policyName <string> -priority <positive_integer>
    [-gotoPriorityExpression <expression>]
bind aaa user <userName> -policy <string> [-priority <
    positive_integer>] [-type <type>] [-gotoPriorityExpression <
    expression>]
bind aaa group <groupName> -policy <string> [-priority <
    positive_integer>] [-type <type>] [-gotoPriorityExpression <
    expression>]
```

- **unbind**

```
unbind vpn vserver <name> -policy <string>
unbind vpn global -policyName <string>
unbind aaa user <name> -policy <string>
unbind aaa group <name> -policy <string>
```

Note: Bind Points are aaauser, aaagroup, vpnvserver and vpnglobal.

エンドポイントポリシーの設定

March 26, 2020

エンドポイント分析は、ユーザーデバイスをスキャンし、オペレーティングシステムの存在やバージョンレベル、ウイルス対策ソフトウェア、ファイアウォールソフトウェア、または Web ブラウザソフトウェアなどの情報を検出するプロセスです。エンドポイント分析を使用して、ネットワークへの接続を許可するか、ユーザーがログオンした後も接続したままにする前に、ユーザーデバイスが要件を満たしていることを確認できます。ユーザーセッション中にユーザーデバイス上のファイル、プロセス、およびレジストリエントリを監視して、デバイスが引き続き要件を満たしていることを確認できます。

エンドポイントポリシーのしくみ

March 26, 2020

ユーザーがログオンする前に、ユーザーデバイスが特定のセキュリティ要件を満たしているかどうかを確認するように Citrix Gateway を構成できます。これを事前認証ポリシーと呼びます。ポリシー内で指定したウイルス対策、ファイアウォール、スパム対策、プロセス、ファイル、レジストリエントリ、インターネットセキュリティ、またはオペレーティングシステムについて、ユーザーデバイスをチェックするように Citrix Gateway を構成できます。ユーザーデバイスが事前認証スキャンに失敗した場合、ユーザーはログオンできません。

事前認証ポリシーで使用されない追加のセキュリティ要件を構成する必要がある場合は、セッションポリシーを構成し、ユーザーまたはグループにバインドします。このタイプのポリシーは、認証後ポリシーと呼ばれ、ウイルス対策ソフトウェアやプロセスなどの必要な項目が確実に当てはまるように、ユーザーセッション中に実行されます。

事前認証または認証後のポリシーを構成すると、Citrix Gateway はエンドポイント分析プラグインをダウンロードし、スキャンを実行します。ユーザーがログオンするたびに、エンドポイント分析プラグインが自動的に実行されます。

エンドポイントポリシーを設定するには、次の 3 種類のポリシーを使用します。

- yes または no パラメータを使用する事前認証ポリシー。スキャンによって、ユーザーデバイスが指定した要件を満たしているかどうかが判断されます。スキャンが失敗した場合、ユーザーはログオンページで資格情報を入力できません。
- 条件付きで、SmartAccess で使用できるセッションポリシー。
- セッションポリシー内のクライアントセキュリティ式。ユーザーデバイスがクライアントセキュリティ式の要件を満たさない場合は、ユーザーを検疫グループに配置するように設定できます。ユーザーデバイスがスキャンにパスした場合、ユーザーは別のグループに所属し、追加のチェックが必要になる場合があります。

検出された情報をポリシーに組み込んで、ユーザーデバイスに基づいて異なるレベルのアクセスを許可できます。たとえば、最新のウイルス対策ソフトウェアおよびファイアウォールソフトウェア要件を持つユーザーデバイスからリモートで接続するユーザーに、ダウンロード権限を持つフルアクセスを提供できます。信頼されていないコンピュー

タから接続しているユーザーには、より制限されたレベルのアクセスを提供して、ユーザーがリモートサーバー上のドキュメントをダウンロードせずに編集することができます。

エンドポイント分析では、次の基本的な手順が実行されます。

- ユーザーデバイスに関する情報の初期セットを調べ、適用するスキャンを決定します。
- 適用可能なすべてのスキャンを実行します。ユーザーが接続を試みると、Endpoint Analysis プラグインは、事前認証またはセッションポリシーで指定された要件をユーザーデバイス上でチェックします。ユーザーデバイスがスキャンにパスすると、ユーザーはログオンできます。ユーザーデバイスがスキャンに失敗した場合、ユーザーはログオンできません。
  注：エンドポイント分析のスキャンは、ユーザーセッションがライセンスを使用する前に完了します。
- ユーザーデバイス上で検出されたプロパティ値と、設定したスキャンでリストされた必要なプロパティ値を比較します。
- 必要なプロパティ値が見つかったかどうかを検証する出力を生成します。

> 注意：エンドポイント分析ポリシーの作成手順は一般的なガイドラインです。1 つのセッションポリシー内に多数の設定を使用できます。セッションポリシーを構成する具体的な手順には、特定の設定を構成するための指示が含まれている場合があります。ただし、その設定は、セッションプロファイルとポリシーに含まれる多くの設定の 1 つになる場合があります。

ユーザー・ログオン・オプションの評価

March 26, 2020

ユーザーがログオンするときに、エンドポイント分析スキャンをスキップすることを選択できます。ユーザーがスキャンをスキップすると、Citrix Gateway はこのアクションを失敗したエンドポイント分析として処理します。ユーザーがスキャンに失敗した場合、Web Interface またはクライアントレスアクセスでのみアクセスできます。

たとえば、Citrix Gateway プラグインを使用してユーザーにアクセスを許可する場合などです。プラグインを使用して Citrix Gateway にログオンするには、ユーザーがノートンアンチウイルスなどのウイルス対策アプリケーションを実行している必要があります。ユーザーデバイスでアプリケーションが実行されていない場合、ユーザーは Receiver でのみログオンし、公開アプリケーションを使用できます。クライアントレスアクセスを構成することもできます。これにより、Outlook Web Access などの特定のアプリケーションへのアクセスが制限されます。

このログオンシナリオを実現するように Citrix Gateway を構成するには、デフォルトのポリシーとして制限セッションポリシーを割り当てます。次に、ユーザーデバイスがエンドポイント分析スキャンに合格したときに、特権セッションポリシーにユーザーをアップグレードする設定を構成します。この時点で、ユーザーはネットワークレイヤーにアクセスでき、Citrix Gateway プラグインを使用してログオンできます。

最初に制限セッションポリシーを適用するように Citrix Gateway を構成するには、次の手順に従います。

- 指定したアプリケーションがユーザーデバイスで実行されていない場合は、ICA プロキシを有効にしてグローバル設定を行い、その他の必要な設定を行います。

- Citrix Gateway プラグインを有効にするセッションポリシーとプロファイルを作成します。
- セッションポリシーの規則部分内に次のような式を作成して、アプリケーションを指定します。

  （クライアント. アプリケーション. プロセス（symantec.exe）が存在する）

ユーザーがログオンすると、最初にセッションポリシーが適用されます。エンドポイントの分析が失敗した場合、またはユーザーがスキャンをスキップした場合、Citrix Gateway はセッションポリシーの設定を無視します（セッションポリシーの式は false とみなされます）。その結果、ユーザは Web Interface またはクライアントレスアクセスを使用したアクセスが制限されます。エンドポイントの分析に成功すると、Citrix Gateway はセッションポリシーを適用し、ユーザーは Citrix Gateway プラグインを使用してフルにアクセスできます。

事前認証ポリシーのプライオリティの設定

March 26, 2020

異なるレベルにバインドされた複数の事前認証ポリシーを持つことができます。たとえば、AAA Global にバインドされた特定のアンチウイルスアプリケーションをチェックするポリシーと、仮想サーバにバインドされたファイアウォールポリシーがあるとします。ユーザーがログオンすると、仮想サーバーにバインドされているポリシーが最初に適用されます。AAA Global でバインドされたポリシーが 2 番目に適用されます。

事前認証スキャンの順序を変更できます。Citrix Gateway でグローバルポリシーを適用するには、仮想サーバーにバインドされているポリシーの優先度番号を変更し、グローバルにバインドされているポリシーよりも高い優先度番号を設定します。たとえば、グローバルポリシーのプライオリティ番号を 1 に設定し、仮想サーバポリシーを 2 に設定します。ユーザーがログオンすると、Citrix Gateway が最初にグローバルポリシースキャンを実行し、次に仮想サーバーポリシースキャンを実行します。

事前認証ポリシーの優先順位を変更するには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、仮想サーバーを選択し、[開く] をクリックします。
3. [ポリシー] タブで、[事前認証] をクリックします。
4. [優先度] で、ポリシーの優先度番号を入力し、[OK] をクリックします。

事前認証ポリシーおよびプロファイルの設定

March 26, 2020

> 警告
>
> AAA 事前認証ポリシーは、NetScaler 12.0 ビルド 56.20 以降では非推奨です。代わりに、NfacCitrix 認証を使用することをお勧めします。詳細については、「多要素 (nFactor) 認証」を参照してください。

ユーザーが認証される前にクライアント側のセキュリティをチェックするように Citrix Gateway を構成できます。この方法では、Citrix Gateway とのセッションを確立するユーザーデバイスがセキュリティ要件に準拠していることを保証します。クライアント側のセキュリティチェックは、次の 2 つの手順で説明するように、仮想サーバまたはグローバルに固有の事前認証ポリシーを使用して設定します。

事前認証ポリシーは、プロファイルと式で構成されます。ユーザーデバイスでのプロセスの実行を許可または拒否するアクションを使用するように、プロファイルを構成します。たとえば、テキストファイル clienttext.txt がユーザーデバイスで実行されているとします。ユーザーが Citrix Gateway にログオンするときに、テキストファイルが実行されている場合はアクセスを許可または拒否できます。プロセスの実行中にユーザーにログオンを許可しない場合は、ユーザーがログオンする前にプロセスが停止するようにプロファイルを構成します。

事前認証ポリシーには、次の設定を構成できます。

- Expression. エクスプレッションの作成に役立つ次の設定が含まれています。
  - Expression. 作成されたエクスプレッションをすべて表示します。
  - Match Any Expression. 選択した式のリストにある式のいずれかに一致するように、ポリシーを設定します。
  - Match All Expressions. 選択した式のリストに存在するすべての式に一致するようにポリシーを設定します。
  - Tabular Expressions. OR (|||) または AND (&&) 演算子を使用して、既存の式を使用して複合式を作成します。
  - Advanced Free-Form. 式名と OR (|||) および AND (&&) 演算子を使用して、カスタムの複合式を作成します。必要なエクスプレッションのみを選択し、選択したエクスプレッションのリストから他のエクスプレッションを省略します。
  - Add 新しい式を作成します。
  - Modify. 既存の式を修正します。
  - Remove- 選択したエクスプレッションを複合エクスプレッションリストから削除します。
  - Named Expressions. 構成済みの名前付き式を選択します。Citrix Gateway にすでに存在する式のドロップダウンリストから、名前付き式を選択できます。
  - Add Expression. 選択した名前付き式をポリシーに追加します。
  - Replace Expression. 選択した名前付き式をポリシーに置き換えます。
  - Preview Expression. 名前付き式を選択したときに Citrix Gateway で構成される詳細なクライアントセキュリティ文字列が表示されます。

構成ユーティリティを使用して事前認証プロファイルをグローバルに設定するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。

2. 詳細ウィンドウで、[設定] の [事前認証設定の変更] をクリックします。
3. [グローバル事前認証設定] ダイアログボックスで、次の設定を構成します。
   a)「アクション」で、「許可」または「拒否」を選択します。
   エンドポイントの分析後にユーザーがログオンすることを拒否または許可します。
   b)「取消するプロセス」に、プロセスを入力します。
   エンドポイント分析プラグインで停止するプロセスを指定します。
   c)「削除するファイル」にファイル名を入力します。
   エンドポイント分析プラグインによって削除するファイルを指定します。
4. Expression では、式を ns_true のままにしておくか、ウイルス対策ソフトウェアやセキュリティソフトウェアなどの特定のアプリケーション用の式を作成し、[OK] をクリックします。

構成ユーティリティを使用して事前認証プロファイルを構成するには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway]、[ポリシー]、[認証/承認] の順に展開し、[認証前 EPA] をクリックします。
2. 詳細ウィンドウの [プロファイル] タブで、[追加] をクリックします。
3. [名前] に、確認するアプリケーションの名前を入力します。
4.「アクション」で、「使用する」または「拒否」を選択します。
5. [キャンセルするプロセス] に、停止するプロセスの名前を入力します。
6. [削除するファイル] ボックスに、削除するファイルの名前を入力します (c:\clientext.txt など)。[作成] をクリックし、[閉じる] をクリックします。

> 注記: ファイルを削除したり、プロセスを停止したりすると、確認を求めるメッセージが表示されます。
> ステップ 5 と 6 はオプションのパラメータです。

構成ユーティリティを使用して事前認証プロファイルを構成する場合は、[ポリシー] タブの [追加] をクリックして事前認証ポリシーを作成します。[事前認証ポリシーの作成] ダイアログボックスで、[要求プロファイル] ドロップダウンリストからプロファイルを選択します。

エンドポイント分析式の設定

March 26, 2020

事前認証およびクライアントセキュリティセッションポリシーには、プロファイルと式が含まれます。ポリシーには、1 つのプロファイルと複数の式を含めることができます。ユーザーデバイスをスキャンしてアプリケーション、ファイル、プロセス、またはレジストリエントリを検索するには、ポリシー内に式または複合式を作成します。

式のタイプ

式は、式タイプと式のパラメータで構成されます。式には、次のタイプがあります。

- 一般
- クライアントのセキュリティ
- ネットワークベース

事前認証ポリシーへの事前設定式の追加

Citrix Gateway には、名前付き式と呼ばれる構成済みの式が付属しています。ポリシーを設定する場合、ポリシーに名前付き式を使用できます。たとえば、事前認証ポリシーで、ウイルス定義が更新された Symantec AntiVirus 10 の有無を確認するとします。事前認証ポリシーを作成し、次の手順に従って式を追加します。

事前認証またはセッションポリシーを作成するときに、ポリシーを作成するときに式を作成できます。その後、式を使用してポリシーを仮想サーバに適用するか、グローバルに適用できます。

次の手順では、構成ユーティリティを使用して、構成済みのウイルス対策式をポリシーに追加する方法について説明します。

事前認証ポリシーに名前付き式を追加するには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway]、[ポリシー]、[認証/承認] の順に展開し、[認証前 EPA] をクリックします。
2. 詳細ペインでポリシーを選択し、[開く] をクリックします。
3. [名前付き式] の横にある [アンチウイルス] を選択し、一覧からウイルス対策製品を選択し、[式の追加]、[作成]、[閉じる] の順にクリックします。

カスタム式の設定

March 26, 2020

カスタム式は、ポリシー内に作成する式です。式を作成するときは、式のパラメータを設定します。

カスタムクライアントセキュリティ式を作成して、よく使用されるクライアントセキュリティ文字列を参照することもできます。これにより、事前認証ポリシーの設定プロセスや、設定済みの式のメンテナンスが容易になります。

たとえば、Symantec AntiVirus 10 用のカスタムのクライアントセキュリティ式を作成し、ウイルス定義が 3 日以内であることを確認します。新しいポリシーを作成し、ウイルス定義を指定する式を構成します。

次の手順は、事前認証ポリシーでクライアントセキュリティポリシーを作成する方法を示しています。セッションポリシーで同じ手順を使用できます。

事前認証ポリシーとカスタムクライアントセキュリティ式を作成するには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway]、[ポリシー]、[認証/承認] の順に展開し、[認証前 EPA] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。[事前認証ポリシーの作成] ダイアログボックスが表示されます。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [認証プロファイルの作成] ダイアログボックスの [名前] にプロファイルの名前を入力し、[操作] で [許可] を選択し、[作成] をクリックします。
6. [事前認証ポリシーの作成] ダイアログボックスで、[任意の式に一致] の横にある [追加] をクリックします。
7.「式の種類」で、「クライアント・セキュリティ」を選択します。
8. 次のオプションを構成します:
   a) [コンポーネント] で、[アンチウイルス] を選択します。
   b) [名前] に、アプリケーションの名前を入力します。
   c)「修飾子」で、「バージョン」を選択します。
   d)「演算子」で「= =」を選択します。
   e) [値] に値を入力します。
   f) [鮮度] に 3 と入力し、[OK] をクリックします。
9. [事前認証ポリシーの作成] ダイアログボックスで、[作成] をクリックし、[閉じる] をクリックします。

カスタム式を構成すると、ポリシーダイアログボックスの [式] ボックスにカスタム式が追加されます。

複合式を設定する

April 9, 2020

事前認証ポリシーには、1 つのプロファイルと複数の式を含めることができます。複合式を設定する場合は、演算子を使用して式の条件を指定します。たとえば、複合式を構成して、ユーザーデバイスで次のいずれかのウイルス対策アプリケーションの実行を要求できます。

- Symantec Antivirus 10
- McAfee Antivirus 11
- Sophos Antivirus 4

上記の 3 つのアプリケーションを確認するには、OR 演算子を使用して式を構成します。Citrix Gateway がユーザーデバイス上のアプリケーションの正しいバージョンを検出すると、ユーザーはログオンできます。ポリシーダイアログボックスの式は、次のように表示されます。

av_5_Symantec_1	av_5_McAfeevirus	av_5_sophos_4

複合エクスプレッションの詳細については、「複合式を設定する」を参照してください。

事前認証ポリシーのバインド

March 26, 2020

事前認証またはクライアントセキュリティセッションポリシーを作成したら、ポリシーを適用するレベルにバインドします。事前認証ポリシーは、仮想サーバに、またはグローバルにバインドできます。

事前認証ポリシーをグローバルに作成およびバインドするには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[事前認証設定の変更] をクリックします。
3. [グローバル事前認証設定] ダイアログボックスの [操作] で、[許可] または [拒否] を選択します。
4. [名前] に、ポリシーの名前を入力します。
5. [グローバル事前認証 settigns] ダイアログボックスで、[名前付き式] の横にある [全般]、[True value]、[式の追加]、[作成]、[閉じる] の順にクリックします。

事前認証ポリシーを仮想サーバにバインドするには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、仮想サーバーを選択し、[開く] をクリックします。
3. Citrix Gateway 仮想サーバーの構成］ダイアログボックスで、［ポリシー］タブをクリックし、［事前認証］をクリックします。
4. [詳細] の [ポリシーの挿入] をクリックし、[ポリシー名] で事前認証ポリシーを選択します。
5. ［OK］をクリックします。

事前認証ポリシーのバインド解除と削除

March 26, 2020

必要に応じて、Citrix Gateway から事前認証ポリシーを削除できます。事前認証ポリシーを削除する前に、仮想サーバから、またはグローバルにバインド解除します。

グローバルな事前認証ポリシーをバインド解除するには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway]、[ポリシー]、[認証/承認] の順に展開し、[認証前 EPA] をクリックします。
2. 詳細ペインでポリシーを選択し、[操作] で [グローバルバインド] をクリックします。

3. [事前認証ポリシーをグローバルにバインド/バインド解除] ダイアログボックスで、ポリシーを選択し、[ポリシーのバインド解除] をクリックして、[OK] をクリックします。

仮想サーバから事前認証ポリシーをバインド解除するには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. Citrix Gateway 仮想サーバーの構成］ダイアログボックスで、［ポリシー］タブをクリックし、［事前認証］をクリックします。
3. ポリシーを選択し、[ポリシーのバインド解除] をクリックします。

事前認証ポリシーがバインド解除されている場合は、Citrix Gateway からポリシーを削除できます。

事前認証ポリシーを削除するには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway]、[ポリシー]、[認証/承認] の順に展開し、[認証前 EPA] をクリックします。
2. で、ポリシーを選択し、[削除] をクリックします。

認証後ポリシーの設定

April 9, 2020

認証後のポリシーは、セッションをアクティブに保つためにユーザーデバイスが満たす必要のある汎用規則のセットです。ポリシーが失敗すると、Citrix Gateway への接続は終了します。認証後のポリシーを構成する場合、条件付きにできるユーザー接続の設定を構成できます。

> 注：この機能は、Citrix Gateway プラグインでのみ機能します。ユーザーが Citrix Workspace アプリでログオンした場合、エンドポイント分析スキャンはログオン時にのみ実行されます。

セッションポリシーを使用して、認証後のポリシーを設定します。まず、ポリシーを適用するユーザーを作成します。次に、ユーザーをグループに追加します。次に、セッション、トラフィックポリシー、およびイントラネットアプリケーションをグループにバインドします。

承認グループとしてグループを指定することもできます。このタイプのグループでは、セッションポリシー内のクライアントセキュリティ表現に基づいて、ユーザーをグループに割り当てることができます。

また、ユーザーデバイスがポリシーの要件を満たしていない場合に、ユーザーを隔離グループに入れるように認証後のポリシーを設定することもできます。単純なポリシーには、クライアントセキュリティ式とクライアントセキュリティメッセージが含まれます。ユーザーが検疫グループに属している場合、ユーザーは Citrix Gateway にログオンできますが、ネットワークリソースへのアクセスは制限されます。

同じセッションプロファイルとポリシーを使用して、承認グループと検疫グループを作成することはできません。認証後のポリシーを作成する手順は同じです。セッションポリシーを作成するときは、承認グループまたは検疫グループを選択します。2 つのセッションポリシーを作成し、各ポリシーをグループにバインドできます。

認証後のポリシーは、SmartAccess でも使用されます。SmartAccess について詳しくは、「Citrix Gateway での SmartAccess 構成」を参照してください。

認証後ポリシーの設定

March 26, 2020

セッションポリシーを使用して、認証後のポリシーを構成します。単純なポリシーには、クライアントセキュリティ式とクライアントセキュリティメッセージが含まれます。

認証後のポリシーを構成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、[**Citrix Gateway**] **>** [ポリシー] の順に展開し、[セッション] をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. [セキュリティ] タブで、[詳細設定] をクリックします。
7. [クライアントセキュリティ] で、[グローバルに上書き] をクリックし、[新規] をクリックします。
8. クライアントセキュリティ式を構成し、[Create] をクリックします。
9. [Client Security] の [検疫グループ] で、グループを選択します。
10. [エラーメッセージ] に、認証後のスキャンが失敗した場合にユーザーに受信させるメッセージを入力します。
11. [承認グループ] の [グローバルに上書き] をクリックし、グループを選択して [追加] をクリックし、[OK] をクリックして、[作成] をクリックします。
12. [セッションポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [全般]、[True value]、[式の追加]、[作成]、[閉じる] の順にクリックします。

認証後スキャンの頻度の設定

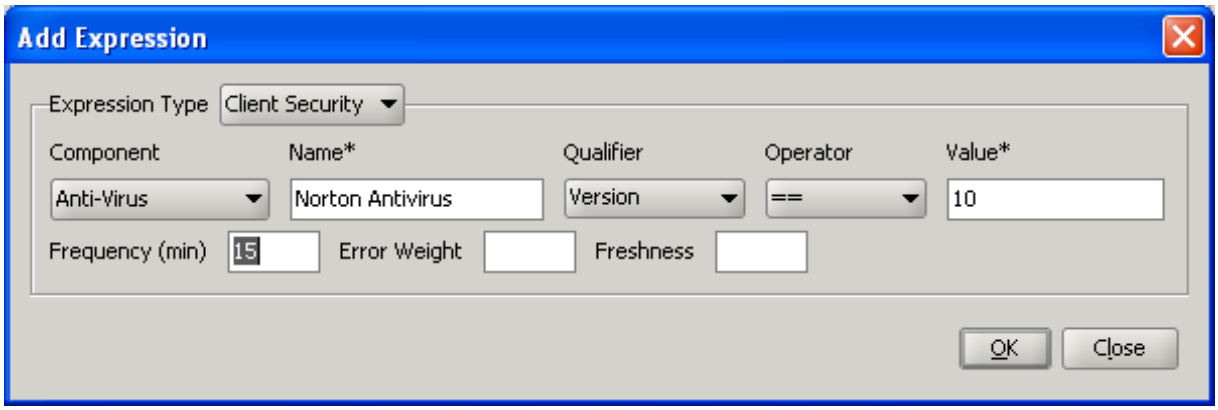
April 9, 2020

指定した間隔で認証後のポリシーを実行するように Citrix Gateway を構成できます。たとえば、クライアントセキュリティポリシーを構成し、10 分ごとにユーザーデバイスで実行するとします。この頻度は、ポリシー内でカスタム式を作成することによって設定できます。

> 注：認証後のポリシーの頻度チェック機能は、Citrix Gateway プラグインでのみ機能します。ユーザーが Citrix Workspace アプリでログオンした場合、エンドポイント分析スキャンはログオン時にのみ実行されます。

この手順認証後ポリシーの設定に従って、クライアントセキュリティポリシーを構成するときに、頻度 (分単位) を設定できます。次の図は、[式の追加] ダイアログボックスで頻度値を入力できる場所を示しています。

図 1：認証後のスキャンの頻度を設定するためのダイアログボックス



検疫および認可グループの設定

March 26, 2020

ユーザーが Citrix Gateway にログオンすると、Citrix Gateway またはセキュリティで保護されたネットワーク内の認証サーバーで構成したグループに割り当てられます。ユーザーが認証後のスキャンに失敗した場合、そのユーザーを検疫グループと呼ばれる制限されたグループに割り当てることができます。これにより、ネットワークリソースへのアクセスが制限されます。

また、認可グループを使用して、ネットワークリソースへのユーザーアクセスを制限することもできます。たとえば、電子メールサーバーとファイル共有にのみアクセスできる契約担当者のグループがあるとします。ユーザーデバイスが Citrix Gateway で定義したセキュリティ要件に合格すると、ユーザーは動的にグループのメンバーになることができます。

ユーザー、グループ、または仮想サーバーにバインドされた検疫グループと承認グループを構成するには、グローバル設定またはセッションポリシーのいずれかを使用します。セッションポリシー内のクライアントセキュリティ表現に基づいて、ユーザーをグループに割り当てることができます。ユーザーがグループのメンバーである場合、Citrix Gateway はグループメンバーシップに基づいてセッションポリシーを適用します。

隔離グループの設定

March 26, 2020

隔離グループを構成する場合、セッションプロファイル内の [セキュリティ設定-詳細設定] ダイアログボックスを使用して、クライアントセキュリティ式を構成します。

検疫グループのクライアントセキュリティ式を構成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. [セキュリティ] タブで、[詳細設定] をクリックします。
7. [クライアントセキュリティ] で、[グローバルに上書き] をクリックし、[新規] をクリックします。
8. [クライアント式] ダイアログボックスで、クライアントセキュリティ式を構成し、[作成] をクリックします。
9. [検疫グループ] で、グループを選択します。
10. [エラーメッセージ] で、ユーザーの問題を説明するメッセージを入力し、[作成] をクリックします。
11. [セッションポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [全般]、[True value]、[式の追加]、[作成]、[閉じる] の順にクリックします。

セッション・ポリシーを作成したら、ユーザー、グループ、または仮想サーバーにバインドします。

> 注
>
> エンドポイント分析スキャンが失敗し、ユーザーが検疫グループに入った場合、検疫グループにバインドされたポリシーは、その検疫グループにバインドされたポリシーと同等または低い優先順位を持つユーザーに直接バインドされたポリシーがない場合にのみ有効になります。

グローバル隔離グループを構成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [セキュリティ] タブで、[詳細設定] をクリックします。
4. [クライアントセキュリティ] で、クライアントセキュリティ式を構成します。
5. [検疫グループ] で、グループを選択します。
6. [エラーメッセージ] で、ユーザーの問題を説明するメッセージを入力し、[OK] をクリックします。

認可グループの設定

March 26, 2020

エンドポイント分析スキャンを設定する場合、ユーザーデバイスがスキャンに合格したときにユーザーを許可グループに動的に追加できます。たとえば、ユーザーデバイスのドメインのメンバーシップをチェックするエンドポイント分析スキャンを作成します。Citrix Gateway で、ドメインに参加したコンピュータと呼ばれるローカルグループを作成し、スキャンに合格したユーザーの承認グループとして追加します。ユーザーがグループに参加すると、ユーザーはグループに関連付けられたポリシーを継承します。

認可ポリシーをグローバルにバインドすることも、仮想サーバにバインドすることもできません。ユーザーが Citrix Gateway 上の別のグループのメンバーとして構成されていない場合、承認グループを使用して、デフォルトの承認ポリシーセットを提供できます。

セッションポリシーを使用して承認グループを構成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. [セキュリティ] タブで、[詳細設定] をクリックします。
7. [承認グループ] の [グローバルに上書き] をクリックし、ドロップダウンリストからグループを選択し、[追加] をクリックして [OK] をクリックし、[作成] をクリックします。
8. [セッションポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [全般]、[True value]、[式の追加]、[作成]、[閉じる] の順にクリックします。

セッション・ポリシーを作成したら、ユーザー、グループ、または仮想サーバーにバインドできます。

グローバル認可グループを設定するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [セキュリティ] タブで、[詳細設定] をクリックします。
4. [承認グループ] で、ドロップダウンリストからグループを選択し、[追加] をクリックし、[OK] を 2 回クリックします。

承認グループをグローバルにまたはセッションポリシーから削除する場合は、[セキュリティの設定-詳細] ダイアログボックスで、リストから承認グループを選択し、[削除] をクリックします。

ユーザデバイスのセキュリティ事前認証式の設定

March 26, 2020

Citrix Gateway では、ユーザーのログオン時やセッション中の他の構成時にさまざまなエンドポイントセキュリティチェックが提供され、セキュリティの向上に役立ちます。Citrix Gateway セッションを確立できるのは、これらのセキュリティチェックに合格したユーザーデバイスだけです。

Citrix Gateway 上で構成できるユーザーデバイスのセキュリティチェックの種類を次に示します。

- アンチスパム
- アンチウイルス
- ファイル・ポリシー
- インターネットセキュリティ
- OS
- パーソナルファイアウォール
- プロセスポリシー
- レジストリポリシー
- サービスポリシー

ユーザーデバイスでセキュリティチェックが失敗した場合、後続のチェックに合格するまで新しい接続は行われません（定期的なチェックの場合）。ただし、既存の接続を通過するトラフィックは、Citrix Gateway を経由してトンネルされ続けます。

設定ユーティリティを使用すると、ユーザデバイス上でセキュリティチェックを実行するように設計されたセッションポリシー内で、事前認証ポリシーまたはセキュリティ表現を設定できます。

ウイルス対策、ファイアウォール、インターネットセキュリティ、またはスパム対策の式を構成する

March 26, 2020

ウイルス対策ポリシー、ファイアウォールポリシー、インターネットセキュリティポリシー、およびスパム対策ポリシーの設定は、[式の追加] ダイアログボックスで行います。各ポリシーの設定は同じです。相違点は選択した値です。たとえば、Norton AntiVirus バージョン 10 および ZoneAlarm Pro のユーザーデバイスを確認する場合は、セッションポリシーまたは事前認証ポリシー内で、各アプリケーションの名前とバージョン番号を指定する 2 つの式を作成します。

式の種類として [Client Security] を選択すると、次の項目を構成できます。

- コンポーネント: アンチウイルス、ファイアウォール、レジストリエントリなど、クライアントセキュリティのタイプ。

- 名前: アプリケーション、プロセス、ファイル、レジストリエントリ、またはオペレーティングシステムの名前。
- 修飾子: 式がチェックするコンポーネントのバージョンまたは値。
- 演算子: 値が存在するか、値と等しいかどうかをチェックします。
- 値: ユーザーデバイス上のアンチウイルス、ファイアウォール、インターネットセキュリティ、またはスパム対策ソフトウェアのアプリケーションバージョンです。
- 頻度: 認証後のスキャンを実行する頻度 (分単位)。
- エラー重み: 複数の式が異なるエラー文字列を持つ場合に、ネストされた式に含まれる各エラーメッセージに割り当てられた重み。重みによって、表示されるエラーメッセージが決まります。
- 新鮮さ: ウイルス定義がどれくらい古いかを定義します。たとえば、ウイルス定義が 3 日以内に経過しないように式を構成できます。

クライアントセキュリティポリシーを事前認証またはセッションポリシーに追加するには

1. 構成ユーティリティのナビゲーションペインで、次のいずれかの操作を行います。
   a) 構成ユーティリティーの構成タブのナビゲーションペインで、[Citrix Gateway] > [ポリシー] の順に展開し、[セッション] をクリックします。
   b) 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway]、[ポリシー]、[認証/承認] の順に展開し、[認証前 EPA] をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [任意の式と一致] の横にある [追加] をクリックします。
5. [式の追加] ダイアログボックスの [式の種類] で、[クライアントセキュリティ] を選択します。
6. 次の設定を行います。
   a)「コンポーネント」で、スキャンするアイテムを選択します。
   b) [名前] に、アプリケーションの名前を入力します。
   c)「修飾子」で、「バージョン」を選択します。
   d)「演算子」で、値を選択します。
   e) [値] にクライアントのセキュリティ文字列を入力し、[OK] をクリックし、[作成] をクリックして [閉じる] をクリックします。

サービスポリシーの設定

March 26, 2020

サービスは、ユーザーデバイス上でサイレントに実行されるプログラムです。セッションまたは事前認証ポリシーを作成するときに、セッションが確立されたときにユーザーデバイスが特定のサービスを確実に実行するようにする式を作成できます。

サービスポリシーを設定するには

1. 構成ユーティリティのナビゲーションペインで、次のいずれかの操作を行います。
   a) 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］ > ［ポリシー］の順に展開し、［セッション］ をクリックします。
   b) 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway]、[ポリシー]、[認証/承認] の順に展開し、[認証前 EPA] をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [任意の式と一致] の横にある [追加] をクリックします。
5. [式の追加] ダイアログボックスの [式の種類] で、[クライアントセキュリティ] を選択します。
6. 次の設定を行います。
   a)「コンポーネント」で、「サービス」を選択します。
   b) [名前] に、サービスの名前を入力します。
   c)「修飾子」で、空白のままにするか、「バージョン」を選択します。
   d)「修飾子」での選択に応じて、次のいずれかの操作を行います。
      - 空白のままの場合は、「演算子」で「==」または「!」を選択します。=
      - [バージョン] を選択した場合は、[演算子] の [値] に値を入力し、[OK] をクリックして、[閉じる] をクリックします。

使用可能なすべてのサービスの一覧と、次の場所にある Windows ベースのコンピュータ上の各サービスの状態を確認できます。

[コントロールパネル] > [管理ツール] > [サービス]

> 注**:** 各サービスのサービス名は、リストされている名前とは異なります。[
> プロパティ] ダイアログボックスを表示して、サービスの名前を確認します。

プロセスポリシーの設定

March 26, 2020

セッションまたは事前認証ポリシーを作成するときに、ユーザーのログオン時にすべてのユーザーデバイスに特定のプロセスが実行されるように要求するルールを定義できます。このプロセスは、任意のアプリケーションであり、カスタマイズされたアプリケーションを含むことができます。

注:Windows ベースのコンピューターで実行されているすべてのプロセスの一覧は、Windows タスクマネージャーの [
プロセス] タブに表示されます。

プロセスポリシーを設定するには

1. 構成ユーティリティのナビゲーションペインで、次のいずれかの操作を行います。
   a) 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］ > ［ポリシー］の順に展開し、［セッション］をクリックします。
   b) 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway]、[ポリシー]、[認証/承認] の順に展開し、[認証前 EPA] をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [任意の式と一致] の横にある [追加] をクリックします。
5. [式の追加] ダイアログボックスの [式の種類] で、[クライアントセキュリティ] を選択します。
6. 次の設定を行います。
   a)「コンポーネント」で、「プロセス」を選択します。
   b) [名前] に、アプリケーションの名前を入力します。
   c)「演算子」で、「EXISTS」または「NOTEXISTS」を選択し、「OK」をクリックして「閉じる」をクリックします。

エンドポイント分析ポリシー（事前認証または認証後）を設定してプロセスをチェックする場合、MD5 チェックサムを設定できます。

ポリシーの式を作成するときに、チェックするプロセスに MD5 チェックサムを追加できます。たとえば、ユーザーデバイス上で notepad.exe が実行されているかどうかを確認する場合、式は次のようになります。
CLIENT.APPLICATION.PROCESS(notepad.exe_md5_388b8fbc36a8558587afc90fb23a3b00) EXISTS

オペレーティングシステムポリシーの構成

March 26, 2020

セッションまたは事前認証ポリシーを作成するときに、クライアントのセキュリティ文字列を構成して、ユーザーのログオン時にユーザーデバイスが特定のオペレーティングシステムを実行しているかどうかを判断できます。また、式を構成して、特定の Service Pack または修正プログラムを確認することもできます。

Windows および Macintosh の値は次のとおりです。

OS	値
Mac OS X	macos
Windows 8.1	win8.1
Windows 8	win8
Windows 7	win7

OS	値
Windows Vista	vista
Windows XP	winxp
Windows Server 2008	win2008
Windows Server 2003	win2003
Windows 2000 Server	win2000
Windows 64-bit platform	win64

オペレーティングシステムポリシーを構成するには

1. 構成ユーティリティのナビゲーションペインで、次のいずれかの操作を行います。
   a) 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
   b) 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway]、[ポリシー]、[認証/承認] の順に展開し、[認証前 EPA] をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [任意の式と一致] の横にある [追加] をクリックします。
5. [式の追加] ダイアログボックスの [式の種類] で、[クライアントセキュリティ] を選択します。
6. 次の設定を行います。
   a)「コンポーネント」で、「オペレーティング・システム」を選択します。
   b) [名前] に、オペレーティングシステムの名前を入力します。
   c)「修飾子」で、次のいずれかの操作を行います。
      - 空白のままにします。
      - [サービスパック] を選択します。
      -「修正プログラム」を選択します。
      -「バージョン」(Mac OS X のみ) を選択します。
   d) 手順 C での選択に応じて、「演算子」で次のいずれかの操作を行います。
      - 修飾子が空白の場合は、「演算子」で「等式 (= =)」、「NOTEQUAL (!」=)、存在または注意事項。
      - [サービスパック] または [修正プログラム] を選択した場合は、演算子を選択し、[値] に値を入力します。
7. ［Create］をクリックしてから、［Close］をクリックします。

client.os（winxp）.sp などのサービスパックを構成する場合、［値］フィールドに数値が含まれていない場合、式が無効であるため、Citrix Gateway からエラーメッセージが返されます。

オペレーティングシステムに Service Pack 3 や Service Pack 4 などのサービスパックが存在する場合は、Service Pack 4 の存在が自動的に以前のサービスパックが存在することを示すため、Service Pack 4 のチェックのみを構成

できます。

レジストリポリシーの構成

March 26, 2020

セッションまたは事前認証ポリシーを作成するときに、ユーザーデバイス上のレジストリエントリの存在と値を確認できます。セッションが確立されるのは、特定のエントリが存在するか、設定済みまたはそれ以上の値がある場合だけです。

レジストリ式を設定する場合は、次のガイドラインに従ってください。

- 4 つのバックスラッシュは、キーとサブキーを区切るために使用されます。たとえば、

  HKEY_LOCAL_MACHINE\\\\SOFTWARE

- アンダースコアは、サブキーと関連する値の名前を区切るために使用されます。たとえば、

  HKEY_LOCAL_MACHINE\\\\SOFTWARE\\\\VirusSoftware_Version

- バックスラッシュ (\) は、次の 2 つの例のように、スペースを表すために使用されます。

  HKEY_LOCAL_MACHINE\\\\SOFTWARE\\Citrix\\\\Secure\ Access\ Client_ProductVersion

  CLIENT.REG(HKEY_LOCAL_MACHINE\\\\Software\\\\Symantec\\Norton\ AntiVirus_Version).VALUE == 12.8.0.4 -frequency 5

以下は、ユーザーのログオン時に Citrix Gateway プラグインのレジストリキーを検索するレジストリ式です。

CLIENT.REG(secureaccess).VALUE==HKEY_LOCAL_MACHINE\\\\SOFTWARE\\\\CITRIX\\\\Secure\Access\Client_Pro

> 注意**:** レジストリ・キーと値をスキャンし、「
> 式」ダイアログ・ボックスで「
> 高度なフリー・フォーム」を選択した場合、式は
> CLIENT.REG で始まる必要があります。

レジストリチェックは、次の最も一般的な 5 つのタイプでサポートされています。

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

チェックするレジストリ値は、次のタイプを使用します。

- 文字列

  文字列値の型の場合、大文字と小文字の区別がチェックされます。

- DWORD

  DWORD 型の場合、値は比較され、等しくなければなりません。

- 展開された文字列

  バイナリやマルチストリングなどの他の型はサポートされていません。

- '==' 比較演算子のみがサポートされています。
- <、> などの比較演算子や、大文字と小文字を区別する比較演算子はサポートされていません。
- レジストリ文字列の長さの合計は 256 バイト未満である必要があります。

式に値を追加できます。値には、ソフトウェアバージョン、サービスパックのバージョン、またはレジストリに表示されるその他の値を指定できます。レジストリ内のデータ値がテスト対象の値と一致しない場合、ユーザーはログオンを拒否されます。

> 注：サブキー内の値をスキャンすることはできません。スキャンは、名前付きの値と関連するデータ値と一致する必要があります。

レジストリポリシーを構成するには

1. 構成ユーティリティのナビゲーションペインで、次のいずれかの操作を行います。
   a) 構成ユーティリティーの構成タブのナビゲーションペインで、[Citrix Gateway] > [ポリシー] の順に展開し、[セッション] をクリックします。
   b) 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway]、[ポリシー]、[認証/承認] の順に展開し、[認証前 EPA] をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [任意の式と一致] の横にある [追加] をクリックします。
5. [式の追加] ダイアログボックスの [式の種類] で、[クライアントセキュリティ] を選択します。
6. 次の設定を行います。
   a)「コンポーネント」で、「レジストリ」を選択します。
   b) [名前] に、レジストリキーの名前を入力します。
   c)「修飾子」で、空白のままにするか、「値」を選択します。
   d)「演算子」で、次のいずれかの操作を行います。
      - 修飾子が空白のままの場合は、[存在する] または [メモ] を選択します。
      -「修飾子」で「値」を選択した場合は、「==」または「!」のいずれかを選択します。==
   e) [値] で、レジストリエディターに表示される値を入力し、[OK] をクリックし、[閉じる] をクリックします。

複合クライアントセキュリティ式の設定

March 26, 2020

クライアントセキュリティ文字列を組み合わせて、複合クライアントセキュリティ式を作成できます。

Citrix Gateway でサポートされているブール演算子は次のとおりです。

- And (&&)
- Or (||)
- Not (!)

精度を高めるために、括弧を使用して文字列をグループ化することができます。

> 注**:** コマンドラインを使用して式を設定する場合は、複合式を作成するときに、カッコを使用してセキュリティ式をグループ化します。カッコを使用すると、クライアント式の理解とデバッグが向上します。

AND (&&) 演算子を使用したポリシーの構成

AND (&&) 演算子は、2 つのクライアントセキュリティ文字列を組み合わせて機能し、両方のチェックが true の場合にのみ複合チェックに合格するようにします。式は左から右に評価され、最初のチェックが失敗した場合、2 番目のチェックは実行されません。

AND（&&）演算子は、キーワード「AND」または記号'&&&' を使用して構成できます。

例:

以下は、ユーザーデバイスにバージョン 7.0 の Sophos AntiVirus がインストールされ、実行されているかどうかを判断するクライアントセキュリティチェックです。また、同じコンピュータ上で netlogon サービスが実行されているかどうかも確認します。

CLIENT.APPLICATION.AV(sophos).version==7.0 AND CLIENT.SVC(netlogon) EXISTS

この文字列は、次のように設定することもできます。

CLIENT.APPLICATION.AV(sophos).version==7.0 && CLIENT.SVC(netlogon) EXISTS

OR (||) 演算子を使用したポリシーの構成

OR (	）演算子は、2 つのセキュリティ文字列を組み合わせることによって機能します。いずれかのチェックが true の場合、複合チェックは合格します。式は左から右に評価され、最初のチェックが合格した場合、2 番目のチェックは実行されません。最初のチェックが合格しない場合は、2 番目のチェックが実行されます。

次を構成できます。 OR（	) 演算子。次を使用： ‘OR’ または記号’	’.

例：

以下は、ユーザーデバイスにファイル c:\file.txt があるか、putty.exe プロセスが実行されているかを判断するクライアントのセキュリティチェックです。

client.file(c:\\\\file.txt) EXISTS) OR (client.proc(putty.exe) EXISTS

この文字列は、次のように構成できます。

client.file(c:\\\\file.txt) EXISTS)	(client.proc(putty.exe) EXISTS

NOT (!) 演算子を使用したポリシーの構成

NOT (!) または否定演算子は、クライアントのセキュリティ文字列を否定します。

例：

ファイル c:\sophos_virus_defs.dat ファイルが 2 日以内に経過している場合、次のクライアントセキュリティチェックはパスします。

!(client.file(c:\\\\sophos_virus_defs.dat).timestamp==2dy)

高度なエンドポイント分析スキャン

March 26, 2020

高度なエンドポイント分析（EPA）は、Citrix Gateway アプライアンス上で構成されたエンドポイントセキュリティ要件について、ユーザーデバイスをスキャンするために使用されます。ユーザーデバイスが Citrix Gateway アプライアンスにアクセスしようとすると、管理者が Citrix Gateway アプライアンスへのアクセスを許可する前に、デバイス上でオペレーティングシステム、ウイルス対策、Web ブラウザーのバージョンなどのセキュリティ情報がスキャンされます。

高度な EPA スキャンはポリシーベースのスキャンで、Citrix Gateway アプライアンスで事前認証セッションと認証後のセッションを構成できます。ポリシーは、ユーザーデバイスでレジストリチェックを実行し、評価に基づいて Citrix ADC ネットワークへのアクセスを許可または拒否します。

EPA スキャンには、OPSWAT スキャンとシステムスキャンの 2 種類があります。次のセクションでは、スキャンの種類とその詳細について説明します。

OPSWAT スキャン。スキャンメカニズムは、次のようなさまざまなレベルでセキュリティを提供します。

- 製品固有のスキャン
- ベンダー固有のスキャン
- 汎用スキャン

製品固有のスキャン: 特定の製品 (例:**Avast!** 特定のベンダー（例：****AVAST Software a.s**.）が提供する無料アンチウイルス（例：****** アンチウイルス）。アクセスは、指定した条件を満たすコンピューターにのみ許可されます。**

ベンダー固有のスキャン：特定のベンダー（例：**AVAST Software a.s**.）のスキャン基準を設定できます（例：ウイルス対策)。構成済みのスキャンでは、ベンダーが提供するすべての製品について、指定した基準がチェックされます。アクセスは、指定した条件を満たすコンピューターにのみ許可されます。

汎用スキャン: 特定のカテゴリのスキャン基準を設定できます (例: ウイルス対策)。構成済みのスキャンでは、すべてのベンダーおよびベンダーが提供する製品について、指定された基準がチェックされます。アクセスは、指定した条件を満たすコンピューターにのみ許可されます。

システムスキャン。システムスキャンは、MAC アドレスなどのシステムレベルの属性にセキュリティを提供します。システム属性（**MAC** アドレスなど）のスキャン基準を設定できます。アクセスは、指定した条件を満たすコンピューターにのみ許可されます。

高度なエンドポイント分析スキャンの設定

March 26, 2020

EPA スキャンには、OPSWAT スキャンとシステムスキャンの 2 種類を設定できます。

OPSWAT スキャンの設定

以下の OPSWAT スキャンは、Citrix Gateway アプライアンス上で構成されます。

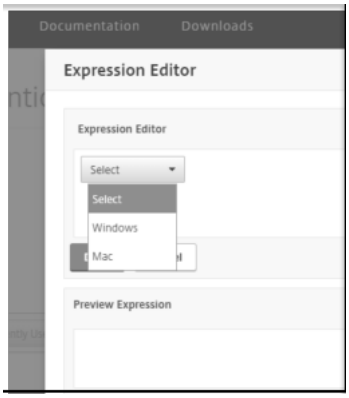
- 製品固有のスキャン
- ベンダー固有のスキャン
- 汎用スキャン

注：特定の製品でサポートされているスキャンは、GUI に表示されます。また、次の OPSWAT スキャン設定では、事前認証 EPA を例として採用しています。OPSWAT スキャンは、認証後の EPA にも設定できます。

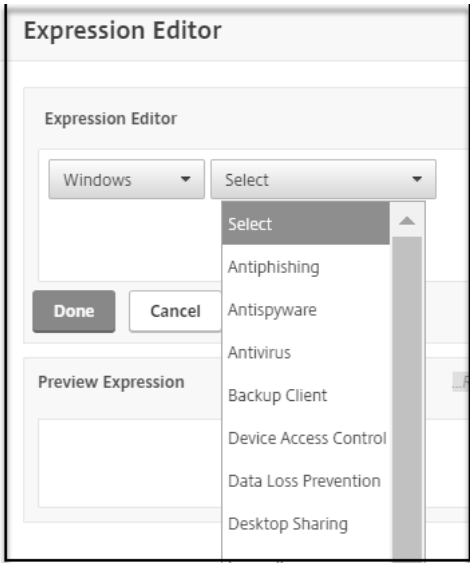
製品固有の **OPSWAT** スキャンの設定

NetScaler GUI を使用して製品固有の OPSWAT スキャンを構成するには、次の手順に従います。

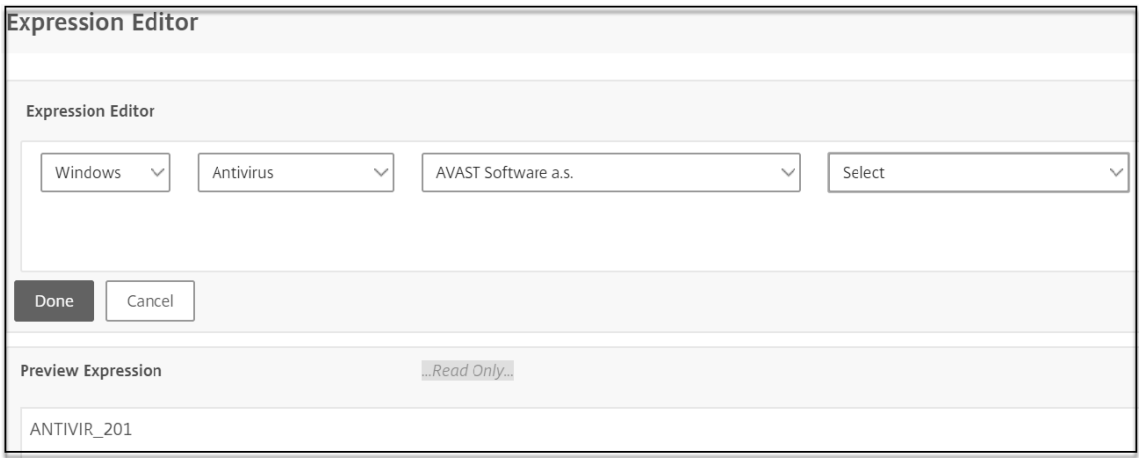
1. 「構成」**>**「**Citrix NetScaler>**「グローバル設定」に移動します。
2. [グローバル設定**]** ページで、[事前認証設定の変更] リンクをクリックします。
3. [**AAA** 事前認証パラメータの設定] ページで、[**OPSWAT EPA** エディタ] リンクをクリックします。
4. [式エディタ] 領域で、オペレーティングシステムを選択します。



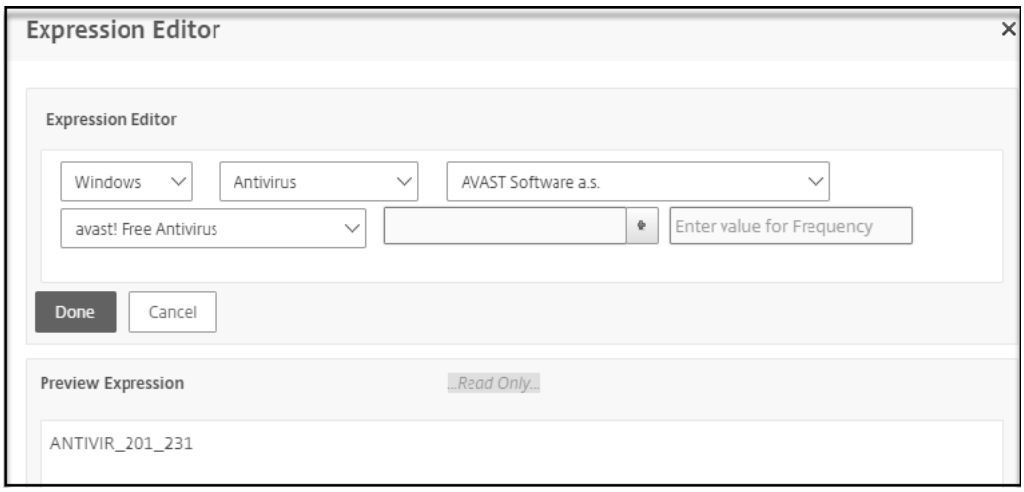
5. カテゴリ（アンチウイルスなど）を選択します。



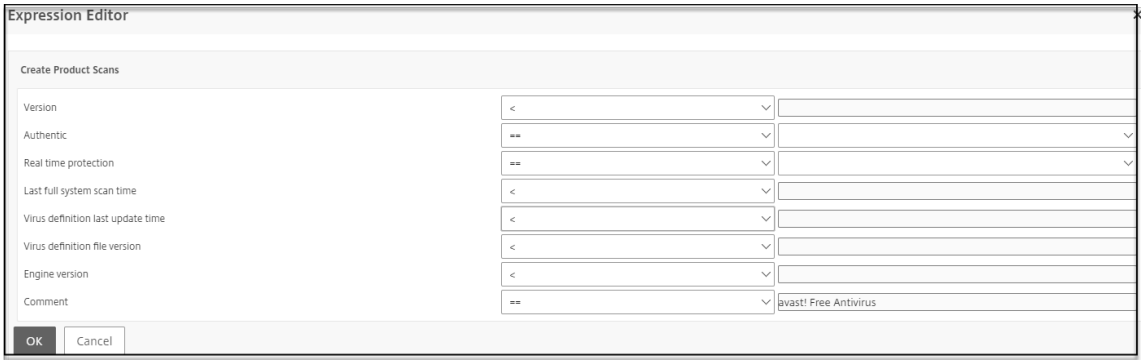
6. ベンダー（例：**AVAST** ソフトウェア **a.s**）を選択します。



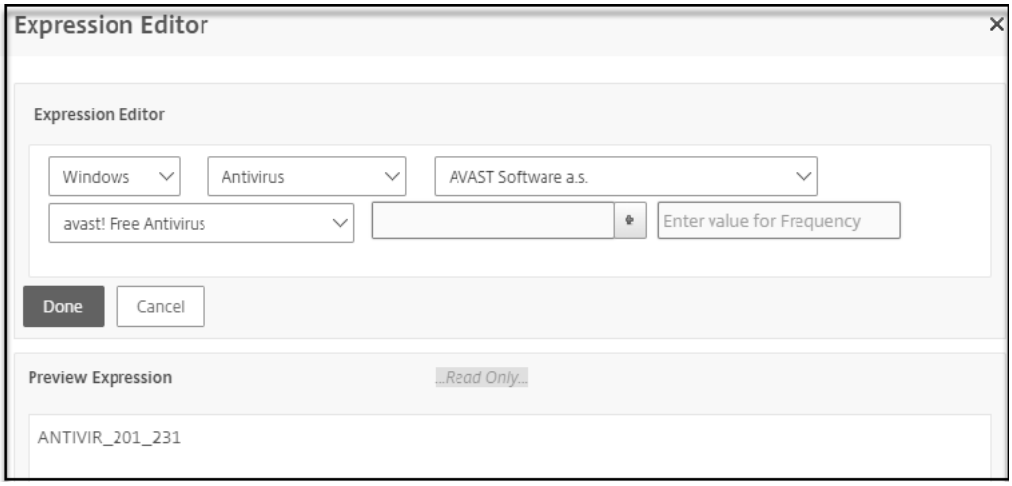
7. 製品を選択します。たとえば、**Avast!** 無料アンチウイルス。



8. 製品ドロップダウンメニューの隣にある [**+**] をクリックして、製品スキャンを設定します。



9. 定期スキャンを行う場合は、必要に応じて、スキャン頻度の値を入力します。

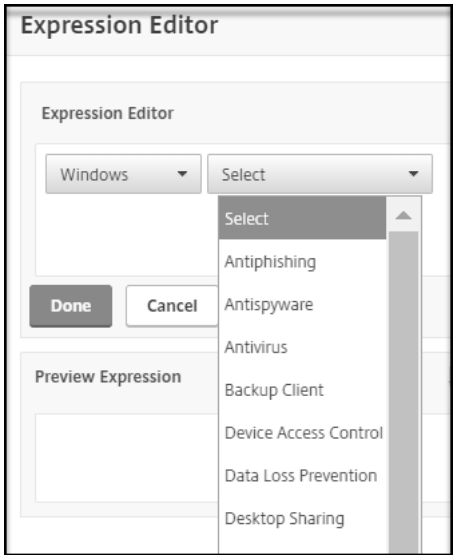


ベンダー固有の **OPSWAT** スキャンの設定

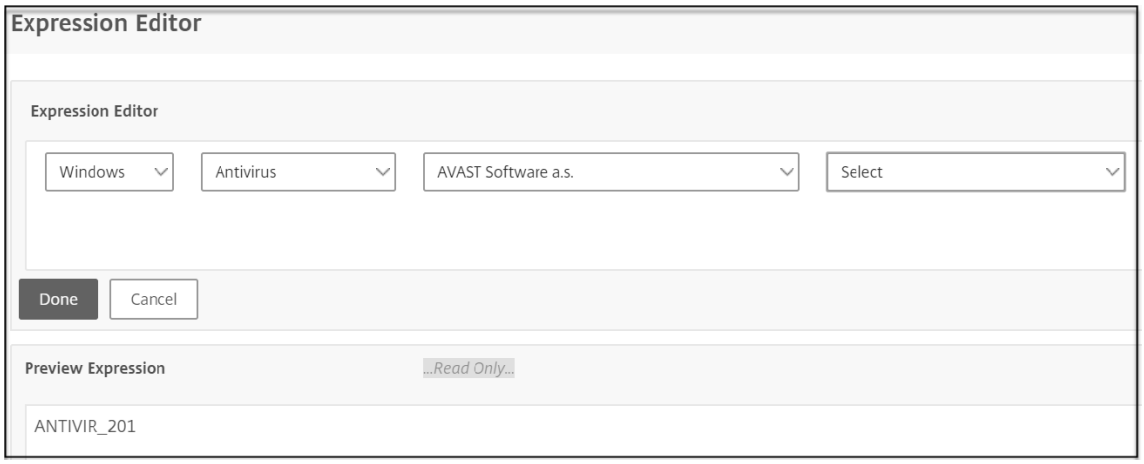
NetScaler GUI を使用してベンダー固有の OPSWAT スキャンを構成するには、次の手順に従います。

1. 「構成」**>**「**Citrix NetScaler>**「グローバル設定」に移動します。
2. [グローバル設定**]** ページで、[事前認証設定の変更] リンクをクリックします。
3. [**AAA** 事前認証パラメータの設定] ページで、[**OPSWAT EPA** エディタ] リンクをクリックします。
4. [式エディタ] 領域で、オペレーティングシステムを選択します。

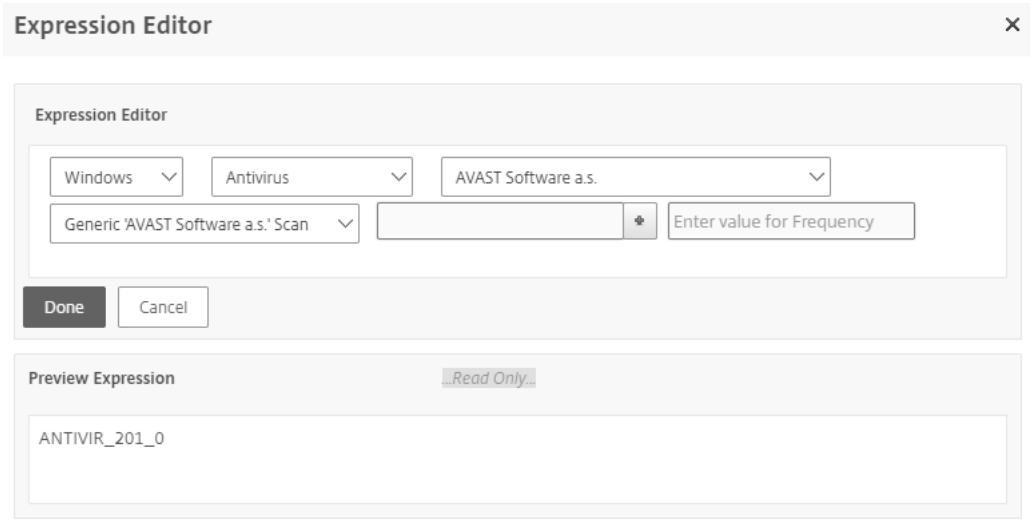
5. カテゴリ（アンチウイルスなど）を選択します。



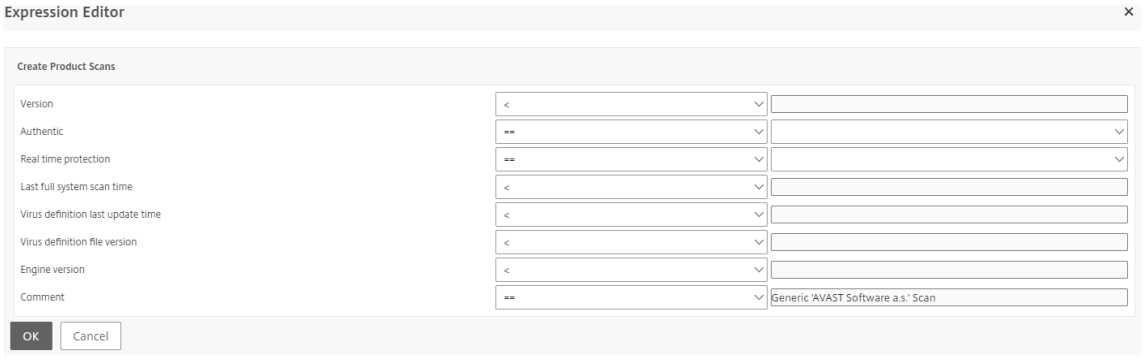
6. ベンダー（例：**AVAST** ソフトウェア **a.s**）を選択します。



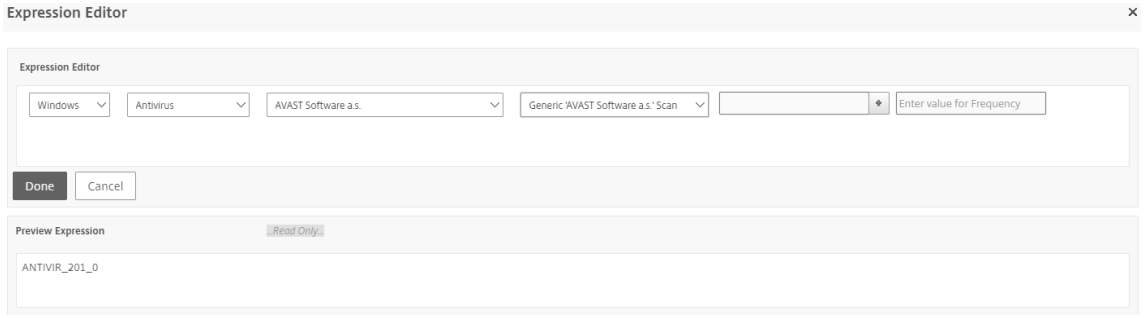
7. 汎用「**AVAST** ソフトウェア」を選択します。ベンダー固有のスキャンをスキャンします。



8. 製品ドロップダウンメニューの隣にある [**+**] をクリックして、スキャンを設定します。



9. 定期スキャンを行う場合は、必要に応じて、スキャン頻度の値を入力します。



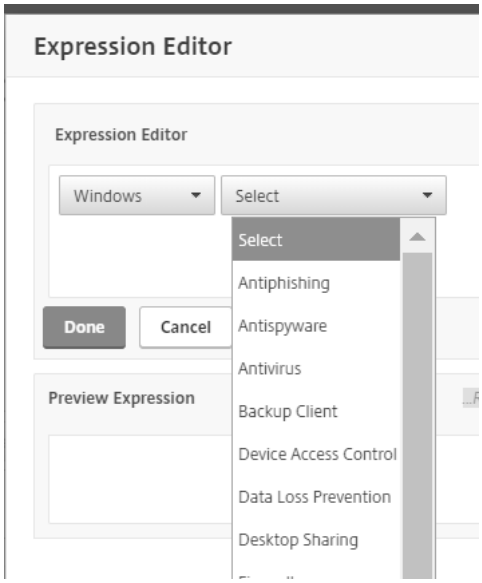
汎用 **OPSWAT** スキャンの設定

NetScaler の GUI を使用して汎用 OPSWAT スキャンを構成するには、次の手順に従います。

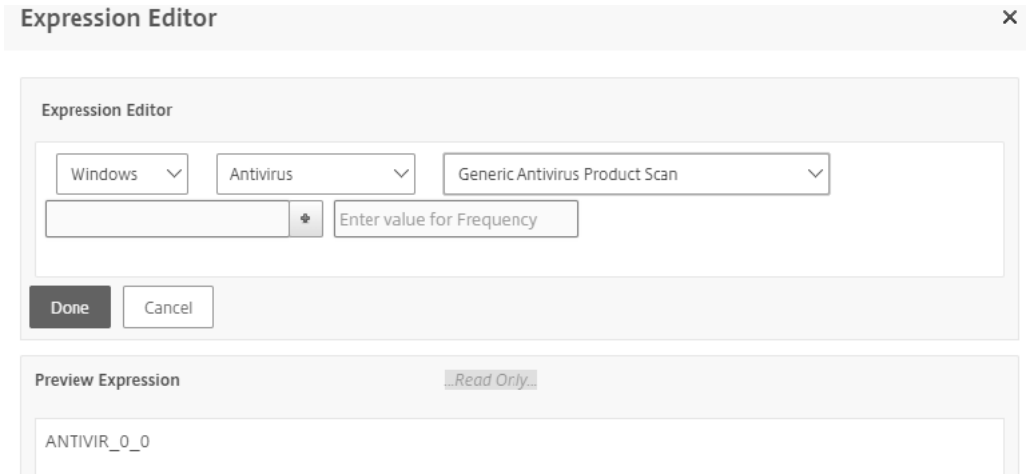
1. 「構成」**>**「**Citrix NetScaler>**「グローバル設定」に移動します。
2. [グローバル設定] ページで、[事前認証設定の変更] リンクをクリックします。
3. [AAA 事前認証パラメータの設定] ページで、[**OPSWAT EPA** エディタ] リンクをクリックします。

4. [式エディタ] 領域で、オペレーティングシステムを選択します。

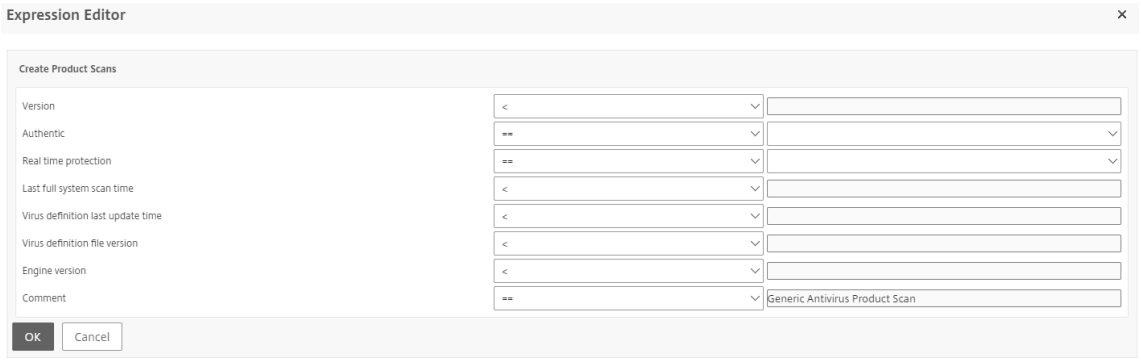
5. カテゴリ（アンチウイルスなど）を選択します。



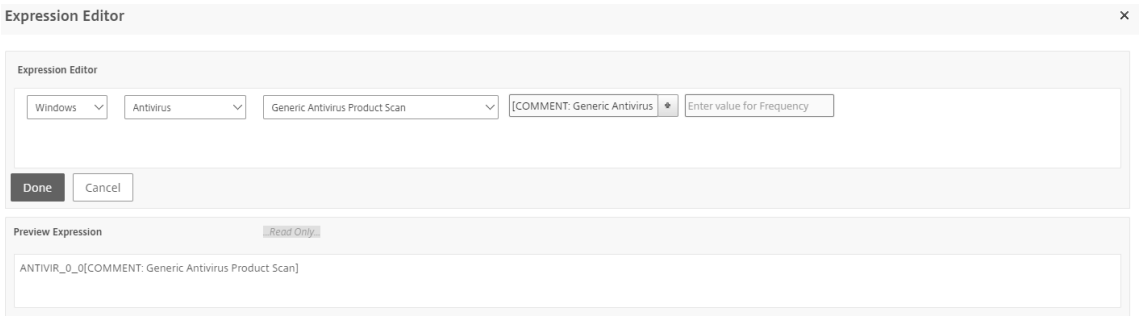
6.「汎用」カテゴリ固有のスキャン（「汎用ウイルス対策製品スキャン」など）を選択します。



7. 製品ドロップダウンメニューの隣にある [**+**] をクリックして、スキャンを設定します。



8. 定期スキャンを行う場合は、必要に応じて、スキャンの頻度の値を入力します。



システムスキャンの設定

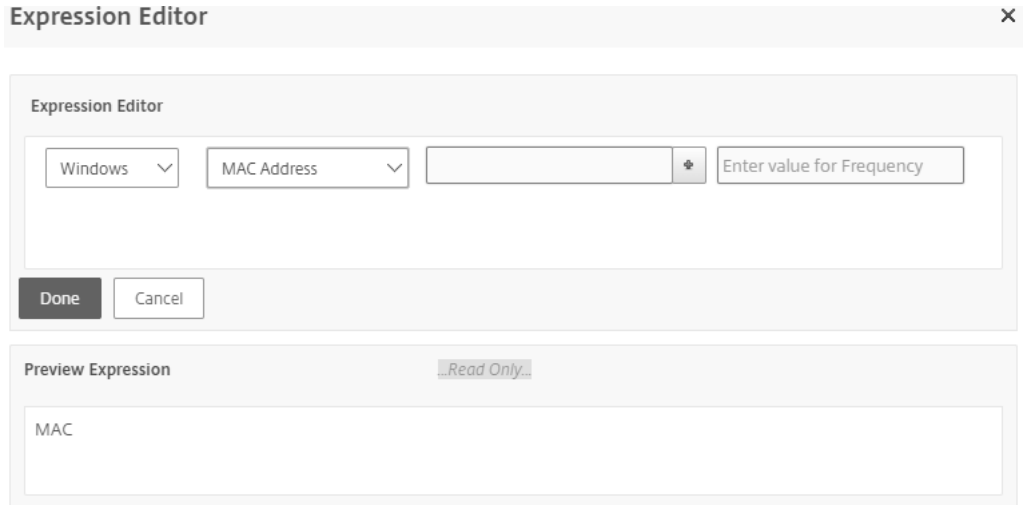
Citrix Gateway アプライアンスでは、次のシステムスキャンが構成されます。

- MAC アドレス
- ドメインチェック
- 数値レジストリ
- 非数値レジストリ
- Windows Update

NetScaler GUI を使用して OPSWAT システムスキャンを構成するには、次の手順に従います。

1. 「構成」**>**「**Citrix NetScaler>**「グローバル設定」に移動します。
2. [グローバル設定**]** ページで、[事前認証設定の変更] リンクをクリックします。
3. [**AAA** 事前認証パラメータの設定] ページで、[**OPSWAT EPA** エディタ] リンクをクリックします。
4. [式エディタ] 領域で、オペレーティングシステムを選択します。

5. ドロップダウンメニューから目的のシステムスキャンを選択します。たとえば、**MAC** アドレスなどです。



6. 製品ドロップダウンメニューの隣にある [**+**] をクリックして、スキャンを設定します。

7. 定期スキャンを行う場合は、必要に応じて、スキャンの頻度の値を入力します。

EPA ライブラリのアップグレード

NetScaler GUI を使用して EPA ライブラリをアップグレードするには、次の手順に従います。

1. 「構成」**>**「**Citrix NetScaler>**「クライアントコンポーネントの更新」の順に選択します。
2. [クライアントコンポーネントの更新**]** で、 [**EPA** ライブラリのアップグレード] リンクをクリックします。
3. 必要なファイルを選択し、[アップグレード] をクリックします。

Citrix ADC スキャンで OPSWAT がサポートする Windows および MAC アプリケーションの一覧については、https://support.citrix.com/article/CTX207623をクリックしてください。

高度なエンドポイント分析式を使用して事前認証プロファイルを設定するには

1. 構成ユーティリティーのナビゲーションペインで、[Citrix Gateway] ノードを展開し、[ポリシー] サブノードを展開します。
2. [事前認証] を選択します。
3. 詳細ウィンドウの [プロファイル] タブで、[追加] をクリックします。
4. プロファイルの名前を入力します。
5. アクションを選択します。
6. オプションで、停止するプロセスまたはクライアントエンドポイントシステム上で削除するファイルの名前を入力します。
7. [作成] をクリックします。

プロファイルは、リクエストアクションとして事前認証ポリシーで使用できるようになりました

高度なエンドポイント分析式を使用して事前認証ポリシーを設定するには

1. 構成ユーティリティーのナビゲーションペインで、[Citrix Gateway] ノードを展開し、[ポリシー] サブノードを展開します。
2. [事前認証] を選択します。
3. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
4. ポリシーの名前を入力します。

5.「アクションの要求」メニューから、目的のプロファイルを選択します。
6. [式] ペインで、[OPSWAT EPA エディタ] を選択します。
7. 最初のプルダウン・メニューで、クライアント・オペレーティング・システムを選択します。
8. 表示される 2 番目のプルダウンメニューで、スキャンの種類を選択します。
9. ポリシーの構築が完了したら、[Create] をクリックします。

高度なエンドポイント分析事前認証ポリシーをバインドして有効にする必要があります。

事前認証ポリシーをバインドするには

1. 構成ユーティリティーのナビゲーションペインで、［Citrix Gateway］ノードを展開し、［ポリシー］サブノードを展開します。
2. [事前認証] を選択します。
3. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
4.「アクション」メニューから「グローバル・バインディング」を選択します。
5. ［バインド］をクリックします。
6. 表示される [Policies] 詳細ペインで、目的のポリシーの横にあるチェックボックスをオンにします。
7. ［Insert］をクリックします。
8. ポリシーには自動的にプライオリティ（重み）が割り当てられます。[優先順位] エントリをクリックして、必要に応じて編集します。
9. [OK] をクリックしてポリシーをバインドします。

特定のセッションに対して高度なエンドポイント分析ポリシーを設定するには

1. 構成ユーティリティーのナビゲーションペインで、［Citrix Gateway］ノードを展開し、［ポリシー］サブノードを展開します。
2.「セッション」を選択します。
3. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
4. ポリシーの名前を入力します。
5. [操作] メニューで、次のいずれかの操作を行います。
   - a. 既存のアクションを選択します。
   - b. プラスアイコンをクリックすると、セッション・ポリシーで設定できる構成パラメータが表示されます。構成オプションの右側にある「オーバーライド」(Override Global) チェックボックスをクリックしてアクティブにします。［Create］を選択します。
6. [式] ペインで、[OPSWAT EPA エディタ] を選択します。
7. 最初のプルダウン・メニューで、クライアント・オペレーティング・システムを選択します。
8. 表示される 2 番目のプルダウンメニューで、スキャンの種類を選択します。
9. ポリシーの構築が完了したら、[Create] をクリックします。

アドバンスドエンドポイント分析セッションポリシーをバインドして有効にする必要があります。

セッションポリシーをバインドするには

1. 構成ユーティリティーのナビゲーションペインで、[Citrix Gateway] ノードを展開し、[ポリシー] サブノードを展開します。
2.「セッション」を選択します。
3. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
4.「アクション」メニューから「グローバル・バインディング」を選択します。
5. [バインド] をクリックします。
6. 表示される [Policies] 詳細ペインで、目的のポリシーの横にあるチェックボックスをオンにします。
7. [Insert] をクリックします。
8. ポリシーには自動的にプライオリティ（重み）が割り当てられます。[優先順位] エントリをクリックして、必要に応じて編集します。
9. [OK] をクリックしてポリシーをバインドします。

高度なエンドポイント分析ポリシー式リファレンス

March 26, 2020

このリファレンスでは、高度なエンドポイント分析式の形式と構成について説明します。ここに含まれる式要素は、Citrix Gateway 構成ユーティリティによって自動的に構築されるため、手動で構成する必要はありません。

式の書式

高度なエンドポイント分析式の形式は次のとおりです。

```
CLIENT.APPLICATION (SCAN-type_ Product-id_ Method-name _ Method-comparator_
 Method-param _…)
```

各項目の意味は次の通りです:

SCAN-type は、分析されるアプリケーションのタイプです。

product-id は、分析されたアプリケーションの製品識別情報です。

Method-name は、分析対象の製品またはシステム属性です。

方法-コンパレータは、分析のために選択されたコンパレータです。

Method-param は、分析対象の 1 つまたは複数の属性値です。

次に例を示します:

client.application(ANTIVIR_2600*RTP*==_TRUE)

> 注意**:** アプリケーション以外のスキャン・タイプの場合、式のプレフィックスは
> CLIENT.
> APPLICATION ではなく CLIENT.SYSTEM です。

式文字列

高度なエンドポイント分析でサポートされている各スキャンタイプでは、式に一意の識別子が使用されます。次の表は、スキャンの種類ごとの文字列を列挙したものです。

スキャンの種類	スキャンタイプの式文字列
フィッシング対策	ANTIPHI
スパイウェア対策	ANTISPY
アンチウイルス	ANTIVIR
バックアップクライアント	BACKUP
デバイスアクセスの制御	DEV-CONT
データ損失防止	DATA-PREV
デスクトップ共有	DESK-SHARE
ファイアウォール	FIREWALL
ヘルスエージェント	HEALTH
ハードディスク暗号化	HD-ENC
インスタントメッセンジャー	IM
Web ブラウザー	BROWSER
P2P	P2P
パッチ管理	PATCH
URL フィルタリング	URL-FILT
MAC アドレス	MAC
ドメインチェック	DOMAIN
数値レジストリスキャン	REG-NUM
数値以外のレジストリスキャン	REG-NON-NUM

> メモ**:** Mac OS X 固有のスキャンでは，メソッドタイプの前に
> MAC-というプレフィックスが式に含まれます。したがって、ウイルス対策スキャンとフィッシング対策スキャ

> ンでは、方法はそれぞれ
> MAC-ANTIVIR と
> MAC-ANTIPHI です。例：pre codeblock
> client.application(MAC-ANTIVIR_2600*RTP*==_TRUE)

アプリケーションスキャンの方法

高度なエンドポイント分析式を設定する場合、メソッドを使用してエンドポイントスキャンのパラメータを定義します。これらのメソッドには、メソッド名、コンパレータ、および値が含まれます。次の表は、式で使用できるすべてのメソッドを列挙しています。

一般的なスキャン方法**:**

次のメソッドは、複数のタイプのアプリケーションスキャンに使用されます。

方法	説明	比較演算子	指定可能な値
バージョン *	アプリケーションのバージョンを指定します。	<, <=, >, >=, !=, ==	バージョン文字列
AUTHENTIC**	与えられたアプリケーションが本物であるかどうかを確認してください。	==	TRUE
ENABLED	アプリケーションが有効になっているかどうかを確認します。	==	TRUE
RUNNING	アプリケーションが実行されているかどうかを確認します。	==	TRUE
COMMENT	コメントフィールド (スキャンでは無視)。式内では [] によって区切られます。	==	任意のテキスト

* VERSION 文字列は、1.2.3.4 のように最大 4 つの値から成る 10 進文字列を指定できます。

**AUTHENTIC チェックは、アプリケーションのバイナリファイルの信頼性を検証します。

> 注意**:** アプリケーションスキャンのタイプには、汎用バージョンを選択できます。一般的なスキャンを選択すると、商品 ID は 0 になります。

Gateway には、ソフトウェアの種類ごとに汎用スキャンを設定するオプションがあります。一般的なスキャンを使用して、管理者は、任意の特定の製品にスキャンチェックを制限することなく、クライアントマシンをスキャンする

ことができます。

汎用スキャンでは、ユーザーシステムにインストールされている製品がそのスキャン方法をサポートしている場合にのみスキャン方法が機能します。特定のスキャン方法をサポートする製品については、Citrix サポートにお問い合わせください。

固有のスキャン方法**:**

次のメソッドは、指定した種類のスキャンに固有のものです。

方法	説明	比較演算子	指定可能な値
ENABLED-FOR	選択したアプリケーションでフィッシング対策ソフトウェアが有効になっているかどうかを確認します。	allof, anyof,noneof	**Windows** の場合: Internet Explorer, Mozilla Firefox, Google Chrome, Opera, Safari.**Mac** の場合: Safari, Mozilla Firefox, Google, Chrome, Opera

表 2. スパイウェア対策とウイルス対策

方法	説明	比較演算子	指定可能な値
RTP	リアルタイム保護がオンになっているかどうかを確認します。	==	TRUE
SCAN-TIME	システム全体のスキャンが実行されてからの 時間(分)。	<, <=, >, >=, !=, ==	任意の正の数
VIRDEF-FILE-TIME	ウイルス定義ファイルが更新されてからの時間 **(**つまり、ウイルス定義ファイルのスタンプから現在のタイムスタンプまでの分数**)**。	<, <=, >, >=, !=, ==	任意の正の数
VIRDEF-FILE-VERSION	定義ファイルのバージョン。	<, <=, >, >=, !=, ==	バージョン文字列
ENGINE-VERSION	エンジンのバージョン。	<, <=, >, >=, !=, ==	バージョン文字列

表 3. バックアップ・クライアント

方法	説明	比較演算子	指定可能な値
LAST-BK-ACTIVITY	最後のバックアップ・アクティビティが完了してから何 分経過したか。	<, <=, >, >=, !=, ==	任意の正の数

表 4. データ消失防止

方法	説明	比較演算子	指定可能な値
ENABLED	アプリケーションが有効かどうか、および時間保護がオンになっているかどうかをチェックします。	==	TRUE

表 5. ヘルスチェックエージェント

方法	説明	比較演算子	指定可能な値
SYSTEM-COMPL	システムが準拠しているかどうかを確認します。	==	TRUE

表 6. ハードディスク暗号化

方法	説明	比較演算子	指定可能な値
ENC-PATH	暗号化ステータスを確認するための PATH。	NO OPERATOR	任意のテキスト
ENC-TYPE	指定されたパスの暗号化の種類を確認します。	すべての, 任意の, なし	次のオプションを含むリスト: 非暗号化、一部、暗号化、仮想化、サスペンド、保全中

表 7. Web ブラウザー

方法	説明	比較演算子	指定可能な値
DEFAULT	デフォルトのブラウザとして設定されているかどうかを確認します。	==	TRUE

表 8. パッチ管理 </caption>

方法	説明	比較演算子	指定可能な値
SCAN-TIME	パッチの最後のスキャンが実行されてからの時間（分）。	<, <=, >, >=, !=, ==	任意の正の数
MISSED-PATCH	クライアントシステムでは、これらのタイプのパッチが欠落していません。	anyof, noneof	事前選択された（パッチ・マネージャ・サーバ上で事前に選択されたパッチ）
NON|

方法	説明	比較演算子	指定可能な値
ADDR	クライアントマシンの MAC アドレスが指定されたリストに含まれているかどうかをチェックします。	anyof, noneof	編集可能リスト

表 10. ドメインメンバシップ </caption>
方法	説明	比較演算子	指定可能な値
SUFFIX	指定されたリストにクライアントマシンが存在するか、存在しないかを確認してください。	anyof, noneof	編集可能リスト

方法	説明	比較演算子	指定可能な値
PATH	レジストリチェックのパス。形式：HKEY_LOCAL_MACHINE Access Client\EnableAutoUpda 特殊文字のエスケープは必要ありません。すべてのレジストリルートキー:HKEY_LOCAL_MACHI HKEY_CURRENT_USER HKEY_CLASSES_ROOT、HKEY_CURRENT_CONF	NO OPERATOR	任意のテキスト

方法	説明	比較演算子	指定可能な値
REDIR-64	64 ビットリダイレクトに従います。TRUE に設定すると、WOW リダイレクトが実行されます（32 ビットシステムではレジストリパスがチェックされますが、64 ビットシステムでは WOW リダイレクトパスがチェックされます）。設定されていない場合、WOW リダイレクトは行われません（つまり、32 ビットおよび 64 ビットシステムの場合、同じレジストリパスがチェックされます）。リダイレクトされないレジストリエントリの場合、この設定は無効です。64 ビットシステムでリダイレクトされるレジストリキーの一覧については、次の資料を参照してください。 http://msdn.microsoft.com/en-us/library/aa384253%28v=vs.85%29.aspx	==	TRUE
VALUE	上記のパスに期待される値。このスキャンは、レジストリの種類の REG_DWORD と REG_QWORD に対してのみ機能します。	<, <=, >, >=, !=, ==	任意の数

方法	説明	比較演算子	指定可能な値

|PATH| レジストリチェックのパス。
レジストリスキャンで数値タイプを確認します。|NO OPERATOR| 任意のテキスト |
|REDIR-64|64 ビットリダイレクトに従います。
レジストリスキャンで数値型をチェックしてください。|==|TRUE|
|VALUE| 上記のパスに期待される値。文字列型のレジストリエントリの場合、レジストリ値は期待値に対して直接比較されます。REG_BINARY レジストリエントリの種類では、レジストリ値が大文字の 16 進文字列に変換され、この文字列が期待値と比較されます。|==,! =| 任意のテキスト |

高度なエンドポイント分析スキャンのトラブルシューティング

March 26, 2020

高度なエンドポイント分析スキャンのトラブルシューティングを支援するために、クライアントプラグインはログ情報をクライアントエンドポイントシステム上のファイルに書き込みます。これらのログファイルは、ユーザーのオペレーティングシステムに応じて、次のディレクトリにあります。

Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10:

C:\Users\<username>\AppData\Local\Citrix\AGEE\nsepa.txt

Windows XP:

C:\Documents and Settings\All Users\Application Data\Citrix\AGEE\nsepa.txt

Mac OS X systems:

~/Library/Application Support/Citrix/EPAPlugin/epaplugin.log

(~ 記号は、該当する Mac OS X ユーザのホームディレクトリパスを示します)。

ユーザー・セッションの管理

March 26, 2020

ユーザー・セッションは、「アクティブ・ユーザー・セッション」ダイアログ・ボックスの構成ユーティリティで管理できます。このダイアログボックスには、Citrix Gateway 上のアクティブなユーザーセッションのリストが表示されます。

このダイアログボックスでは、ユーザー名、グループ名、または IP アドレスを使用して、ユーザーまたはグループセッションを終了できます。

このダイアログボックスでは、アクティブなセッションを表示することもできます。セッション情報には以下が含まれます。

- ユーザー名
- ユーザーデバイスの IP アドレス
- ユーザーデバイスのポート番号
- 仮想サーバの IP アドレス
- 仮想サーバのポート番号
- ユーザーに割り当てられたイントラネット IP アドレス

ユーザー・セッションを表示するには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］をクリックします。
2. 詳細ウィンドウの [接続の監視] で、[アクティブなユーザーセッション] をクリックします。
3. [セッション] の下のセッションの一覧を表示します。

セッション・リストを更新するには

Citrix Gateway へのセッションに関する更新情報を取得できます。

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］をクリックします。
2. 詳細ウィンドウの [接続の監視] で、[アクティブなユーザーセッション] をクリックします。
3. [更新] をクリックします。

ユーザーまたはグループのセッションを終了するには

ユーザーおよびグループのセッションを終了できます。特定のイントラネット IP アドレスとサブネットマスクを持つセッションを終了することもできます。

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］をクリックします。
2. 詳細ウィンドウの [接続の監視] で、[アクティブなユーザーセッション] をクリックします。
3. [セッション] で、ユーザーまたはグループを選択し、[終了] をクリックします。

イントラネット **IP** アドレスを使用してセッションを終了するには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］をクリックします。
2. 詳細ウィンドウの [接続の監視] で、[アクティブなユーザーセッション] をクリックします。
3. イントラネット IP の選択
4. [イントラネット IP] に IP アドレスを入力します。
5. [ネットマスク] にサブネットマスクを入力し、[終了] をクリックします。

AlwaysON

March 26, 2020

Citrix Gateway の AlwaysON 機能を使用すると、ユーザーは常に企業ネットワークに接続できます。この永続的な VPN 接続は、VPN トンネルの自動確立によって実現されます。

> 注
>
> AlwaysON 機能は、Citrix ADC 12.0 ビルド 51.24 以降のキャプティブポータルをサポートします。

AlwaysON にするタイミング

AlwaysON は、ユーザーの位置に基づいてシームレスな VPN 接続を提供し、VPN に接続していないユーザーによるネットワークアクセスを防止する必要がある場合に使用します。

次のシナリオは、AlwaysON の使用方法を示しています。

- 従業員は、企業ネットワークの外部でラップトップを起動し、VPN 接続を確立するための支援を必要としています。
  解決策**:** ラップトップが企業ネットワークの外部で起動されると、AlwaysON はトンネルをシームレスに確立し、VPN 接続を提供します。
- VPN 接続を使用する従業員は、企業ネットワークに移行します。従業員は企業ネットワークに切り替えられますが、VPN トンネルに接続されたままですが、これは望ましい状態ではありません。
  解決策**:** 従業員が企業ネットワークに移行すると、AlwaysOn は VPN トンネルを切断し、従業員を企業ネットワークにシームレスに切り替えます。
- 従業員が企業ネットワークの外に移動して、ラップトップを閉じます (シャットダウンしません)。従業員は、ラップトップで作業を再開する際、VPN 接続を確立するための支援を必要とします。
  解決策：従業員が企業ネットワークの外に移動すると、AlwaysON はトンネルをシームレスに確立し、VPN 接続を提供します。
- ある企業は、VPN トンネルに接続されていないユーザに対して提供されるネットワークアクセスを規制したいと考えています。
  解決方法**:** 設定に応じて、AlwaysON はアクセスを制限し、ユーザーは Gateway ネットワークのみにアクセスできるようにします。

AlwaysON フレームワークについて

AlwaysON は、クライアントが以前に確立した VPN トンネルにユーザを自動的に接続します。ユーザーが初めて VPN トンネルを必要とする場合、ユーザーは Citrix Gateway の URL に接続してトンネルを確立する必要があります。AlwaysON 設定がクライアントにダウンロードされた後、この設定はトンネルのその後の確立を駆動します。

Citrix Gateway クライアント実行可能ファイルは、常にクライアントマシンで実行されます。ユーザーがログオンしたりネットワークが変更されたりすると、Citrix Gateway クライアントはユーザーのラップトップが企業ネット

ワーク上にあるかどうかを判断します。場所と構成に応じて、Citrix Gateway クライアントはトンネルを確立するか、既存のトンネルを切断します。

トンネルの確立は、ユーザーがコンピューターにログオンした後にのみ開始されます。Citrix Gateway クライアントは、クライアントマシンの資格情報を使用して Gateway サーバーとの認証を行い、トンネルの確立を試みます。

トンネルの自動再確立

VPN トンネルが Citrix Gateway によって切断されると、トンネルの自動再確立がトリガーされます。

> 注
>
> エンドポイント分析の失敗で、Citrix Gateway クライアントはトンネルの確立を再試行しませんが、エラーメッセージを表示します。認証に失敗した場合、Citrix Gateway クライアントはユーザーに資格情報の入力を要求します。

シームレスなトンネル確立でサポートされるユーザ認証方式

サポートされているユーザー認証方法は次のとおりです。

- ユーザー名と AD パスワード: 認証に Windows のユーザー名とパスワードが使用されている場合、Citrix Gateway クライアントはこれらの資格情報を使用してトンネルをシームレスに確立します。
- ユーザー証明書: 認証にユーザー証明書が使用され、マシン上に証明書が 1 つしかない場合、Citrix Gateway クライアントはこの証明書を使用してトンネルをシームレスに確立します。複数のクライアント証明書がインストールされている場合、ユーザが優先証明書を選択した後にトンネルが確立されます。Citrix Gateway クライアントは、後で確立されたトンネルに対してこの設定を使用します。
- ユーザー証明書とユーザー名 + AD パスワード: この認証方法は、前述の認証方法の組み合わせです。

> 注
>
> その他の認証メカニズムはすべてサポートされていますが、トンネルの確立は他の認証方式に対してシームレスではありません。他のすべての認証方法では、ユーザーの介入が必要です。

AlwaysON の設定要件

エンタープライズ管理者は、管理対象デバイスに対して次のことを強制する必要があります。

- 特定の構成のプロセス/サービスを終了できないこと
- ユーザーが特定の構成のためにパッケージをアンインストールできないこと
- ユーザーは特定のレジストリエントリを変更できません

> 注
>
> 管理対象外のデバイスの場合と同様に、ユーザーが管理権限を持っている場合、この機能は期待どおりに機能しないことがあります。

AlwaysON 機能を有効にする際の考慮事項

AlwaysON 機能を有効にする前に、次のセクションを確認してください。

プライマリネットワークアクセス: トンネルが確立されると、企業ネットワークへのトラフィックはスプリットトンネルの構成に基づいて決定されます。この動作をオーバーライドするための追加の設定は提供されません。

クライアントマシンのプロキシ設定: クライアントマシンのプロキシ設定は、Gateway サーバーへの接続時に無視されます。

> 注
>
> Citrix ADC アプライアンスのプロキシ構成は無視されません。クライアントマシンのプロキシ設定のみが無視されます。システムにプロキシが設定されているユーザには、VPN プラグインがプロキシ設定を無視したことが通知されます。

構成値が「拒否」に設定されている場合、次の変更が適用されます。

- クライアント UI-プラグインのコンテキストメニューとプラグイン UI の [ログオフ] オプションと [終了] オプションが無効になります。ユーザーは Gateway URL を変更できません。
- ブラウザのログオン-別の Gateway へのブラウザのログオンは許可されていません。クライアントコントロールは無効です。

AlwaysON の構成

AlwaysON を構成するには、Citrix Gateway way アプライアンスで AlwaysOn プロファイルを作成し、プロファイルを適用します。

AlwaysOn プロファイルを作成するには、次の手順に従います。

1. Citrix ADC GUI で、［構成］**>**［**Citrix Gateway**］**>**［ポリシー］**>**［**AlwaysON**］の順に選択します。
2. [AlwaysON プロファイル] ページで、[追加] をクリックします。
3. [AlwaysON プロファイルの作成] ページで、次の詳細を入力します。
    - **[** 名前**]** — プロファイルの名前。
    - ロケーションベースの **VPN** — 次のいずれかの設定を選択します。
        - **[** リモート]: クライアントが企業ネットワーク内にあるかどうかを検出し、企業ネットワーク内にない場合はトンネルを確立できるようにします。これがデフォルトの設定です。
        - クライアントの場所に関係なく、クライアントが場所の検出をスキップしてトンネルを確立できるようにする場所
    - 「クライアント制御」— 次のいずれかの設定を選択します。
        - ユーザーがログオフして別の Gateway に接続できないようにするには、[拒否] をクリックします。これがデフォルトの設定です。
        - ユーザーがログオフして別の Gateway に接続できるようにすることを許可します。
    - 「**VPN** でのネットワークアクセス障害」— 次のいずれかの設定を選択します。
        - **[** フルアクセス**]** : トンネルが確立されていないときに、クライアントとの間でネットワークトラフィックが送受信されるようにします。これがデフォルトの設定です。

- トンネルが確立されていないときに、クライアントとの間でネットワークトラフィックが流れるのを防ぐには、**[Gateway** へのみ**]** を選択します。ただし、Gateway IP アドレスとの間で送受信されるトラフィックは許可されます。

4. [作成] をクリックして、プロファイルの作成を終了します。

AlwaysOn プロファイルを適用するには、次の手順に従います。

1. Citrix ADC インターフェイスで、［構成］＞ **Citrix Gateway** ＞［グローバル設定］を選択します。
2. [グローバル設定] ページで、[グローバル設定の変更**]** リンクをクリックし、[クライアントエクスペリエンス] タブを選択します。
3. [**AlwaysON** プロファイル名] ドロップダウンメニューから、新しく作成したプロファイルを選択し、[**OK**] をクリックします。

> 注
>
> 同様の構成は、グループレベル、サーバーレバー、またはユーザーレベルでポリシーを適用するために、セッションプロファイルで行うことができます。

管理ユーザと非管理者ユーザに対するさまざまな設定の動作の要約

次の表は、さまざまな構成の動作をまとめたものです。また、AlwaysON 機能に影響を与える可能性のある特定のユーザー操作の可能性についても詳しく説明します。

networkAccessONVPNFailure	クライアント制御	管理者以外のユーザー	管理者ユーザー
fullaccess	許可	トンネルは自動的に確立されます。ユーザーはログオフしてネットワークから離れることができます。ユーザーは、別の Citrix Gateway をポイントすることもできます。	トンネルは自動的に確立されます。ユーザーはログオフして、エンタープライズネットワークから離れたままにすることができます。ユーザーは、別の Citrix Gateway をポイントすることもできます。
fullaccess	禁止	トンネルが自動的に確立されます。ユーザーがログオフしたり、別の Citrix Gateway をポイントしたりすることはできません。	トンネルは自動的に確立されます。ユーザーは、Citrix Gateway クライアントをアンインストールしたり、別の Citrix Gateway に移動したりできます。

networkAccessONVPNFailure	クライアント制御	管理者以外のユーザー	管理者ユーザー
onlyToGateway	許可	トンネルは自動的に確立されます。ユーザーはログオフできます（ネットワークアクセスなし）。ユーザーは、別の Citrix Gateway をポイントすることもできます。この場合、アクセスは新しくポイントされた Citrix Gateway にのみ与えられます。	トンネルは自動的に確立されます。ユーザーは、Citrix Gateway クライアントをアンインストールしたり、別の Citrix Gateway に移動したりできます。
onlyToGateway	禁止	トンネルが自動的に確立されます。ユーザーがログオフしたり、別の Citrix Gateway をポイントしたりすることはできません。	トンネルは自動的に確立されます。ユーザーは、Citrix Gateway クライアントをアンインストールしたり、別の Citrix Gateway に移動したりできます。

AlwaysOn がダウンしているときに **URL** をホワイトリストに登録する

AlwaysON がダウンし、ネットワークがロックされている場合でも、ユーザーはいくつかの Web サイトにアクセスできます。管理者は **AlwaysOnWhitelist** レジストリを使用して、AlwaysOn が停止しているときにアクセスを有効にする Web サイトを追加できます。

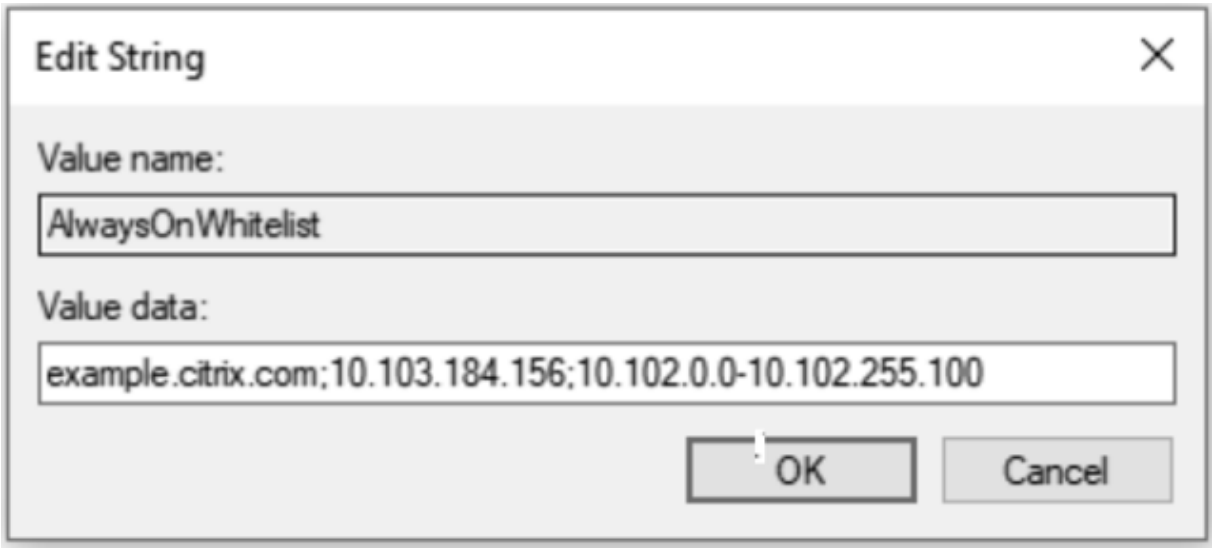
> 注:
>
> - **AlwaysOnWhitelist** レジストリは、リリース 13.0 ビルド 47.x 以降でサポートされています。
> - **AlwaysOnWhitelist** レジストリの場所は Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client。
> - Wildcard URLs/FQDNs は **AlwaysOnWhitelist** レジストリでサポートされていません。

AlwaysOnWhitelist レジストリを設定するには

AlwaysOnWhitelist レジストリに、アクセスを許可する FQDN、IP アドレス範囲、または IP アドレスのセミコロン区切りのリストを設定します。

例： mycompany.com-mycdn.com-10.120.67.0-10.120.67.255,67.67.67.67

次の図は、**AlwaysOnWhitelist** レジストリのサンプルを示しています。



Windows ログオン前に AlwaysON VPN (正式には AlwaysOn サービス)

April 9, 2020

Windows ログオン前の **AlwaysOn VPN** 機能を使用すると、ユーザーが Windows システムにログインする前でも、マシンレベルの VPN トンネルを確立できます。トンネルは、マシンがシャットダウンするまでアクティブのままです。ユーザログイン後、デバイスレベルの VPN トンネルはユーザレベルの VPN トンネルによって引き継がれます。ユーザがログオフすると、ユーザレベルトンネルが切断され、デバイスレベルトンネルが確立されます。Windows ログオン前の AlwaysOn VPN は、高度なポリシーのみを使用して構成できます。詳しくは、「Windows ログオン前に AlwaysON の VPN を構成する」を参照してください。

Windows ログオン前に AlwaysON VPN には、次の項目が含まれます。

- Windows マシンは、企業のアクティブディレクトリ（AD）を使用してユーザーのログイン資格情報を検証することができ、マシン上の Windows 資格情報はキャッシュされません。また、新しい企業の AD ユーザーは、マシンにシームレスにログオンできます。
- Windows マシンは、ユーザーがログインする前でも企業イントラネットの一部となり、IT 管理者はデバッグ目的で企業ネットワークからクライアントマシンにアクセスできます。
- 異なるユーザーがマシンにログインしたりログアウトしたりしても、Windows マシンの VPN トンネルは接続されたままです。

注意事項**:**

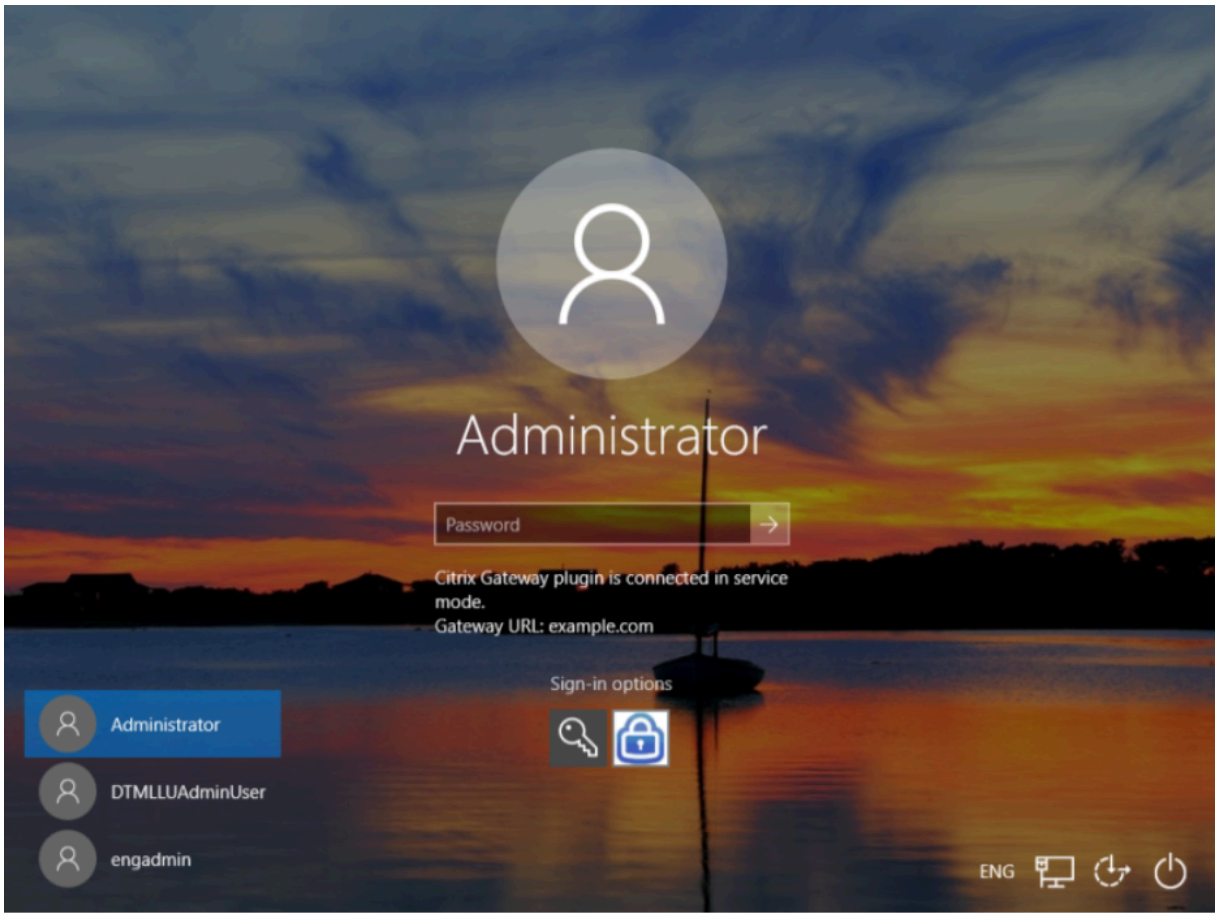
- Citrix Gateway および VPN プラグインは、バージョン 13.0.41.20 以降である必要があります。
- クライアントマシンにインターネット接続がない場合、Windows ログオン前に AlwaysOn VPN は、VPN トンネルを確立する前に、インターネット接続が使用可能になるまで待機します。
- クライアントマシンがキャプティブポータルネットワークに接続されている場合、Windows ログオンの前に AlwaysOn VPN は、ユーザーがキャプティブポータルへの認証を待機します。ユーザーがログインしてイン

ターネットアクセスが有効になると、Windows ログオン前に AlwaysOn VPN によって VPN トンネルが確立されます。

- Windows ログオン前の VPN 機能では、Citrix ADC のキャプティブポータルがサポートされます。
- Windows でログオン資格情報のキャッシュオプションが有効になっていない場合、ユーザーは、次のシナリオでログオンできません。
  - マシンにインターネット接続がありません
  - マシンがキャプティブポータルネットワークに接続されている

Windows ログオン構成の前に、**AlwaysOn VPN** の後の **Windows** 資格情報マネージャーの画面

Windows ログオン前に AlwaysOn VPN 機能を設定すると、Windows 資格情報マネージャー画面が次のように変更されます。



ログオン画面で [サインインオプション] をクリックすると、次の情報が表示されます。

- Citrix Gateway アイコンは、マシンが Citrix Gateway に接続されているかどうかを示します。
- ユーザ構成モードに応じて、次のいずれかのステートメントがログオン画面に表示されます。
  - Citrix Gateway がサービスモードで接続されている
  - Citrix Gateway がユーザーモードで接続されている

Windows ログオン前に AlwaysON の VPN を構成する

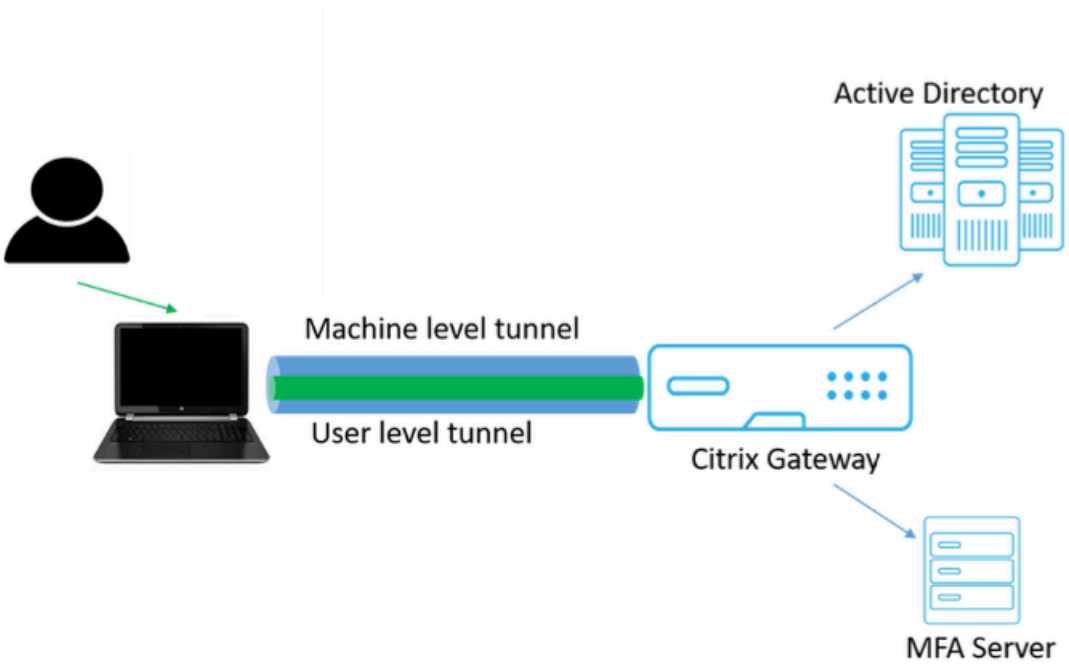
April 9, 2020

Windows ログオン前の AlwaysON の VPN では、次の機能が提供されます。

- 管理者は、ユーザーがドメイン Controller に接続してパスワードを変更できるを使用して、リモートで作業する最初のユーザーにワンタイムパスワードを提供します。
- 管理者は、ユーザーがログインする前にデバイスに対して AD ポリシーをリモートで管理/適用します。
- 管理者は、ユーザーがログオンした後、ユーザーグループに基づいて、ユーザーにきめ細かいレベルの制御を提供します。たとえば、ユーザーレベルのトンネルを使用して、特定のユーザーグループに対するリソースへのアクセスを制限または提供することができます。
- ユーザートンネルは、ユーザーの要件に従って MFA 用に設定できます。
- 複数のユーザーが同じマシンを使用することができ、選択的なリソースへのアクセスは、ユーザープロファイルに基づいて提供されます。たとえば、キオスクでは、複数のユーザーが手間をかけずにマシンを使用できます。
- リモートで作業しているユーザーは、ドメイン Controller に接続してパスワードを変更します。

Windows ログオン前の AlwaysON の VPN について

Windows ログオン機能前に AlwaysOn VPN のイベントのフローを次に示します。



- ユーザーがラップトップをオンにすると、デバイス証明書をアイデンティティとして使用して Citrix Gateway に向けてマシンレベルのトンネルが確立されます。

- ユーザーは、AD 資格情報を使用してラップトップにログインします。
- ログイン後、ユーザーは MFA に挑戦されます。
- 認証に成功すると、マシンレベルのトンネルがユーザレベルのトンネルに置き換えられます。
- ユーザがログアウトすると、ユーザレベルのトンネルはマシンレベルのトンネルに置き換えられます。

GUI を使用して **Windows** ログオン前に **AlwaysON** の **VPN** を構成する

前提要件

- Citrix Gateway および VPN プラグインは、バージョン 13.0.41.20 以降である必要があります。
- Citrix ADC アドバンストエディション以降は、ソリューションが動作するために必要とされます.
- この機能を構成するには、高度なポリシーを使用します。

構成には、次の大まかな手順が含まれます。

- 認証プロファイルの作成
- 認証仮想サーバーを作成する
- 認証ポリシーの作成
- 認証プロファイルにポリシーをバインドする

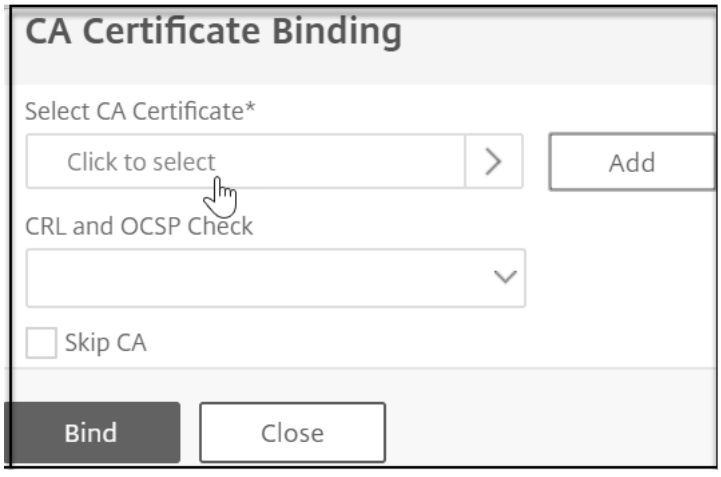
GUI を使用して機能を設定するには

クライアント証明書ベースの認証

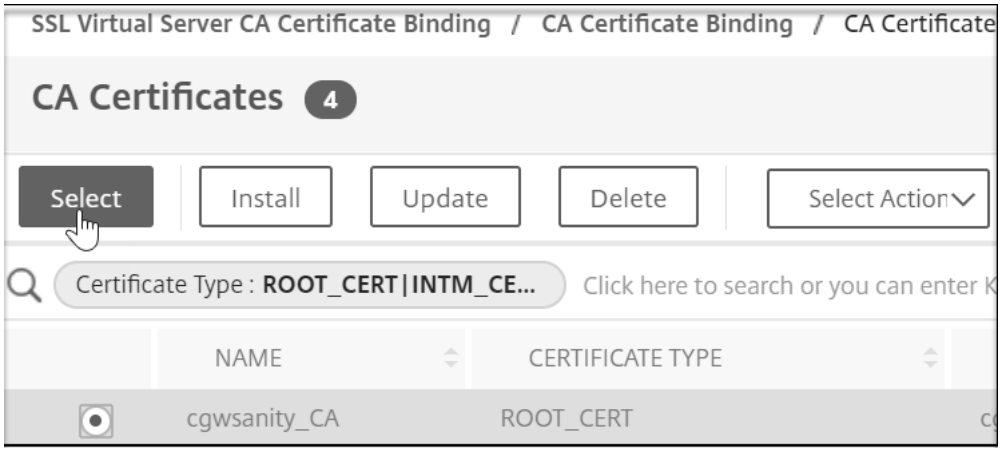
1. ［構成］タブで、［**Citrix Gateway**］**>** ［仮想サーバー］に移動します。
2. ［Citrix Gateway 仮想サーバー］ページで、既存の仮想サーバーを選択し、［編集］をクリックします。
3. [VPN 仮想サーバー] ページで、[編集] アイコンをクリックします。
4. [デバイス証明書の **CA**] セクションの横にある [追加] をクリックし、[**OK**] をクリックします。

注**:** [デバイス証明書を有効にする] チェックボックスは選択しないでください。

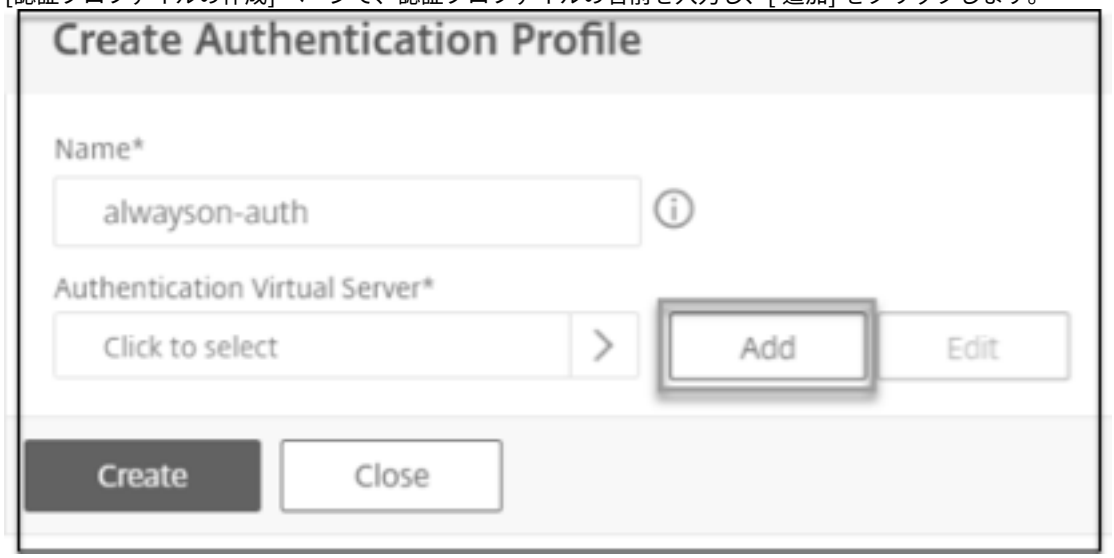
5. CA 証明書を仮想サーバーにバインドするには、[証明書] セクションの [**CA **** 証明書 ******] をクリックします。[**SSL** 仮想サーバー **CA** 証明書のバインド**]** ページの **[**バインドの追加] をクリックします。
6. [クリックして必要な証明書 を選択する**]** というテキストをクリックします。



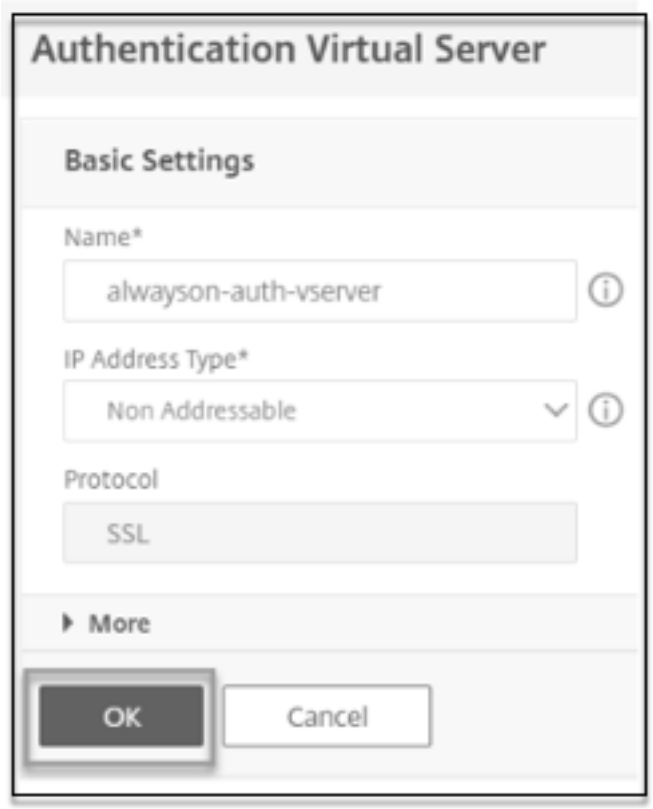
7. 必要な CA 証明書を選択します。



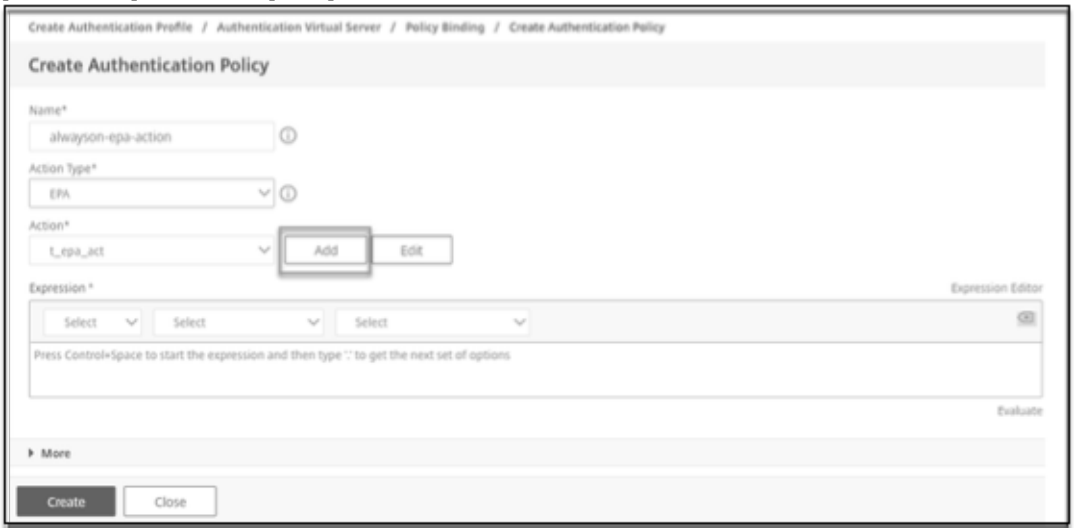
8. ［バインド］をクリックします。
9. [VPN 仮想サーバー] ページの [認証プロファイル] セクションで、[追加] をクリックします。
10. [認証プロファイルの作成] ページで、認証プロファイルの名前を入力し、[追加] をクリックします。



11. [認証仮想サーバー] ページで、認証仮想サーバーの名前を入力し、[IP アドレスの種類] として [アドレス不可能] を選択し、[**OK**] をクリックします。



12. [高度な認証ポリシー] で、[認証ポリシー] をクリックします。
13. [ポリシーのバインド] ページで、[ポリシーの選択] の横にある [追加] をクリックします。
14. [認証ポリシーの作成] ページで、
    a) 事前認証ポリシーの名前を入力します。
    b) [アクションタイプ] リストから **[**EPA**]** を選択します。
    c) [アクション] の横にある [追加] をクリックします。



15. [認証 EPA アクションの作成] ページで、

    a) 作成する EPA アクションの名前を入力します。

    b)「****** 式」フィールドに「**sys.client_expr**」(「デバイス証明書 **0_0**」) と入力します。******

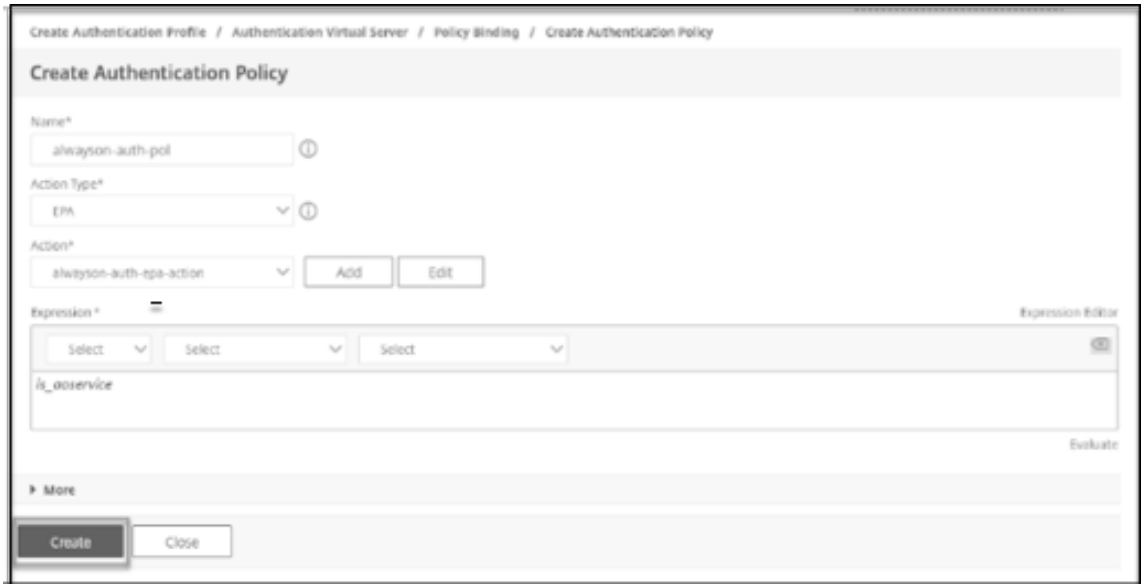
    c) [作成] をクリックします。

16. [認証ポリシーの作成] ページで、

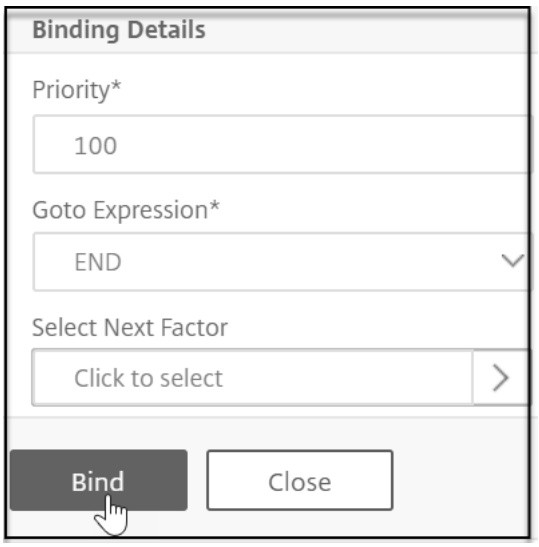
    a) 認証ポリシーの名前を入力します。

    b) [式] フィールドに **is_aoservice** と入力します。

    c) [作成] をクリックします。



17. [ポリシーバインディング] ページで、[優先度] に **100** と入力し、[バインド] をクリックします。



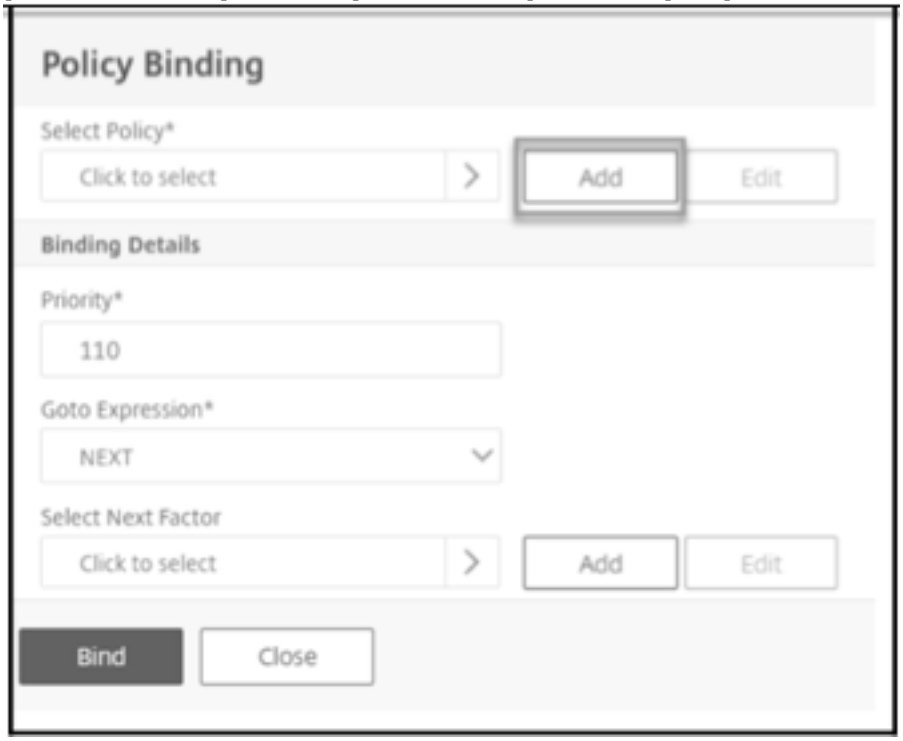
> 注：マシンレベルのトンネル設定はこれで完了です。Windows ログオン後にユーザーレベルのトンネルを使用しない場合は、手順 18 ～25 をスキップして、クライアント側の構成を続行できます。

Windows ログオン後にマシンレベルのトンネルをユーザーレベルのトンネルに置き換えるには、以下の設定を続行します。

18. 手順 17 でバインドされたポリシーの [終了 **]** ではなく **[**次の式へ移動] を変更します。

19. [認証仮想サーバー] ページで、[認証ポリシー] をクリックします。
20. [認証ポリシー] ページで、[バインドの追加] タブをクリックします。

21. [ポリシーのバインド] ページで、[ポリシーの選択] の横にある [追加] をクリックします。



22. [認証ポリシーの作成] ページで、

    a) 作成する「認証なし」ポリシーの名前を入力します。

    b) アクションタイプを **No_AUTHN** として選択します。

    c) [式] フィールドに **is_aoservice.** in と入力します。

    d) [作成] をクリックします。

    > 注：式 **is_aoservice.in** t は、Citrix Gateway バージョン 13.0 ビルド 41.20 以降から有効です。

23. [ポリシーのバインディング] ページで、[優先度] に **110** と入力し、[次の 要素の選択] の横にある [追加] をクリックします。

24. [認証ポリシーのラベル] ページで、LDAP 認証ポリシーを作成します。LDAP 認証ポリシーを作成するには、次の記事を参照してください。詳細については、構成ユーティリティを使用して LDAP 認証を構成するにはを参照してください。

25. [ポリシーの バインド] ページで [バインド] をクリックします。

クライアント側の構成

AlwaysOn、locationDetection、およびサフィックスリストのレジストリはオプションであり、ロケーション検出機能が必要な場合にのみ必要です。

レジストリキー	レジストリの種類	値と説明
AlwaysOnService	REG_DWORD	1 => ユーザーペルソナなしで AlwaysOn サービスを有効にする; 2 => ユーザーペルソナで AlwaysOn サービスを有効にする
常に URL に付いています	REG SZ	接続先の Citrix Gateway 仮想サーバーユーザーの URL です。例: `https://xyz.companyDomain.com`
AlwaysOn	REG_DWORD	1 => VPN 障害時にネットワークアクセスを許可する; 2=> VPN 障害時にネットワークアクセスをブロックする
locationDetection	REG_DWORD	1 => 位置検出を有効にするには、0 => 位置検出を無効にするには
suffixList	REG SZ	イントラネットドメインのカンマ区切りリスト。位置検出が有効な場合に使用されます。

これらのレジストリエントリの詳細については、「AlwaysOn」を参照してください。

クラシックポリシーを使用して Windows ログオンの前に AlwaysOn VPN を構成するには、「クラシックポリシーを使用して Windows ログオン前に常時 VPN を構成する」を参照してください。

Citrix Gateway の構成

April 9, 2020

Citrix Gateway を使用する Citrix ADC: 1 つの URL

Citrix Gateway を搭載した Citrix ADC により、デスクトップユーザーおよびモバイルユーザー向けの単一の URL を介して、あらゆるアプリケーションへのセキュアなアクセスを簡素化できます。この単一の URL の背後にある管理者は、アプリケーションへのリモートアクセスの構成、セキュリティ、および制御を一元管理できます。また、リモートユーザーは、必要なすべてのアプリケーションへのシームレスなシングルサインオンとログイン/ログアウトの使いやすさにより、エクスペリエンスが向上しています。

これを実現するために、Citrix ADC with Gateway は、Citrix ADC のコンテンツスイッチング機能および広範な認証インフラストラクチャとともに、この単一の URL を介して組織のサイトやアプリケーションへのアクセスを提供します。さらに、リモートユーザーは、iOS または Android のモバイルデバイス、および Citrix Gateway クライアントプラグインとともに Linux、PC、または Mac システムを使用して、どこにいても Citrix GatewayURL に統一されたアクセスが可能です。

Citrix Gateway デプロイメントでは、次のカテゴリのアプリケーションへの単一 URL アクセスを許可します。

- イントラネットアプリケーション。
- クライアントレスアプリケーション
- サービスとしてのソフトウェアアプリケーション
- Citrix ADC によって提供される構成済みアプリケーション
- Citrix Virtual Apps and Desktops の公開アプリケーション

イントラネットアプリケーションは、セキュアなエンタープライズネットワーク内に存在する任意の Web ベースアプリケーションです。これらは、組織のイントラネットサイト、バグ追跡アプリケーション、Wiki などの内部リソースです。

通常、セキュアな企業ネットワーク内に常駐する クライアントレスアプリケーション Citrix Gateway は、Outlook Web Access および SharePoint への単一の URL アクセスを提供します。これらのアプリケーションは、リモートユーザーが利用できる必要のある、専用のクライアントソフトウェアを使用せずに、Exchange メールおよびチームリソースへのアクセスを提供します。

SaaS アプリケーションは、クラウドアプリケーションとも呼ばれ、Sharefile、SalesForce、NetSuite などの組織が依存する外部のクラウドベースのアプリケーションです。SAML ベースのシングルサインオンは、これを提供する SaaS アプリケーションでサポートされています。

組織によっては、**Citrix ADC** の負荷分散構成で展開された **Citrix ADC** のアプリケーションがあらかじめ構成されている場合があります。多くの場合、これは「リバースプロキシ」アプリケーションとも呼ばれます。Citrix Gateway は、展開用の仮想サーバーが同じ Citrix ADC Citrix Gateway インスタンスまたはアプライアンス上にある場合に、これらのアプリケーションをサポートします。これらのアプリケーションは、Citrix Gateway 構成とは独立した独自の認証構成を持つ場合があります。

公開されている **Citrix Virtual Apps and Desktops** の公開アプリケーションは、Citrix Gateway の URL から利用できます。SmartAccess および SmartControl ポリシーは、必要に応じて、詳細なポリシーおよびこれらのリソースへのアクセス制御に適用できます。

Citrix Gateway 構成ウィザード

CitrixCitrix Gateway 構成ウィザードを使用して Citrix ADC を構成する場合、推奨される方法は、Citrix Gateway 構成ウィザードを使用することです。ウィザードでは、構成を順を追って実行し、必要なすべての仮想サーバー、ポリシー、および式を作成し、提供された詳細に基づいて設定を適用します。初期セットアップ後、ウィザードを使用して配置を管理し、その動作を監視できます。

> 注:
> Citrix Gateway 構成ウィザードでは、システムの初期構成は実行されません。Citrix Gateway を構成する前に、Citrix Gateway アプライアンスまたは VPX インスタンスの基本インストールが完了している必要があります。基本的な設定を完了初回セットアップウィザードを使用した Citrix Gateway の構成するには、のインストール手順を参照してください。

ウィザードによって構成される Citrix Gateway の要素は次のとおりです。

- Citrix Gateway のプライマリ仮想サーバー
- Citrix Gateway 仮想サーバーの SSL サーバー証明書
- プライマリ認証および任意のオプションのセカンダリ認証設定
- ポータル・テーマの選択とオプションのカスタマイズ
- Citrix Gateway ポータルからアクセスされるユーザーアプリケーション

これらの要素ごとに、設定情報を指定する必要があります。Citrix Gateway の基本的な展開では、次の情報が必要です。

- プライマリ Citrix Gateway 仮想サーバーの場合、展開環境のパブリック IP アドレスと IP ポート番号。これは、DNS で Citrix Gateway の URL のホスト名に解決される IP アドレスです。たとえば、Citrix Gateway デプロイメントの URL が`https://mycompany.com/`の場合、IP アドレスは mycompany.com に解決する必要があります。
- デプロイメント用の署名付き SSL サーバー証明書。Citrix Gateway は、PEM または PFX 形式の証明書をサポートしています。
- プライマリ認証サーバ情報。この認証構成でサポートされる認証システムは、LDAP/Active Directory、RADIUS、および証明書ベースです。セカンダリ LDAP または RADIUS 認証設定を作成することもできます。認証サーバの IP アドレスは、関連する管理者の資格情報またはディレクトリ属性とともに提供する必要があります。証明書認証では、デバイス証明書アトリビュートと CA 証明書を指定する必要があります。
- ポータル・テーマを選択できます。カスタマイズまたはブランド化されたポータル・デザインが必要な場合は、ウィザードを使用してカスタム・グラフィックをシステムにアップロードできます。
- Web ベースのユーザアプリケーションの場合、個々のアプリケーションの URL を指定する必要があります。SAML シングルサインオン認証を利用する Web アプリケーションの場合、ユーティリティはアサーションコンシューマーサービス URL を他のオプションの SAML パラメータとともに収集します。SAML 認証システムを使用するアプリケーションの構成の詳細を事前に収集します。
- Citrix Gateway 展開で Citrix Virtual Apps and Desktops の公開リソースを利用できるようにするには、統合ポイント（StoreFront、Web Interface、または Citrix ADC 上の Web Interface）を指定する必要があります。ユーティリティには、統合ポイントの完全修飾ドメイン名、サイトパス、シングルサインオンドメイン、Secure Ticket Authority (STA) サーバー URL、および統合ポイントの種類に応じてその他のものが必要です。

追加の構成管理

代替 SSL 設定やセッションポリシーなど、Citrix Gateway 構成ユーティリティでは利用できないサイト固有の設定については、Citrix Gateway 構成ユーティリティで必要な設定を管理できます。Citrix Gateway 構成ユーティリティによって作成されたコンテンツスイッチングまたは VPN 仮想サーバーでこれらの設定を変更できます。

コンテンツスイッチング仮想サーバ

これは、展開のメイン IP アドレスと URL の背後にある Citrix ADC 構成エンティティです。SSL サーバーの証明書とパラメーターは、この仮想サーバー上で管理されます。この仮想サーバは展開の応答ネットワークホストであるため、必要に応じて ICMP サーバの応答と RHI の状態をこの仮想サーバ上で変更できます。コンテンツスイッチング仮想サーバーは、[トラフィック管理] > [コンテンツスイッチング] > [仮想サーバー] の [設定] タブにあります。

VPN 仮想サーバー

Citrix Gateway 構成の他の VPN パラメータ、プロファイル、ポリシーバインディングはすべて、メイン認証構成を含め、この仮想サーバー上で管理されます。このエンティティは、Citrix Gateway > 仮想サーバーの「構成」タブで管理されます。関連する VPN 仮想サーバーの名前には、Citrix Gateway の初期構成時にコンテンツスイッチング仮想サーバーに与えられた名前が含まれます。

> 注:
> Citrix Gateway 展開用に作成された VPN 仮想サーバーはアドレス指定できず、0.0.0.0 の IP アドレスが割り当てられます。

Unified Gateway に関する **FAQ**

March 26, 2020

Unified Gateway とは
**

Unified Gateway は、Citrix ADC 11.0 リリースの新機能であり、単一の仮想サーバー（Unified Gateway 仮想サーバーと呼ばれます）でトラフィックを受信し、必要に応じてそのトラフィックを内部的に転送して、Unified Gateway 仮想サーバーにバインドされた仮想サーバーに転送する機能を提供します。

Unified Gateway 機能を使用すると、エンドユーザは、単一の IP アドレスまたは URL（Unified Gateway 仮想サーバに関連付けられている）を使用して複数のサービスにアクセスできます。管理者は、IP アドレスを解放し、Citrix Gateway 展開の構成を簡素化できます。

各 Unified Gateway 仮想サーバーは、1 台の Citrix Gateway 仮想サーバーをフロントエンドできます。また、フォーメーションの一環として、ゼロ個以上の負荷分散仮想サーバーをフロントエンドできます。Unified Gateway は、Citrix ADC アプライアンスのコンテンツスイッチング機能を利用して機能します。

Unified Gateway の配置の例を次に示します。

- Unified Gateway 仮想サーバー-> [1 つの Citrix Gateway 仮想サーバー]
- Unified Gateway 仮想サーバー-> [Citrix Gateway 仮想サーバー 1 つ、負荷分散仮想サーバー 1 つ]
- Unified Gateway 仮想サーバー-> [Citrix Gateway 仮想サーバー 1 台、負荷分散仮想サーバー 2 台]
- Unified Gateway 仮想サーバー-> [Citrix Gateway 仮想サーバー 1 台、負荷分散仮想サーバー 3 台]

各負荷分散仮想サーバーには、Microsoft Exchange や Citrix ShareFile などのバックエンドサービスをホストする標準の負荷分散サーバーを使用できます。

Unified Gateway を使用する理由
**

Unified Gateway 機能を使用すると、エンドユーザは、単一の IP アドレスまたは URL（Unified Gateway 仮想サーバに関連付けられている）を使用して複数のサービスにアクセスできます。管理者は、IP アドレスを解放し、Citrix Gateway 展開の構成を簡素化できるという利点があります。

複数の Unified Gateway 仮想サーバを使用できますか。
**

はい。Unified Gateway 仮想サーバは必要な数だけ存在できます。

Unified Gateway でコンテンツスイッチングが必要なのはなぜですか。
**

コンテンツスイッチング仮想サーバは、トラフィックを受信し、内部的に適切な仮想サーバに送信するため、コンテンツスイッチング機能が必要です。コンテンツスイッチング仮想サーバは、Unified Gateway 機能のプライマリコンポーネントです。

11.0 より前のリリースでは、コンテンツスイッチングを使用して、複数の仮想サーバのトラフィックを受信できます。その使用は Unified Gateway とも呼ばれていますか。
**

複数の仮想サーバのトラフィックを受信するためのコンテンツスイッチング仮想サーバの使用は、11.0 より前のリリースでサポートされています。ただし、コンテンツスイッチングでは、Citrix Gateway 仮想サーバーにトラフィックを送信できませんでした。

11.0 の機能強化により、コンテンツスイッチング仮想サーバーは Citrix Gateway 仮想サーバーを含む任意の仮想サーバーにトラフィックを転送できます。

Unified Gateway のコンテンツスイッチングポリシーで何が変わったのですか。
**

1. コンテンツスイッチングアクションに新しいコマンドラインパラメータ「-targetVserver」が追加されました。新しいパラメーターは、ターゲットの Citrix Gateway 仮想サーバーを指定するために使用されます。例:

> アクション UG_CSACT_MyUG ターゲット V サーバ UG_VPN_MyUG を追加

Citrix Gateway 構成ユーティリティでは、コンテンツスイッチング操作に、Citrix Gateway 仮想サーバーを参照できる「ターゲット仮想サーバー」という新しいオプションが追加されました。

2. 新しい高度なポリシー表現 is_vpn_url を使用して、Citrix Gateway および認証固有の要求を照合できます。

Unified Gateway では現在サポートされていない Citrix Gateway の機能は何ですか?
**

Unified Gateway では、すべての機能がサポートされています。ただし、VPN プラグインを介したネイティブログオンでは、マイナーな問題 (問題 ID 544325) が報告されています。この場合、シームレスなシングルサインオン (SSO) は機能しません。

Unified Gateway では、EPA スキャンの動作はどのようなものですか。
**

Unified Gateway では、エンドポイント分析は Citrix Gateway のアクセス方法でのみトリガーされ、AAA-TM アクセスではトリガーされません。Citrix Gateway 仮想サーバーで認証が行われた場合でも、ユーザーが AAA-TM 仮想サーバーにアクセスしようとすると、EPA スキャンはトリガーされません。ただし、ユーザがクライアントレス VPN/フル VPN アクセスを取得しようとすると、設定された EPA スキャンがトリガーされます。この場合、認証またはシームレスな SSO のいずれかが実行されます。

セットアップ

Unified Gateway のライセンス要件はどのようなものですか。
**

Unified Gateway は、アドバンストライセンスとプレミアムライセンスでのみサポートされます。Citrix Gateway のみまたは標準ライセンスエディションでは使用できません。

Unified Gateway で使用される Citrix Gateway 仮想サーバーには、IP/ポート/SSL 構成が必要ですか?
**

Unified Gateway 仮想サーバーで使用される Citrix Gateway 仮想サーバーの場合、Citrix Gateway 仮想サーバー上で IP/ポート/SSL 構成は必要ありません。ただし、RDP プロキシ機能では、同じ SSL/TLS サーバー証明書を Citrix Gateway 仮想サーバーにバインドできます。

Unified Gateway 仮想サーバーで使用するために、Citrix Gateway 仮想サーバー上にある SSL/TLS 証明書を再プロビジョニングする必要がありますか?
**

現在 Citrix Gateway 仮想サーバーにバインドされている証明書を再プロビジョニングする必要はありません。既存の SSL 証明書は自由に再利用でき、これらを Unified Gateway 仮想サーバにバインドできます。

単一 URL とマルチホスト展開の違いは何ですか? どちらが必要ですか?
**

単一の URL とは、Unified Gateway 仮想サーバが 1 つの完全修飾ドメイン名 (FQDN) のトラフィックを処理する機能です。この制限は、Unified Gateway が、FQDN が設定された証明書のサブジェクトを持つ SSL/TLS サーバ証明書を使用する場合に発生します。たとえば、次のように入力します。

ただし、Unified Gateway がワイルドカードサーバ証明書を使用している場合、複数のサブドメインのトラフィックを処理できます。例:*.citrix.com

もう 1 つのオプションは、複数の SSL/TLS サーバー証明書のバインドを可能にするサーバー名インジケータ (SNI) 機能を持つ SSL/TLS 構成です。例：オーサトリックス、オーサトリックス、オーサトリックス、オーサトリックス

単一ホストと複数ホストは、Web サイトが Web サーバー (Apache HTTP サーバーや Microsoft インターネットインフォメーションサービス (IIS) など) でホストされる方法に似ています。ホストが 1 つある場合は、Apache でエイリアスまたは「仮想ディレクトリ」を使用する場合と同じ方法で、サイトパスを使用してトラフィックを切り替えることができます。複数のホストがある場合は、Apache で仮想ホストを使用する方法と同様に、ホストヘッダーを使用してトラフィックを切り替えます。

認証

Unified Gateway ではどのような認証メカニズムを使用できますか。
**

Citrix Gateway で動作する既存の認証メカニズムはすべて、Unified Gateway で動作します。

これには、LDAP、RADIUS、SAML、Kerberos、証明書ベースの認証などがあります。

Citrix Gateway 仮想サーバーが Unified Gateway 仮想サーバーの背後に配置されるときに、アップグレードが自動的に使用される前に、Citrix Gateway 仮想サーバー上で構成されている認証メカニズム。アドレス指定できない IP アドレス（0.0.0.0）を Citrix Gateway 仮想サーバーに割り当てる以外に、追加の構成手順は必要ありません。

「自己認証」認証とは何ですか?
**

SelfAuth は認証タイプではありません。SelfAuth は、URL の作成方法を記述します。VPN URL 設定では、新しいコマンドラインパラメータ ssotype を使用できます。例:

```
\> add vpn url RGB RGB "http://blue.citrix.lab/"-vServerName Blue -ssotype
selfauth
```

SelfAuth は、ssotype パラメータの値の 1 つです。このタイプの URL を使用して、Unified Gateway 仮想サーバと同じドメイン内にないリソースにアクセスできます。この設定は、ブックマークを設定するときに構成ユーティリティに表示されます。

「ステップアップ」認証」とは何ですか?
**

AAA-TM リソースへのアクセスに、さらに安全なレベルの認証が必要な場合は、StepUp 認証を使用できます。コマンドラインで authnProfile コマンドを使用して、認証レベルパラメータを設定します。例:

> add authentication authnProfile AuthProfile -authnVsName AAATMVserver -AuthenticationHost auth.citrix.lab -AuthenticationDomain citrix.lab -AuthenticationLevel 100

この認証プロファイルは、負荷分散仮想サーバーにバインドされます。

ステップアップ認証は AAA-TM 仮想サーバでサポートされていますか。
**

はい、サポートされています。

一度ログイン/ログアウトとは何ですか?
**

1 回ログインする: VPN ユーザーは、AAA-TM または Citrix Gateway 仮想サーバーに 1 回ログインします。その後、VPN ユーザーはすべてのエンタープライズ/クラウド/Web アプリケーションにシームレスにアクセスできます。ユーザーを再認証する必要はありません。ただし、再認証は、AAA-TM StepUp などの特殊な場合に行われます。

一度ログアウトする: 最初の AAA-TM セッションまたは Citrix Gateway セッションが作成されると、そのユーザーの後続の AAA-TM セッションまたは Citrix Gateway セッションの作成に使用されます。これらのセッションのいずれかがログアウトされると、Citrix ADC アプライアンスはユーザーの他のアプリケーションまたはセッションもログアウトします。

共通認証ポリシーは、ロードバランシング仮想サーバレベルで AAA-TM ロードバランシング仮想サーバ固有の認証バインドを使用して Unified Gateway レベルで指定できますか。このユースケースをサポートするための構成手順は何ですか?
**

Unified Gateway の背後にある AAA-TM 仮想サーバに対して個別の認証ポリシーを指定する必要がある場合は、別個のアドレス指定可能な認証仮想サーバが必要です（通常の AAA-TM 設定と同様）。負荷分散仮想サーバーの認証ホストの設定は、この認証仮想サーバーを指している必要があります。

バインドされた AAA-TM 仮想サーバに独自の認証ポリシーが設定されるように、Unified Gateway をどのように設定しますか。
**

このシナリオでは、ロードバランシングサーバに、AAA-TM 仮想サーバを指すように認証 FQDN オプションが設定されている必要があります。AAA-TM 仮想サーバーは独立した IP アドレスを持っており、Citrix ADC およびクライアントから到達可能である必要があります。

Unified Gateway 仮想サーバを経由するユーザを認証するには、AAA-TM 認証仮想サーバが必要ですか。
**

いいえ。Citrix Gateway 仮想サーバーは、AAA-TM ユーザーも認証します。

Citrix Gateway 認証ポリシーは、Unified Gateway 仮想サーバーと Citrix Gateway 仮想サーバーのどちらで指定しますか?
**

認証ポリシーは、Citrix Gateway 仮想サーバーにバインドされます。

Unified Gateway コンテンツスイッチング仮想サーバの背後にある AAA-TM 仮想サーバで認証を有効にするにはどうすればよいですか。
**

AAA-TM で認証を有効にし、認証ホストを Unified Gateway コンテンツスイッチング FQDN にポイントします。

AAA-Traffic Management

コンテンツスイッチングの背後に TM 仮想サーバーを追加するにはどうすればよいですか（単一 URL とマルチホスト）?
**

単一の URL に AAA-TM 仮想サーバを追加することと、複数のホストに追加することには違いはありません。いずれの場合も、仮想サーバーはコンテンツスイッチングアクションのターゲットとして追加されます。単一の URL とマルチホストの違いは、コンテンツスイッチングポリシールールによって実装されます。

仮想サーバが Unified Gateway 仮想サーバの背後に移動された場合、AAA-TM ロードバランシング仮想サーバにバインドされた認証ポリシーはどうなりますか。
**

認証ポリシーは認証仮想サーバーにバインドされ、認証仮想サーバーは負荷分散仮想サーバーにバインドされます。Unified Gateway 仮想サーバーの場合、Citrix Gateway 仮想サーバーを単一の認証ポイントとして使用することをお勧めします。これにより、認証仮想サーバー上で認証を実行する必要がなくなります（または特定の認証仮想サーバーを使用する必要もあります）。認証ホストを Unified Gateway 仮想サーバー FQDN にポイントすると、認証が Citrix Gateway 仮想サーバーによって行われることが保証されます。Unified Gateway のコンテンツスイッチングを認証ホストにポイントしても、認証仮想サーバがバインドされている場合、認証仮想サーバにバインドされた認証ポリシーは無視されます。ただし、認証ホストをアドレス指定可能な独立した認証仮想サーバーに指定すると、バインドされた認証ポリシーが有効になります。

AAA-TM セッションのセッションポリシーをどのように設定しますか。
**

Unified Gateway で、AAA-TM 仮想サーバーに認証仮想サーバーが指定されていない場合、AAA-TM セッションは Citrix Gateway セッションポリシーを継承します。認証仮想サーバが指定されている場合、その仮想サーバにバインドされた AAA-TM セッションポリシーが適用されます。

ポータルのカスタマイズ

Citrix ADC 11.0 での Citrix Gateway ポータルへの変更は何ですか?
**

Citrix ADC リリース 11.0 より前のバージョンでは、単一のポータルのカスタマイズをグローバルレベルで設定できます。特定の Citrix ADC アプライアンスのすべての Gateway 仮想サーバーは、グローバルポータルのカスタマイズを使用します。

Citrix ADC 11.0 では、ポータル・テーマ機能を使用して、複数のポータル・テーマを設定できます。テーマは、グローバルにバインドすることも、特定の仮想サーバーにバインドすることもできます。

Citrix ADC 11.0 は、Citrix Gateway ポータルのカスタマイズをサポートしていますか?
**

構成ユーティリティーを使用すると、新しいポータル・テーマ機能を使用して、新しいポータル・テーマを完全にカスタマイズおよび作成できます。異なる画像をアップロードしたり、カラースキームを設定したり、テキストラベルを変更したりすることができます。

カスタマイズ可能なポータル・ページは次のとおりです。

- ログインページ
- エンドポイント分析ページ
- エンドポイント分析エラーページ
- ポストエンドポイント分析ページ
- VPN 接続ページ
- ポータルのホームページ

このリリースでは、Citrix Gateway 仮想サーバーを独自のポータル設計でカスタマイズできます。

ポータル・テーマは、Citrix ADC 高可用性またはクラスター展開でサポートされていますか?
**

はい。ポータルのテーマは、Citrix ADC 高可用性およびクラスター展開でサポートされています。

Citrix ADC 11.0 のアップグレードプロセスの一部としてカスタマイズが移行されますか?
**

いいえ。rc.conf/rc.netscaler ファイルの変更または 10.1/10.5 のカスタムテーマ機能を使用して呼び出される Citrix Gateway ポータルページの既存のカスタマイズは、Citrix ADC 11.0 へのアップグレード時に自動的に移行されません。

Citrix ADC 11.0 でポータル・テーマの準備のために従うべきアップグレード前の手順はありますか?
**

既存のカスタマイズはすべて、rc.conf ファイルまたは rc.netscaler ファイルから削除する必要があります。

もう 1 つのオプションは、カスタムテーマを使用する場合は、[既定] の設定を割り当てる必要があることです。

［構成］**> Citrix Gateway >** ［グローバル設定］に移動します。

[グローバル設定の変更] をクリックします。[クライアントエクスペリエンス] をクリックし、[**UI** テーマ] ドロップダウンリストから [デフォルト] を選択します。

私は、rc.conf または rc.netscaler によって呼び出される Citrix ADC インスタンスに保存されているカスタマイズを持っています。ポータル・テーマに移動する方法
**

Citrix ADC ナレッジセンターの記事CTX126206では、Citrix ADC 9.3 と 10.0 のビルド 73.5001.e まで、このような構成の詳細をリリースします。Citrix ADC 10.0 は 10.0 73.5002.e（10.1 および 10.5 を含む）をビルドするため、UITHEME カスタムパラメータを使用すると、再起動後もカスタマイズを維持できます。カスタマイズが Citrix ADC ハードドライブに保存されていて、これらのカスタマイズを引き続き使用する場合は、11.0 の GUI ファイルをバックアップし、既存のカスタムテーマファイルに挿入します。ポータル・テーマに移動する場合は、まず、「クライアント・エクスペリエンス」の「グローバル設定」または「セッション・プロファイル」の「UITHEME」パラメーターの設定を解除する必要があります。または、デフォルトまたはグリーンバブルに設定することもできます。その後、ポータル・テーマの作成とバインドを開始できます。

Citrix ADC 11.0 にアップグレードする前に、現在のカスタマイズをエクスポートして保存するにはどうすればよいですか? エクスポートしたファイルを別の Citrix ADC アプライアンスに移動できますか?
**

ns_gui_custom フォルダにアップロードされたカスタマイズされたファイルは、ディスク上にあり、アップグレード後も保持されます。ただし、これらのファイルは、新しい Citrix ADC 11.0 カーネルおよびカーネルの一部である他の GUI ファイルと完全には互換性がない場合があります。したがって、11.0 の GUI ファイルをバックアップし、バックアップをカスタマイズすることをお勧めします。

さらに、構成ユーティリティーには、ns_custom_gui フォルダーを別の Citrix ADC アプライアンスにエクスポートするユーティリティーはありません。Citrix ADC インスタンスからファイルを削除するには、SSH または WinSCP などのファイル転送ユーティリティを使用する必要があります。

ポータル・テーマは AAA-TM 仮想サーバーでサポートされていますか?
**

はい。ポータルテーマは、AAA-TM 仮想サーバーでサポートされています。

RDP プロキシ

Citrix Gateway 11.0 の RDP プロキシで何が変更されましたか?
**

Citrix ADC 10.5.e 拡張リリース以降、RDP プロキシには多くの機能が強化されています。Citrix ADC 11.0 では、この機能は最初にリリースされたビルドから利用できます。

ライセンスの変更

Citrix ADC 11.0 の RDP プロキシ機能は、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使用できます。Citrix 同時ユーザー（CCU）ライセンスは、ユーザーごとに取得する必要があります。

コマンドを有効にする

Citrix ADC 10.5.e では、RDP プロキシを有効にするコマンドはありませんでした。Citrix ADC 11.0 では、次のコマンドが追加されました。

> フィーチャー rdpproxy の有効化

このコマンドを実行するには、機能のライセンスが必要です。

その他の **RDP** プロキシの変更

サーバプロファイルの PSK（事前共有キー）属性が必須になりました。

RDP プロキシ用の既存の Citrix ADC 10.5.e 構成を Citrix ADC 11.0 に移行するには、以下の詳細を理解し、対処する必要があります。

管理者が既存の RDP プロキシ設定を選択した Unified Gateway 配置に追加する場合は、次の手順を実行します。

- Citrix Gateway 仮想サーバーの IP アドレスを編集し、アドレス指定できない IP アドレス（0.0.0.0）に設定する必要があります。
- SSL/TLS サーバー証明書、認証ポリシーは、選択した Unified Gateway 構成の一部である Citrix Gateway way 仮想サーバーにバインドする必要があります。

Citrix ADC 10.5.e に基づくリモートデスクトッププロトコル（RDP）プロキシ構成を Citrix ADC 11.0 に移行するにはどうすればよいですか?
**

オプション 1：プレミアムライセンスまたはアドバンスライセンスを使用して、既存の Citrix Gateway 仮想サーバーを RDP プロキシ構成のままにします。

オプション 2：既存の Citrix Gateway 仮想サーバーを RDP プロキシ構成で移動し、Unified Gateway 仮想サーバーの背後に配置します。

オプション 3：RDP プロキシ構成を持つスタンドアロンの Citrix Gateway 仮想サーバーを既存の標準エディションアプライアンスに追加します。

Citrix ADC 11.0 リリースを使用して、RDP プロキシ構成用に Citrix Gateway をどのようにセットアップしますか?
**

NS 11.0 リリースを使用して RDP プロキシを展開するには、次の 2 つのオプションがあります。

1）外部に面した Citrix Gateway 仮想サーバーを使用する。これには、Citrix Gateway 仮想サーバーの外部から見える IP アドレス/FQDN が 1 つ必要です。このオプションは、Citrix ADC 10.5.e で利用できるものです。

2）Citrix Gateway 仮想サーバーのフロントエンドの Unified Gateway 仮想サーバーを使用する。

オプション 2 では、アドレス指定不可能な IP アドレス（0.0.0.0）を使用するため、Citrix Gateway 仮想サーバーは独自の IP アドレス/FQDN を必要としません。

他の **Citrix** ソフトウェアとの統合

HDX Insight は Unified Gateway と連携しますか?
**

Citrix Gateway を Unified Gateway で展開する場合、Citrix Gateway 仮想サーバーには有効な SSL 証明書がバインドされている必要があります。また、HDX Insight レポート用に Citrix ADCInsight Center 用の AppFlow レコードを生成するには、その証明書が UP 状態である必要があります。

既存の HDX Insight 構成を移行するにはどうすればよいですか?
**

移行は不要です。Citrix Gateway 仮想サーバーにバインドされた AppFlow ポリシーは、その Citrix Gateway 仮想サーバーが Unified Gateway 仮想サーバーの背後に配置されている場合に引き継がれます。

Citrix Gateway 仮想サーバーの Citrix ADC Insight Center にある既存のデータについては、次の 2 つの可能性があります。

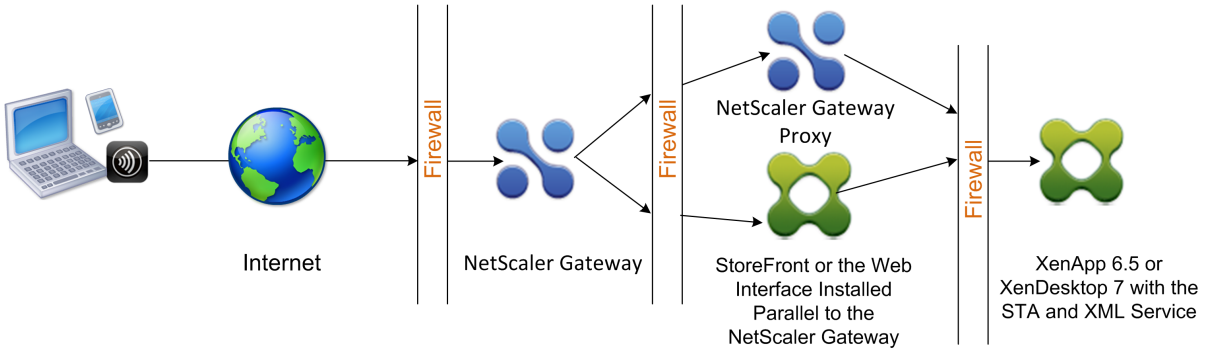
- Citrix Gateway 仮想サーバーの IP アドレスが、Unified Gateway への移行の一環として Unified Gateway 仮想サーバーに割り当てられている場合、データは Citrix Gateway 仮想サーバーにリンクされたままになります。
- Unified Gateway 仮想サーバーに別の IP アドレスが割り当てられている場合、Citrix Gateway 仮想サーバーの AppFlow データはその新しい IP アドレスにリンクされます。したがって、既存のデータは新しいデータの一部にはなりません。

ダブルホップ **DMZ** での展開

March 26, 2020

内部ネットワークを保護するために、3 つのファイアウォールを使用する場合があります。3 つのファイアウォールは、DMZ を 2 つの段階にわけて、内部ネットワークにさらなるセキュリティを提供します。このネットワーク構成を、ダブルホップ DMZ と呼びます。

図 1: ダブルホップ DMZ にデプロイされた Citrix Gateway アプライアンス



> 注：説明のため、前述の例では、StoreFront、Web Interface および Citrix Virtual Apps で 3 つのファイアウォールを使用したダブルホップ構成について説明していますが、DMZ 内に 1 つのアプライアンス、安全なネットワーク内に 1 つのアプライアンスを含むダブルホップ DMZ を使用することもできます。DMZ 内の 1 つのアプライアンスとセキュアネットワーク内の 1 つのアプライアンスでダブルホップ構成を構成する場合、3 番目のファイアウォールでポートを開く手順は無視できます。

ダブルホップ DMZ は、Citrix StoreFront または CitrixCitrix Gateway プロキシと並行してインストールされた Web Interface と連携するように構成できます。ユーザーは、Citrix Workspace アプリを使用して接続します。

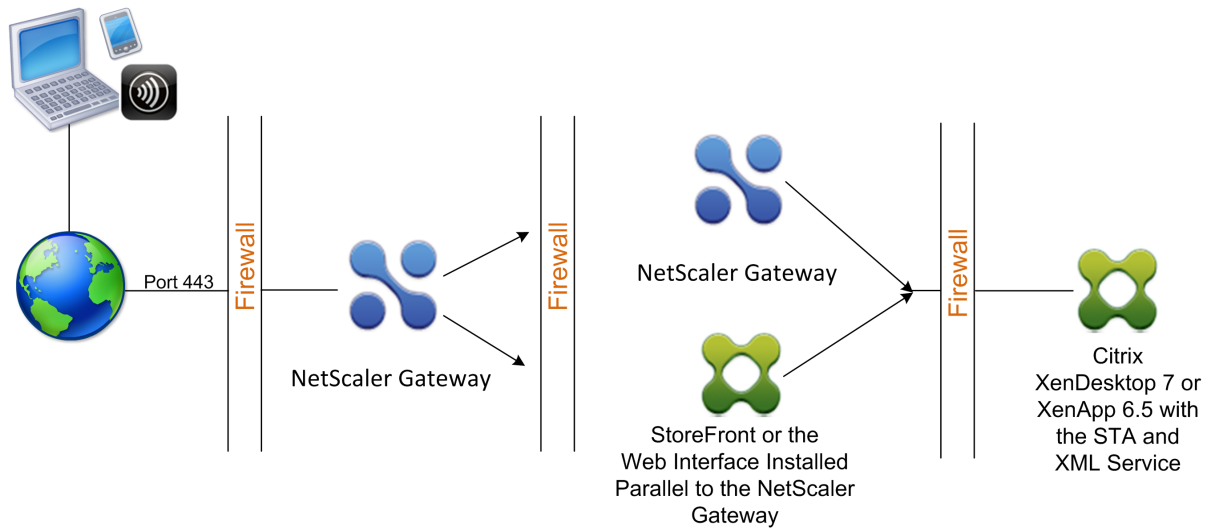
> 注：StoreFront を使用してダブルホップ DMZ に Citrix Gateway を展開すると、Citrix Workspace アプリの電子メールベースの自動検出が機能しません。

ダブルホップ **DMZ** での **Citrix Gateway** の展開

March 26, 2020

内部ネットワークを保護するために、3 つのファイアウォールを使用する場合があります。3 つのファイアウォールは、DMZ を 2 つの段階にわけて、内部ネットワークにさらなるセキュリティを提供します。このネットワーク構成を、ダブルホップ DMZ と呼びます。Citrix Virtual Apps および StoreFront を使用して、ダブルホップ DMZ に Citrix Gateway を展開できます。

図 1：ダブルホップ DMZ にデプロイされた Citrix Gateway アプライアンス



注：説明のため、前述の例では、3 つのファイアウォールと Web Interface を使用したダブルホップ構成について説明していますが、DMZ 内の 1 つのアプライアンスとセキュアネットワーク内の 1 つのアプライアンスを持つダブルホップ DMZ を使用することもできます。DMZ 内の 1 つのアプライアンスとセキュアネットワーク内の 1 つのアプライアンスでダブルホップ構成を構成する場合、3 番目のファイアウォールでポートを開く手順は無視できます。

ダブルホップ DMZ は、Citrix StoreFront または Web Interface で動作するように構成できます。ユーザーは、Citrix Workspace アプリを使用して接続します。

> 注
>
> StoreFront を使用してダブルホップ DMZ に Citrix Gateway を展開すると、Citrix Workspace アプリの電子メールベースの自動検出が機能しません。

ダブルホップ展開の仕組み

March 26, 2020

Citrix Gateway アプライアンスをダブルホップ DMZ に展開して、Citrix Virtual Apps を実行しているサーバーへのアクセスを制御できます。ダブルホップ展開での接続は、次のように行われます。

- ユーザーは、Web ブラウザーを使用し、Citrix Workspace アプリを使用して公開アプリケーションを選択することにより、最初の DMZ で Citrix Gateway に接続します。
- Citrix Workspace は、ユーザーデバイス上で起動されます。ユーザーは、Citrix Gateway に接続して、セキュアネットワーク内のサーバーファームで実行されている公開アプリケーションにアクセスします。

  注：ダブルホップ DMZ 展開では、Secure Hub と Citrix Gateway プラグインはサポートされていません。ユーザー接続には、Citrix Workspace アプリのみが使用されます。
- 最初の DMZ の Citrix 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 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、内部ネットワーク上のサーバーへのアクセスを制御します。
- 2 つ目の DMZ の Citrix Gateway は、Citrix Gateway のプロキシデバイスとして機能します。この Citrix Gateway では、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。最初の DMZ の Citrix Gateway と内部ネットワークの Secure Ticket Authority（STA）間の通信も、2 番目の DMZ の Citrix Gateway を介してプロキシされます。

Citrix Gateway は、IPv4 および IPv6 接続をサポートしています。構成ユーティリティを使用して IPv6 アドレスを構成できます。

次の表に、さまざまな ICA 機能のダブルホップ展開のサポートを示します。

ICA 機能	ダブルホップのサポート
SmartAccess	はい
SmartControl	はい
Enlightened Data Transport（EDT）	はい
HDX Insight	はい

ICA 機能	ダブルホップのサポート
ICA セッションの信頼性（ポート 2598）	はい
ICA セッションの移行	はい
ICA セッションのタイムアウト	はい
マルチストリーム ICA	はい
Framehawk	いいえ
UDP オーディオ	いいえ

ダブルホップ **DMZ** 配置における通信フロー

April 9, 2020

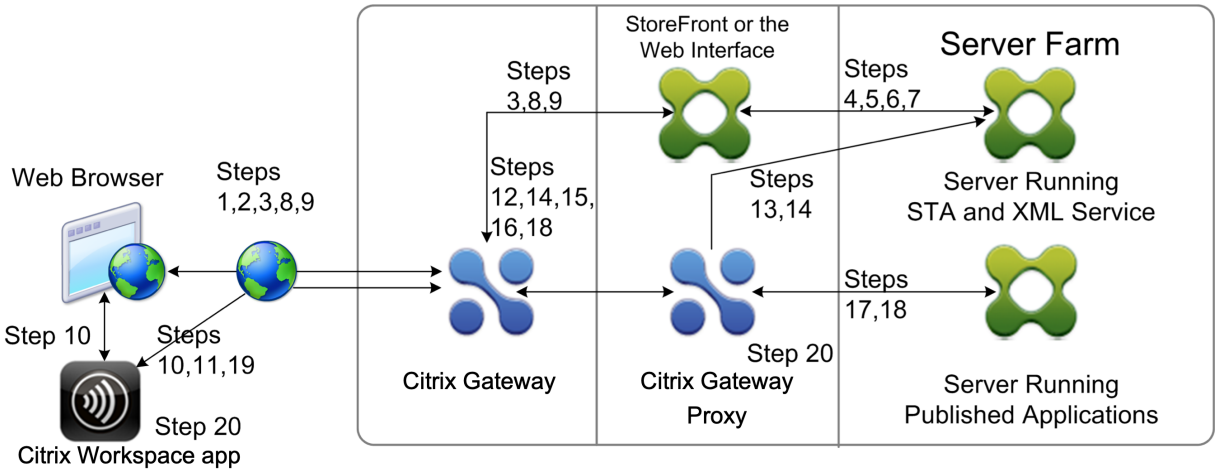
ダブルホップ DMZ 展開に関連する構成上の問題を理解するには、ダブルホップ DMZ 展開におけるさまざまな Citrix Gateway コンポーネントと Citrix Virtual Apps コンポーネントがどのように通信してユーザー接続をサポートしているかを理解する必要があります。StoreFront と Web Interface の接続プロセスは同じです。

ユーザー接続プロセスは 1 つの連続フローで行われますが、手順については、次の 4 つのトピックで詳しく説明します。

- ユーザーの認証
- Session Ticket の作成
- Citrix Workspace アプリの起動
- 接続の完了

次の図は、StoreFront または Web Interface へのユーザー接続プロセスで発生する手順を示しています。セキュアなネットワークでは、Citrix Virtual Apps を実行しているコンピューターは、Secure Ticket Authority（STA）、XML サービス、および公開アプリケーションも実行します。

図 1: ダブルホップ DMZ ユーザ接続プロセス

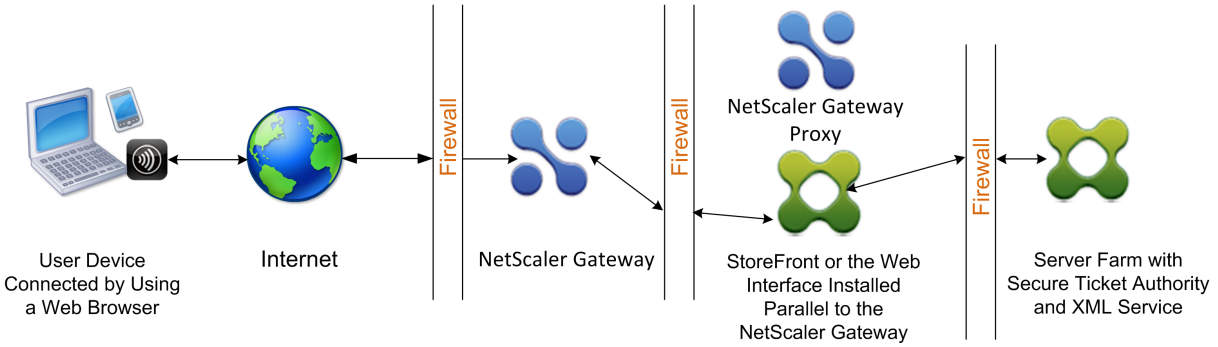


ユーザーの認証

March 26, 2020

ユーザ認証は、ダブルホップ DMZ 展開におけるユーザ接続プロセスの最初のステップです。次の図は、この展開におけるユーザー接続プロセスを示しています。

図 1: ダブルホップ DMZ におけるユーザ認証のための通信フロー



ユーザー認証段階では、次の基本プロセスが実行されます。

1. ユーザーは、最初の DMZ で Citrix Gateway に接続する Web ブラウザーなどで、Citrix Gateway のアドレス（https://www.ng.wxyco.comなど）を入力します。Citrix Gateway ateway でログオンページ認証を有効にした場合、Citrix Gateway はユーザーを認証します。
2. 最初の DMZ 内の Citrix Gateway は、要求を受信します。
3. Citrix Gateway は、Web ブラウザーの接続を Web Interface にリダイレクトします。
4. Web Interface は、内部ネットワークのサーバーファームで実行されている Citrix XML Service にユーザーの資格情報を送信します。
5. Citrix の XML サービスは、ユーザーを認証します。

6. XML サービスは、ユーザーがアクセスを許可されている公開アプリケーションのリストを作成し、このリストを Web Interface に送信します。

Citrix Gateway で認証を有効にすると、アプライアンスは Citrix Gateway のログオンページをユーザーに送信します。ユーザーがログオン・ページで認証資格情報を入力すると、アプライアンスはユーザーを認証します。その後 Citrix Gateway ユーザーの資格情報が Web Interface に返されます。

認証を有効にしない場合、Citrix Gateway は認証を実行しません。アプライアンスは Web Interface に接続し、Web Interface ログオン・ページを取得し、Web Interface ログオン・ページをユーザーに送信します。ユーザーが Web Interface ログオンページで認証資格情報を入力すると、Citrix Gateway がユーザーの資格情報を Web Interface に戻します。

セッション・チケットの作成

March 26, 2020

セッション・チケットの作成は、ダブルホップ DMZ 展開におけるユーザー接続プロセスの第 2 段階です。

セッション・チケット作成段階では、次の基本プロセスが実行されます。

1. Web Interface は内部ネットワークの XML サービスと Secure Ticket Authority（STA）の両方と通信し、ユーザーがアクセスを許可されている公開アプリケーションのセッション・チケットを生成します。セッションチケットには、公開アプリケーションをホストする Citrix Virtual Apps を実行しているコンピューターのエイリアスアドレスが含まれています。
2. STA は、公開アプリケーションをホストするサーバーの IP アドレスを保存します。STA は、要求されたセッション・チケットを Web Interface に送信します。各セッション・チケットには、公開アプリケーションをホストするサーバーの IP アドレスを表すエイリアスが含まれますが、実際の IP アドレスは含まれません。
3. Web Interface は、公開アプリケーションごとに ICA ファイルを生成します。ICA ファイルには、STA が発行したチケットが含まれています。次に、Web Interface によって Web ページが作成され、公開アプリケーションへのリンクのリストが入力され、この Web ページがユーザーデバイス上の Web ブラウザに送信されます。

Citrix Workspace アプリの起動

March 26, 2020

Citrix Workspace アプリの起動は、ダブルホップ DMZ 展開におけるユーザー接続プロセスの第 3 段階です。基本的なプロセスは次のとおりです。

1. ユーザーは、Web Interface で公開アプリケーションへのリンクをクリックします。Web Interface は、その公開アプリケーションの ICA ファイルをユーザーデバイスのブラウザに送信します。

ICA ファイルには、Web ブラウザに Receiver を起動するように指示するデータが含まれています。

ICA ファイルには、最初の DMZ の Citrix Gateway の完全修飾ドメイン名（FQDN）またはドメインネームシステム（DNS）名も含まれます。

2. Web ブラウザーで Receiver が起動し、ユーザーは ICA ファイルの Citrix Gateway 名を使用して最初の DMZ の Citrix Gateway に接続します。初期 SSL/TLS ハンドシェイクが行われ、Citrix Gateway を実行しているサーバーの識別情報が確立されます。

接続の完了

March 26, 2020

接続の完了は、ダブルホップ DMZ 展開におけるユーザー接続プロセスの第 4 段階と最終段階です。

接続完了段階では、次の基本プロセスが実行されます。

- ユーザーは、Web Interface で公開アプリケーションへのリンクをクリックします。
- Web ブラウザは、Web Interface によって生成された ICA ファイルを受信し、Citrix Workspace アプリを起動します。
  注：ICA ファイルには、Citrix Workspace アプリを起動するように Web ブラウザーに指示するコードが含まれています。
- Citrix Workspace アプリは、最初の DMZ で Citrix Gateway への ICA 接続を開始します。
- 最初の DMZ の Citrix Gateway は、内部ネットワークの Secure Ticket Authority（STA）と通信し、セッションチケットのエイリアスアドレスを、Citrix Virtual Apps または StoreFront を実行しているコンピュータの実際の IP アドレスに解決します。この通信は、Citrix Gateway プロキシによって 2 番目の DMZ を介してプロキシされます。
- 最初の DMZ の Citrix Gateway は、Citrix Workspace アプリへの ICA 接続を完了します。
- Citrix Workspace アプリは、両方の Citrix Gateway アプライアンスを経由して、内部ネットワーク上の Citrix Virtual Apps を実行しているコンピューターと通信できるようになりました。

ユーザー接続プロセスを完了するための詳細な手順は次のとおりです。

1. Citrix Workspace アプリは、公開アプリケーションの STA チケットを最初の DMZ の Citrix Gateway に送信します。
2. 最初の DMZ の Citrix Gateway は、チケットの検証のために内部ネットワークの STA に接続します。STA に接続するために、Citrix Gateway は、2 番目の DMZ の Citrix Gateway プロキシに SSL 接続を備えた SOCKS または SOCKS を確立します。
3. 2 番目の DMZ の Citrix Gateway プロキシは、チケット検証要求を内部ネットワークの STA に渡します。STA はチケットを検証し、公開アプリケーションをホストする Citrix Virtual Apps を実行しているコンピュータにチケットをマッピングします。
4. STA は、2 番目の DMZ の Citrix Gateway プロキシに応答を送信します。このプロキシは最初の DMZ の Citrix Gateway に渡されます。この応答は、チケットの検証を完了し、公開アプリケーションをホストする

コンピューターの IP アドレスが含まれます。

5. 最初の DMZ の Citrix Gateway は、Citrix Virtual Apps サーバーのアドレスをユーザー接続パケットに組み込み、このパケットを 2 番目の DMZ の Citrix Gateway プロキシに送信します。
6. 2 番目の DMZ の Citrix Gateway プロキシは、接続パケットで指定されたサーバーへの接続要求を行います。
7. サーバーは、2 番目の DMZ の Citrix Gateway プロキシに応答します。2 番目の DMZ の Citrix Gateway プロキシは、この応答を最初の DMZ の Citrix Gateway に渡して、最初の DMZ のサーバーと Citrix Gateway 間の接続を完了します。
8. 最初の DMZ の Citrix Gateway は、最終的な接続パケットをユーザーデバイスに渡すことによって、ユーザーデバイスとの SSL/TLS ハンドシェイクを完了します。ユーザーデバイスからサーバーへの接続が確立されます。
9. ICA トラフィックは、ユーザーデバイスとサーバー間で、最初の DMZ では Citrix Gateway と、2 番目の DMZ では Citrix Gateway プロキシを経由して流れます。

ダブルホップ **DMZ** 配置の準備

March 26, 2020

ダブルホップ DMZ 配置の設定時に適切に準備し、不要な問題を回避するには、次の質問に答える必要があります。

- 負荷分散をサポートしますか?
- ファイアウォールでどのポートを開く必要がありますか。
- SSL 証明書はいくつ必要ですか?
- 展開を開始する前にどのようなコンポーネントが必要ですか。

このセクションのトピックには、環境に応じてこれらの質問に答えるための情報が含まれています。

配置を開始するために必要なコンポーネント

ダブルホップ DMZ 展開を開始する前に、次のコンポーネントがあることを確認します。

- 少なくとも、2 つの Citrix Gateway アプライアンス（DMZ ごとに 1 つずつ）が利用可能である必要があります。
- Citrix Virtual Apps を実行しているサーバーは、内部ネットワークにインストールされ、動作している必要があります。
- Web Interface または Storefront を 2 番目の DMZ にインストールし、内部ネットワークのサーバーファームで動作するように構成する必要があります。
- 少なくとも、最初の DMZ の Citrix Gateway に 1 つの SSL サーバー証明書をインストールする必要があります。この証明書により、Citrix Gateway への Web ブラウザーとユーザー接続が暗号化されます。

  ダブルホップ DMZ 展開の他のコンポーネント間で発生する接続を暗号化する場合は、追加の証明書が必要です。

ダブルホップ DMZ での Citrix Gateway のインストールと構成

March 26, 2020

ダブルホップ DMZ に Citrix Gateway を展開するには、いくつかの手順を実行する必要があります。手順には、両方の DMZ にアプライアンスをインストールし、ユーザー・デバイス接続用にアプライアンスを構成する手順が含まれます。

最初の DMZ への Citrix Gateway のインストール

最初の DMZ に Citrix Gateway をインストールするには、の手順に従いますModel MPX 5500 アプライアンスのインストール。

最初の DMZ に複数の Citrix Gateway アプライアンスをインストールする場合は、ロードバランサーの背後にアプライアンスを展開できます。

最初の DMZ での Citrix Gateway の構成

ダブルホップ DMZ 展開では、最初の DMZ 内の各 Citrix Gateway を構成して、2 番目の DMZ の StoreFront または Web Interface に接続をリダイレクトする必要があります。

StoreFront または Web Interface へのリダイレクトは、Citrix Gateway グローバルまたは仮想サーバーレベルで実行されます。Citrix Gateway 経由で Web Interface に接続するには、ユーザーが Web Interface へのリダイレクトが有効になっている Citrix Gateway ユーザーグループに関連付けられている必要があります。

2 番目の DMZ への Citrix Gateway のインストール

2 つ目の DMZ の Citrix Gateway アプライアンスは、2 つ目の DMZ で ICA および STA (Secure Ticket Authority) トラフィックをプロキシするため、Citrix Gateway プロキシと呼ばれます。

Model MPX 5500 アプライアンスのインストールの手順に従って、各 Citrix Gateway アプライアンスを 2 つ目の DMZ にインストールします。

このインストール手順を使用して、2 台目の DMZ に追加のアプライアンスをインストールできます。

2 つ目の DMZ に Citrix Gateway アプライアンスをインストールした後、次の設定を構成します。

- Citrix Gateway プロキシで仮想サーバーを構成します。
- 最初の DMZ と 2 番目の DMZ で Citrix Gateway アプライアンスが相互に通信するように構成します。
- 2 つ目の DMZ の Citrix Gateway をグローバルにバインドするか、仮想サーバーにバインドします。
- 第 1 DMZ のアプランスで STA を構成します。
- ファイアウォールで DMZ を分離して、ポートを開きます。
- アプライアンスに証明書をインストールします。

Citrix Gateway プロキシ上の仮想サーバーでの設定の構成

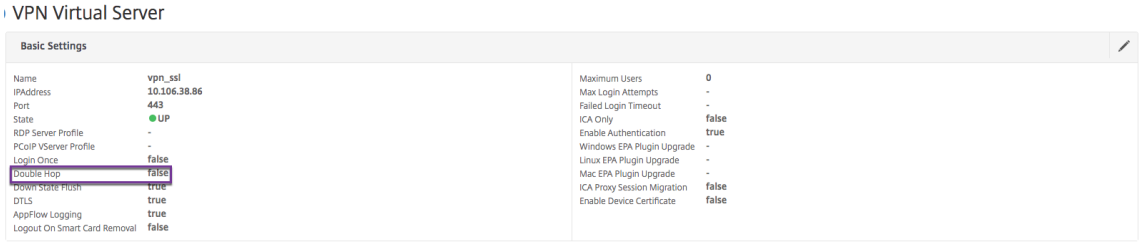
March 26, 2020

Citrix Gateway アプライアンス間で接続を許可するには、Citrix Gateway プロキシ上の仮想サーバーでダブルホップを有効にします。

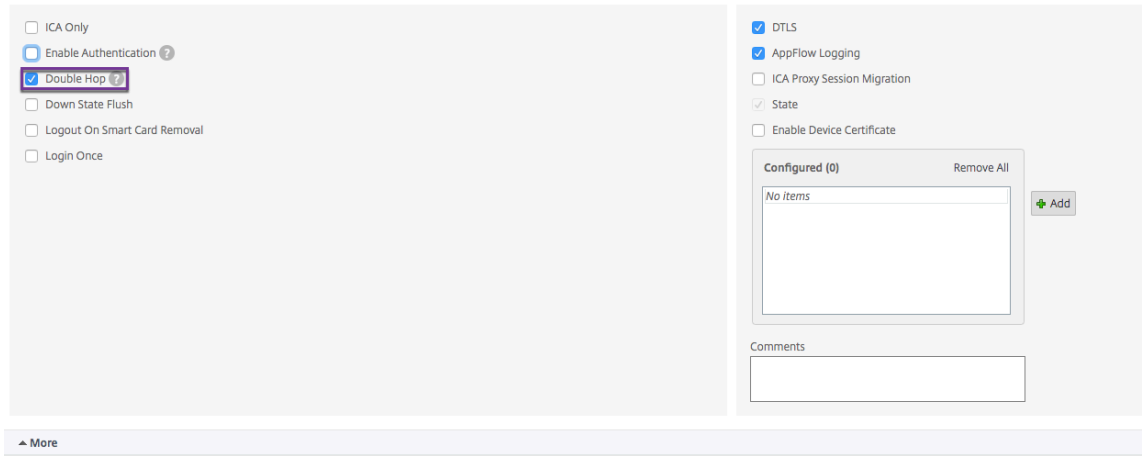
ユーザーが接続すると、Citrix Gateway アプライアンスはユーザーを認証し、プロキシアプライアンスへの接続をプロキシします。最初の DMZ の Citrix Gateway で、2 番目の DMZ の Citrix Gateway と通信するように仮想サーバーを構成します。Citrix Gateway プロキシでは、認証やポリシーを構成しないでください。仮想サーバーでの認証を無効にすることをお勧めします。

GUI を使用して Citrix Gateway プロキシ上の仮想サーバーでダブルホップを有効にするには

1. ［構成］**> Citrix Gateway >** ［仮想サーバー］に移動します。
2. 仮想サーバを選択し、[**Edit**] をクリックします。
3. [基本設定**]** セクションで、[編集] アイコンをクリックし、[その他] をクリックします。



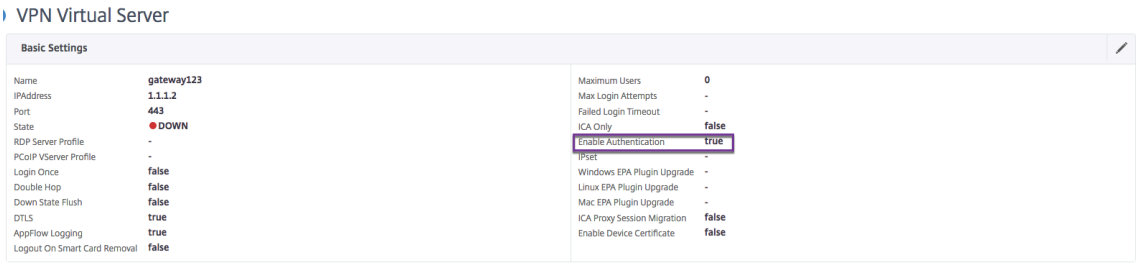
4. [ダブルホップ] を選択します。



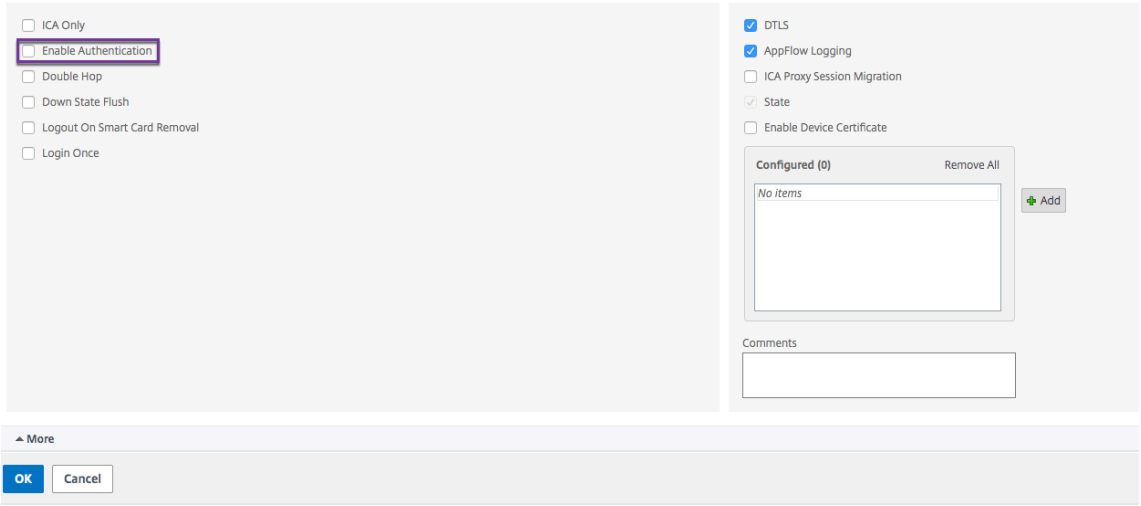
5. ［**OK**］をクリックします。

GUI を使用して **Citrix Gateway** プロキシ上の仮想サーバーの認証を無効にするには

1. ［構成］**> Citrix Gateway >** ［仮想サーバー］に移動します。
2. 仮想サーバを選択し、[**Edit**] をクリックします。
3. [基本設定**]** セクションで、[編集] アイコンをクリックし、[その他] をクリックします。



4. [認証を有効にする] チェックボックスをオフにします。



5. ［**OK**］をクリックします。

アプライアンスのプロキシと通信するためのアプライアンスの設定

March 26, 2020

ダブルホップ DMZ で Citrix Gateway を展開する場合、最初の DMZ で Citrix Gateway を構成して、2 番目の DMZ の Citrix Gateway プロキシと通信する必要があります。

2 台目の DMZ に複数のアプライアンスを展開する場合は、1 台目の DMZ 内の各アプライアンスを構成して、2 台目の DMZ 内のすべてのプロキシアプライアンスと通信します。

注: IPv6 を使用する場合は、構成ユーティリティを使用してネクストホップサーバーを構成します。これを行うには、［Citrix Gateway］>［リソース］を展開し、

[ネクストホップサーバー] をクリックします。次の手順に従い、[
IPv6] チェックボックスをオンにします。

Citrix Gateway プロキシと通信するように Citrix Gateway を構成するには

1. 構成ユーティリティの [構成] タブで、[Citrix Gateway] > [リソース] を展開し、[ネクストホップサーバー] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前] に、最初の Citrix Gateway の名前を入力します。
4. [IP アドレス] に、2 番目の DMZ の Citrix Gateway プロキシの仮想サーバーの IP アドレスを入力します。
5. [ポート] にポート番号を入力し、[作成]、[閉じる] の順にクリックします。443 などのセキュアポートを使用している場合は、[Secure] を選択します。

最初の DMZ にインストールされた各 Citrix Gateway は、2 番目の DMZ にインストールされているすべての Citrix Gateway プロキシアプライアンスと通信するように構成する必要があります。

Citrix Gateway プロキシの設定を構成したら、ポリシーを Citrix Gateway グローバルまたは仮想サーバーにバインドします。

Citrix Gateway ネクストホップサーバーをグローバルにバインドするには

1. 構成ユーティリティの [構成] タブで、[Citrix Gateway] > [リソース] を展開し、[ネクストホップサーバー] をクリックします。
2. 詳細ペインでネクストホップサーバーを選択し、[操作] で [グローバルバインディング] を選択します。
3. [ネクストホップサーバのグローバルバインドの構成] ダイアログボックスの [ネクストホップサーバ名] でプロキシアプライアンスを選択し、[OK] をクリックします。

Citrix Gateway のネクストホップサーバーを仮想サーバーにバインドするには

1. 構成ユーティリティの [構成] タブで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、仮想サーバーを選択し、[開く] をクリックします。
3. [公開アプリケーション] タブの [ネクストホップサーバー] で、項目をクリックし、[OK] をクリックします。

[公開アプリケーション] タブからネクストホップサーバーを追加することもできます。

STA トラフィックと ICA トラフィックを処理するように Citrix Gateway を構成する

March 26, 2020

ダブルホップ DMZ で Citrix Gateway を展開する場合、最初の DMZ で Citrix Gateway を構成して、Secure Ticket Authority（STA）および ICA トラフィックとの通信を適切に処理する必要があります。STA を実行しているサーバは、グローバルにバインドすることも、仮想サーバにバインドすることもできます。

STA を構成したら、STA をグローバルにバインドすることも、仮想サーバにバインドすることもできます。

STA をグローバルに構成およびバインドするには、次の手順を実行します。

1. 構成ユーティリティの [構成] タブで、[Citrix Gateway] を展開し、[グローバル設定] をクリックします。
2. 詳細ペインの [サーバー] で、[Secure Ticket Authority が使用する STA サーバーのバインド/バインド解除] をクリックします。
3. [STA サーバのバインド/バインド解除] ダイアログ・ボックスで、[追加] をクリックします。
4. [STA サーバーの構成] ダイアログボックスの [URL] に、STA を実行するサーバーのパス (http://mycompany.comまたはhttp://ipAddressなど) を入力し、[作成] をクリックします。

STA を構成して仮想サーバにバインドするには、次の手順で行います。

1. 構成ユーティリティの [構成] タブで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、仮想サーバーを選択し、[開く] をクリックします。
3. [公開アプリケーション] タブの [Secure Ticket Authority] で、[追加] をクリックします。
4. [STA サーバーの構成] ダイアログボックスの [URL] に、STA を実行するサーバーのパス (http://mycompany.comまたはhttp://ipAddressなど) を入力し、[作成] をクリックします。

ファイアウォールで適切なポートを開く

March 26, 2020

ダブルホップ DMZ 展開に関連するさまざまなコンポーネント間で発生するさまざまな接続をサポートするために、ファイアウォールで適切なポートが開いていることを確認する必要があります。接続処理の詳細については、「ダブルホップ DMZ 配置における通信フロー」を参照してください。

次の図は、ダブルホップ DMZ 配置で使用できる一般的なポートを示しています。

次の表に、最初のファイアウォールを介して発生する接続と、接続をサポートするために開く必要があるポートを示します。

最初のファイアウォールを介した接続	使用するポート
インターネットからの Web ブラウザは、最初の DMZ で Citrix Gateway に接続します。注： Citrix Gateway には、ポート 80 で行われた接続をセキュアなポートにリダイレクトするオプションがあります。Citrix Gateway でこのオプションを有効にすると、最初のファイアウォールからポート 80 を開くことができます。ユーザーがポート 80 で Citrix Gateway に暗号化されていない接続を行うと、Citrix Gateway は自動的に安全なポートにリダイレクトされます。	最初のファイアウォールを介して TCP ポート 443 を開きます。
インターネットからの Citrix Workspace アプリは、最初の DMZ で Citrix Gateway に接続します.	最初のファイアウォールを介して TCP ポート 443 を開きます。

次の表に、2 番目のファイアウォールを介して発生する接続と、接続をサポートするために開く必要があるポートを示します。

2 番目のファイアウォールを介した接続	使用するポート
最初の DMZ の Citrix Gateway は、2 番目の DMZ の Web Interface に接続します.	セキュリティで保護されていない接続の場合は TCP ポート 80、2 番目のファイアウォールを経由してセキュリティで保護された接続の場合は TCP ポート 443 のいずれかを開きます。
最初の DMZ の Citrix Gateway は、2 番目の DMZ の Citrix Gateway に接続します.	TCP ポート 443 を開いて、2 番目のファイアウォールを介したセキュアな SOCKS 接続を確立します。
最初の DMZ で Citrix Gateway で認証を有効にした場合、このアプライアンスは内部ネットワークの認証サーバーに接続する必要があります。	認証サーバが接続をリッスンする TCP ポートを開きます。たとえば、RADIUS 用のポート 1812、LDAP 用のポート 389 などがあります。

次の表に、3 番目のファイアウォールを介して発生する接続と、接続をサポートするために開く必要があるポートを示します。

3 番目のファイアウォールを介した接続	使用するポート
StoreFront または 2 番目の DMZ の Web Interface は、内部ネットワークのサーバーでホストされている XML サービスに接続します。	セキュリティで保護されていない接続の場合はポート 80、3 番目のファイアウォールを介した安全な接続の場合はポート 443 のいずれかを開きます。

3 番目のファイアウォールを介した接続	使用するポート
StoreFront または 2 番目の DMZ の Web Interface は、内部ネットワークのサーバーでホストされている Secure Ticket Authority（STA）に接続します。	セキュリティで保護されていない接続の場合はポート 80、3 番目のファイアウォールを介した安全な接続の場合はポート 443 のいずれかを開きます。
2 つ目の DMZ の Citrix Gateway は、安全なネットワーク内に存在する STA に接続します。	セキュリティで保護されていない接続の場合はポート 80、3 番目のファイアウォールを介した安全な接続の場合はポート 443 のいずれかを開きます。
2 番目の DMZ の Citrix Gateway は、内部ネットワーク上のサーバー上の公開アプリケーションまたは仮想デスクトップに ICA 接続を行います。	TCP ポート 1494 を開き、3 番目のファイアウォールを介した ICA 接続をサポートします。Citrix Virtual Apps セッション画面の保持を有効にした場合は、1494 ではなく TCP ポート 2598 を開きます。
最初の DMZ で Citrix Gateway で認証を有効にした場合、このアプライアンスは内部ネットワークの認証サーバーに接続する必要があります。	認証サーバが接続をリッスンする TCP ポートを開きます。たとえば、RADIUS 用のポート 1812、LDAP 用のポート 389 などがあります。

ダブルホップ **DMZ** 配置での **SSL** 証明書の管理

March 26, 2020

ダブルホップ DMZ 展開では、コンポーネント間の接続を暗号化するために必要な SSL 証明書をインストールする必要があります。

ダブルホップ DMZ 配置では、配置に関係するさまざまなコンポーネント間でいくつかの異なるタイプの接続が発生します。これらの接続には、エンドツーエンドの SSL 暗号化はありません。ただし、各接続は個別に暗号化できます。

接続を暗号化するには、接続に関係するコンポーネントに適切な SSL 証明書 (信頼されたルートまたはサーバー証明書) をインストールする必要があります。

次の表に、最初のファイアウォールを介して発生する接続と、これらの各接続の暗号化に必要な SSL 証明書を示します。インターネット経由で送信されるトラフィックを保護するには、最初のファイアウォールを介した接続を暗号化する必要があります。

最初のファイアウォールを介した接続	暗号化に必要な証明書
インターネットからの Web ブラウザは、最初の DMZ で Citrix Gateway に接続します。	最初の DMZ の Citrix Gateway には、SSL サーバー証明書がインストールされている必要があります。Web ブラウザーには、Citrix Gateway のサーバー証明書と同じ認証局（CA）によって署名されたルート証明書がインストールされている必要があります。
インターネットからの Citrix Workspace アプリは、最初の DMZ で Citrix Gateway に接続します.	この接続の証明書管理は、Web ブラウザーから Citrix Gateway への接続と同じです。Web ブラウザ接続を暗号化するために証明書をインストールした場合、この接続もこれらの証明書を使用して暗号化されます。

次の表に、2 番目のファイアウォールを介して発生する接続と、これらの各接続の暗号化に必要な SSL 証明書を示します。これらの接続を暗号化するとセキュリティが強化されますが、必須ではありません。

2 番目のファイアウォールを介した接続	暗号化に必要な証明書
最初の DMZ の Citrix Gateway は、2 番目の DMZ の Web Interface に接続します.	StoreFront または Web Interface に SSL サーバー証明書がインストールされている必要があります。最初の DMZ の Citrix Gateway には、Web Interface 上のサーバー証明書と同じ CA によって署名されたルート証明書がインストールされている必要があります。
最初の DMZ の Citrix Gateway は、2 番目の DMZ の Citrix Gateway に接続します.	2 つ目の DMZ の Citrix Gateway には、SSL サーバー証明書がインストールされている必要があります。最初の DMZ の Citrix Gateway には、2 番目の DMZ の Citrix Gateway 上のサーバー証明書と同じ CA によって署名されたルート証明書がインストールされている必要があります。

次の表に、3 番目のファイアウォールを介して発生する接続と、これらの各接続の暗号化に必要な SSL 証明書を示します。これらの接続を暗号化するとセキュリティが強化されますが、必須ではありません。

3 番目のファイアウォールを介した接続	暗号化に必要な証明書
StoreFront または 2 番目の DMZ の Web Interface は、内部ネットワークのサーバーでホストされている XML サービスに接続します。	Citrix Virtual Apps サーバー上の Microsoft インターネットインフォメーションサービス（IIS）サーバー上で XML サービスを実行する場合は、IIS サーバーに SSL サーバー証明書をインストールする必要があります。XML サービスが標準の Windows サービス (IIS に存在しない) である場合は、SSL サーバー証明書をサーバーの SSL リレー内にインストールする必要があります。StoreFront または Web Interface には、Microsoft IIS サーバーまたは SSL リレーにインストールされたサーバー証明書と同じ CA によって署名されたルート証明書がインストールされている必要があります。
StoreFront または 2 番目の DMZ の Web Interface は、内部ネットワークのサーバーでホストされている STA に接続します。	この接続の証明書管理は、Web Interface から XML サービスへの接続と同じです。同じ証明書を使用して、この接続を暗号化できます。(サーバー証明書は、Microsoft IIS サーバーまたは SSL リレーのいずれかに存在する必要があります。対応するルート証明書は、Web Interface にインストールする必要があります)。
2 番目の DMZ の Citrix Gateway は、内部ネットワークのサーバーでホストされている STA に接続します。	この接続での STA の SSL サーバー証明書の管理は、この表で説明した 2 つの接続で説明したものと同じです。(サーバー証明書は、Microsoft IIS サーバーまたは SSL リレーのいずれかに存在する必要があります)。2 番目の DMZ の Citrix Gateway には、STA および XML サービスで使用されるサーバー証明書と同じ CA によって署名されたルート証明書がインストールされている必要があります。
2 番目の DMZ の Citrix Gateway は、内部ネットワーク上のサーバー上の公開アプリケーションへの ICA 接続を行います.	SSL サーバー証明書は、公開アプリケーションをホストするサーバー上の SSL リレー内にインストールする必要があります。2 番目の DMZ の Citrix Gateway プロキシには、SSL リレー内にインストールされたサーバー証明書と同じ CA によって署名されたルート証明書がインストールされている必要があります。

高可用性の使用

March 26, 2020

2 つの Citrix Gateway アプライアンスの高可用性を展開すると、どのトランザクションでも中断のない操作を実現できます。一方のアプライアンスをプライマリノードとして設定し、もう一方のアプライアンスをセカンダリノードとして設定すると、プライマリノードは接続を受け入れ、サーバを管理し、セカンダリノードはプライマリノードを監視します。何らかの理由でプライマリノードが接続を受け付けることができなくなると、セカンダリノードが処理を引き継ぎます。

セカンダリノードは、定期的なメッセージ（ハートビートメッセージまたはヘルスチェックとも呼ばれる）を送信してプライマリを監視し、プライマリノードが接続を受け付けているかどうかを判断します。ヘルスチェックが失敗した場合、セカンダリノードは指定された期間接続を再試行します。その後、プライマリノードが正常に機能していないと判断されます。次に、セカンダリ・ノードがプライマリ・ノードを引き継ぎます（フェイルオーバーと呼ばれるプロセス）。

フェイルオーバー後、すべてのクライアントが管理対象サーバーへの接続を再確立する必要がありますが、セッション永続性ルールはフェイルオーバー前と同じように維持されます。

Web サーバーのロギングの永続性を有効にすると、フェールオーバーによってログデータが失われることはありません。ロギングの永続性を有効にするには、ログサーバー設定が log.conf ファイルに両方のシステムのエントリを保持する必要があります。

次の図は、高可用性ペアを使用したネットワーク構成を示しています。

図 1：高可用性構成での Citrix Gateway アプライアンス

高可用性を設定する基本的な手順は次のとおりです。

1. 両方のノードが同じサブネットにある基本設定を作成します。
2. ノードがヘルスチェック情報を通信する間隔をカスタマイズします。
3. ノードが同期を維持するプロセスをカスタマイズします。
4. プライマリからセカンダリへのコマンドの伝播をカスタマイズします。
5. オプションで、フェイルセーフモードを設定して、どちらのノードもプライマリでない状況を回避します。
6. Citrix Gateway の無償 ARP メッセージを受け付けないデバイスが環境に含まれている場合は、仮想 MAC アドレスを構成します。

より複雑な構成の準備ができたら、異なるサブネットで高可用性ノードを構成できます。

高可用性セットアップの信頼性を向上させるために、ルートモニタを設定し、冗長リンクを作成できます。トラブルシューティングやメンテナンスタスクの実行など、状況によっては、ノードを強制的にフェイルオーバーする（プライマリステータスを他のノードに割り当てる）場合や、セカンダリノードを強制的にセカンダリにしたり、プライマリノードをプライマリにしたりしたい場合があります。

高可用性の仕組み

April 9, 2020

高可用性ペアで Citrix Gateway を構成すると、セカンダリ Citrix Gateway は定期的なメッセージ（ハートビートメッセージまたはヘルスチェックとも呼ばれる）を送信して最初のアプライアンスを監視し、最初のアプライアンスが接続を受け付けているかどうかを判断します。ヘルスチェックが失敗した場合、セカンダリ Citrix Gateway は、プライマリアプライアンスが動作していないと判断するまで、指定した時間だけ接続を再試行します。セカンダリアプライアンスがヘルスチェックの失敗を確認すると、セカンダリ Citrix Gateway がプライマリ Citrix Gateway を引き継ぎます。これをフェールオーバーと呼びます。

Citrix Gateway アプライアンス間で高可用性に関連する情報を交換するには、以下のポートを使用します。

- UDP ポート 3003 は、hello パケットを交換してインターバルのステータスを通信するために使用されます。
- TCP ポート 3010 は、高可用性設定の同期化に使用されます。
- 構成設定の同期には、TCP ポート 3011 が使用されます。

高可用性の設定に関するガイドライン

高可用性ペアを設定する前に、次の注意事項を確認してください。

- 各 Citrix Gateway アプライアンスは、同じバージョンの Citrix Gateway ソフトウェアを実行している必要があります。バージョン番号は、構成ユーティリティのページ上部にあります。
- Citrix Gateway では、2 つのアプライアンス間でパスワードが自動的に同期されることはありません。ペア内の他のアプライアンスのユーザー名とパスワードを使用して、各 Citrix Gateway を構成できます。
- プライマリとセカンダリの両方の Citrix Gateway で構成ファイル ns.conf のエントリが一致している必要があります。ただし、次の例外があります。
  - プライマリおよびセカンダリ Citrix Gateway アプライアンスは、それぞれ固有のシステム IP アドレスを使用して構成する必要があります。セットアップウィザードを使用して、いずれかの Citrix Gateway でシステム IP アドレスを構成または変更します。
  - 高可用性ペアでは、Citrix Gateway ID と関連する IP アドレスが他の Citrix Gateway を指している必要があります。
    たとえば、AG1 と AG2 という 2 つのアプライアンスがある場合、AG1 を一意の Citrix Gateway ID と IP アドレスの AG2 を使用して AG1 を構成する必要があります。AG2 は、一意の Citrix Gateway ID と AG1 の IP アドレスで構成する必要があります。
    注：各 Citrix Gateway アプライアンスは常にノード 0 として識別されます。各アプライアンスに一意のノード ID を設定します。
- 高可用性ペアの各アプライアンスには、同じライセンスが必要です。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。
- 構成ユーティリティまたはコマンドラインインターフェイスを直接使用しない方法 (たとえば、SSL 証明書のインポート、スタートアップスクリプトへの変更) を使用して、いずれかのノードで構成ファイルを作成する場合は、構成ファイルを他のノードにコピーするか、同一のファイルを作成します。

- 高可用性ペアを設定する場合は、プライマリアプライアンスとセカンダリアプライアンスのマッピングされた IP アドレスとデフォルト Gateway アドレスが同一であることを確認します。必要に応じて、セットアップウィザードを実行して、マッピングされた IP アドレスをいつでも変更できます。

インストール前のチェックリストを使用して、高可用性展開で構成する必要がある特定の設定の一覧を表示できます。詳細については、「インストール前のチェックリスト」を参照してください。

高可用性の設定

March 26, 2020

高可用性構成をセットアップするには、2 つのノードを作成します。各ノードで、もう一方の Citrix Gateway IP アドレスがリモートノードとして定義されます。まず、高可用性を構成する 2 つの Citrix ADC アプライアンスのいずれかにログオンし、ノードを追加します。別のアプライアンスの Citrix Gateway IP アドレスを新しいノードのアドレスとして指定します。次に、もう一方のアプライアンスにログオンし、最初のアプライアンスの Citrix Gateway IP アドレスを持つノードを追加します。アルゴリズムは、どのノードがプライマリになり、どのノードがセカンダリになるかを決定します。

アプライアンスを構成する前に、高可用性ノードを追加します。このノードは、高可用性ペアの 1 つ目または 2 つ目の Citrix Gateway を表します。高可用性を構成するには、まずノードを作成し、次に高可用性設定を構成します。

高可用性ノードを追加するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. 詳細ウィンドウの [ノード] タブで、[追加] をクリックします。
3. ［高可用性セットアップ］ダイアログボックスの［高可用性セットアップ］ダイアログボックスの［リモートノードの IP アドレス］テキストボックスに、リモートノードとして追加する Citrix ADC NSIP アドレスを入力します。Citrix Gateway の IP アドレスが IPv6 アドレスの場合は、アドレスを入力する前に IPv6 チェックボックスをオンにします。
4. ローカルノードをリモートノードに自動的に追加する場合は、[リモートシステムを構成して高可用性セットアップに参加する] を選択します。このオプションを選択しない場合は、リモートノードで表されるアプライアンスにログインし、現在構成しているノードを追加する必要があります。
5. クリックすると、ダウンしているインターフェイスまたはチャネルの HA モニタをオフにするが有効になります。
6. リモートアプライアンスのユーザー名とパスワードが異なる場合は、[リモートシステムログオンクレデンシャル] で、[リモートシステムのログインクレデンシャルがセルフノードとは異なる] をクリックします。
7. [ユーザー名] に、リモートアプライアンスのユーザー名を入力します。
8. [パスワード] に、リモートアプライアンスのパスワードを入力します。
9. ［OK］をクリックします。

セカンダリノードを有効または無効にするには

セカンダリノードのみを有効または無効にできます。セカンダリノードを無効にすると、プライマリノードへのハートビートメッセージの送信が停止されるため、プライマリノードはセカンダリノードのステータスを確認できなくなります。ノードを有効にすると、ノードは高可用性構成に参加します。

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. 詳細ペインの [ノード] タブで、ローカルノードを選択し、[開く] をクリックします。
3. [HA ノードの構成] ダイアログボックスの [高可用性ステータス] で、[ENABLED (HA に参加しない)] を選択します。
4. [OK] をクリックします。ステータスバーに、ノードが正常に構成されたことを示すメッセージが表示されます。

高可用性の設定を構成するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. 詳細ペインの [ノード] タブでノードを選択し、[編集] をクリックします。
3. [HA ノードの構成] ダイアログボックスの [ID] に、ノード識別子の番号を入力します。ID は、他のアプライアンスの一意のノード番号を指定します。
4. [IP アドレス] にシステムの IP アドレスを入力し、[OK] をクリックします。IP アドレスは、他のアプライアンスの IP アドレスを指定します。

注: 高可用性ペアのノードの最大 ID は 64 です。

RPC ノードのパスワードの変更

March 26, 2020

他の Citrix Gateway アプライアンスと通信するには、各アプライアンスに Citrix Gateway での認証方法など、他のアプライアンスに関する知識が必要です。RPC ノードは、構成およびセッション情報のシステム間通信に使用される内部システムエンティティです。各 Citrix Gateway に 1 つの RPC ノードが存在し、他の Citrix Gateway アプライアンスの IP アドレスや認証に使用されるパスワードなどの情報が格納されます。別の Citrix Gateway と通信する Citrix Gateway は、RPC ノード内のパスワードをチェックします。

Citrix Gateway では、高可用性ペアの両方のアプライアンスで RPC ノードパスワードが必要です。最初に、各 Citrix Gateway は同じ RPC ノードパスワードを使用して構成されます。セキュリティを強化するには、既定の RPC ノードパスワードを変更する必要があります。構成ユーティリティを使用して、RPC ノードを構成および変更できます。

RPC ノードは、ノードの追加またはグローバルサーバー負荷分散 (GSLB) サイトの追加時に暗黙的に作成されます。RPC ノードを手動で作成または削除することはできません。

重要：アプライアンス間のネットワーク接続もセキュリティで保護する必要があります。RPC ノードのパスワードを設定するときに、[セキュリティ で保護する] チェックボックスをオンにすると、セキュリティを構成できます。

RPC ノードのパスワードを変更し、セキュリティで保護された接続を有効にするには

1. [システム] > [ネットワーク] > [RPC] に移動します。
2. 詳細ペインでノードを選択し、[編集] をクリックします。
3. [パスワード] と [パスワードの確認] に、新しいパスワードを入力します。
4. [送信元 IP アドレス］に、他の Citrix Gateway アプライアンスのシステム IP アドレスを入力します。
5. [セキュリティで保護する] をクリックし、[OK] をクリックします。

> 注：「セキュア」オプションを有効にすると、アプライアンスはノードから他の RPC ノードに送信されたすべての通信を暗号化し、RPC 通信を保護します。

CLI を使用して RPC ノードのパスワードを変更するには

コマンドプロンプトで、次のように入力します。

```
set ns rpcNode <IPAddress> {
 -password }
  [-secure ( YES | NO )]

show ns rpcNode
<!--NeedCopy-->
```

例：

```
> set ns rpcNode 192.0.2.4 -password mypassword -secure YES
 Done
> show rpcNode
.
.
.
 IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
     SrcIP:  *           Secure:  ON
Done
>
<!--NeedCopy-->
```


プライマリアプライアンスとセカンダリアプライアンスの高可用性の構成

March 26, 2020

RPC ノードのパスワードを変更し、セキュアな通信を有効にしたら、構成ユーティリティを使用して、プライマリおよびセカンダリ Citrix Gateway の高可用性ノードを構成します。

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. 詳細ペインの [ノード] タブでノードを選択し、[編集] をクリックします。
3. [高可用性ステータス] で、[有効 (HA にアクティブに参加する)] をクリックし、[OK] をクリックします。

通信間隔の構成

March 26, 2020

Citrix Gateway を高可用性ペアとして構成する場合、セカンダリ Citrix Gateway がミリ秒（ミリ秒）単位でリッスンするように構成できます。これらの間隔は、hello 間隔およびデッドインターバルと呼ばれます。

hello 間隔は、ハートビートメッセージがピアノードに送信される間隔です。デッドインターバルは、ハートビートパケットが受信されなかった場合に、ピアノードが DOWN とマークされるまでの時間間隔です。ハートビートメッセージは、高可用性ペアの他のノードのポート 3003 に送信される UDP パケットです。

hello インターバルを設定する場合は、200 ～1000 の値を使用できます。デフォルト値は 200 です。デッドインターバル値は 3 ～60 です。デフォルト値は 3 です。

> 注
>
> デッドインターバルは、hello インターバルの倍数として設定する必要があります。

セカンダリ **Citrix Gateway** の通信間隔を構成するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. 詳細ペインの [ノード] タブでノードを選択し、[編集] をクリックします。
3. [間隔] で、次のいずれかまたは両方を実行します。
   - [ハロー間隔 (ミリ秒)] に値を入力し、[OK] をクリックします。デフォルトは 200 ミリ秒です。
   - [デッド間隔 (秒)] に値を入力し、[OK] をクリックします。デフォルト設定は 3 秒です。

Citrix Gateway アプライアンスの同期

March 26, 2020

高可用性ペアでの Citrix Gateway アプライアンスの自動同期は、デフォルトで有効になっています。自動同期を使用すると、1 つのアプライアンスを変更して、その変更を 2 番目のアプライアンスに自動的に反映させることができます。同期ではポート 3010 が使用されます。

同期は、次の場合に開始されます。

- セカンダリノードが再起動します。
- プライマリノードは、フェールオーバー後にセカンダリになります。

同期を無効にすると、プライマリアプライアンスで変更が発生したときに、セカンダリ Citrix Gateway ateway がプライマリ Citrix Gateway と構成を同期できなくなります。同期を強制することもできます。

ペアのセカンダリノードで高可用性同期を有効または無効にします。

高可用性同期を有効または無効にするには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. 詳細ペインの [ノード] タブでノードを選択し、[編集] をクリックします。
3. [ノードの構成] ダイアログボックスの [HA 同期] で、次のいずれかの操作を行います。
   - 同期を無効にするには、[セカンダリノードがプライマリから構成をフェッチする] チェックボックスをオフにします。
   - 同期を有効にするには、[セカンダリノードがプライマリから構成をフェッチする] チェックボックスをオンにします。
4. ［OK］をクリックします。ノード構成が成功したことを示すメッセージがステータスバーに表示されます。

アプライアンス間で強制的に同期するには

Citrix Gateway では、自動同期に加えて、高可用性ペアの 2 つのノード間の強制同期もサポートされています。

プライマリおよびセカンダリ Citrix Gateway アプライアンスの両方で同期を強制できます。ただし、同期がすでに進行中の場合、コマンドは失敗し、Citrix Gateway に警告が表示されます。強制同期は、次の状況でも失敗します。

- スタンドアロンシステム上で同期を強制します。
- セカンダリノードは無効です。
- セカンダリノードで高可用性の同期を無効にします。

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. [ノード] タブで、[同期の強制] をクリックします。

高可用性セットアップでの構成ファイルの同期

March 26, 2020

高可用性セットアップでは、プライマリノードからセカンダリノードにさまざまな構成ファイルを同期できます。

高可用性セットアップでファイルを同期するためのパラメータ

- モード

実行する同期のタイプ。次の説明には、オプションを指定するコマンドライン引数がカッコ内に含まれます。
- ライセンスと **rc.conf (all)** を除くすべて。システム構成、Citrix Gateway ブックマーク、SSL 証明書、SSL CRL リスト、HTML インジェクションスクリプト、アプリケーションファイアウォールの XML オブジェクトに関連するファイルを同期します。
- ブックマーク (ブックマーク)。すべての Citrix Gateway のブックマークを同期します。
- **SSL** 証明書とキー (ssl)。SSL 機能のすべての証明書、キー、および CRL を同期します。
- ライセンスと **rc.conf** (その他)。すべてのライセンスファイルと rc.conf ファイルを同期します。
- ライセンスと **rc.conf (**その他のオプション**)** を含むすべてのもの。システム構成、Citrix Gateway ブックマーク、SSL 証明書、SSL CRL リスト、HTML インジェクションスクリプト、アプリケーションファイアウォール XML オブジェクト、ライセンス、および rc.conf ファイルに関連するファイルを同期します。

注：アプライアンスに Citrix ADC ライセンスをインストールする場合は、さらに多くのオプションを使用できます。

構成ユーティリティを使用して高可用性セットアップのファイルを同期するには

1. ナビゲーションウィンドウで、[システム] を展開し、[診断] をクリックします。
2. 詳細ペインの [ユーティリティ] で、[HA ファイルの同期の開始] をクリックします。
3. [ファイル同期の開始] ダイアログボックスの [モード] ドロップダウンリストで、適切な同期の種類 ([ライセンス以外のすべて] や [rc.conf] など) を選択し、[OK] をクリックします。

コマンド伝播の設定

March 26, 2020

高可用性セットアップでは、プライマリノードで発行されたコマンドは、プライマリノードでコマンドが実行される前に、セカンダリノードに対して自動的に伝達され、実行されます。コマンドの伝播が失敗した場合、またはセカンダリノードでコマンドの実行が失敗した場合、プライマリノードはコマンドを実行し、エラーをログに記録します。コマンド伝播では、ポート 3011 が使用されます。

高可用性ペア構成では、プライマリノードとセカンダリノードの両方でコマンドの伝播がデフォルトで有効になっています。高可用性ペアのいずれかのノードで、コマンド伝播を有効または無効にできます。1 次ノードでコマンド伝

達を無効にすると、コマンドは二次ノードに伝達されません。セカンダリノードでコマンドの伝播を無効にすると、プライマリノードから伝播されたコマンドはセカンダリノードで実行されません。

注意: 伝播を再度有効化した後は、必ず同期化を強制してください。

注意: 伝播を無効にしている間に同期が発生した場合、伝播を無効にする前に行った構成関連の変更は、セカンダリ・ノードと同期されます。これは、同期の進行中に伝播が無効になっている場合にも当てはまります。

プライマリ・ノードで伝播を有効または無効にするには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. 詳細ペインの [ノード] タブでノードを選択し、[編集] をクリックします。
3. [HA 伝播] で、次のいずれかを実行します。
   - 高可用性の伝播を無効にするには、[プライマリノードが構成をセカンダリに伝達する] チェックボックスをオフにします。
   - 高可用性の伝播を有効にするには、[プライマリノードが構成をセカンダリに伝達する] チェックボックスをオンにします。
4. [OK] をクリックします。

コマンド伝播のトラブルシューティング

March 26, 2020

次に、コマンドの伝播が失敗する理由と、設定を復元するための解決策を説明します。

- ネットワーク接続がアクティブではありません。コマンドの伝播が失敗した場合は、プライマリとセカンダリ Citrix Gateway アプライアンスの間のネットワーク接続を確認します。
- セカンダリ Citrix Gateway にリソースがありません。プライマリ Citrix Gateway でコマンドの実行が成功しても、セカンダリ Citrix Gateway に伝播できない場合は、セカンダリ Citrix Gateway でコマンドを直接実行して、エラーメッセージを確認します。コマンドに必要なリソースがプライマリ Citrix Gateway に存在し、セカンダリ Citrix Gateway では使用できないために、エラーが発生した可能性があります。また、各アプライアンスのライセンスファイルが一致することを確認します。

  たとえば、すべての SSL（セキュア・ソケット・レイヤー）証明書が各 Citrix Gateway に存在することを確認します。初期化スクリプトのカスタマイズが両方の Citrix Gateway アプライアンスに存在することを確認します。
- 認証エラー。認証失敗のエラーメッセージが表示された場合は、各アプライアンスの RPC ノード設定を確認します。

フェールセーフモードの設定

March 26, 2020

高可用性構成では、フェイルセーフモードでは、両方のノードがヘルスチェックに不合格になったときに 1 つのノードが常にプライマリになります。フェイルセーフモードでは、ノードが部分的にしか使用できない場合に、バックアップメソッドをアクティブ化してトラフィックを処理できます。

高可用性フェイルセーフモードは、ノードごとに個別に構成します。

次の表は、フェイルセーフのケースの一部を示しています。NOT_UP 状態は、ノードがヘルスチェックに失敗したが、ノードが部分的に利用可能であることを意味します。UP 状態は、ノードがヘルスチェックに合格したことを意味します。

表 1. フェールセーフモードの場合

ノード A（プライマリ）のヘルス状態	ノード B（セカンダリ）のヘルス状態	デフォルトの高可用性動作	フェールセーフが有効な高可用性の動作	説明
NOT_UP (最後に失敗しました)	NOT_UP (最初に失敗しました)	A（セカンダリ）、B（セカンダリ）	A（プライマリ）、B（セカンダリ）	両方のノードが次々と故障した場合、最後のプライマリノードであったノードはプライマリのままです。
NOT_UP (最初に失敗しました)	NOT_UP (最後に失敗しました)	A（セカンダリ）、B（セカンダリ）	A（セカンダリ）、B（プライマリ）	両方のノードが次々と故障した場合、最後のプライマリノードであったノードはプライマリのままです。
UP	UP	A（プライマリ）、B（セカンダリ）	A（プライマリ）、B（セカンダリ）	両方のノードがヘルスチェックに合格した場合、フェイルセーフを有効にした場合の動作は変更されません。

ノード A（プライマリ）のヘルス状態	ノード B（セカンダリ）のヘルス状態	デフォルトの高可用性動作	フェールセーフが有効な高可用性の動作	説明
UP	NOT_UP	A（プライマリ）、B（セカンダリ）	A（プライマリ）、B（セカンダリ）	セカンダリノードのみで障害が発生した場合、フェイルセーフを有効にした場合の動作は変更されません。
NOT_UP	UP	A（セカンダリ）、B（プライマリ）	A（セカンダリ）、B（プライマリ）	プライマリだけが故障した場合、フェイルセーフを有効にした場合の動作は変更されません。
NOT_UP	UP (STAYSECONDARY)	A（セカンダリ）、B（セカンダリ）	A（プライマリ）、B（セカンダリ）	セカンダリが STAYSECONDARY として設定されている場合、プライマリは、障害が発生してもプライマリのままです。

フェールセーフモードを構成するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. 詳細ペインの [ノード] タブでノードを選択し、[編集] をクリックします。
3. [ノードの構成] ダイアログボックスの [フェイルセーフモード] で、[両方のノードが正常でない場合でも 1 つのプライマリノードを保持] を選択し、[OK] をクリックします。

仮想 **MAC** アドレスの設定

March 26, 2020

仮想 MAC アドレスは、高可用性セットアップでプライマリおよびセカンダリ Citrix Gateway アプライアンスによって共有されます。

高可用性設定では、プライマリ Citrix Gateway は、マッピングされた IP アドレスや仮想 IP アドレスなど、すべて

のフローティング IP アドレスを所有します。この IP アドレスに対するアドレス解決プロトコル (ARP) 要求に対して、独自の MAC アドレスで応答します。その結果、外部デバイス（ルーターなど）の ARP テーブルが、フローティング IP アドレスとプライマリ Citrix Gateway MAC アドレスで更新されます。フェイルオーバーが発生すると、セカンダリ Citrix Gateway が新しいプライマリ Citrix Gateway として引き継がれます。次に、無償アドレス解決プロトコル（GARP）を使用して、プライマリアプライアンスから取得したフローティング IP アドレスをアドバタイズします。新しいプライマリアプライアンスがアドバタイズする MAC アドレスは、自身のインターフェイスの MAC アドレスです。

一部のデバイスは、Citrix Gateway によって生成された GARP メッセージを受け付けません。その結果、一部の外部デバイスは、古いプライマリ Citrix Gateway によってアドバタイズされた古い IP/MAC マッピングを保持します。この状況により、サイトが使用できなくなる可能性があります。この問題を解決するには、高可用性ペアの両方の Citrix Gateway アプライアンスで仮想 MAC アドレスを構成します。この構成は、両方の Citrix Gateway アプライアンスの MAC アドレスが同じであることを意味します。その結果、フェイルオーバーが発生しても、セカンダリ Citrix Gateway の MAC アドレスは変更されず、外部デバイス上の ARP テーブルを更新する必要はありません。

仮想 MAC アドレスを作成するには、仮想ルータ ID（ID）を作成し、インターフェイスにバインドします。高可用性設定では、ユーザーは両方のアプライアンスのインターフェイスに ID をバインドする必要があります。

仮想ルータ ID がインターフェイスにバインドされると、システムは仮想ルータ ID を最後のオクテットとする仮想 MAC アドレスを生成します。一般的な仮想 MAC アドレスの例は、00:00:5 e: 00:01: <VRID> です。たとえば、値 60 の仮想ルータ ID を作成してインターフェイスにバインドした場合、結果の仮想 MAC アドレスは 00:00:5 e: 00:01:3 c になります。ここで、3c は仮想ルータ ID の 16 進表現です。1 ～254 の範囲の 255 の仮想ルータ ID を作成できます。

IPv4 および IPv6 の仮想 MAC アドレスを設定できます。

IPv4 仮想 MAC アドレスの設定

March 26, 2020

IPv4 仮想 MAC アドレスを作成してインターフェイスにバインドすると、インターフェイスから送信されるすべての IPv4 パケットは、インターフェイスにバインドされた仮想 MAC アドレスを使用します。インターフェイスにバインドされた IPv4 仮想 MAC アドレスがない場合は、インターフェイスの物理 MAC アドレスが使用されます。

汎用仮想 MAC アドレスの形式は 00:00:5 e: 00:01: <VRID> です。たとえば、値 60 の VRID を作成してインターフェイスにバインドすると、その仮想 MAC アドレスは 00:00:5 e: 00:01:3 c になります。3c は VRID の 16 進表現です。1 ～255 の値で 255 個の VRID を作成できます。

IPv4 仮想 MAC アドレスの作成または変更

March 26, 2020

IPv4 仮想 MAC アドレスを作成するには、仮想ルータ ID を割り当てます。その後、仮想 MAC アドレスをインターフェイスにバインドできます。複数の仮想ルータ ID を同じインターフェイスにバインドすることはできません。仮想 MAC アドレス設定を確認するには、仮想 MAC アドレスと仮想 MAC アドレスにバインドされたインターフェイスを表示して調べる必要があります。

仮想 **MAC** アドレスを設定するためのパラメータ

- VrID

仮想 **MAC** アドレスを識別する仮想ルータ **ID**。指定できる値は **1** ～**255** です。

```
ifnum
```

仮想 MAC アドレスにバインドされるインターフェイス番号（スロット/ポート表記）。

仮想 **MAC** アドレスを設定するには

1. 構成ユーティリティの [構成] タブで、[システム] > [ネットワーク] を展開し、[VMAC] をクリックします。
2. 詳細ペインの [VMAC] タブで、[追加] をクリックします。
3. [VMAC の作成] ダイアログボックスの [仮想ルーター ID] に値を入力します。
4. [関連付けられたインターフェイス] の [使用可能なインターフェイス] で、ネットワークインターフェイスを選択し、[追加]、[作成]、[閉じる] の順にクリックします。

仮想 MAC アドレスを作成すると、設定ユーティリティに表示されます。ネットワークインターフェイスを選択した場合、仮想ルーター ID はそのインターフェイスにバインドされます。

仮想 **MAC** アドレスを削除するには

仮想 MAC アドレスを削除するには、対応する仮想ルータ ID を削除する必要があります。

1. 構成ユーティリティの [構成] タブで、[システム] > [ネットワーク] を展開し、[VMAC] をクリックします。
2. 詳細ペインでアイテムを選択し、[削除] をクリックします。

仮想 **MAC** アドレスをバインドおよびバインド解除するには

仮想ルーター ID を作成したら、Citrix Gateway でネットワークインターフェイスを選択し、仮想ルーター ID をネットワークインターフェイスにバインドしました。また、ネットワークインターフェイスから仮想 MAC アドレスをバインド解除し、Citrix Gateway で設定した MAC アドレスをそのままにすることもできます。

1. 構成ユーティリティの [構成] タブで、[システム] > [ネットワーク] を展開し、[VMAC] をクリックします。
2. 詳細ペインでアイテムを選択し、[開く] をクリックします。

3. [構成されたインターフェイス] で、ネットワークインターフェイスを選択し、[削除]、[OK]、[閉じる] の順にクリックします。

IPv6 仮想 MAC アドレスの設定

March 26, 2020

Citrix Gateway は、IPv6 パケットの仮想 MAC アドレスをサポートします。IPv4 仮想 MAC アドレスがインターフェイスにバインドされている場合でも、任意のインターフェイスを IPv6 の仮想 MAC アドレスにバインドできます。インターフェイスから送信される IPv6 パケットは、そのインターフェイスにバインドされた仮想 MAC アドレスを使用します。インターフェイスにバインドされた仮想 MAC アドレスがない場合、IPv6 パケットは物理 MAC を使用します。

IPv6 用の仮想 MAC アドレスの作成または変更

March 26, 2020

IPv6 仮想 MAC アドレスを作成するには、IPv6 仮想ルータ ID を割り当てます。その後、仮想 MAC アドレスをインターフェイスにバインドできます。複数の IPv6 仮想ルータ ID を 1 つのインターフェイスにバインドすることはできません。仮想 MAC アドレス設定を確認するには、仮想 MAC アドレスと仮想 MAC アドレスにバインドされたインターフェイスを表示して調べる必要があります。

IPv6 用の仮想 MAC アドレスを設定するためのパラメータ

- 仮想ルータ ID

仮想 **MAC** アドレスを識別する仮想ルータ **ID**。指定できる値は **1** ～**255** です。

```
1 ifnum
```

仮想 MAC アドレスにバインドされるインターフェイス番号（スロット/ポート表記）。

IPv6 の仮想 MAC アドレスを設定するには

1. 構成ユーティリティの [構成] タブで、[システム] > [ネットワーク] を展開し、[VMAC] をクリックします。
2. 詳細ペインの [VMAC6] タブで、次のいずれかの操作を行います。
    - 新しい仮想 MAC アドレスを作成するには、[Add] をクリックします。
    - 既存の仮想 MAC アドレスを変更するには、[Open] をクリックします。

3. [VMAC6 の作成] または [VMAC6 の構成] ダイアログボックスの [仮想ルーター ID] に、vrID6 などの値を入力します。
4. [インターフェイスの関連付け] で、[追加]、[作成]、[閉じる] の順にクリックします。ステータスバーに、仮想 MAC アドレスが設定されていることを示すメッセージが表示されます。

IPv6 の仮想 **MAC** アドレスを削除するには

1. 構成ユーティリティの [構成] タブで、[システム] > [ネットワーク] を展開し、[VMAC] をクリックします。
2. 詳細ペインの [VMAC6] タブで、削除する仮想ルータ ID を選択し、[削除] をクリックします。ステータスバーに、仮想 MAC アドレスが削除されたことを示すメッセージが表示されます。

異なるサブネットでの高可用性ペアの設定

March 26, 2020

一般的な高可用性展開は、高可用性ペアの両方のアプライアンスが同じサブネット上に存在する場合です。高可用性展開は、各アプライアンスが異なるネットワークに配置されている 2 つの Citrix Gateway アプライアンスで構成することもできます。このトピックでは、後者の設定について説明し、設定例と、1 つのネットワーク内およびネットワーク間の高可用性設定の違いの一覧を示します。

リンクの冗長性とルートモニタを設定することもできます。これらの Citrix Gateway 機能は、ネットワーク間の高可用性構成に役立ちます。また、各 Citrix Gateway でパートナーアプライアンスがアクティブであることを確認するために使用するヘルスチェックプロセスについても説明します。

独立したネットワーク構成の仕組み

Citrix Gateway アプライアンスは、2 つの異なるネットワーク上の異なるルーター（R3 と R4 と呼ばれる）に接続されています。アプライアンスは、これらのルータを介してハートビートパケットを交換します。ハートビートパケットは、接続がまだアクティブであることを保証する一定の間隔で発生する信号です。この設定を拡張して、任意の数のインターフェイスが関与する配置に対応できます。

注：ネットワークでスタティックルーティングを使用する場合は、ハートビートパケットが正常に送受信されるように、すべてのシステム間にスタティックルートを追加する必要があります。（システムでダイナミックルーティングを使用する場合、スタティックルートは不要です）。

高可用性ペアのアプライアンスが 2 つの異なるネットワーク上に存在する場合、セカンダリ Citrix Gateway には独立したネットワーク構成が必要です。つまり、異なるネットワーク上の Citrix Gateway アプライアンスは、マッピングされた IP アドレス、仮想 LAN、またはネットワークルートを共有できません。高可用性ペアの Citrix Gateway アプライアンスの設定可能なパラメーターが異なるこのタイプの構成は、独立したネットワーク構成または対称ネットワーク構成と呼ばれます。

次の表は、独立したネットワーク構成の構成可能なパラメーターの概要と、各 Citrix Gateway での設定方法を示しています。

設定可能なパラメータ	動作
IP アドレス	Citrix Gateway 固有です。そのアプライアンスでのみアクティブです。
仮想 IP アドレス	フローティング。
仮想 LAN	Citrix Gateway 固有です。そのアプライアンスでのみアクティブです。
ルート	Citrix Gateway 固有です。そのアプライアンスでのみアクティブです。リンクロードバランシング（LLB）ルートがフローティング状態です。
アクセスコントロールリスト（ACL）	フローティング (共通)。両方のアプライアンスでアクティブです。
動的ルーティング	Citrix Gateway 固有です。そのアプライアンスでのみアクティブです。セカンダリ Citrix Gateway もルーティングプロトコルを実行し、アップストリームルーターとピアリングする必要があります。
L2 モード	フローティング (共通)。両方のアプライアンスでアクティブです。
L3 モード	フローティング (共通)。両方のアプライアンスでアクティブです。
逆方向ネットワークアドレス変換 (NAT)	Citrix Gateway 固有です。NAT IP アドレスがフローティング状態であるため、仮想 IP アドレスを持つリバース NAT。

リモートノードの追加

March 26, 2020

高可用性ペアの 2 つのノードが異なるサブネット上に存在する場合、各ノードは異なるネットワーク構成を持つ必要があります。したがって、2 つの独立したシステムが高可用性ペアとして機能するように設定するには、設定プロセス中に独立したネットワークコンピューティングモードを指定する必要があります。

高可用性ノードを追加する場合は、接続されていないインターフェイスまたはトラフィックに使用されていないインターフェイスごとに、高可用性モニタを無効にする必要があります。

独立したネットワークコンピューティングモード用にリモートノードを追加するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. 詳細ウィンドウで、[ノード] タブをクリックし、[追加] をクリックします。
3. ［高可用性セットアップ］ダイアログボックスの［リモートノードの IP アドレス］テキストボックスに、リモートノードであるアプライアンスの Citrix Gateway IP アドレスを入力します。

   IPv6 アドレスを使用するには、IP アドレスを入力する前に [IPv6] チェックボックスをオンにします。
4. ローカルノードをリモートノードに自動的に追加する場合は、[リモートシステムを構成して高可用性セットアップに参加する] を選択します。このオプションを選択しない場合は、リモートノードで表されるアプライアンスにログオンし、現在構成しているノードを追加する必要があります。
5. クリックすると、ダウンしているインターフェイスまたはチャネルの HA モニタをオフにするが有効になります。
6. [セルフモードで INC (独立ネットワーク構成) モードをオンにする] をクリックして有効にします。
7. ［OK］をクリックします。[Nodes] ページには、高可用性構成のローカルノードとリモートノードが表示されます。

リモートノードを削除するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. 詳細ペインで、[ノード] タブをクリックします。
3. 削除するノードを選択し、[削除] をクリックし、[はい] をクリックします。

ルートモニタの設定

March 26, 2020

ルートモニタを使用すると、テーブルにダイナミックに学習されたルートまたはスタティックルートが含まれているかどうかにかかわらず、高可用性状態を内部ルーティングテーブルに依存させることができます。高可用性構成では、各ノードのルートモニタが内部ルーティングテーブルをチェックし、特定のネットワークに到達するためのルートエントリが常に存在することを確認します。ルートエントリが存在しない場合、ルートモニタの状態は DOWN に変わります。

Citrix Gateway アプライアンスにネットワークに到達するための静的ルートのみがあり、ネットワークのルートモニターを作成する場合は、静的ルートに対して監視対象の静的ルートを有効にする必要があります。モニタ対象のスタティックルートは、内部ルーティングテーブルから到達不能なスタティックルートを削除します。スタティックル

ートでモニタ対象のスタティックルートを無効にすると、到達不能なスタティックルートが内部ルーティングテーブルに残り、ルートモニタの目的がなくなります。

ルートモニタは、[独立ネットワーク構成] の設定を有効または無効にしてサポートされます。次の表は、高可用性セットアップおよび独立ネットワーク構成を有効または無効にした場合のルートモニタの状況を示しています。

無効の独立ネットワーク構成モードでの高可用性のルートモニタ	有効になっている独立ネットワーク構成モードでの高可用性のルートモニタ
ルートモニタはノードによって伝播され、同期中に交換されます。	ルートモニタは、ノードによって伝播されず、同期中に交換されることもありません。
ルートモニタは、現在のプライマリノードでのみアクティブです。	ルートモニタは、プライマリノードとセカンダリノードの両方でアクティブです。
Citrix Gateway アプライアンスは、ルートエントリが内部ルーティングテーブルに存在するかどうかに関係なく、常にルートモニターの状態を UP として表示します。	Citrix Gateway アプライアンスは、対応するルートエントリが内部ルーティングテーブルに存在しない場合、ルートモニターの状態を DOWN と表示します。
ルートモニターは、Citrix Gateway が動的ルートを学習できるようにするために、ルートモニターがルートの監視を開始します。このルートには最大 180 秒かかります。これには、再起動、フェイルオーバー、v6 ルートに対する set route6 コマンド、v4 ルートに対する set route msr の有効化/無効化コマンドの設定、新しいルートモニターの追加	該当なし

ルートモニタは、独立ネットワーク構成モードを無効にし、プライマリノードからの Gateway を高可用性フェールオーバーの条件の 1 つとして到達不能にする場合に便利です。

たとえば、次の図に示すように、Citrix Gateway アプライアンス NS1 と NS2 が同じサブネットにあり、ルーター R1 とスイッチ SW1、SW2、SW3 を持つ 2 アームトポロジーの高可用性セットアップで独立ネットワーク構成を無効にします。このセットアップでは R1 が唯一のルータであるため、現在のプライマリノードから R1 に到達できない場合は常に、高可用性セットアップをフェールオーバーする必要があります。各ノードでルートモニタ（それぞれ RM1 と RM2 など）を設定して、そのノードからの R1 の到達可能性を監視できます。

NS1 を現在のプライマリノードとして使用すると、ネットワークフローは次のようになります。

1. NS1 上のルートモニタ RM1 は、ルータ R1 のルートエントリの存在について、NS1 の内部ルーティングテーブルを監視します。NS1 および NS2 は、スイッチの SW1 または SW3 を介して定期的にハートビートメッセージを交換します。
2. スイッチ SW1 に障害が発生すると、NS1 のルーティングプロトコルは R1 に到達できないことを検出するため、内部ルーティングテーブルから R1 のルートエントリを削除します。NS1 および NS2 は、スイッチの SW3 を介して定期的にハートビートメッセージを交換します。

3. R1 のルートエントリが内部ルーティングテーブルに存在しないことを検出すると、RM1 はフェールオーバーを開始します。NS1 と NS2 の両方から R1 へのルートがダウンしている場合、いずれかのアプライアンスが R1 に到達して接続をリストアできるまで、180 秒ごとにフェイルオーバーが行われます。

ルートモニタの追加または削除

March 26, 2020

高可用性ペアのアプライアンスが異なるネットワーク上に存在する場合、Citrix Gateway の高可用性の状態は、アプライアンスに到達できるかどうかによって異なります。クロスネットワーク高可用性構成では、各 Citrix Gateway のルートモニターが内部ルーティングテーブルをスキャンして、他の Citrix Gateway のエントリが常に存在することを確認します。

ルートモニタを追加するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. [ルートモニタのバインド/バインド解除] ダイアログボックスの [ルートモニタ] タブで、[操作] をクリックし、[構成] をクリックします。
3. [ルートモニターの指定] の [ネットワーク] に、他の Citrix Gateway アプライアンスのネットワークの IP アドレスを入力します。

   IPv6 アドレスを構成するには、[IPv6] をクリックし、IP アドレスを入力します。
4. [ネットマスク] に、他のネットワークのサブネットマスクを入力し、[追加] をクリックし、[OK] をクリックします。

この手順が完了すると、ルートモニターが Citrix Gateway にバインドされます。

注：ルートモニターが Citrix Gateway にバインドされていない場合、いずれかのアプライアンスの高可用性状態はインターフェイスの状態によって決まります。

ルートモニタを削除するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. [ルートモニター] タブで、[操作] をクリックし、[構成] をクリックします。
3. [構成されたルートモニタ] で、モニタを選択し、[削除] をクリックし、[OK] をクリックします。

リンク冗長性の設定

March 26, 2020

リンク冗長性は、ネットワークインターフェイスをグループ化して、他の機能を持つ Citrix Gateway の 1 つのネットワークインターフェイスで障害が発生した場合のフェイルオーバーを防止します。プライマリ Citrix Gateway の最初のインターフェイスで障害が発生すると、フェイルオーバーがトリガーされますが、最初のインターフェイスでは 2 番目のリンクを使用してユーザー要求を処理できます。リンクの冗長性を構成する場合、2 つのインターフェイスをフェイルオーバーインターフェイスセットにグループ化して、プライマリ Citrix Gateway のすべてのインターフェイスが機能しない限り、単一のリンクで障害が発生してセカンダリ Citrix Gateway へのフェイルオーバーを防ぐことができます。

フェールオーバーインターフェイスセット内の各インターフェイスは、独立したブリッジエントリを維持します。Citrix Gateway で有効になっていて、障害が発生したインターフェイスセットにバインドされていない監視インターフェイスは、クリティカルインターフェイスと呼ばれます。これは、これらのインターフェイスのいずれかに障害が発生するとフェイルオーバーがトリガーされるためです。

リンクの冗長性を設定するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. [フェールオーバーインターフェイスセット] タブで、[追加] をクリックします。
3. [名前] に、セットの名前を入力します。
4.「インタフェース」で、「追加」をクリックします。
5. [使用可能なインターフェイス] でインターフェイスを選択し、矢印をクリックしてインターフェイスを [構成済み] に移動します。
6. 2 番目のインターフェイスに対してステップ 4 と 5 を繰り返し、[Create] をクリックします。

インターフェイス間のフェールオーバーに必要な数だけインターフェイスを追加できます。

フェールオーバーインターフェイスセットからインターフェイスを削除するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. [フェールオーバーインターフェイスセット] タブで、セットを選択し、[削除] をクリックします。

フェールオーバーインターフェイスセットを削除するには

フェイルオーバーインターフェイスセットが不要になった場合は、Citrix Gateway から削除できます。

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。

2. [フェールオーバーインターフェイスセット] タブで、セットを選択し、[削除] をクリックします。

フェイルオーバーの原因の理解

April 9, 2020

次のイベントにより、高可用性構成でフェールオーバーが発生する可能性があります。

1. セカンダリノードが、セカンダリに設定されたデッドインターバルを超えた期間、プライマリノードからハートビートパケットを受信しない場合。デッド間隔の設定の詳細については、通信間隔の設定を参照してください。ノードがピアノードからハートビートパケットを受信しない原因としては、次のようなものがあります。
   - ネットワーク構成の問題により、ハートビートが高可用性ノード間のネットワークを通過できなくなります。
   - ピアノードでハードウェアまたはソフトウェアの障害が発生し、そのためにハング（ハング）、再起動、または処理を停止し、ハートビートパケットを転送します。
2. プライマリノードで SSL カードのハードウェア障害が発生します。
3. プライマリノードは、そのネットワークインターフェイス上でハートビートパケットを 3 秒間受信しません。
4. プライマリノードでは、フェールオーバーインターフェイスセット (FIS) またはリンク集約 (LA) チャネルの一部ではなく、高可用性モニター (HAMON) が有効になっているネットワークインターフェイスに障害が発生します。インターフェイスは有効ですが、DOWN ステートになります。
5. プライマリノードでは、FIS のすべてのインターフェイスに障害が発生します。インターフェイスは有効ですが、DOWN ステートになります。
6. プライマリノードで、HAMON が有効になっている LA チャネルが失敗します。インターフェイスは有効ですが、DOWN ステートになります。
7. プライマリノードでは、すべてのインターフェイスに障害が発生します。この場合、フェールオーバーは HAMON 設定に関係なく実行されます。
8. プライマリノードでは、すべてのインターフェイスが手動で無効になります。この場合、フェールオーバーは HAMON 設定に関係なく実行されます。
9. フェイルオーバーを強制するには、いずれかのノードで force failover コマンドを発行します。
10. プライマリノードにバインドされているルートモニタは DOWN になります。

ノードからのフェイルオーバーの強制実行

March 26, 2020

たとえば、プライマリノードを交換またはアップグレードする必要がある場合に、フェールオーバーを強制することができます。プライマリノードまたはセカンダリノードのいずれかからフェイルオーバーを強制できます。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ステータスを表示するには、ノードのステータスを表示します。

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。
- セカンダリノードは無効です。
- セカンダリノードは、セカンダリノードを維持するように構成されています。

強制フェイルオーバーコマンドの実行時に潜在的な問題を検出すると、Citrix Gateway アプライアンスが警告メッセージを表示します。メッセージには、警告をトリガーした情報が含まれており、続行する前に確認を要求します。

プライマリまたはセカンダリノードでのフェイルオーバーの強制実行

March 26, 2020

プライマリノードでフェイルオーバーを強制すると、プライマリがセカンダリになり、セカンダリがプライマリになります。強制フェイルオーバーは、プライマリノードがセカンダリノードが稼働していると判断できる場合にのみ可能です。

セカンダリノードが DOWN の場合、強制フェールオーバーコマンドは次のエラーメッセージを返します。「無効なピアの状態のため操作できません。修正して再試行してください。」

セカンダリシステムが要求状態または非アクティブの場合、コマンドは次のエラーメッセージを返します。「現在操作できません。システムが安定するのを待ってから、再試行してください。」

セカンダリノードから force failover コマンドを実行すると、セカンダリノードはプライマリノードになり、プライマリノードはセカンダリノードになります。強制フェールオーバーは、セカンダリノードの健全性が良好で、ノードがセカンダリノードを維持するように構成されていない場合にのみ発生します。

2 次ノードが 1 次ノードになることができない場合、または 2 次ノードが (STAYSECONDARY オプションを使用して) 2 次ノードに設定されている場合、ノードは次のエラーメッセージを表示します。「状態が無効であるため、操作できません。詳細については、ノードを参照してください。」

プライマリノードまたはセカンダリノードでフェールオーバーを強制するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. 詳細ウィンドウの [ノード] タブで、プライマリノードを選択し、[アクション] で [フェイルオーバーの強制] をクリックします。
3. [警告] ダイアログボックスで、[はい] をクリックします。

プライマリノードを強制的にプライマリに留める

March 26, 2020

高可用性構成では、アプライアンスのフェイルオーバー後もプライマリ Citrix Gateway を強制的にプライマリに維持できます。この設定は、スタンドアロンの Citrix Gateway アプライアンスと、高可用性ペアのプライマリアプライアンスである Citrix Gateway でのみ構成できます。

プライマリノードを強制的にプライマリに維持するには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. 詳細ペインの [ノード] タブでノードを選択し、[編集] をクリックします。
3. [高可用性ステータス] で、[プライマリに保たれる] をクリックし、[OK] をクリックします。

この設定をクリアするには、次のコマンドを使用します。

```
clear configuration full
```

次のコマンドでは、Citrix Gateway の高可用性構成は変更されません。

```
clear configuration basic
```

```
clear configuration extended
```

セカンダリノードを強制的にセカンダリ状態にする

March 26, 2020

高可用性設定では、セカンダリ Citrix Gateway をプライマリ Citrix Gateway の状態とは無関係に強制的にセカンダリを維持できます。セカンダリを維持するように Citrix Gateway を構成すると、プライマリ Citrix Gateway で障害が発生しても、セカンダリ状態のままになります。

たとえば、既存の高可用性セットアップで、プライマリ Citrix Gateway をアップグレードする必要があり、このプロセスに指定した時間がかかるとします。アップグレード中、プライマリ Citrix Gateway は使用できなくなりますが、セカンダリ Citrix Gateway を引き継ぐ必要はありません。プライマリ Citrix Gateway で障害が検出された場合でも、セカンダリ Citrix Gateway のままにしておきます。

高可用性ペアの Citrix Gateway のステータスがセカンダリになるように構成されている場合、高可用性状態マシンの移行には参加しません。Citrix Gateway のステータスは、［ノード］タブの構成ユーティリティで確認できます。

この設定は、スタンドアロンおよびセカンダリ Citrix Gateway の両方で機能します。

高可用性ノードを設定しても、そのノードは伝播または同期されず、設定が構成されている Citrix Gateway にのみ影響します。

セカンダリノードを強制的にセカンダリにするには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. 詳細ペインの [ノード] タブでノードを選択し、[編集] をクリックします。
3. [高可用性の状態] で、[セカンダリ (リッスンモードのまま)] をクリックし、[OK] をクリックします。

Citrix Gateway をアクティブな高可用性アプライアンスとしてサービスに戻すには

1. 構成ユーティリティの [構成] タブのナビゲーションウィンドウで、[システム] を展開し、[高可用性] をクリックします。
2. 詳細ペインの [ノード] タブで、プライマリノードを維持するアプライアンスを選択し、[開く] をクリックします。
3. [高可用性ステータス] で、[有効 (HA にアクティブに参加する)] をクリックし、[OK] をクリックします。

クラスタリングの使用

March 26, 2020

Citrix Gateway をクラスター構成で展開して、VPN クライアントトラフィックに高い処理量、高可用性、およびスケーラビリティを提供できます。クラスターでは、Citrix Gateway アプライアンスまたは仮想マシンのグループは単一のシステムイメージとして動作し、ユーザーセッションを調整し、ネットワークリソースへのトラフィックを管理します。Citrix Gateway クラスタは、最低 2 つ、最大 32 台の Citrix Gateway アプライアンスまたは仮想マシンをクラスタノードとして構成して構築できます。

Citrix Gateway クラスターの構成を開始する前に、
Citrix ADC クラスタリングドキュメントをお読みください。そのドキュメントの次のトピックに特に注意してください。

- 使用予定のシステムが要件を満たしていることを確認するには、ハードウェアおよびソフトウェアの要件を参照してください。
- クラスタリングの概念については、クラスタリングのしくみを参照してください。
- 展開を計画し、環境に関連する警告を特定するには、ノード間通信の設定を参照してください。

Citrix Gateway クラスターは、スポットされた VIP 構成タイプの Citrix ADC クラスターとして動作します。

クラスタリングの構成

April 9, 2020

Citrix Gateway クラスタリングを設定する主なタスクは次のとおりです。

1. 構成コーディネーターにする Citrix Gateway アプライアンスまたは VM を決定し、そのシステムにクラスターインスタンスを作成します（クラスターインスタンスが存在しない場合）。
2. Citrix Gateway システムをノードとしてクラスターに参加させます。
3. STICKY オプションを設定して、クラスタインスタンスにノードグループを作成します。
4. 1 つのクラスタノードをクラスタノードグループにバインドします。
5. 構成コーディネーターで Citrix Gateway 仮想サーバーを構成し、クラスターノードグループにバインドします。

Citrix ADC クラスターを構成するには、複数の方法があります。次の一連のタスクでは、構成ユーティリティで使用できる最も直接的な方法を使用します。

構成ユーティリティを使用して **Citrix Gateway** クラスターインスタンスを作成するには

展開の詳細をすべて整理したら、構成コーディネーターとなる Citrix Gateway で構成を開始します。

注意: クラスターインスタンスを作成すると、設定がクリアされます。参照用に既存のシステム構成を保存する必要がある場合は、クラスタ構成を続行する前にコピーをアーカイブします。クラスターで使用する既存の設定は、クラスターが確立された後、構成コーディネーターで再適用できます。

1. NSIP アドレスで Citrix ADC 構成ユーティリティにログオンします。
2. [システム] ノードを展開し、[クラスタ] サブノードを展開します。
3. 詳細ウィンドウで、[クラスターの管理] をクリックします。
4. [クラスタ構成] ダイアログボックスで、クラスタの作成に必要なパラメータを設定します。
   a) クラスタインスタンス ID を入力します。これは、クラスターインスタンスの数値識別子です。デフォルト値は 1 ですが、1 ～16 の任意の数値に設定できます。
   b) クラスタ IP アドレスを入力します。これは、クラスターの構成コーディネーター IP アドレスです。これは、クラスターの管理 IP アドレスです。
   c) 優先するバックプレーンインターフェイスを選択します。これは、クラスターノード間の通信に使用する Citrix Gateway インターフェイスです。
5. ［作成］をクリックします。
6. システムの再起動を確認するプロンプトで、[Yes] をクリックします。
7. ノードが UP 状態になり、同期が成功したら、クラスタ IP アドレスから、ノードとクラスタ IP アドレスの両方の RPC 資格情報を変更します。RPC ノードパスワードの変更の詳細については、RPC ノードのパスワードを変更するを参照してください。
8. システムが再起動するまで待ちます。使用可能になったら、手順 4 (2) で構成したクラスタ IP アドレスで構成ユーティリティにログオンします。

注: [System Information] 詳細ペインで、NSIP アドレスのローカルノードが構成コーディネータとして報告されます。これにより、基本クラスタインスタンスが現在動作していることが確認されます。

構成コーディネータのローカルノードが自動的にクラスタに追加されます。次のタスクでは、さらにノードを追加できます。

Citrix Gateway クラスターへのノードの追加

クラスターインスタンスが確立されたら、他の Citrix Gateway ノードをクラスターに追加できます。

クラスターにさらに Citrix Gateway システムを追加するには、構成ユーティリティーを使用して、クラスターノード作成およびクラスター結合の設定をリモートで発行します。

注：クラスターへのノードの追加は、Citrix Gateway のセットアップを構成する前に完了する必要があります。この方法では、クラスター構成に何か問題があり、クラスターを削除して再度開始する場合は、Citrix Gateway 構成を繰り返す必要はありません。

1. クラスタ IP アドレスで Citrix ADC 構成ユーティリティにログオンします。
2. [システム] ノードを展開し、[クラスタ] サブノードを展開します。
3. 詳細ウィンドウで、[クラスターの管理] をクリックします。
4. [クラスターノード] の詳細ウィンドウで、[追加] をクリックします。
5. [クラスタノードの作成] ペインで、このノードの一意のノード ID を入力します。
6. クラスタノードとして追加するシステムの Citrix ADC IP アドレスを入力します。
7. クラスターノードの資格情報ペインで、リモート Citrix Gateway システムの Citrix Gateway ユーザー名とパスワードを入力します。
8. [構成コーディネーターの資格情報] ウィンドウで、ローカルで承認されたユーザーのパスワードを入力します。
9. ［作成］をクリックします。
10. プロンプトが表示されたら、[はい] をクリックしてシステム構成を保存し、リモート Citrix Gateway のウォームリブートを実行します。
11. ノードが UP 状態になり、同期が成功したら、クラスタ IP アドレスから、ノードとクラスタ IP アドレスの両方の RPC 資格情報を変更します。RPC ノードパスワードの変更の詳細については、RPC ノードのパスワードを変更するを参照してください。

クラスターノードとして構成する追加のリモート Citrix Gateway システムごとに、手順 4〜11 を繰り返します。

クラスタノードが [クラスタノード] 詳細ペインの [アクティブノードリスト] に含まれていることを確認します。欠落しているノードがある場合は、必要なノードがすべて一覧表示されるまで、手順 4 〜10 を繰り返します。

クラスタノードグループの作成

クラスタノードを追加したら、クラスタノードグループを作成できます。

1. クラスタ IP アドレスで Citrix ADC 構成ユーティリティにログオンします。
2. [システム] ノードを展開し、[クラスタ] サブノードを展開します。
3. [ノードグループ] をクリックします。
4. 詳細ウィンドウで、[追加] をクリックします。
5. クラスタノードグループの名前を入力します。
6. [スティッキー] オプションを選択します。これは、Citrix Gateway 仮想サーバーの種類をサポートするために必要です。
7. ［続行］をクリックします。

これで、クラスタノードグループが確立されます。構成ユーティリティーのこの領域を離れる前に、ローカルの Citrix Gateway ノードを新しいクラスターノードグループにバインドできます。これは、クラスタグループにバインドされている唯一のノードです。

ローカルクラスタノードをクラスタノードグループにバインドする

Citrix Gateway クラスター構成はスポットの種類であるため、ノードグループにバインドできるノードは 1 つだけです。次の手順では、構成コーディネーター上のローカルノードをノードグループにバインドしますが、このバインドにはクラスター内の任意のノードを使用できます。

1. [詳細設定] ウィンドウで、[クラスターノード] を展開します。
2. 中央の [クラスタノード] ペインで、[クラスタノードなし] を選択します。
3. クラスタノードの構成画面で、[バインド] をクリックします。
4. この Citrix Gateway システムの NSIP アドレスで表されるローカルノードを選択します。
5. ［Insert］をクリックします。
6. ［OK］をクリックします。
7. ［完了］をクリックします。

クラスターが作成され、以下のタスクによって構成された Citrix Gateway 仮想サーバーを共有する準備が整いました。

クラスターノードグループへの **Citrix Gateway** 仮想サーバーのバインド

クラスターを確立したら、クラスター展開の目的とする Citrix Gateway 構成を構築できます。構成をクラスタに結び付けるには、Citrix Gateway 仮想サーバーを作成し、Sticky タイプに設定されているクラスタノードグループにバインドする必要があります。仮想サーバーをクラスターノードグループにバインドした後で、引き続き Citrix Gateway を構成できます。

複数の Citrix Gateway 仮想サーバーを構成する場合は、それらをクラスターノードグループにもバインドする必要があります。

注: Citrix Gateway 仮想サーバーを構成していない場合は、まず、［
システム］>［設定］>［基本機能の構成］で、Citrix Gateway と認証、承認、監査機能を有効にする必要があります。

1. クラスタ IP アドレスで Citrix ADC 構成ユーティリティにログオンします。
2. [システム] ノードを展開し、[クラスタ] サブノードを展開します。
3. [ノードグループ] をクリックします。
4. [Node Group] ペインで、目的のノードグループ名を選択し、[Edit] をクリックします。
5. 右側の [詳細設定] ペインで、[仮想サーバー] オプションを展開し、[+] アイコンをクリックして仮想サーバーを追加します。
6. VPN 仮想サーバーの種類を選択し、[続行] をクリックします。
7. ［バインド］をクリックします。

8. 必要な仮想サーバーが表示されている場合は、その仮想サーバーを選択して [挿入] をクリックし、[OK] をクリックします。
9. 新しい仮想サーバーを作成する必要がある場合は、[追加] をクリックします。Citrix ADC 仮想サーバーの構成に進みます。最低限必要なのは、仮想サーバをクラスタ・ノード・グループにバインドできるように作成することだけです。
10. Citrix Gateway 仮想サーバー］リストで仮想サーバーが使用可能になったら、その仮想サーバーを選択して［挿入］をクリックします。
11. ［OK］をクリックします。
12. ［完了］をクリックします。

注：複数の Citrix Gateway 仮想サーバーを構成する場合、これらも同じ方法でクラスターノードグループにバインドする必要があります。

システムのメンテナンスとモニタリング

March 26, 2020

Citrix Gateway の構成が完了したら、アプライアンスを保守および監視する必要があります。これを行うには、次の方法があります。

- Citrix Gateway を最新バージョンにアップグレードできます。Citrix Web サイトにログオンすると、Citrix Gateway のダウンロードサイトとソフトウェアのダウンロードに移動できます。メンテナンスビルドの Readme は、Citrix ナレッジセンターで見つけることができます。
- Citrix Gateway の構成タスクと管理タスクは、グループの異なるメンバーに割り当てることができます。委任管理では、ユーザーにアクセスレベルを割り当てて、Citrix Gateway で特定のタスクを実行するように制限できます。
- Citrix Gateway の構成は、アプライアンスまたはコンピューター上のファイルに保存できます。現在の実行構成と保存構成を比較できます。また、Citrix Gateway から設定をクリアすることもできます。
- Citrix Gateway 構成ユーティリティーでは、ユーザーセッションの表示、更新、およびエンドユーザーセッションを実行できます。
- Citrix Gateway でログオンを構成できます。ログはアプライアンスに関する重要な情報を提供し、問題が発生した場合に役立ちます。

委任された管理者の構成

March 26, 2020

Citrix Gateway には、デフォルトの管理者ユーザー名とパスワードが設定されています。デフォルトのユーザー名とパスワードは nsroot です。セットアップウィザードを初めて実行するときは、管理者パスワードを変更できます。

追加の管理者アカウントを作成し、各アカウントに異なるレベルの Citrix Gateway を割り当てることができます。これらの追加アカウントは、委任された管理者と呼ばれます。たとえば、Citrix Gateway の接続とログを監視するユーザーと、Citrix Gateway で特定の設定の構成を担当するユーザーがあるとします。最初の管理者には読み取り専用アクセスがあり、2 番目の管理者にはアプライアンスへのアクセスが制限されています。

委任された管理者を設定するには、コマンドポリシーとシステムユーザーとグループを使用します。

委任された管理者を構成する場合、構成プロセスは次のようになります。

- システムユーザーを追加します。システムユーザは、指定された権限を持つ管理者です。すべての管理者は、自分が属するグループのポリシーを継承します。
- システムグループを追加します。システムグループには、特定の権限を持つシステムユーザーが含まれます。システムグループのメンバーは、所属する 1 つまたは複数のグループのポリシーを継承します。
- コマンドポリシーを作成します。コマンドポリシーでは、ユーザーまたはグループがアクセスおよび変更を許可する Citrix Gateway 構成の部分を定義できます。また、コマンドグループ、仮想サーバ、管理者やグループの設定を許可するその他の要素などのコマンドも規制できます。
- 優先度を設定して、コマンドポリシーをユーザーまたはグループにバインドします。委任管理を構成するときは、管理者またはグループに優先順位を割り当てて、Citrix Gateway が優先するポリシーを決定できるようにします。

Citrix Gateway には、デフォルトのシステムコマンド拒否ポリシーがあります。コマンドポリシーはグローバルにバインドできません。ポリシーは、システム管理者（ユーザー）またはグループに直接バインドする必要があります。ユーザーとグループにコマンドポリシーが関連付けられていない場合は、デフォルトの拒否ポリシーが適用され、ユーザーはコマンドを実行したり、Citrix Gateway を構成したりできません。

カスタムコマンドポリシーを構成して、ユーザー権利の割り当ての詳細レベルを定義できます。たとえば、セッションポリシーを Citrix Gateway に追加することは許可されますが、他の構成は許可されません。

委任された管理者のコマンドポリシーの設定

March 26, 2020

Citrix Gateway には、委任管理に使用できる 4 つのコマンドポリシーが組み込まれています。

- 読み取り専用。システムコマンドグループおよび ns.conf show コマンドを除くすべてのコマンドを表示するための読み取り専用アクセスを許可します。
- 演算子。読み取り専用アクセスを許可し、サービスのコマンドを有効または無効にするアクセスを許可します。また、このポリシーでは、サービスおよびサーバーを「アクセス停止」として設定します。
- ネットワーク。システムコマンドとシェルコマンドを除いて、ほぼ完全なシステムアクセスを許可します。
- スーパーユーザー。デフォルトの管理者である nsroot に付与される権限など、完全なシステム権限を付与します。

コマンドポリシーには、組み込みの式が含まれています。構成ユーティリティを使用して、システムユーザ、システムグループ、コマンドポリシーを作成し、権限を定義します。

Citrix Gateway で管理ユーザーを作成するには

1. 構成ユーティリティのナビゲーションペインの [構成] タブで、[システム] > [ユーザー管理] を展開し、[システムユーザー] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [ユーザー名] にユーザー名を入力します。
4.「パスワード」および「パスワードの確認」フィールドにパスワードを入力します。
5. グループにユーザーを追加するには、[所属するメンバー] で [追加] をクリックします。
6.「使用可能」でグループを選択し、右矢印をクリックします。
7. [コマンドポリシー] の [アクション] で、[挿入] をクリックします。
8. [コマンドポリシーの挿入] ダイアログボックスで、コマンドを選択し、[OK]、[作成]、[閉じる] の順にクリックします。

管理グループの作成

管理グループには、Citrix Gateway の管理者権限を持つユーザーが含まれます。管理グループは、構成ユーティリティで作成できます。

構成ユーティリティを使用して管理グループを構成するには

1. 構成ユーティリティのナビゲーションペインの [構成] タブで、[システム] > [ユーザー管理] を展開し、[システムグループ] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [グループ名] に、グループの名前を入力します。
4. 既存のユーザーをグループに追加するには、[メンバー] で [追加] をクリックします。
5. [使用可能] でユーザーを選択し、右矢印をクリックします。
6. [コマンドポリシー] の [アクション] で [挿入] をクリックし、ポリシーを選択して [**OK**] をクリックし、[作成] をクリックして、[閉じる] をクリックします。

委任された管理者のカスタムコマンドポリシーの設定

March 26, 2020

カスタムコマンドポリシーを設定する場合は、ポリシー名を指定し、ポリシーコンポーネントを設定して、コマンド仕様を作成します。コマンド仕様では、管理者が使用できるコマンドを制限できます。たとえば、管理者が remove コマンドを使用できないようにする場合です。ポリシーを設定するときは、アクションを deny に設定してから、パラメータを設定します。

単純なコマンドポリシーまたは高度なコマンドポリシーを設定できます。単純なポリシーを構成する場合は、Citrix Gateway や認証などのコンポーネントを構成します。高度なポリシーを設定する場合は、エンティティグループと

呼ばれるコンポーネントを選択し、そのグループ内で管理者が実行できるコマンドを選択します。

単純なカスタムコマンドポリシーを作成するには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[システム] > [ユーザー管理] を展開し、[コマンドポリシー] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [ポリシー名] に、ポリシーの名前を入力します。
4.「アクション」で、「許可」または「拒否」を選択します。
5. [コマンドスペック] で、[追加] をクリックします。
6. [コマンドの追加] ダイアログボックスの [簡易] タブの [操作] で、委任された管理者が実行できる操作を選択します。
7.「エンティティ・グループ」で、1 つ以上のグループを選択します。

   Ctrl キーを押すと、複数のグループを選択できます。
8. [**Create**] をクリックしてから、[**Close**] をクリックします。

高度なカスタムコマンドポリシーを作成するには

1. 構成ユーティリティのナビゲーションペインの [構成] タブで、[システム] > [ユーザー管理] を展開し、[コマンドポリシー] をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [ポリシー名] に、ポリシーの名前を入力します。
4.「アクション」で、「許可」または「拒否」を選択します。
5. [コマンドスペック] で、[追加] をクリックします。
6. [コマンドの追加] ダイアログボックスで、[詳細設定] タブをクリックします。
7. [エンティティグループ] で、認証や高可用性など、コマンドが属するグループを選択します。
8. [エンティティ] で、ポリシーを選択します。

   Ctrl キーを押すと、リスト内の複数の項目を選択できます。
9.「操作」でコマンドを選択し、「作成」をクリックしてから「閉じる」をクリックします。

   Ctrl キーを押すと、リスト内の複数の項目を選択できます。
10. [**Create**] をクリックしてから、[**Close**] をクリックします。
11. [コマンドポリシーの作成] ダイアログボックスで、[作成] をクリックし、[閉じる] をクリックします。

[作成] をクリックすると、[コマンドポリシーの作成] ダイアログボックスの [コマンドスペック] の下に式が表示されます。

カスタムコマンドポリシーを作成したら、ユーザーまたはグループにバインドできます。

> 注: カスタムコマンドポリシーは、作成したユーザーまたはグループにのみバインドできます。カスタムコマンドポリシーをユーザー nsroot にバインドすることはできません。

カスタムコマンドポリシーをユーザーまたはグループにバインドするには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[システム] > [ユーザー管理**]** を展開し、**[**システムユーザー] をクリックするか、[システムグループ] をクリックします。
2. 詳細情報のウィンドウ領域で、リストからユーザーまたはグループを選択し、[開く] をクリックします。
3. [コマンドポリシー] でポリシーを選択し、[**OK**] をクリックします。

Citrix Gateway での監査の構成

March 26, 2020

Citrix Gateway では、アプライアンスが収集する状態とステータス情報をログに記録できます。監査ログを使用して、イベント履歴を時系列で表示できます。ログ内のメッセージには、メッセージを生成したイベントに関する情報、タイムスタンプ、メッセージタイプ、定義済みのログレベルとメッセージ情報が含まれます。ログに記録される情報と、メッセージが格納される場所を決定する設定を構成できます。

Citrix Gateway は現在、2 つのログ形式をサポートしています。ローカルログ専用のログ形式と、Syslog サーバーで使用する Syslog 形式です。監査ログを構成して、次の情報を提供できます。

レベル	説明
緊急	重大なエラーのみをログに記録します。ログ内のエントリは、Citrix Gateway が使用できない重大な問題が発生していることを示しています。
アラート	Citrix Gateway が正しく機能しない可能性があるが、操作に重要ではない問題をログに記録します。Citrix Gateway が重大な問題を起こさないようにするには、できるだけ早く修正措置を講じる必要があります。
重大	Citrix Gateway の動作を制限しないが、大きな問題にエスカレーションする可能性がある重大な状態をログに記録します。
エラー	Citrix Gateway での操作が失敗したために発生したエントリをログに記録します。

レベル	説明
警告	エラーまたは重大なエラーの原因となる可能性のある問題をログに記録します。
通知	情報レベルのログよりも詳細な問題をログに記録しますが、通知と同じ目的を果たします。
情報	Citrix Gateway で実行されたアクションをログに記録します。このレベルは、問題のトラブルシューティングに役立ちます。

TCP 圧縮を構成する場合、Citrix Gateway の監査ログには Citrix Gateway の圧縮統計情報も保存されます。異なるデータに対して達成された圧縮率は、ユーザーセッションごとにログファイルに保存されます。

Citrix Gateway では、ログ署名のセッション ID が使用されます。これにより、ユーザーごとではなくセッションごとにログを追跡できます。セッションの一部として生成されるログは、同じ SessionID を持ちます。ユーザーが同じ IP アドレスを使用して同じユーザーデバイスから 2 つのセッションを確立する場合、各セッションには一意の SessionID が割り当てられます。

> 重要**:** カスタムログ解析スクリプトを作成している場合は、カスタム解析スクリプト内でこのシグニチャを変更する必要があります。

Citrix Gateway でのログの設定

March 26, 2020

Citrix Gateway でログオンを構成する場合、監査ログを Citrix Gateway に保存するか、または Syslog サーバーに送信するかを選択できます。監査ポリシーを作成し、監査ログを保存する設定を構成するには、構成ユーティリティを使用します。

監査ポリシーを作成するには

1. 構成ユーティリティの [構成] タブで、[**Citrix Gateway**]、[ポリシー]、[監査] の順に展開します。
2. [名前**]** に、ポリシーの名前を入力します。
3. 次のいずれかを選択します:
   - Syslog サーバにログを送信する場合は、Syslog。
   - [Nslog] をクリックして、ログを Citrix Gateway に保存します。

     > 注：このオプションを選択すると、ログはアプライアンスの /var/log フォルダに保存されます。
4. 詳細ウィンドウで、[追加] をクリックします。
5. ログが格納されているサーバー情報について、次の情報を入力します。

- [名前] に、サーバーの名前を入力します。
- [サーバー] に、ログサーバーの名前または IP アドレスを入力します。

6. [Create] をクリックしてから、[Close] をクリックします。

監査ポリシーを作成したら、ポリシーを次の組み合わせにバインドできます。

- グローバル
- 仮想サーバー
- グループ
- ユーザー

監査ポリシーをグローバルにバインドするには

1. 構成ユーティリティの [構成] タブで、[**Citrix Gateway**]、[ポリシー]、[監査] の順に展開します。
2. [**Syslog**] または [**Nslog**] のいずれかを選択します。
3. 詳細ウィンドウで、[操作] をクリックし、[グローバルバインド] をクリックします。
4. [監査ポリシーを ** グローバルにバインド/バインド解除 **] ダイアログボックスの [詳細] で、[ポリシーの挿入] をクリックします。
5. [ポリシー名] でポリシーを選択し、[**OK**] をクリックします。

監査ポリシーを変更するには

既存の監査ポリシーを変更して、ログの送信先サーバーを変更できます。

1. 構成ユーティリティの「構成」タブで、「**Citrix Gateway** 」>「ポリシー」>「監査」の順に展開します。
2. [**Syslog**] または [**Nslog**] のいずれかを選択します。
3. 詳細ペインでポリシーをクリックし、[開く] をクリックします。
4. [サーバー] で、新しいサーバーを選択し、[**OK**] をクリックします。

監査ポリシーを削除するには

Citrix Gateway から監査ポリシーを削除できます。監査ポリシーを削除すると、ポリシーは自動的にバインド解除されます。

1. 構成ユーティリティの [構成] タブで、[**Citrix Gateway**]、[ポリシー]、[監査] の順に展開します。
2. [**Syslog**] または [**Nslog**] のいずれかを選択します。
3. 詳細情報のウィンドウ領域で、ポリシーをクリックし、[削除] をクリックします。

ACL ロギングの設定

March 26, 2020

拡張アクセス制御リスト（ACL）と一致するパケットの詳細をログに記録するように Citrix Gateway を構成できます。ACL 名に加えて、ログに記録される詳細には、送信元および宛先 IP アドレスなどのパケット固有の情報が含まれます。情報は、有効にするログのタイプ（Syslog または nslog）に応じて、syslog または nslog ファイルに保存されます。

ロギングは、グローバルレベルと ACL レベルの両方で有効にできます。ただし、ACL レベルでロギングを有効にするには、グローバルレベルでも有効にする必要があります。グローバル設定が優先されます。

ロギングを最適化するために、同じフローからの複数のパケットが ACL と一致する場合、最初のパケットの詳細だけがログに記録されます。カウンタは、同じフローに属する他のすべてのパケットに対して増分されます。フローは、次のパラメータに同じ値を持つパケットのセットとして定義されます。

- 接続元 IP
- 接続先 IP
- 送信元ポート
- 送信先ポート
- プロトコル（TCP または UDP）

パケットが同じフローからのものでない場合、または期間が平均時間を超えている場合は、新しいフローが作成されます。平均時間は、同じフローのパケットが追加のメッセージを生成しない時間です（ただし、カウンタが増加します）。

> 注：任意の時点でログに記録できる異なるフローの合計数は 10,000 に制限されています。

次の表では、拡張 ACL のルールレベルで ACL ロギングを設定できるパラメータについて説明します。

パラメーター名	説明
[ログ状態]	ACL のロギング機能の状態。設定可能な値:ENABLED と DISABLED。デフォルト： DISABLED。
Ratelimit	特定の ACL が生成できるログメッセージの数。デフォルトは 100 です。

構成ユーティリティを使用して **ACL** ロギングを構成するには

ACL のロギングを設定し、ルールが生成できるログメッセージの数を指定できます。

1. 構成ユーティリティのナビゲーションペインで、[システム] > [ネットワーク] を展開し、[ACL] をクリックします。
2. 詳細ウィンドウで、[拡張 **ACL**] タブをクリックし、[追加] をクリックします。
3. [拡張 **ACL** の作成] ダイアログボックスの [名前] に、ポリシーの名前を入力します。
4. [ログの状態] チェックボックスをオンにします。
5. [ログレート制限] テキストボックスに、ルールに指定するレート制限を入力し、[作成] をクリックします。

ACL ロギングを構成したら、Citrix Gateway で有効にすることができます。監査ポリシーを作成し、ユーザー、グループ、仮想サーバー、またはグローバルにバインドします。

Citrix Gateway で **ACL** または **TCP** ログを有効にするには

1. 構成ユーティリティのナビゲーションペインで、[**Citrix Gateway**] > [ポリシー] > [監査] の順に展開します。
2. syslog または nslog のいずれかを選択します。
3. [サーバー] タブで、[追加] をクリックします。
4. [監査サーバーの作成] ダイアログボックスの [名前] に、サーバーの名前を入力し、サーバーの設定を構成します。
5. [**ACL** ロギング] または [**TCP** ロギング] をクリックし、[作成] をクリックします。

Citrix Gateway プラグインのログ記録の有効化

March 26, 2020

ユーザーデバイスに保存されているテキストファイルにすべてのエラーをログに記録するように、Citrix Gateway プラグインを構成できます。ユーザーは、Citrix Gateway プラグインを構成して、ユーザーデバイスでのログオンレベルを設定し、特定のユーザーアクティビティを記録できます。ユーザーがロギングを構成すると、プラグインによってユーザーデバイス上に次の 2 つのファイルが作成されます。

- hooklog <num> .txt は、Citrix Gateway プラグインが生成する傍受メッセージをログに記録します。
- nssslvpn.txt。プラグインのエラーが一覧表示されます。

> 注**:** hooklog.txt ファイルは自動的には削除されません。定期的にファイルを削除することをお勧めします。

ユーザーログは、ユーザーデバイス上の Windows の次のディレクトリにあります。

- Windows XP (all users): %SystemDrive%:\Documents and Settings\All Users\Application Data\Citrix\AGEE
- Windows XP (user-specific): %SystemDrive%:\Documents and Settings\%username%\Local Settings\Application Data\Citrix\AGEE
- Windows Vista (all users): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows Vista (user-specific): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE
- Windows 7 (all users): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows 7 (user-specific): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE
- Windows 8 (all users): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows 8 (user-specific): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE

これらのログファイルを使用して、Citrix Gateway プラグインのトラブルシューティングを行うことができます。ユーザーは、ログファイルをテクニカルサポートに電子メールで送信できます。

［構成］ダイアログボックスで、Citrix Gateway プラグインのログレベルを設定できます。ログレベルは次のとおりです。

- エラーメッセージを記録する
- イベントメッセージを記録する
- Citrix Gateway プラグインの統計を記録する
- すべてのエラー、イベントメッセージ、および統計を記録する

ログを有効にするには

1. ユーザーデバイスで、通知領域にある Citrix Gateway のアイコンを右クリックし、［Citrix Gateway の構成］をクリックします。
2. [トレース] タブをクリックし、ログレベルを選択して [OK] をクリックします。

> 注：［
> 構成］ダイアログボックスを開くには、Citrix Gateway プラグインを使用してログオンする必要があります。

ICA 接続を監視するには

March 26, 2020

「

ICA 接続」ダイアログ・ボックスを使用して、サーバー・ファーム上のアクティブなユーザー・セッションを監視できます。このダイアログボックスには、次の情報が表示されます。

- サーバー・ファームに接続しているユーザーのユーザー名
- サーバー・ファームのドメイン名
- ユーザーデバイスの IP アドレス
- ユーザーデバイスのポート番号
- Citrix Virtual Apps and Desktops を実行しているサーバーの IP アドレス
- Citrix Virtual Apps and Desktops を実行しているサーバーのポート番号

1. 構成ユーティリティのナビゲーションペインで、［Citrix ADC Gateway］をクリックします。
2. 詳細ペインの [モニタの接続] で、[ICA 接続] をクリックして、[モニタリング] ダイアログボックスを表示します。

Citrix 製品との統合

March 26, 2020

Citrix Gateway のインストールと構成を担当するシステム管理者は、Citrix Endpoint Management、StoreFront、および Web Interface で動作するようにアプライアンスを構成できます。

ユーザーは、内部ネットワークまたはリモートの場所から直接 Endpoint Management に接続できます。ユーザーが接続すると、Web、SaaS、およびモバイルアプリにアクセスできます。また、ShareFile にあるドキュメントをどのデバイスからでも操作できます。

Citrix Gateway を介したサーバーファームへのユーザー接続を許可するには、StoreFront または Web Interface、および Citrix Gateway で設定を構成します。ユーザーが接続すると、公開アプリケーションおよび仮想デスクトップにアクセスできます。

Citrix Gateway を Endpoint Management、StoreFront および Web Interface と統合するための構成手順は、次のことを前提としています。

- Citrix Gateway は DMZ 内に存在し、既存のネットワークに接続されています。
- Citrix Gateway はスタンドアロンアプライアンスとして展開され、リモートユーザーは Citrix Gateway に直接接続します。
- StoreFront、Endpoint Management、Citrix Virtual Apps、Citrix Virtual Desktops、および Web Interface は、安全なネットワークに存在します。
- ShareFile は、Endpoint Management で設定されます。ShareFile の詳細については、ShareFileトピックとユーザーアクセス用の ShareFile 構成トピックを参照してください。

StoreFront と Endpoint Management 展開方法は、モバイルデバイスに提供するアプリによって異なります。MDX Toolkit でラップされた MDX アプリにユーザーがアクセスできる場合、Endpoint Management はセキュアネットワークの StoreFront の前に存在します。MDX アプリケーションへのアクセスを提供しない場合、StoreFront はセキュアネットワークの Endpoint Management の前に存在します。

ユーザーがアプリケーション、デスクトップ、ShareFile に接続する方法

March 26, 2020

展開環境に Citrix Endpoint Management がある場合、ユーザーは次の方法で接続できます。

- 内部ネットワークのリソースへの完全な VPN トンネルを確立する Citrix Gateway プラグイン。セッションプロファイルを作成して、Windows 用の Citrix Gateway プラグインまたは Mac 用の Citrix Gateway プラグインを選択します。ユーザーがプラグインを使用してログオンすると、エンドポイントの分析スキャンをユーザーデバイスで実行できます。

> 注：エンドポイント分析スキャンを Mac コンピューターで実行できるようにするには、Citrix Gateway 10.1、Build 120.1316.e 以降をインストールする必要があります。

- Citrix Workspace アプリを使用して、ShareFile から Endpoint Management を介してウェブ、SaaS、エンタープライズアプリケーション、Web リンク、およびドキュメントに接続します。ユーザーが Citrix Workspace アプリでログオンすると、Citrix Gateway は接続を Endpoint Management にルーティングします。Citrix Workspace アプリが接続を確立すると、ユーザーのアプリケーションとドキュメントが Citrix Workspace アプリに表示されます。ユーザーが Citrix Workspace アプリでログオンし、Endpoint Management に直接接続する場合は、Citrix Gateway でクライアントレスアクセスを有効にする必要があります。この展開では、StoreFront は必要ありません。
- Citrix Workspace アプリを使用して、StoreFront または Web Interface を介して公開アプリケーションおよび仮想デスクトップに接続できます。ユーザーが Citrix Workspace アプリでログオンすると、Citrix Gateway は StoreFront または Web Interface への接続をルーティングします。Citrix Workspace アプリが接続を確立すると、ユーザーアプリケーションとデスクトップが Citrix Workspace アプリに表示されます。
- Secure Hub は、Endpoint Management を介してモバイルデバイスから WorxMail や WorxWeb などの iOS および Android アプリに接続します。ユーザーは、Secure Hub にログオンすると、Endpoint Management で設定したモバイルアプリにアクセスできます。Citrix Gateway が Micro VPN 接続を確立すると、ユーザーのモバイルアプリが Secure Hub ウィンドウに表示されます。ユーザーは Secure Hub からアプリを起動できます。一部のアプリでは、ユーザーがモバイルデバイスにアプリをダウンロードしてインストールする必要があります。

前述のシナリオのいずれかで、ユーザーが Citrix Gateway 経由で接続する場合は、次の操作を行います。

- ユーザーは、Citrix Gateway プラグインまたは Citrix Workspace アプリを使用してログオンします。初めてログオンするには、ユーザーが Web ブラウザーを開き、Citrix Gateway または Citrix Workspace アプリの完全修飾ドメイン名（FQDN）を入力します。モバイルデバイスを持つユーザーは、Secure Hub を使用してログオンします。
- ログオンページで、ユーザーは自分の資格情報を入力し、認証されます。
- 認証後、ユーザーセッションは、展開環境に応じて StoreFront または Endpoint Management にリダイレクトされます。
- StoreFront と Endpoint Management の両方を展開する場合、Citrix Gateway は展開の最初のサーバーに接続します。たとえば、Endpoint Management で MDX モバイルアプリを構成する場合、Endpoint Management 背後に StoreFront を展開します。MDX モバイルアプリケーションへのアクセスを提供しない場合は、StoreFront の背後に Endpoint Management を展開します。
- ユーザーのデスクトップ、ドキュメント、Web、SaaS、Windows ベースのアプリケーションはすべて Citrix Workspace アプリまたは Secure Hub に表示されます。

Exchange、ファイル共有、内部 Web サイトなど、内部ネットワーク上の他のリソースにアクセスする必要がある場合は、Citrix Gateway プラグインを使用してログオンすることもできます。たとえば、ユーザーがネットワーク内の Microsoft Exchange サーバーに接続する場合、ユーザーは自分のコンピュータで Outlook を起動します。セキュアな接続は、Citrix Gateway に接続する Citrix Gateway プラグインを使用して行われます。SSL VPN トンネ

ルが Exchange Server に作成され、ユーザは自分の電子メールにアクセスできます。

> 重要：Citrix Gateway 仮想サーバーで認証を構成することをお勧めします。Citrix Gateway で認証を無効にすると、認証されていない HTTP リクエストが、内部ネットワークの Web Interface、StoreFront または Endpoint Management を実行しているサーバーに直接送信されます。

Citrix Endpoint Management、Citrix Virtual Apps、およびデスクトップを使用した展開

October 22, 2021

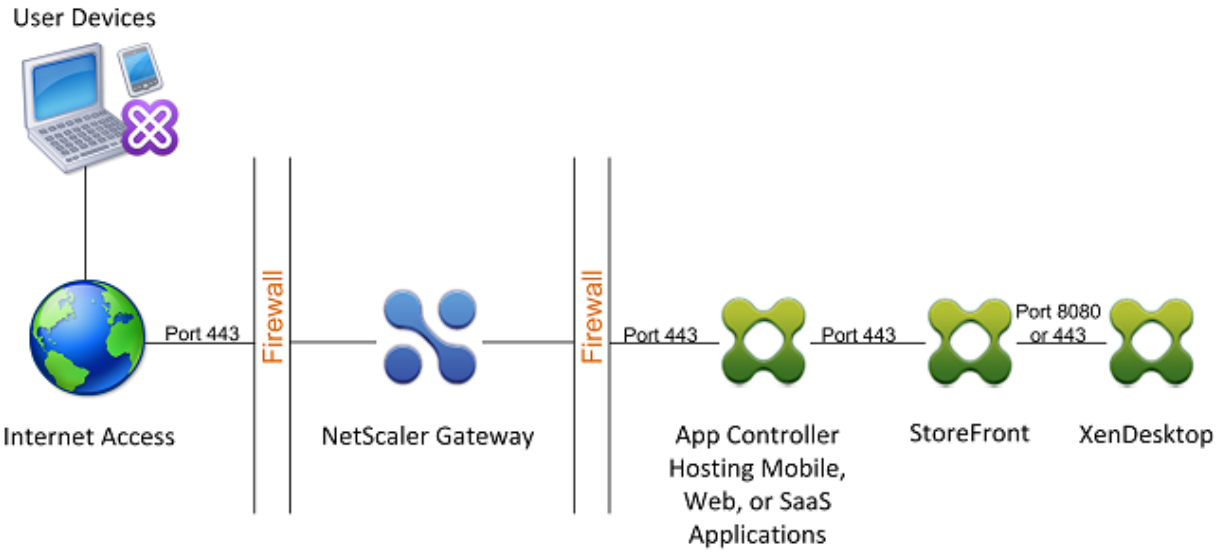
ユーザーは、Windows、Web、SaaS、およびモバイルアプリケーション、およびネットワークでホストされている仮想デスクトップに接続できます。Citrix Gateway、Citrix Endpoint Management、および Citrix Virtual Apps and Desktops を使用して、リモートユーザーおよび内部ユーザーにアプリケーションおよびデスクトップへのアクセスを提供できます。Citrix Gateway は、ユーザーを認証し、Citrix Workspace アプリまたは Secure Hub を使用してアプリケーションへのアクセスを許可します。

ユーザーは、Citrix Workspace アプリと StoreFront を使用して、Citrix Virtual Apps で公開された Windows ベースのアプリと Citrix Virtual Desktops で公開された仮想デスクトップに接続します。

Citrix Endpoint Management には、ユーザーが Web、SaaS、および MDX アプリケーションに接続できるようにする Citrix Endpoint Management が含まれています。Endpoint Management では、ShareFile ドキュメントとともに、シングルサインオン（SSO）用のウェブ、SaaS、MDX アプリケーションを管理できます。Endpoint Management は、内部ネットワークにインストールします。リモートユーザーは、Citrix Gateway を介して Endpoint Management に接続し、アプリケーションおよび ShareFile データにアクセスします。リモートユーザーは、Citrix Gateway プラグイン、Citrix Workspace アプリ、または Secure Hub のいずれかを使用して接続し、アプリケーションおよび ShareFile にアクセスできます。内部ネットワークにいるユーザーは、Citrix Workspace アプリを使用して Endpoint Management に直接接続できます。次の図は、Endpoint Management と StoreFront を使用して展開された Citrix Gateway を示しています。

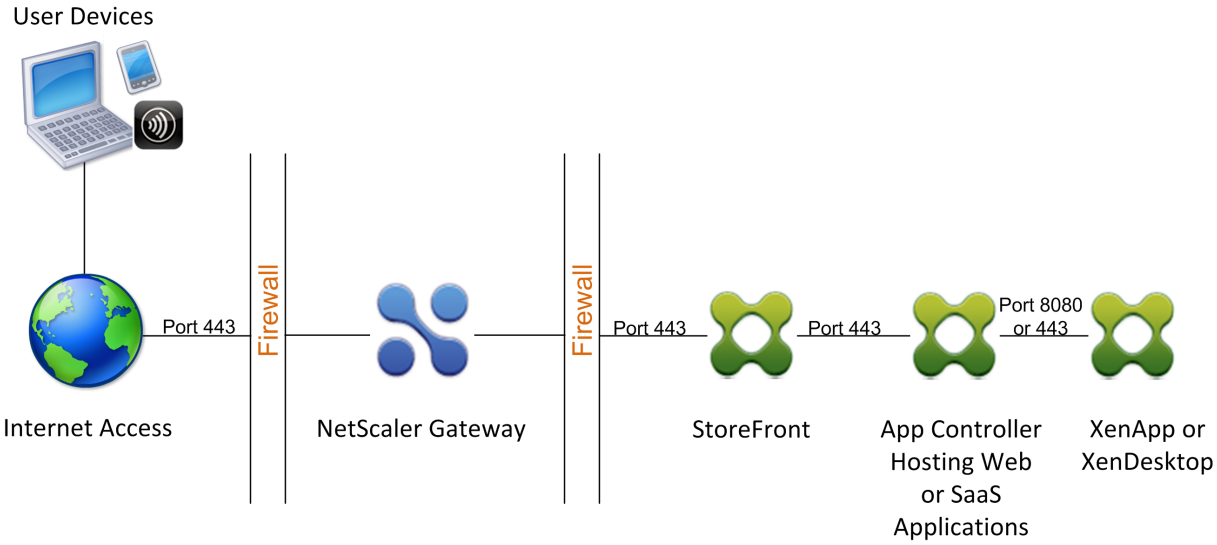
展開環境で、Endpoint Management から MDX アプリケーションにアクセスでき、StoreFront から Windows ベースのアプリケーションにアクセスできる場合は、次の図に示すように、StoreFront の前に Endpoint Management を展開します。

図 1：StoreFront の前で Endpoint Management を使用した Citrix Gateway の展開



展開環境で MDX アプリケーションへのアクセスが提供されていない場合、StoreFront は、次の図に示すように、Endpoint Management の前に存在します。

図 2: Endpoint Management の前で StoreFront を使用した Citrix Gateway の展開



展開するたびに、StoreFront と Endpoint Management が内部ネットワークに存在し、Citrix Gateway が DMZ に存在する必要があります。Endpoint Management の展開について詳しくは、「Endpoint Management インストール」を参照してください。

StoreFront の展開について詳しくは、「StoreFront」を参照してください。

Web Interface を使用した Citrix Virtual Apps and Desktops リソースへのアクセス

March 26, 2020

Citrix Virtual Apps and Desktops を実行している 1 台以上のコンピューターがサーバーファームを作成します。企業ネットワークにサーバーファームが含まれている場合は、Citrix Gateway を展開して、Web Interface を使用して公開アプリケーションまたは仮想デスクトップにセキュアなインターネットアクセスを提供できます。

このような展開では、Citrix Gateway は Web Interface および Secure Ticket Authorority（STA）と連携して、Citrix Virtual Apps を実行しているコンピューターでホストされている公開アプリケーションまたは Citrix Virtual Desktops が提供する仮想デスクトップへの認証、承認、リダイレクトを行います。

この機能は、Citrix Gateway と Web Interface、Citrix Virtual Apps、およびデスクトップを統合することによって実現されます。この統合により、高度な認証と Web Interface へのアクセス制御オプションが提供されます。Web Interface の詳細については、Citrix ドキュメントライブラリの Web Interface ドキュメントを参照してください。

サーバーファームへのリモート接続には、Citrix Gateway プラグインは必要ありません。公開アプリケーションまたはデスクトップにアクセスするには、ユーザーは Citrix Workspace アプリを使用して接続します。

Citrix Gateway と Citrix Virtual Apps and Desktops の統合

April 9, 2020

ユーザー接続用に Citrix Gateway を構成する場合、Citrix 仮想アプリ、Citrix Virtual Desktops、またはその両方へのネットワークトラフィックの設定を含めることができます。これを行うには、Citrix Gateway と Web Interface が相互に通信するように構成します。

これらの製品を統合するためのタスクは次のとおりです。

- Citrix Virtual Apps and Desktops ファームで Web Interface サイトを作成する。
- Citrix Gateway 経由でユーザー接続をルーティングするための Web Interface 内の設定を構成する。
- Web Interface および Secure Ticket Authority（STA）と通信するように Citrix Gateway を構成する。

また、ダブルホップ DMZ に Citrix Gateway を展開することで、Citrix Virtual Apps サーバーファームと通信するように Citrix Gateway を構成することもできます。詳しくは、「ダブルホップ DMZ での Citrix Gateway の展開」を参照してください。

Citrix Gateway および Web Interface は、STA および Citrix XML サービスを使用してユーザー接続を確立します。STA および XML サービスは、Citrix Virtual Apps and Desktops サーバー上で実行されます。

サーバファームへのセキュアな接続の確立

March 26, 2020

以下の例は、DMZ にデプロイされた Citrix Gateway が Web Interface と連携して、セキュアなエンタープライズネットワークで使用可能な公開リソースへのセキュアな単一アクセスポイントを提供する方法を示しています。

この例では、次のすべての条件が存在します。

- インターネットからのユーザーデバイスは、Citrix Workspace アプリを使用して Citrix Gateway に接続します。
- Web Interface は、安全なネットワーク内の Citrix Gateway の背後に存在します。ユーザーデバイスによって Citrix Gateway への初期接続が確立され、その接続が Web Interface に渡されます。
- セキュアネットワークには、サーバファームが含まれています。このサーバーファーム内の 1 つのサーバーが、Secure Ticket Authority（STA）と Citrix XML サービスを実行します。STA と XML サービスは、Citrix Virtual Apps and Desktops のいずれかで実行できます。

プロセスの概要**:** サーバーファームで公開されたリソースへのユーザーアクセス

1. リモートユーザーは、Citrix Gateway のアドレス（例: `https://www.ag.wxyco.com`）を Web ブラウザのアドレスフィールドに入力します。ユーザーデバイスは、ポート 443 でこの SSL 接続を試行します。接続が成功するには、ファイアウォールを介して開かれている必要があります。
2. Citrix Gateway は接続要求を受信し、ユーザーに資格情報の入力を求められます。資格情報は Citrix Gateway 経由で戻され、ユーザーが認証され、接続が Web Interface に渡されます。
3. Web Interface は、サーバーファームで実行されている Citrix XML サービスにユーザーの資格情報を送信します。
4. XML サービスは、ユーザーの資格情報を認証し、ユーザーがアクセスを許可されている公開アプリケーションまたはデスクトップのリストを Web Interface に送信します。
5. Web Interface では、ユーザーがアクセスを許可されている公開リソース（アプリケーションまたはデスクトップ）のリストが Web ページに入力され、この Web ページをユーザーデバイスに送信します。
6. ユーザーが公開アプリケーションまたはデスクトップリンクをクリックします。ユーザーがクリックした公開リソースを示す HTTP リクエストが Web Interface に送信されます。
7. Web インタフェースは、XML サービスと対話し、公開されたリソースが実行されているサーバーを示すチケットを受け取ります。
8. Web Interface は、セッション・チケット要求を STA に送信します。この要求は、公開リソースが実行されるサーバーの IP アドレスを指定します。STA がこの IP アドレスを保存し、要求されたセッションチケットを Web Interface に送信します。
9. Web Interface により、STA が発行したチケットを含む ICA ファイルが生成され、ユーザーデバイスの Web ブラウザに送信されます。Web Interface によって生成された ICA ファイルには、Citrix Gateway の完全修飾ドメイン名（FQDN）またはドメインネームシステム（DNS）名が含まれています。要求されたリソースを実行しているサーバーの IP アドレスがユーザーに公開されることはありません。

10. ICA ファイルには、Web ブラウザに Citrix Workspace アプリを起動するように指示するデータが含まれています。ユーザーデバイスは、ICA ファイル内の Citrix Gateway の FQDN または DNS 名を使用して Citrix Gateway に接続します。初期 SSL/TLS ハンドシェイクが実行され、Citrix Gateway のアイデンティティが確立されます。
11. ユーザーデバイスがセッションチケットを Citrix Gateway に送信し、Citrix Gateway が STA に接続してチケットの検証を行います。
12. STA は、要求されたアプリケーションが存在するサーバーの IP アドレスを Citrix Gateway に返します。
13. Citrix Gateway は、サーバーへの TCP 接続を確立します。
14. Citrix Gateway はユーザーデバイスとの接続ハンドシェイクを完了し、サーバーとの接続が確立されたことをユーザーデバイスに通知します。ユーザーデバイスとサーバー間のトラフィックはすべて、Citrix Gateway を介してプロキシされます。ユーザーデバイスと Citrix Gateway の間のトラフィックは暗号化されます。Citrix Gateway とサーバー間のトラフィックは個別に暗号化できますが、デフォルトでは暗号化されません。

Web Interface を使用したデプロイ

April 9, 2020

Citrix Gateway を展開して CitrixCitrix Virtual Apps and Desktops へのセキュアなリモートアクセスを提供する場合、Citrix Gateway は Web Interface および Secure Ticket Authorority（STA）と連携して、サーバーファームでホストされている公開アプリケーションおよびデスクトップへのアクセスを提供します。

DMZ での Citrix Gateway の展開は、Citrix Gateway がサーバーファームで動作する場合の最も一般的な構成です。この構成では、Citrix Gateway は、Web ブラウザーと Citrix Workspace アプリに対して、Web Interface を介して公開されたリソースにアクセスするための安全な単一アクセスポイントを提供します。このセクションでは、この展開オプションに関する基本的な側面について説明します。

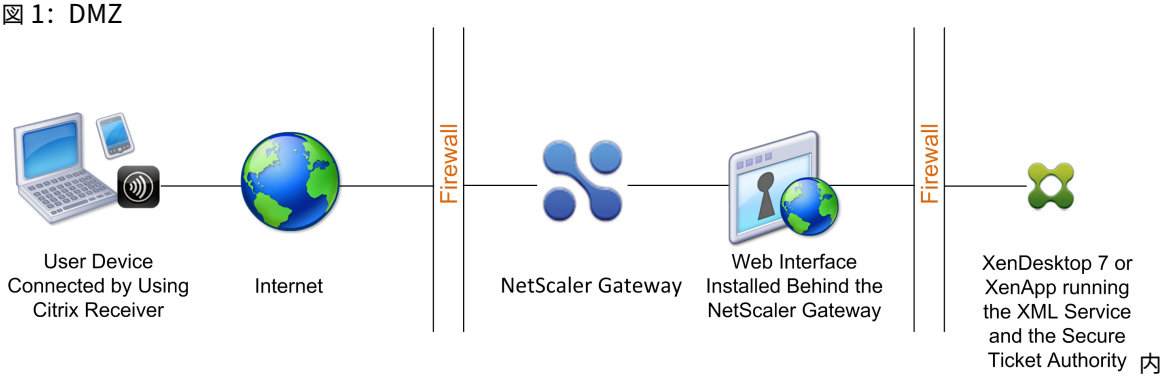
組織のネットワーク構成によって、Citrix Gateway がサーバーファームで動作する場合の展開場所が決まります。次の 2 つのオプションが使用できます:

- 組織が単一の DMZ で内部ネットワークを保護する場合は、DMZ に Citrix Gateway を展開します。
- 組織が 2 つの DMZ を使用して内部ネットワークを保護する場合は、ダブルホップ DMZ 構成内の 2 つのネットワークセグメントそれぞれに 1 つの Citrix Gateway を展開します。詳しくは、「ダブルホップ DMZ での Citrix Gateway の展開」を参照してください。
  注：セキュアネットワーク内の 2 番目の Citrix Gateway アプライアンスでダブルホップ DMZ を構成することもできます。

サーバーファームへのリモートアクセスを提供するために Citrix Gateway を DMZ に展開する場合、以下の 3 つの展開オプションのいずれかを実装できます。

- DMZ 内の Citrix Gateway の背後にある Web Interface を展開します。この構成では、次の図に示すように、Citrix Gateway と Web Interface の両方が DMZ に展開されます。最初のユーザー接続は Citrix Gateway に送信され、Web Interface にリダイレクトされます。

図 1: DMZ



内の Citrix Gateway の背後にある Web Interface

- DMZ の Web Interface と並行して Citrix Gateway を展開します。この構成では、Citrix Gateway と Web Interface の両方が DMZ に展開されますが、最初のユーザー接続は Citrix Gateway ではなく Web Interface に送信されます。
- DMZ に Citrix Gateway を展開し、内部ネットワークに Web Interface を展開します。この構成では、Citrix Gateway はユーザーの要求を認証してから、セキュリティで保護されたネットワーク内の Web Interface に要求を中継します。Web Interface は認証を実行しませんが、STA と対話して ICA ファイルを生成し、ICA トラフィックが Citrix Gateway 経由でサーバーファームにルーティングされるようにします。

Web Interface を展開する場所は、次のようなさまざまな要因によって異なります。

- 認証。ユーザーがログオンすると、Citrix Gateway または Web Interface でユーザーの資格情報を認証できます。Web Interface をネットワークに配置することは、ユーザーが認証する場所を部分的に決定する要素です。
- ユーザーソフトウェア。ユーザーは、Citrix Gateway プラグインまたは Citrix Workspace アプリを使用して Web Interface に接続できます。Citrix Workspace アプリのみを使用してユーザーがアクセスできるリソースを制限したり、Citrix Gateway プラグインを使用してユーザーにネットワークアクセスを強化したりできます。ユーザーの接続方法、およびユーザーの接続を許可するリソースは、ネットワーク内の Web Interface を展開する場所を決定するのに役立ちます。

セキュアネットワークでの **Web Interface** の展開

March 26, 2020

この展開では、Web Interface は安全な内部ネットワークに存在します。Citrix Gateway は DMZ にあります。Citrix Gateway は、Web Interface にリクエストを送信する前に、ユーザーのリクエストを認証します。

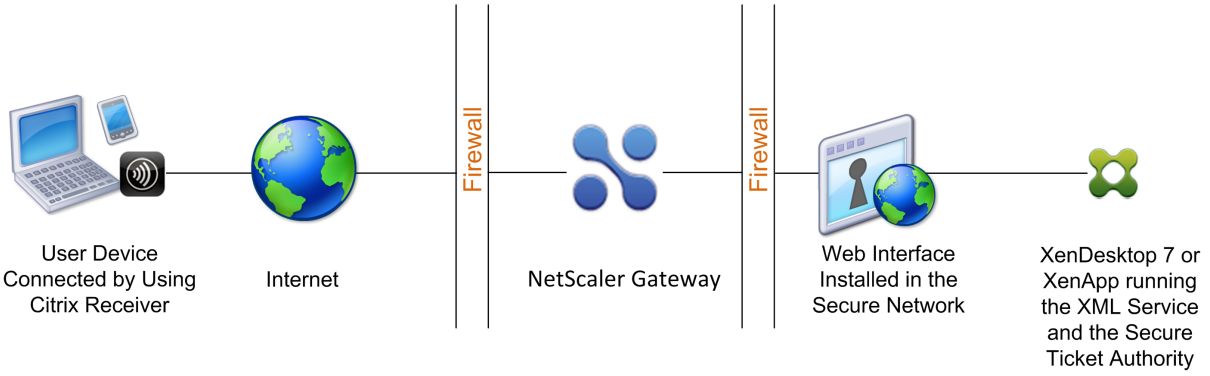
セキュリティで保護されたネットワークに Web Interface を展開する場合は、Citrix Gateway で認証を構成する必要があります。

Citrix Virtual Apps and Desktops を使用して Web Interface を展開する場合、Web Interface をセキュリティで保護されたネットワークに展開することがデフォルトの展開シナリオです。デスクトップ Delivery Controller ー

をインストールすると、カスタムバージョンの Web Interface もインストールされます。

> 重要:
> Web Interface が安全なネットワーク内にある場合は、Citrix Gateway で認証を有効にする必要があります。ユーザーは、Citrix Gateway に接続し、資格情報を入力して、Web Interface に接続します。認証を無効にすると、認証されていない HTTP 要求は Web Interface を実行しているサーバーに直接送信されます。Citrix Gateway での認証を無効にするのは、Web Interface が DMZ 内にあり、ユーザーが Web Interface に直接接続する場合のみです。

図 1: セキュアなネットワーク内にある Web Interface



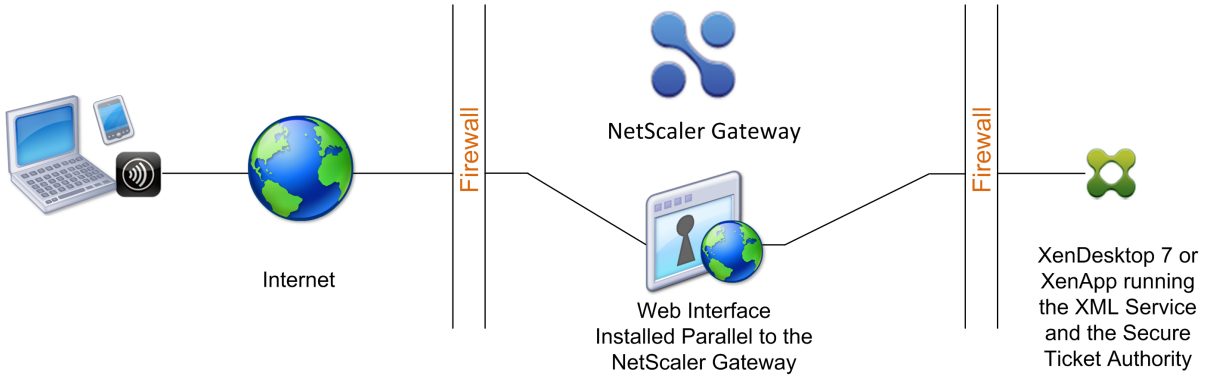
DMZ での Citrix Gateway と並行して Web インターフェイスを展開する

March 26, 2020

この展開では、Web Interface と Citrix Gateway の両方が DMZ に存在します。ユーザーは、Web ブラウザーまたは Citrix Workspace アプリを使用して Web Interface に直接接続します。ユーザー接続は、最初に認証のために Web Interface に送信されます。認証後、接続は Citrix Gateway 経由でルーティングされます。ユーザーは、Web Interface に正常にログオンすると、サーバーファーム内の公開アプリケーションまたはデスクトップにアクセスできます。ユーザーがアプリケーションまたはデスクトップを起動すると、Web Interface によって ICA ファイルが送信されます。このファイルは、Secure Gateway Gateway を実行しているサーバーであるかのように Citrix Gateway 経由で ICA トラフィックをルーティングする手順が含まれています。Web Interface によって配信される ICA ファイルには、Secure Ticket Authority（STA）によって生成されたセッションチケットが含まれています。

Citrix Workspace アプリが Citrix Gateway に接続すると、チケットが表示されます。Citrix Gateway は STA に接続し、セッションチケットを検証します。チケットがまだ有効な場合、ユーザーの ICA トラフィックはサーバーファーム内のサーバーに中継されます。次の図は、この展開を示しています。

図 1: Citrix Gateway と並行してインストールされる Web Interface



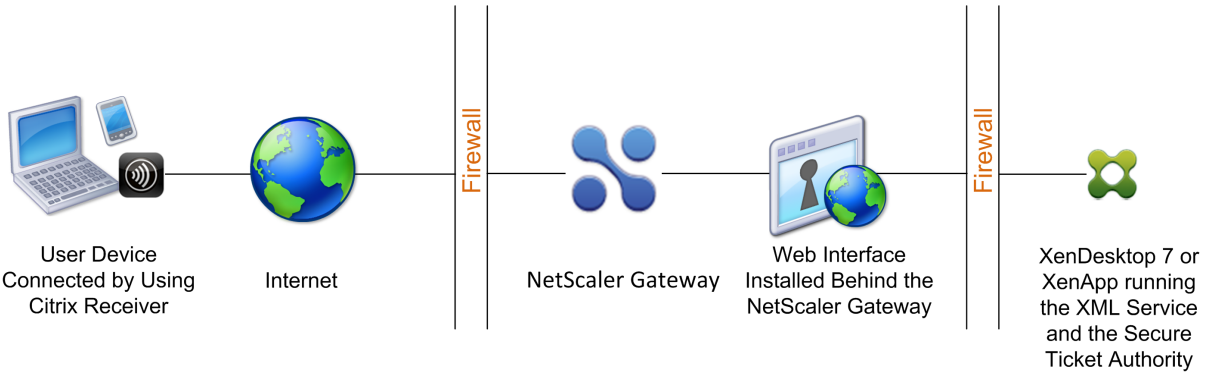
Web Interface が DMZ で Citrix Gateway と並行して実行されている場合は、Citrix Gateway で認証を構成する必要はありません。Web Interface はユーザーを認証します。

DMZ での Citrix Gateway の背後にある Web インターフェイスの展開

March 26, 2020

この構成では、Citrix Gateway と Web Interface の両方が DMZ に展開されます。ユーザーが Citrix Workspace アプリでログオンすると、最初のユーザー接続は Citrix Gateway に送信され、Web Interface にリダイレクトされます。すべての HTTPS および ICA トラフィックを単一の外部ポート経由でルーティングし、単一の SSL 証明書の使用を要求するには、Citrix Gateway は Web Interface のリバース Web プロキシとして機能します。

図 1: Citrix Gateway の背後にある Web Interface



Web Interface を DMZ の Citrix Gateway の背後に展開する場合、アプライアンス上で認証を構成することはできますが、必須ではありません。両方が DMZ に存在するため、Citrix Gateway または Web Interface でユーザーを認証できます。

Web Interface サイトの動作設定

March 26, 2020

Web Interface を使用すると、ユーザーは Citrix Virtual Apps アプリケーションやコンテンツ、および Citrix Virtual Desktops にアクセスできます。ユーザーは、標準の Web ブラウザまたは Citrix Workspace アプリを使用して、公開アプリケーションおよびデスクトップにアクセスします。

アクセス管理コンソールを使用して Web Interface 5.1 サイトを構成し、Web Interface 管理コンソールを使用して、バージョン 5.2、5.3、および 5.4 の Web Interface サイトを作成できます。コンソールは、Windows ベースのプラットフォームにのみインストールできます。

Citrix Gateway と連携するように Web Interface を構成するには、以下を実行する必要があります。

- 使用しているバージョンの Web Interface サイトを作成します。
- Web Interface で設定を行います。
- Citrix Gateway で Web Interface 設定を構成します。

Web Interface の機能

March 26, 2020

Citrix Gateway で動作するように Web Interface を構成する前に、Citrix Virtual Apps の Web サイトと Citrix Virtual Apps サービスサイトの違いを理解する必要があります。

- **Citrix Virtual Apps Web** サイト。Web Interface は、Citrix Virtual Apps Web サイトを作成および管理するための機能を提供します。ユーザーは、Web ブラウザとプラグインを使用して、公開リソースやストリーム配信アプリケーションにリモートでアクセスします。
- **Citrix Virtual Apps** サービスサイト。Citrix Virtual Apps は、柔軟性と構成の容易さを考慮して設計されたプラグインです。Citrix Virtual Apps を Web Interface 上の Citrix Virtual Apps サービスサイトと組み合わせて使用することで、公開リソースをユーザーのデスクトップと統合できます。ユーザーは、デスクトップまたは [スタート] メニューのアイコンをクリックするか、コンピュータデスクトップの通知領域をクリックして、リモートアプリケーションとストリームアプリケーション、およびリモートデスクトップとコンテンツにアクセスします。オーディオ、ディスプレイ、ログオンの設定など、ユーザーがアクセスして変更できる構成オプションを決定できます。

  > 注：このオプションを選択すると、仮想デスクトップへのアクセスはサポートされていません。

詳細については、Citrix eDocs ライブラリの［テクノロジ］ノードにある Web Interface のドキュメントを参照してください。

Web Interface のサイトのセットアップ

April 9, 2020

セキュアなネットワークに Web Interface を展開し、Citrix Gateway で認証を構成すると、ユーザーが Citrix Gateway に接続すると、アプライアンスはユーザーを認証します。

> 重要：Citrix Gateway を構成する前に、Web Interface をインストールして構成してください。詳細については、Citrix eDocs ライブラリの［
> テクノロジ］ノードにある Web Interface のドキュメントを参照してください。

Web Interface サイトを作成する手順は次のとおりです。

- ユーザーのログオン方法を選択します。これは、Web ブラウザ、Citrix Gateway プラグイン、または Citrix Workspace アプリを介して行うことができます。詳細については、Web Interface の機能を参照してください。
- ユーザーの認証元を特定します。Citrix Gateway または Web Interface。

> 注：Web Interface がセキュアなネットワーク内にある場合は、Citrix Gateway の仮想サーバーで認証を有効にします。認証を無効にすると、認証されていない HTTP 要求は Web Interface を実行しているサーバーに直接送信されます。Citrix Gateway での認証を無効にするのは、Web Interface が DMZ 内にあり、ユーザーが Web Interface に直接接続する場合のみです。

Citrix Gateway に有効なサーバー証明書をインストールしてください。証明書の取り扱いについて詳しくは、「証明書のインストールと管理」を参照してください。

> 重要：Web Interface を Citrix Gateway 10.1 で正しく動作させるには、Web Interface を実行するサーバーが Citrix Gateway 証明書を信頼し、仮想サーバーの完全修飾ドメイン名（FQDN）を正しい IP アドレスに解決できる必要があります。

Web Interface 5.4 サイトの作成

March 26, 2020

Citrix Web Interface 管理コンソールは、Microsoft 管理コンソール（MMC）3.0 スナップインで、Microsoft インターネットインフォメーションサービス（IIS）でホストされている Citrix Virtual Apps Web サイトおよび Citrix Virtual Apps サービスサイトを作成および構成できます。Web Interface サイトの種類は、左側のウィンドウに表示されます。中央の結果ウィンドウには、左側のウィンドウで選択したサイトタイプコンテナ内で使用可能なサイトが表示されます。

Citrix Web Interface 管理コンソールを使用すると、日常の管理タスクをすばやく簡単に実行できます。[操作] ウィンドウには、現在使用可能なタスクが一覧表示されます。左ペインで選択したアイテムに関連するタスクが上部に表示され、結果ペインで選択したアイテムに対して使用可能なアクションが下に表示されます。

コンソールを使用する場合、コンソールを使用して変更をコミットすると、設定が有効になります。その結果、一部の Web Interface 設定は、その値が現在の構成に関連せず、対応する設定が WebInterface.conf のデフォルト値にリセットされると、無効になることがあります。サイトの WebInterface.conf ファイルと config.xml ファイルのバックアップを定期的に作成することをお勧めします。

Microsoft インターネットインフォメーションサービス用の Web Interface をインストールすると、Citrix Web Interface Management コンソールが自動的にインストールされます。［スタート］＞［すべてのプログラム］＞［Citrix］＞［管理コンソール］＞［Citrix Web Interface 管理］の順にクリックして、コンソールを実行します。

> 注:
> Web Interface をインストールするサーバー上に MMC 3.0 がインストールされていることを確認する必要があります。これは、Citrix Web Interface 管理コンソールをインストールするための前提条件です。MMC 3.0 は、Web Interface のホストでサポートされているすべての Windows プラットフォームで既定で使用できます。

設定ファイルの使用

Web Interface サイトを構成するには、次の構成ファイルを編集できます。

- Web Interface 構成ファイル：Web Interface 構成ファイル WebInterface.conf を使用すると、多くの Web Interface のプロパティを変更できます。これは、Microsoft インターネットインフォメーションサービス (IIS) と Java アプリケーションサーバーの両方で使用できます。このファイルを使用して、日常的な管理タスクを実行し、さらに多くの設定をカスタマイズできます。WebInterface.conf の値を編集し、更新したファイルを保存して変更を適用します。WebInterface.conf を使用して Web Interface を構成する方法の詳細については、Citrix eDocs のテクノロジノードにある Web Interface のドキュメントを参照してください。
- Citrix オンライン・プラグイン構成ファイル。Citrix オンラインプラグインは、Web Interface サーバー上の config.xml ファイルを使用して構成できます。

Citrix Web Interface 管理コンソールを使用したサイトの構成

March 26, 2020

Citrix Web Interface 管理コンソールは、Microsoft 管理コンソール（MMC）3.0 スナップインで、Microsoft インターネットインフォメーションサービス（IIS）でホストされている Citrix Virtual Apps Web サイトおよび Citrix Virtual Apps サービスサイトを作成および構成できます。Web Interface サイトの種類は、左側のウィンドウに表示されます。中央の結果ウィンドウには、左側のウィンドウで選択したサイトタイプコンテナ内で使用可能なサイトが表示されます。

Citrix Web Interface 管理コンソールを使用すると、日常の管理タスクをすばやく簡単に実行できます。[操作] ウィンドウには、現在使用可能なタスクが一覧表示されます。左ペインで選択したアイテムに関連するタスクが上部に表示され、結果ペインで選択したアイテムに対して使用可能なアクションが下に表示されます。

コンソールを使用する場合、コンソールを使用して変更をコミットすると、設定が有効になります。その結果、一部の Web Interface 設定は、その値が現在の構成に関連せず、対応する設定が WebInterface.conf のデフォルト値にリセットされると、無効になることがあります。サイトの WebInterface.conf ファイルと config.xml ファイルのバックアップを定期的に作成することをお勧めします。

Citrix Web Interface 管理コンソールは、Microsoft IIS 用 Web Interface をインストールすると自動的にインストールされます。［スタート］＞［すべてのプログラム］＞［Citrix］＞［管理コンソール］＞［Citrix Web Interface 管理］の順にクリックして、コンソールを実行します。

注：Web Interface をインストールするサーバー上に MMC 3.0 がインストールされていることを確認する必要があります。これは、Citrix Web Interface 管理コンソールをインストールするための前提条件です。MMC 3.0 は、Web Interface のホストでサポートされているすべての Windows プラットフォームで既定で使用できます。

Web Interface5.4 での Citrix Gateway 設定の構成

March 26, 2020

展開環境で Citrix Gateway を使用するには、アプライアンスをサポートする Web Interface を構成する必要があります。これを行うには、Citrix Web Interface 管理コンソールでセキュリティで保護されたアクセスタスクを使用します。

Web Interface で Citrix Gateway 設定を構成するには

1. Windows の [スタート] メニューで、[すべてのプログラム] > [Citrix 管理コンソール] > [Citrix Web Interface 管理] の順にクリックします。

2. Citrix Web Interface 管理コンソールの左側のペインで、［Citrix Virtual Apps Web サイト］または［Citrix Virtual Apps サービスサイト］のいずれかをクリックし、結果ペインでサイトを選択します。

3. [操作] ウィンドウで、[セキュリティで保護されたアクセス] をクリックします。

4. [アクセス方法の指定] ページで、次のいずれかの操作を行います。

   - [Add] をクリックして、新しいアクセスルートを追加します。
   - リストから既存のルートを選択し、[Edit] をクリックします。

5. [アクセス方法] ボックスの一覧で、次のいずれかのオプションを選択します。

   - Citrix サーバーの実際のアドレスを Citrix Gateway に送信する場合は、「Citrix Gateway ダイレクト」を選択します。
   - Citrix Virtual Apps サーバーの代替アドレスを Citrix Gateway に送信する場合は、「Citrix Gateway の代替」を選択します。

     注：代替アドレスが使用されている場合、Citrix Virtual Desktops にはアクセスできません。

- Citrix Gateway に指定されたアドレスを、Web Interface で設定されたアドレス変換マッピングによって決定する場合は、「ゲートウェイ変換」を選択します。

6. クライアントネットワークを識別するネットワークアドレスとサブネットマスクを入力します。[Move Up] ボタンと [Move Down] ボタンを使用して、[User device addresses] テーブルでアクセスルートを優先度順に配置し、[Next] をクリックします。

7. Gateway アドレス変換を使用していない場合は、ステップ 10 に進みます。Gateway アドレス変換を使用している場合は、[アドレス変換の指定] ページで次のいずれかの操作を行います。

- [Add] をクリックして、新しいアドレス変換を追加します。
- リストから既存のアドレス変換を選択し、[Edit] をクリックします。

8. [アクセスタイプ] 領域で、次のいずれかのオプションを選択します。

- Citrix Gateway で変換されたアドレスを使用して Citrix サーバーに接続する場合は、［ゲートウェイルート変換］を選択します。
- ［ユーザーデバイスアドレス］テーブルでクライアント変換ルートを構成し、Citrix クライアントと Citrix Gateway の両方で変換されたアドレスを使用して Citrix サーバーに接続する場合は、［ユーザーデバイスと Gateway のルート変換］を選択します。

9. Citrix サーバーの内部ポートと外部（変換済み）ポートとアドレスを入力し、[OK] をクリックし、[次へ] をクリックします。
Citrix Gateway は、Citrix サーバーに接続するときに、外部ポート番号とアドレスを使用します。作成するマッピングが、サーバー・ファームで使用されているアドレッシングのタイプと一致していることを確認します。

10. ［ゲートウェイ設定の指定］ページで、クライアントが使用する必要のある Citrix Gateway アプライアンスの完全修飾ドメイン名（FQDN）とポート番号を指定します。FQDN は、Gateway にインストールされている証明書の内容と一致する必要があります。

11. クライアントが自動的に再接続を試行する間、切断されたセッションを開いたままにする場合は、Citrix セッションの画面の保持を有効にする］を選択します。

12. セッション画面の保持を有効にし、2 台の STA（Secure Ticket Authorority）サーバーから同時にチケットを発行する場合は、「2 つの STA からチケットを要求する」を選択します。このオプションを有効にすると、Web Interface は 2 つの異なる STA からチケットを取得し、セッション中に 1 つの STA が使用できなくなっても、ユーザー・セッションが中断されないようにします。何らかの理由で Web Interface が 2 つの STA に接続できない場合は、1 つの STA を使用するようにフォールバックします。［次へ］をクリックします。

13. [Secure Ticket Authority 設定の指定] ページで、次のいずれかの操作を行います。

- 「追加」をクリックして、Web インタフェースが使用できる STA の URL を指定します。
- リストからエントリを選択し、[Edit] をクリックします。

[上へ移動] ボタンと [下へ移動] ボタンを使用して、STA を優先順に配置します。
STA は、Citrix XML サービスに含まれています（例: `http\[s\]://servername.domain.com/scripts/ctxsta.dll`）。

フォールトトレランスには複数の STA を指定できますが、この目的には外部ロードバランサーを使用しないことをお勧めします。

14. STA 間のロード・バランシングを有効にするかどうかを選択するには、「ロード・バランシングに使用」を選択します。

負荷分散を有効にすると、1 台のサーバーが過負荷にならないように、サーバー間で接続を均等に分散できます。

15. 到達不能な STA をバイパスする期間を指定するには、[障害が発生したサーバをバイパスする] を選択します。

Web Interface は、STA URL リストのサーバー間にフォールト・トレランスを提供するため、通信エラーが発生した場合、指定された期間にわたって障害が発生したサーバーはバイパスされます。

Web Interface 5.3 サイトの作成

March 26, 2020

Web Interface 5.3 サイトを作成するときに、Web ブラウザー、Citrix Workspace アプリ、または Citrix デスクトップ Citrix Workspace アプリのいずれかを使用してログオンするようにユーザーに要求できます。Citrix Web Interface 管理コンソールを使用して、複数の Web Interface サイトを作成できます。

Web Interface 5.3 を使用した Web Interface に対しては、スマートカードを使用したシングルサインオンのみを有効にできます。このバージョンの Web Interface は、Citrix Virtual Apps 4.5、5.0、6.0 で実行できます。

Web Interface 5.3 は、次のオペレーティングシステムで実行されます。

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

> 注:
> Citrix Virtual Apps 6.0 は、Windows サーバー 2008 R2 でのみ実行されます。

Web Interface 5.3 のサイトを作成するには

1. ［スタート］＞［すべてのプログラム］＞［Citrix］＞［管理コンソール］＞［Citrix Web Interface 管理］の順にクリックします。
2. 左側のペインで、［Citrix Virtual Apps］［Web サイト］を選択します。ユーザーは、Web ブラウザを使用して Web Interface にログオンします。
3. [操作] メニューの [サイトの作成] をクリックします。
4. 既定のインターネットインフォメーションサービス (IIS) サイトとパスをそのまま使用し、[次へ] をクリックします。

   デフォルトのサイトパスは/Citrix/Citrix Virtual Apps です。パスを指定することもできます。

> 注:
> デフォルトパスを使用する既存の Citrix Virtual Apps Web サイトがある場合は、新しいサイトを区別するために適切な増分が追加されます。

5. 「ユーザー認証を実行する場所の指定」で、次のいずれかを選択します。
   - Web Interface で、ユーザーが Web Interface を使用して認証するようにします。

     Web Interface が、非武装地帯（DMZ）で Citrix Gateway と並行するスタンドアロンサーバーとして展開される場合は、このオプションを選択します。
   - Access Gateway で、Citrix Gateway アプライアンスを使用してユーザーを認証します。

     このオプションを選択した場合、Citrix Gateway はユーザーを認証し、Web Interface がアプライアンス上で構成されている場合、Web Interface へのシングルサインオンを開始します。

   > 注:
   > Citrix Gateway で SmartAccess が構成されている場合、この設定では Citrix Virtual Apps and Desktops で SmartAccess が有効になります。
6. [次へ] をクリックします。
7. 手順 5 の「認証サービスの URL」に、Citrix Gateway 認証サービスの URL への Web アドレス（`https://access.company.com/CitrixAuthService/AuthService.asmx`など）を入力し、「次へ」をクリックします。
8. [認証オプション] で、ユーザーのログオン方法を選択します。
   - 明示的。ユーザーは、Web ブラウザーを使用してログオンします。
   - スマートカード。ユーザーは、スマートカードを使用してログオンします。
9. [次へ] をクリックします。
10. 手順 8 で [スマートカード] を選択した場合は、次のいずれかを選択します。

```
1 - ユーザーにPINを要求します。ユーザーは、公開アプリケーションまたはデスクトップを起動するときに、個人識別番号 (PIN) を入力します。
2 - 公開アプリケーションまたはデスクトップを起動するときに、ユーザーは PIN を入力する必要はありません。
```

設定を示す概要画面が表示されます。[
次へ] をクリックして、Web Interface サイトを作成します。サイトが正常に作成されると、Web Interface の残りの設定を構成するように求められます。ウィザードの指示に従って構成を完了します。

Web Interface5.3 での Citrix Gateway 設定の構成

March 26, 2020

Web Interface 5.3 サイトを作成したら、Citrix Web Interface 管理を使用して Citrix Gateway の設定を構成できます。

Citrix Gateway の Web Interface5.3 設定を構成するには

1. ［スタート］＞［すべてのプログラム］＞［Citrix］＞［管理コンソール］＞［Citrix Web Interface 管理］の順にクリックします。
2. Citrix の Web Interface 管理の左側のペインで、［Citrix 仮想アプリケーションの Web サイト］をクリックします。
3. [操作] ウィンドウで、[セキュリティで保護されたアクセス] をクリックします。
4. ［セキュアアクセス設定の編集］ダイアログボックスの［追加］をクリックします。
5. [アクセスルートの追加] ダイアログボックスで、ユーザーデバイスアドレス、サブネットマスクを入力し、[アクセス方法] で [ゲートウェイダイレクト] を選択し、[OK] をクリックして、[次へ] をクリックします。ユーザーデバイスアドレスとサブネットマスクを指定しない場合、「Gateway direct」オプションはすべてのユーザーデバイスに適用されます。「Gateway direct」オプションは、内部ネットワークの外部から接続するユーザーデバイスに適しています。一方、「Direct」オプションは、内部ネットワーク内から接続するユーザーデバイスに適しています。
6. ［アドレス（FQDN）］に、Citrix Gateway の完全修飾ドメイン名（FQDN）を入力します。これは、Citrix Gateway 証明書で使用されているのと同じ FQDN である必要があります。
7. ［Port］ボックスにポート番号を入力します。デフォルトは 443 です。
8. セッションの画面の保持を有効にするには、[セッション画面の保持を有効にする] をクリックし、[次へ] をクリックします。
9. 「Secure Ticket Authority URL」で、「追加」をクリックします。
10. ［Secure Ticket Authority URL］に、Citrix Virtual Apps XML サービスを実行するマスターサーバーの名前を入力し、［OK］をクリックし、［完了］をクリックします。たとえば、`http://Citrix Virtual Appssrv01/Scripts/CtxSta.dll`と入力します。

Web Interface で設定を構成したら、Citrix Gateway で設定を構成できます。

単一のサイトへの Citrix Virtual Apps and Desktops の追加

March 26, 2020

Citrix Virtual Apps and Desktops を実行している場合は、両方のアプリケーションを 1 つの Web Interface サイトに追加できます。この構成では、Citrix Virtual Apps and Desktops から同じ Secure Ticket Authority（STA）サーバーを使用できます。

> 注:

> Citrix Virtual Desktops は Web Interface をサポートしています。Web Interface の最低限必要なバージョンは 5.0 です。

Web Interface 5.3 または 5.4 を使用している場合は、Web Interface 管理コンソールを使用して Citrix Virtual Apps and Desktops サイトを組み合わせます。

> 注:
> サーバーファームが異なるドメインにある場合は、ドメイン間で双方向の信頼を確立する必要があります。

Web Interface 5.3 または **5.4** を使用して **Citrix Virtual Apps and Desktops** を単一のサイトに追加するには

1. ［スタート］＞［すべてのプログラム］＞［**Citrix**］＞［管理コンソール］＞［**Citrix Web Interface** 管理］の順にクリックします。
2. 左側のペインで、［**Citrix Virtual Apps**］［**Web** サイト］を選択します。
3. [操作] ウィンドウで、サイトを右クリックし、[サーバーファーム] をクリックします。
4. [サーバーファームの管理] ダイアログボックスで、[追加] をクリックします。
5. サーバーファームの設定を完了し、[**OK**] を 2 回クリックします。

Citrix Virtual Desktops を使用する場合は、WebInterface.conf 構成ファイルで「ユーザーインターフェイスのブランディング」の設定を「デスクトップ」に変更します。

Citrix Gateway を介したユーザー接続のルーティング

October 22, 2021

Citrix Virtual Apps and Desktops では、Citrix Gateway 経由でルーティングされる接続のみを受け入れるようにサーバーを構成できます。Citrix XenApp 6.5 では、CitrixCitrix Gateway 経由で接続をルーティングするように Citrix アプリケーションセンターでポリシーを構成します。Citrix Virtual Desktops 7.1 では、Citrix Studio を使用して設定を構成します。

Citrix Gateway 経由でルーティングされた接続のみを受け付けるように **Citrix XenApp 6.5** サーバーのプロパティを構成するには

1. ［スタート］＞［管理ツール］＞［Citrix］＞［管理コンソール］＞［Citrix AppCenter］の順にクリックします。
2.「NetScaler リソース」>「Citrix Virtual Apps」>「ファーム名」の順に展開します。ファーム名はサーバーファームの名前です。
3. [ポリシー] をクリックします。
4. 中央のウィンドウで、[コンピューター] または [ユーザー] をクリックし、[新規作成] をクリックします。
5. 新しいポリシーウィザードの [名前] にポリシーの名前を入力し、[次へ] をクリックします。
6. [カテゴリ] の [サーバー設定**]** をクリックします。

7. [設定] の [接続アクセス制御] の横にある [追加] をクリックします。
8. ［設定の追加］- ［接続アクセス制御］ダイアログボックスの［値］で［**Citrix Access Gateway** 接続のみ］を選択し、［**OK**］をクリックします。
9. [次へ] を **2** 回クリックし、[作成] をクリックします。Citrix Virtual Apps によってポリシーが作成されます。

Citrix Gateway 経由でルーティングされた接続のみを受け入れるように **Citrix Virtual Desktops** サーバーのプロパティを構成するには

デリバリーグループのマシンへのアクセスを制限できます。Citrix Gateway 経由のユーザー接続をフィルタリングする SmartAccess を使用して、ユーザーのアクセスを制限できます。このタスクは、Studio の［ポリシー］ノードで実行するか、クイックリファレンステーブルで説明されているポリシー設定を使用して実行できます。

1. Studio の［デリバリーグループ］で、制限するデリバリーグループを選択します。
2. ［デリバリーグループの編集］をクリックし、［アクセスポリシー］をクリックします。
3. ［アクセスポリシー］ページで［Citrix Gateway を介した接続］を選択します。Citrix Gateway を介した接続のみが許可されます。
4. これらの接続のサブセットを選択するには、[次のいずれかのフィルタを満たす接続] を選択します。
   a) Citrix Gateway サイトを定義します。
   b) デリバリーグループに許可されるユーザーアクセスシナリオを定義する SmartAccess 文字列を追加、編集、または削除します。SmartAccess の設定の詳細については、Citrix Gateway での SmartAccess 構成を参照してください。

Web Interface との通信の設定

March 26, 2020

Citrix Virtual Apps and Desktops で実行されている Web Interface と通信するように、Citrix Gateway を構成できます。これを行うには、Citrix Gateway で仮想サーバーを構成します。次に、署名付きサーバー証明書と認証、セッション、事前認証、および認証後のポリシーを仮想サーバーにバインドします。Citrix Gateway は、仮想サーバーの IP アドレスを使用して、ユーザー接続を Web Interface にルーティングします。

公開アプリケーションウィザードでは、ユーザー接続を Web Interface にルーティングするように Citrix Gateway を構成できます。Citrix Gateway は、ユーザー接続に Secure Ticket Authority（STA）を使用します。

公開アプリケーションおよびデスクトップのポリシーの構成

March 26, 2020

Citrix Virtual Apps and Desktops サーバーとの通信を確立するには、サーバーを認識するように Citrix Gateway を構成する必要があります。設定をグローバルに構成することも、ユーザー、グループ、または仮想サーバーにバインドされたポリシーを使用することもできます。

Citrix Gateway で **Web Interface** をグローバルに設定するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. ［グローバル Citrix Gateway 設定］ダイアログボックスの［クライアントエクスペリエンス］タブで、次の操作を行います。
   a)「プラグインの種類」で「Java」を選択します。
   b)「クライアントレス・アクセス」で、「許可」を選択します。

   > 注：iOS 向け Citrix Workspace アプリや Android 向け Citrix Workspace アプリなど、VPN 対応の Citrix Workspace アプリをサポートするには、ステップ 3 を実行します。モバイル Citrix Workspace アプリをサポートするには, あなたは、Access Gateway の最小をインストールする必要があります 10, ビルド 69.6 または Access Gateway 10, ビルド 71.6014.e. Access Gateway 9.3 を実行している場合は、この手順を実行する必要はありません。
4. [公開アプリケーション] タブの [ICA プロキシ] の横にある [ON] を選択します。
5. [Web Interface アドレス] の横に Web Interface の Web アドレスを入力し、[**OK**] をクリックします。

Web Interface のセッションポリシーを設定するには

セッション・ポリシーを構成し、仮想サーバーにバインドして、Web Interface へのアクセスを制限できます。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで［Citrix Gateway ポリシー］を展開し、［セッション］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [セッションポリシーの作成] ダイアログボックスの [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [セッションプロファイルの作成] ダイアログボックスの [名前] に、プロファイルの名前を入力します。
6. [クライアントエクスペリエンス] タブで、次の操作を行います。
   a) プラグインの種類の横にある「グローバル上書き」を選択し、「Java」を選択します。
   b)「クライアントレスアクセス」の横にある「グローバル上書き」を選択し、「許可」を選択します。
7. ICA プロキシの横にある「グローバルオーバーライド」をクリックし、「オン」を選択します。
8. [Web Interface アドレス] の横の [グローバル上書き] をクリックし、Web Interface の Web アドレスを入力して、[作成] をクリックします。
9. [セッションポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [全般]、[True value]、[式の追加]、[作成]、[閉じる] の順にクリックします。

セッション・ポリシーを作成したら、ポリシーを仮想サーバーにバインドします。

セッション・ポリシーを仮想サーバにバインドするには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、仮想サーバーを選択し、[開く] をクリックします。
3. [ポリシー] タブで、[セッション] をクリックし、[ポリシーの挿入] をクリックします。
4. リストからセッションポリシーを選択し、優先度番号（オプション）を入力して、[OK] をクリックします。

公開アプリケーションウィザードによる設定の構成

March 26, 2020

Web Interface を使用して Citrix Gateway を構成するには、次の情報が必要です。

- Citrix Virtual Apps and Desktops を実行しているサーバーの IP アドレス。
- Web Interface を実行しているサーバーの完全修飾ドメイン名（FQDN）。
- Citrix Gateway 上で構成された仮想サーバー。
- SmartAccess 用に設定されたセッションポリシー。
- Web Interface フェイルオーバーを構成する場合は、Web Interface を実行する追加サーバーの IP アドレス。

公開アプリケーションウィザードを使用して **Web Interface** 設定を構成するには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］をクリックします。
2. 詳細ウィンドウの [はじめに] で、[公開アプリケーションウィザード] をクリックします。
3. [次へ] をクリックし、ウィザードの指示に従います。

公開アプリケーション・ウィザード内から、Secure Ticket Authority（STA）を構成およびアクティブ化できます。公開アプリケーションウィザードを完了すると、設定はグローバルにバインドされます。

Citrix Gateway での **Secure Ticket Authority** の構成

March 26, 2020

Secure Ticket Authority（STA）は、Citrix Virtual Apps 上の公開アプリケーションおよび Citrix Virtual Desktops 上の公開デスクトップに対する接続要求に応答してセッションチケットを発行する役割を担います。これらのセッションチケットは、公開されたリソースへのアクセスのための認証と承認の基礎を形成します。

STA は、グローバルにバインドすることも、仮想サーバにバインドすることもできます。また、仮想サーバを構成するときに、STA を実行する複数のサーバを追加することもできます。

Citrix Gateway と STA 間の通信をセキュリティで保護する場合は、STA を実行するサーバーにサーバー証明書がインストールされていることを確認してください。

STA の詳細については、記事NetScaler Gateway Secure Ticket Authorityを参照してください。

STA をグローバルにバインドするには

1. **Citrix Gateway >**［グローバル設定］に移動します。
2. 詳細ペインの [サーバー] で、[Secure Ticket Authority が使用する **STA** サーバーのバインド/バインド解除] をクリックします。
3. [**STA** サーバのバインド/バインド解除] ダイアログ・ボックスで、[追加] をクリックします。
4. [**STA** サーバーの構成] ダイアログボックスで、STA サーバーの URL を入力し、[作成] をクリックし、[**OK**] をクリックします。
5. [**STA** サーバー] ダイアログボックスの [URL] に、STA を実行しているサーバーの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力し、[作成] をクリックします。

   > 注:
   > STA を実行している複数のサーバをリストに追加できます。Web Interface に表示される STA は、Citrix Gateway 上で構成されている STA と一致する必要があります。複数の STA を構成する場合は、Citrix Gateway と STA を実行しているサーバー間で負荷分散を使用しないでください。

STA を仮想サーバにバインドするには

1. ［**Citrix Gateway**］**>**［仮想サーバー］に移動します。
2. 詳細ウィンドウで、仮想サーバーを選択し、[編集] をクリックします。
3. [公開アプリケーション] タブの [Secure Ticket Authority] で、[追加] をクリックします。
4. [**STA** サーバの構成] ダイアログ・ボックスで、STA サーバの URL を入力し、[作成] をクリックします。
5. ステップ 4 を繰り返して STA サーバを追加し、[**OK]** をクリックします。

Citrix Gateway での追加の **Web Interface** 設定の構成

April 9, 2020

Citrix Gateway を Web Interface 環境に展開する場合は、次のオプションタスクを実行できます。

- Web Interface フェールオーバーの設定Web Interface を実行するセカンダリサーバーにフェイルオーバーするように、Citrix Gateway を構成します。
- Web Interface を使用したスマートカードアクセスの構成Citrix Workspace アプリとスマートカード認証を使用して、Web Interface に直接ログオンするようにユーザーセッションを構成します。

Web Interface フェールオーバーの設定

March 26, 2020

公開アプリケーションウィザードを使用して、Web Interface を実行するセカンダリサーバーにフェイルオーバーするように Citrix Gateway を構成できます。

Web Interface フェイルオーバーにより、プライマリ Web Interface に障害が発生した場合でも、ユーザー接続をアクティブなままにできます。フェールオーバーを設定する場合は、システム IP アドレス、マッピング IP アドレス、または仮想サーバの IP アドレスに加えて、新しい IP アドレスを定義します。新しい IP アドレスは、システムまたはマッピング IP アドレスと同じサブネット上にある必要があります。

Citrix Gateway で Web Interface フェイルオーバーを構成すると、新しい IP アドレスに送信されるネットワークトラフィックはプライマリ Web Interface に中継されます。公開アプリケーションウィザードで選択した仮想サーバーは、ネットワークアドレス変換 (NAT) IP アドレスとして機能します。実際の IP アドレスは、Web Interface の IP アドレスです。プライマリ Web Interface に障害が発生すると、ネットワークトラフィックがセカンダリ Web Interface に送信されます。

Web Interface フェールオーバーを構成するには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］をクリックします。
2. 詳細ウィンドウの [はじめに] で、[公開アプリケーションウィザード] をクリックします。
3. [次へ] をクリックし、仮想サーバーを選択して、[次へ] をクリックします。
4. [クライアント接続の構成] ページで、[Web Interface フェールオーバーの構成] をクリックします。
5. [プライマリ Web Interface] の [Web Interface サーバー] に、プライマリ Web Interface の IP アドレスを入力します。
6. [Web Interface サーバーポート] に、プライマリ Web Interface のポート番号を入力します。
7. [仮想サーバー IP] に、フェールオーバー用の新しい IP アドレスを入力します。
8. [仮想サーバーのポート] に、仮想サーバーのポート番号を入力します。
9. [Web Interface のバックアップ] の [Web Interface サーバー] に、Web Interface を実行しているサーバーの IP アドレスを入力するか、一覧からサーバーを選択します。
10. [Web Interface サーバーポート] で、Web Interface のポート番号を入力し、[OK] をクリックします。
11. [次へ] をクリックし、指示に従ってウィザードを完了します。

Web Interface を使用したスマートカードアクセスの構成

April 9, 2020

スマートカード認証を使用するように Web Interface を構成する場合、ユーザーのログオン方法に応じて、Citrix Gateway を統合するために次の展開シナリオを構成できます。

- ユーザーが Citrix Workspace アプリとスマートカード認証を使用して Web Interface に直接ログオンする場合、Web Interface は DMZ の Citrix Gateway と並行する必要があります。Web Interface を実行するサーバーもドメインメンバーである必要があります。

  このシナリオでは、Citrix Gateway と Web Interface の両方が SSL 終了を実行します。Web Interface は、ユーザー認証、公開アプリケーションの表示、公開アプリケーションの開始など、セキュリティで保護された HTTP トラフィックを終了します。Citrix Gateway は、着信 ICA 接続の SSL を終了します。

- ユーザーが Citrix Gateway プラグインを使用してログオンすると、Citrix Gateway は初期認証を実行します。Citrix Gateway が VPN トンネルを確立すると、ユーザーはスマートカードを使用して Web Interface にログオンできます。このシナリオでは、Citrix Gateway の背後に Web Interface を DMZ またはセキュリティで保護されたネットワークにインストールできます。

> 注:
> Citrix Gateway では、クライアント証明書を使用した認証にスマートカードを使用することもできます。

詳細については、「
スマートカード認証の構成」を参照してください。

Web Interface でのアプリケーションおよび **Virtual Desktops** へのアクセスの構成

April 9, 2020

Citrix Gateway を構成して、Receiver ではなく Citrix Gateway プラグインを使用して、公開アプリケーションや仮想デスクトップへのアクセスをユーザーに許可できます。アプリケーションおよびデスクトップへのアクセスを構成するには、Citrix Gateway 上の構成を、Citrix Gateway への接続にのみ Receiver を使用する構成から、Web Interface へのシングルサインオンで Citrix Gateway プラグインを使用して接続を有効にする構成に変更します。たとえば、すべてのユーザーが Citrix Gateway プラグインを使用して接続し、Web Interface をホームページとして使用するように Citrix Gateway を構成します。このシナリオでは、Web Interface へのシングル・サインオンがサポートされています。

アプリケーションやデスクトップへのアクセスに加えて、ユーザーデバイスにインストールされたアプリケーションを実行して、VPN トンネルを経由してネットワーク接続を行うこともできます。

設定を開始するには、次の注意事項に従ってください。

- Web Interface サイトを作成します。
- アクセス制御の詳細設定を構成します。
- SmartAccess 構成します。
- Citrix Gateway でエンドポイント分析を構成します。
- Citrix Virtual Apps and Desktops ポリシーとフィルターを構成します。

- Citrix Gateway プラグインを使用してユーザーがログオンし、公開アプリケーションおよび仮想デスクトップにアクセスするように Citrix Gateway を構成します。

詳細については、Citrix eDocs の以下のトピックを参照してください。

- 「Web Interface のサイトのセットアップ」を参照してください。
- Citrix Virtual Apps and Desktops での SmartAccess のしくみ
- エンドポイントポリシーの設定
- Citrix Virtual Apps ポリシーとフィルターの構成
- Citrix Virtual Desktops でポリシーとフィルターを構成するには 5
- Web Interface と通信するための Citrix Gateway の構成

Citrix Virtual Apps and Desktops へのユーザーのログオンを構成するときは、まずセッションプロファイルを作成し、Windows 用の Citrix Gateway プラグインを選択します。次に、Citrix Virtual Apps、Citrix Virtual Desktops、および Web Interface にアクセスするためのイントラネットアプリケーションのプロファイルを作成します。

アプリケーションおよびデスクトップにアクセスするための **Citrix Gateway** プラグインのグローバル設定を構成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. ［公開アプリケーション］タブで、［ICA プロキシ］の横にある［OFF］を選択します。
4. [Web Interface アドレス] に、Web Interface サイトの URL を入力します。これがユーザーのホームページになります。
5. [シングルサインオンドメイン] に、Active Directory ドメイン名を入力します。
6. [クライアントエクスペリエンス] タブで、[プラグインの種類] の横にある [Windows/Mac OS X] を選択し、[OK] をクリックします。

イントラネットアプリケーションを構成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［リソース］の順に展開し、［イントラネットアプリケーション］をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前] に、アプリケーションの名前を入力します。
4. [透明] をクリックします。
5. [プロトコル] で、[TCP]、[UDP]、または [任意] を選択します。
6. [宛先の種類] で、[IP アドレス] と [ネットマスク] を選択します。たとえば、172.16.100.x サブネット上のすべてのサーバーを表すには、172.16.100.0 とサブネットマスク 255.255.255.0 と入力します。Web

Interface、Citrix Virtual Apps、およびユーザーが接続する他のすべてのサーバーの IP アドレスは、イントラネットアプリケーションとして定義されたサブネットのいずれかにある必要があります。

イントラネットアプリケーションを作成したら、グローバルにバインドすることも、仮想サーバーにバインドすることもできます。

7. [IP アドレス] と [ネットマスク] に、内部ネットワークを表す IP アドレスとサブネットマスクを入力し、[作成] をクリックし、[閉じる] をクリックします。

   イントラネットアプリケーションを作成したら、グローバルにバインドすることも、仮想サーバーにバインドすることもできます。

イントラネットアプリケーションをグローバルにバインドするには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ペインの［イントラネットアプリケーション］で、［Java 用 Citrix Gateway プラグインのセキュリティで保護されたネットワーク内の TCP アプリケーションへのマッピングを作成する］をクリックします。
3. [VPN イントラネットアプリケーションの構成] ダイアログボックスで、[追加] をクリックします。
4. [使用可能] で、1 つまたは複数のイントラネットアプリケーションを選択し、矢印をクリックしてイントラネットアプリケーションを [構成済み] に移動し、[OK] をクリックします。

イントラネットアプリケーションを仮想サーバーにバインドするには

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、仮想サーバーを選択し、[開く] をクリックします。
3. Citrix Gateway 仮想サーバーの構成］ダイアログボックスで、［イントラネットアプリケーション］タブをクリックします。
4. [使用可能なアプリケーション名] で、イントラネットアプリケーションを選択し、[追加] をクリックし、[OK] をクリックします。

ユーザーが Citrix Gateway プラグインを使用してログオンすると、VPN トンネルが確立され、Receiver または Web Interface がホームページとして使用されます。

SmartAccess 設定

March 26, 2020

SmartAccess を Citrix Virtual Apps and Desktops とともに使用すると、公開アプリケーションおよび仮想デスクトップをユーザーにインテリジェントに配信できます。

SmartAccess では、Citrix Gateway セッションポリシーを使用して、サーバー上の公開アプリケーションおよびデスクトップへのアクセスを制御できます。公開されたリソースへのアクセスには、事前認証および認証後のチェックを条件として、他の条件とともに使用します。その他の条件には、プリンター帯域幅制限、ユーザーデバイスドライブのマッピング、クリップボード、オーディオ、プリンターマッピングなど、Citrix Virtual Apps and Desktops ポリシーで制御できるものが含まれます。ユーザーが Citrix Gateway のチェックに合格したかどうかに基づいて、Citrix Virtual Apps and Desktops ポリシーを適用できます。

Citrix Gateway では、Web Interface、ICA プロキシアクセス、クライアントレスアクセス、および Citrix Gateway アクセスで使用できるオプションと同じオプションを使用して、Citrix Virtual Desktops を配信できます。

この機能は、Citrix Gateway コンポーネントを Web Interface および Citrix 仮想アプリケーションおよびデスクトップと統合することによって実現されます。この統合により、Web Interface への高度な認証とアクセス制御オプションが提供されます。詳細については、Citrix eDocs ライブラリの［テクノロジ］ノードにある Web Interface のドキュメントを参照してください。

サーバーファームへのリモート接続には、Citrix Gateway プラグインは必要ありません。ユーザーは Citrix Workspace アプリで接続できます。ユーザーは、Citrix Gateway プラグインを使用してログオンし、Citrix Gateway のデフォルトのホームページであるアクセスインターフェイスを介して公開アプリケーションおよび仮想デスクトップを受信できます。

Citrix Virtual Apps and Desktops での SmartAccess のしくみ

March 26, 2020

SmartAccess を構成するには、Web Interface で Citrix Gateway 設定を構成し、Citrix Gateway でセッションポリシーを構成する必要があります。公開アプリケーションウィザードを実行すると、SmartAccess 用に作成したセッションポリシーを選択できます。

SmartAccess を構成すると、この機能は次のように動作します。

1. ユーザーが Web ブラウザで仮想サーバの Web アドレスを入力すると、設定した事前認証ポリシーがユーザデバイスにダウンロードされます。
2. Citrix Gateway は、事前認証とセッションポリシー名をフィルターとして Web Interface に送信します。ポリシー条件が true に設定されている場合、ポリシーは常にフィルタ名として送信されます。ポリシー条件が満たされない場合、フィルタ名は送信されません。これにより、エンドポイント分析の結果に基づいて、Citrix Virtual Apps および Desktops を実行しているコンピューター上の公開アプリケーションおよびデスクトップのリストと有効なポリシーを区別できます。
3. Web Interface は Citrix Virtual Apps and Desktops サーバーに接続し、公開されたリソースリストをユーザーに返します。フィルターが適用されたリソースは、フィルターの条件が満たされない限り、ユーザーのリストに表示されません。

Citrix Gateway で SmartAccess エンドポイント分析を構成できます。エンドポイント分析を構成するには、ICA プロキシ設定を有効にするセッションポリシーを作成し、クライアントのセキュリティ文字列を構成します。

ユーザーがログオンすると、エンドポイント分析ポリシーによって、Citrix Gateway で構成したクライアントセキュリティ文字列を使用してユーザーデバイスのセキュリティチェックが実行されます。

たとえば、ソフォスアンチウイルスの特定のバージョンを確認する場合などです。式エディタでは、クライアントのセキュリティ文字列は次のように表示されます。

```
client.application.av(sophos).version == 10.0.2
<!--NeedCopy-->
```

セッション・ポリシーを構成したら、ユーザー、グループ、または仮想サーバーにバインドします。ユーザーがログオンすると、SmartAccess ポリシーチェックが開始され、ユーザーデバイスにバージョン 10.0.2 以降の Sophos Antivirus がインストールされているかどうかが検証されます。

SmartAccess エンドポイント分析チェックが成功すると、クライアントレスセッションの場合は Web Interface ポータルが表示されます。それ以外の場合は、アクセスインターフェイスが表示されます。

SmartAccess のセッションポリシーを作成すると、セッションプロファイルに設定が構成されず、ヌルプロファイルが作成されます。この場合、Citrix Gateway は、SmartAccess 用にグローバルに構成された Web InterfaceURL を使用します。

Citrix Virtual Apps ポリシーとフィルターの構成

March 26, 2020

Citrix Gateway でセッションポリシーを作成したら、エンドポイント分析の構成に従ってユーザーに適用される Citrix Virtual Apps を実行しているコンピューターでポリシーとフィルターを構成します。

Citrix XenApp 6.5 のポリシーとフィルターを構成するには

1. Citrix Virtual Apps を実行しているサーバーで、［スタート］＞［管理ツール］＞［Citrix］＞［Citrix Virtual Apps］の順にクリックします。プロンプトが表示されたら、検出を構成して実行します。
2. 左側のペインで、［Citrix ADC リソース］>［Citrix Virtual Apps］>［ファーム名］の順に展開します。ファーム名はサーバーファームの名前です。
3. [アプリケーション] をクリックします。
4. 中央のウィンドウで、アプリケーションを右クリックし、[アプリケーションのプロパティ] をクリックします。
5. ナビゲーションウィンドウの [プロパティ] で、[詳細設定] > [アクセス制御] をクリックします。
6. 右側のウィンドウで、[次のフィルタのいずれかに一致する任意の接続] をクリックし、[追加] をクリックします。
7.「Access Gateway」ファームで、Citrix Gateway 仮想サーバーの名前を入力します。
8. [Access Gateway filter] にエンドポイントセッションポリシーの名前を入力し、[OK] をクリックします。
9. [アプリケーションのプロパティ] ダイアログボックスで、[他のすべての接続を許可する] をオフにし、[OK] をクリックします。

SmartAccess のセッションポリシーを構成するには

March 26, 2020

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [セッションポリシーの作成] ダイアログボックスの [名前] に、[ValidEndpoint] などのポリシーの名前を入力します。
4. [要求プロファイル] で、[新規] をクリックし、[名前] にプロファイルの名前 (Null など) を入力し、[作成] をクリックします。
5. [セッションポリシーの作成] ダイアログボックスで、クライアントセキュリティ式を作成し、[作成]、[閉じる] の順にクリックします。

クライアントセキュリティ式は、有効なエンドポイントと無効なエンドポイントを区別するために使用されます。エンドポイント分析の結果に基づいて、公開アプリケーションまたはデスクトップにさまざまなレベルのアクセスを提供できます。

セッション・ポリシーを作成したら、グローバルまたは仮想サーバーにバインドします。

Citrix Virtual Apps でのユーザーデバイスマッピングの構成

March 26, 2020

Citrix Virtual Apps を実行しているコンピューター上のポリシーに適用される Citrix Gateway フィルターを使用できます。フィルターにより、ユーザーは、エンドポイント分析の結果に基づいて、ユーザーデバイスのドライブマッピング、プリンターマッピング、クリップボードマッピングなどの Citrix Virtual Apps 機能にアクセスできます。

Citrix Workspace アプリは、ユーザーデバイス上のデバイスのマッピングをサポートしているため、ユーザーはユーザーセッション内で外部デバイスにアクセスできます。ユーザー・デバイス・マッピングにより、次の機能が提供されます。

- ローカル・ドライブとポートへのアクセス
- ユーザー・セッションとローカル・クリップボード間のカット・アンド・ペーストによるデータ転送
- ユーザーセッションからのオーディオ（システムサウンドと.wav ファイル）再生

ログオン中、ユーザーデバイスは、使用可能なユーザードライブと COM ポートをサーバーに通知します。Citrix XenApp 6.5 では、ユーザードライブがサーバーにマップされ、ユーザーデバイスのドライブ文字が使用されます。マップされたクライアント側デバイスは、そのセッションを実行中のユーザーだけが使用できます。マッピングは、ユーザーがログオフし、ユーザーが次回ログオンしたときに再作成されるときに削除されます。

XML サービスを有効にしたあと、ユーザーデバイスマッピングのポリシーを設定する必要があります。

SmartAccess フィルターに基づいてユーザーデバイスマッピングポリシーを適用するには、サーバー上に次の 2 つのポリシーを作成します。

- ユーザーデバイスマッピングを無効にし、すべての Citrix Gateway ユーザーに適用される制限付き ICA ポリシー。
- ユーザーデバイスマッピングを有効にし、エンドポイント分析セッションポリシーを満たすユーザーのみに適用される完全な ICA ポリシー
  注：フィルタリングされた非制限 ICA ポリシーは、制限 ICA ポリシーよりも高い優先度を与える必要があります。これにより、ユーザーに適用されるときに、非制限ポリシーは、ユーザーデバイスマッピングを無効にするポリシーを上書きします。

Citrix XenApp 6.5 で制限ポリシーと非制限ポリシーを構成するには、Citrix AppCenter を使用します。

Citrix XenApp 6.5 で制限ポリシーを構成するには

March 26, 2020

1. ［スタート］＞［管理ツール］＞［管理コンソール］＞［Citrix AppCenter］の順にクリックします。
2. 左側のペインで、［Citrix Virtual Apps］を展開し、［ポリシー］をクリックします。
3. [ポリシー] ペインで、[ユーザー] タブをクリックし、[新規] をクリックします。
4. [名前] にポリシーの名前を入力し、[次へ] をクリックします。
5. [カテゴリ] の [すべての設定] をクリックします。
6. [設定] の [クライアントドライブの自動接続] で、[追加] をクリックします。
7. [設定の追加] ダイアログボックスで、[無効]、[OK]、[次へ] の順にクリックします。
8. [カテゴリ] の [すべてのフィルタ] をクリックします。
9. [フィルタ] の [アクセス制御] で、[追加] をクリックします。
10. [新しいフィルタ] ダイアログボックスで、[追加] をクリックします。
11. [モード] で、[拒否] をクリックします。
12. [接続の種類] で、[Access Gateway あり] を選択します。
13. [AG ファーム] に、仮想サーバー名を入力します。
14. ［アクセス条件］で、Citrix Gateway で構成されているセッションポリシー名を入力または選択し、［OK］を 2 回クリックし、［次へ］をクリックし、［作成］をクリックしてウィザードを完了します。

Citrix XenApp 6.5 で非制限ポリシーを構成するには

March 26, 2020

1. ［スタート］＞［管理ツール］＞［管理コンソール］＞［Citrix AppCenter］の順にクリックします。
2. 左側のペインで、［Citrix Virtual Apps］を展開し、［ポリシー］をクリックします。

3. [ポリシー] ペインで、[ユーザー] タブをクリックし、[新規] をクリックします。
4. [名前] にポリシーの名前を入力し、[次へ] をクリックします。
5. [カテゴリ] の [すべての設定] をクリックします。
6. [設定] の [クライアントドライブの自動接続] で、[追加] をクリックします。
7. [有効]、[OK]、[次へ] の順にクリックします。
8. [カテゴリ] の [すべてのフィルタ] をクリックします。
9. [フィルタ] の [アクセス制御] で、[追加] をクリックします。
10. [新しいフィルタ] ダイアログボックスで、[追加] をクリックします。
11. [モード] で、[許可] をクリックします。
12. [接続の種類] で、[Access Gateway あり] を選択します。
13. [AG ファーム] に、仮想サーバー名を入力します。
14. ［アクセス条件］で、Citrix Gateway で構成されているセッションポリシー名を入力または選択し、［OK］を 2 回クリックし、［次へ］をクリックし、［作成］をクリックしてウィザードを完了します。

隔離アクセス方法としての **Citrix Virtual Apps** 有効化

March 26, 2020

Citrix Gateway でエンドポイント分析を構成している場合、エンドポイントスキャンに合格したユーザーは、Citrix Gateway で設定したすべてのリソースにアクセスできます。エンドポイントスキャンに失敗したユーザーを検疫グループに入れることができます。これらのユーザーは、Citrix Virtual Apps からのみ公開アプリケーションにアクセスできます。エンドポイント分析スキャンの成功または失敗によって、ユーザーが利用できるアクセス方法が決まります。

たとえば、ユーザーがログオンしたときにメモ帳がユーザーデバイスで実行されているかどうかを確認するエンドポイント分析スキャンを作成します。メモ帳が実行されている場合、ユーザーは Citrix Gateway プラグインを使用してログオンできます。メモ帳が実行されていない場合、ユーザーは公開アプリケーションの一覧のみを受け取ります。

制限されたユーザーアクセスを構成するには、Citrix Gateway で隔離グループを作成します。セッションプロファイル内で隔離グループを作成し、そのプロファイルをセッションポリシーに追加します。

隔離グループのセッションポリシーおよびエンドポイント分析スキャンの作成

March 26, 2020

Citrix Virtual Apps 検疫アクセス方法として有効にするには、Citrix Gateway で隔離グループとして使用するグループを作成します。次に、グループを選択するセッションポリシーを作成します。

セッションポリシーを作成したら、そのポリシーを隔離グループにバインドします。ポリシーを設定してグループにバインドしたら、結果をテストします。たとえば、ユーザーが正常にログオンするには、メモ帳がユーザーデバイス

で実行されている必要があります。メモ帳が実行されている場合、ユーザーは Citrix Gateway プラグインを使用してログオンできます。メモ帳が実行されていない場合、ユーザーは Citrix Workspace アプリでログオンできます。

エンドポイント分析ポリシーの設定の詳細については、エンドポイントポリシーの設定を参照してください。

エンドポイント分析スキャンを作成して検疫グループを追加するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [セッションポリシーの作成] ダイアログボックスの [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [セッションプロファイルの作成] ダイアログボックスの [名前] に、プロファイルの名前を入力します。
6. [セキュリティ] タブで、[詳細設定] をクリックします。
7. [セキュリティの設定-詳細] ダイアログボックスの [Client Security] で、[グローバルに上書き] をクリックし、[新規] をクリックします。
8. [式を作成] ダイアログボックスで、[任意の式に一致] の横にある [追加] をクリックします。
9. 「式の種類」で、「クライアント・セキュリティ」を選択します。
10. 「コンポーネント」で、「プロセス」を選択します。
11. [名前] ボックスに「notepad.exe」と入力し、[OK] をクリックし、[作成] をクリックします。
12. [セキュリティの設定-詳細] ダイアログボックスの [隔離グループ] で、隔離グループを選択し、[作成] をクリックし、[OK] をクリックして [作成] をクリックします。
13. [セッションポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [True value] を選択し、[式の追加] をクリックして、[作成] をクリックして、[閉じる] をクリックします。

SmartAccess 用の Citrix Virtual Desktops の構成

March 26, 2020

Citrix Gateway を使用すると、Citrix Virtual Desktops がリモートユーザーにセキュアなデスクトップを配信できます。Citrix Virtual Desktops では、Citrix Gateway の SmartAccess 機能を使用してデスクトップをインテリジェントに配信できます。Citrix Virtual Desktops のデリバリーサービスコンソールを使用してデスクトップグループを作成する場合は、アクセス制御のポリシーとフィルタを構成します。

公開デスクトップを配信するように Citrix Gateway を構成するには、Web Interface、ICA プロキシアクセス、クライアントレスアクセス、および Citrix Gateway アクセスで使用できるものと同じオプションを使用します。

セッションポリシーを作成し、［公開アプリケーション］タブで設定を構成する場合は、Citrix Virtual Desktops Web Interface サイトの Web アドレスを使用します。ポリシーを作成したら、仮想サーバにバインドします。次に、設定を構成しないヌルセッションプロファイルを作成します。Web Interface の構成は、グローバル設定から継承されます。

Citrix Virtual Desktops を使用した **SmartAccess** のセッションポリシーを構成するには

March 26, 2020

Citrix Virtual Desktops にアクセスするように Citrix Gateway 上の SmartAccess を構成するには、仮想サーバーにバインドされたセッションポリシーを作成します。

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [セッションポリシーの作成] ダイアログボックスの [名前] に、[Citrix Virtual Desktops ポリシー] などのポリシーの名前を入力します。
4.「要求プロファイル」で、「新規」をクリックします。
5.［セッションプロファイルの作成］ダイアログボックスの［名前］に、［Citrix Virtual Desktops プロファイル］などのプロファイルの名前を入力します。
6. [公開アプリケーション] タブの [ICA プロキシ] の横にある [グローバル上書き] をクリックし、[ON] を選択します。
7. [Web Interface アドレス] で、[グローバルに上書き] をクリックし、Citrix Virtual Desktops Web Interface サイトの URL を入力します。
8.［Single Sign-On Domain］で［グローバルに上書き］をクリックし、ドメイン名を入力して［作成］をクリックします。
9. [セッションポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [True Value] を選択し、[式の追加] をクリックして、[作成] をクリックして、[閉じる] をクリックします。

また、仮想サーバーにバインドされたヌルセッションポリシーを作成する必要があります。セッションプロファイルには設定が含まれていないため、ヌルプロファイルになります。セッションポリシーで、True Value 式を追加し、ポリシーを保存します。

両方のセッション・ポリシーを作成したら、両方のポリシーを仮想サーバにバインドします。

Citrix Virtual Desktops でポリシーとフィルターを構成するには **5**

March 26, 2020

Citrix Virtual Desktops 5 の設定は、Desktop Studio またはグループポリシーエディターを使用して構成できます。Citrix Virtual Desktops で Citrix Gateway 設定を構成する場合は、Citrix Gateway 仮想サーバー名とセッションポリシー名を使用します。次に、定義されたフィルタを満たす接続を許可するようにアクセス制御を設定します。SmartAccess ポリシーを使用することもできます。

1. Citrix Virtual Desktops サーバーで、[スタート] > [すべてのプログラム] > [Citrix] > [Desktop Studio] の順にクリックします。
2. 左側のペインで、[HDX Policy] をクリックして展開し、中央のペインの [User] タブをクリックします。
3. [ユーザー] で、[新規作成] をクリックします。
4. [新しいポリシー] ダイアログボックスの [ポリシーの識別] で、[名前] に名前を入力します。
5. [次へ] を 2 回クリックします。
6. [新しいポリシー] ダイアログボックスの [フィルター] タブで、[フィルター] の下の [アクセス制御] をクリックし、[追加] をクリックします。
7. [新しいフィルタ] ダイアログボックスで、[追加] をクリックします。
8. [新しいフィルタ要素] ダイアログボックスの [接続の種類] で、[Access Gateway] を選択します。

   Citrix Gateway ポリシーを考慮せずに、Citrix Gateway 経由で行われた接続にポリシーを適用するには、AG ファーム名とアクセス条件をデフォルトのままにします。
9. 既存の Citrix Gateway ポリシーに基づいて、Citrix Gateway 経由の接続にポリシーを適用する場合は、次の操作を行います。

   a) [AG ファーム名] に、仮想サーバー名を入力します。
   b) [アクセス条件] に、エンドポイント分析ポリシーまたはセッションポリシーの名前を入力します。

   > 重要: Citrix Virtual Desktops では、Citrix Gateway 仮想サーバー、エンドポイント分析ポリシー、セッションポリシー名は検証されません。情報が正しいことを確認します。
10. [OK] を 2 回クリックし、[次へ]、[作成] の順にクリックします。

デスクトップ **Delivery Controller** を **STA** として追加するには

March 26, 2020

Citrix Virtual Desktops との ICA 接続を確立するには、デスクトップ Delivery Controller IP アドレスを仮想サーバーに Secure Ticket Authority（STA）として追加します。

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、仮想サーバーを選択し、[開く] をクリックします。
3. [公開アプリケーション] タブの [Secure Ticket Authority] で、[追加] をクリックします。
4. [STA サーバの構成] ダイアログ・ボックスで、STA サーバの URL を入力し、[作成] をクリックします。
5. 手順 4 を繰り返して STA サーバーを追加し、Citrix Gateway 仮想サーバーの構成］ダイアログボックスで［OK］をクリックします。

スマートコントロールの設定

March 26, 2020

Smart Control を使用すると、管理者は詳細なポリシーを定義して、Citrix Gateway 上の Citrix Virtual Apps and Desktops のユーザー環境属性を構成および適用できます。Smart Control を使用すると、管理者はこれらのサーバータイプの各インスタンスではなく、1 つの場所からこれらのポリシーを管理できます。

スマートコントロールは、Citrix Gateway の ICA ポリシーによって実装されます。各 ICA ポリシーは、ユーザー、グループ、仮想サーバー、およびグローバルに適用できる式とアクセスプロファイルの組み合わせです。ICA ポリシーは、セッション確立時にユーザーが認証した後に評価されます。

次の表に、Smart Control で適用できるユーザー環境属性を示します。

| | |
| ——————————————————————————— | ——————————————————————————— |
| クライアントドライブを接続します | ユーザーがログオンするときのクライアントドライブへの既定の接続を指定します。
接続クライアント LPT ポート	ユーザーがログオンしたときに、クライアントからの LPT ポートの自動接続を指定します。LPT ポートはローカルプリンタポートです。
クライアントオーディオリダイレクト	クライアントコンピュータにインストールされているサウンドデバイスを介してオーディオを送信するために、サーバーでホストされているアプリケーションを指定します。
クライアントクリップボードリダイレクト	クライアントデバイス上のクリップボードアクセスを指定して構成し、クリップボードをサーバーにマッピングします。
クライアント構成リダイレクト	クライアントへの COM ポートのリダイレクトを指定します。COM ポートは COM ポートです。これらはシリアル・ポートです。
クライアントドライブリダイレクト	クライアントへのドライブリダイレクトとクライアントからのドライブリダイレクトを指定します。
マルチストリーム	指定したユーザのマルチストリーム機能を指定します。
クライアント USB デバイスリダイレクト	クライアントへの USB デバイスのリダイレクションを指定します（ワークステーションホストのみ）。
ローカルリモートデータ	Citrix Workspace アプリの HTML5 ファイルのアップロードダウンロード機能を指定します。
クライアントプリンタのリダイレクト	ユーザーがセッションにログオンするときにサーバーにマップされるクライアントプリンターを指定します。
ポリシー	アクション	アクセスプロファイル
追加	編集	削除
バインドの表示	ポリシーマネージャ	アクション

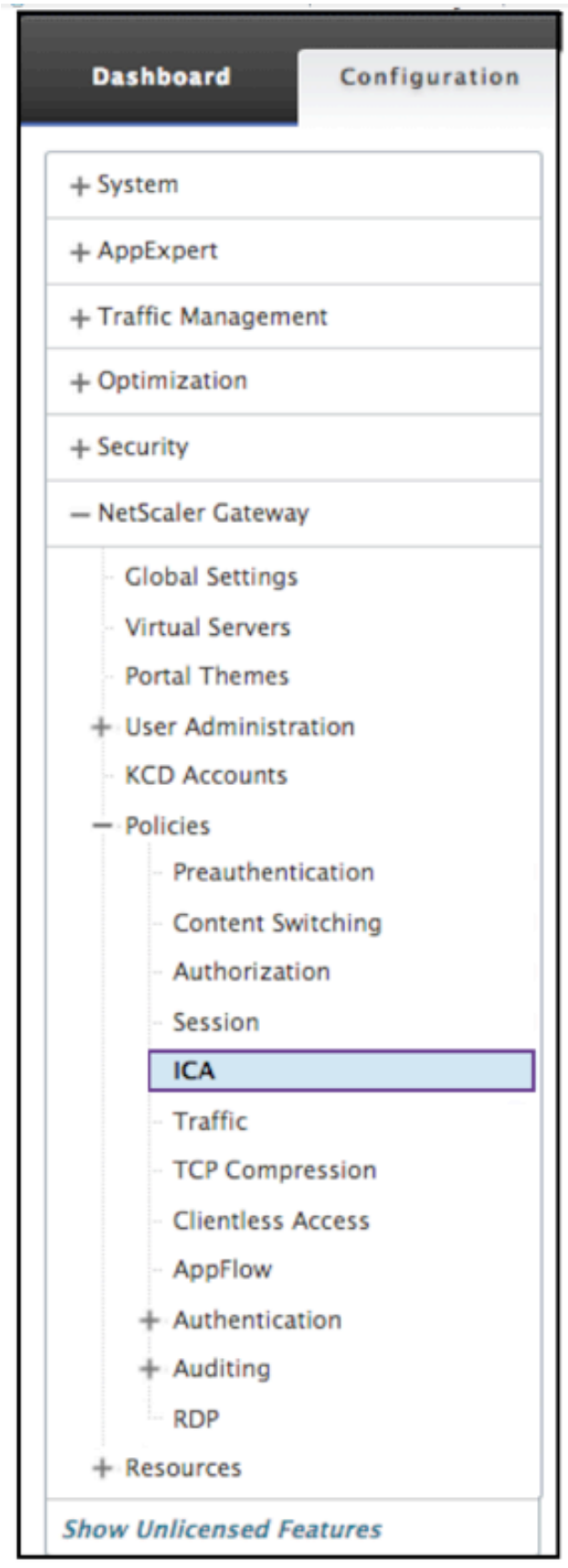
ポリシー

ICA ポリシーは、アクション、アクセスプロファイル、式、およびオプションでログアクションを指定します。[ポリシー] タブでは、次のコマンドを使用できます。

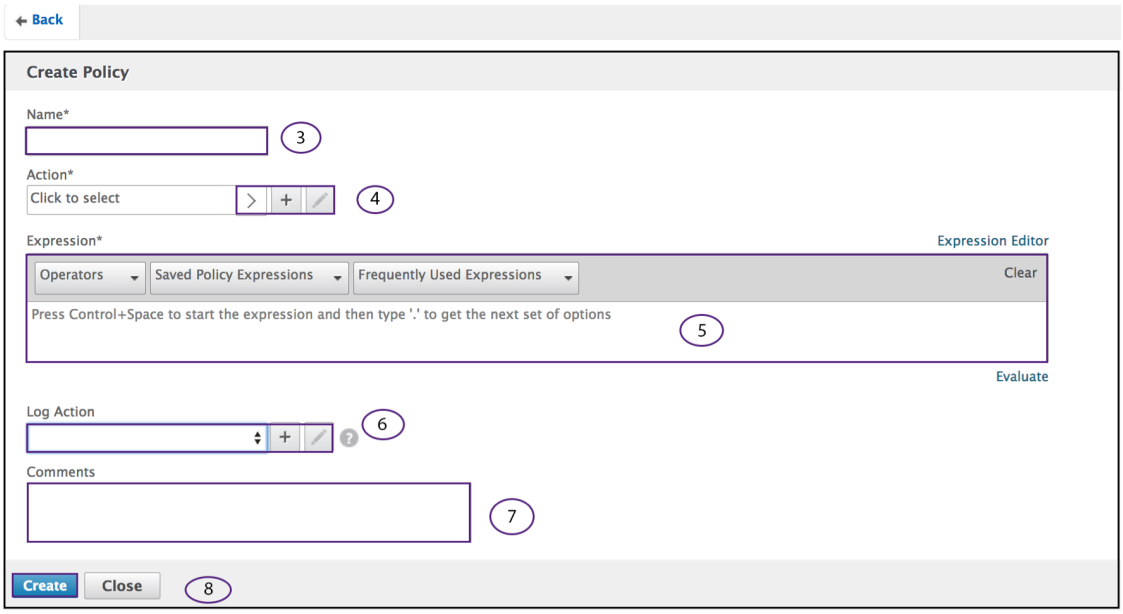
- 追加
- 編集
- 削除
- バインディングを表示
- ポリシーマネージャ
- 操作（アクション）

追加

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［ICA］をクリックします。



2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. 次の画面が開きます。[名前] ダイアログボックスで、ポリシーの名前を入力します。これは必須フィールドです。必須フィールドはすべてアスタリスクで示されます。

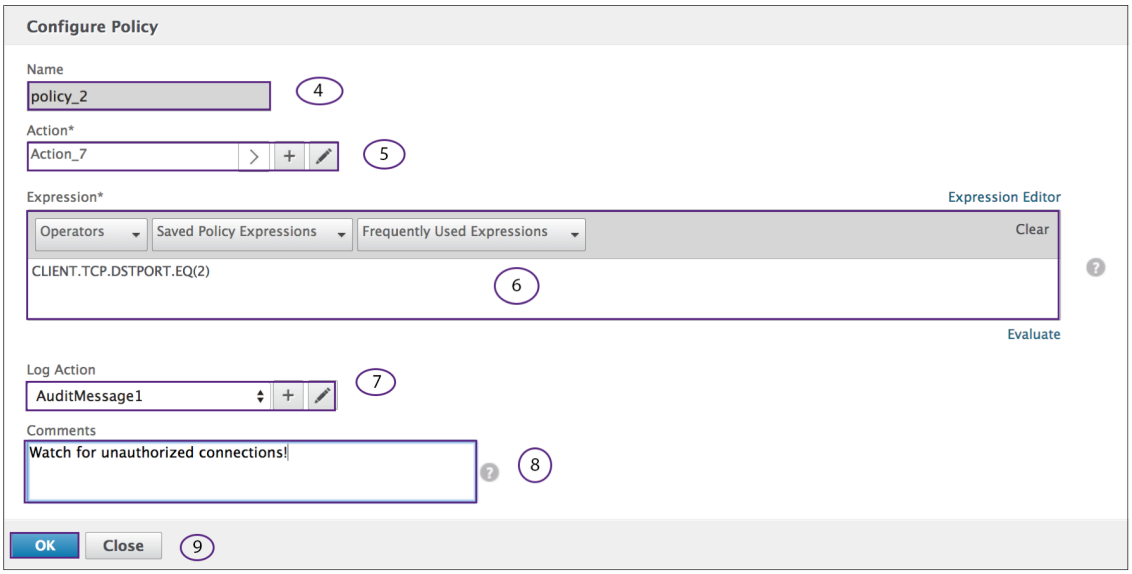


4. [アクション] の横で次のいずれかの操作を行います。
   - [**>**] アイコンをクリックして、既存のアクションを選択します。詳細については、(#common-processes) の [操作を選択] を参照してください。
   - [**+**] アイコンをクリックして、新しいアクションを作成します。詳細については、(#common-processes) の [新しいアクションを作成する] を参照してください。
   - 鉛筆アイコンは無効になります。
5. 式を作成します。
6. ログアクションを作成します。詳細については、ログアクションの作成を参照してください。
7. [コメント] ボックスにメッセージを入力します。コメントはメッセージログに書き込まれます。この情報は入力しなくても構いません。
8. [作成] をクリックします。

編集

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、[Citrix Gateway] > [ポリシー] の順に展開し、[ICA] をクリックします。
2. リストから ICA ポリシーを選択します。
3. 詳細ウィンドウの [ポリシー] タブで、[編集] をクリックします。

4. ポリシー名を確認します。



5. アクションを修正するには、次のいずれかの操作を行います。

   - 既存の アクションを修正するには、[**>**] アイコンをクリックします。詳細については、(#common-processes) の [操作を選択] を参照してください。
   - [**+**] をクリックして、新しい アクションを作成します。詳細については、(#common-processes) の [新しいアクションを作成する] を参照してください。
   - 鉛筆アイコンをクリックして、[アクセスプロファイル] を修正します。

6. 必要に応じて、式を修正します。詳細については、(#common-processes) の [式] を参照してください。
7. ログアクションを修正するには、次のいずれかの操作を行います。

   - [+] をクリックして、新しい ログアクションを作成します。
   - 鉛筆アイコンをクリックして、監査メッセージを設定します。

8. 必要に応じてコメントを修正します。
9. [**OK]** をクリックします。

削除

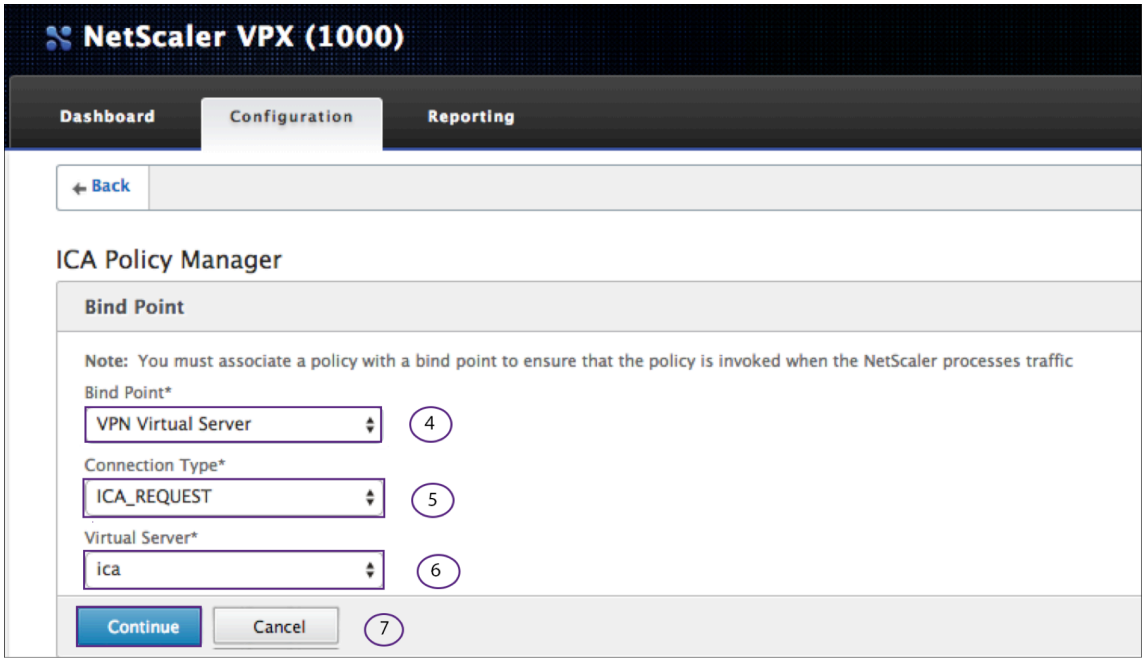
1. 構成ユーティリティの［構成］タブのナビゲーションペインで、[Citrix Gateway］＞［ポリシー］の順に展開し、［ICA］をクリックします。
2. リストから目的の ICA ポリシーを選択します。
3. 詳細ウィンドウの [ポリシー] タブで、[削除] をクリックします。
4. [**Yes**] をクリックして、ポリシーを削除することを確認します。

バインドを表示

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［ICA］をクリックします。
2. リストから ICA ポリシーを選択します。
3. 詳細ウィンドウの [ポリシー] タブで、[バインドの表示] をクリックします。

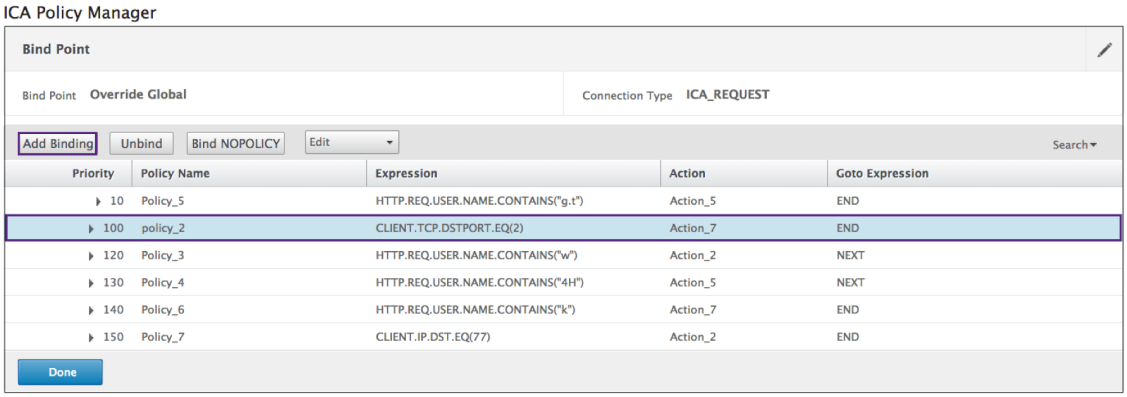
ポリシーマネージャ

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［ICA］をクリックします。
2. リストから目的の ICA ポリシーを選択します。
3. 詳細ペインの [ポリシー] タブで、[ポリシーマネージャ] をクリックします。
4. [Bind Point] ダイアログボックスで、ドロップダウンメニューからポリシーを選択します。次の選択肢があります。
   - グローバルをオーバーライド
   - VPN 仮想サーバー
   - キャッシュのリダイレクト仮想サーバー
   - デフォルトグローバル
5. [Connection Type] ダイアログボックスで、ドロップダウンメニューからバインディングポリシーを選択します。
6. VPN 仮想サーバーまたはキャッシュリダイレクト仮想サーバーのいずれかを選択した場合は、ドロップダウンボックスを使用してサーバーに接続します。
7. [続行] をクリックします。



バインドの追加

1. [Continue] を選択すると、この画面が表示されます。
2. バインディングをアタッチするポリシーを選択します。
3. 「バインドを追加」を選択します。

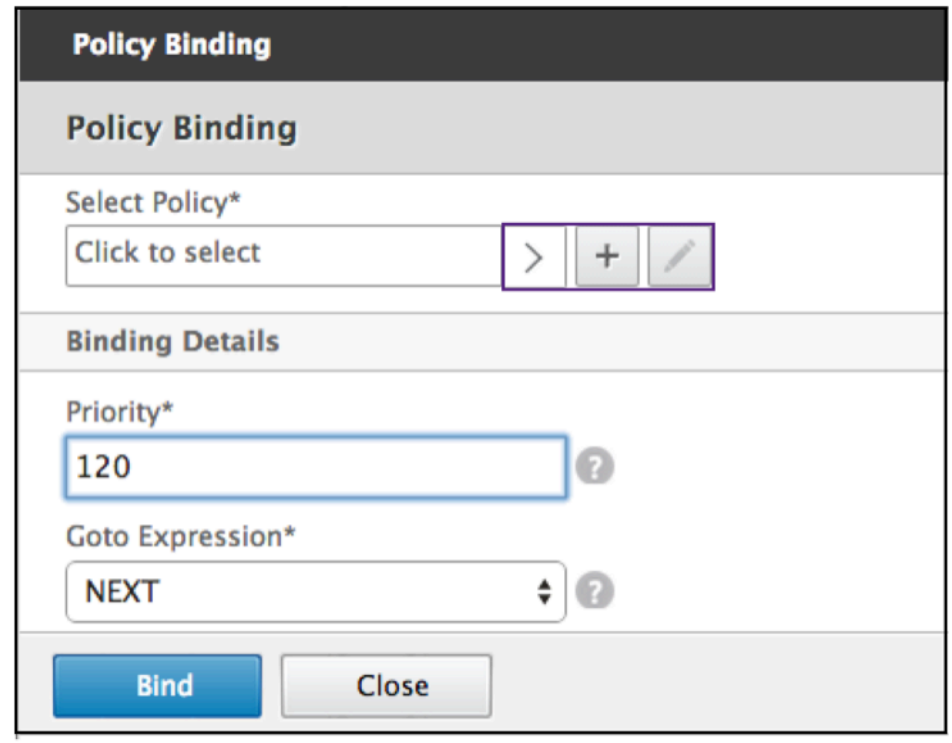


ポリシーバインディング

1. [完了] を選択すると、この画面が表示されます。

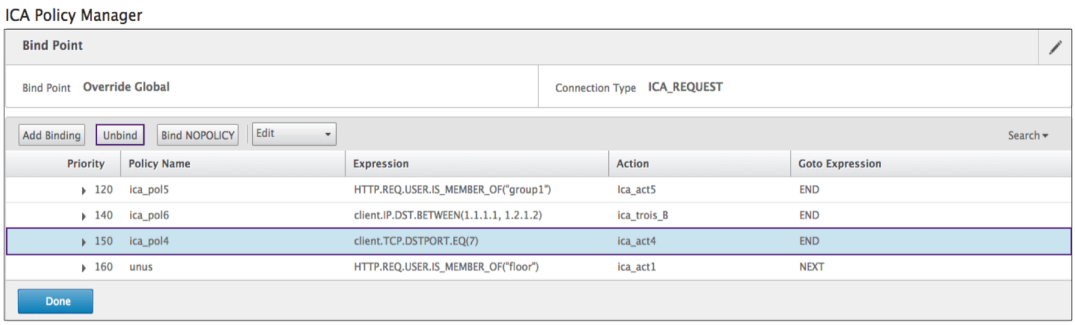
- [**>]** アイコンをクリックして、既存のポリシーを選択します。詳細については、既存のポリシーの選択を参照してください。

- [**+**] をクリックして、新しいポリシーを作成します。詳細については、新しいポリシーの作成を参照してください。



ポリシーのバインド解除

1. バインド解除するポリシーを選択し、[**Unbind**] ボタンをクリックします。



2. [完了] をクリックします。
3. ポップアップ画面で「はい」ボタンをクリックして、選択したエンティティのバインドを解除することを確認します。

バインドノポリシー

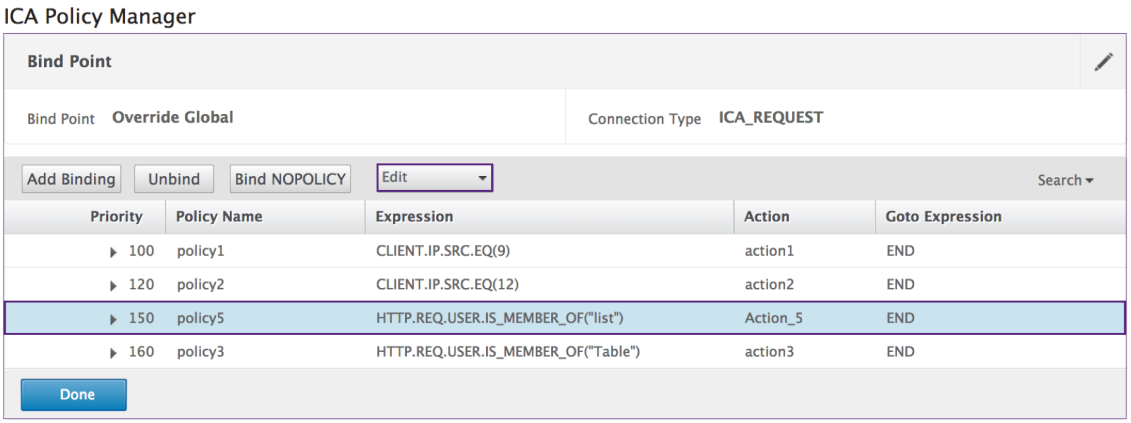
1. NOPOLICY を必要とするポリシーを選択し、[**Bind NOPOLICY**] ボタンをクリックします。

2. [完了] をクリックします。

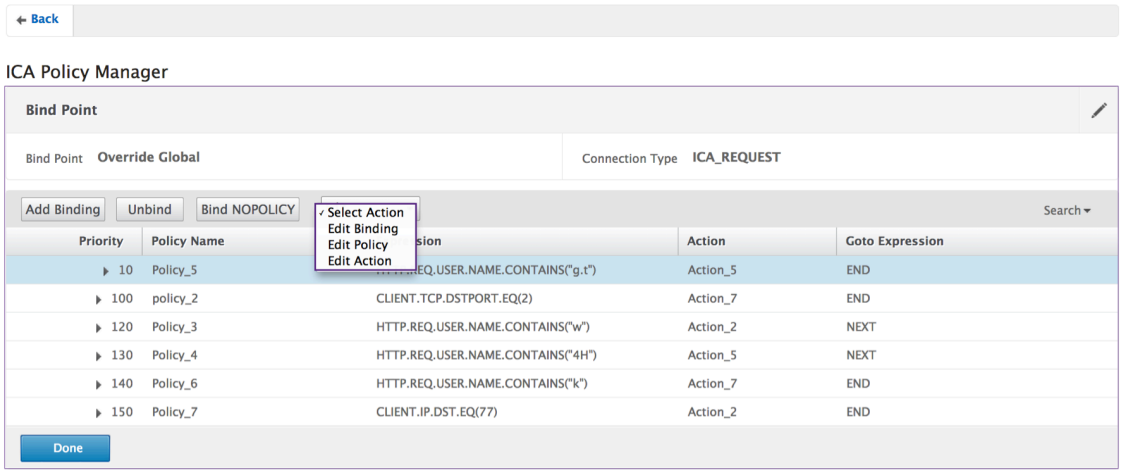
編集

ICA ポリシーマネージャから編集できます。

1. 編集するポリシーを選択し、[**Edit**] を選択します。



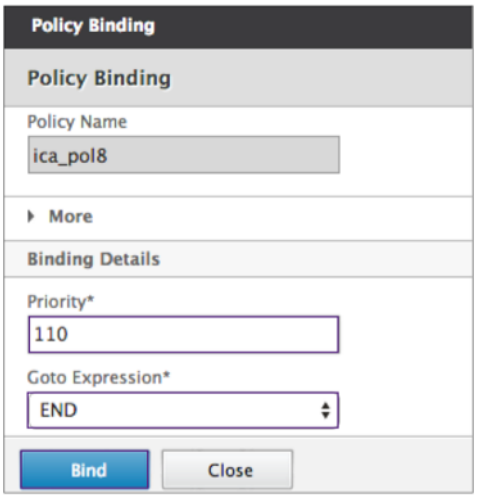
2. 次の編集を行うオプションがあります: [バインディングの編集。]。**[ポリシーの編集]、[アクションの編集]**。



詳しくは **[バインドの編集]、[ポリシーの編集]、[アクションの編集] を参照してください。**

バインドの編集

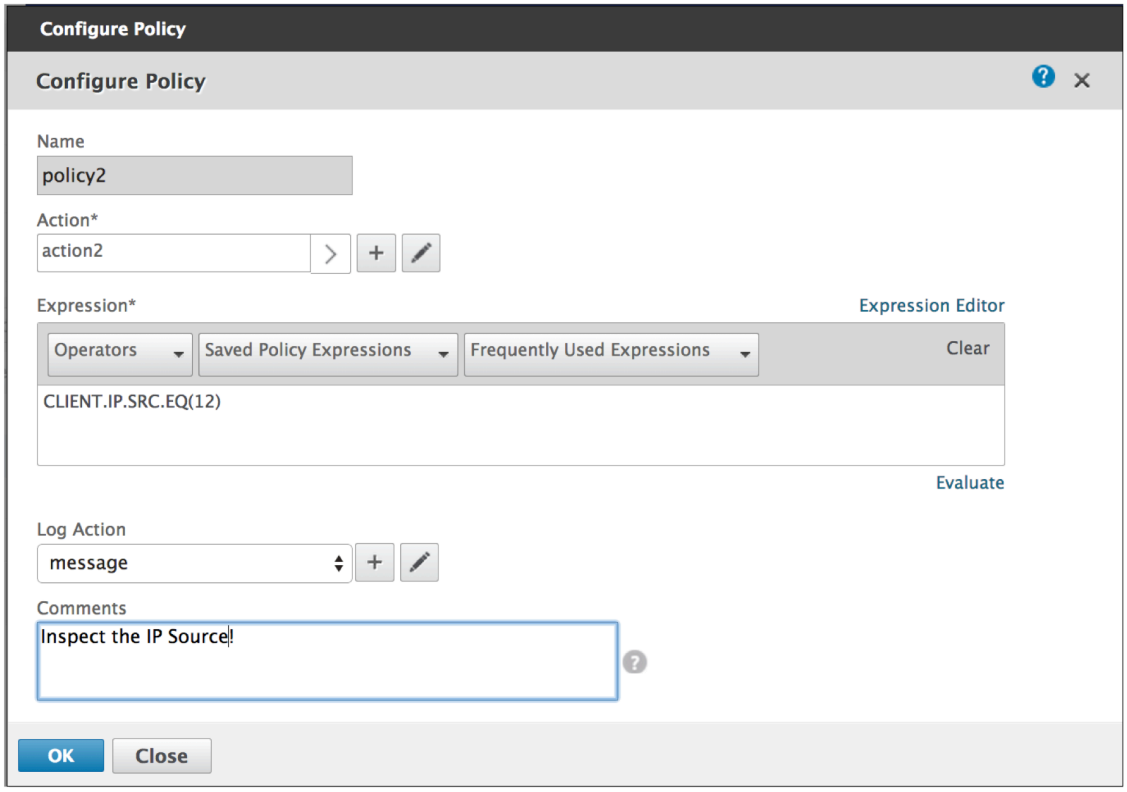
1. ポリシーが選択されている状態で、[バインディングの編集] をクリックします。
2. 目的のポリシーを編集していることを確認します。このポリシー名は編集できません。



3. 必要に応じて [優先度] を設定します。
4. 必要に応じて [式に移動] を設定します。
5. [バインド] ボタンをクリックします。

ポリシーの編集

1. ポリシーを選択した状態で、[ポリシーの編集] をクリックします。
2. ポリシーの [Name] を確認し、目的のポリシーを編集していることを確認します。このフィールドは編集できません。



3. アクションポリシーを変更するには、次のいずれかの操作を行います。

   - 「**>**」アイコンをクリックして、既存のアクションを選択します。詳細については、(#common-processes) の [操作を選択] を参照してください。
   - アクションを作成するには、[**+**] アイコンをクリックします。詳細については、(#common-processes) の [新しいアクションを作成する] を参照してください。
   - 鉛筆アイコンをクリックして、アクセスプロファイルを修正します。詳細については、(#common-processes) の [既存のアクセスプロファイルの選択] を参照してください。

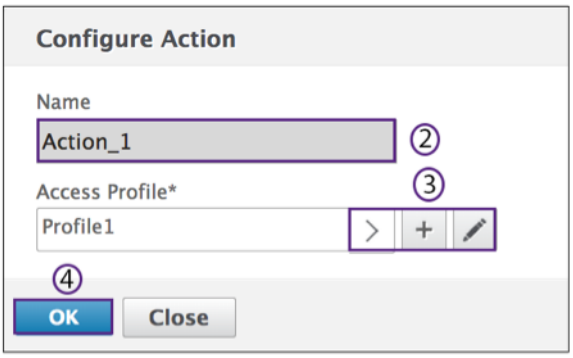
4. 必要に応じて、式を修正します。詳細については、(#common-processes) の [式] を参照してください。
5. ドロップダウンメニューから目的のメッセージタイプを選択します。ログアクションを作成するには、次のいずれかの操作を行います。

   - アクションを作成するには、[**+**] アイコンをクリックします。詳しくは、ログアクションの作成を参照してください。
   - 鉛筆アイコンをクリックして、「監査メッセージの設定」アクションを修正します。詳しくは、監査メッセージアクションの構成を参照してください。

6. ICA ポリシーに関するコメントを入力します。
7. 編集が完了したら、[**OK]** をクリックします。

アクションの編集

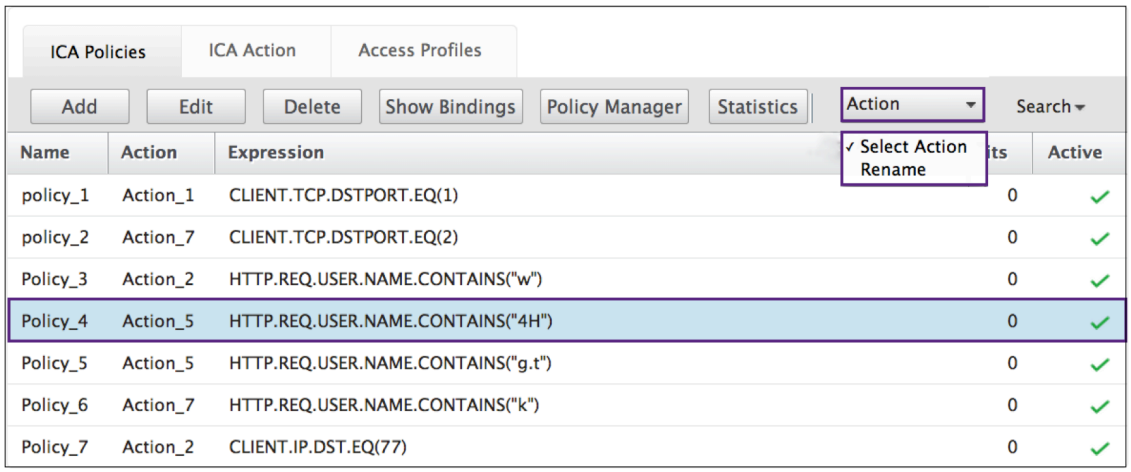
1. ポリシーを選択した状態で、[**Edit Action**] をクリックします。
2. 「アクション名」を確認し、目的のアクションを編集していることを確認します。このフィールドは編集できません。
3. [アクセスプロファイル] の横で、次のいずれかの操作を行います。
   - [**>]** アイコンをクリックして、別のアクセスプロファイルを選択します。詳細については、アクションの構成を参照してください。
   - [**+**] アイコンをクリックして、新しいチャネルプロファイルを選択します。 アクセスプロファイルの作成。
   - 鉛筆アイコンをクリックして、アクセスプロファイルを修正します。詳細については、(#common-processes) の [既存のアクセスプロファイルの選択] を参照してください。
4. [**OK]** をクリックします。



操作（アクション）

[ポリシー] > [アクション] コマンドを使用して、アクションの名前を変更します。

1. リストから目的の ICA アクションを選択します。
2. [ICA ポリシー] タブで、[操作] をクリックします。ドロップダウンメニューから [名前の変更] を選択します。



3. アクションの名前を変更します。
4. [**OK**] をクリックします。

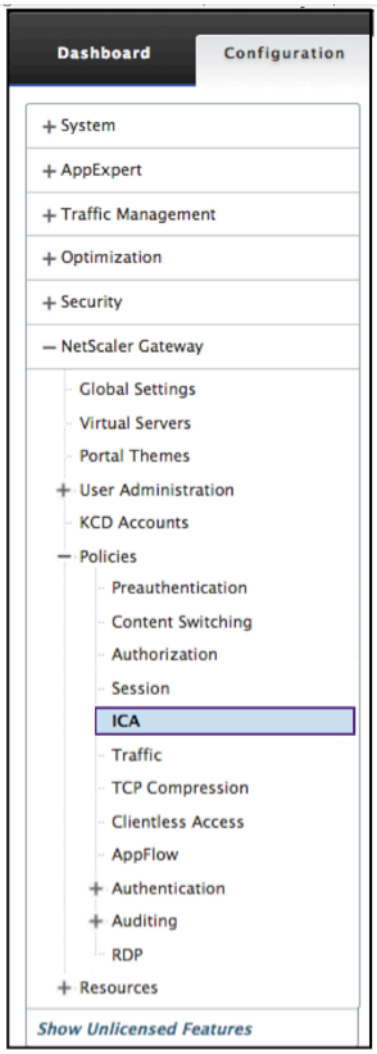
操作（アクション）

アクションは、ポリシーをアクセスプロファイルと接続します。[ポリシー] タブでは、次のコマンドを使用できます。

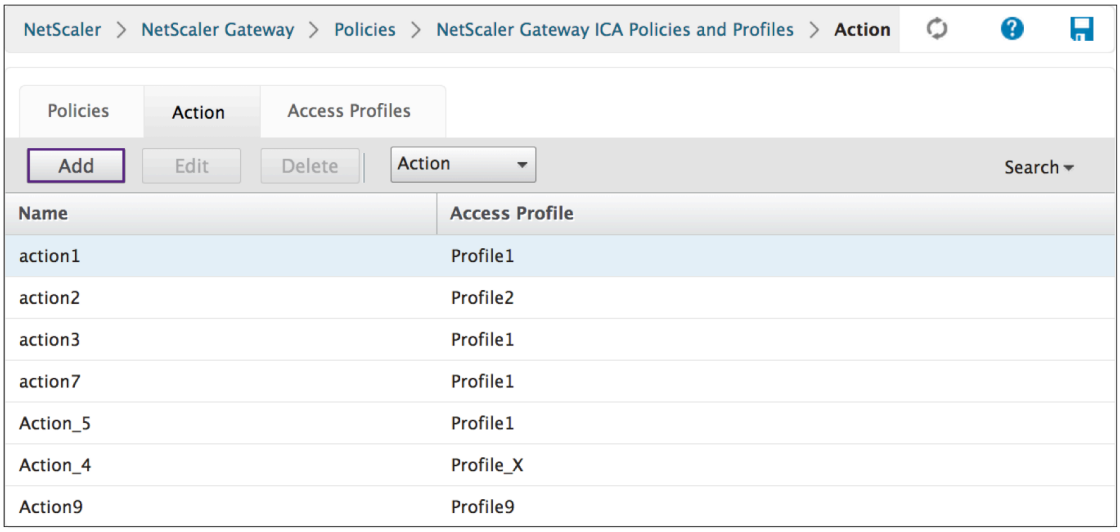
- 追加
- 編集
- 削除
- 操作（アクション）

追加

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、[Citrix Gateway］>［ポリシー］の順に展開し、[ICA］をクリックします。

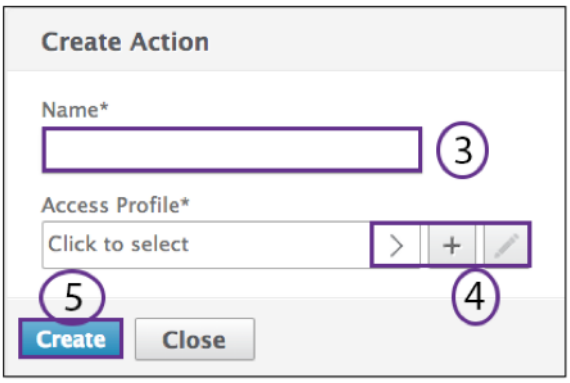


2. 詳細ウィンドウの [操作] タブで、[追加] をクリックします。



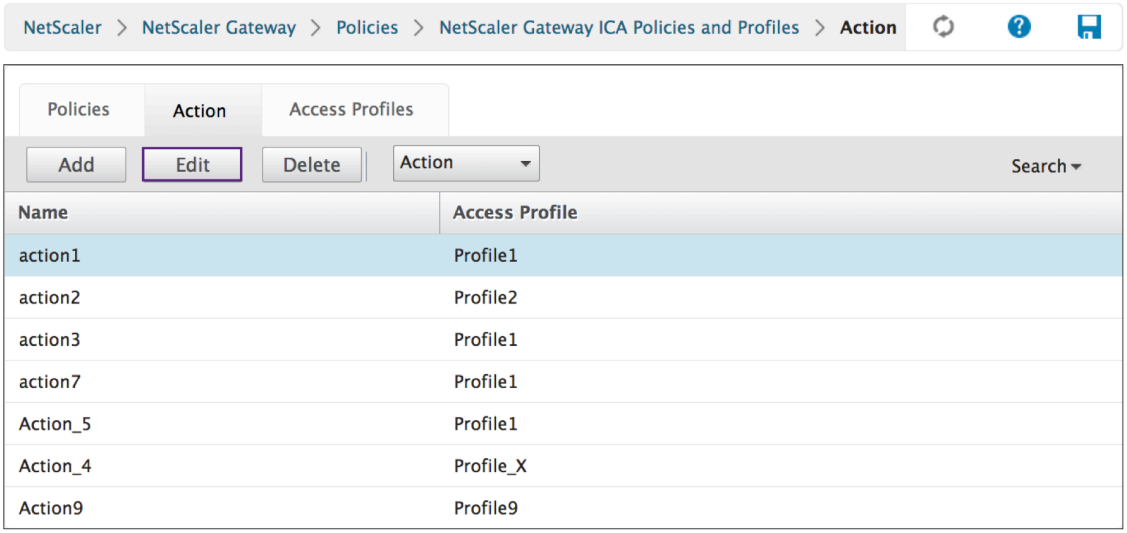
- [**>]** アイコンをクリックして、既存のアクセスプロファイルを選択します。詳細については、(#common-processes) の [既存のアクセスプロファイルの選択] を参照してください。
- [**+**] アイコンをクリックして、新しいアクセスプロファイルを作成します。詳細については、アクセスプロファイルを作成します。を参照してください。
- この画面では、鉛筆アイコンは無効になっています。

3. [**Create**] をクリックします。



編集

1. リストから目的の ICA ポリシーを選択します。

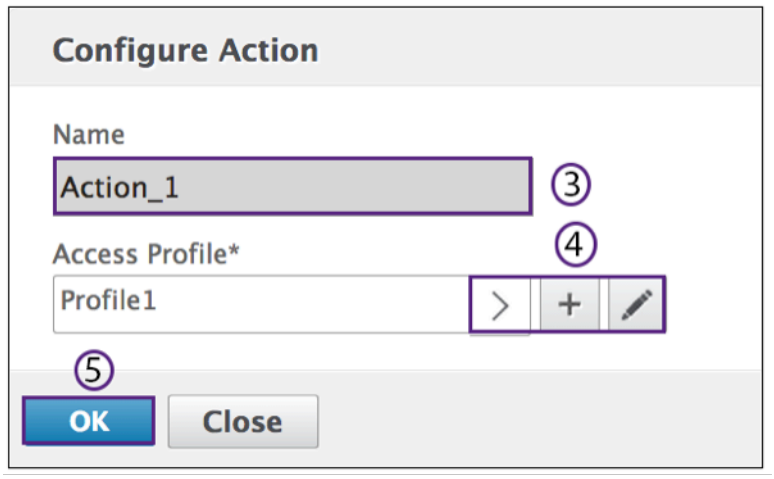


2. 詳細ウィンドウの [操作] タブで、[編集] をクリックします。

アクションの構成

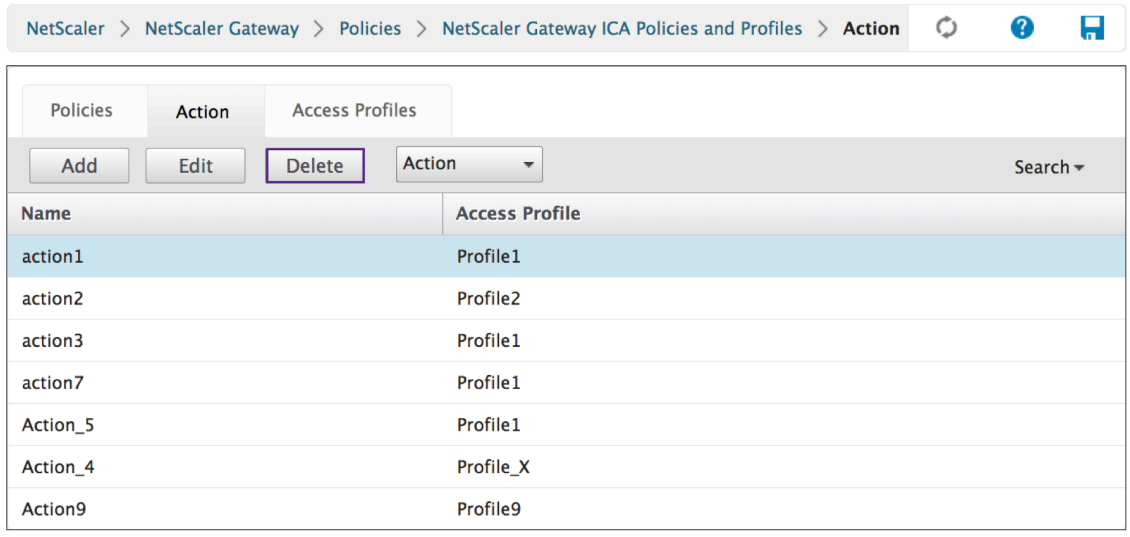
1.「アクション名」を確認し、目的のアクションを編集していることを確認します。このフィールドは編集できません。

2. [アクセスプロファイル] の横で、次のいずれかの操作を行います。
   - [**>**] をクリックして、既存のアクセスプロファイルを選択します。詳細については、(#common-processes) の [既存のアクセスプロファイルの選択] を参照してください。
   - [**+**] をクリックして、新しいアクセスプロファイルを作成します。詳細については、アクセスプロファイルの作成を参照してください。
   - 鉛筆アイコンをクリックして、アクセスプロファイルの設定をクリックします。
3. [**OK**] をクリックします。



削除

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［Citrix Gateway］>［操作］の順に展開し、［ICA］をクリックします。
2. リストから目的の ICA アクションを選択します。
3. 詳細ウィンドウの [操作] タブで、[削除] をクリックします。

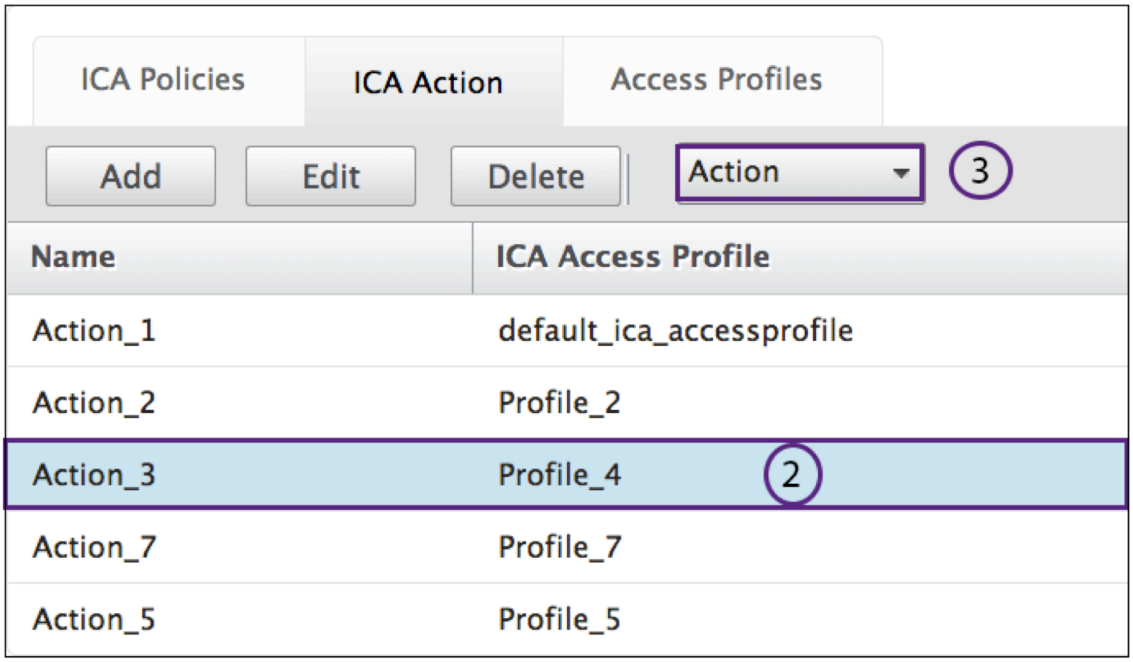


4. [はい] をクリックして、ポリシーを削除するアクションを確認します。

操作（アクション）

「ICA アクション」>「アクション」コマンドを使用して、アクションの名前を変更します。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［Citrix Gateway］>［操作］の順に展開し、［ICA］をクリックします。
2. リストから目的の ICA アクションを選択します。
3. 詳細ウィンドウの [操作] タブで、[操作] をクリックします。



4. ドロップダウンメニューから「アクション」>「名前変更」を選択します。
5. アクションの名前を変更します。
6. ［**OK**］をクリックします。

アクセスプロファイル

ICA プロファイルは、ユーザー接続の設定を定義します。

アクセスプロファイルでは、ユーザーデバイスがポリシー式の条件を満たしている場合に、ユーザーの Citrix Virtual Apps and Desktops 環境 ICA に適用されるアクションを指定します。構成ユーティリティを使用して、ICA ポリシーとは別に ICA プロファイルを作成し、そのプロファイルを複数のポリシーに使用できます。ポリシーで使用できるプロファイルは 1 つだけです。

アクセスプロファイルは、ICA ポリシーとは独立して作成できます。ポリシーを作成するときに、ポリシーにアタッチするアクセスプロファイルを選択できます。アクセスプロファイルは、ユーザーが利用できるリソースを指定します。[ポリシー] タブでは、次のコマンドを使用できます。

- 追加
- 編集
- 削除

設定ユーティリティを使用したアクセスプロファイルの作成

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、[Citrix Gateway］>［ポリシー］の順に展開し、[ICA］をクリックします。
2. 詳細ウィンドウで、[アクセスプロファイル] タブをクリックし、[追加] をクリックします。
3. プロファイルの設定を構成し、[作成]、[閉じる] の順にクリックします。プロファイルを作成したら、ICA ポリシーに含めることができます。

設定ユーティリティを使用したポリシーへのアクセスプロファイルの追加

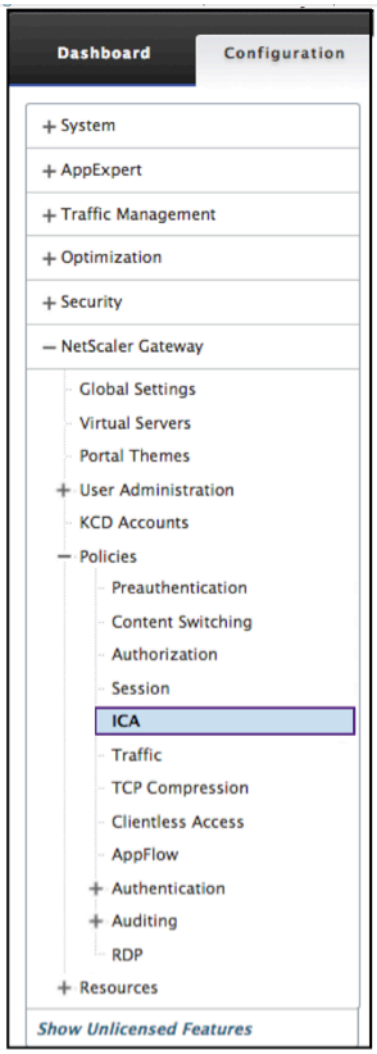
1. 構成ユーティリティのナビゲーションペインで、[Citrix Gateway］>［ポリシー］の順に展開し、[ICA］をクリックします。
2. [ポリシー] タブで、次のいずれかの操作を行います。
   - [追加] をクリックして、新しい ICA ポリシーを作成します。
   - ポリシーを選択し、[Open] をクリックします。
3.「アクション」メニューで、リストからアクセスプロファイルを選択します。
4. ICA ポリシーの構成を完了し、次のいずれかの操作を行います。

   a. [Create] をクリックし、[Close] をクリックしてポリシーを作成します。

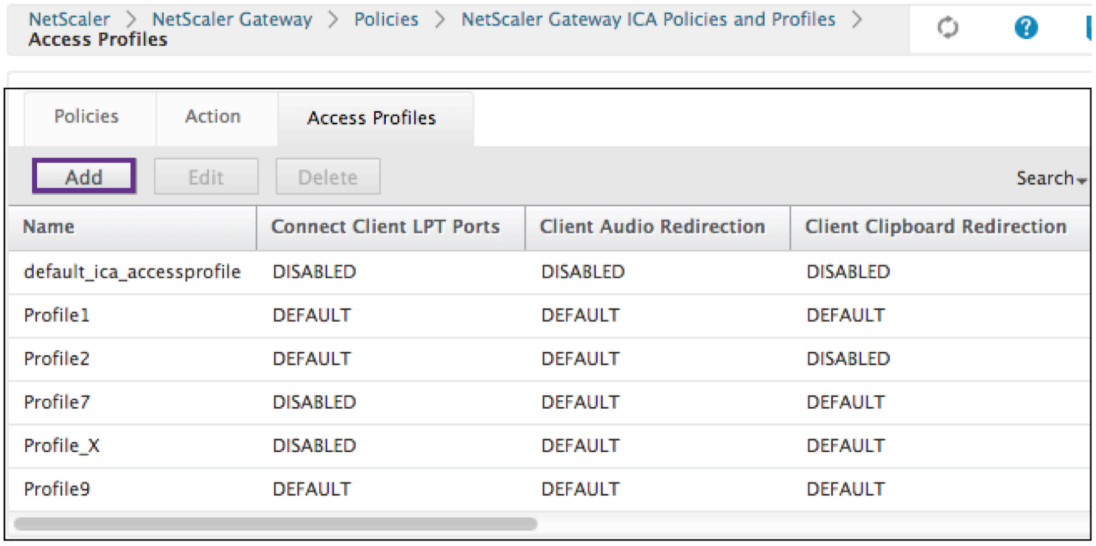
   b. [OK] をクリックし、[閉じる] をクリックしてポリシーを変更します。

追加

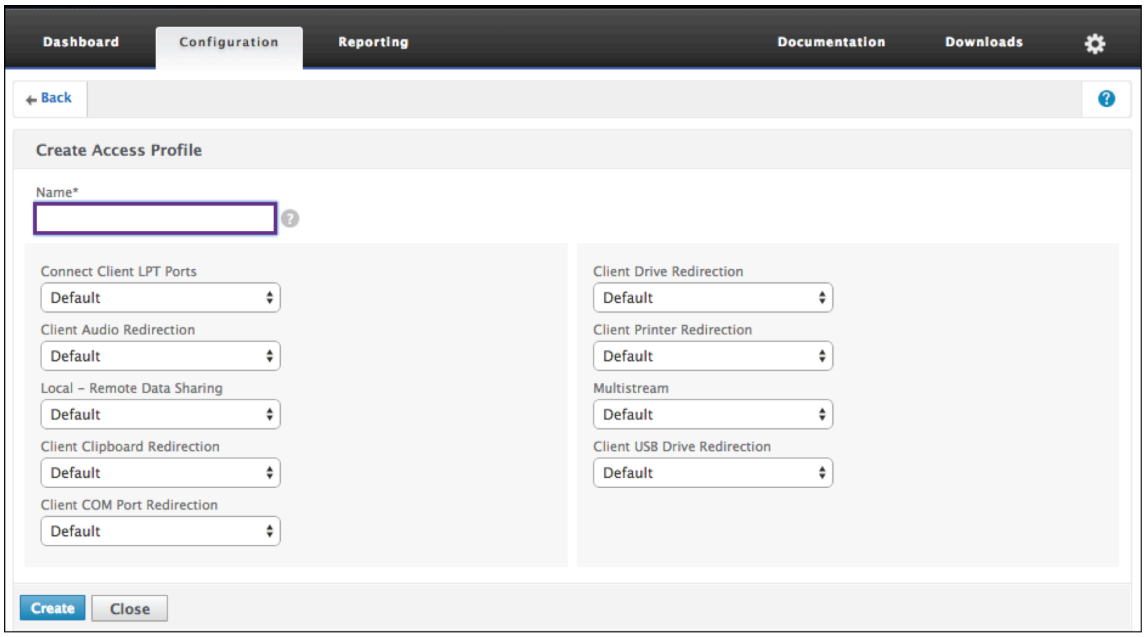
1. 構成ユーティリティの［構成］タブのナビゲーションペインで、[Citrix Gateway］>［ポリシー］の順に展開し、[ICA］をクリックします。



2. 詳細ペインの [アクセスプロファイル] タブで、[追加] をクリックします。**



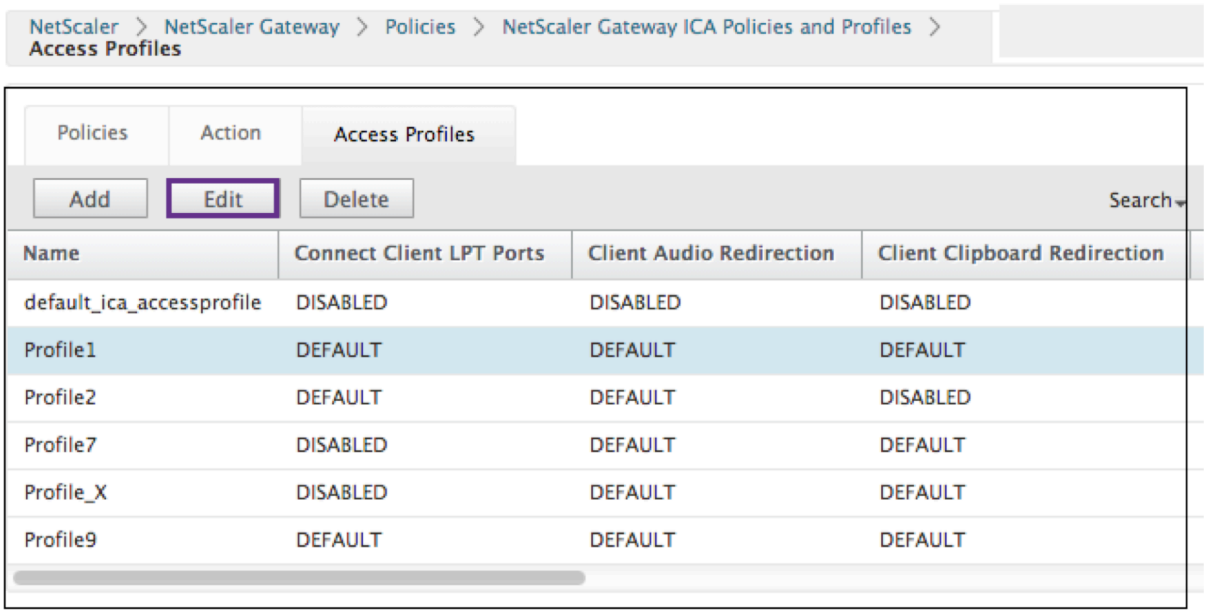
3. [名前] に、アクセスプロファイルの名前を入力します。これは必須フィールド ** です。**



4. 表示されるプルダウン・メニューから「デフォルト」または「無効」を選択して、アクセス・プロファイルを作成します。
5. [作成] をクリックします。

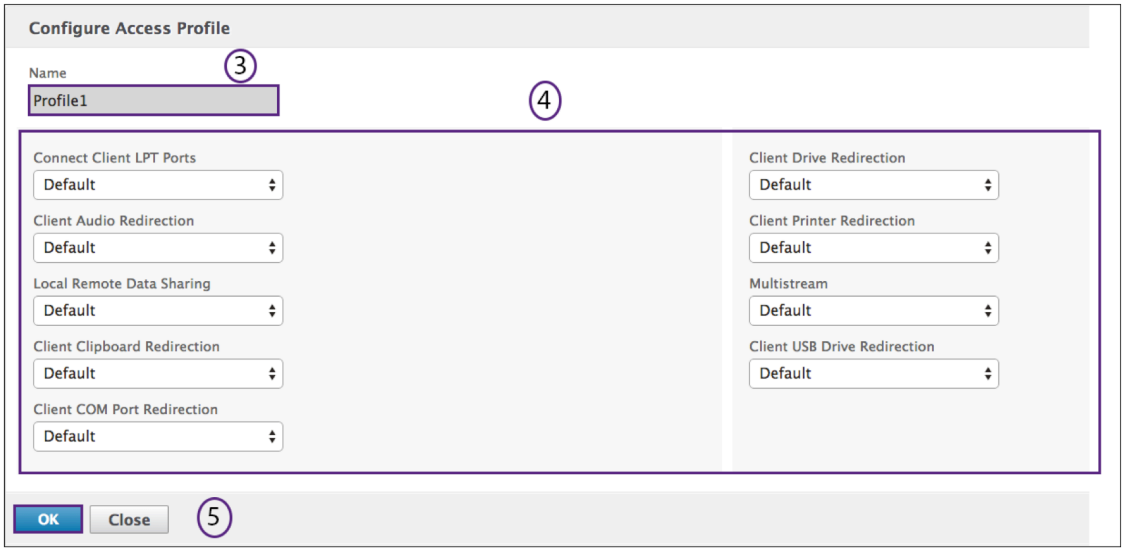
編集

1. 編集するアクセスプロファイルを選択します。
2. 詳細ペインの [アクセスプロファイル] タブで、[編集] をクリックします。



アクセスプロファイルの設定

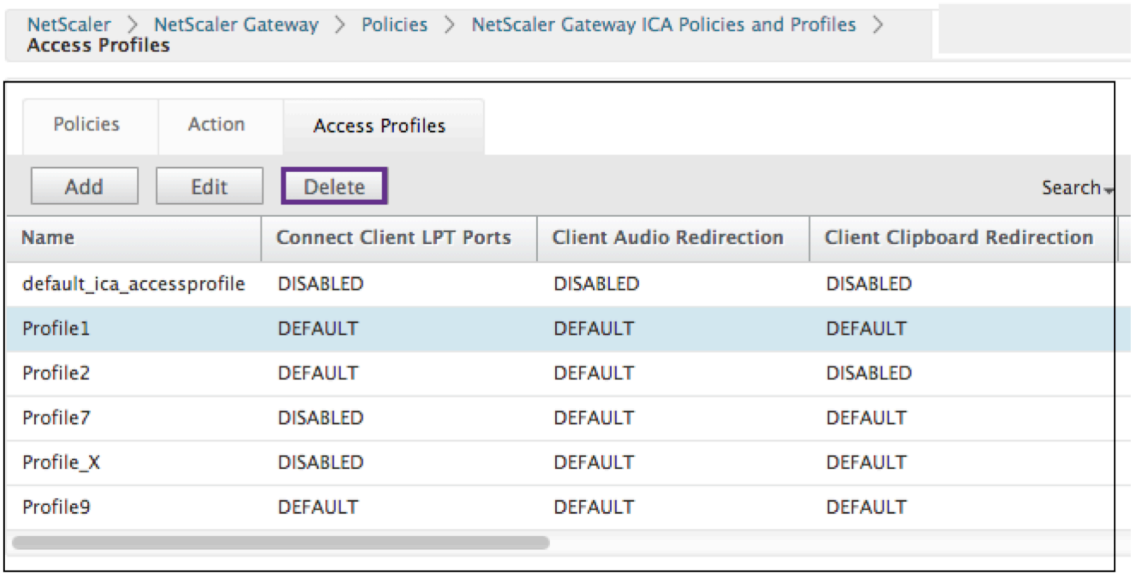
1. 名前が、改訂する名前であることを確認します。



2. プルダウン・メニューから「デフォルト」または「無効」を選択して、必要に応じて構成します。
3. [**OK**] をクリックします。

削除

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［Citrix Gateway］>［操作］の順に展開し、［ICA］をクリックします。
2. リストから目的の ICA アクションを選択します。
3. 詳細ウィンドウの [操作] タブで、[削除] をクリックします。

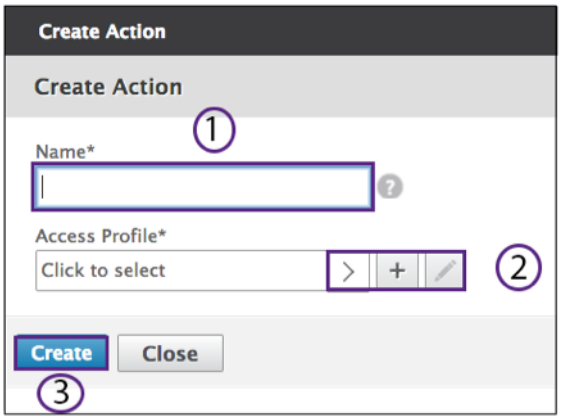


4. [**Yes**] をクリックして、削除するアクセスプロファイルを確認します。

共通プロセス

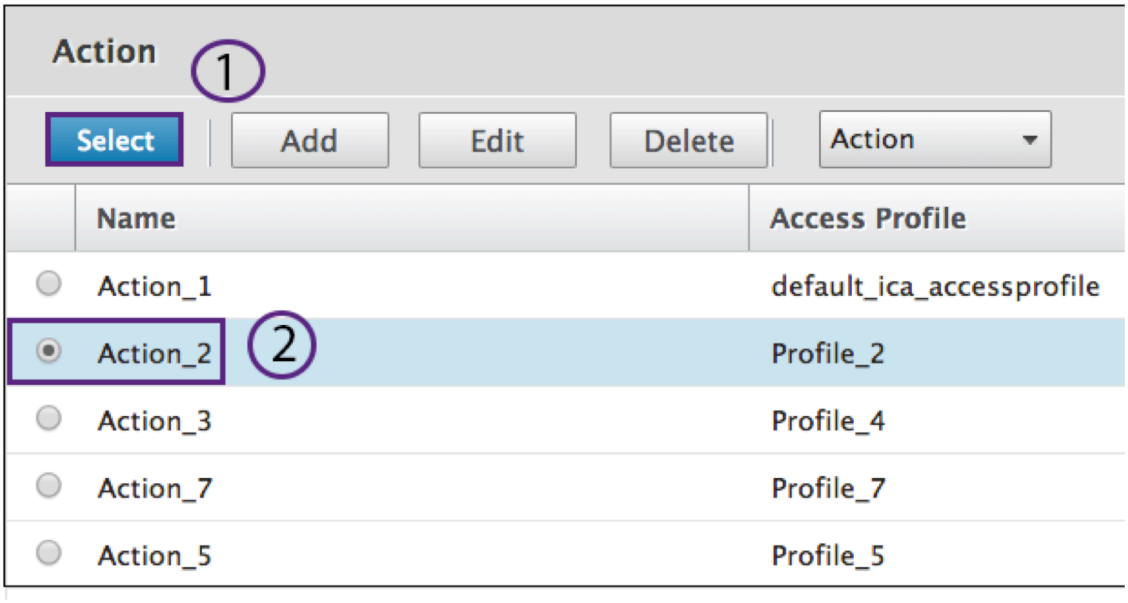
新しいアクションを作成する

1. アクションの名前を入力します。
2. アクセスプロファイルを指定するには、次のいずれかを選択します。
   - [**>**] をクリックして、既存のアクセスプロファイルを選択します。詳細については、(#common-processes) の [既存のアクセスプロファイルの選択] を参照してください。
   - [**+**] をクリックして、新しいアクセスプロファイルを作成します。詳しくは、アクセスプロファイルの作成を参照してください。
   - 鉛筆アイコンは無効になります。
3. [作成] をクリックします。



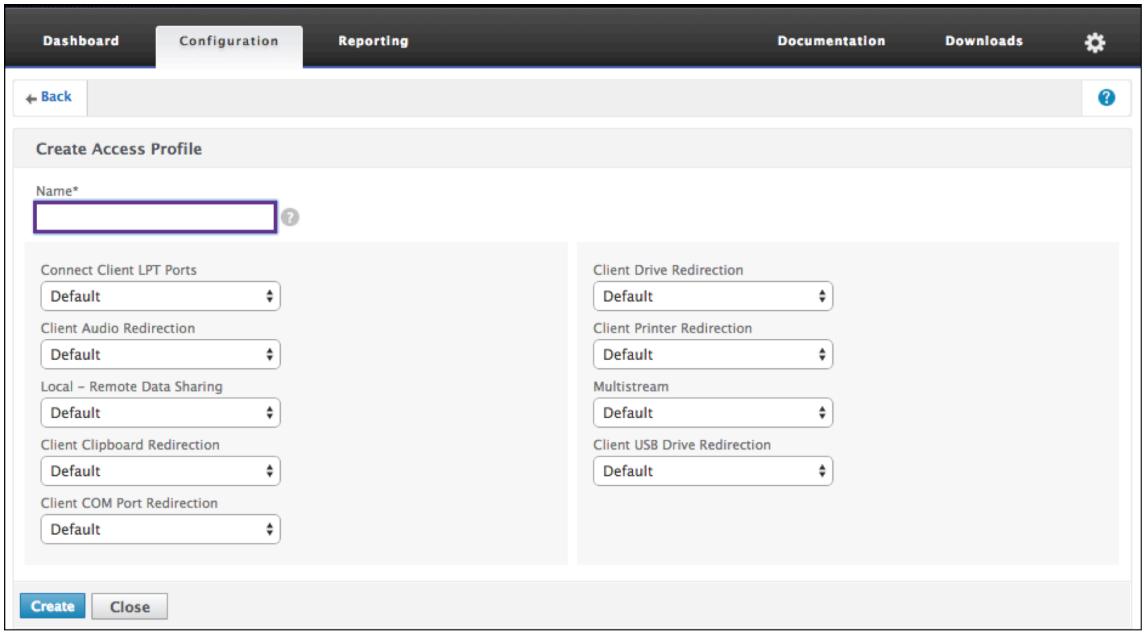
操作を選択

1. アクションの左側にあるラジオボタンをクリックして、アクションを選択します。関連付けられたアクセス・プロファイルは、許可されるユーザー機能を指定します。
2. [選択] ボタンをクリックします。



アクセスプロファイルの作成

1. アクセスプロファイルに名前を付けます。



2. このメニューからアクセスプロファイルを設定することもできます。

3.［作成］をクリックします。

既存のアクセスプロファイルの選択

1. アクセスプロファイルをクリックして選択します。
2.［編集］をクリックします。
3. アクセスプロファイルを設定します。詳しくは、アクセスプロファイルの設定を参照してください。

式

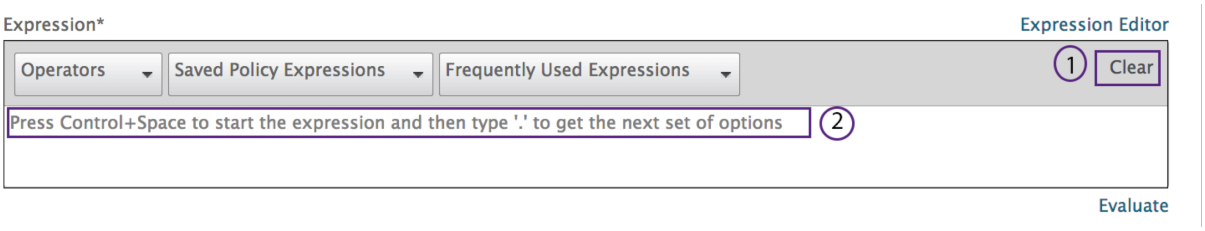
1. 既存の式を作成または修正するには、「消去」を選択します。

これらは典型的な ICA 式です。HTTP 式の場合は、「」を付けて名前を入力し、() を削除します。

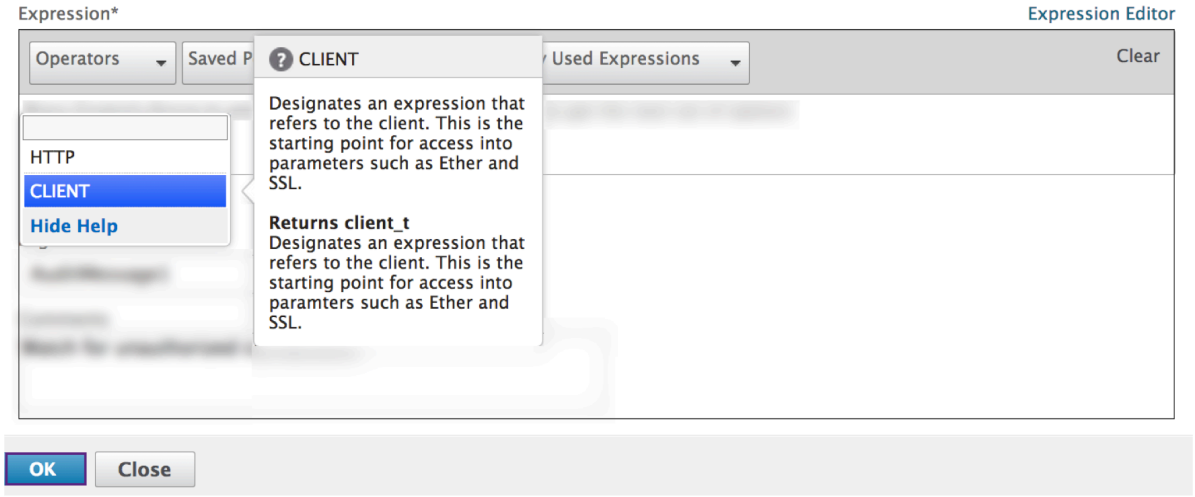
ICA.SERVER.PORT	この式は、指定されたポートが、ユーザーが接続しようとしている Citrix Virtual Appsand Desktops のポート番号と一致しているかどうかをチェックします。
ICA.SERVER.IP	この式は、指定された IP が、ユーザーが接続しようとしている Citrix Virtual Appsand Desktops 上の IP アドレスと一致しているかどうかをチェックします。
HTTP.REQ.USER.IS_MEMBER_OF(“”).NOT	この式は、指定されたグループ名のメンバーではないユーザーが現在の接続にアクセスしているかどうかをチェックします。
HTTP.REQ.USER.IS_MEMBER_OF(“groupname”)	この式は、現在の接続にアクセスするユーザーが指定したグループのメンバーであるかどうかをチェックします。
HTTP.REQ.USERNAME.CONTAINS(“”).NOT	この式は、現在の接続にアクセスしているユーザーが指定したグループのメンバーでないかどうかをチェックします。
HTTP.REQ.USERNAME.CONTAINS (「ユーザー名の入力」) ユーザー名のリソースを指定します。	この式は、現在の接続が指定された名前でアクセスしているかどうかをチェックします。
CLIENT.IP.DST.EQ(enter ip address here).NOT	この式は、現在のトラフィックの宛先 IP が、指定された IP アドレスと等しくないかどうかをチェックします。
CLIENT.IP.DST.EQ(enter ip address here)	この式は、現在のトラフィックの宛先 IP が、指定された IP アドレスと等しいかどうかをチェックします。

CLIENT.TCP.DSTPORT.EQ (enter port number).NOT	この式は、宛先ポートが指定されたポート番号と等しくないかどうかをチェックします。
CLIENT.TCP.DSTPORT.EQ (enter port number)	この式は、宛先ポートが指定されたポート番号と等しいかどうかをチェックします。

2. 同時に、[コントロール] と [スペース] バーを選択すると、オプションが表示されます。



3. 期間を入力します。選択を行い、スペースバーを押します。
4. 上の表の式の各ピリオドに、ピリオドを入力します。選択を行い、スペースバーを押します。
5. [**OK**] をクリックします。

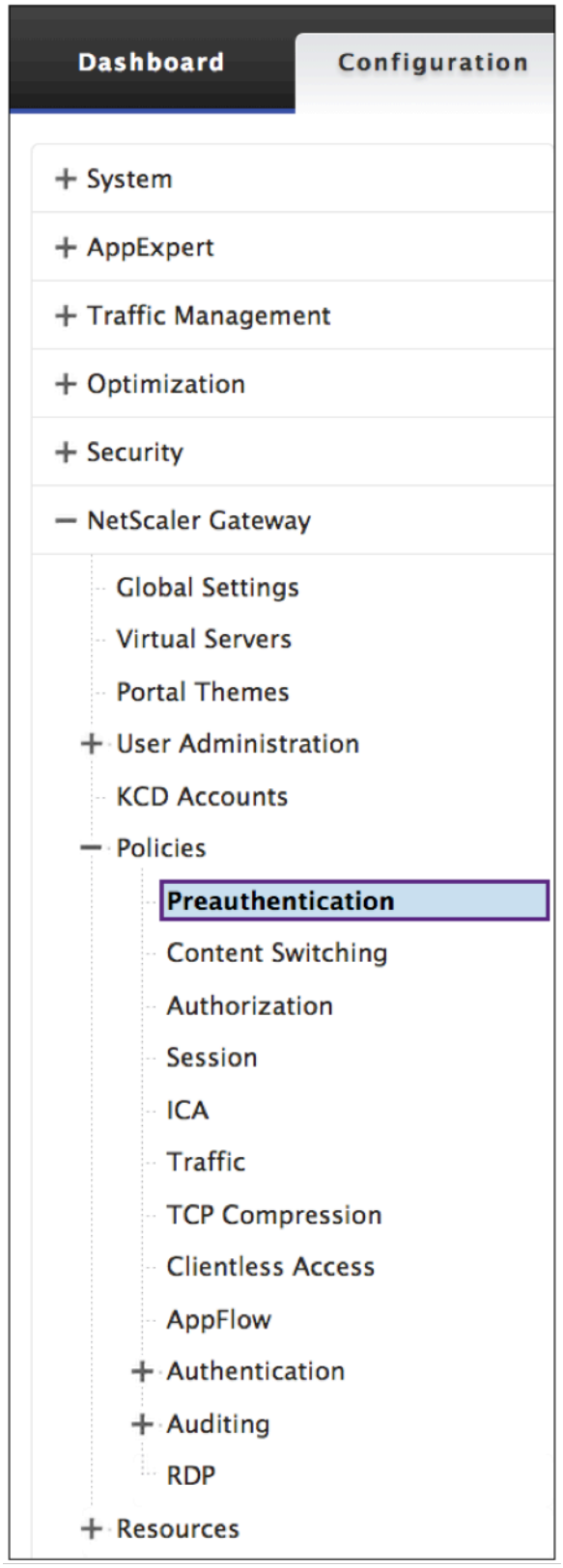


グループ識別

グループ名変数を持つ式は、事前認証関数またはセッション関数によって定義されます。

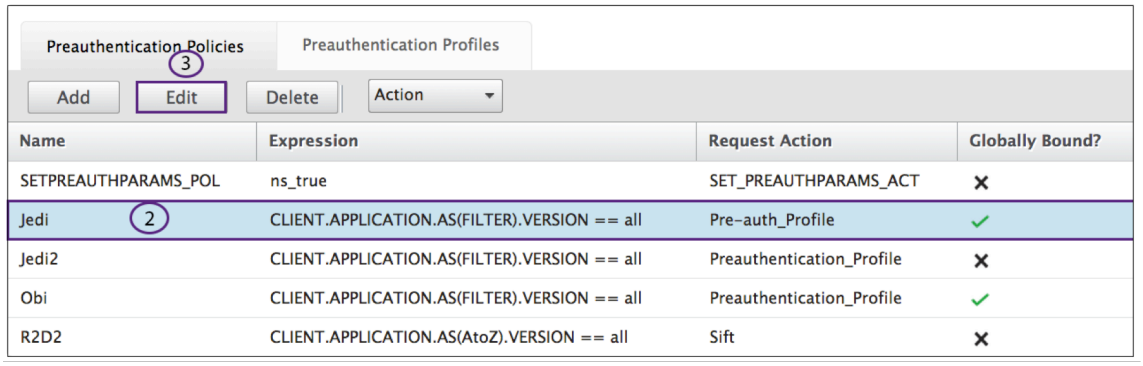
事前認証

1. 設定ペインで [事前認証] を選択します。

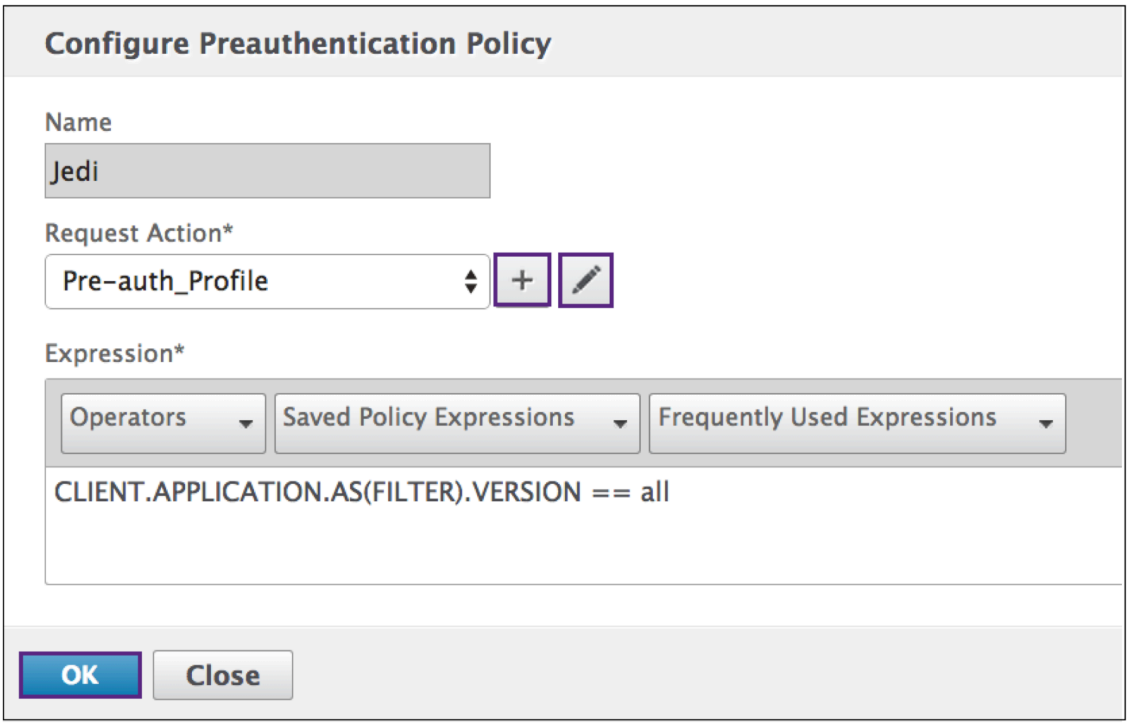


1. 事前認証ポリシーから名前を選択します。

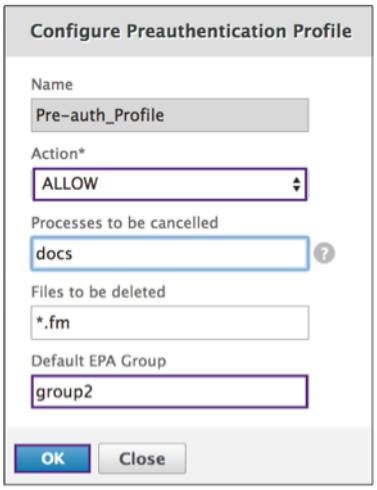
2. [事前認証ポリシー] タブで [編集] を選択します。



3.「アクションを要求」ダイアログボックスの横にある 鉛筆アイコンまたは「**+**」を選択します。

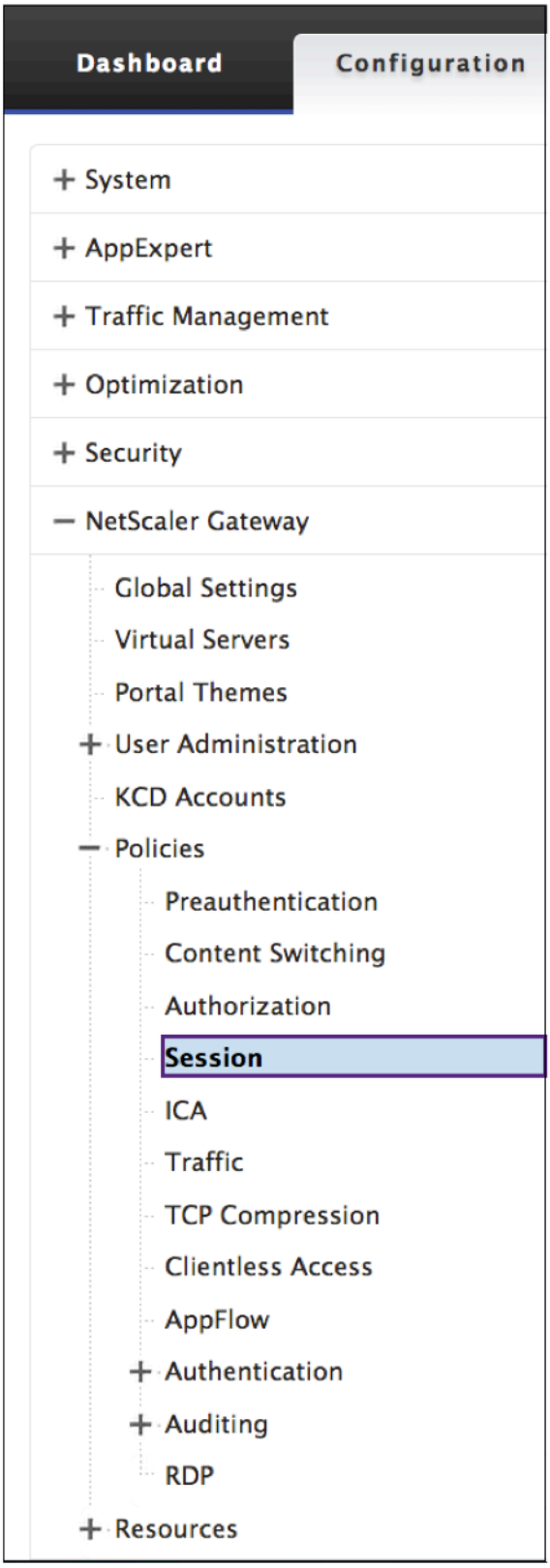


4. [<groupname> デフォルト EPA グループ] ダイアログボックスで (「」) を定義します。



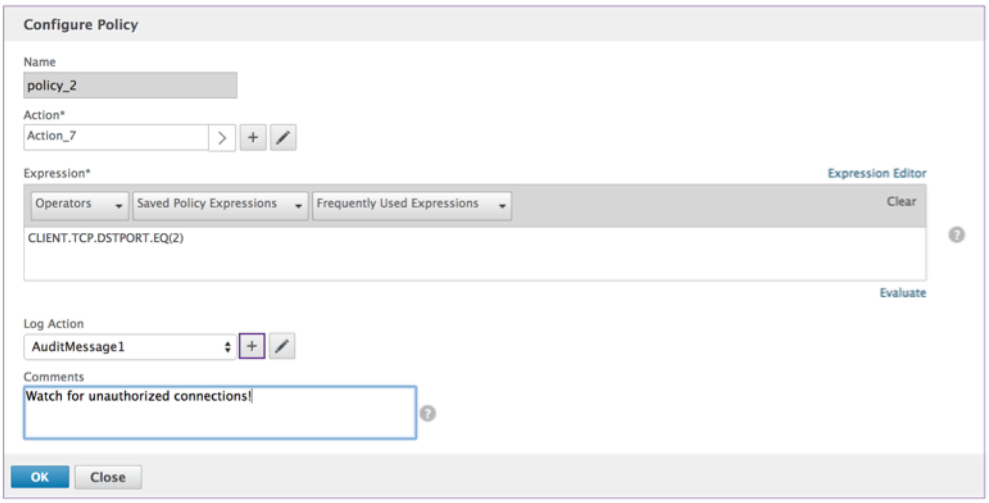
セッション

1. 設定ペインから [Session] を選択します。



ログアクションの作成

1. [ポリシーの設定] 画面で、[ログアクション] ダイアログボックスの横にある [+] アイコンを選択します。



監査メッセージ作成アクション

2. 「監査メッセージアクションの作成」画面が表示されます。監査メッセージに名前を付けます。監査メッセージには、数字、文字、またはアンダースコア文字のみを使用できます。

3. プルダウンメニューから、監査ログレベルを指定します。

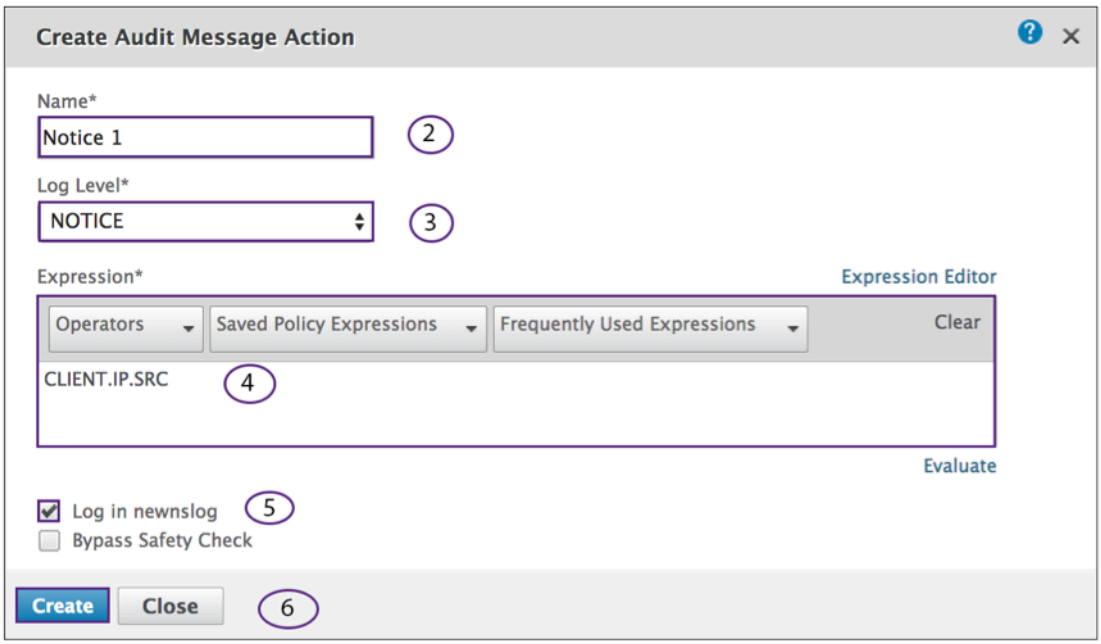
緊急	サーバー上の即時の危機を示すイベント。
アラート	アクションが必要なイベント。
重大	差し迫ったサーバーの危機を示すイベント。
エラー	何らかのエラーを示すイベント。
警告	近い将来に行動が必要なイベント。
ご注意	管理者が知っておくべきイベント。
情報	低レベル以外のすべてのイベント。
デバッグ	すべてのイベント, 極端な詳細.

4. 式を入力します。式は、ログの形式と内容を定義します。

5. チェックボックス。

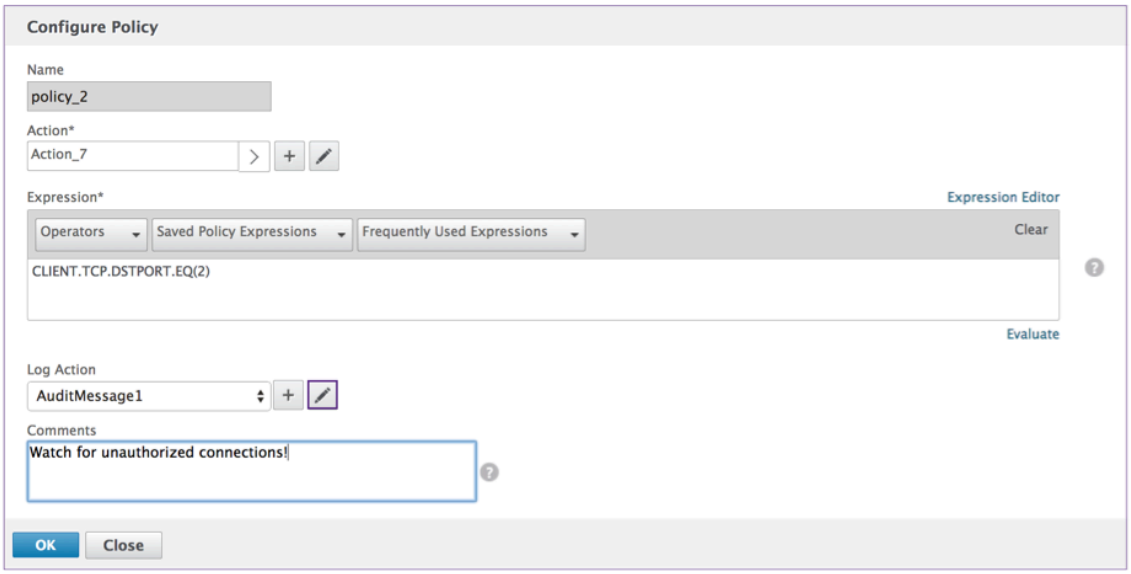
- 新しい ns ログにメッセージを送信するには、[newnslog にログイン] をオンにします。
- 安全チェックをバイパスするには、[安全チェックをバイパス] をオンにします。これにより、安全でない式が許可されます。

6. ［作成］をクリックします。



ログアクションの改訂

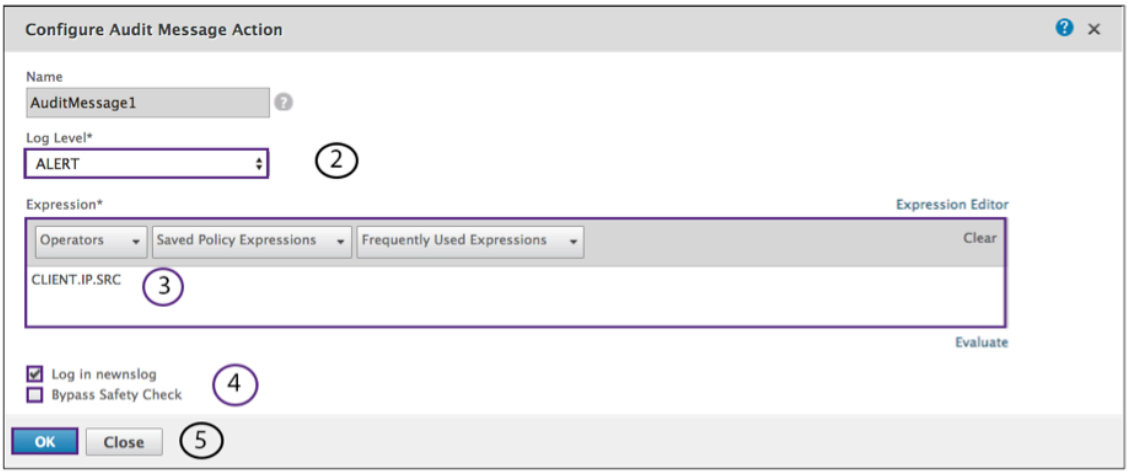
1. [ポリシーの構成] 画面で、[ログアクション] ダイアログボックスの横にあるアイコンをクリックします。



監査メッセージアクションの構成

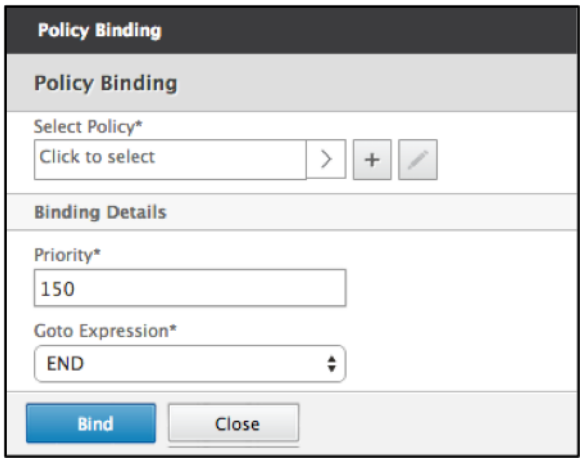
編集可能なフィールドは次のとおりです。

1. プルダウンメニューから、監査ログレベルを指定します。
2. 式を入力します。式は、ログの形式と内容を定義します。
3. チェックボックスは次のとおりです。
   - 新しい ns ログにメッセージを送信するには、[newnslog にログイン] をオンにします。
   - 安全チェックをバイパスするには、[安全チェックをバイパス] をオンにします。これにより、安全でない式が許可されます。
4. [**OK**] をクリックします。

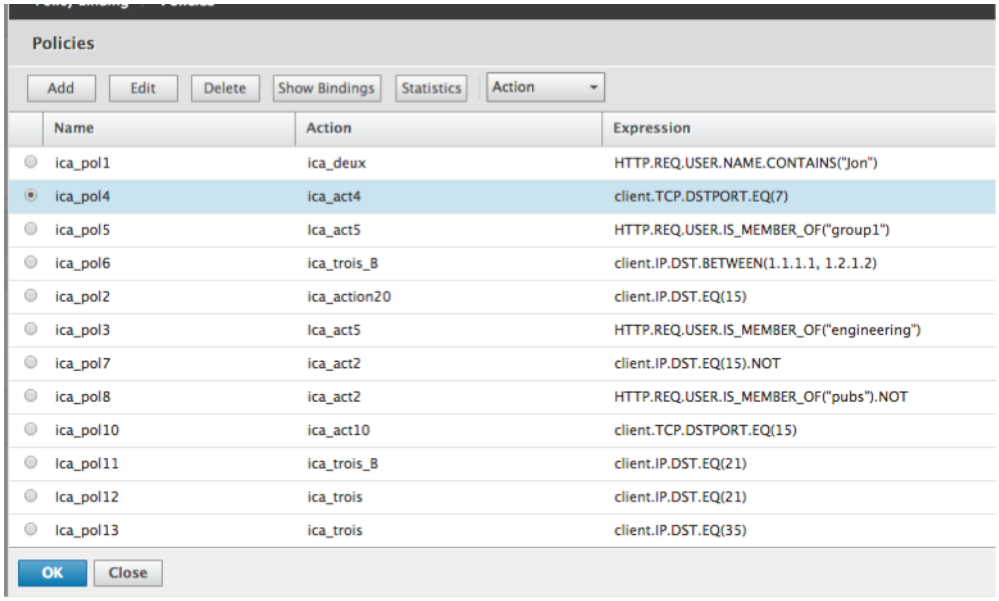


既存のポリシーの選択

1. [**>**] アイコンをクリックして、既存のポリシーを選択します。

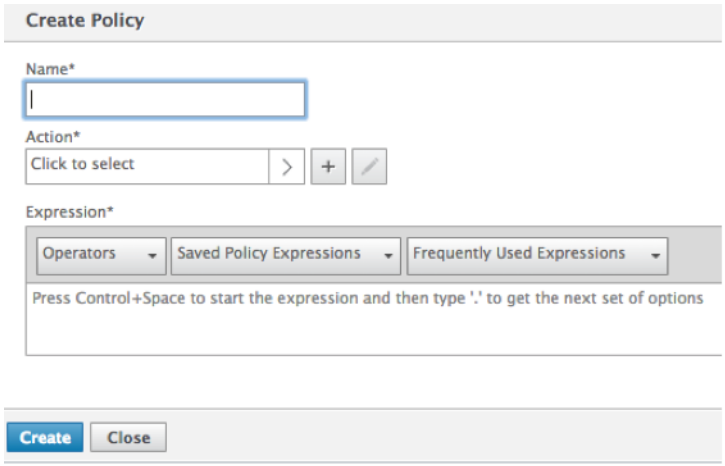


2. 目的のポリシーのオプションボタンを選択します。

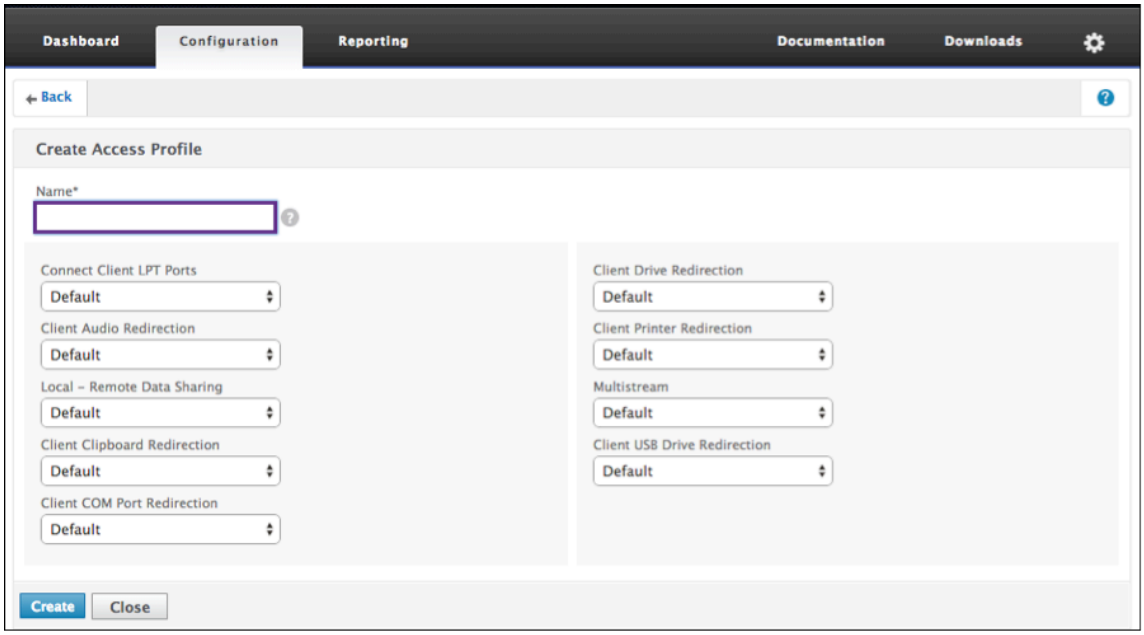


新しいポリシーの作成

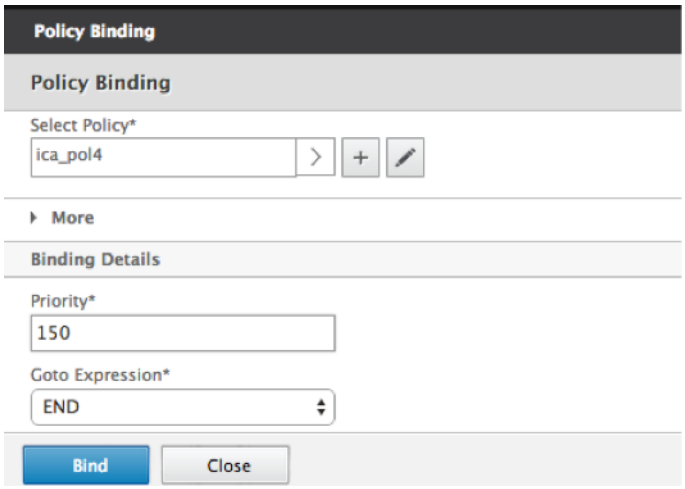
1. [名前] に、ポリシーの名前を入力します。これは必須フィールドです。
2. [**+**] をクリックして、新しいポリシーを作成します。



3. アクションを作成します。詳細については、「新しいアクションを作成する」を参照してください。
4. アクセスプロファイルに名前を付けます。



5. このメニューからアクセスプロファイルを設定します。
6. ［作成］をクリックします。
7. ［バインド］をクリックします。



事前認証および認証後のエンドポイント分析の設定

ここでは、認証後および認証前エンドポイント分析（EPA）の設定方法について説明します。

Smartcontrol を使用して認証後 EPA を設定するには、VPN セッションアクションから Smartgroup パラメータを使用します。EPA 式は VPN セッションポリシーで設定されます。

smartgroup パラメータのグループ名を指定できます。このグループ名は任意の文字列です。groupname は、アクティブディレクトリの既存のグループである必要はありません。

ICA ポリシーを HTTP.REQ.IS_MEMBER_OF（「グループ名」）という式で構成します。Smartgroup に対して以前に指定したグループ名を使用します。

Smartcontrol で事前認証 EPA を設定するには、事前認証プロファイルの Default EPA グループパラメータを使用します。EPA 式は、事前認証ポリシーで設定されます。

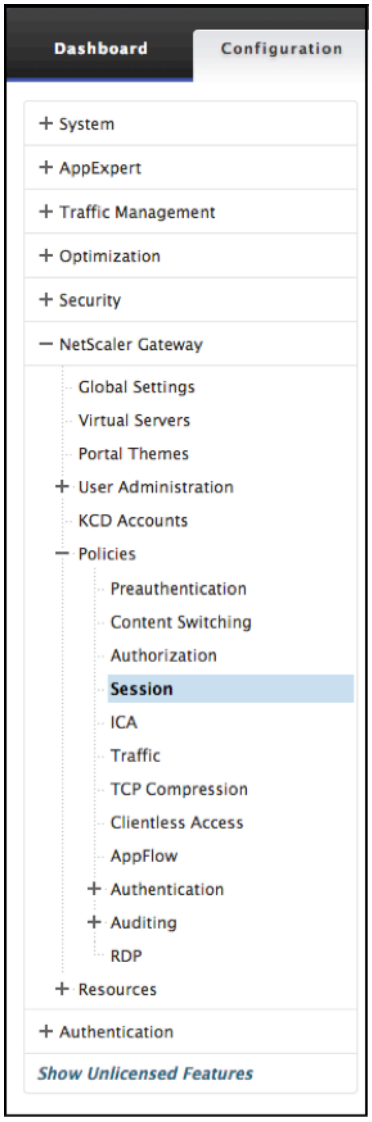
Default EPA グループパラメータには、グループ名を指定できます。このグループ名は任意の文字列です。groupname は、アクティブディレクトリの既存のグループである必要はありません。

ICA ポリシーを HTTP.REQ.IS_MEMBER_OF（「グループ名」）という式で構成し、デフォルト EPA グループに対して以前に指定したグループ名を使用します。

認証後の設定

以下の手順に従って、認証後の構成用にスマートグループを設定します。

1. ［Citrix NetScaler> ポリシー］ > ［セッション］に移動します。



2. [セッションプロファイル] > [追加] に移動します。

Citrix Gateway セッションプロファイルの作成

1. ［セキュリティ］ タブを選択します。
2. Citrix Gateway プロファイルの 名前を入力します（アクション）。
3. プルダウンメニューの右側にあるボックスを選択し、希望する デフォルトの承認アクションを選択します。

   ユーザーが内部ネットワークにログオンするときにアクセスできるネットワークリソースを指定します。認可のデフォルト設定では、すべてのネットワークリソースへのアクセスを拒否します。デフォルトのグローバル設定を使用し、承認ポリシーを作成して、ユーザーがアクセスできるネットワークリソースを定義することをお勧めします。デフォルトの認可ポリシーを DENY に設定した場合は、ネットワークリソースへのアクセスを明示的に許可する必要があります。これにより、セキュリティが向上します。

4. プルダウンメニューの右側にあるボックスを選択し、必要な **Secure Browse** を選択します。

   Citrix Workspace アプリを使用して、ユーザーが Citrix Gateway 経由で iOS および Android モバイルデバイスからネットワークリソースに接続できるようにします。セキュアなネットワーク内のリソースにアクセスするために、ユーザは完全な VPN トンネルを確立する必要はありません。

5. プルダウンメニューの右側にあるボックスを選択し、**Smartgroup** 名を入力します。

   これは、このセッションアクションに関連付けられている sessionpolicy が成功したときにユーザーが配置されるグループです。vpn セッションポリシーはポスト認証 EPA チェックを行い、チェックが成功した場合、ユーザは Smartgroup で指定されたグループに配置されます。次に、is_member_of (http.req.user.is_member_of) 式をポリシーとともに使用して、このスマートグループに属するユーザーに EPA が渡されたかどうかを確認できます。

6. ［作成］をクリックします。
7. Citrix NetScaler >Policies>**Session** の順に選択します。
8. [セッションポリシー] > [追加] に移動します。
9. このフィールドに 「名前」を入力します。

   これは、ユーザーが Citrix Gateway にログオンした後に適用される新しいセッションポリシーの名前です。

10. ドロップダウンメニューを使用して、「プロファイル」アクションを選択します。

    これは、ルール基準が満たされた場合に新しいセッションポリシーによって適用されるアクションです。

    > 目的のプロファイルを作成する必要がある場合は、[+] を選択します。詳細については、「**Citrix Gateway** セッションプロファイルの作成」を参照してください。

11. このフィールドに「式」と入力します。

    このフィールドは、ポリシーに一致するトラフィックを指定する名前付き式を定義します。式は、デフォルト構文またはクラシック構文のいずれかで記述できます。式のリテラル文字列の最大長は 255 文字です。長い文字列は、それぞれ 255 文字までの小さな文字列に分割でき、小さい文字列は + 演算子で連結されます。たとえば、500 文字の文字列を作成できます。”””+”””

    > 以下の要件は、Citrix ADC CLI にのみ適用されます。

    * 式に 1 つ以上のスペースが含まれる場合は、式全体を二重引用符で囲みます。式自体に二重引用符が含まれている場合は、文字を使用して引用符をエスケープします。また、一重引用符を使用してルールを囲むこともできます。では、二重引用符をエスケープする必要はありません。

12. ［作成］をクリックします。
13. セッションポリシーに移動します。
14. セッション・ポリシーの 名前を選択します。
15. 「アクション」ドロップダウンメニューから「グローバルバインディング」を選択します。
16. 「バインドを追加」を選択します。

17. 既存のポリシーを選択するには、**>** を選択します。

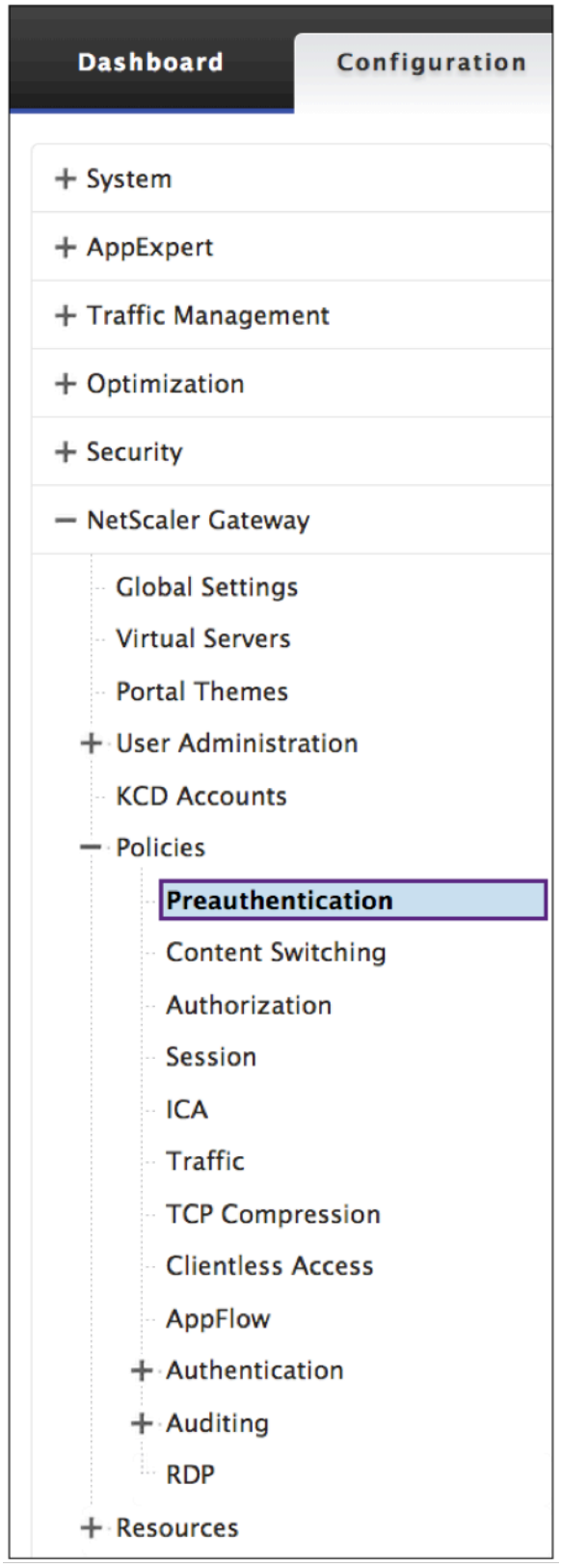
    注: 新しいポリシーを作成するには、[**+**] を選択します。詳細については、「**Citrix Gateway** セッションプロファイルの作成」を参照してください。

18. リストから名前を選択し、**Select** (選択) ボタンを押します。
19. [優先度] を入力し、[バインド] をクリックします。
20. [完了] をクリックします。
21. チェックによって、選択内容が [グローバルバインド] であることが示されます。

事前認証の設定

事前認証構成を設定するには、次の手順に従います。

1. ［Citrix NetScaler> ポリシー］ >［事前認証］の順に選択します。



2. [事前認証プロファイル] タブを選択し、[追加] を選択します。

3. 名前を入力

   これは、事前認証アクションの名前です。名前は、文字、数字、またはアンダースコア文字 (_) で始まり、文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等しい (=)、コロン (:)、およびアンダースコア文字のみで構成する必要があります。事前認証アクションが作成された後は変更できません。

   > 注：次の要件は、Citrix ADC CLI にのみ適用されます。
   > 名前に 1 つ以上のスペースが含まれる場合は、名前を二重引用符または一重引用符で囲みます。

4. ドロップダウンメニューから「アクションのリクエスト」を選択します。これは、接続がポリシーと一致したときにポリシーが呼び出すアクションです。

   > 注: 事前認証プロファイルを作成または作成する場合は、[+] を選択します。詳細については、事前認証プロファイルの作成を参照してください。

5. 式を入力

   これは、Citrix ADC 名前付きルールの名前、またはポリシーに一致する接続を定義するデフォルトの構文式です。

6. ［作成］をクリックします。
7. [事前認証ポリシー] タブに移動し、目的のポリシーを選択します。
8. 「アクション」ドロップダウンメニューから「グローバルバインディング」を選択します。
9. 「バインディングの追加」を選択します。
10. 既存のポリシーを選択するには、**>** を選択します。

    > [**+**] を選択して、新しいポリシーを作成します。詳細については、「Citrix Gateway セッションプロファイルの作成」を参照してください。

11. **[** ポリシー**]** を選択します。
12. [優先度] を入力し、[バインド] をクリックします。
13. ［完了］をクリックします。
14. このチェックでは、事前認証ポリシーが グローバルにバインドされていることが示されます。

事前認証プロファイルの作成

1. 「名前」を入力します。

   これは、事前認証アクション の名前です。名前は、文字、数字、またはアンダースコア文字 (_) で始まり、文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等しい (=)、コロン (:)、およびアンダースコア文字のみで構成する必要があります。事前認証アクションが作成された後は変更できません。

   > 以下の要件は、Citrix ADC CLI にのみ適用されます。
   > 名前に 1 つ以上のスペースが含まれる場合は、名前を二重引用符または一重引用符で囲みます。

2. ドロップダウン・メニューから「アクション」を入力します。

   このオプションは、エンドポイント分析 (EPA) の結果後にログオンを許可または拒否します。

3. キャンセルするプロセス

   このオプションは、エンドポイント分析 (EPA) ツールによって終了される一連のプロセスを指定します。

4. 削除するファイル

   このオプションは、エンドポイント解析 (EPA) ツールによって削除するファイルのパスと名前を指定する文字列を指定します。

5. デフォルト **EPA** グループ

   これは、EPA チェックが成功したときに選択されるデフォルトのグループです。

6. ［作成］をクリックします。

Web Interface へのシングルサインオンの設定

April 9, 2020

Web ベース認証を使用する内部ネットワーク内のサーバーにシングルサインオンを提供するように Citrix Gateway を構成できます。シングルサインオンを使用すると、SharePoint サイトや Web Interface などのカスタムホームページにユーザーをリダイレクトできます。Citrix Gateway プラグインを使用して、アクセスインターフェイスで構成されたブックマークや、ユーザーが Web ブラウザで入力した Web アドレスからリソースへのシングルサインオンを構成することもできます。

アクセスインターフェイスを SharePoint サイトまたは Web Interface にリダイレクトする場合は、サイトの Web アドレスを指定します。Citrix Gateway または外部認証サーバーによってユーザーが認証されると、ユーザーは指定されたホームページにリダイレクトされ、自動的にログオンします。ユーザクレデンシャルは、Web サーバに透過的に渡されます。Web サーバーが資格情報を受け入れると、ユーザーは自動的にログオンします。Web サーバがクレデンシャルを拒否すると、ユーザ名とパスワードを要求する認証プロンプトが表示されます。

Web アプリケーションへのシングルサインオンは、グローバルに構成することも、セッションポリシーを使用して構成することもできます。

スマートカードを使用して Web Interface へのシングルサインオンを構成することもできます。詳しくは、「スマートカードを使用した Web Interface へのシングルサインオンの構成」を参照してください。

Citrix Gateway は、次のバージョンの Web Interface で動作します。

- Web Interface 4.5
- Web Interface 5.0
- Web Interface 5.1
- Web Interface 5.2

- Web Interface 5.3
- Web Interface 5.4

シングルサインオンを構成する前に、Web Interface がすでに構成されており、Citrix Gateway で動作していることを確認してください。

Web アプリケーションへのシングルサインオンをグローバルに設定するには

March 26, 2020

シングルサインオンをグローバルに適用すると、すべての Web アプリケーションセッションを Citrix Gateway で認証するのではなく、Web サービスで認証できるようになります。

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで **Citrix Gateway** を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. **Citrix Gateway** のグローバル設定］ダイアログボックスの ［クライアントエクスペリエンス］タブで、［Web アプリケーションへの シングルサインオン］をクリックし、［**OK**］をクリックします。

セッションポリシーを使用して **Web** アプリケーションへのシングルサインオンを構成するには

March 26, 2020

1. 構成ユーティリティーの 構成タブのナビゲーションペインで、［**Citrix Gateway**］ > ［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ペインの [プロファイル] タブでポリシーを選択し、[追加] をクリックします。
3. [セッションポリシーの構成] ダイアログボックスで、[要求プロファイル] の横にある [変更] をクリックします。
4. [セッションプロファイルの構成] ダイアログボックスの [クライアントエクスペリエンス] タブで、[Web アプリケーションへのシングルサインオン] の横にある [グローバルオーバーライド] をクリックし、[**Web** アプリケーションへのシングルサインオン] をクリックして、[**OK**] をクリックします。

Web アプリケーションへのシングルサインオン用の **HTTP** ポートを定義するには

March 26, 2020

シングルサインオンは、宛先ポートが HTTP ポートと見なされるネットワークトラフィックに対してのみ試行されます。HTTP トラフィックにポート 80 以外のポートを使用するアプリケーションへのシングルサインオンを許可するには、Citrix Gateway で 1 つ以上のポート番号を追加します。複数のポートを有効にできます。ポートはグローバルに設定します。

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで **Citrix Gateway** を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [ネットワークの構成] タブで、[詳細設定] をクリックします。
4. [HTTP ポート] にポート番号を入力し、[追加] をクリックし、[**OK**] をクリックします。

> 注: 内部ネットワーク内の Web アプリケーションで異なるポート番号を使用する場合は、ポート番号を入力して [追加] をクリックします。Web Interface などの Web アプリケーションへのシングル・サインオンを許可するには、HTTP ポート番号を定義する必要があります。

その他の設定時の注意事項

March 26, 2020

Web Interface をシングル・サインオン用に構成する場合は、次のガイドラインに従ってください。

- 認証サービスの URL は https で始まる必要があります。
- Web Interface を実行するサーバーは、Citrix Gateway 証明書を信頼し、証明書の完全修飾ドメイン名（FQDN）を仮想サーバーの IP アドレスに解決できる必要があります。
- Web Interface は、Citrix Gateway 仮想サーバーへの接続を開くことができる必要があります。この目的にはどの Citrix Gateway 仮想サーバーでも使用できます。ユーザーがログオンする仮想サーバーである必要はありません。
- Web Interface と Citrix Gateway の間にファイアウォールがある場合、ファイアウォールルールによってユーザーアクセスが妨げられ、Web Interface へのシングルサインオンが無効になります。この問題を回避するには、ファイアウォールルールを緩和するか、Web Interface が接続できる別の仮想サーバーを Citrix Gateway 上に作成します。仮想サーバーには、内部ネットワーク内の IP アドレスが必要です。Web Interface に接続する場合は、セキュアポート 443 を宛先ポートとして使用します。
- 仮想サーバーのプライベート証明機関 (CA) からの証明書を使用している場合は、Microsoft 管理コンソール (MMC) で、証明書スナップインを使用して、Web Interface を実行しているサーバー上のローカルコンピュータの証明書ストアに CA ルート証明書をインストールします。
- ユーザーがログオンし、アクセス拒否のエラーメッセージが表示される場合は、Web Interface イベントビューアで詳細を確認してください。
- 公開アプリケーションまたはデスクトップに正常に接続するには、Citrix Gateway で構成した Secure Ticket Authority（STA）が、Web Interface で構成した STA と一致している必要があります。

Web Interface へのシングルサインオン接続をテストするには

March 26, 2020

Web Interface 用のシングル・サインオンを構成した後、クライアント・デバイスから Web ブラウザを開き、正常な接続をテストします。

1. Web ブラウザで、`https://NetScalerGatewayFQDN`と入力します。NetScalerGatewayFQDN は、仮想サーバーにバインドされた証明書内の完全修飾ドメイン名（FQDN）です。
2. Active Directory のドメインユーザーアカウントにログオンします。ログオン時に、Web Interface にリダイレクトされます。

アプリケーションは、追加の認証なしで自動的に表示されます。ユーザーが公開アプリケーションを起動すると、Citrix Workspace アプリは Citrix Gateway アプライアンスを介してファーム内のサーバーにトラフィックを転送します。

スマートカードを使用した **Web Interface** へのシングルサインオンの構成

October 22, 2021

ユーザーのログオンにスマートカードを使用する場合は、Web Interface へのシングルサインオンを構成できます。Citrix Gateway で設定を構成し、スマートカードでシングルサインオンを受け入れるように Web Interface を構成します。シングルサインオンは、パススルー認証とも呼ばれます。

Web Interface バージョン 5.3 および 5.4 では、スマートカードを使用した Web Interface へのシングル・サインオンがサポートされています。NetScaler バージョン 10 で使用可能な Citrix ADC 上の Web Interface 機能を有効にすると、スマートカードでシングルサインオンを使用することもできます。この機能の設定について詳しくは、「Citrix Gateway を介した Web Interface でのスマートカード認証の使用」を参照してください。

ユーザーは、証明書の操作でユーザー名の抽出が SubjectAltName: PrincipalName である限り、シングルサインオンが機能するために Active Directory 内の複数の CN グループに属することができます。パラメータ Subject: CN を使用する場合、ユーザーは複数の CN グループに属することはできません。

スマートカードを使用して Web Interface にシングルサインオンするように Citrix Gateway を構成するには、次の操作を行う必要があります。

- 認証局 (CA) からの署名付きサーバー証明書をインストールします。詳しくは、「Citrix Gateway への署名付き証明書のインストール」を参照してください。
- Citrix Gateway とユーザーデバイスにルート証明書をインストールします。
- Web Interface 用のログオンポイントとして仮想サーバーを作成します。仮想サーバーを構成するときは、クライアント証明書の SSL パラメーターを [Optional] に設定する必要があります。仮想サーバの設定の詳細については、仮想サーバーの作成を参照してください。

- SSL パラメータでクライアント認証を無効にするセカンダリ仮想サーバを作成します。この構成により、ユーザーは個人識別番号 (PIN) の二次要求を受信できなくなります。
- クライアント証明書の認証ポリシーを作成します。[ユーザー名フィールド] で、サブジェクト AltName: PrincipalName パラメータを使用して、複数のグループからユーザーを抽出します。[グループ名] フィールドは空白のままにします。
- Citrix Gateway でセッションポリシーとプロファイルを作成します。セッションプロファイル内で、ICA プロキシを有効にし、シングル・サインオンに使用する Web Interface とドメインを指定します。

スマートカードを使用したシングルサインオン用のセッションプロファイルを作成するには、次の手順に従います。

スマートカードを使用してシングルサインオン用のセッションプロファイルを作成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで［Citrix Gateway ポリシー］を展開し、［セッション］をクリックします。
2. 詳細ウィンドウで、[プロファイル] タブをクリックし、[追加] をクリックします。

3. [クライアントエクスペリエンス] タブで、[ホームページ] の横にある [グローバルに上書き] をクリックし、[ホームページの表示] をオフにします。

1.「Web アプリケーションへのシングル・サインオン」の横にある「グローバルに上書き」をクリックし、「Web アプリケーションへのシングル・サインオン」をクリックします。
2. ［Published Applications］タブをクリックします。
3. ICA プロキシの横にある「グローバルオーバーライド」をクリックし、「ON」を選択します。
4. [Web Interface アドレス] で、[グローバルに上書き] をクリックし、完全修飾ドメイン名 (FQDN) または Web Interface を入力します。
5. ［Single Sign-On Domain］で［グローバルに上書き］をクリックし、ドメイン名を入力します。

   > 注: domain.com の形式ではなく、ドメインの形式を使用する必要があります。

6. ［**Create**］をクリックしてから、［**Close**］をクリックします。

セッションプロファイルを完了したら、セッションポリシーを設定し、そのプロファイルをポリシーの一部として使用します。その後、セッション・ポリシーを仮想サーバにバインドできます。

スマートカードを使用してシングルサインオン用にクライアント証明書を構成するには

March 26, 2020

スマートカードを使用して Web Interface へのシングルサインオンを構成する場合は、[仮想サーバー] ダイアログボックスの [
証明書] で [

クライアント認証] を選択し、クライアント証明書を [
オプション] として構成する必要があります。[
必須] を選択すると、Web Interface へのシングルサインオンは失敗します。

1. 構成ユーティリティの [構成] タブのナビゲーションペインで、[Citrix Gateway] を展開し、[仮想サーバー] をクリックします。
2. 詳細ウィンドウで、仮想サーバーをクリックし、[開く] をクリックします。
3. Citrix Gateway 仮想サーバーの構成］ダイアログボックスの［証明書］タブで、［SSL パラメータ］をクリックします。
4. [SSL パラメータの構成] ダイアログボックスの [その他] で、[クライアント認証] をクリックします。
5. [クライアント証明書] で [オプション] を選択し、[OK] を 2 回クリックします。

Citrix Virtual Apps ファイル共有のシングルサインオンを構成するには

March 26, 2020

ユーザーが Citrix Virtual Apps を実行し、SmartAccess を使用してサーバーに接続している場合は、サーバーファームに接続するユーザーのシングルサインオンを構成できます。セッションポリシーとプロファイルを使用して公開アプリケーションへのアクセスを構成する場合は、サーバーファームのドメイン名を使用します。

また、ネットワーク内のファイル共有にシングルサインオンを構成することもできます。

1. 構成ユーティリティーの 構成タブのナビゲーションペインで、［**Citrix Gateway**］ > ［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ペインの [ポリシー] タブでセッションポリシーを選択し、[開く] をクリックします。
3. [セッションポリシーの構成] ダイアログボックスで、[要求プロファイル] の横にある [変更] をクリックします。
4. [セッションプロファイルの構成] ダイアログボックスの [公開アプリケーション] タブの [シングルサインオンドメイン] で [グローバル上書き] をクリックし、ドメイン名 を入力して **[OK**] を 2 回クリックします。

ファイルタイプの関連付けの許可

March 26, 2020

ファイルタイプの関連付けにより、ユーザーは Citrix Virtual Apps または Desktops 7 で公開されたアプリケーションでドキュメントを開くことができます。この権限を使用すると、信頼された環境にあるサーバー上のドキュメントを開いたり編集したり、ドキュメントがユーザーデバイスに送信されないようにすることができます。ファイルタイプの関連付けは、公開アプリケーションに関連付けられているドキュメントタイプに対してのみ使用できます。また、Citrix Gateway で仮想サーバーのプロパティが正しく構成されている場合にのみ使用できます。

リソースドキュメントを編集するための唯一の手段としてファイルタイプの関連付けを提供することは、ユーザーデバイスではなくサーバー上で編集を行う必要があるため、セキュリティを強化するのに役立ちます。たとえば、従業員が進行中のプロジェクト会議のレポートを投稿するファイル共有に対して、ファイルの種類の関連付けを許可し、ダウンロードまたはアップロードを行えるようにすることができます。

ファイルタイプの関連付けを行うには、次のことが必要です。

- ユーザーは、ユーザーデバイス上で Citrix Workspace アプリを実行します。
- ユーザーは、トラフィックポリシーがバインドされている仮想サーバーを介して接続し、Citrix Virtual Apps のポリシーを構成します。
- ユーザーは、Citrix Virtual Apps and Desktops 7 で目的のアプリケーションに割り当てられます。
- 管理者は、Citrix Gateway と連携するように Citrix 仮想アプリケーションを構成します。

ファイルタイプの関連付けを作成する手順は、次のとおりです。

- Web Interface サイトを作成します。
- Citrix Gateway でトラフィックポリシーを使用してファイルタイプの関連付けを構成する。
- Citrix Virtual Apps and Desktops 7 でファイル拡張子を定義する。

Web Interface サイトの作成

March 26, 2020

ファイルの種類の関連付けを使用するように Web Interface を構成するには、最初に Web Interface サイトを作成します。Web Interface サイトは、直接アクセス制御または高度なアクセス制御にすることができます。Web Interface サイトに次のディレクトリをコピーします。

- app_data
- 認証
- サイト

これらのディレクトリを Web Interface サイトにコピーすると、既存のディレクトリが上書きされます。

Web Interface 4.6 または 5.0 を使用している場合は、Web Interface サイトディレクトリに web.config ファイルを開き、次のコードを追加します。このコードは、Citrix サポートサイト（http://support.citrix.com/article/ctx116253）からダウンロードできます。

```
pre codeblock
<location path="site/contentLaunch.ica">
<system.web>
<httpHandlers>
<add verb="\*" path="\*.ica" type="System.Web.UI.PageHandlerFactory"/>
</httpHandlers>
</system.web>
</location>
```



```
<location path="site/contentLaunch.rad">
<system.web>
<httpHandlers>
<add verb="\*" path="\*.rad" type="System.Web.UI.PageHandlerFactory"/>
</httpHandlers>
</system.web>
</location>
<!--NeedCopy-->
```

このコードは、web.config ファイルの次のセクションの後に追加する必要があります。

```
pre codeblock
<location path="site/launch.rad">
        <system.web>
            <httpHandlers>
                <add verb="\*" path="\*.rad" type="System.Web.UI.
                   PageHandlerFactory"/>
            </httpHandlers>
        </system.web>
    </location>
<!--NeedCopy-->
```

ファイルタイプの関連付けのための **Citrix Gateway** の構成

October 22, 2021

Citrix Gateway でファイルタイプの関連付けを構成する前に、ファイルタイプの関連付けを使用するように Web Interface サイトを構成します。Web Interface を作成して構成したら、Citrix Gateway で設定を作成する必要があります。手順は次のとおりです。

- 新しい仮想サーバーを作成するか、既存の仮想サーバーを使用します。仮想サーバの作成の詳細については、仮想サーバーの作成を参照してください。
- Web Interface が設定された新しいセッションポリシーとプロファイルの作成。
- 仮想サーバーへのセッション・ポリシーのバインド。
- トラフィックポリシーの作成。

セッションポリシーを作成して仮想サーバにバインドしたら、トラフィックポリシーを作成し、仮想サーバにバインドします。

ファイルタイプの関連付けのトラフィックポリシーを設定する場合は、ファイル拡張子を定義する式を作成します。たとえば、Microsoft Word と Excel のファイルの種類の関連付けを有効にしたいとします。式の例を次に示します。

```
REQ.HTTP.URL == /\*.doc || REQ.HTTP.URL == /\*.xls
```


ファイルタイプの関連付けのセッションポリシーとプロファイルを作成するには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［**Citrix Gateway**］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. [公開アプリケーション] タブで、次の設定を構成します。
   a) [Web Interface アドレス] の横の [グローバル上書き] をクリックし、Web Interface の Web アドレスを入力します。
   b) [Web Interface Portal Mode] の横にある [グローバルに上書き] をクリックし、[標準] または [コンパクト] を選択します。
   c)［Single Sign-On Domain］の横にある［グローバルに上書き］をクリックし、ユーザーアカウントが存在するドメインの名前を入力して［作成］をクリックします。
7. [セッションポリシーの作成] ダイアログボックスで、[名前付き式] の横にある [**True value**] を選択し、[式の追加] をクリックし、[作成] をクリックして、[閉じる] をクリックします。

ファイルタイプの関連付けのトラフィックプロファイルを作成するには

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで［Citrix Gateway ポリシー］を展開し、［トラフィック］をクリックします。
2. 詳細ウィンドウで、[プロファイル] タブをクリックし、[追加] をクリックします。
3. [名前] に、プロファイルの名前を入力します。
4.「ファイルタイプの関連付け」で「ON」を選択し、「作成」をクリックしてから「閉じる」をクリックします。

トラフィックポリシーでファイルタイプの関連付けを構成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで［Citrix Gateway ポリシー］を展開し、［トラフィック］をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4.「要求プロファイル」で、プロファイルを選択します。
5. [トラフィックポリシーの作成] ダイアログボックスの [式] で、[高度なフリーフォーム] を選択し、[追加] をクリックします。
6. [式の追加] ダイアログボックスで、次の操作を行います。
   a) [式の種類] で、[一般] をクリックします。
   b)「フローの種類」で「REQ」を選択します。
   c)「プロトコル」で、「HTTP」を選択します。
   d)「修飾子」で「URL」を選択します。

e)「演算子」で「= =」を選択します。

f) [値] ボックスに「/*. ファイル拡張の種類」と入力します。. ファイル拡張の種類は.doc や.xls などのファイルの種類で、[**OK**] をクリックします。

7. [トラフィックポリシーの作成] ダイアログボックスの [式] で、[高度なフリーフォーム] の横にある [**OR**] をクリックします。
8. 追加するファイル拡張子ごとに手順 4、5、6 を繰り返し、「作成」をクリックし、「閉じる」をクリックします。

Citrix Gateway と Citrix Virtual Apps and Desktops の統合

March 26, 2020

公開リソースおよびデータへのアクセスを管理するには、StoreFront サーバーを展開および構成します。リモートアクセスの場合は、Citrix Gateway を StoreFront の前に追加することをお勧めします。

> 注
>
> Citrix Virtual Apps and Desktops を Citrix Gateway と統合する構成手順については、StoreFront のドキュメントを参照してください。

次の図は、Citrix Gateway を含む Citrix の簡易展開の例を示しています。Citrix Gateway は StoreFront と通信して、Citrix Virtual Apps and Desktops が配信するアプリやデータを保護します。ユーザーデバイスは Citrix Workspace アプリを実行してセキュリティで保護された接続を構築し、アプリ、デスクトップ、ファイルにアクセスします。

ユーザーは、Citrix Gateway を使用してログオンおよび認証を行います。Citrix Gateway は、DMZ で展開およびセキュリティ保護されます。2 要素認証が構成されます。ユーザーの資格情報に基づいて、ユーザーに該当のリソースおよびアプリケーションが提供されます。アプリケーションとデータは適切なサーバー上に存在します（図には表示されていません)。セキュリティ上機微なアプリケーションとデータについては、別のサーバーが使用されます。

Citrix Gateway と StoreFront の統合

March 26, 2020

Citrix Virtual Apps and Desktops ウィザードを使用して、StoreFront と Citrix Gateway を統合します。この統合により、Citrix Gateway を介して、ホストされた仮想デスクトップ（XenDesktop）およびホストされた Windows 仮想アプリケーション（XenApp）へのアクセスが容易になります。

Storefront と Citrix Gateway をシームレスに統合するために、Citrix Virtual Apps and Desktops ウィザードのワークフローが次の機能で強化されました。

- サポートされている **StoreFront** で構成されたストアの取得：サポートされている Store Front で構成されたストアをクリックするだけで取得できます。これにより、手作業による介入を避けるため、人為的なミス（タイプミス）を避けることができます。
- **StoreFront** 構成ファイルのエクスポートサポート：**StoreFront** 構成ファイルは Citrix Gateway でエクスポートできます。このファイルは、サポートされている StoreFront サーバーにダウンロードしてインポートできます。ファイルがインポートされると、NetScaler の統合が完了します。
- 認証サーバーとしての **StoreFront**： 認証サービスの認証サーバーとして StoreFront を使用する高度な認証アクションを導入することで、認証が簡略化されます。

> 注:
> 認証サーバーは、Citrix Virtual Apps and Desktops 以外の展開にも使用できます。

StoreFront で使用するように **Citrix Gateway** を構成する方法

前提条件

NetScaler を StoreFront と統合するには、次の情報が必要です。

- Citrix Gateway 仮想サーバーの IP アドレス
- StoreFront サーバーの完全修飾ドメイン名（FQDN）
- Citrix Gateway のサーバー証明書
- 認証サーバの詳細

以下についても、確認してください。

- Citrix Gateway と StoreFront 間のファイアウォールポートが開いている
- StoreFront に LAN アクセス可能

Citrix GatewayGUI を使用して **StoreFront** と **Citrix Gateway** を統合するには:

1. ［構成］> ［**Citrix Virtual Apps and Desktops** ］に移動します。
2. [は じめに**]** をクリックします。
3.「**StoreFront** 」を選択し、「続行」をクリックします。
4. ［Citrix Gateway］エリアで次のフィールドに値を入力し、［続行］をクリックします。
    - **Gateway** の完全修飾ドメイン名 — Citrix Gateway の完全修飾ドメイン名
    - **GatewayIP** アドレス — Citrix Gateway の IP アドレス
    - ポート — Citrix Gateway のポート
5. [サーバー証明書] 領域に次のファイルをインポートし、[続行] をクリックします。証明書ファイル -Citrix Gateway のサーバー証明書。
6. **StoreFront** 領域に次の情報を入力し、「続行」をクリックします。
    - **StoreFront URL** — StoreFront サーバーの URL

- **Receiver for Web** パス -StoreFront で既に構成されている Web サイトへのパス
- デフォルトの **Active Directory** ドメイン -内部ネットワークのシングルサインオンアプリケーションに使用されるシングルサインオンドメイン
- **Secure Ticket Authority URL** — Secure Ticket Authority URL。これは通常、配信 Controller 上に存在します。

> 注**:**「
> ストアの取得」Citrix Gateway が StoreFront に接続し、StoreFront で構成されているすべてのストア情報を返します。次に、ドロップダウンメニューから [優先するストア] を選択します。「ストアの取得」オプションは、最新の StoreFront サーバーでのみ機能します。

7. 新しい認証設定では、ユーザーは新しい認証ポリシーを作成するか、既存の認証ポリシーを使用できます。

   新しいドメインベース認証ポリシーを作成するには、の次のフィールドに値を入力し、[**Continue**] をクリックします。

8. ドロップダウンメニューから認証タイプ **-** ドメインの選択を選択します。
9. [新しいサーバーの追加**]** または ****[**要件に基づいて既存のサーバーを使用する]** を選択します。
   - **IP** アドレス：ドメイン・サーバの IP アドレス
   - ポート：ドメイン・サーバのポート
   - ベース **DN** -ユーザーが配置されるベース DN
   - サービスアカウント -Active Directory のクエリに使用するアカウント
   - パスワード -ドメイン・サーバへのログオンに必要なパスワード
   - タイムアウト：ドメイン・ディレクトリが検索される期間
   - サーバーのログオン名属性 -NetScaler アプライアンスが外部ドメインサーバーまたは Active Directory を照会するために使用する名前属性。

   オプションで [接続のテスト] をクリックすると、サーバが到達可能であり、有効な資格情報が提供されていることを確認できます。

   > 注：既存の認証ポリシーを使用するには、「認証タイプの選択」ドロップダウンから必要な認証タイプを選択し、上記の情報を入力します。

10. [Citrix Gateway の設定］ページで［完了］をクリックします。
11. [ファイルのダウンロード**]** をクリックします。

StoreFront GUI で必要な構成手順は次のとおりです。

1. Gateway 構成の.zip ファイルを StoreFront にコピーします。
2. [ストア] をクリックします。
3. [**Citrix Gateway** の管理］を選択し、[**Citrix Gateway** の管理］ウィンドウで［ファイルからインポート］リンクをクリックします。
4. [**NetScaler** 構成のインポート**]** ウィンドウの [ファイルの選択] 領域で、[次へ] をクリックします。

5. ［ログオンタイプの選択］領域で、オプションで StoreFront が Citrix Gateway に接続するための コールバック **URL** を指定し、［次へ］をクリックします。
6. 「チケット認証局」で「次へ」をクリックします。
7. [変更の確認] で、[次へ] をクリックします。
8. ［完了］をクリックします。

Citrix Endpoint Management 環境の設定の構成

April 9, 2020

Citrix Endpoint Management 用 Citrix ADC ウィザードの指示に従って、Citrix Endpoint Management 展開用の Citrix ADC 機能の構成を行います。このウィザードを使用すると、次の操作を実行できます。

- マイクロ **VPN** を設定します。このシナリオでは、リモートユーザーは内部ネットワークのアプリやデスクトップにアクセスできます。
  - Citrix Endpoint Management MAM 専用モードでは、認証に Citrix Gateway を使用する必要があります。
  - MDM の展開では、モバイルデバイス VPN として Citrix Gateway をお勧めします。
  - ENT 展開では、ユーザーが MDM 登録をオプトアウトすると、デバイスは従来の MAM モードで動作し、Citrix Gateway の FQDN を使用して登録されます。
- 証明書ベースの認証を構成します。**Citrix Endpoint Management** デフォルト構成は、ユーザー名とパスワード認証です。Citrix Endpoint Management 環境への登録とアクセスのセキュリティをさらに強化するには、証明書ベースの認証の使用を検討してください。
- **Citrix Endpoint Management** サーバーの負荷を分散します。Citrix ADC の負荷分散は、複数の Citrix Endpoint Management サーバーがある場合、または Citrix Endpoint Management が DMZ または内部ネットワーク内にある場合（したがって、デバイスから Citrix ADC にトラフィックが流れる）、すべての Citrix Endpoint Management デバイスモードに必要です。このシナリオでは、Citrix ADC アプライアンスはユーザーデバイスと Citrix Endpoint Management サーバー間の DMZ に存在し、モバイルデバイスから Citrix Endpoint Management サーバーに暗号化された送信データを負荷分散します。
- メールフィルタリング機能を備えた **Microsoft Exchange** サーバの負荷を分散します。このシナリオでは、Citrix ADC アプライアンスは、ユーザーデバイスと Citrix Endpoint Management Citrix ADC コネクタ（XNC）との間、およびユーザーデバイスと Microsoft Exchange CAS サーバーの間にあります。ユーザーデバイスからの要求はすべて Citrix Gateway アプライアンスに送信され、XNC と通信してデバイスに関する情報を取得します。XNC からの応答に応じて、Citrix ADC アプライアンスはホワイトリストに登録されたデバイスから内部ネットワークのサーバーに要求を転送するか、ブラックリストに登録されたデバイスからの接続を切断します。

- 要求されたコンテンツの種類に基づいて、**ShareFile** ストレージゾーン・コネクタのロード・バランシングを行います。このシナリオでは、StorageZones Controller 環境に関する基本情報の入力を求められ、次の処理を行う構成が生成されます。
  - ストレージ・ゾーン・コントローラ間でトラフィックのロード・バランシングを行います。
  - ストレージ・ゾーン・コネクタのユーザー認証を提供します。
  - ShareFile アップロードとダウンロードの URI 署名を検証します。
  - Citrix ADC アプライアンスで SSL 接続を終了します。

ShareFile の構成について詳しくは、「StorageZones Controller 用の Citrix ADC 構成」を参照してください。

> 重要
>
> Citrix Endpoint Management ウィザードを使用する前に、以下の Citrix Endpoint Management の展開に関する記事を参照して、設計と展開に関する情報と推奨事項を確認してください。
>
> Citrix Endpoint Management 統合
>
> Citrix Gateway および Citrix ADC との統合
>
> MDX アプリの SSO とプロキシの考慮事項
>
> 認証
>
> Citrix Endpoint Management 用 Citrix ADC ウィザードは、1 回だけ使用できます。テスト環境、開発環境、実稼働環境など、複数の Citrix Endpoint Management インスタンスが必要な場合は、追加の環境用に Citrix ADC を手動で構成する必要があります。以下のサポート記事では、ウィザードで実行されるコマンドの一覧と、それらのコマンドを実行して新しい Citrix ADC インスタンスを作成する方法を説明します。
>
> Citrix ADC-SSL ブリッジで Citrix Endpoint Management ウィザードによって生成されるコマンド
>
> Citrix ADC-SSL オフロードで Citrix Endpoint Management ウィザードによって生成されるコマンド

Citrix ADC 機能のライセンス要件

以下の Citrix ADC 機能を有効にするには、ライセンスをインストールする必要があります。

- Citrix Endpoint Management MDM 負荷分散には、Citrix ADC 標準ライセンスが必要です。
- ストレージゾーンを使用した ShareFile 負荷分散には、Citrix ADC 標準ライセンスが必要です。
- Exchange の負荷分散には、Citrix ADC ライセンスまたは統合キャッシュライセンスを追加した Advanced ライセンスが必要です。

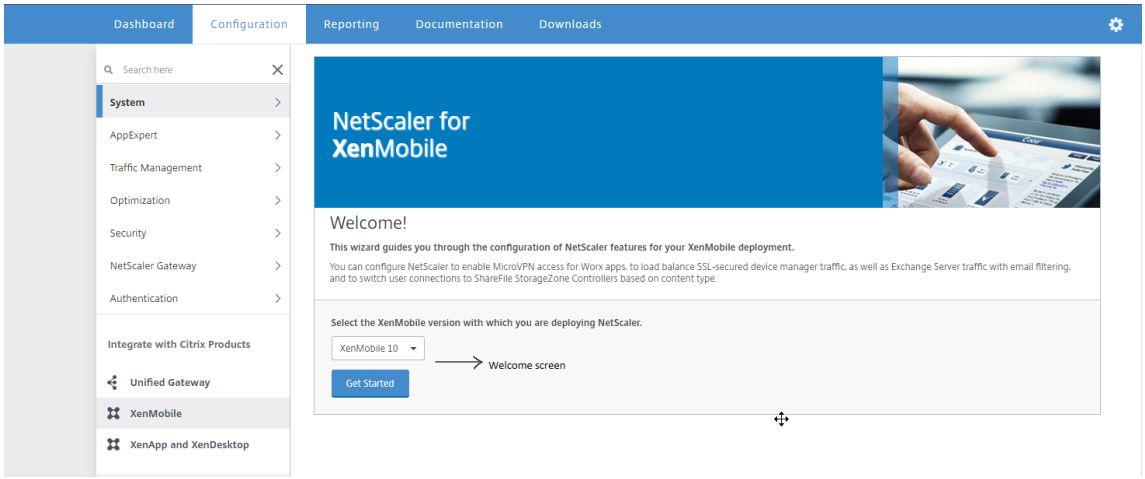
Citrix Endpoint Management ウィザード用 **Citrix ADC** ウィザード

このセクションでは、Citrix ADC for Citrix Endpoint Management ウィザードを使用して以下の操作を行う例を示します。

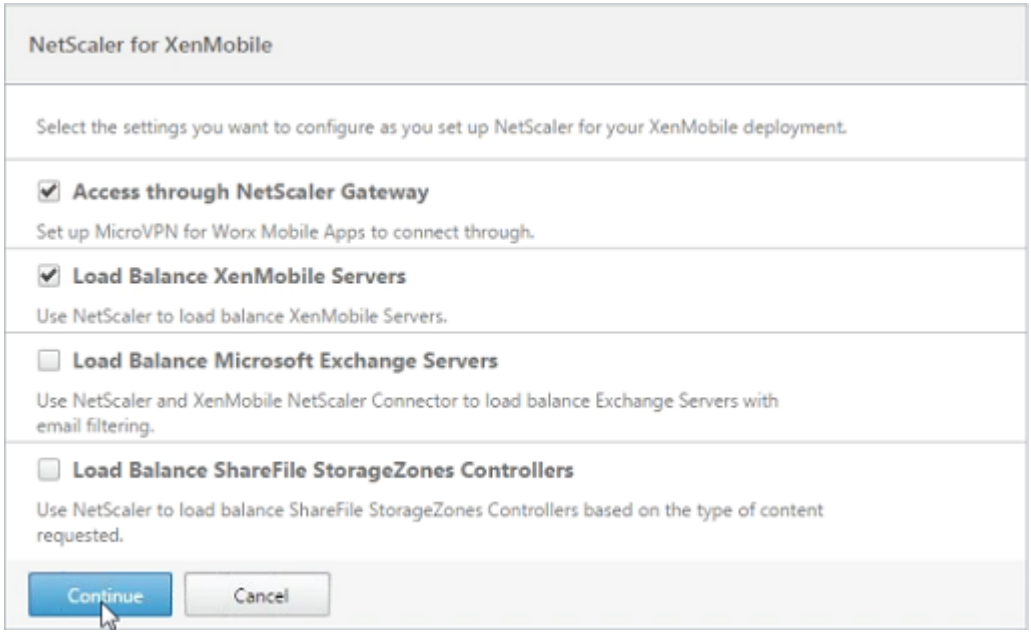
- 内部ネットワーク内の Citrix Endpoint Management で管理されるリソースへのリモートユーザー接続用のマイクロ VPN アクセスをセットアップする
- 証明書ベースの認証を構成します。パブリック SSL 証明書の取得とインストールについては、「証明書のインストールと管理」を参照してください。
- Citrix Endpoint Management サーバーの負荷分散を構成します。

ウィザードを使用するには、次の手順に従います。

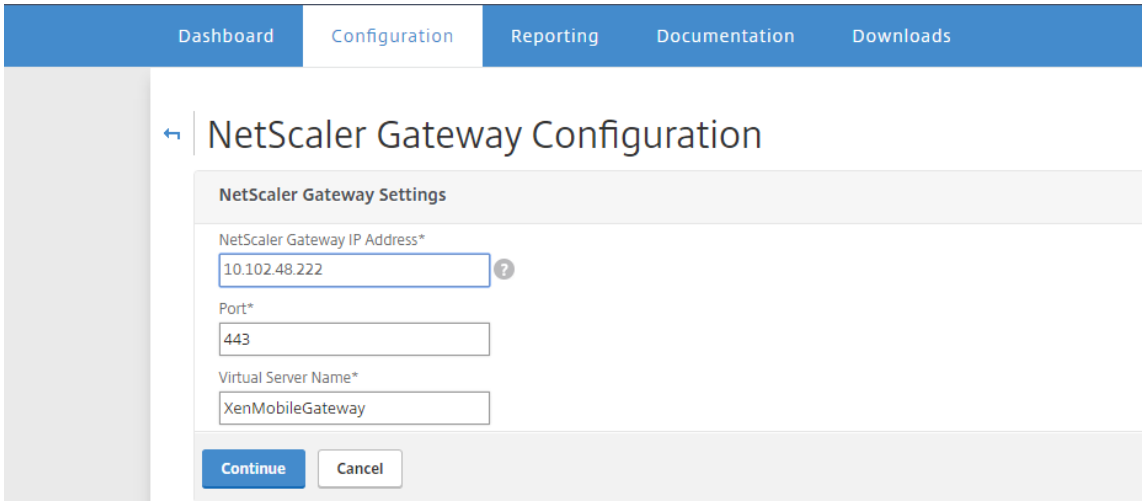
1. 構成ユーティリティで、[構成] タブをクリックし、[**Citrix Endpoint Management**] をクリックします。



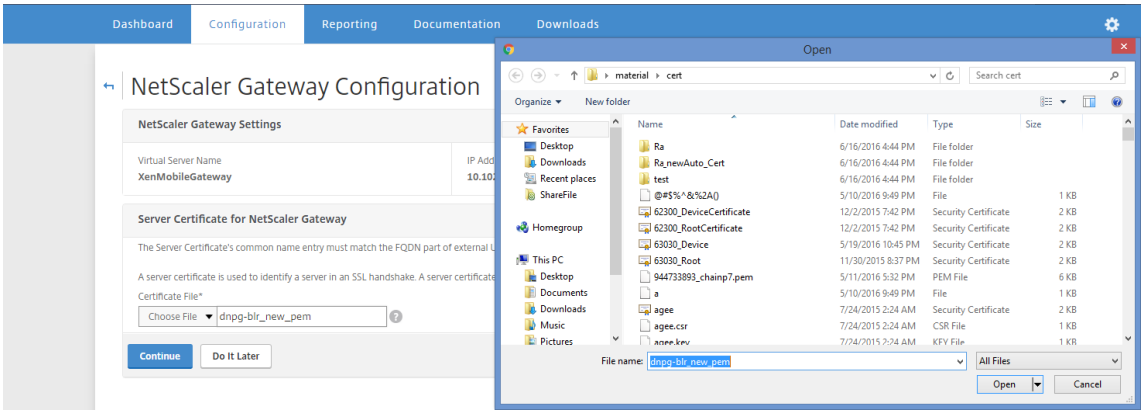
2. Citrix Endpoint Management のバージョンを選択し、[開始] をクリックします。
3. 設定する機能のチェックボックスをオンにします。このウィザードは 1 回だけ使用できるため、以降の構成を手動で実行する必要があります。これらの手順は、次の設定を選択することを前提としています。
   Citrix Gateway 経由のアクセス（ENT モードまたは MAM モードで実行されている Citrix Endpoint Management 用）
   負荷分散 **Citrix Endpoint Management** サーバー



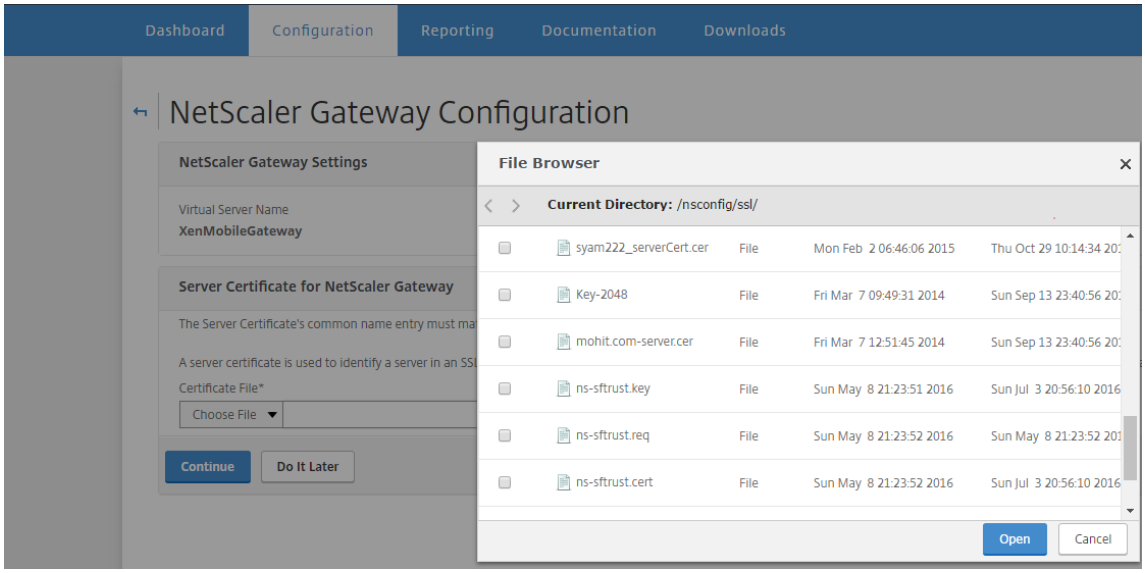
4. **Citrix Gateway** 設定ページで、外部の **Citrix Gateway** の **IP** アドレス、ポート、仮想サーバー名の値を入力します。



5. **Citrix Gateway** のサーバー証明書］ページの［証明書ファイル］ドロップダウンメニューから、［ローカル］または［アプライアンス］から証明書ファイルを選択します。証明書がローカルマシン上にある場合:



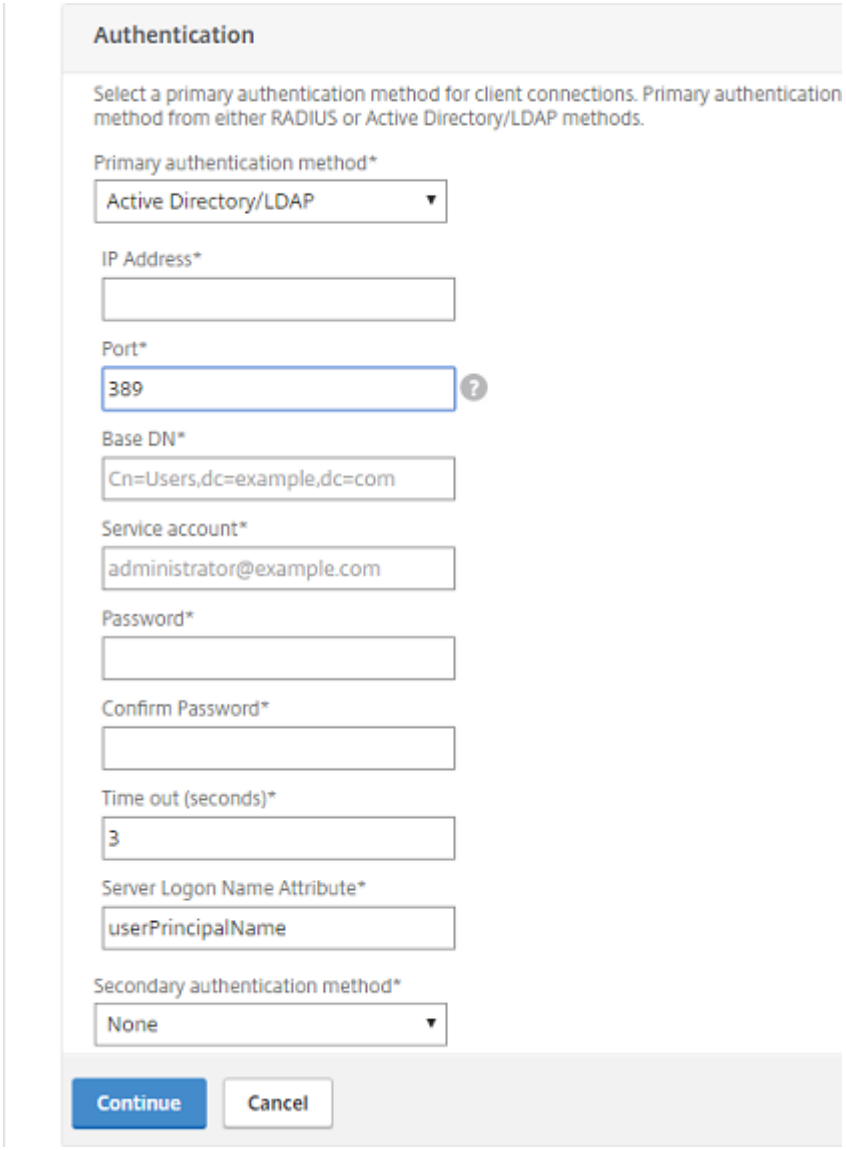
証明書がアプライアンス上にある場合:



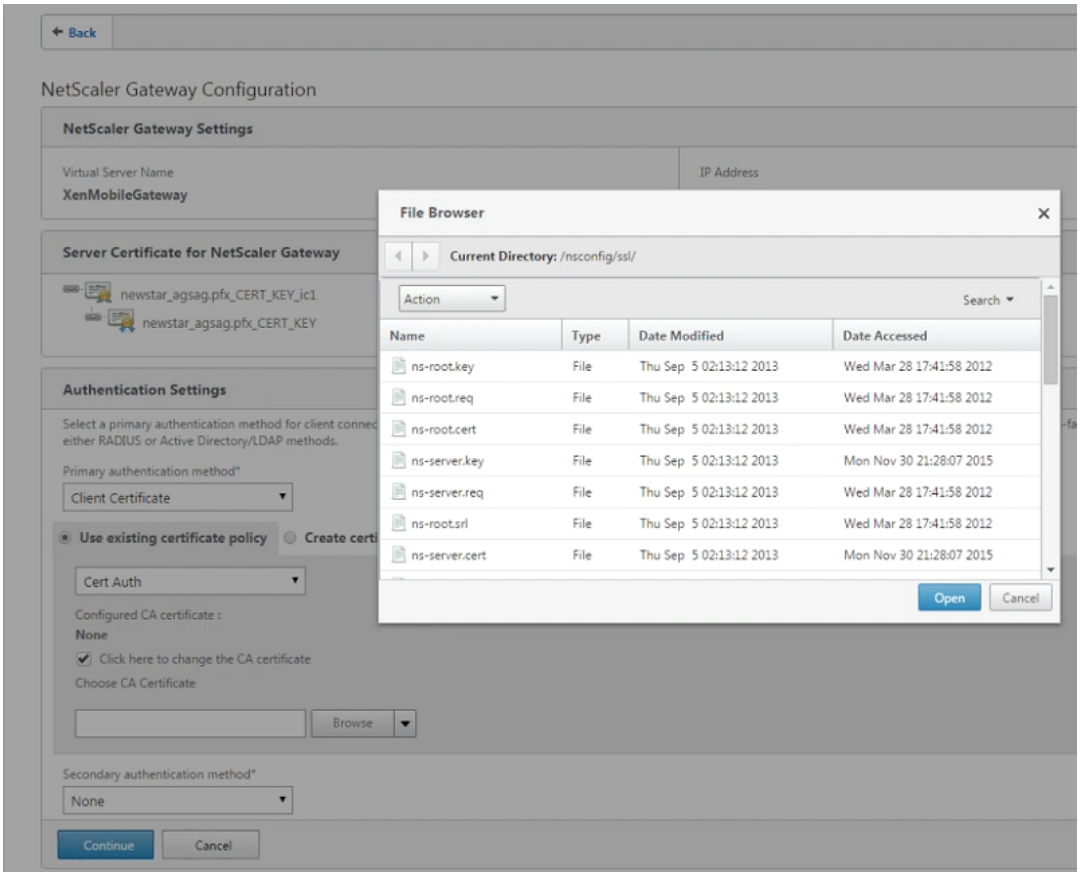
6. [認証設定] ページの **[**プライマリ認証方法] フィールドで、[クライアント証明書] を選択します。

   これによって、次の 2 つのフィールドで自動的に [**Use existing certificate policy**] および [**Cert Auth**] を選択します。次の手順では、証明書ポリシーがすでにあることを前提しています。

   証明書を作成する必要がある場合、 [**Create certificate policy**] をクリックして、設定を完了します。[**Citrix Endpoint Management** 証明書] 画面で、既存のサーバー証明書を選択するか、新しい証明書をインストールします。複数の Citrix Endpoint Management サーバーを実行している場合は、それぞれに証明書を追加します。[サーバーログオン名の属性] で、要件に応じて、ユーザープリンシパル名または **samAccountName** を指定します。



- a.**[** ここをクリックして **CA** 証明書を変更してください**]** を選択し、[参照**]** ボックスの一覧で目的の CA 証明書に移動します。



- b. プライマリ認証タイプとしてクライアント証明書を使用する場合、セカンダリ認証タイプとして LDPA（または RADIUS）を設定できます。

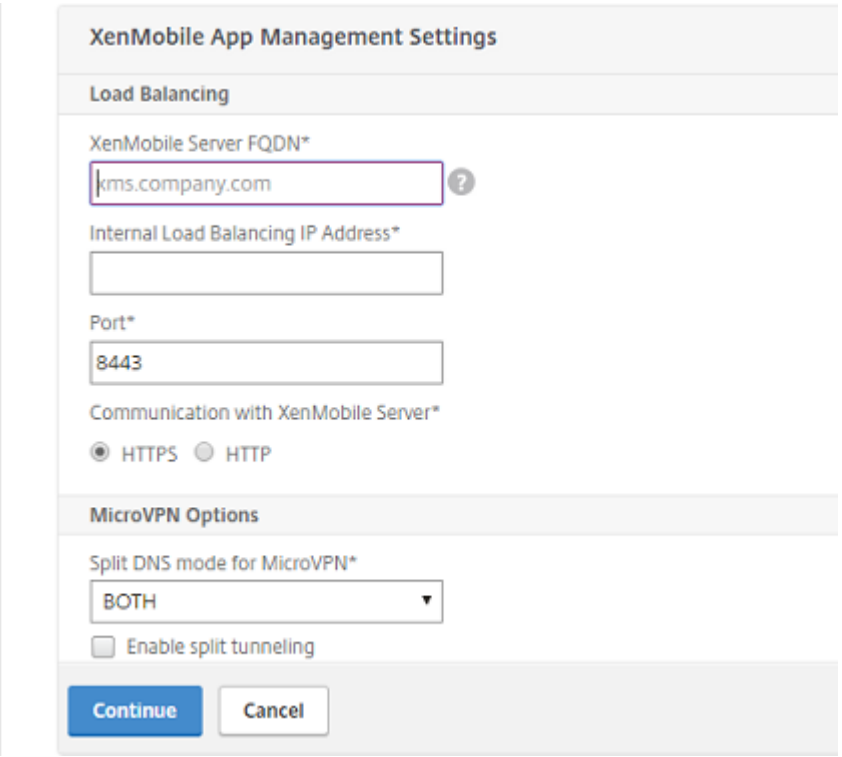
  クライアント証明書認証のみを使用するには、[**2** 番目の認証方法] を [なし] のままにして、[続行] をクリックします。

  クライアント証明書 + ドメイン (LDAP) 認証を使用するには、[**2** 番目の認証方法] を [**LDAP**] に変更し、認証サーバーの設定を構成します。

- c. ［デバイス証明書］画面で、証明書がまだインストールされていない場合は、Citrix Endpoint Management コンソールからこの証明書をエクスポートする必要があります。コンソールで、右上隅にある歯車アイコンをクリックして ［設定］画面を開きます。
- d. [証明書] をクリックし、一覧から CA 証明書を選択します。
- e.［エクスポート］をクリックします。
- f. Citrix ADC ウィザードに戻り、エクスポートした（ダウンロードした）証明書を選択してインストールします。
- g.［続行］をクリックします。

設定した Citrix Endpoint Management IP アドレスが表示されます。

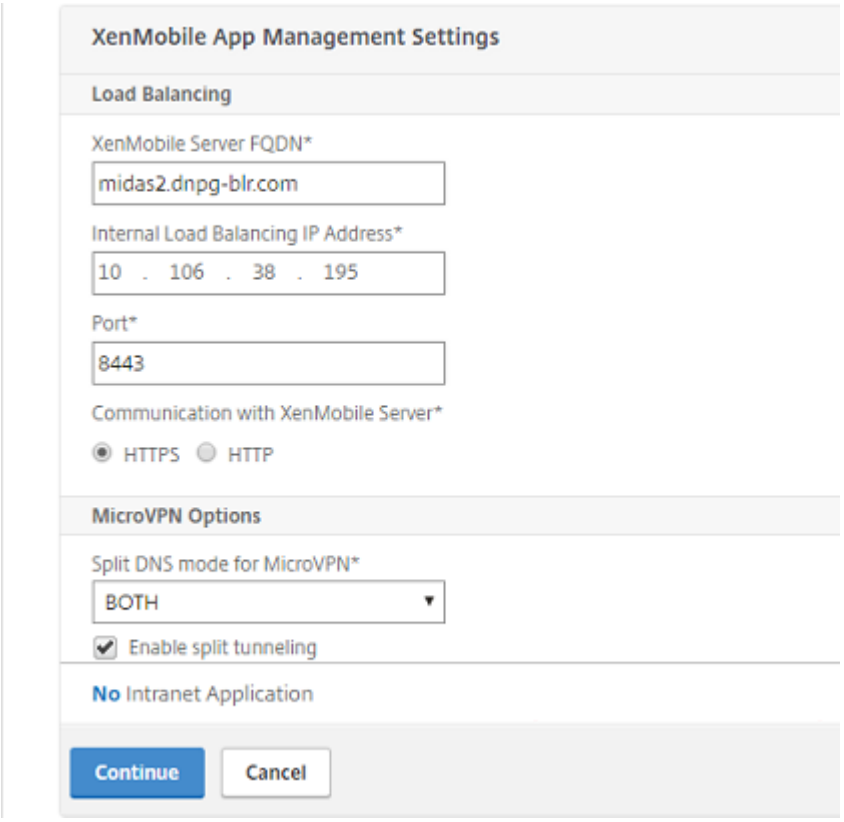
7. **Citrix Endpoint Management** アプリケーションの管理設定を構成します。



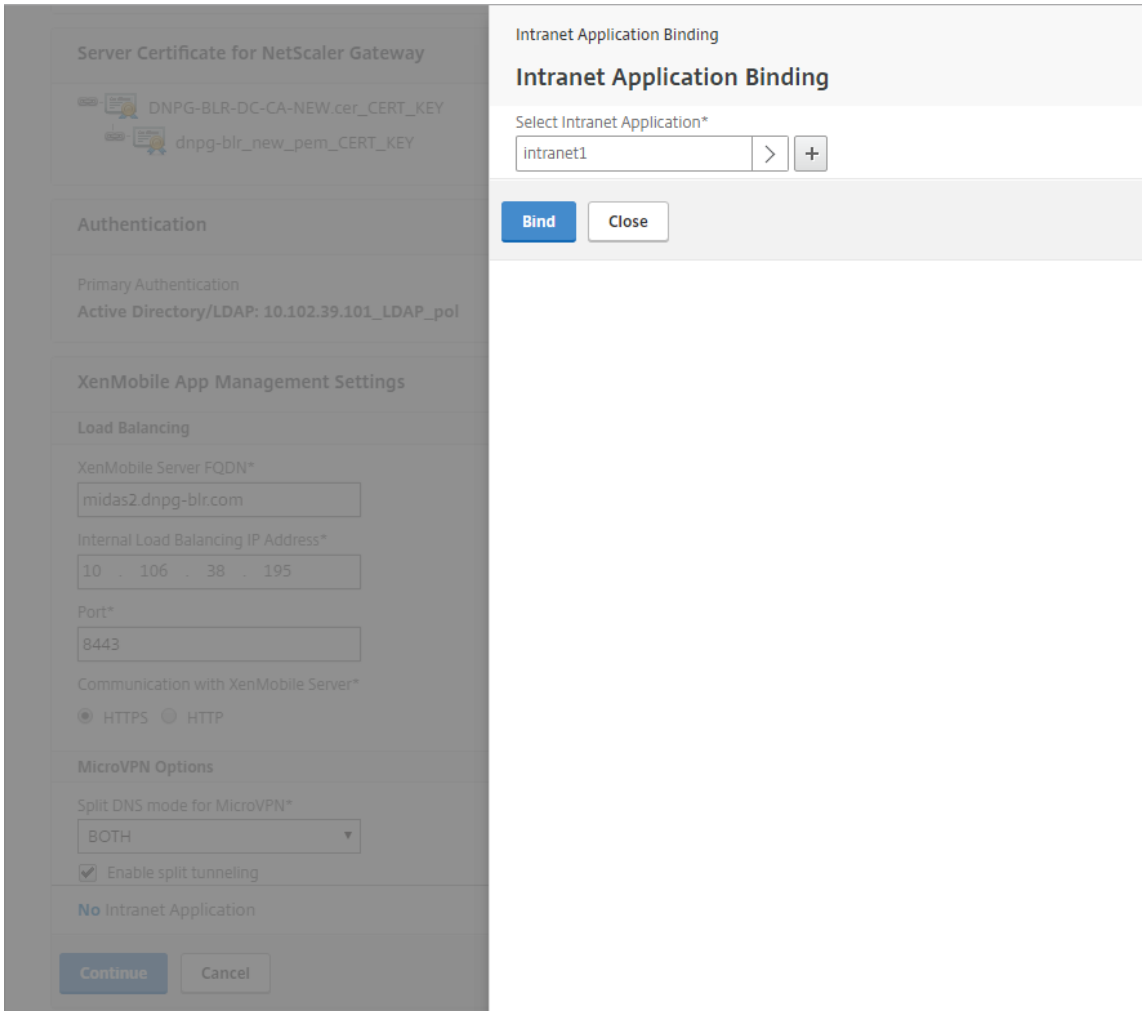
- **Citrix Endpoint Management** の **FQDN** を入力します。これは MAM のロードバランシング FQDN です。
- Citrix Endpoint Management サーバーの 負荷分散を行う仮想サーバーの、**MAM** 専用内部負荷分散 **IP** アドレスを入力します。Citrix Gateway は、この MAM 負荷分散仮想 IP を介して Citrix Endpoint Management と通信します。
- これは SSL オフロード展開であるため、［**Citrix Endpoint Management** サーバーとの通信］で［**HTTP** ］を選択します。
- **MicroVPN** フィールドのスプリット **DNS** モードは自動的に 両方に設定されます。

展開で分割トンネリングが必要な場合は、[分割トンネリングを有効にする] を選択します。次に、分割トンネリングを有効にする場合は、イントラネットアプリケーションバインディングを設定する必要があります。

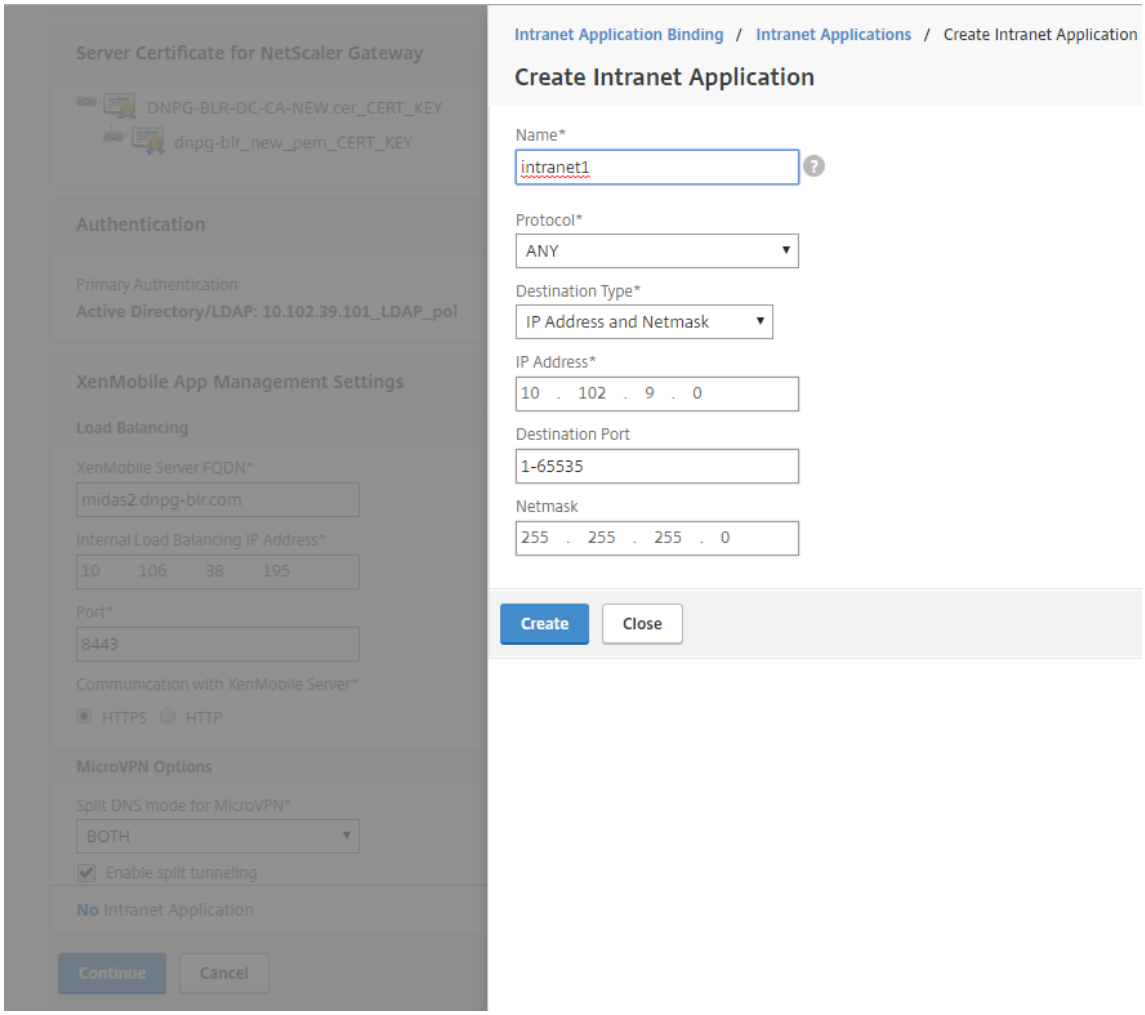
デフォルトでは、Secure Web アクセスは内部ネットワークにトンネリングされます。つまり、Secure Web はすべてのネットワークアクセスに対してアプリケーションごとの VPN トンネルを内部ネットワークに戻し、Citrix ADC アプライアンスは分割トンネル設定を使用します。



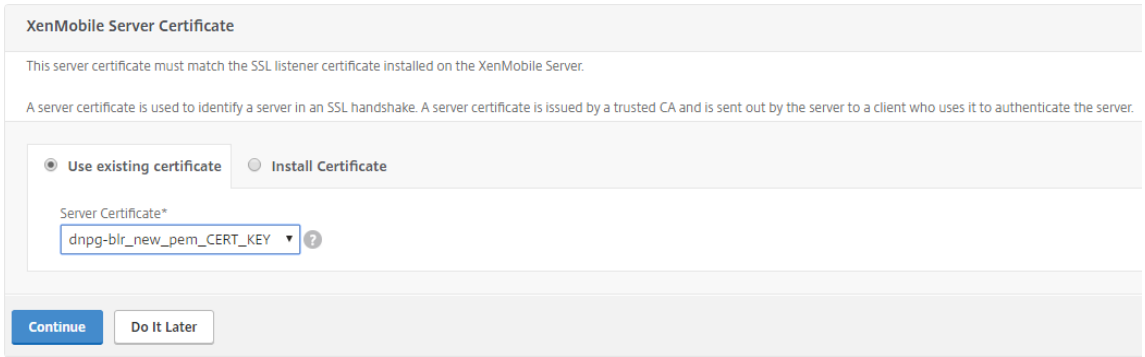
8. Citrix Gateway でユーザー接続の傍受ルールを構成するには、イントラネットアプリケーションのバインドを構成する必要があります。バインドを追加するには、[+] をクリックします。



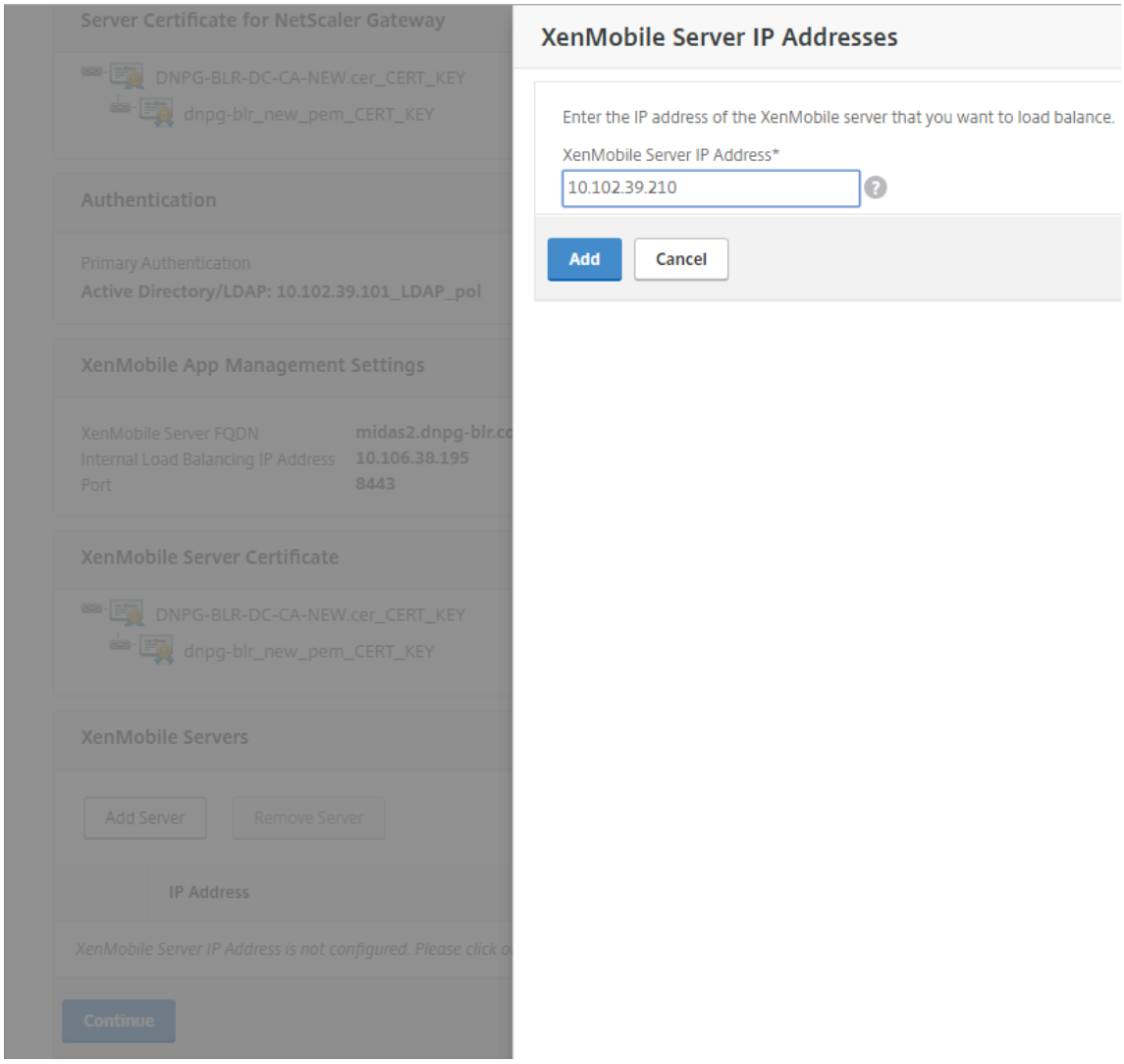
9. ネットワークアクセスを許可するためのパラメータを入力し、[**Create**] をクリックします。



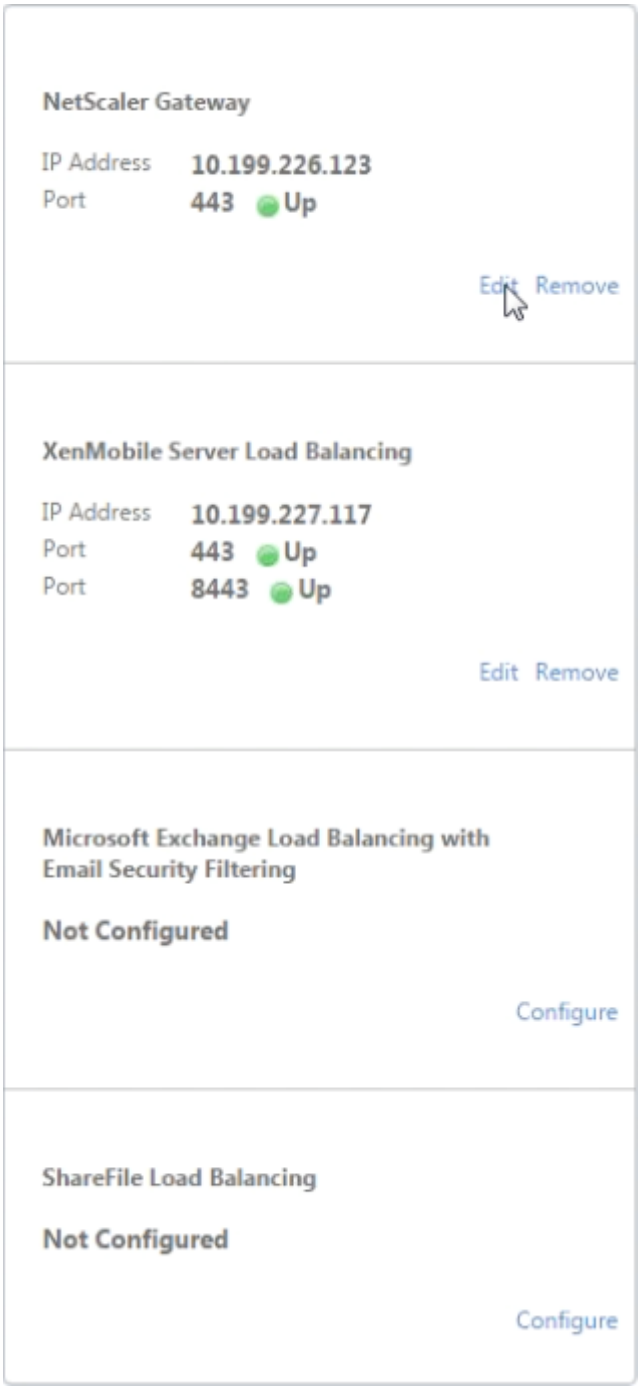
10. Citrix Endpoint Management 証明書を追加します。これは、MAM 負荷分散仮想サーバーに使用されます。



11. [**Citrix Endpoint Management** サーバー] で [サーバーの追加] をクリックして、負荷分散仮想 **IP** にバインドする **Citrix Endpoint Management**IP アドレスを追加します。



12. Citrix ADC ダッシュボードで、Citrix Gateway と Citrix Endpoint Management 負荷分散が次のように構成されていることを確認します。



ユーザープリンシパル名 (UPN) の代わりとしてユーザー証明書で sAMAccount 属性を使用する場合は、の説明に従って証明書プロファイルを構成クライアント証明書認証のための Citrix Gateway の手動構成します。

Citrix Endpoint Management または Citrix XenMobile サーバー用の負荷分散サーバーの構成

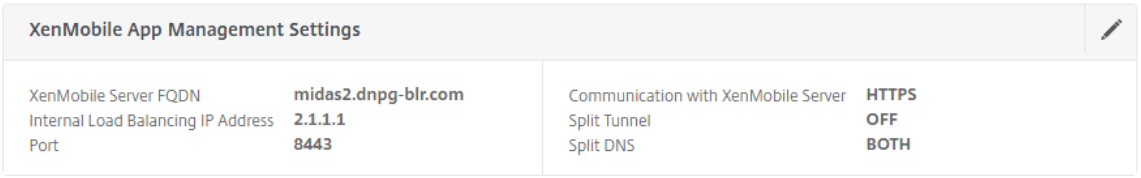
March 26, 2020

Citrix Endpoint Management 用 **Citrix ADC** ウィザードを使用して初期セットアップした後、このセクションで説明するように、Citrix Gateway 構成ユーティリティを使用して負荷分散を構成します。Citrix Endpoint Management の場合は、SSL オフロードを使用します。Citrix Endpoint Management Server の場合は、『Citrix Gateway および Citrix ADC との統合』の「展開の概要」の下にある負荷分散モードに関する推奨事項を参照してください。

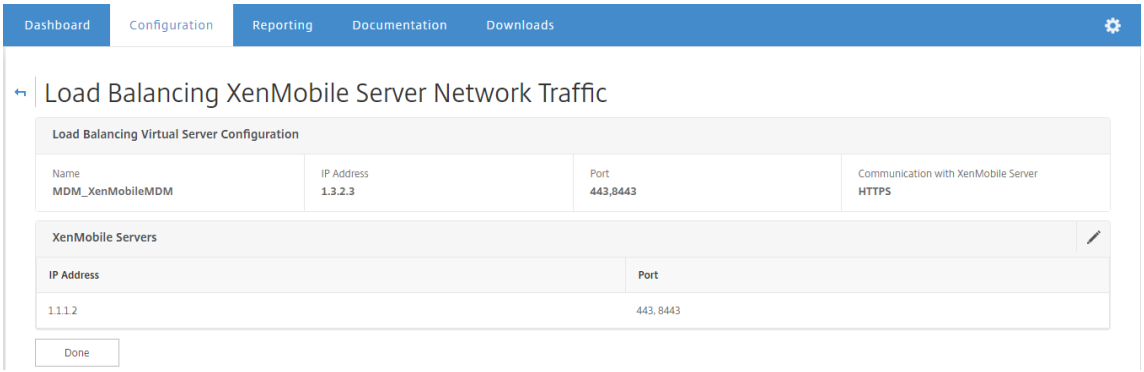
Citrix ADC VIP で SSL ブリッジモードを使用するには

Citrix Endpoint Management が DMZ にある場合は、SSL ブリッジモードを使用します。SSL ブリッジモードで Citrix ADC VIP を使用して Citrix Endpoint Management を負荷分散すると、インターネットトラフィックは Citrix Endpoint Management サーバーに直接流れ、そこで接続が終了します。SSL ブリッジモードはセットアップとトラブルシューティングが最も簡単なモードです。

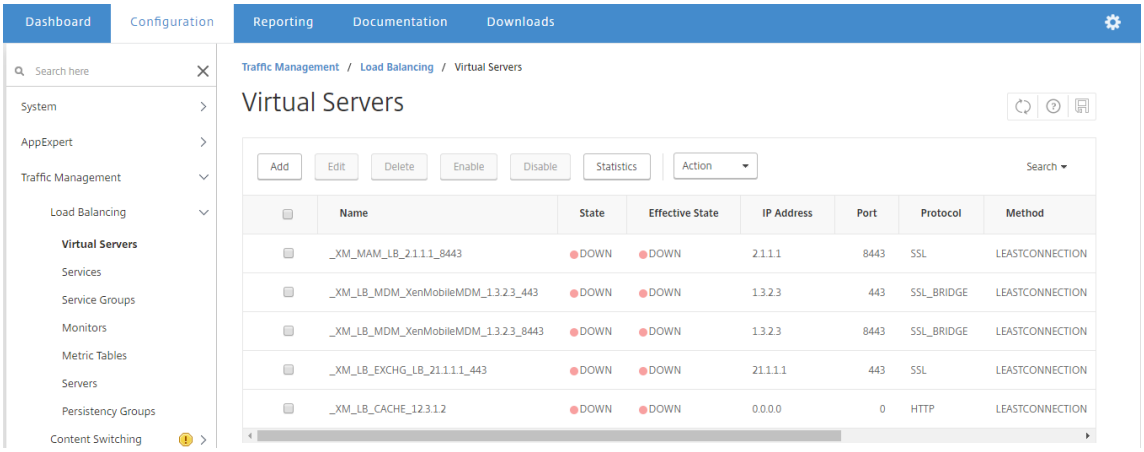
1. SSL ブリッジモードを構成する前に、**Citrix Endpoint Management** アプリケーション管理設定に移動し、**Citrix Endpoint Management** サーバーとの通信が **HTTPS** であることを確認します。



2. 構成ユーティリティにログオンした後、[ホーム] タブの **MDM** サーバー **LB** で、[構成] をクリックします。
3. [デバイス管理用 **LB** 仮想サーバー**]** の **[**名前**]** に、サーバーの名前を入力します。
4. [**IP** アドレス] に、仮想サーバーの IP アドレスを入力し、[続行] をクリックします。
5. [**Citrix Endpoint Management MDM** サーバーの負荷分散] ページで、手順 3 と 4 を繰り返し、[作成] をクリックします。
6. 設定が正しいことを確認し、[完了] をクリックします。



7. ロードバランシング設定を確認するには、[トラフィック管理] **>** [仮想サーバー] に移動します。



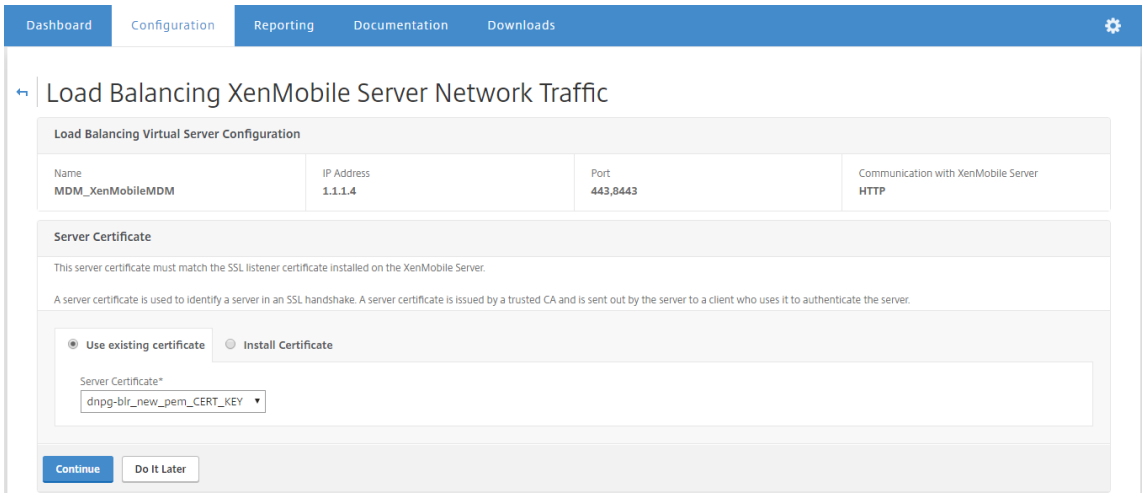
Citrix ADC VIP で SSL オフロードモードを使用するには

Citrix Endpoint Management には SSL オフロードを使用します。また、セキュリティ基準を満たすために必要な場合は、オンプレミスの Citrix Endpoint Management が内部ネットワークにある場合は、SSL オフロードを使用します。SSL オフロードモードで Citrix ADC VIP を使用して Citrix Endpoint Management を負荷分散すると、インターネットトラフィックは Citrix ADC アプライアンスに直接流れ、そこで接続が終了します。その後、Citrix Gateway は、アプライアンスから Citrix Endpoint Management への新しいセッションを確立します。SSL オフロードモードでのセットアップとトラブルシューティングはさらに複雑です。

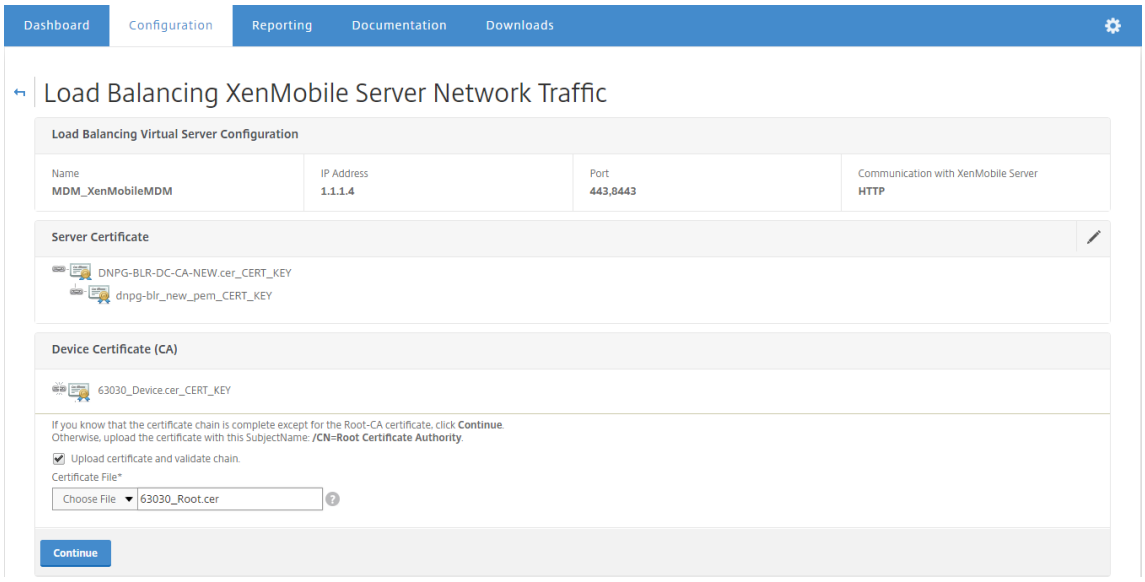
1. SSL オフロードモードを構成する前に、[**Citrix Endpoint Management** アプリケーション管理設定] に移動し、[**Citrix Endpoint Management** サーバーとの通信] が [**HTTP**] であることを確認します。

2. 構成ユーティリティにログオンします。[ホーム] タブの [**MDM** サーバー **LB**] で、[構成] をクリックします。
3. [デバイス管理用 **LB** 仮想サーバー] の [名前] に、サーバーの名前を入力します。

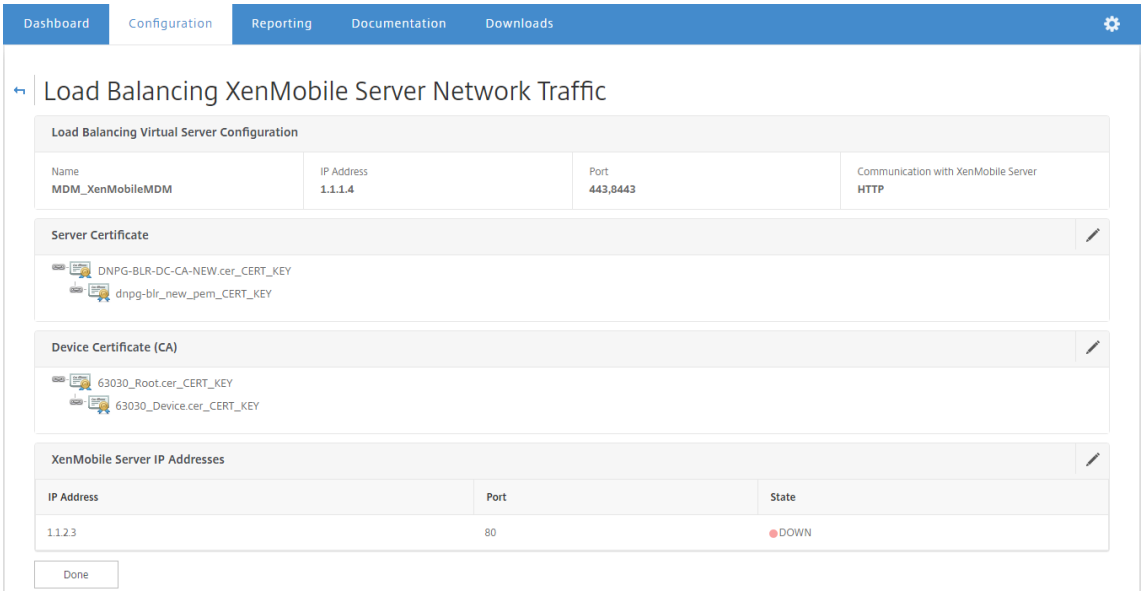
4. [**IP** アドレス] に、仮想サーバーの IP アドレスを入力し、[続行] をクリックします。
5. [**Citrix Endpoint Management MDM** サーバーの負荷分散] ページで、手順 3 と 4 を繰り返し、[作成] をクリックします。
6. 設定を確認し、[完了] をクリックします。
7. サーバ証明書を追加するかどうかを確認するメッセージが表示されたら、サーバ証明書を選択し、[**Continue**] をクリックします。



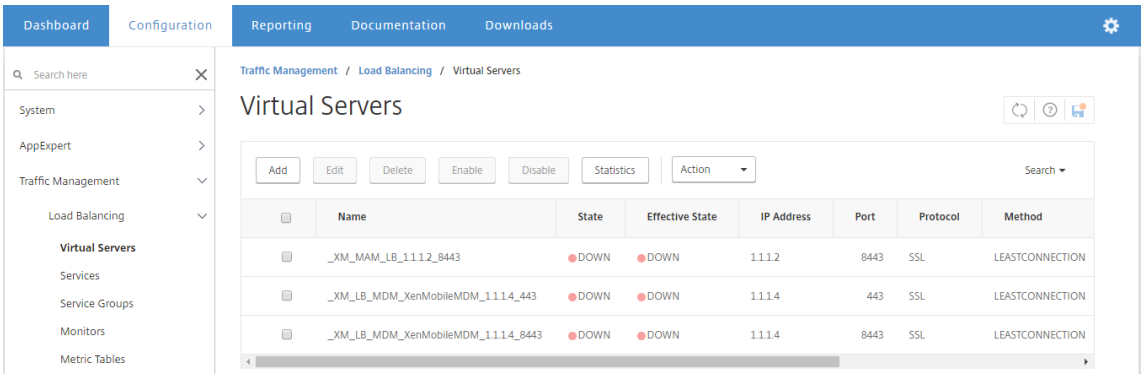
8. CA 証明書を指定し、[続行] をクリックします。



9. 同じ Citrix Endpoint Management IP アドレスを使用します。［完了］をクリックします。



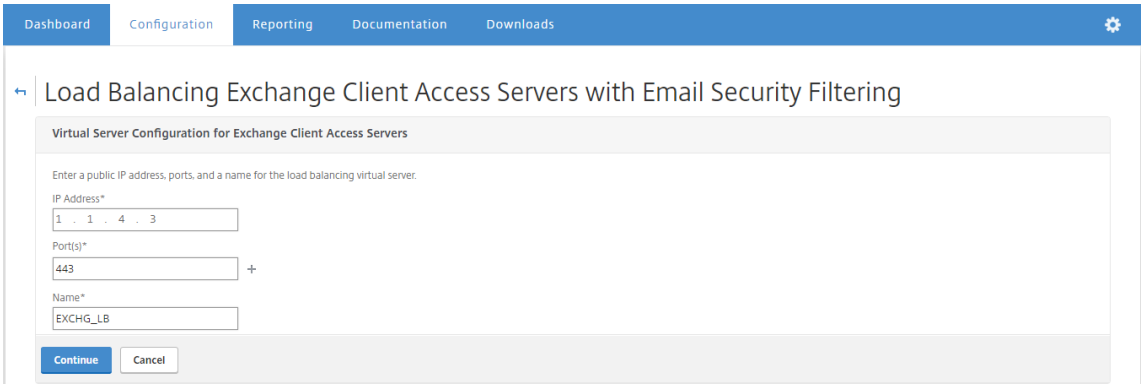
10. ロードバランシング設定を確認するには、[トラフィック管理] **>** [仮想サーバー] に移動します。



電子メールセキュリティフィルタリングを使用した **Microsoft Exchange** 用のロードバランシングサーバーの構成

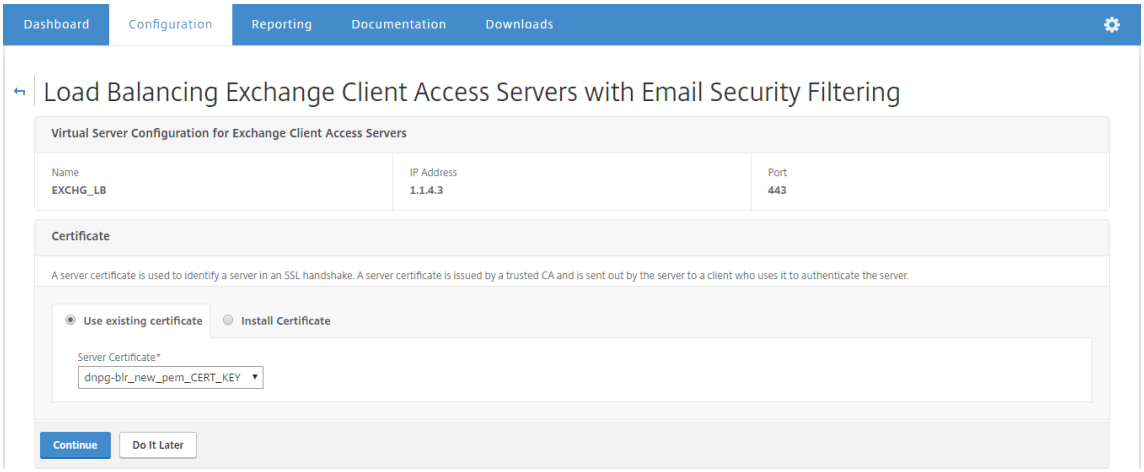
March 26, 2020

1. [ホーム] タブの [**MDM** サーバー **LB**] で、[構成] をクリックします。
2. [**Exchange CAS** 用 **LB** 仮想サーバー**]** の **[**名前**]** に、サーバーの名前を入力します。
3. [**IP** アドレス**]** に、仮想サーバーの IP アドレスを入力します。
4. [**Port**] ボックスにポート番号を入力します。さらにポートを追加するには、プラス記号 (**+**) をクリックし、ポート番号を入力します。
5. [続行] をクリックします。

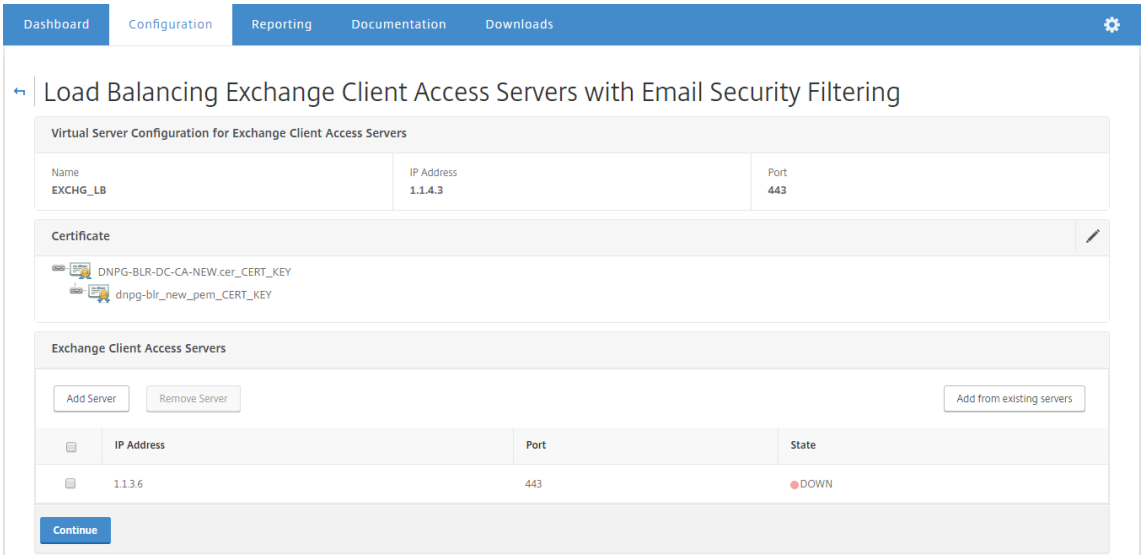


6. [証明書] で、既存の証明書を選択するか、コンピュータ（ローカル）または Citrix ADC アプライアンス（アプライアンス）にインストールします。

7. [続行] をクリックします。



8. [**Exchange CAS** サービスインスタンス] で、仮想サーバーの名前、IP アドレス、ポート番号を入力します。次に、[追加して 続行] をクリックします。



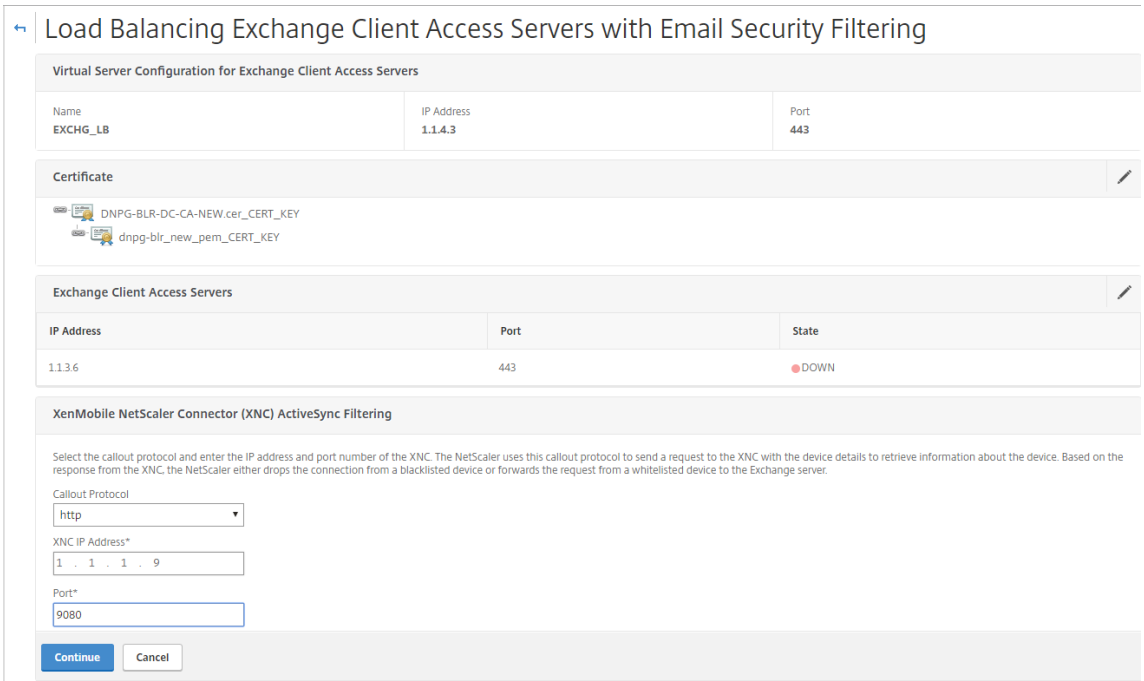
［完了］をクリックすると、Citrix Endpoint Management Citrix ADC コネクタ（XNC）ActiveSync フィルタリングを構成するためのフィールドが表示されます。

Citrix Endpoint Management Citrix ADC コネクタ（XNC）ActiveSync フィルタリングの構成

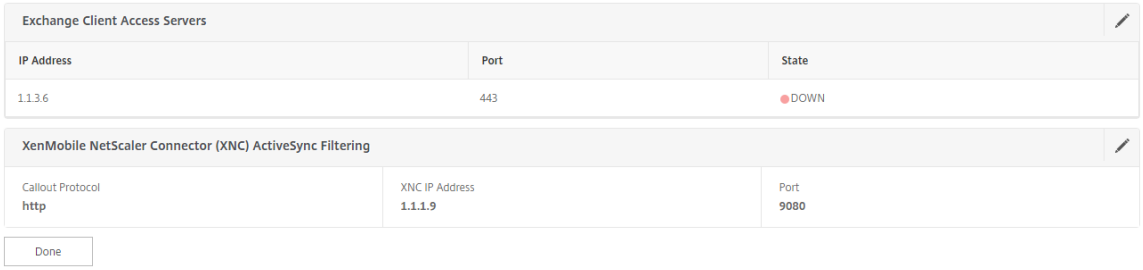
March 26, 2020

Citrix Endpoint Management Citrix ADC コネクタ（XNC）は、Exchange ActiveSync プロトコルのリバースプロキシとして機能する Citrix ADC に対して、ActiveSync クライアントのデバイスレベルの認証サービスを提供します。認証は、Citrix Endpoint Management 内で定義されたポリシーと、XNC によってローカルに定義されたルールの組み合わせによって制御されます。

1. ［**Citrix Endpoint Management**］［**Citrix ADC** コネクタ（**XNC**）**ActiveSync** フィルタリング］で、［コールアウトプロトコル］で［**http**］または［**https**］を選択します。
2. ［**XNC IP** アドレス］に、Citrix Endpoint Management の Citrix ADC コネクタの IP アドレスを入力します。
3. ［ポート］で、HTTP ネットワークトラフィックの場合は **9080**、HTTPS ネットワークトラフィックの場合は **9443** と入力し、［続行］をクリックします。



設定が表示されます。



Citrix モバイル生産性アプリを使用したモバイルデバイスからのアクセスの許可

October 22, 2021

Citrix ADC for XenMobile ウィザードでは、サポートされているデバイスから Citrix Gateway 経由で内部ネットワークのモバイルアプリやリソースに接続するために必要な設定を構成します。ユーザーは、Secure Hub（以前は Worx Home）を使用して接続し、Micro VPN トンネルを確立します。ユーザーが接続すると、VPN トンネルが Citrix Gateway に開き、内部ネットワークの XenMobile に渡されます。ユーザーは、XenMobile から Web、モバイル、および SaaS アプリケーションにアクセスできます。

複数のデバイスで Citrix Gateway に同時に接続するときに、ユーザーが単一のユニバーサルライセンスを使用できるようにするには、仮想サーバーでセッション転送を有効にします。詳しくは、「仮想サーバでの接続タイプの設定」を参照してください。

Citrix ADC for XenMobile ウィザードを使用した後に構成を変更する必要がある場合は、この記事のセクションを参照してください。設定を変更する前に、変更の影響を理解しておいてください。詳細については、XenMobile の展開記事を参照してください。

Citrix Gateway での Secure Browse 構成

Secure Browse は、グローバル設定の一部として、またはセッションプロファイルの一部として変更できます。セッション・ポリシーは、ユーザー、グループ、または仮想サーバーにバインドできます。Secure Browse を設定する場合は、クライアントレスアクセスも有効にする必要があります。ただし、クライアントレスアクセスでは、Secure Browse を有効にする必要はありません。クライアントレスアクセスを設定する場合は、**[**クライアントレスアクセス **URL** エンコーディング**]** を **[**クリア**]** に設定します。

Secure Browse をグローバルに構成するには:

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで **Citrix Gateway** を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. ［グローバル **Citrix Gateway** 設定］ダイアログボックスの［セキュリティ］タブで、［セキュリティで **Secure Browse** をクリックし、［**OK**］をクリックします。

セッション・ポリシーおよびプロファイルで Secure Browse を構成するには:

1. 構成ユーティリティーの 構成タブのナビゲーションペインで、[**Citrix Gateway**] **>** [ポリシー] の順に展開し、[セッション] をクリックします。
2. 詳細ウィンドウで、次のいずれかの操作を行います。
   - 新しいセッションポリシーを作成する場合は、[**Add**] をクリックします。
   - 既存のポリシーを変更する場合は、ポリシーを選択して [開く] をクリックします。
3. ポリシーで、新しいプロファイルを作成するか、既存のプロファイルを変更します。これを行うには、次のいずれかの操作を行います。
   - [プロファイルの要求] の横にある [新規] をクリックします。
   - [プロファイルの要求] の横にある [変更] をクリックします。
4. [セキュリティ] タブの [セキュリティで **Secure Browse**] の横にある [グローバルに上書き] をクリックし、[セキュリティで保護された参照] を選択します。
5. 次のいずれかを行います:
   - 新しいプロファイルを作成する場合は、[**Create**] をクリックし、ポリシーダイアログボックスで式を設定し、[**Create**] をクリックして、[**Close**] をクリックします。
   - 既存のプロファイルを修正する場合は、選択後に [**OK**] を 2 回クリックします。

セキュア Secure Browse モードで Secure Web のトラフィックポリシーを設定するには:

次の手順に従って、Secure Web トラフィックをセキュア Secure Browse モードでプロキシサーバー経由でルーティングするトラフィックポリシーを設定します。

1. 構成ユーティリティの [構成] タブで、[**Citrix Gateway] > [**ポリシー] を展開し、[トラフィック] をクリックします。
2. 右ペインで、[**Traffic Profiles**] タブをクリックし、[**Add**] をクリックします。
3. [名前] にプロファイルの名前を入力し、[プロトコル] として [**TCP**] を選択し、残りの設定はそのままにします。
4. [作成] をクリックします。
5. [トラフィックプロファイル] タブをクリックし、[追加] をクリックします。
6. [名前**]** にプロファイルの名前を入力し、[プロトコル] として [**HTTP**] を選択します。
   このトラフィックプロファイルは、HTTP と SSL の両方用です。CVPN トラフィックは、宛先ポートまたはサービスタイプに関係なく、設計上 HTTP トラフィックです。したがって、トラフィックプロファイルで SSL トラフィックと HTTP トラフィックの両方を **HTTP** として指定します。
7. 「プロキシ」に、プロキシ・サーバーの IP アドレスを入力します。「ポート」に、プロキシ・サーバーのポート番号を入力します。
8. [作成] をクリックします。
9. [トラフィックプロファイル] タブをクリックし、[追加] をクリックします。
10. トラフィックポリシーの 名前を入力し、[**Request Profile**] で、ステップ 3 で作成したトラフィックプロファイルを選択します。次の 式を入力し、[作成] をクリックします。

REQ.HTT HOST に Ac- tiveSync Server が含まれています	REQ.HTT User- Agent CON- TAINS Worx- Mail	REQ.HTT User- Agent CON- TAINS com.zen	REQ.HTT User- Agent CON- TAINS Worx- Home	REQ.HTT CON- TAINS AGSer- vices	REQ.HTTP.URL CON- TAINS StoreWeb

このルールは、ホストヘッダーに基づいてチェックを実行します。プロキシからのアクティブ同期トラフィックをバイパスするには、**ActiveSyncServer** を適切な **ActiveSync c** サーバー名に置き換えます。

11. [トラフィックプロファイル] タブをクリックし、[追加] をクリックします。トラフィックポリシーの 名前を入力し、[**Request Profile**] で、ステップ 6 で作成したトラフィックプロファイルを選択します。次の 式を入力し、[作成] をクリックします。

(REQ.HTTP.HEADE User-Agent CONTAINS Mozilla	REQ.HTTP.HEADEI User-Agent CONTAINS com.citrix.browse	REQ.HTTP.HEADER User-Agent CONTAINS WorxWeb) && REQ.TCP.DESTPORT == 80

12. [トラフィックプロファイル] タブをクリックし、[追加] をクリックします。トラフィックポリシーの 名前を入力し、[**Request Profile**] で、ステップ 6 で作成したトラフィックプロファイルを選択します。次の 式を入力し、[作成] をクリックします。

(REQ.HTTP.HEADE User-Agent CONTAINS Mozilla	REQ.HTTP.HEADEI User-Agent CONTAINS com.citrix.browse	REQ.HTTP.HEADER User-Agent CONTAINS WorxWeb) && REQ.TCP.DESTPORT == 443

13. [**Citrix Gateway**] **>** [仮想サーバー] に移動し、右側のペインで仮想サーバーを選択し、[編集] をクリックします。
14. [ポリシー] 行で、[**+**] をクリックします。

15. [ポリシーの選択] メニューから、[トラフィック] を選択します。
16. [続行] をクリックします。
17. [ポリシーのバインド] の [ポリシーの選択] で、[**>**] をクリックします。
18. 手順 10 で作成したポリシーを選択し、[**OK**] をクリックします。
19. [バインド] をクリックします。
20. [ポリシー] で、[トラフィックポリシー] をクリックします。
21. [**VPN** 仮想サーバートラフィックポリシーバインディング] で、[バインドの追加] をクリックします。
22. [ポリシーのバインド] で、[ポリシーの選択] メニューの横にある [**>**] をクリックしてポリシーのリストを表示します。
23. 手順 17 で作成したポリシーを選択し、[**OK**] をクリックします。
24. [バインド] をクリックします。
25. [ポリシー] で、[トラフィックポリシー] をクリックします。
26. [**VPN** 仮想サーバートラフィックポリシーバインディング] で、[バインドの追加] をクリックします。
27. [ポリシーのバインド] で、[ポリシーの選択] メニューの横にある [**>**] をクリックしてポリシーのリストを表示します。
28. 手順 18 で作成したポリシーを選択し、[**OK**] をクリックします。
29. [バインド] をクリックします。
30. [閉じる] をクリックします。
31. [完了] をクリックします。

XenMobile コンソールで Secure Web（WorxWeb）アプリを構成してください。[設定**] > [**アプリ] に移動し、[Secure Web アプリ] を選択し、[編集] をクリックして、次の変更を行います。

- [アプリの情報] ページで、[初期 **VPN** モード**]** を **[Secure Browse** に変更します。
- [**iOS**] ページで、[初期 **VPN** モード**]** を [**Secure Browse]** に変更します。
- [**Android**] ページで、[優先 **VPN** モード**]** を [**Secure Browse]** に変更します。

アプリケーションおよび **MDX** トークンのタイムアウトの構成

ユーザーが iOS または Android デバイスからログオンすると、アプリケーショントークンまたは MDX トークンが発行されます。トークンは、Secure Ticket Authority（STA）に似ています。

トークンがアクティブになる秒数または分数を設定できます。トークンの有効期限が切れた場合、ユーザーはアプリケーションや Web ページなどの要求されたリソースにアクセスできません。

トークンのタイムアウトはグローバル設定です。この設定を構成すると、Citrix Gateway にログオンするすべてのユーザーに適用されます。

1. 構成ユーティリティの ［構成］タブのナビゲーションペインで **Citrix Gateway** を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. ［グローバル **Citrix Gateway** 設定］ダイアログボックスの［クライアントエクスペリエンス］タブで、［詳細設定］をクリックします。
4. [全般] タブの [アプリケーショントークンのタイムアウト **(**秒**)**] に、トークンの有効期限が切れるまでの秒数を入力します。デフォルトは **100** 秒です。
5. [**MDX** トークンのタイムアウト **(**分**)**] に、トークンの有効期限が切れるまでの分数を入力し、[**OK**] をクリックします。デフォルトは **10** 分です。

モバイルデバイスのエンドポイント分析の無効化

エンドポイント分析を設定する場合は、エンドポイント分析スキャンが Android または iOS モバイルデバイスで実行されないように、ポリシー式を設定する必要があります。エンドポイント分析スキャンは、モバイルデバイスではサポートされていません。

エンドポイント分析ポリシーを仮想サーバーにバインドする場合は、モバイルデバイス用のセカンダリ仮想サーバーを作成する必要があります。事前認証または認証後のポリシーは、モバイルデバイスの仮想サーバーにバインドしないでください。

事前認証ポリシーでポリシー式を設定する場合は、ユーザーエージェント文字列を追加して Android または iOS を除外します。ユーザーがこれらのデバイスのいずれかからログオンし、デバイスタイプを除外すると、エンドポイント分析は実行されません。

たとえば、ユーザーエージェントに Android が含まれているかどうか、アプリケーション virus.exe が存在しない場合、および事前認証プロファイルを使用して実行されている場合 keylogger.exe プロセスを終了するには、次のポリシー式を作成します。ポリシー表現は次のようになります。

REQ.HTTP.HEADER User-Agent NOTCONTAINS Android && CLIENT.APPLICATION.PROCESS に含まれる	CLIENT.APPLICATION.PROCESS (virus.exe) に含まれる

事前認証ポリシーとプロファイルを作成したら、ポリシーを仮想サーバーにバインドします。ユーザーが Android または iOS デバイスからログオンすると、スキャンは実行されません。ユーザーが Windows ベースのデバイスからログオンすると、スキャンが実行されます。

事前認証ポリシーの構成について詳しくは、「エンドポイントポリシーの設定」を参照してください。

Android デバイスで **DNS** サフィックスを使用した **DNS** クエリのサポート

ユーザーが Android デバイスから Micro VPN 接続を確立すると、Citrix Gateway はスプリット DNS 設定をユーザーデバイスに送信します。Citrix Gateway では、構成したスプリット DNS 設定に基づいて、スプリット DNS クエリがサポートされます。Citrix Gateway では、アプライアンス上で構成した DNS サフィックスに基づいたスプリット DNS クエリもサポートできます。ユーザーが Android デバイスから接続する場合は、Citrix Gateway で DNS 設定を構成する必要があります。

スプリット DNS は次のように動作します。

- スプリット DNS を **[**ローカル**]** に設定すると、Android デバイスはすべての DNS 要求をローカル DNS サーバーに送信します。
- スプリット DNS を リモートに設定すると、すべての DNS 要求が Citrix Gateway（リモート DNS サーバー）で構成された DNS サーバーに送信され、解決されます。
- スプリット DNS を [両方] に設定すると、Android デバイスは DNS 要求の種類をチェックします。
  - DNS 要求の種類が「A」でない場合は、DNS 要求パケットをローカルおよびリモートの DNS サーバーに送信します。
  - DNS リクエストタイプが「A」の場合、Android プラグインはクエリ FQDN を抽出し、その FQDN を Citrix ADC で設定された DNS サフィックスリストと照合します。DNS 要求の FQDN が一致すると、DNS 要求がリモート DNS サーバーに送信されます。FQDN が一致しない場合、DNS 要求はローカル DNS サーバーに送信されます。

次の表は、タイプ A のレコードとサフィックス一覧に基づく分割 DNS の動作をまとめたものです。

スプリット DNS 設定	それはタイプ A レコードですか?	接尾辞リストに載っていますか?	DNS 要求が送信される場所
Local	[はい] または [いいえ] の両方	[はい] または [いいえ] の両方	Local
Remote	[はい] または [いいえ] の両方	[はい] または [いいえ] の両方	Remote
Both	いいえ	-	Both
Both	はい	はい	Remote
Both	はい	いいえ	Local

DNS サフィックスを構成するには、次の手順を実行します。

1. 構成ユーティリティーの 構成タブのナビゲーションペインで、[**Citrix Gateway**] **>** [ポリシー] の順に展開し、[セッション] をクリックします。
2. 詳細ペインの [ポリシー] タブでセッションポリシーを選択し、[開く] をクリックします。
3. [プロファイルの要求] の横にある [変更] をクリックします。
4. [ネットワーク構成] タブで、[詳細設定] をクリックします。

5. [イントラネット **IP DNS** サフィックス] の横の [グローバル上書き] をクリックし、DNS サフィックスを入力して [**OK**] を 3 回クリックします。

Citrix Gateway でスプリット DNS をグローバルに設定するには:

1. 構成ユーティリティの ［構成］ タブのナビゲーションペインで **Citrix Gateway** を展開し、［グローバル設定］ をクリックします。
2. 詳細ウィンドウで、[設定] の [グローバル設定の変更] をクリックします。
3. [クライアントエクスペリエンス] タブで、[詳細設定] をクリックします。
4. [全般] タブの [スプリット **DNS**] で、[両方]、[リモート]、または [ローカル] を選択し、[**OK**] をクリックします。

Citrix Gateway のセッションポリシーでスプリット DNS を構成するには:

1. 構成ユーティリティーの 構成タブのナビゲーションペインで、［**Citrix Gateway**］ **>** ［ポリシー］ の順に展開し、［セッション］ をクリックします。
2. 詳細ウィンドウの [ポリシー] タブで、[追加] をクリックします。
3. [名前**]** に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [名前**]** に、プロファイルの名前を入力します。
6. [クライアントエクスペリエンス] タブで、[詳細設定] をクリックします。
7. [全般] タブの [スプリット **DNS**] の横にある [グローバル上書き] をクリックし、[両方]、[リモート]、または [ローカル] を選択して、[**OK**] をクリックします。
8. [セッションポリシーの作成] ダイアログボックスで、[名前付き式**]** の横にある **[**** 全般]、[**True**]、[式の追加 ******]、[作成]、[閉じる] の順にクリックします。

Citrix Endpoint Management のためのドメインおよびセキュリティトークン認証の構成

April 9, 2020

RADIUS プロトコルを使用して、LDAP 資格情報およびワンタイムパスワードによる認証をユーザーに要求するように、Citrix Endpoint Management を構成できます。このセクションでは、その 2 要素認証タイプに必要な Citrix Gateway 構成について説明します。

前提条件

Citrix Endpoint Management 用 Citrix ADC ウィザードをまだ実行していない場合は、Citrix Endpoint Management 環境の設定の構成の *Citrix Endpoint Management* ウィザードの *Citrix ADC* セクションを参照してください。Citrix ADC 構成に以下が含まれていることを確認します。

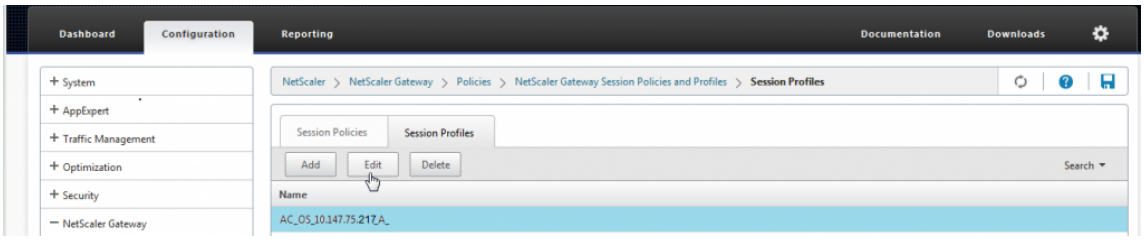
- **LDAP** ポート番号 = **636** （セキュア・LDAP 接続のデフォルト・ポート）

- サーバーログオン名属性 = **samAccountName** または ユーザーの要件に従ってユーザープリンシパル名

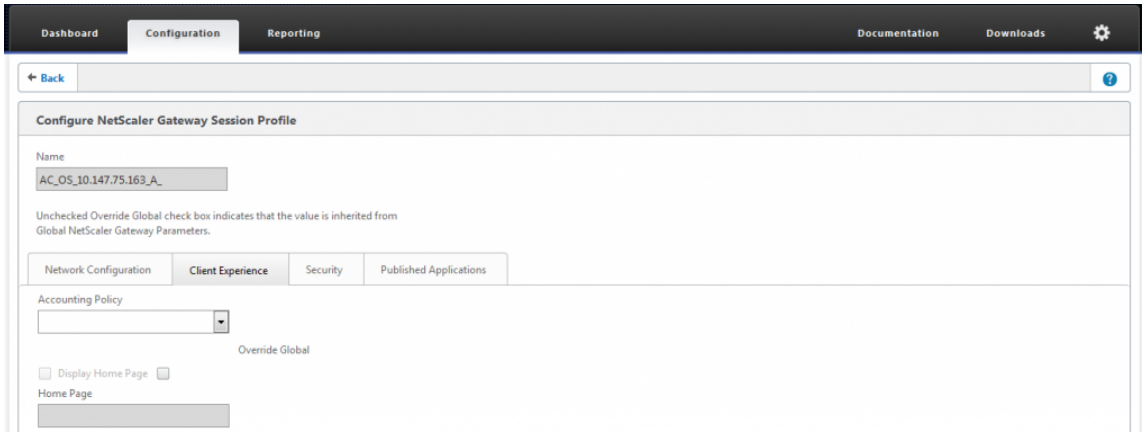
ドメイン認証とセキュリティトークン認証を構成するには

1. **Citrix Gateway >** ［仮想サーバー］ の順に選択します。仮想サーバを選択し、[**Edit**] をクリックします。
2. [**CA** 証明書なし**]** をクリックします。
3. 「**CA** 証明書の選択」で証明書を選択し、「**OK**」、「バインド」、「完了」の順にクリックします。

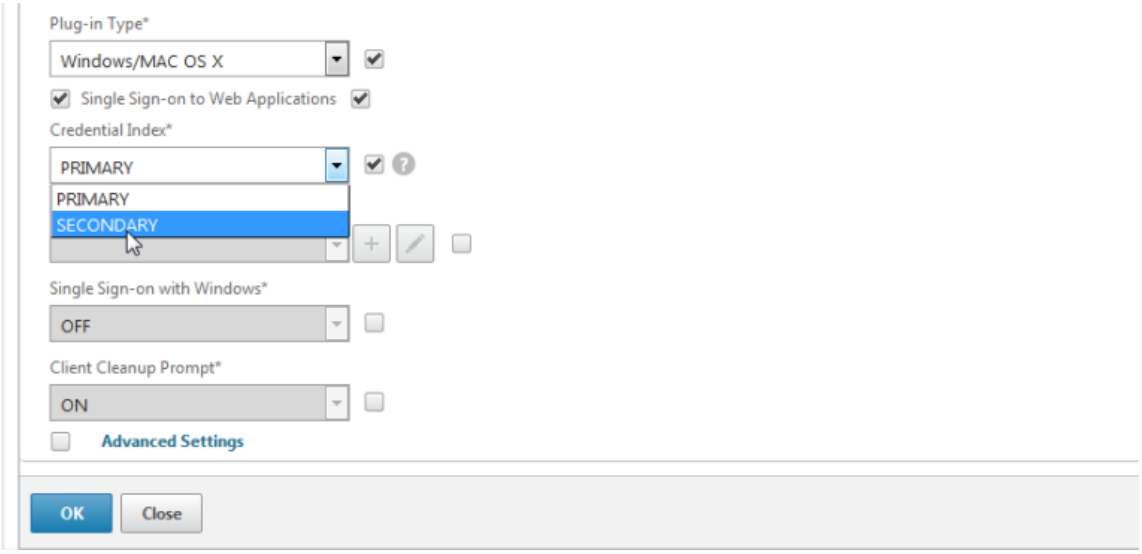
4. **[** ポリシー**] > [**セッション**] > [**セッションプロファイル] に移動し、**AC_OS** で始まるプロファイルを選択して [編集] をクリックします。



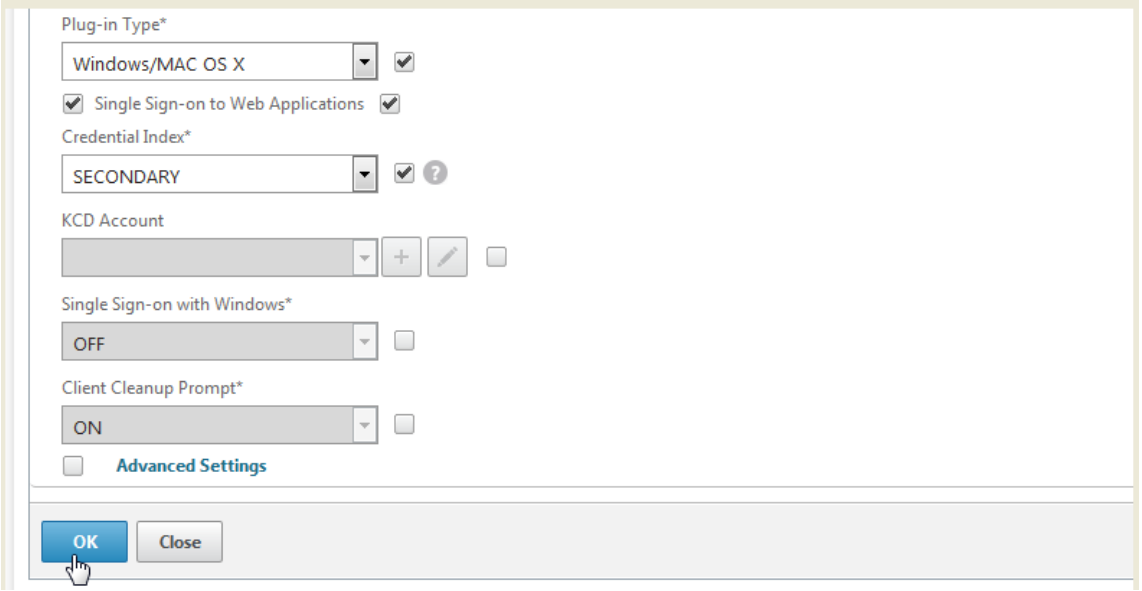
5. [クライアントエクスペリエンス] タブをクリックし、ページの下部に移動します。



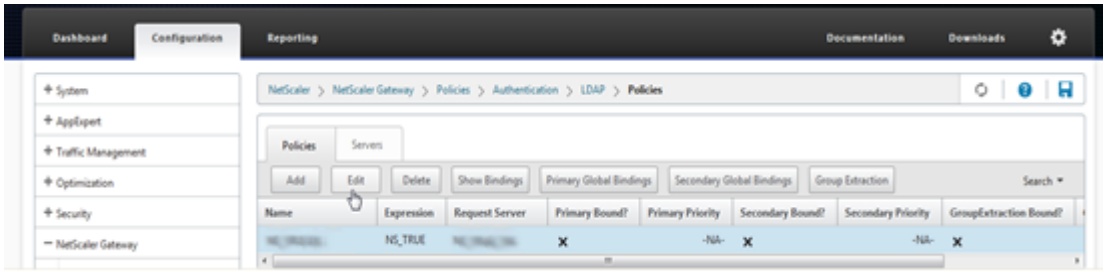
6. 「認証情報インデックス」から、「**SECONDARY**」を選択します。



7. [**OK**] をクリックします。

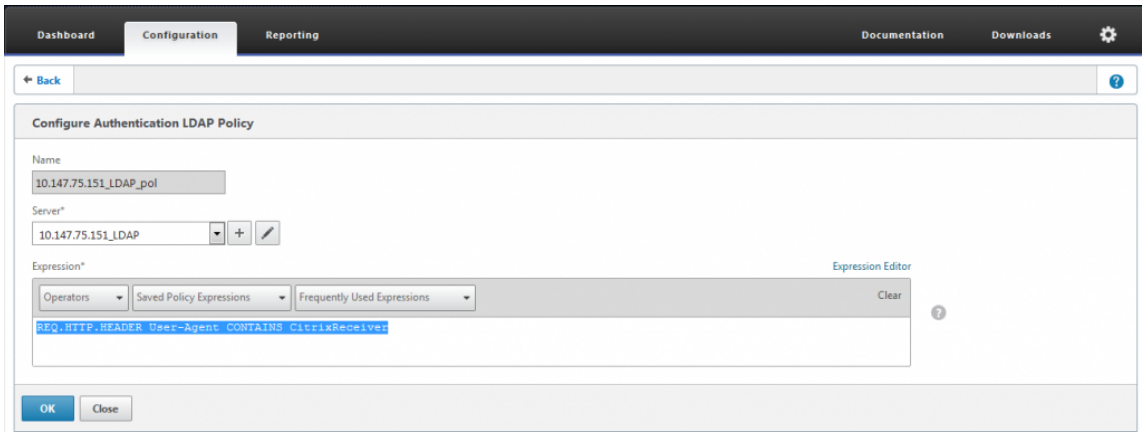


8. [ポリシー**] > [**認証**] > [LDAP**] に移動し、[**LDAP** ポリシー] タブをクリックして [編集] をクリックします。

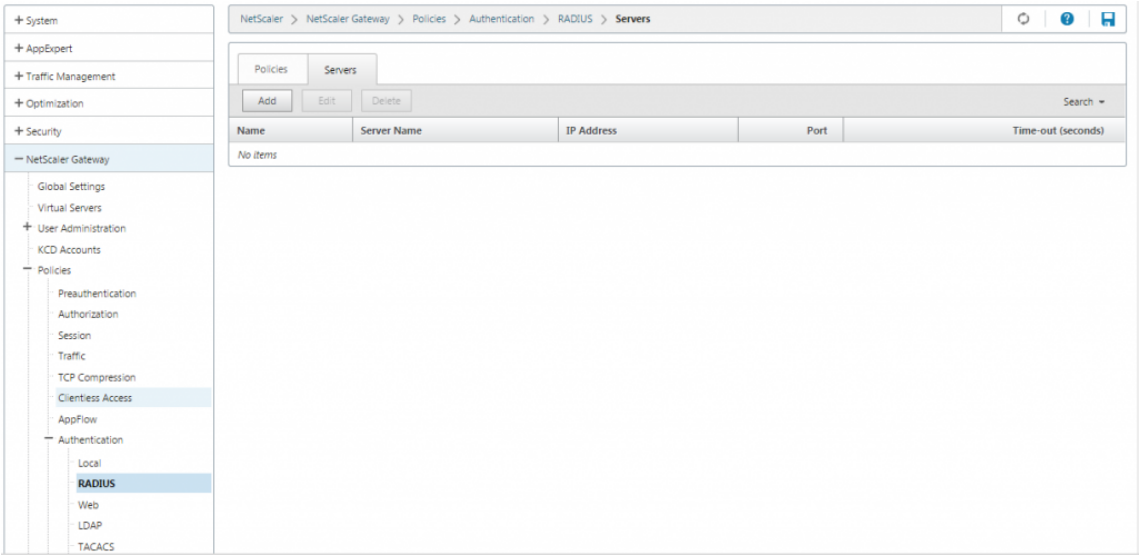


9. Citrix Endpoint Management と Citrix Endpoint Management および Citrix Virtual Apps and Desktops に個別の Citrix Gateway VIP を使用するには、**Expression** で **NS_TRUE** を次のように置き換えます。

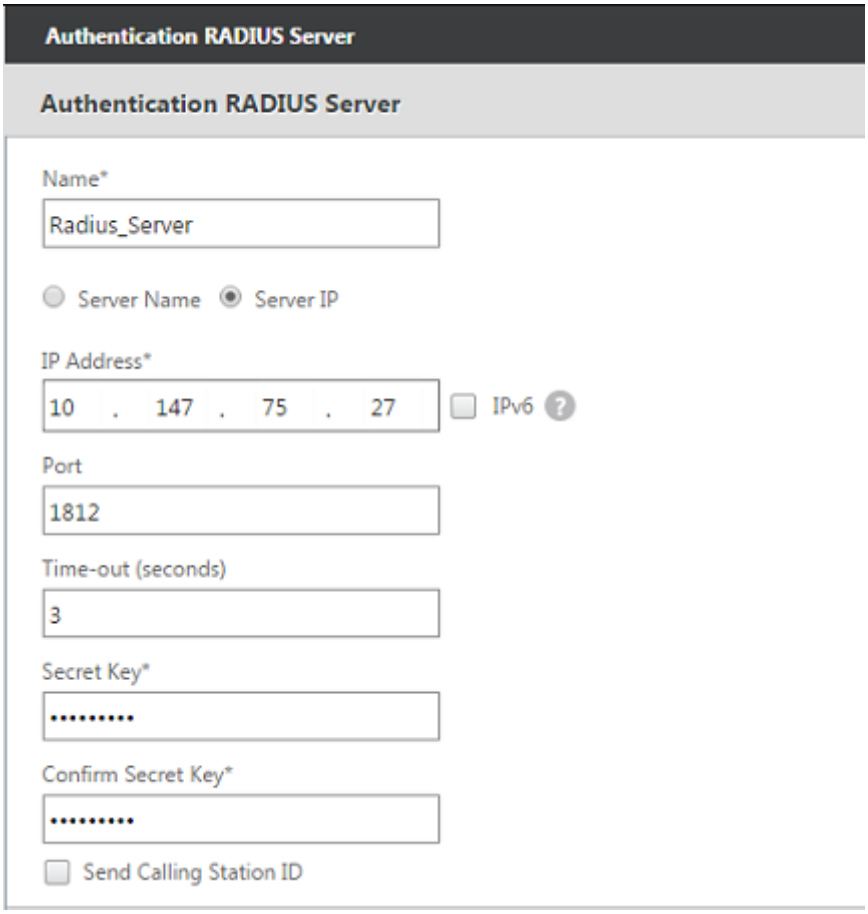
   REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver



10. [ポリシー**] > [**認証**] > [RADIUS**] に移動し、[サーバー] タブをクリックします。



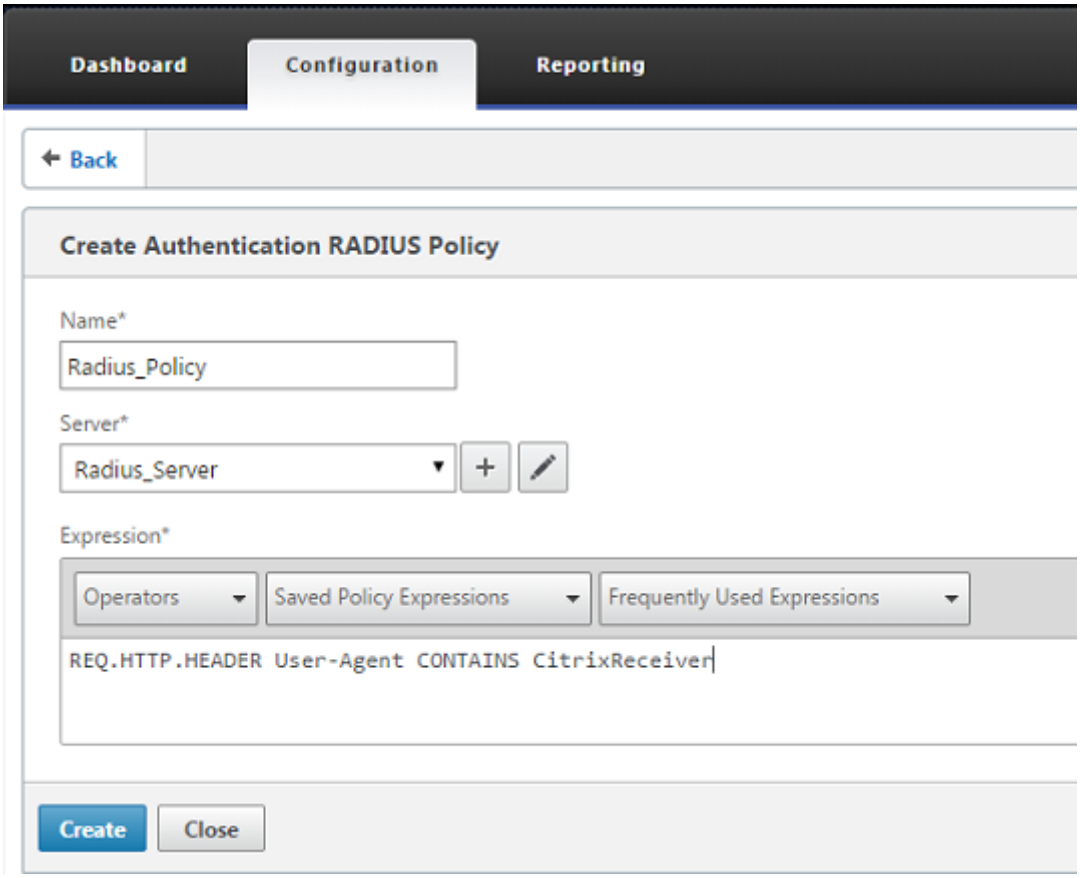
11. [追加] をクリックし、Radius サーバの詳細を入力して、[作成] をクリックします。



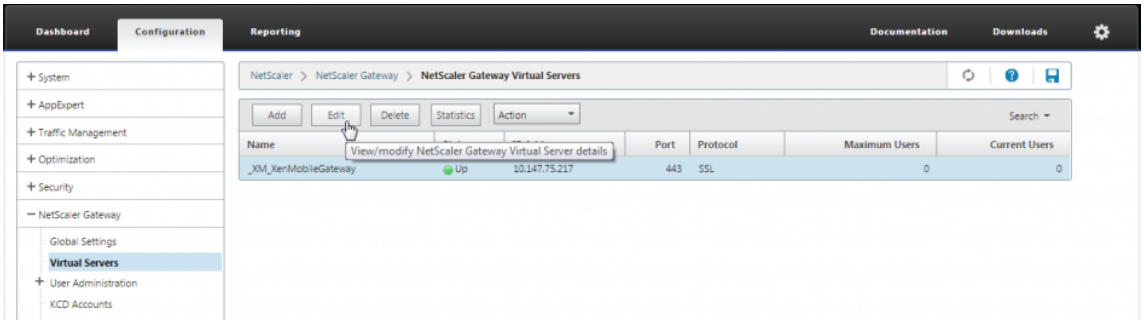
12. [ポリシー] に移動し、[追加] をクリックします。

13. ポリシーの 名前を入力します。[サーバー] ドロップダウンメニューから、Radius サーバー名 (この例では **Radius_Server**) を選択します。

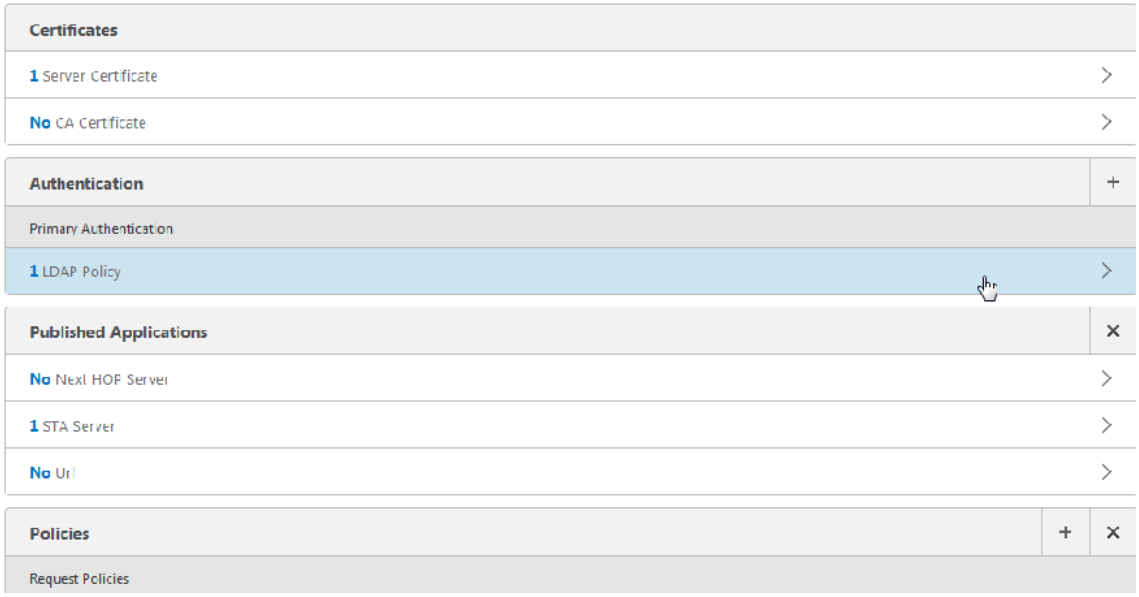
14. **[** 式] に、「**REQ.HTTP.HEADER** ユーザーエージェントが **Citrix Receiver** を含む」と入力し、[作成] をクリックします。



15. 仮想サーバを選択し、[**Edit**] をクリックします。

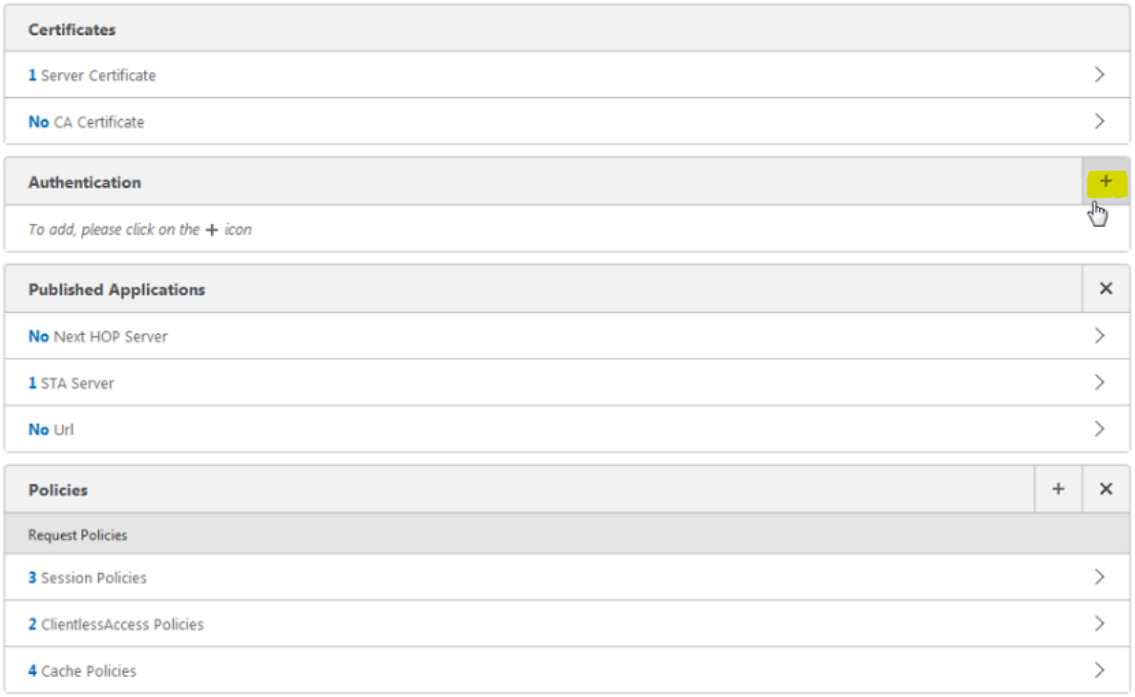


16. [プライマリ認証] で、[**LDAP** ポリシー] をクリックします。

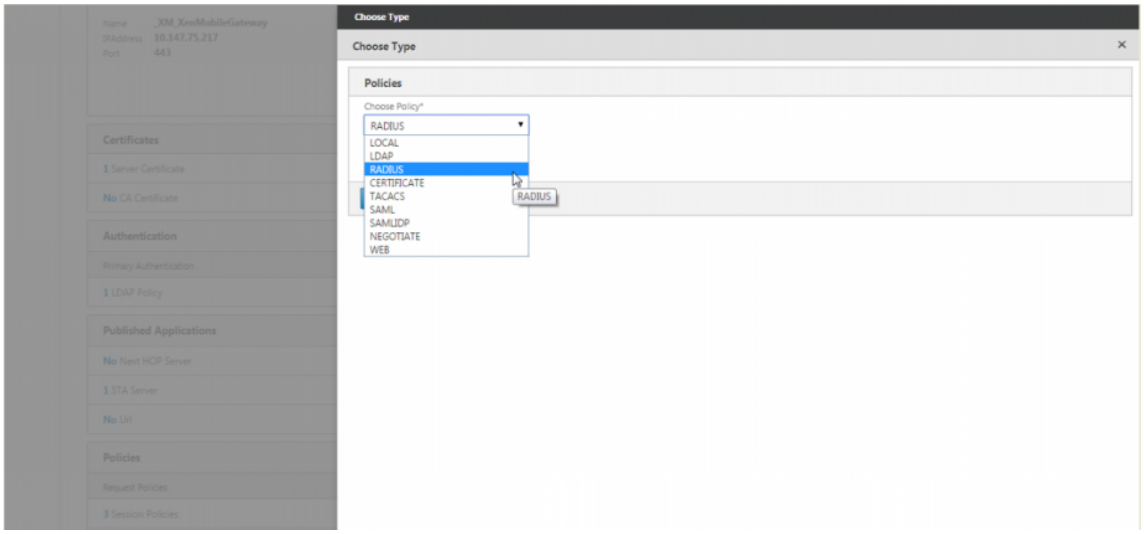


17. ポリシーを選択し、[バインド解除] をクリックして、[閉じる] をクリックします。

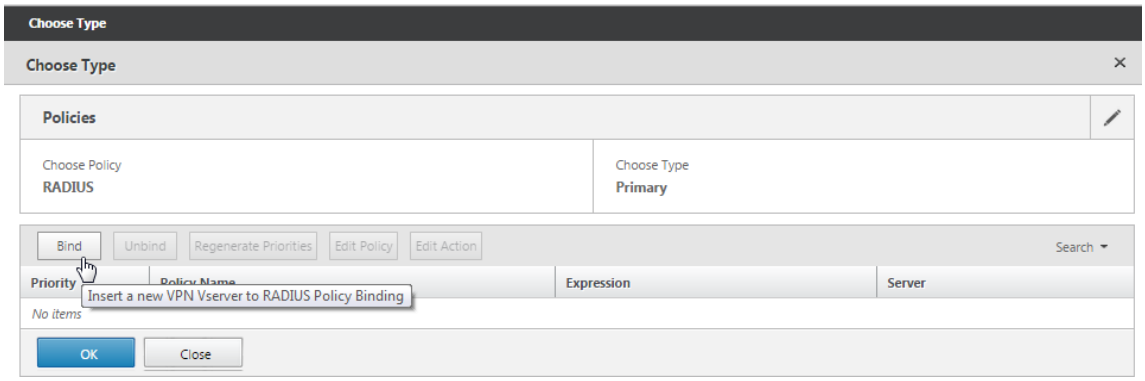
18. [認証] 行で、[+] をクリックして Radius 認証を追加します。



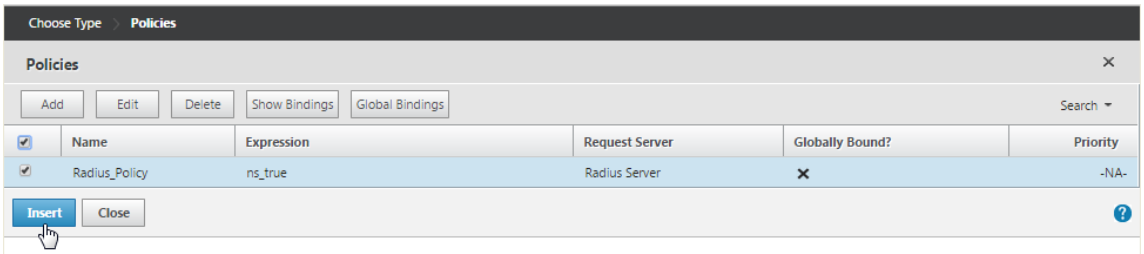
19. [タイプの選択] で、[ポリシーの選択] から [**RADIUS**] を選択します。



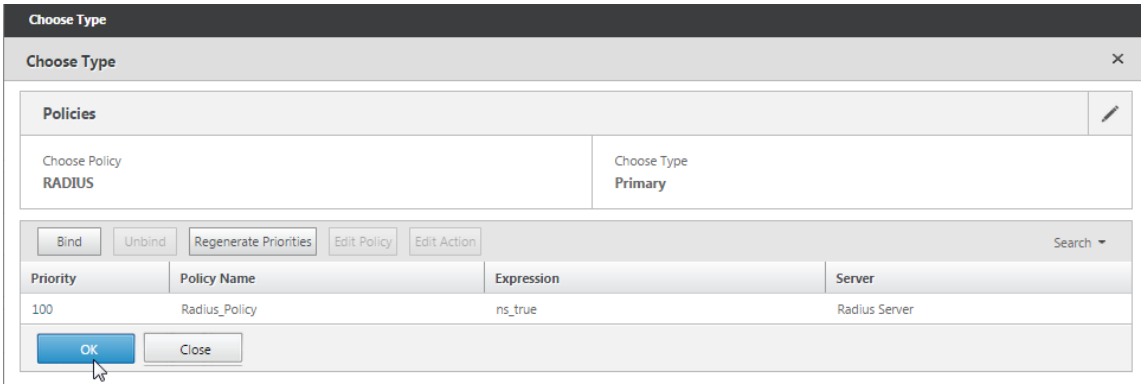
20. [バインド] をクリックします。



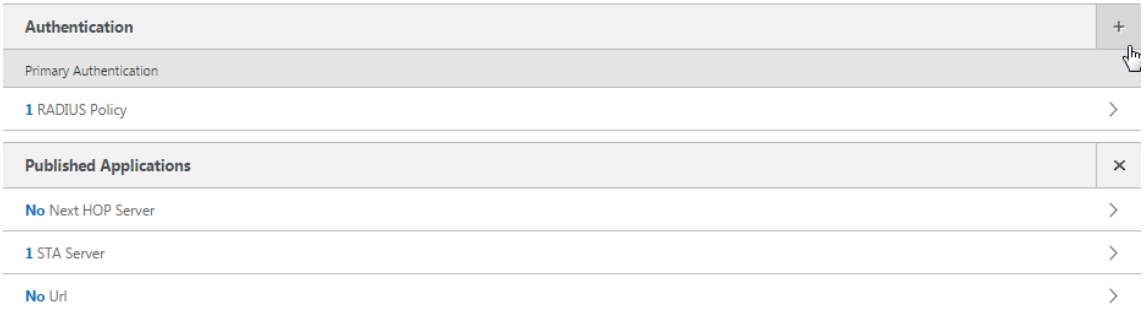
21. 前に作成した Radius 認証ポリシーを選択し、[**Insert**] をクリックします。



22. [**OK**] をクリックします。



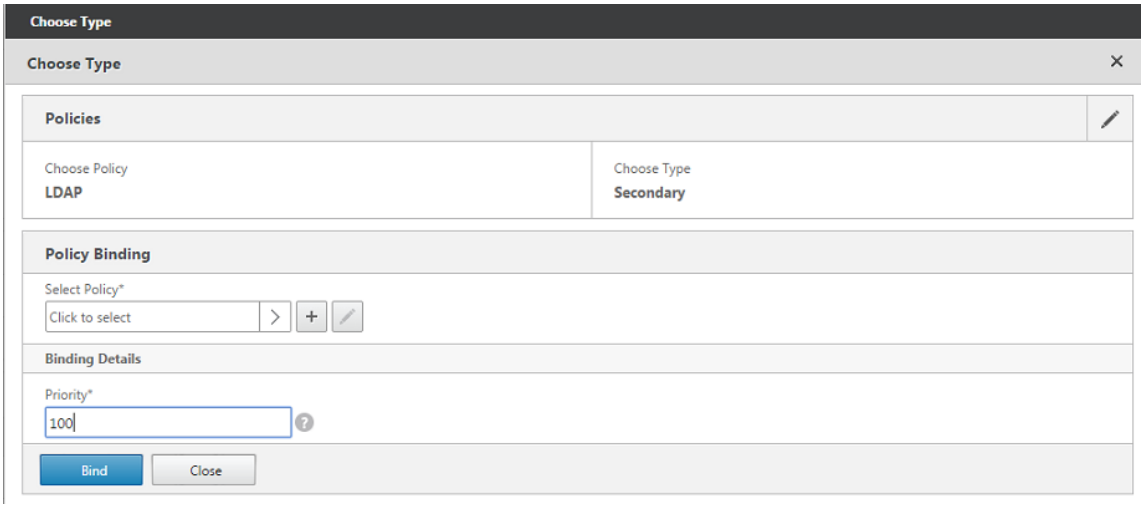
23. LDAP をセカンダリ認証ポリシーとして追加するには、[認証] 行で [**+**] をクリックします。



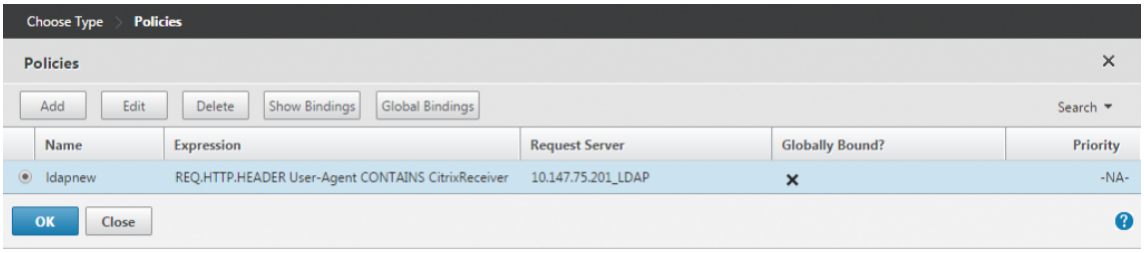
24.「ポリシーの選択」から「**LDAP**」を選択します。

25.「タイプの選択」から「セカンダリ」を選択します。

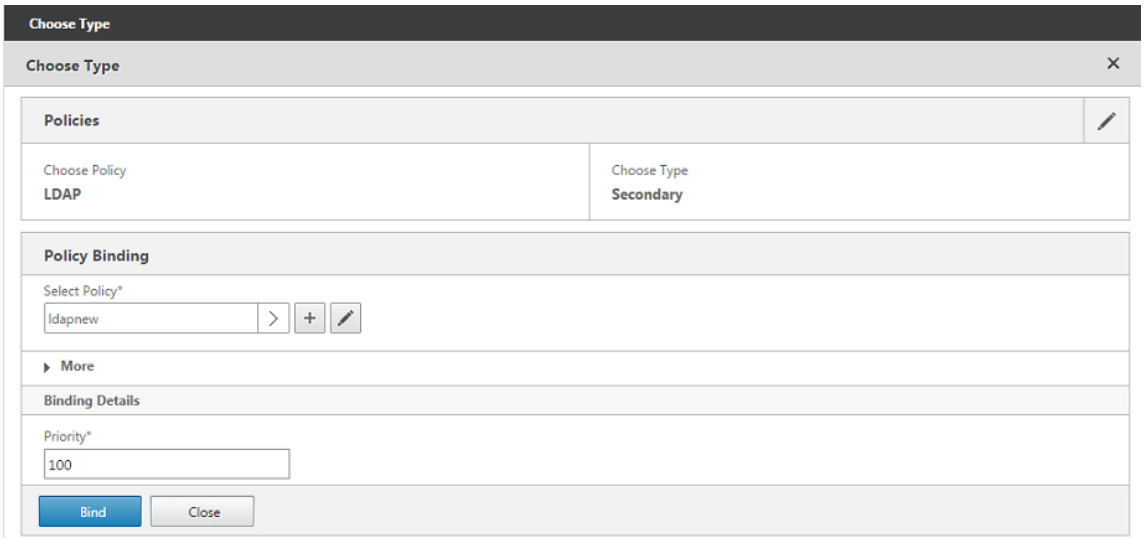
26.「ポリシーの選択」から、LDAP ポリシーを選択します。



27. ポリシーを選択し、[**OK**] をクリックします。



28. [バインド] をクリックします。



29. [完了] をクリックします。

30. 作成したポリシーの優先順位が最も高いことを確認します。これにより、モバイル以外のユーザーに対して追加のポリシーが追加された場合でも、ユーザーの優先順位が最も高くなります。詳細については、「認証ポリシーの優先順位の設定」を参照してください。

クライアント証明書またはクライアント証明書およびドメイン認証の設定

March 26, 2020

Citrix ADC for Citrix Endpoint Management ウィザードを使用して、Citrix ADC 証明書のみの認証または証明書とドメイン認証を使用する場合に、Citrix Endpoint Management に必要な構成を実行できます。Citrix Endpoint Management 用 Citrix ADC ウィザードは、1 回だけ実行できます。作成ウィザードの使用について詳しくは、「Citrix Endpoint Management 環境の設定の構成」を参照してください)。

ウィザードを既に使用している場合は、この記事の手順に従って、クライアント証明書の認証またはクライアント証明書とドメイン認証に必要な追加構成を行います。

MAM 専用モードのデバイスのユーザーがデバイス上の既存の証明書を使用して認証できないようにするには、この記事の後半の「Citrix ADC 証明書失効リスト（CRL)」を参照してください。

クライアント証明書認証のための **Citrix Gateway** の手動構成

1. [トラフィック管理] **> [**負荷分散**] > [**仮想サーバー] で、各仮想サーバー (443 と 8443 の両方) に移動し、**SSL** パラメーターを更新し、**[**セッション再利用の有効化**]** を **[**DISABLED] に設定します。
2. Citrix Gateway 仮想サーバーで、「クライアント 認証を有効にする」**->**「クライアント証明書」で「クライアント認証」を選択し、「クライアント証明書」で「必須」を選択します。
3. 認証証明書ポリシーを作成し、Citrix Endpoint Management が Secure Hub から Citrix Gateway に提供されるクライアント証明書から ユーザープリンシパル名または **sAMAccount** を抽出できるようにします。詳しくは、「XenMobile 用 Citrix ADC ADC ウィザード」を参照してください。
4. 証明書プロファイルの次のパラメータを設定します。

   Authentication Type：**CERT**

   2 つの要素：**OFF** （証明書のみの認証用）

   ユーザー名フィールド: 件名: **CN**

   Group Name Field：**SubjectAltName:PrincipalName**
5. Citrix Gateway 仮想サーバーで、証明書認証ポリシーのみを プライマリ認証としてバインドします。
6. ルート CA 証明書をバインドして、Citrix Gateway に提示されたクライアント証明書の信頼を検証します。

クライアント証明書とドメイン認証のための **Citrix Gateway** の手動構成

1. [トラフィック管理] **> [**負荷分散**] > [**仮想サーバー] で、各仮想サーバー (443 と 8443 の両方) に移動し、**SSL** パラメーターを更新し、**[**セッション再利用の有効化] を [**DISABLED**] に設定します。
2. 「ポリシー」**>**「認証」**>**「証明書」の順に選択し、「サーバー」タブを選択して「追加」をクリックします。
3. プロファイルの 名前を入力し、[**2** ファクタ] を [オン] に設定し、[ユーザ名フィールド] から [サブジェクト **AltNamePrincipalName]** を選択します。
4. [ポリシー] に移動し、[追加] をクリックします。
5. ポリシーの 名前を入力し、[サーバ] から証明書プロファイルを選択し、[式] を **ns_true** に設定して、 [作成] をクリックします。
6. 「仮想サーバー」に移動し、仮想サーバーを選択して「編集」をクリックします。
7. [認証] の横の [**+**] をクリックして、証明書認証を追加します。
8. 認証方法を選択するには、「ポリシーの選択」から「証明書」を選択します。
9. 「タイプの選択」で、「プライマリ」を選択します。これにより、LDAP 認証タイプと同じプライオリティのプライマリ認証として証明書認証がバインドされます。
10. [ポリシーのバインド] で、**[**クリックして選択**]** をクリックして、以前に作成した証明書ポリシーを選択します。

11. 前に作成した証明書ポリシーを選択し、[**OK**] をクリックします。
12. [優先度] を **100** に設定し、[バインド] をクリックします。後続の手順で LDAP 認証ポリシーを設定する場合は、同じプライオリティ番号を使用します。
13. [**LDAP** ポリシー] の行で、[**>**] をクリックします。
14. ポリシーを選択し、「編集」ドロップダウンメニューから「バインディングの編集」をクリックします。
15. 証明書ポリシーに指定したのと同じ [優先度] 値を入力します。［バインド］をクリックします。
16. ［閉じる］をクリックします。
17. [詳細設定] の **[SSL** パラメータ**]** をクリックします。
18. [クライアント認証] チェックボックスをオンにし、[クライアント証明書] から [必須] を選択し、[**OK**] をクリックします。
19. ［完了］をクリックします。

Citrix ADC 証明書失効リスト **(CRL)**

Citrix Endpoint Management では、サードパーティの認証局に対してのみ証明書失効リスト（CRL）がサポートされます。Microsoft CA を構成している場合、Citrix Endpoint Management は Citrix ADC を使用して失効を管理します。クライアント証明書ベースの認証を構成する場合は、Citrix ADC 証明書失効リスト（CRL）設定の「CRL 自動更新を有効にする」を構成する必要があるかどうかを検討します。この手順を使用すると、MAM-only モードのデバイスのユーザーがデバイス上の既存の証明書を使用して認証できなくなります。Citrix Endpoint Management では、新しい証明書が再発行されます。これは、ユーザーが失効した場合にユーザー証明書を生成できないためです。この設定は、CRL が期限切れの PKI エンティティを確認する場合、PKI エンティティのセキュリティを強化します。

CloudBridge によるネットワークトラフィックの最適化

March 26, 2020

ユーザーが Citrix Gateway プラグインを使用してログオンする場合、CloudBridge プラグインを使用して接続を最適化できます。このプラグインは、CloudBridge からユーザーデバイスにインストールされます。CloudBridge プラグインを使用して接続が最適化されると、ネットワークトラフィックは Citrix Gateway を介して圧縮され、高速化されます。接続で CloudBridge を有効にすると、Citrix Gateway の TCP 圧縮ポリシーが無効になります。

CloudBridge プラグインがデプロイされ、Citrix Gateway プラグインと連動します。

Citrix Gateway は、リピータープラグインのバージョン 5.5 および 6.1 と、CloudBridge プラグインのバージョン 6.2 および 7.0 をサポートしています。

CloudBridge の最適化とフロー制御は、動的なコンテンツ変更を必要とする Citrix Gateway の最適化機能よりも優先されます。HTTP トラフィックに対して CloudBridge 最適化が有効になっている場合、次の Citrix Gateway 機能は使用できません。

- Web アプリケーションへのシングル・サインオン
- ファイルタイプの関連付け
- ウェブ認証

Web アプリケーションへのシングルサインオンを許可するには、HTTP でアクセラレーションを無効にします。これを行うには、コマンドラインを使用します。Citrix Gateway シリアルコンソールにログオンし、コマンドプロンプトで次のように入力します。

add vpn trafficAction ssoact http -SSO ON

Citrix Gateway で設定された HTTP ポート宛てのネットワークトラフィックは、CloudBridge の最適化から自動的に除外されます。これがデフォルトの設定です。HTTP ポートで CloudBridge 最適化のトラフィックポリシーを設定すると、トラフィックポリシーが適用され、ネットワークトラフィックは CloudBridge によって最適化されます。ただし、Citrix Gateway の最適化機能は、そのポリシーの影響を受けるすべてのトラフィックに対して無効になります。CloudBridge は、他の Citrix Gateway 機能に影響を与えることなく、非 HTTP ポート宛てのネットワークトラフィックを高速化できます。

トラフィックポリシーを使用して、CloudBridge プラグインを使用するようにユーザー接続を設定します。その後、ポリシーをユーザー、グループ、仮想サーバー、またはグローバルにバインドできます。ポリシーは、ポリシーをバインドする場所に基づいて、またはポリシーに付与された優先順位番号に基づいて優先順位付けされます。

トラフィックポリシーを作成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで［Citrix Gateway ポリシー］を展開し、［トラフィック］をクリックします。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [名前] に、ポリシーの名前を入力します。
4. [プロファイルの要求] の横にある [新規] をクリックします。
5. [名前] に、プロファイルの名前を入力します。
6. [ブランチリピーター] で [オン] を選択し、[作成] をクリックします。
7. [トラフィックポリシーの作成] ダイアログボックスの [式の 追加] の横で、CloudBridge アクセラレーションを有効にするトラフィックタイプを表す式を選択または入力します。[式の 追加] をクリックし、[作成] をクリックして、[閉じる] をクリックします。

式を追加するときは、CloudBridge が高速化するように設定されているのと同じ IP アドレスとポート範囲を使用するネットワーク式を選択します。CloudBridge アクセラレーションを実行するには、Citrix Gateway で設定されたトラフィックの種類が、CloudBridge で設定されたサービスクラスポリシーと一致している必要があります。

すべての TCP トラフィックは、CloudBridge アクセラレーションの恩恵を受けています。シングルサインオンの使用を計画している場合は、アクセラレーションによってシングルサインオンが無効になるため、HTTP トラフィック

を加速しないでください。

Gateway UX 設定での RfWebUI パーソナ

March 26, 2020

RfWebUI ペルソナは、Citrix Gateway を介してログオンする Citrix Gateway ユーザーのための新しいログオンとポータルページを提供するテーマです。ポータルでは、Receiver、Storefront、および Citrix Endpoint Management ユーザーに、これらの製品に直接アクセスする場合と同じ GUI が提供されます。

RfWebUI ペルソナを使用するタイミング

Citrix Gateway の RfWebUI ペルソナは、Web アプリケーションや SaaS（サービスとしてのソフトウェア）アプリケーション、仮想 Windows アプリケーション、デスクトップなど、異なる CITRIX 製品で提供されるすべてのアプリケーションを単一のウィンドウで表示する必要がある場合に使用します。

次のシナリオは、RfWebUI ペルソナの使用方法を示しています。

- ユーザーが Gateway を使用して Storefront にアクセスすると、Gateway を使用せずに製品にアクセスしたときに表示される GUI とは異なる GUI が検出されます。
  解決策**:** ユーザーが Gateway を使用して Storefront にアクセスすると、RfWebUI テーマは、Gateway を使用せずに製品にアクセスしたときと同様のユーザーインターフェイスを提供します。
- ユーザーは、Gateway を使用して Citrix Workspace アプリ、Storefront、および Citrix Endpoint Management アプリケーションにアクセスし、アプリケーションが論理的にグループ化されないため、目的のアプリケーションの検索に苦労します。
  解決策： RfWebUI ペルソナは、Receiver、Storefront、Citrix Endpoint Management などの異なる製品によって提供されるアプリケーションの論理的なバンドルを作成することで、単一のペインビューのユーザーエクスペリエンスを提供します。

RfWebUI ペルソナが提供する機能

新しい RfWebUI には、次の機能があります。

- 移動
- アプリケーションの集約
- ユーザー設定の RDP プロキシリンク
- お気に入りのアプリケーション

移動

GO: Go 機能は、クリントレス VPN（CVPN）を介して Web ページへのアクセスを提供します。ユーザーは、[ブックマーク] タブの [URL] セクションに URL を入力し、[**GO**] をクリックします。

現在、**GO** 機能では、Outlook Web アプリケーション (OWA) と SharePoint の URL のみがサポートされています。

> 注**:**
> [**GO**] タブは、セッションポリシーの *clientlessAccessVPNMode* パラメーターが [有効**]** である場合にのみ表示されます。

アプリケーションの集約

アプリケーションの集約: RfWebUI テーマは、説明バナーの下に異なる製品によって提供されるアプリケーションをバンドルすることにより、単一ペインビューを提供します。たとえば、Citrix ADC 管理者が設定したすべての VPN URL は、**Web** アプリケーションおよび **SaaS** アプリケーションという名前のバンドルに含まれており、ユーザー固有の Web ブックマークは「個人用ブックマーク」の下にあります。StoreFront で Citrix Virtual Apps and Desktops アプリケーションバンドルが構成されている場合、Citrix Gateway の単一ペインビューにもこれらのバンドルが表示されます。

ユーザ設定の **RDP** プロキシリンク

ユーザーは、リモートデスクトッププロトコル (RDP) プロキシリンクを個人用ブックマークとして追加できます。個人用ブックマークが [デスクトップ] タブに表示されます。

次の RDP モードがサポートされています。

- 単一 Gateway
- ステートレス（デュアル）Gateway

> 注**:**
> RDP プロキシリンクを追加できるのは、*RDP* クライアントプロファイルが構成されている場合のみです。RDP 構成の詳細については、*RDP* プロキシのドキュメントを参照してください。

お気に入りのアプリケーション

ユーザーは、アプリケーション名の横にある **[**お気に入りに ****** 追加**]** リンクをクリックして、**[**Web** および **SaaS** アプリケーション] の下および [お気に入り] タブに ****** 個人用ブックマークにリストされている目的のアプリケーションを追加できます。一度追加されたアプリケーションは、**[**** お気に入り] タブの下に見ることができます。同じことは、[お気に入り] タブ内のアプリケーションの横にある **REMOVE** リンクをクリックして、[お気に入り] タブから削除することができます。

RfWebUI ペルソナを有効にする際の考慮事項

RfWebUI ペルソナでは、次の機能が完全にはサポートされていません。

ファイル共有機能 SMB ファイル共有にアクセスするためのファイル共有機能はサポートされていません。
メールホーム：［メールホーム］VPN パラメーターは、Citrix Gateway ポータルの埋め込みビューとして使用できません。これは、RfWebUI の **APPS** タブの下にある **Web** および **SaaS** アプリバンドル内のアプリケーションとしてアクセスすることができます。
Java クライアント： SSL トンネルを確立するためのブラウザベースの Java クライアントはこのテーマでは使用できません。

RfWebUI ペルソナの設定

RfWebUI ペルソナを適用するには：

1. Citrix ADC インターフェイスで、［構成］**>**［**Citrix Gateway** ポータルのテーマ］に移動します。
2. [ポータルのテーマ] ページで、[**RfWebUI**] チェックボックスを選択します。
3. ポータル・テーマ・ページの右上隅にある「保存」アイコンをクリックします。
4. [保存の確認] ダイアログボックスで、[はい] をクリックします。

RDP プロキシ

March 26, 2020

Citrix Gateway による **RDP** プロキシの概要と機能拡張

以下の RDP プロキシ機能を使用すると、Citrix Gateway 経由でリモートデスクトップファームにアクセスできます。

- CVPN または ICA プロキシモード（フルトンネルなし）を介して RDP トラフィックを保護します。
- Citrix Gateway を介して RDP サーバーへのシングルサインオン（SSO）。また、必要に応じて SSO を無効にするオプションも用意されています）。
- 適用（SmartAccess）機能。Citrix ADC 管理者は、Citrix Gateway 構成を通じて特定の RDP 機能を無効にできます。
- すべてのニーズに対応するシングル/ステートレス（デュアル）Gateway ソリューション（VPN/ICA/RDP/Citrix Endpoint Management）。
- カスタムクライアントを必要とせずに、RDP 用のネイティブ Windows MSTSC クライアントとの互換性。
- Microsoft が提供する既存の RDP クライアントを MACOSX、iOS、Android で使用する。

導入の概要

次の図は、展開の概要を示しています。

RDP プロキシ機能は、Citrix Gateway の一部として提供されます。一般的な展開では、RDP クライアントはリモートユーザーのマシンで実行されます。Citrix Gateway アプライアンスは DMZ 内に展開され、RDP サーバーファームは社内ネットワークにあります。リモートユーザーは、Citrix Gateway のパブリック IP アドレスに接続し、SSL VPN 接続を確立し、自己認証を行います。その後、ユーザーは Citrix Gateway アプライアンスを介してリモートデスクトップにアクセスできます。

RDP プロキシ機能は、CVPN および ICA プロキシモードでサポートされています。

> 注：Citrix Gateway は、リモートデスクトップセッションホスト（RDSH）/リモートアプリケーション/RDS マルチユーザー RDP セッションをサポートしていません。

CVPN を介した配置

このモードでは、RDP リンクは、Gateway のホームページまたはポータルに、ブックマークとして、「Add vpn URL」構成を介して、または外部ポータル経由で公開されます。ユーザーは、これらのリンクをクリックして、リモートデスクトップにアクセスできます。

ICA プロキシによる展開

このモードでは、wihome パラメーターを使用して、Gateway VIP にカスタムホームページが設定されます。このホームページは、ユーザーがアクセスできるリモートデスクトップリソースの一覧を使用してカスタマイズできます。このカスタムページは、Citrix ADC でホストできます。外部の場合は、既存の Gateway ポータルページの iFrame にすることができます。

どちらのモードでも、プロビジョニングされた RDP リンクまたはアイコンをクリックすると、対応するリソースに対する HTTPS リクエストが Citrix Gateway に到着します。Gateway は、要求された接続の RDP ファイルのコンテンツを生成し、クライアントにプッシュします。ネイティブ RDP クライアントが呼び出され、Gateway 上の RDP リスナーに接続します。Gateway は、適用（SmartAccess）をサポートすることにより、RDP サーバーへの SSO を実行します。SmartAccess では、Citrix ADC 構成に基づいてゲートウェイが特定の RDP 機能へのクライアントアクセスをブロックし、RDP クライアントとサーバー間の RDP トラフィックをプロキシします。

強制の詳細

Citrix ADC 管理者は、Citrix Gateway 構成を使用して特定の RDP 機能を設定できます。Citrix Gateway では、重要な RDP パラメーターに対して「RDP 強制」機能が提供されます。Citrix ADC は、クライアントがブロックされたパラメータを有効にできないようにします。ブロックされたパラメータが有効になっている場合、RDP 強制機能はクライアント対応パラメータよりも優先され、これらのパラメータは考慮されません。

適用でサポートされる **RDP** パラメータ

次のリダイレクションパラメータの適用がサポートされています。これらは、RDP クライアントプロファイルの一部として構成できます。

- クリップボードのリダイレクト
- プリンタのリダイレクト
- ディスクドライブのリダイレクト
- COM ポートのリダイレクト
- pnp デバイスのリダイレクト

接続フロー

接続フローは、次の 2 つのステップに分けることができます。

- RDP リソースの列挙と RDP ファイルのダウンロード。
- RDP 接続の起動。

上記の接続フローに基づいて、2 つの展開ソリューションがあります。

- ステートレス（デュアル）Gateway ソリューション-RDP リソースの列挙と RDP ファイルのダウンロードはオーセンティケータ Gateway を介して行われますが、RDP 接続の起動は RDP リスナー Gateway を介して行われます。
- 単一 Gateway ソリューション-RDP リソース列挙、RDP ファイルのダウンロード、および RDP 接続の起動は、同じ Gateway を介して行われます。

ステートレス（デュアル）**Gateway** 互換性

次の図は、展開を示しています。

- ユーザはオーセンティケータゲートウェイ VIP に接続し、クレデンシャルを提供します。
- Gateway へのログインに成功すると、ユーザーはホームページまたは外部ポータルにリダイレクトされ、ユーザーがアクセスできるリモートデスクトップリソースが列挙されます。
- ユーザーが RDP リソースを選択すると、ユーザーがクリックした公開リソースを示す形式`https://vserver-vip/rdpproxy/rdptarget/listener`で、オーセンティケータゲートウェイ VIP によって要求が受信されます。この要求には、ユーザーが選択した RDP サーバーの IP アドレスとポートに関する情報が含まれます。
- /rdpproxy/ 要求は、オーセンティケータゲートウェイによって処理されます。ユーザーはすでに認証されているため、このリクエストには有効な Gateway クッキーが付属しています。

- RDPTarget および RDPUser 情報は STA サーバーに格納され、STA チケットが生成されます。STA サーバに保存された情報は、構成済みの事前共有キーを使用して暗号化されます。オーセンティケータ Gateway は、Gateway 仮想サーバ上に構成されている STA サーバの 1 つを使用します。
- /rdpproxy/要求で取得された「リスナー」情報は、「fulladdress」として.rdp ファイルに格納され、STA チケット（STA 認証 ID が先頭に付属）は、「loadbalanceinfo」として.rdp ファイルに格納されます。
- .rdp ファイルは、クライアントエンドポイントに送り返されます。
- ネイティブ RDP クライアントが起動し、RDPListener Gateway に接続します。STA チケットを初期パケットで送信します。

  RDPListener Gateway は、STA チケットを検証し、RDPTarget および RDPUser の情報を取得します。使用する STA サーバーは、ロードバランス情報に存在する 'AuthID' を使用して取得されます。

シングル **Gateway** の互換性

次の図は、展開を示しています。

単一 Gateway 配置の場合、STA サーバーは必要ありません。オーセンティケータ Gateway は、RDPTarget と Citrix ADC AAA セッション Cookie を安全にエンコードし、.rdp ファイルに負荷分散情報として送信します。RDP クライアントが最初のパケットでこのトークンを送信すると、オーセンティケータ Gateway は RDPTarget 情報をデコードし、セッションを検索して RDPTarget に接続します。

RDP プロキシのライセンス要件

プレミアムエディション、アドバンスエディション

> 注**:** Gateway プラットフォームライセンスのみまたは標準エディションのみをお持ちのお客様には、RDP Proxy 機能をご利用いただけません。

RDP プロキシが機能するには、RDP プロキシ機能を有効にする必要があります。

```
enable feature rdpProxy
<!--NeedCopy-->
```

構成の手順

構成手順の概要は、次のとおりです。

1. 機能の有効化
2. Gateway ポータルでブックマークを作成するか、RDP リソースを列挙するカスタマイズされた Gateway ポータルを使用する
3. RDP クライアントプロファイルの構成
4. RDP サーバープロファイルの構成

必要な機能とモードを有効にする

- enable ns feature ssl
- enable ns feature sslvpn
- enable ns feature rdpproxy
- enable mode usnip

ブックマークの作成

1. RDP リソースにアクセスするために、ポータルページにブックマークを作成します (actualURL は rdp: // で始まります)。
2. vpn url <urlName> <linkName> <actualURL>の追加
   - URL は、次の形式である必要があります: rdp://<TargetIP:Port>。
   - ステートレス RDP プロキシモードの場合、URL は次の形式である必要があります: rdp://<TargetIP:Port>/<ListenerIP:Port>。
   - URL は、次の形式でポータルに公開されます:
     https://<VPN-VIP>/rdpproxy/<TargetIP:Port>
     https://<VPN-VIP>/rdpproxy/<TargetIP:Port>/<ListenerIP:Port>。
3. ブックマークをユーザ、グループ、または vpn 仮想サーバ、または vpn グローバルにバインドします。

クライアントプロファイルの設定

オーセンティケータ Gateway でクライアントプロファイルを設定します。次に、設定例を示します。

```
1 add rdpClient profile <name> [-addUserNameInRdpFile ( YES | NO )] [-
    audioCaptureMode ( ENABLE | DISABLE )] [-keyboardHook <keyboardHook
    >] [-multiMonitorSupport ( ENABLE | DISABLE )] [-psk <string>] [-
    rdpCookieValidity <positive_integer>] [-rdpCustomParams <string>] [-
    rdpFileName <string>] [-rdpHost <optional FQDN that will be put in
    the RDP file as 'fulladdress>] [-rdpUrlOverride ( ENABLE | DISABLE
    )] [-redirectClipboard ( ENABLE | DISABLE )] [-redirectComPorts (
    ENABLE | DISABLE )] [-redirectDrives ( ENABLE | DISABLE )] [-
    redirectPnpDevices ( ENABLE | DISABLE )] [-redirectPrinters ( ENABLE
     | DISABLE )] [-videoPlaybackMode ( ENABLE | DISABLE )]
2 <!--NeedCopy-->
```

RDP クライアントプロファイルを vpn vserver に関連付けます。

これは、sessionAction+sessionPolicy を設定するか、グローバル vpn パラメータを設定することによって実行できます。

例:

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>

add vpn sessionpolicy <polname> NS_TRUE <actname>

bind vpn vserver <vservername> -policy <polname> -priority <prioritynumber>
```

または

```
set vpn parameter -rdpClientprofile <name>
```

サーバプロファイルの設定

リスナー Gateway でサーバープロファイルを設定します。

- `add rdpServer Profile <profilename> -rdpIP <IPV4 address of the RDP listener> -rdpPort <port for terminating RDP client connections> -psk <key to decrypt RDPTarget/RDPUser information, needed while using STA>`

rdpServer プロファイルは、「vpn 仮想サーバー」で構成する必要があります。

- `add vpn vserver v1 SSL <publicIP> <portforterminatingvpnconnections> -rdpServerProfile <rdpServer Profile>`

構成例

- 必要な機能とモードを有効にする
  - enable ns feature ssl
  - enable ns feature sslvpn
  - enable ns feature rdpproxy
  - enable mode usnip
- ターゲット情報を持つユーザーの VPN URL を追加する

```
1  add aaa user Administrator  -password freebsd123$%^
2
3  add vpn url rdp RdpLink rdp://rdpserverinfo
4
5  add dns addrec rdpserverinfo 10.102.147.132
6
7  bind aaa user Administrator   -urlName rdp
8  <!--NeedCopy-->
```

- VPN 接続用の RDP クライアントとサーバープロファイルを構成する


```
add rdp clientprofile p1  -psk citrix -redirectClipboard ENABLE

add rdp serverprofile p1 -rdpIP 10.102.147.134 -psk citrix

add vpn vserver mygateway SSL  10.102.147.134 443  -
    rdpserverprofile p1

set vpn parameter -clientlessVpnMode ON -
    defaultAuthorizationAction ALLOW -rdpClientProfileName p1

add ssl certKey gatewaykey -cert rdp_rootcert.pem  -key
    rdp_rootkey

bind ssl vserver mygateway -certkeyName gatewaykey
<!--NeedCopy-->
```

- Citrix ADC からターゲットに接続するための SNIP を追加

```
add ns ip 10.102.147.135  255.255.255.0  -type SNIP
<!--NeedCopy-->
```

SSO を無効にするオプション

RDP プロキシを使用した SSO（シングルサインオン）機能は、Citrix ADC トラフィックポリシーを構成することで無効にできます。これにより、ユーザーは常に資格情報の入力を求められます。SSO が無効になっていると、RDP の適用 (SmartAccess) が機能しません。

設定例:

```
add vpn trafficaction <TrafficActionName> HTTP -SSO OFF
<!--NeedCopy-->
```

トラフィックポリシーは、要件に従って設定できます。次に、2 つの例を示します。

• すべてのトラフィックの SSO を無効にするには、次の手順を実行します。

```
add vpn trafficpolicy <TrafficPolicyName>  "url contains rdpproxy" <
    TrafficActionName>
<!--NeedCopy-->
```

• 送信元/宛先 IP/FQDN に基づいて SSO を無効にするには

```
add vpn trafficPolicy <TrafficPolicyName>  "REQ.HTTP.URL CONTAINS
    rdpproxy && REQ.IP.SOURCEIP == <IP/FQDN>" <TrafficActionName> bind
    vpnvserver rdp -policy <TrafficActionName>
```



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

単一リスナーのサポート

- RDP トラフィックと SSL トラフィックの両方に対する単一リスナー。
- RDP ファイルのダウンロードと RDP トラフィックは、Citrix ADC 上の同じ 2 タプル（IP とポート）を介して処理できます。

ブックマーク

ポータル経由の **RDP** リンク生成。ユーザーの RDP リンクを構成したり、外部ポータル経由で RDP リンクを公開したりする代わりに、targerIP: Port を指定することで、ユーザーに独自の URL を生成するオプションを与えることができます。ステートレス RDP プロキシ展開の場合、管理者は RDP クライアントプロファイルの一部として FQDN: ポート形式で RDP リスナー情報を含めることができます。これは、rdpListener オプションの下で行われます。この構成は、デュアル Gateway モードでポータルを介した RDP リンク生成に使用されます。

RDP プロキシの設定

RDP プロキシを設定するには、次の手順を実行します。

1. [**Citrix Gateway**] を展開し、[ポリシー] を展開し、[RDP] を右クリックして [機能を有効にする] をクリックします。
2. 左側の [RDP] をクリックします。右側の [クライアントプロファイル] タブに切り替えて、[追加] をクリックします。
3. クライアントプロファイルに名前を付け、必要に応じて構成します。下にスクロールする
4. [RDP ホスト] フィールドに、RDP プロキシリスナーに解決する FQDN を入力します。これは通常、Citrix Gateway アプライアンスの FDQN と同じ FQDN です。
5. 下部付近には事前共有キーがあります。パスワードを入力し、[**OK**] をクリックします。これは後で必要になります。
6. サーバプロファイルに名前を付けます。
7. これをバインドする Gateway 仮想サーバーの IP アドレスを入力します。
8. RDP クライアントプロファイルに設定したのと同じ事前共有キーを入力します。[作成] をクリックします。
9. クライアントレスアクセスのポータルページに RDP ブックマークを配置する場合は、左側で [**Citrix Gateway**]、[リソース]、[ブックマーク] の順に展開します。
10. 右側の [追加] をクリックします。
11. ブックマークに名前を付けます。

12. URL には、「rdp: //IP または DNS を使用して MyRDP サーバ」と入力します。
13. [Citrix Gateway をリバースプロキシとして使用] の横にあるチェックボックスをオンにし、[作成] をクリックします。
14. 必要に応じて、さらにブックマークを作成します。
15. セッションプロファイルまたはポリシーを作成または編集します。
16. [セキュリティ] タブで、[既定の承認操作] を [許可] に設定します。または、承認ポリシーを使用してアクセスを制御することもできます。
17. [リモートデスクトップ] タブで、前に作成した RDP クライアントプロファイルを選択します。
18. ブックマークを使用する場合は、[クライアントエクスペリエンス] タブで、[クライアントレスアクセス] を **[**オン] に設定します。
19. [公開アプリケーション] タブで、**ICA** プロキシが **OFF** になっていることを確認します。
20. Gateway 仮想サーバーを変更または作成します。
21. [基本設定**]** セクションで、[詳細] をクリックします。
22. RDP サーバープロファイルリストを使用して、前に作成した RDP サーバープロファイルを選択します。
23. 下にスクロールします。[**ICA** のみ**]** がオフになっていることを確認します。
24. 証明書をバインドします。
25. バインド認証ポリシー。
26. RDP クライアントプロファイルが設定されているセッションポリシー/プロファイルをバインドします。
27. ブックマークは、Citrix Gateway 仮想サーバーまたは Citrix ADC AAA グループにバインドできます。Citrix Gateway 仮想サーバーにバインドするには、右側の［詳細設定］セクションで［公開アプリケーション］をクリックします。
28. 左側の [公開アプリケーション] セクションで、[**URL** なし] をクリックします。
29. ブックマークをバインドします。
30. この Citrix Gateway 仮想サーバーには ICA のみが指定されていないため、Citrix Gateway ユニバーサルライセンスが正しく構成されていることを確認してください。左側で **Citrix Gateway** を展開し、［グローバル設定］をクリックします。
31. 右側の [認証 **AAA** 設定の変更] をクリックします。
32. [最大ユーザー数**]** をライセンス制限に変更します。
33. DNS を使用して RDP サーバーに接続する場合は、アプライアンスで DNS サーバーが設定されていることを確認します（トラフィック管理 **> DNS >** ネームサーバー）。
34. FQDN の代わりに短い名前を使用する場合は、D**NS** サフィックスを追加します **([**トラフィック管理**] > [DNS] > [DNS** サフィックス**])**。

35. Gateway に接続してログオンします。
36. ブックマークを設定した場合は、**** ブックマーク ** をクリックします。
37. アドレスバーを **/rdpproxy/MyRDPServer** に変更することができます。IP アドレス (例:rdpproxy/192.168.1.50) または DNS 名 (/rdpproxy/myserver) を入力できます。
38. ダウンロードした.rdp ファイルを開きます。
39. **Citrix Gateway** ポリシー］**>**［**RDP**］の順に選択して、現在接続しているユーザーを表示できます。**** 右側は **[**** 接続] タブです。

ステートレス **RDP** プロキシ

March 26, 2020

ステートレス RDP プロキシは、RDP ホストにアクセスします。ユーザーが別の Citrix Gateway オーセンティケータで認証を行うと、Citrix Gateway 上の RDPListener によってアクセスが許可されます。Citrix Gateway の RDPListener に必要な情報は、STA サーバーに安全に保存されます。

ここでは、この機能用に作成されたフローノブと新しいノブについて説明します。

前提条件

- ユーザーは Citrix Gateway 認証システム上で認証されます。
- 最初の /rdpproxy URL および RDP クライアントは、別の RDPListener Citrix Gateway に接続されています。
- RDPListener Gateway 情報は、STA サーバを使用してオーセンティケータゲートウェイによって安全に渡されます。

構成

- 新しい *rdpServer* プロファイルを追加します。サーバプロファイルは、RDPListener Gateway 上で構成されます。

```
1  add rdpServer Profile [profilename] -rdpIP [IPV4 address of the
      RDP listener] -rdpPort [port for terminating RDP client
      connections] -psk [key to decrypt RDPTarget/RDPUser
      information, needed while using STA].
2  <!--NeedCopy-->
```

  ステートレス RDP プロキシの場合、STA サーバーは、RDP クライアントから送信される STA チケットを検証して、RDP ターゲット/RDPUser 情報を取得します。

rdpServer プロファイルは、次のコマンドを使用して vpn 仮想サーバ上で設定します。

```
1  add vpn vserver v1 SSL [publicIP] [
       portforterminatingvpnconnections] -rdpServerProfile [rdpServer
        Profile]
2  <!--NeedCopy-->
```

> 警告:
> rdpServerProfile が仮想サーバ上で構成されると、変更することはできません。また、同じ server-Profile を別の vpn 仮想サーバで再利用することはできません。

rdp プロファイルコマンドの名前が **rdpClient** プロファイルに変更され、新しいパラメータが追加されました。マルチモニターサポートコマンドが追加されました。また、RDP クライアントプロファイルの一部としてサポートされていないカスタムパラメータを設定するオプションが追加されました。接続は常にセキュリティで保護されているため、clientSSL パラメータが削除されました。クライアントプロファイルは、オーセンティケータ Gateway で設定されます。

```
1  add rdpClient profile <name> -rdpHost <optional FQDN that will be put
       in the RDP file as  'fulladdress' > [-rdpUrlOverride ( ENABLE |
       DISABLE )] [-redirectClipboard ( ENABLE | DISABLE )] [-
       redirectDrives ( ENABLE | DISABLE )]
2
3            [-redirectPrinters ( ENABLE | DISABLE )] [-keyboardHook <
                keyboardHook>] [-audioCaptureMode ( ENABLE | DISABLE )] [-
                videoPlaybackMode ( ENABLE | DISABLE )]
4
5            [-rdpCookieValidity <positive_integer>][-multiMonitorSupport (
                ENABLE | DISABLE )] [-rdpCustomParams <string>] – rdpHost 構
                成 は 、 単 一 の  Gateway 展 開 で 使 用 さ れ ま す 。
```

- RDP プロファイルを vpn 仮想サーバに関連付けます。

これは、sessionAction+sessionPolicy を設定するか、グローバル vpn パラメータを設定することによって実行できます。

例

```
1  add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>
2
3  add vpn sessionpolicy <polname> NS_TRUE <actname>
4
5  bind vpn vserver <vservername> -policy <polname> -priority <
       prioritynumber>
6
7   ま た は
8
```



```
set vpn parameter  - rdpClientprofile <name>
```

接続カウンタ

新しい接続カウンタ ns_rdp_tot_curr_active_conn が追加されました。このカウンタは、使用中のアクティブな接続数の記録を保持します。これは、NetScaler シェル上の nsconmsg コマンドの一部として見ることができます。後で、このカウンタを表示する新しい CLI コマンドを提供します。

接続フロー

RDP プロキシフローには 2 つの接続があります。最初の接続は、Citrix Gateway VIP へのユーザーの SSL VPN 接続であり、RDP リソースの列挙です。

2 番目の接続は、Citrix Gateway 上の RDP リスナーへのネイティブ RDP クライアント接続（rdpIP と rdpPort を使用して構成）であり、その後 RDP クライアントからサーバーパケットへのセキュアなプロキシです。

1. ユーザは、オーセンティケータゲートウェイ VIP に接続し、クレデンシャルを提供します。
2. Gateway へのログインに成功すると、ユーザーはホームページ/外部ポータルにリダイレクトされ、ユーザーがアクセスできるリモートデスクトップリソースを列挙します。
3. ユーザーが RDP リソースを選択すると、ユーザーがクリックした公開リソース`https://AGVIP/rdpproxy/ip:port/rdptargetproxy` を示す形式で、オーセンティケータゲートウェイ VIP によって要求が受信されます。この要求には、ユーザーが選択した RDP サーバーの IP およびポートに関する情報が含まれます。
4. /rdpproxy/ 要求は、オーセンティケータゲートウェイによって処理されます。ユーザーはすでに認証されているため、このリクエストには有効な Gateway クッキーが付属しています。
5. RDPTarget および RDPUser 情報は STA サーバーに格納され、STA チケットが生成されます。情報は XML BLOB として保存されます。XML BLOB は、設定済みの事前共有キーを使用してオプションで暗号化されます。暗号化されている場合、BLOB は base64 でエンコードされ、保存されます。オーセンティケータゲートウェイは、Gateway 仮想サーバ上に構成されている STA サーバの 1 つを使用します。
6. XML BLOB は次の形式になります。

   <Value name=”IPAddress”>ipaddr</Value>\n<Value name=”Port”>port</Value>\n

   <Value name=”Username”>username</Value>\n<Value name=”Password”>pwd</Value>
7. /rdpproxy/リクエストで取得した「rdptargetproxy」は「フルアドレス」として配置され、STA チケット（STA 認証 ID の前に付加される）は.rdp ファイルの「ロードバランス情報」として配置されます。
8. .rdp ファイルは、クライアントエンドポイントに送り返されます。
9. ネイティブ RDP クライアントが起動し、RDPListener Gateway に接続します。STA チケットを最初の x.224 パケットで送信します。

10. RDPListener Gateway は、STA チケットを検証し、RDPTarget および RDPUser の情報を取得します。使用する STA サーバーは、ロードバランス情報に存在する 'AuthID' を使用して取得されます。
11. Gateway セッションは、認可/監査ポリシーを保存するために作成されます。そのユーザーのセッションがすでに存在する場合、そのセッションは再利用されます。
12. RDPListener Gateway は RDPTarget に接続し、CREDSSP を使用してシングルサインオンします。

シングル **Gateway** の互換性

RDP ファイルが /rdpproxy/rdptarget/rdptargetproxy URL を使用して生成される場合は、STA チケットが生成されます。そうでない場合は、セッションを直接参照する 'loadbalanceinfo' の現在のメソッドが使用されます。

単一の Gateway 展開の場合、/rdpproxy URL はオーセンティケータゲートウェイ自体に送信されます。STA サーバは必要ありません。オーセンティケータ Gateway は、RDPTarget および AAA セッションクッキーを安全にエンコードし、これを.rdp ファイル内の「loadbalanceinfo」として送信します。RDP クライアントが x.224 パケットでこのトークンを送信すると、オーセンティケータ Gateway は RDPTarget 情報をデコードし、セッションを検索して RDPTarget に接続します。

アップグレードに関する注意事項

以前の構成は、この新しいリリースでは機能しません。これは、vpn vserver 上で以前に構成されていたパラメータ rdpIP および rdpPort が rdpServerProfile の一部になるように更新され、'rdp プロファイル 'の名前が 'rdp クライアントプロファイル' に変更され、古いパラメータ clientSSL が削除されているためです。

RDP サーバープロファイルの作成

1. Citrix Gateway >［ポリシー］>［RDP］の順に選択します。
2.「サーバープロファイル」タブに移動し、「追加」をクリックします。
3. RDP サーバープロファイルを作成するには、次の情報を入力します。

RDP クライアントプロファイルの構成

1. Citrix Gateway > ポリシー >RDP に移動します。
2. [クライアントプロファイル] タブに移動し、[追加] をクリックします。
3. RDP サーバープロファイルを構成するには、次の情報を入力します。

仮想サーバーのセットアップ

1. Citrix Gateway >［仮想サーバー］の順に選択します。

2. [追加] をクリックして、新しい RDP サーバーを作成します。
3. この [基本設定] ページのデータを入力し、[**OK**] をクリックします。
4. 鉛筆をクリックしてページを編集します。

RDP 接続リダイレクト

March 26, 2020

Citrix Gateway アプライアンスは、接続ブローカーまたはセッションディレクトリの存在下で RDP 接続リダイレクトをサポートするようになりました。RDP プロキシ通信では、クライアントからサーバーへのすべての接続に排他的な URL が必要なくなりました。代わりに、プロキシは単一の URL を使用して RDP サーバーファームに接続するため、管理者のメンテナンスと構成のオーバーヘッドが軽減されます。

注意点:

- RDP 接続リダイレクトは、SSO が有効になっている場合にのみサポートされ、シングル Gateway モード、ステートレスモード、デュアル Gateway モード、エンフォースメント（Smart Access）の両方でサポートされます。
- RDP プロキシ機能は、IP クッキーをサポートするトークンベースのリダイレクトでのみサポートされます。IP ベースのルーティングトークン「msts=」は、「IP アドレスリダイレクトを使用する」機能が無効になっていると、Windows セッションブローカーまたは接続ブローカーによって引き渡されます。
- RDP プロキシ接続用の専用リダイレクタを構成できます。

接続ブローカの存在下で **RDPProxy** を展開する

接続ブローカが存在する RDPProxy は、次の 2 つの方法で展開できます。

- RD セッションホストサーバーが RD 接続ブローカーの負荷分散に参加している場合。
- RDP ロードバランシング機能が存在する場合。

RD 接続ブローカーの負荷分散に参加する **RD** セッションホストサーバーの場合:

この場合、RDP URL リンクは、リダイレクタとして機能する宛先サーバーとして RDP サーバーの 1 つを指すように構成できます。また、ファーム内の RDP サーバーの 1 つを宛先サーバーとして持つことも可能です（この場合、サーバーは RDP セッションを受け付けません）。詳細については、リモートデスクトッププロトコル (RDP) サーバーの負荷分散を参照してください。

RDP ロードバランシング機能が存在する場合:

接続ブローカーの負荷分散が有効になっていない場合, 我々は、接続ブローカーの存在下で RDP セッションの必要な負荷分散を行うために、Citrix ADC 上で利用可能な RDP 負荷分散機能を持つことができます. この場合、RDP URL リンクは、RDP ロードバランサーを宛先サーバーとして設定する必要があります。RDP ロードバランサーは、RDP

プロキシと同じ Citrix Gateway アプライアンス上に配置できます。詳細については、ロードバランシング rdp サーバを参照してください。

> 注:
> 接続ブローカーの存在下で RDPProxy をサポートするには、Citrix Gateway で RDP 接続リダイレクトを有効にする必要があります。

接続ブローカの存在下で **RDPProxy** を構成する

コマンドラインインターフェイスを使用して **RDP** 接続リダイレクトを構成するには、コマンドプロンプトで次のように入力します。

```
1     add rdpserverprofile <Name> -psk <string> -rdpRedirection ( ENABLE
          | DISABLE )
2
3     add rdpserverprofile serverProfileName -psk  “secretString”  -
          rdpRedirection ENABLE
4 <!--NeedCopy-->
```

Citrix ADC GUI を使用して RDP 接続リダイレクトを構成するには:

1. **Citrix Gateway >** ［ポリシー］**>** ［**RDP**］に移動します。
2. RDP を右クリックして **RDP** リダイレクト機能 を有効または 無効にします。

LDAP 属性に基づいて **RDP URL** を設定する

March 26, 2020

LDAP サーバー属性から RDP サーバー（IP/FQDN）のリストを取得するように Citrix Gateway アプライアンスを構成できます。取得したリストに基づいて、アプライアンスは特定のユーザーがアクセスするサーバーの RDP URL を表示します。

LDAP 属性に基づく **RDP URL** の設定機能の構成

コマンドラインインターフェイスを使用して **LDAP** 属性に基づいて **RDP URL** を設定するには、コマンドプロンプトで次のように入力します。

```
1     add rdpclientprofile <Name>  - rdpUrlLinkAttribute <string>
2
3 <!--NeedCopy-->
```



```
1     add rdpclientprofile clientProfileName  - rdpUrlLinkAttribute
          rdpServerAttribute
2
3  <!--NeedCopy-->
```

上記の例では、rdpServerAttribute は、LDAP サーバー上の特定のユーザーの rdp サーバーの詳細に対応します。

注：LDAP サーバーから LDAP 属性の詳細をフェッチするには、次のように pUrlLinkAttribute で設定した文字列と同じ文字列で LDAP アクションを設定する必要があります。

```
1     add authentication ldapAction dnpg_ldap -serverIP <IP address>-
          ldapBase <"domain name"> -ldapBindDn <username> -ldapLoginName
          sAMAccountName -ldapbindDnpassword <password>
2
3  <!--NeedCopy-->
```

```
1     dd authentication ldapAction dnpg_ldap -serverIP 10.102.39.101 -
          ldapBase "dc=dnpg-blr,dc=com" -ldapBindDn sqladmin@dnpg-blr.com
          -ldapLoginName sAMAccountName -ldapbindDnpassword xxxx
2
3  <!--NeedCopy-->
```

```
1     add authentication ldapPolicy dnpg_ldap_pol ns_true dnpg_ldap
2
3  <!--NeedCopy-->
```

```
1  bind vpn vs vserver\<name> -pol dnpg_ldap_pol
2
3  set ldapaction dnpg_ldap -attributes "rdpServerAttribute"
4
5  set rdpclientprofile ldap -rdpLinkAttribute rdpServerAttribute
6
7  <!--NeedCopy-->
```

LDAP サーバで、次の手順を実行します。

1. 特定の ユーザーに移動します。
2. **AD** ユーザーとコンピュータで、[表示] をクリックし、[詳細] をクリックします。
3. ユーザ名を右クリックし、アトリビュートエディタ **(Attribute Editor)** を選択します。
4. 必要な属性 (displayName) の値を変更し、[**OK]** をクリックします。

GUI を使用して LDAP 属性に基づいて RDP URL を入力するには、次の手順を実行します。

1. **Citrix Gateway >** ［ポリシー］ **>** ［**RDP**］ に移動します。

2. [**RDP** プロファイルと接続] ページで、[クライアントプロファイル] タブをクリックし、RDP ファイル名を設定するクライアントプロファイルを選択します。
3. [**RDP** クライアントプロファイルの構成**]** ページで、[**RDP** ファイル名**]** フィールドにファイル名を入力します。

RDP プロキシを使用して **RDP** ファイル名をランダム化する

March 26, 2020

RDP URL をクリックすると、RDP ファイルがダウンロードされます。RDP URL を再度クリックすると、同じ名前の新しい RDP ファイルがダウンロードされ、新しいファイルが既存のファイルに置き換えられるポップアップが表示されます。これを避けるために、管理者は rdp ファイル名をランダム化することを選択できます。ファイル名は現在、フォーマット <rdpFileName>_<outputof time()>.rdp で time () 関数の出力を追加することによってランダム化されています。これにより、アプライアンスはファイルをダウンロードするたびに一意の RDP ファイル名を生成します。

RDP プロキシによる **RDP** ファイル名のランダム化のサポートの構成

コマンドプロンプトでコマンドラインインターフェイスを使用して **RDP** プロキシで **RDP** ファイル名をランダム化するためのサポートを構成するには、次のように入力します。

```
1     add rdpclientprofile <profileName> -rdpfileName <filename> -
          randomizeRDPFilename <YES/NO>
2
3     add rdpclientprofile clientProfileName -rdpfileName testRDP -
          randomizeRDPFilename YES
4 <!--NeedCopy-->
```

Citrix ADC GUI を使用して **RDP** プロキシを使用して **RDP** ファイル名をランダム化するためのサポートを構成するには:

1. **Citrix Gateway** > ［ポリシー］ > ［**RDP** ］ に移動します。
2. [**RDP** プロファイルと接続] ページで、[クライアントプロファイル] タブをクリックし、RDP ファイル名のランダム化機能を構成するクライアントプロファイルを選択します。
3. [**RDP** クライアントプロファイルの設定] ページで、[ランダム化された **RDP** ファイル名] フィールドの横のドロップダウンで [はい] を選択します。

RDP アプリのファイル名を構成する

March 26, 2020

RDP アプリをダウンロードすると、アプリは設定されたファイル名でローカルに保存できます。

RDP アプリのファイル名を構成する

CLI を使用して **RDP** アプリケーションのファイル名を構成するには、コマンドプロンプトで次のように入力します。

```
set rdpclientprofile <Name> -rdpfilename <filename>.rdp
<!--NeedCopy-->
```

GUI を使用して **RDP** アプリケーションのファイル名を構成するには**:**

1. **Citrix Gateway** > ［ポリシー］ > ［**RDP** ］に移動します。
2. [**RDP** プロファイルと接続] ページで、[クライアントプロファイル] タブをクリックします。RDP ファイル名のランダム化機能を構成するクライアントプロファイルを選択します。
3. [**RDP** クライアントプロファイルの構成**]** ページで、[**RDP** ファイル名**]** フィールドに rdp プロファイルの名前を入力します。ファイルの名前は、次の形式である必要があります。名前に使用できる文字数は最大 31 文字です。

Citrix Gateway が VMware ホライゾンビューに対して PCoIP プロキシサポートを有効にしました

March 26, 2020

Citrix Gateway 12.0 は、PC-over-IP（PCoIP）プロトコルをサポートしています。PCoIP（PC-over-IP）プロトコルは、VMware Horizon View を含むいくつかの非 Citrix VDI ソリューションのリモート表示プロトコルです。PCoIP は、Citrix HDX/ICA プロトコルと Microsoft RDP プロトコルに類似しています。PCoIP は UDP ポート 4172 を使用します。

PCoIP が Citrix Gateway を介してプロキシされる場合、Citrix Gateway は、View セキュリティサーバや VMware アクセスポイントなどの従来の PCoIP リモートアクセスソリューションを置き換えることができます。

以下のシナリオは、**Citrix Gateway** 対応の **VMWare Horizon View** ソリューションの使用方法を示しています。

- VMware Horizon View セキュリティサーバまたは VMware アクセスポイントを展開せずに、Citrix Gateway を介して VMware Horizon View デスクトッププールおよびアプリケーションプールにリモートでアクセスする必要がある VMware Horizon PCoIP ユーザー。

- PCoIP ユーザーは、Citrix Gateway を介して他の PCoIP ベースの仮想デスクトップソリューションにリモートアクセスします。

> 注
>
> Citrix Gateway は、リモートアクセスソリューションとして展開されます。

VMWare Horizon ビューの **Citrix Gateway** が有効になっている **PCoIP** プロキシの構成

March 26, 2020

前提条件

バージョン -Citrix ADC 12.0 以降

ユニバーサルライセンス -PCoIP プロキシは、Citrix Gateway のクライアントレスアクセス機能を使用します。つまり、すべての Citrix Gateway 接続に Citrix Gateway ユニバーサル用のライセンスが必要です。Citrix Gateway 仮想サーバーで、「**ICA** のみ」がオフになっていることを確認します。

Horizon View インフラストラクチャ -機能的な内部の Horizon View インフラストラクチャ。Citrix Gateway を使用せずに内部的に Horizon View エージェントに接続できることを確認します。Citrix ADC がプロキシ接続の接続先となる View 接続サーバで、Horizon View **HTTP (S)** セキュアトンネルと **PCoIP Secure Gateway** が有効になっていないことを確認します。
以下のバージョンの VMware Horizon ビューがサポートされています。

- 接続サーバ：7.0.1 以降
- Horizon クライアント：4.2.0 以降（Windows および Mac）

ファイアウォールポート:

次の事項に留意してください。

- UDP 4172 および TCP 443 は、ホライゾンビュークライアントから Citrix Gateway VIP に対して開かれている必要があります。
- UDP 4172 は、Citrix ADC SNIP からすべての内部ホライゾンビューエージェントに対して開かれている必要があります。
- PCoIP プロキシは、NAT の背後に展開された Citrix ADC でサポートされています。考慮すべき重要なポイントは次のとおりです。
  - サポートは、VPN vServer の FQDN パラメータ設定に基づきます。
  - パブリックにアクセス可能な FQDN のみをサポートし、IP はサポートしません。
  - 443 ポートおよび 4172 ポートのみをサポート
  - スタティック NAT である必要があります。

証明書 — Citrix Gateway 仮想サーバーの有効な証明書。

認証：クラシック構文を使用した LDAP 認証ポリシー/サーバ。

Unified Gateway（オプション）：Unified Gateway の場合は、PCoIP 機能を追加する前に Unified Gateway を作成します。

RfWebUI ポータルのテーマ — Horizon View への Web ブラウザーのアクセスでは、Citrix Gateway 仮想サーバーを RfWebUI テーマで構成する必要があります。

Horizon View クライアント — Citrix ADC RfWebUI ポータルを使用して Horizon 公開アイコンにアクセスしている場合でも、Horizon View クライアントをクライアントデバイスにインストールする必要があります。

VMWare Horizon ビューの **PCoIP** プロキシをサポートするように **Citrix Gateway** を構成するには：

1. Citrix ADC 管理 GUI で、［構成］> ［**Citrix Gateway**］**>** ［ポリシー］> ［**PCoIP**］の順に選択します。

2. [PCoIP プロファイルおよび 接続**]** ページで、**VServer** プロファイルと **PCoIP** プロファイルを作成します。

3. VServer プロファイルを作成するには、[**VServer** プロファイル] タブで [追加] をクリックします。

a. VServer プロファイルの名前を入力します。

b. View 接続サーバへのシングルサインオンに使用する Active Directory ドメイン名を入力し、[作成**]** をクリックします。

注： Citrix Gateway 仮想サーバーごとに、1 つの Active Directory ドメインのみがサポートされます。また、ここで指定したドメイン名が Horizon View クライアントに表示されます。

c. [ログイン] をクリックします。

4. PCoIP プロファイルを作成するには、[プロファイル] タブで [追加] をクリックします。

a. PCoIP プロファイルの名前を入力します。

b. 内部 VMware Horizon View 接続サーバの接続 URL を入力し、[作成] をクリックします。

5. ［設定］**>** ［**Citrix Gateway**］> ［ポリシー］> ［セッション］ に移動します。

6. 右側の [セッションプロファイル] タブを選択します。

7.**Citrix Gateway** のセッションポリシーとプロファイルページで、Citrix Gateway セッションプロファイルを作成または編集します。

a. Citrix Gateway セッションプロファイルを作成するには、［追加］ をクリックして名前を指定します。

b. Citrix Gateway セッションプロファイルを編集するには、プロファイルを選択し、「編集」をクリックします。

8. [クライアントエクスペリエンス] タブで、[クライアントレスアクセス] の値が **[**オン**]** に設定されていることを確認します。

9. [セキュリティ] タブで、[既定の承認操作] の値が [許可] に設定されていることを確認します。

10. [**PCoIP**] タブで、必要な PCoIP プロファイルを選択し、[作成] をクリックします。このタブから PCoIP プロファイルを作成または編集することもできます。

11. 「作成」または「**OK**」をクリックして、セッション・プロファイルの作成または編集を終了します。

12. 新しいセッションプロファイルを作成した場合は、対応するセッションポリシーも作成する必要があります。

a. ［設定］**>**［**Citrix Gateway**］>［ポリシー］>［セッション］に移動します。

b. 右側の [セッションポリシー] タブを選択します。

c. 「追加」をクリックし、セッション・ポリシーの名前を指定し、「プロファイル」ドロップダウンから必要なセッション・プロファイル名を選択します。

d. デフォルト構文を使用してセッション・ポリシーを作成する場合は、「式」領域で「true」（引用符なし）と入力し、「作成」をクリックします。注：Unified Gateway のデフォルトは「クラシック構文」です。

e. クラシック構文を使用してセッションポリシーを作成する場合は、まず クラシック構文に切り替えるをクリックしてください。次に、[式] 領域で、「ns_true」(引用符なし) と入力し、[作成] をクリックします。

13. 作成した PCoIP VServer プロファイルとセッションポリシーを Citrix Gateway 仮想サーバーにバインドします。

a.**Citrix Gateway >**［仮想サーバー］の順に選択します。

b. 右側には、新しい Citrix Gateway 仮想サーバー を追加するか、既存の Citrix Gateway 仮想サーバー を編集します。

c. 既存の Citrix Gateway 仮想サーバーを編集する場合は、［基本設定］セクションで鉛筆アイコンをクリックします。

d. 追加と編集の両方について、**[**基本設定**]** セクションで [詳細] をクリックします。

e. [**PCoIP** 仮想サーバープロファイル] ドロップダウンを使用して、必要な PCoIP 仮想サーバープロファイルを選択します。

f. 下にスクロールして、[ICA のみ] がオフになっていることを確認します。次に、[**OK**] をクリックして [基本設定**]** セクションを閉じます。

グラム。新しい Citrix Gateway 仮想サーバーを作成する場合は、証明書をバインドし、LDAP 認証ポリシーをバインドします。

h. [**Policies**] セクションまで下にスクロールし、プラスアイコンをクリックします。

私。「タイプの選択」ページのデフォルトは「セッションおよび 要求」です。［続行］をクリックします。

J. [ポリシーのバインド] セクションで、[クリックして選択] をクリックします。

k. PCoIP プロファイルが設定されている必要なセッションポリシーを選択し、[**Select**] をクリックします。

l. [ポリシーのバインド**]** ページで、**[**バインド] をクリックします。

m. Web ブラウザを使用して VMware Horizon View に接続する場合は、右側の **[**詳細設定**]** で [ポータルテーマ] セクションを追加します。Citrix Gateway への接続に Horizon View クライアントのみを使用している場合は、この手順を実行する必要はありません。

n. [ポータルのテーマ] ドロップダウンを使用して [**RfWebUI**] を選択し、[**OK**] をクリックします。

オー。Horizon View 公開アイコンが RfWebUI ポータルに追加されます。

USB リダイレクトを有効にする手順

クライアントマシンに接続されている USB デバイスには、仮想デスクトップとアプリケーションからアクセスできます。USB リダイレクトを有効にする手順は次のとおりです。

1. VMware Horizon 管理者コンソールにログインします。
2.「インベントリ」>「構成の表示」>「サーバー」に移動します。
3. [接続サーバ] タブを選択します。
4. 表示された接続サーバを選択し、[**Edit**] をクリックします。
5. [全般] タブで、[**HTTP (S)** セキュアトンネル**]** の **[**マシンへのセキュアトンネル接続を使用する] オプションを選択します。[外部 URL] フィールドに NSG 外部 **URL** を指定します。

Unified Gateway のコンテンツスイッチング式の更新

Citrix Gateway 仮想サーバーが Unified Gateway（コンテンツスイッチング仮想サーバー）の背後にある場合は、コンテンツスイッチング式を更新して、PCoIP URL パスを含める必要があります。

1. Citrix ADC GUI で、「設定」>「トラフィック管理」**>**「コンテンツスイッチング」**>**「ポリシー」の順に選択します。

2.**[** 式**]** 領域の下に次の式を追加し、**[**OK**] をクリックします。**

http.req.url	http.req.url	http.req.url client”)	http.req.url.path.contai tunnel”)

PCoIP Gateway を使用

1. 接続するには、Horizon View Client がクライアントデバイスにインストールされている必要があります。インストールが完了したら、Horizon View クライアントのユーザーインターフェイスを使用して Citrix Gateway に接続するか、Citrix Gateway RfWebUI ポータルページを使用して Horizon から公開されたアイコンを表示できます。

2. アクティブな PCoIP 接続を表示するには、**Citrix Gateway >**［**PCoIP**］の順に選択します。

3. 右側の [接続] タブに切り替えます。アクティブなセッションが、ユーザー名、Horizon View クライアント IP、および Horizon View エージェントの宛先 IP のデータとともに表示されます。

4. 接続を終了するには、[接続] タブを右クリックし、[接続の切断] をクリックします。または、[すべての接続を終了] をクリックして、すべての PCoIP 接続を終了します。

VMware Horizon View 接続サーバの構成

March 26, 2020

Citrix Gateway 経由で PCoIP プロキシをサポートするには:

1.**VMware Horizon** 管理者コンソールにログインします。

2.**[I]-> [**** 設定の表示]-> [サーバー] に移動します。**

3. [接続サーバ] タブを選択します。

4. 表示された接続サーバを選択し、[**Edit**] をクリックします。

5. [全般] タブで、[HTTP (S) セキュアトンネル**]** の **[**マシンへのセキュアトンネル接続を使用する] オプションの選択を解除します。

6. [**OK]** をクリックして [接続サーバ設定の編集**]** ウィンドウを閉じます。

7. 一覧表示されたすべての接続サーバで、4 ～6 の手順を実行します。

HDX 対応のデータ転送サポート

March 26, 2020

Citrix Gateway の Enlightened Data Transport（EDT）のサポートにより、Citrix Workspace アプリを実行しているユーザーに対して、仮想デスクトップの高精細な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。

また、Citrix Workspace アプリと VDA 間の EDT 終了のための DTLS 1.0 によるエンドツーエンドの暗号化も容易になります。DTLS 設定の詳細については、DTLSv1.0 プロトコルのサポートをクリックしてください。

EDT 対応の Citrix Gateway は、LAN と WAN の両方の条件で優れたユーザーエクスペリエンスを提供し、一方から他方へのローミング時に管理やユーザー構成を行いません。この利点は、中程度のパケット損失を伴う高遅延ネットワークで最も顕著であり、ユーザーエクスペリエンスは一般に代替案と遅れることになる。

DTLS 1.2 プロトコルのサポート

リリース 13.0 ビルド 47.x 以降、DTLS 1.2 プロトコルは Citrix ADC VPX アプライアンスでサポートされています。VPN 仮想 サーバー **VPX** アプライアンスの **enable_dtls12_vpn_vserver** nsapimgr ノブを使用して、DTLS 1.2 を有効または無効にすることができます。

デフォルトでは、DTLS 1.2 は無効になっており、**enable_dtls12_vpn_vserver** ノブは 0 に設定されています。

DTLS 1.2 を有効にするには、**enable_dtls12_vpn_vserver** ノブを 1 に設定します。ノブ値を変更したら、DTLS をオフにし、ノブを有効にするための`set vpn vserver <vservername> dtls <ON/OFF>` コマンドを使用して再度オンに切り替えます。

> 重要：13.0 ビルド 47.x 以降にアップグレードした後、以前のリリースのビルドで DTLS を有効にし、TLSv1.2 暗号のみを使用している場合は、nsapimgr コマンドを使用して DTLS 1.2 を有効にすることをお勧めします。

Enlightened Data Transport サポートを使用するタイミング

April 9, 2020

以下のシナリオは、EDT 対応の Citrix Gateway の使用方法を示しています。

- ユーザーは、ビジネスリソースにリモートアクセスしながら、LAN 環境と同じくらい優れたエクスペリエンスを求めています。
- ユーザーは、輻輳、高いパケット損失、および高遅延のためにネットワークの品質が悪い、Wi-Fi およびセルラーネットワーク上で、豊富な仮想アプリケーションとデスクトップユーザーエクスペリエンスを必要としています。

EDT を使用している間、以下の点に留意する必要があります。

- 仮想サーバー・レベルの DTLS ノブは、デフォルトで有効になっています。
- DTLS を使用した SNI はサポートされていません。
- DTLS を使用した IPv6 はサポートされていません。
- DTLS が有効になっている場合、スマート制御ポリシーと ICA ポリシーは機能しません。
- また、Receiver と VDA 間の EDT トラフィックに対してダブルホップ機能を使用するようにアプライアンスを構成できるようになりました。詳細については、ダブルホップ DMZ での展開をクリックしてください。

> 注**:** EDT は、リリース 12.1 ビルド 49.xx 以降の MPX FIPS プラットフォームでサポートされています。インテル Coleto SSL チップベースの MPX デバイスでは、リリース 12.1 ビルド 51.16 以降から EDT がサポートされます。

EDT および HDX Insight をサポートするように Citrix Gateway を構成

March 26, 2020

Gateway 経由の EDT トラフィックは、エンドツーエンドの可視性を持つようになりました。Citrix ADM は、リアルタイムおよび履歴の両方の可視性データを使用できるため、さまざまなユースケースをサポートできます。

次のシナリオがサポートされています。

シナリオ	EDT サポート
Citrix Gateway	はい
高可用性（HA）を備えた Citrix Gateway	はい

シナリオ	EDT サポート
高可用性（HA）最適化機能を備えた Citrix Gateway	はい
Unified Gateway を使用する Citrix ADC	はい
GSLB を使用する Citrix Gateway	はい
クラスターを使用した Citrix Gateway	はい
Citrix Workspace アプリから Citrix Gateway の DTLS 暗号化への接続	はい
Citrix Gateway 上のデュアル Secure Ticket Authority（STA）	はい
Citrix Gateway ICA セッションのタイムアウト	はい
Citrix Gateway マルチストリーム ICA	はい
Citrix Gateway セッションの画面の保持性（ポート 2598）	はい
Citrix Gateway・ダブルホップ	はい
Citrix ADC から VDA への DTLS への暗号化	はい
HDX Insight	はい
IPv6 モードの Citrix Gateway	いいえ
Citrix Gateway SOCKS（ポート 1494）	いいえ
Citrix ADC pure LAN proxy	いいえ

Enlightened Data Transport をサポートするように **Citrix Gateway** を構成する

Enlightened Data Transport (EDT) を使用する場合、EDT で使用される UDP 接続を暗号化するには、データグラムトランスポート層セキュリティ (DTLS) を有効にする必要があります。DTLS パラメータは、Gateway VPN 仮想サーバレベルで有効にする必要があります。また、Citrix Virtual Apps and Desktops コンポーネントが正しくアップグレードされ、Gateway VPN 仮想サーバーとユーザーデバイス間のトラフィックが暗号化されるように構成されている必要があります。

> 注：仮想サーバーが DTLS 接続を受信するには、Citrix Gateway フロントエンド仮想サーバー用に構成された UDP ポート（ポート 443 など）を DMZ で開く必要があります。DTLS と CGP は、EDT が Citrix Gateway と連携するための前提条件です。

GUI を使用して **EDT** をサポートするように **Citrix Gateway** を構成するには

1. Citrix Gateway を展開して、StoreFront と通信し Citrix Virtual Apps and Desktops のユーザーを認証するように構成します。
2. Citrix ADC GUI の［構成］タブで、［**Citrix Gateway** を展開し、［仮想サーバー］を選択します。
3. [編集] をクリックして VPN 仮想サーバーの基本設定を表示し、DTLS 設定の状態を確認します。
4. その他の設定オプションを表示するには、「詳細」(**More**) をクリックします。
5. データグラムプロトコルの通信セキュリティを提供するには、[**DTLS**] を選択します。［**OK**］をクリックします。VPN 仮想サーバーの **[基本設定]** 領域には、DTLS フラグが **True** に設定されていることが示されます。

CLI を使用して **EDT** サポート用に **Citrix Gateway** を構成するには

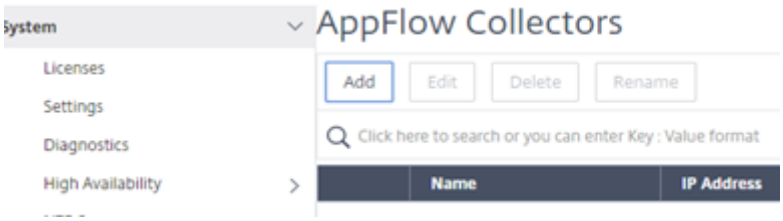
```
set vpn vserver vs1 -DTLS ON
```

HDX Insight をサポートするように **Citrix Gateway** を構成する

HDX Insight は、Citrix ADC を通過する仮想アプリケーションおよびデスクトップへの HDX トラフィックをエンドツーエンドで可視化します。また、管理者は、リアルタイムのクライアントおよびネットワーク遅延メトリック、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。

GUI を使用して **HDX Insight** をサポートするように **Citrix Gateway** を構成するには

1. [構成] タブで、[システム**] > [AppFlow] > [**コレクター] に移動し、[追加] をクリックします。



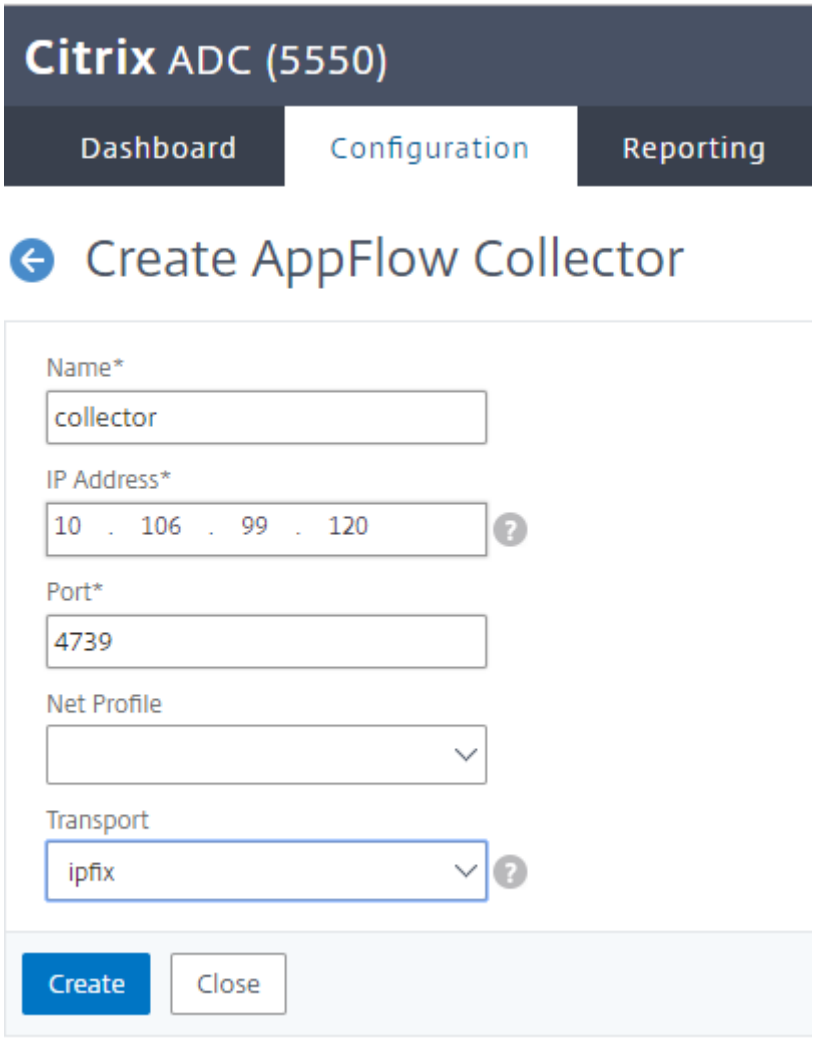
2.「**AppFlow** コレクタの作成」ページで、次のフィールドを入力し、「作成」をクリックします。
「名前」(Name) — コレクターの名前

IP アドレス：コレクタの IPv4 アドレス

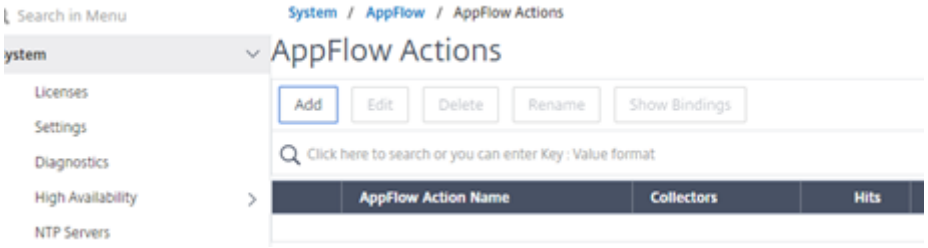
Port：コレクタがリッスンするポート

ネットプロファイル-コレクタに関連付けるネットプロファイル。プロファイルに定義されている IP アドレスは、このコレクタの AppFlow トラフィックの送信元 IP アドレスとして使用されます。このパラメータを設定しない場合、Citrix ADC IP（NSIP）アドレスが送信元 IP アドレスとして使用されます。

「トランスポート」— コレクターのトランスポートタイプ。



3. 「システム」**>**「**AppFlow**」**>**「アクション」に移動し、「追加」をクリックします。

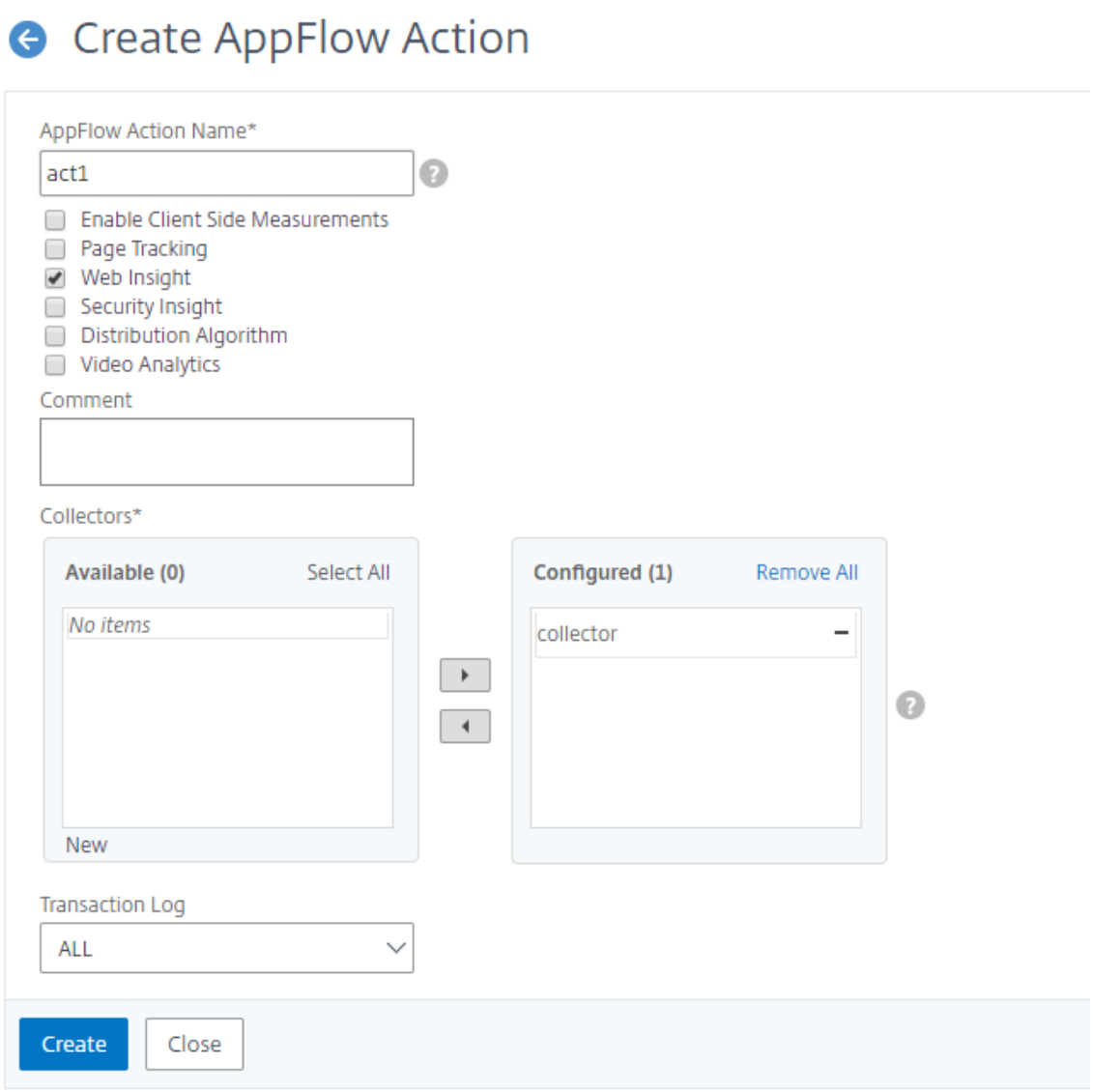


4. 「**AppFlow** アクションの作成」ページで、次のフィールドを入力し、「作成」をクリックします。
   AppFlow アクション名 — アクションの名前

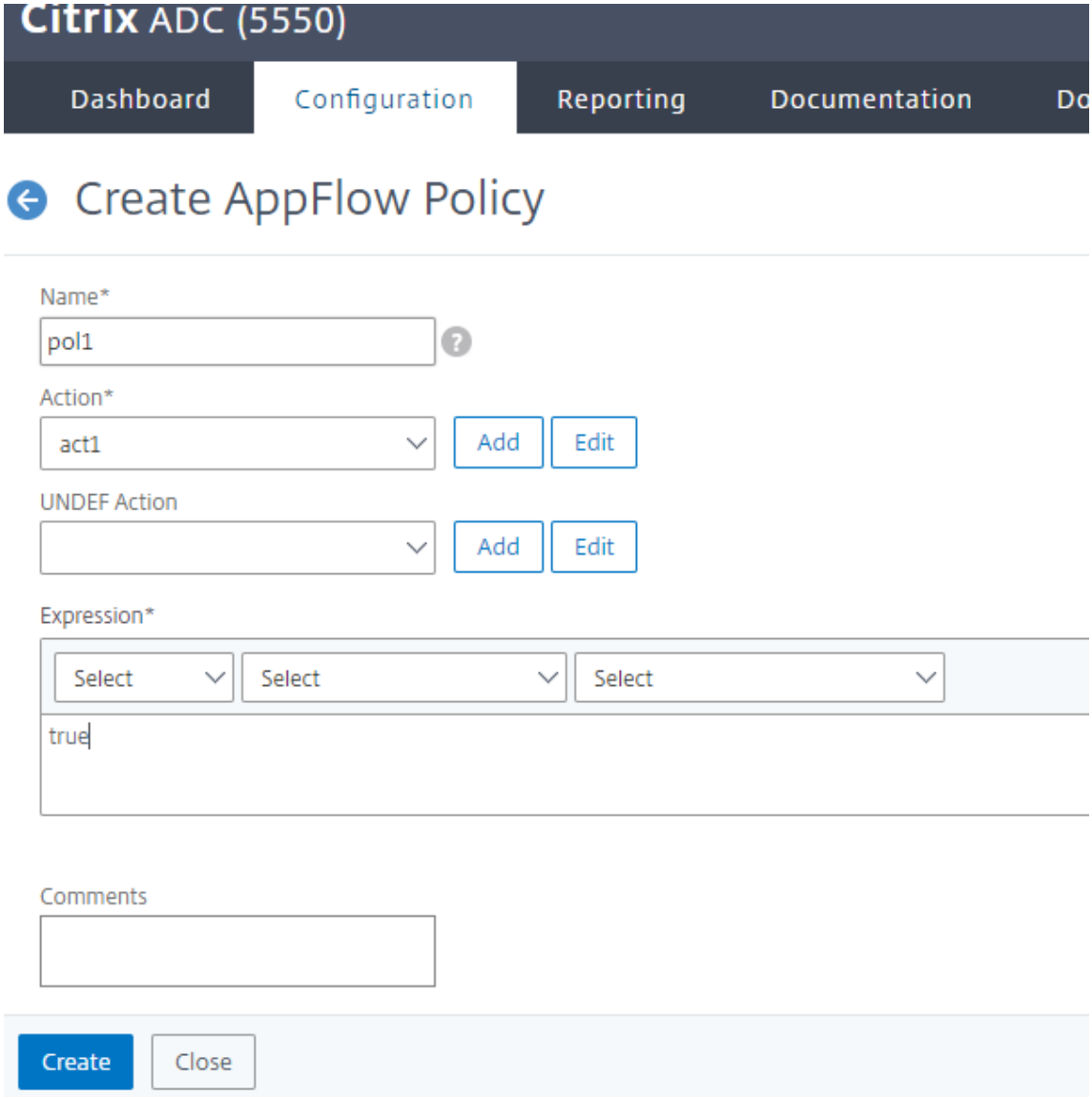
   コメント — アクションに関するコメント

   「コレクタ」— AppFlow アクションに関連付けるコレクタの名前を選択します。

[トランザクションログ] — ログに記録されるトランザクションタイプ。



5.「システム」**>**「**AppFlow**」**>**「ポリシー」に移動し、「追加」をクリックします。



6. 「**AppFlow** ポリシーの作成」ページで、次のフィールドに入力し、「作成」をクリックします。

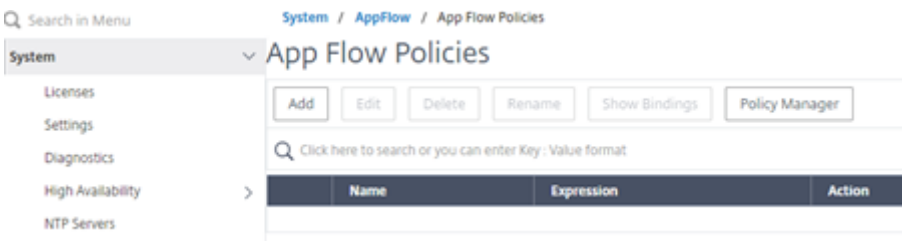
   Name：ポリシーの名前。

   Action：ポリシーに関連付けるアクションの名前。

   UNDEF-未定義のイベントが発生したときにこのポリシーに関連付ける AppFlow アクションの名前。

   Expression：トラフィックが評価される式またはその他の値。ブール式である必要があります。

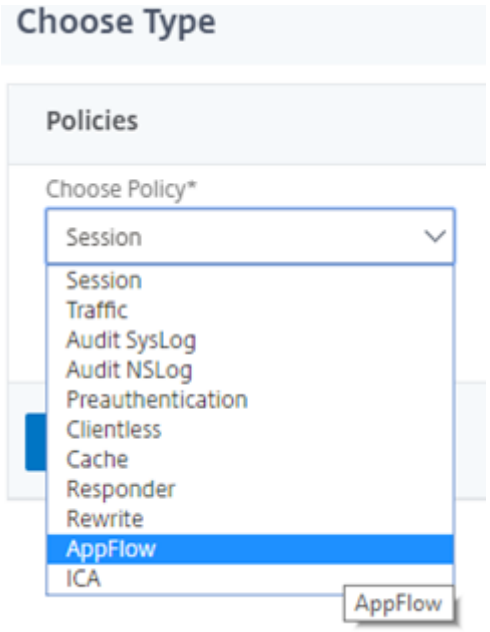
   コメント — このポリシーに関するコメント。



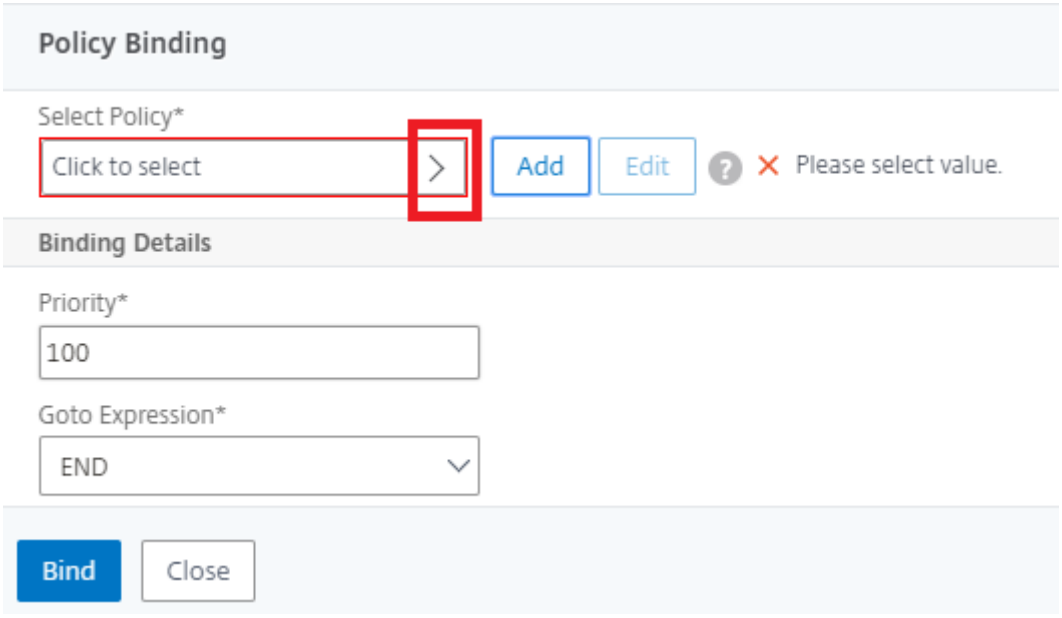
7. [**Citrix Gateway**] **>** [仮想サーバー] に移動し、仮想サーバーを選択して [編集] をクリックします。

8. [**VPN** 仮想サーバー] ページを下にスクロールし、[ポリシー] セクションで [**+**] をクリックします。

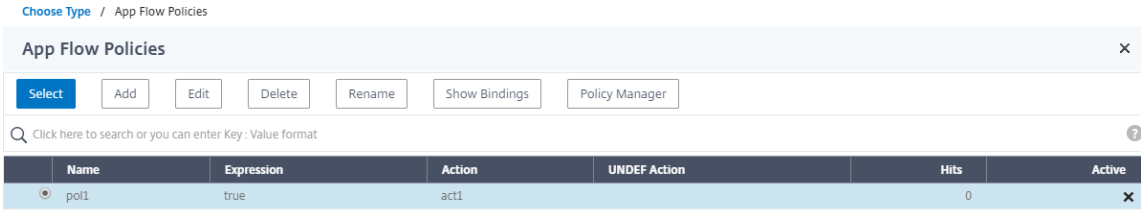
9. [種類の選択] 画面の [ポリシーの選択] ドロップダウンメニューで [**AppFlow**] を選択します。「タイプの選択」ドロップダウンメニューで「要求」または「**ICA **** 要求 ****** 」を選択し、「続行」をクリックします。



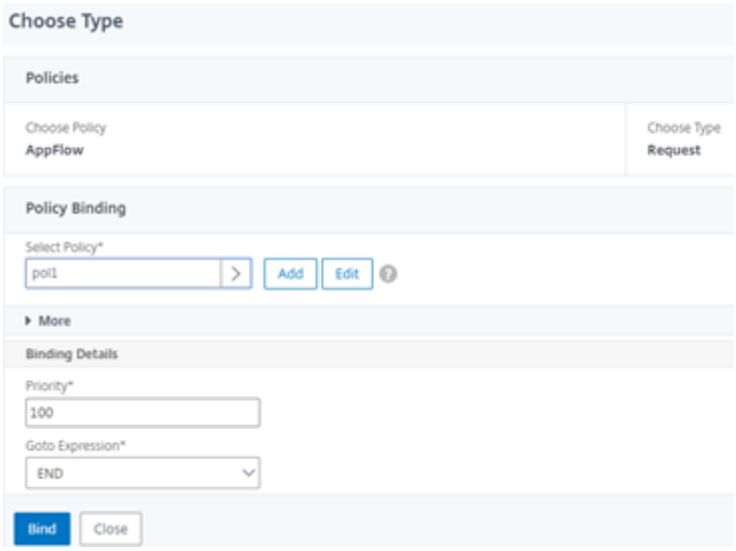
10. [ポリシーの選択] で強調表示された矢印をクリックします。



11. **AppFlow** ポリシーを選択し、「選択」をクリックします。



12. 最後に [バインド] をクリックします。



CLI を使用して **Citrix Gateway** で **HDX Insight** のサポートを構成するには、次のコマンドを入力します

```
1 add appflow collector col3 -IPAddress<ip_mas>
```



```
2 add appflow action act1 <action_name>
3 add appflow policy <policy_name> true <action_name>
4 bind vpn Vserver <vserver_name>  -pol <policy_name> - priority101 END -
     type <ICA_Request>
```

非 **NSAP HDX** セッションの **HDX Insight** を無効にする

Citrix ADC アプライアンスで、NSAP HDX 以外のセッションで HDX Insight を無効にできるようになりました。

コマンドプロンプトで、次のように入力します。

```
1 set ica parameter
2 DisableHDXInsightNonNSAP(YES | NO )
```

デフォルトでは、非 NSAP セッションの HDX Insight が有効になっています。

L7 遅延しきい値

March 26, 2020

HDX Insight の L7 レイテンシーのしきい値処理機能は、エンドツーエンドのネットワークレイテンシーの問題をアプリケーションレベルでアクティブに検出し、プロアクティブなアクションを実行します。L7 レイテンシーのしきい値処理機能は、ライブレイテンシーの監視を実行してスパイクを検出し、レイテンシーが最小観測レイテンシーを超えた場合に Insight Center に通知を送信します。

以前は、平均的なクライアント側とサーバー側の L7 レイテンシー値が 60 秒ごとに Insight Center に送信されていました。この間隔内で検出されたスパイクは平均化され、検出されないままであった。また、これらのスパイクを検出するためのライブ遅延監視もありませんでした。

L7 レイテンシーと **L4** レイテンシーの違い

ネットワーク待ち時間がキャプチャされ、L4 レベルでも表示されます。これらのレイテンシーは TCP レイヤーから計算され、ICA トラフィックの解析は必要ありません。したがって、比較的入手が容易で、CPU の負荷が少なくなります。しかし、L4 レイテンシーの主な欠点は、エンドツーエンドのレイテンシーを理解することです。パスに TCP プロキシがある場合、L4 レイテンシーは Citrix ADC から TCP プロキシへのレイテンシーだけをキャプチャします。これにより、情報が不完全になり、問題のデバッグが困難になる可能性があります。

L7 レイテンシーは、ICA トラフィックを解析することによって計算されます。L7 レイテンシーの計算は ICA レイヤーで行われるため、中間プロキシでは不完全なレイテンシー値は発生しません。したがって、はエンドツーエンドの遅延検出を提供します。

次の図は、TCP プロキシを使用する場合と使用しない場合の展開の種類を示しています。

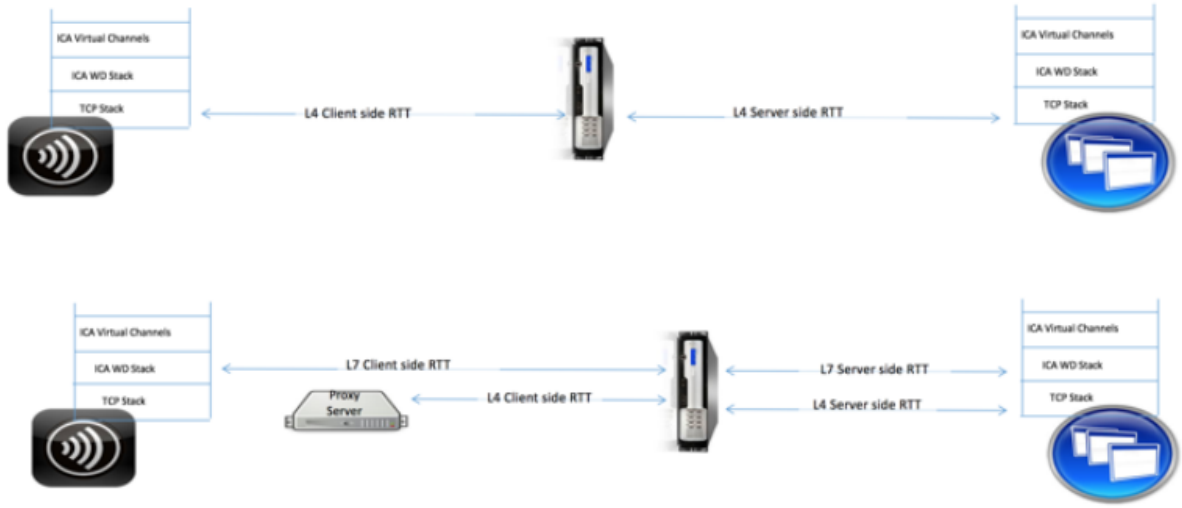


Fig 2. Deployment with TCP Proxies

ICA RTT と **L7** のレイテンシ計算の違い

ICA RTT は、Citrix Workspace アプリから仮想デスクトップエージェント（VDA）への往復時間の合計を表します。L7 レイテンシーは、クライアント側とサーバー側のレイテンシーに関する詳細な詳細を提供します。L7 クライアントのレイテンシーは、Citrix Workspace アプリから Citrix Gateway までのレイテンシーです。L7 サーバーのレイテンシーは、Citrix Gateway から VDA までのレイテンシーです。

> 注：サーバー側の L7 レイテンシーの計算は、Citrix Virtual Apps and Desktops バージョン 7.13 以降でのみサポートされています。

CLI を使用した **L7** 遅延しきい値の設定

1. ICA 遅延プロファイルを追加します。

```
add ica latencyprofile <name> [-l7LatencyMonitoring ( ENABLED |
    DISABLED )] [-l7LatencyThresholdFactor <positive_integer>] [-
    l7LatencyWaitTime <positive_integer>] [-l7LatencyNotifyInterval <
    positive_integer>] [-l7LatencyMaxNotifyCount <positive_integer>]
<!--NeedCopy-->
```

2. ICA アクションを追加します。

```
add ica action <name> [-latencyprofileName <string>]
<!--NeedCopy-->
```

3. ICA ポリシーを追加します。


```
add ica policy <name> -rule <expression> -action <string> [-comment<
    string>] [-logAction <string>
<!--NeedCopy-->
```

4. ICA ポリシーを VPN サーバーまたは ICA グローバルバインドポイントにバインドします。

```
bind ica global -policyName <string> -priority <positive_integer> [-
    gotoPriorityExpression <expression>] [-type ( ICA_REQ_OVERRIDE |
    ICA_REQ_DEFAULT )]
<!--NeedCopy-->
```

または

```
bind vpn vserver <name> -policy <string>  [-priority <positive_integer
    >]
<!--NeedCopy-->
```

または

```
bind cr vserver <name> -policy <string> [-priority <positive _integer>]
<!--NeedCopy-->
```

引数

- レイテンシーモニタリング: L7 しきい値モニタリングを有効または無効にするパラメータ。このパラメータを有効にすると、設定された条件が満たされると Insight Center に通知が送信されます。

  デフォルト値: DISABLED

- **LatencyThresholdFactor**: しきい値を超えたため、通知を Insight Center に送信する必要があると結論付けるために、アクティブレイテンシーが最小観測レイテンシーよりも大きくなければならないファクター。

  デフォルト値:4

  最小値:2

  最大値:65535

- **LatencyWaitTime**: 遅延しきい値を超えてから Insight Center に通知を送信するまでアプライアンスが待機する時間（秒単位）。

  デフォルト値:20

  最小値:1

  最大値:65535

- **LatencyNotifyInterval**: 待機時間が経過した後、アプライアンスが Insight Center に後続の通知を送信する間隔（秒単位）。

  デフォルト値:20

  最小値:1

  最大値:65535

- **LatencyMaxNotifyCount**: レイテンシーがしきい値を超える間隔内に Insight Center に送信できる通知の最大数。

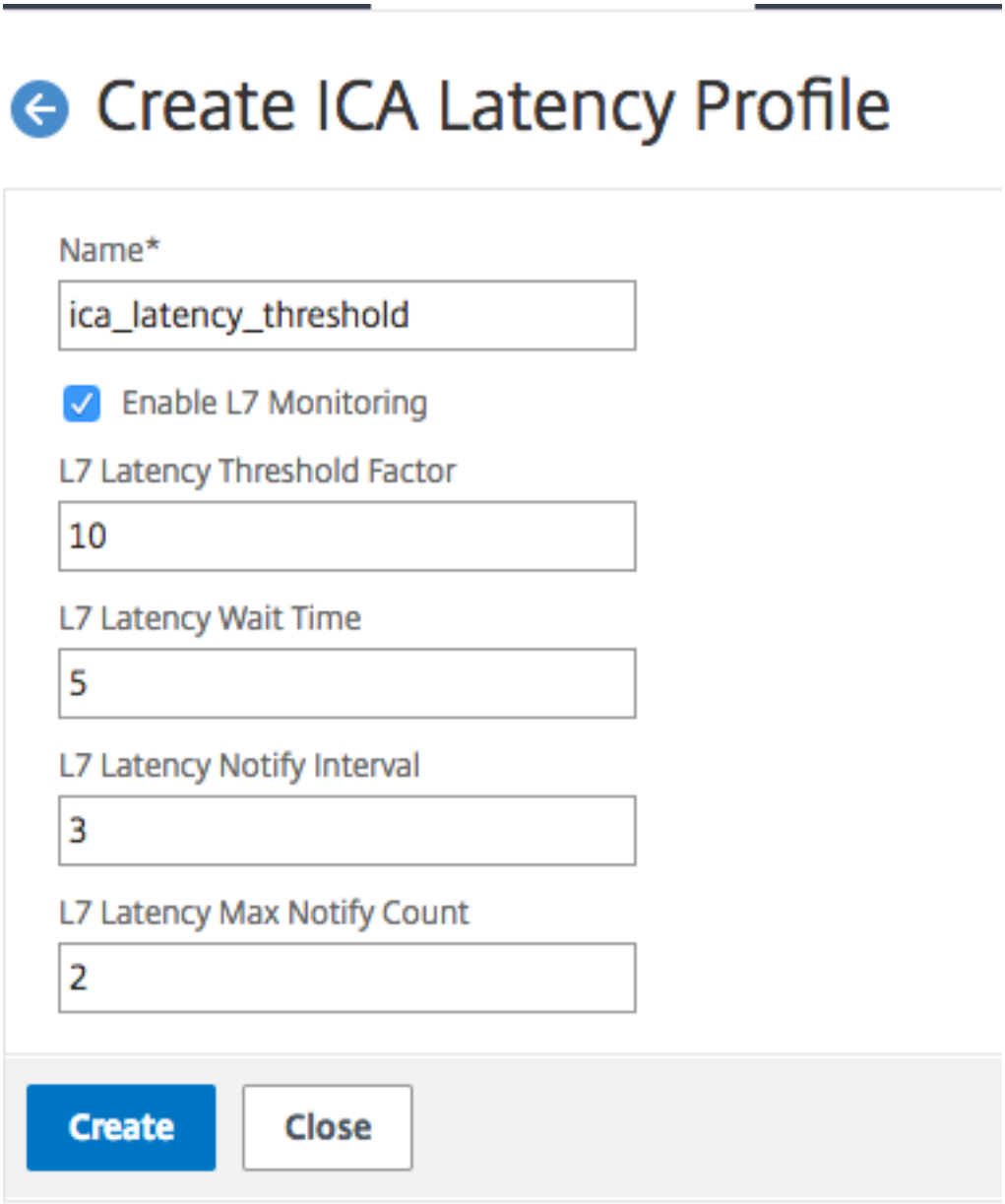
  デフォルト値: 5

GUI を使用した L7 遅延しきい値の設定

1. 「構成」>「**NetScaler Gateway** 」>「ポリシー」>「**ICA** 」に移動します。

2. 「**ICA** レイテンシープロファイル」タブを選択し、「追加」をクリックします。

3.**ICA** レイテンシプロファイルの作成ページで、次の操作を行います。



- [**L7** レイテンシモニタリング] を選択して、L7 しきい値モニタリングを有効にします。
- [**L7** しきい値係数**]** に、Insight Center に通知を送信するために、アクティブなレイテンシーが最小観測レイテンシーを超える値を入力します。
- [**L7** レイテンシー待機時間] に、しきい値を超えてから Insight Center に通知を送信するまでアプライアンスが待機する時間を秒単位で入力します。
- [**L7** 遅延通知間隔] に、待機時間が経過した後にアプライアンスが Insight Center に後続の通知を送信する時間を秒単位で入力します。
- [**L7** レイテンシーの最大通知数] に、レイテンシーがしきい値を超える間隔内に Insight Center に送信できる通知の最大数を入力します。

> 注：L7 レイテンシーの最大通知カウントは、しきい値を超えた時点で適用され、アクティブなレイテンシーがしきい値を下回るとリセットされます。これらの通知の周期性は、通知間隔によって制御されます。

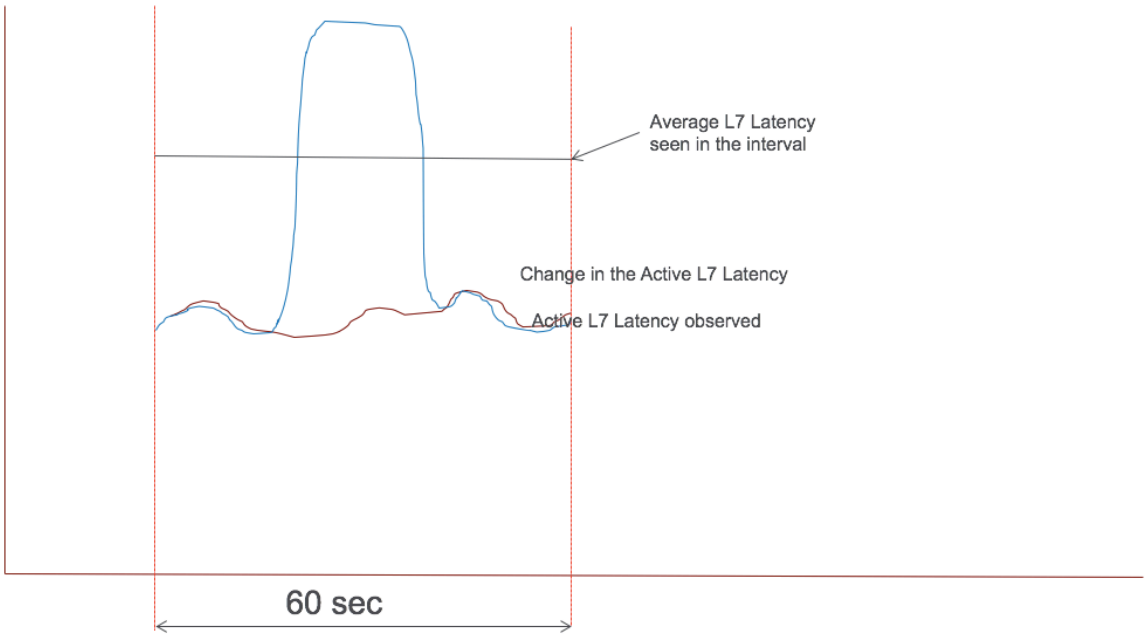
4.［作成］をクリックします。

L7 レイテンシー測定モデルと L7 レイテンシーしきい値レポートモデル

L7 レイテンシー測定モデル

L7 レイテンシー測定モジュールでは、平均クライアント側とサーバー側の L7 レイテンシー値が 60 秒ごとに Insight Center に送信されます。その結果、この間隔内で検出されたスパイクは平均化され、検出されないままになります。また、L7 レイテンシ測定モジュールにはライブレイテンシ監視機能はありません。

次の図は、L7 遅延測定モデルのサンプルを示しています。

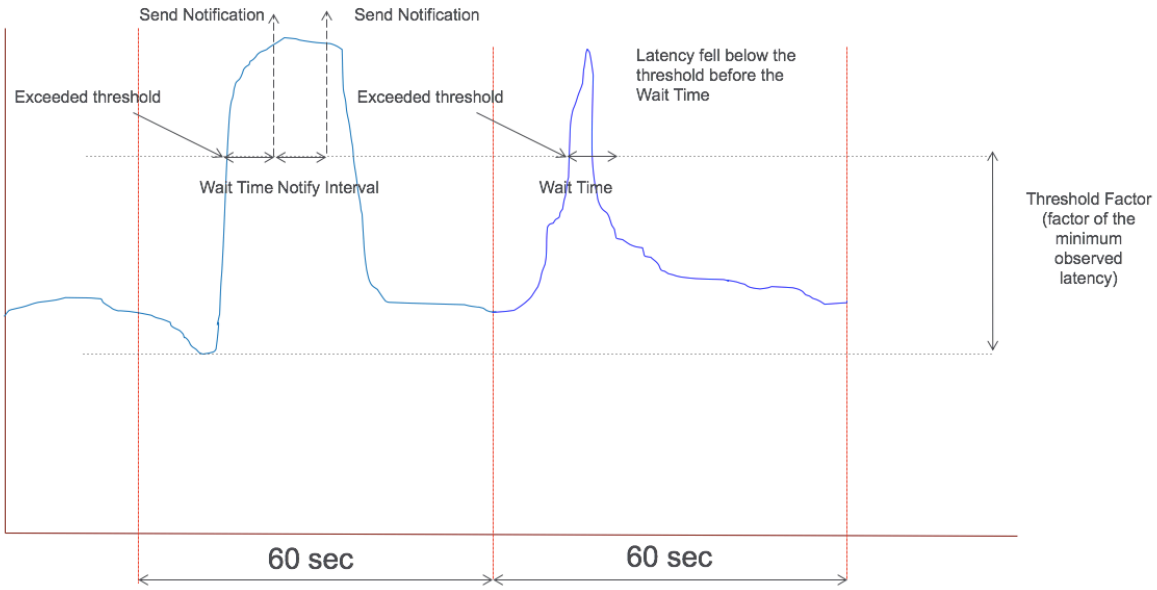


L7 遅延しきい値レポートモデル

L7 遅延しきい値レポートモデルには、スパイクを検出するライブレイテンシーモニタリング機能があります。レイテンシーが観測された最小レイテンシーを超えると、Insight Center に通知が送信されます。

しきい値を超えると、遅延の増加が検出されます。設定されたしきい値の待機時間が経過すると、Insight Center に通知が送信されます。待機時間が経過し、しきい値を超えた後、後続の通知が Insight Center に送信されます。
待機時間が期限切れになる前に待機時間がしきい値係数を下回る場合、通知は Insight Center に送信されません。

次の図は、L7 遅延しきい値レポートモデルのサンプルを示しています。



実行時に次のパラメータを設定できます。

- しきい値モニタリング（ON/OFF）
- しきい値要素
- しきい値の待機時間
- 通知間隔
- 最大通知数

Microsoft Intune 統合

October 22, 2021

Microsoft Intune と Citrix Gateway の統合により、Citrix Gateway と Intune が提供するクラス最高のアプリケーションアクセスとデータ保護ソリューションが提供されます。

E メール、カレンダー、連絡先、メモ作成、ドキュメント編集、リモートアクセスなど、最も包括的な安全性の高い生産性アプリケーションスイートを入手できます。これらはすべて、異なるプラットフォーム間で一元管理できます。Intune と Citrix Gateway の統合により、世界クラスのモバイルデバイス管理 (MDM) 機能が提供されます。一方、Citrix Gateway のクライアント側テクノロジにより、これらの Intune アプリケーションが Citrix Gateway を介して企業データとアプリケーションに安全にアクセスできるようになります。

この統合により、Citrix Gateway は Intune からコンプライアンスデータを取得し、条件付きアクセスポリシーを有効にすることができます。条件付きアクセスポリシーにより、Citrix Gateway では、デバイスの機能などに基づいてアクセスを制御できます。たとえば、管理者は、「カメラ」が無効になっているデバイスのみにアクセス権を付与するポリシーを作成できます。

Citrix Gateway 仮想サーバーが構成されると、Citrix Gateway は Azure の Active Directory ライブラリ（ADAL）トークン認証をサポートします。構成時に、Citrix ネットワーク専用ラッパーまたは SDK でラップされたモバイルアプリケーションは、AAD から直接取得できる ADAL トークンを使用して Citrix Gateway にアクセスします。

Microsoft Endpoint Manager と Citrix マイクロ VPN の統合

Citrix Gateway のお客様は、Microsoft エンドポイントマネージャー（Intune）でマイクロ VPN を使用できます。Citrix micro VPN と Microsoft Endpoint Management との統合により、アプリはオンプレミスのリソースにアクセスできます。

Citrix micro VPN テクノロジーは、VPN トンネルが常にアクティブであるとは限らないため、データ転送コストを削減し、セキュリティを簡素化するオンデマンド VPN を提供します。代わりに、必要なときにのみアクティブになり、リスクが軽減され、デバイスのパフォーマンスが最適化され、ユーザーエクスペリエンスが向上します。これにより、モバイルバッテリーの寿命も向上します。Citrix のマイクロ VPN テクノロジーにより、モバイルユーザーは社内リソースへの安全なアクセスを提供すると同時に、最高のユーザーエクスペリエンスを提供します。

Micro VPN は、次のユースケースでのみサポートされます。

- Intune モバイルアプリケーション管理 (MAM) のみ
- Intune モバイルデバイス管理 (MDM) とモバイルアプリケーション管理 (MAM)

> 重要：
>
> - Citrix Gateway のお客様は、2021 年 1 月まで追加料金なしで、Microsoft エンドポイントマネージャーでマイクロ VPN を使用する権利を有します。
> - マイクロ VPN を使用するには、SSL VPN 機能のために Citrix Gateway アドバンストエディションまたはプレミアムエディション（VPX 3000 以降）が必要です。

Microsoft エンドポイントマネージャーとの Citrix マイクロ VPN 統合の設定の詳細については、「Microsoft エンドポイントマネージャーでマイクロ VPN を使用するための Citrix Gateway のセットアップ」を参照してください。

統合 Intune MDM ソリューションを使用するタイミング

March 26, 2020

次のシナリオは、統合 Intune MDM ソリューションの使用を示しています。

- 新しいお客様が、オンプレミスの Citrix Gateway 導入で Intune をオンプレミスで導入することを決定
- 既存の Citrix Gateway ユーザーが Intune でモバイルデバイス管理を追加しようとしています
- 既存の Intune ユーザーが、会社の DMZ 内の Citrix Gateway の物理アプライアンスまたは仮想アプライアンスを使用して、社内ネットワーク内にあるデータに、モバイルデバイスやアプリケーションにアクセスできるようにしたいと考えています。

> 注
>
> iOS クライアントと Android クライアントのみがサポートされています。

Citrix Gateway と Intune MDM の統合について

March 26, 2020

一般的な Citrix Gateway と Intune MDM の統合におけるイベントのフローの例を次に示します。

1. Intune にモバイルデバイスを登録します。
2. 企業で承認されたアプリケーションとデバイスポリシーがデバイスにプッシュされます。
3. デバイスから SharePoint (オンプレミスアプリケーション) を参照します。
4. ブラウザーの要求は、Citrix Gateway されます。
5. Citrix Gateway アプライアンスは、Intune にデバイスの登録ステータスをチェックします。
6. 準拠したデバイスが正常に登録されると、SharePoint アクセスが許可されます。

デバイスによって条件付きアクセス (CA) ポリシーが満たされない場合、Citrix Gateway VPN クライアントは、Intune がホストするページへのリンクとともにエラーメッセージをユーザーに表示し、デバイスのコンプライアンス状態を登録または修復します。

注: 管理者は、ユーザーがデバイス上のさまざまな証明書を区別できるように、証明書を Intune にプッシュする際に次の点を確認する必要があります。

- 証明書にはサブジェクトの概要が必要です。
- 異なる証明書のサブジェクトの概要は、異なるものでなければなりません。

単一要素ログイン用の Citrix Gateway 仮想サーバーのネットワークアクセス制御デバイスチェックの構成

October 22, 2021

> 重要
>
> 以下のセクションでは、Citrix Gateway で Intune を構成するための手順を示します。Azure ポータルで Citrix Gateway アプリケーションを構成して クライアント **ID**、クライアントシークレット、テナント **ID** を取得する方法については、Azure 製品のドキュメントを参照してください。
>
> 以下の機能を使用するには、**Citrix ADC** アドバンスエディションのライセンスが必要です。

Gateway 展開用に **nFactor** を使用して **Citrix Gateway** 仮想サーバーを追加するには

1. ［Citrix Gateway］ツリーノードの下にある［仮想サーバー］に移動します。
2. ［追加］をクリックします。
3. **[** 基本設定**]** 領域に必要な情報を入力し、[**OK**] をクリックします。
4.「サーバー証明書」を選択します。
5. 必要なサーバー証明書を選択し、[バインド] をクリックします。
6. ［続行］をクリックします。
7. ［続行］をクリックします。
8. ［続行］をクリックします。
9. [**[**ポリシー**]**] の横のプラスアイコン **+** をクリックし、[ポリシーの選択**]** リストから **[**** セッション] を選択し、[タイプの選択**]** リストから **[**** 要求] を選択し、[続行] をクリックします。
10. [ポリシーの選択] の横のプラスアイコン **[**ポリシー**]** をクリックします。
11. **NetScaler Gateway** セッションポリシーの作成ページで、セッションポリシーの名前を入力します。
12. プロファイルの横にある [ポリシー] プラスアイコンをクリックし、**NetScaler Gateway** セッションプロファイルの作成ページでセッションプロファイルの名前を入力します。
13. [クライアントエクスペリエンス] タブで、[クライアントレスアクセス] の横にあるチェックボックスをオンにし、リストから [オフ] を選択します。
14. [プラグインの種類] の横にあるチェックボックスをクリックし、リストから [Windows/Mac OS X] を選択します。
15. ［詳細設定］をクリックし、［クライアント選択］の横にあるチェックボックスをオンにして、その値を［**ON** ］に設定します。
16. [セキュリティ] タブで、[既定の承認操作] の横にあるチェックボックスをオンにし、一覧から **[**許可] を選択します。
17. [公開アプリケーション] タブで、[**ICA** プロキシ] の横にあるチェックボックスをクリックし、リストから [**OFF**] を選択します。
18. ［作成］をクリックします。
19. **NetScaler Gateway** セッションポリシーの作成ページの「式」領域に **NS_TRUE** と入力します。
20. ［作成］をクリックします。
21. ［バインド］をクリックします。
22. [詳細設定**]** で [認証プロファイル] を選択します。
23. プラスアイコン **[**ポリシー**]** をクリックし、認証プロファイルの名前を入力します。

24. プラスアイコン **[**ポリシー**]** をクリックして、認証仮想サーバを作成します。
25. [基本設定**]** 領域で認証仮想サーバーの名前と IP アドレスの種類を指定し、[**OK**] をクリックします。IP アドレスの種類は、アドレス指定不可能なものでもかまいません。
26. [認証ポリシー] をクリックします。
27. 「ポリシーバインディング」ビューで、プラスアイコン **[**ポリシー**]** をクリックして認証ポリシーを作成します。
28. アクションタイプとして **OAUTH** を選択し、プラスアイコン **[**ポリシー**]** をクリックして NAC の OAuth アクションを作成します。
29. クライアント **ID**、**** クライアントシークレット、テナント **ID**** を使用して OAuth アクションを作成します。

    クライアント **ID**、クライアントシークレット、テナント **ID** は、Azure ポータルで Citrix Gateway アプリケーションを構成した後に生成されます。

    https://login.microsoftonline.com/、https://graph.windows.net/、および *.manage.microsoft.com を解決してアクセスできるように、アプライアンス上に適切な DNS ネームサーバーが設定されていることを確認します。
30. **OAuth** アクションの認証ポリシーを作成します。

規則: http.req.header(“User-Agent”).contains(“NAC/1.0”)&& ((http.req.header(“User-Agent”).contains(“iOS”) && http.req.header(“User-Agent”).contains(“NSGiOSplugi	(http.req.header(“User-Agent”).contains(“Android”) && http.req.header(“User-Agent”).contains(“CitrixVPN”)))

31. プラスアイコン **[**ポリシー**]** をクリックして、nextFactor ポリシーラベルを作成します。
32. プラスアイコン **[**ポリシー**]** をクリックして、ログインスキーマを作成します。
33. 認証 スキーマとして「**noschema** 」を選択し、「作成」をクリックします。
34. 作成したログインスキーマを選択したら、[**Continue**] をクリックします。
35. 「ポリシーの選択」で、ユーザー・ログイン用の既存の認証ポリシーを選択するか、プラスアイコン「**+**」をクリックして認証ポリシーを作成します。
    認証ポリシーの作成の詳細については、高度な認証ポリシーの構成を参照してください。
36. ［バインド］をクリックします。
37. ［完了］をクリックします。
38. ［バインド］をクリックします。
39. ［続行］をクリックします。

40. ［完了］をクリックします。

41. ［作成］をクリックします。

42. ［**OK**］をクリックします。

43. ［完了］をクリックします。

/cgi/login 要求の一部としてデバイス **ID** を送信する **VPN** プラグインを示すために、認証ログインスキーマを認証仮想サーバーにバインドするには

1. [セキュリティ] > [**AAA-**アプリケーショントラフィック] > [仮想サーバ] に移動します。
2. 以前に選択した仮想サーバを選択し、[**Edit**] をクリックします。
3. [詳細設定] の [ログインスキーマ] をクリックします。
4. [ログインスキーマ] をクリックしてバインドします。
5. [**[>]**] をクリックして、NAC デバイスチェック用の既存のビルドインログインスキーマポリシーを選択し、バインドします。
6. 認証デプロイメントに適した必要なログインスキーマポリシーを選択し、[**Select**] をクリックします。

   上記の展開では、単一要素認証（LDAP）と NAC OAuth アクションポリシーが使用されるため、**lschema_single_factor_deviceid** が選択されています。
7. ［バインド］をクリックします。
8. ［完了］をクリックします。

Azure ADAL トークン認証について

March 26, 2020

一般的な Citrix Gateway の Microsoft ADAL トークン認証におけるイベントの流れを以下に示します。

1. iOS または Android でアプリを起動すると、アプリは Azure にアクセスします。ユーザーは、ユーザーの資格情報を使用してログオンするように求められます。ログオンに成功すると、アプリは ADAL トークンを取得します。

2. この ADAL トークンは、ADAL トークンを検証するように構成された Citrix Gateway に提示されます。

3. Citrix Gateway は、ADAL トークンの署名を Microsoft の対応する証明書で検証します。

4. 検証に成功すると、Citrix Gateway はユーザーのプリンシパル名（UPN）を抽出し、アプリケーション VPN に内部リソースへのアクセスを許可します。

Microsoft ADAL トークン認証用の Citrix Gateway 仮想サーバーの構成

March 26, 2020

Microsoft ADAL トークン認証を監視するように Citrix Gateway 仮想サーバーを構成するには、次の情報が必要です。

- certEndpoint: ADAL トークン検証用の Json Web キー (JWK) を含むエンドポイントの URL。
- 対象ユーザー：アプリケーションが ADAL トークンを送信する Citrix ADC 仮想サーバーの FQDN です。
- 発行者:AAD 発行者の名前。デフォルトで入力されます。
- テナント ID: Azure ADAL 登録のテナント ID。
- ClientID: ADAL 登録の一環として Gateway アプリに付与される一意の ID です。
- ClientSecret: ADAL 登録の一環として Gateway アプリに与えられるシークレットキー。

1. OAuth アクションを作成します。

   add authentication OAuthAction <oauth_action_name>
   -OAuthType INTUNE –clientid <client_id> -
   clientsecret <client_secret>
   -audience <audience>
   -tenantid <tenantID>
   -issuer <issuer_name> -
   userNameField upn-certEndpoint <certEndpoint_name>

   例:

   add authentication OAuthAction tmp_action -OAuthType INTUNE -clientid id 1204 -clientsecret a -audience “
   http://hello” -tenantid xxxx -issuer “
   https://hello” -userNameField upn -certEndpoint
   https://login.microsoftonline.com/common/discovery/v2.0/keys

2. 新しく作成された OAuth に関連付ける認証ポリシーを作成します。

   add
   authentication Policy <policy_name>
   -rule true -action <oauth intune action>

   例:

   add authentication Policy oauth_intune_pol -rule true -action tmp_action

3. 新しく作成した OAuth を AuthVS にバインドします。

   bind authentication vserver <auth_vserver>
   -policy <oauth_intune_policy>
   -priority 2 -gotoPriorityExpression END

例:

bind authentication vserver auth_vs_for_gw1_intune -policy oauth_pol -priority 2 -gotoPriorityExpression END

4. ログインスキーマを作成します。

   add authentication loginSchema <loginSchemaName>
   -authenticationSchema <authenticationSchema”location”>

   add authentication loginSchemaPolicy <loginSchemaPolicyName>
   -rule true -action <loginSchemaName>

   例:

   add authentication loginSchema oauth_loginschema -authenticationSchema “/nsconfig/login-schema/LoginSchema/OnlyOAuthToken.xml”

   add authentication loginSchemaPolicy oauth_loginschema_pol -rule true -action oauth_loginschema

5. ログインスキーマで認証 VS をバインド:

   bind authentication vserver <auth_vs> **-policy** <oauth _pol> **-priority 2 -gotoPriorityExpression END**

   例:

   bind authentication vserver auth_vs_for_gw1_intune -policy oauth_loginschema_pol -priority 2 -gotoPriorityExpression END

6. authnprofile を追加し、VPN 仮想サーバーに割り当てます。

   add authnprofile <nfactor_profile_name>**-authnvsName** <authvserver>

   set vpn vserver <vserverName>**-authnprofile** <nfactor_profile_name>

   例:

   add authnprofile nfactor_prof_intune -authnvsName auth_vs_for_gw1_intune

   set vpn vserver gw1_intune-authnprofile nfactor_prof_intune

Microsoft エンドポイントマネージャーでマイクロ VPN を使用するための Citrix Gateway のセットアップ

April 9, 2020

Citrix micro VPN と Microsoft Endpoint Management との統合により、アプリはオンプレミスのリソースにアクセスできます。詳しくは、「マイクロソフトのエンドポイントマネージャーと Citrix マイクロ VPN の統合」を参照してください。

システム要件

- Citrix Gateway バージョン 12.0.59.x または 12.1.50.x 以降。

  Citrix Gateway の最新バージョンは、Citrix Gateway ダウンロードページからダウンロードすることもできます。

- Windows 7 以降を実行している Windows デスクトップ（Android アプリのラッピングにのみ対応）
- Microsoft
  - Azure AD アクセス（テナントの管理者特権あり）
  - Intune 対応のテナント
- ファイアウォールのルール
  - ファイアウォールのルールを有効にして、Citrix Gateway のサブネット IP から`*.manage.microsoft.com`、`https://login.microsoftonline.com`、`https://graph.windows.net`（ポート 443）に対する SSL のトラフィックを許可します。
  - Citrix Gateway は、前述の URL を外部から解決できる必要があります。

前提条件

- **Intune** 環境**:** Intune 環境がない場合は、セットアップします。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。
- エッジブラウザアプリ**:** マイクロ VPN SDK は、Microsoft Edge アプリと iOS および Android 用の Intune Managed Browser アプリに統合されています。Managed Browser について詳しくは、Microsoft のManaged Browser のページを参照してください。

Azure の **Active Directory (AAD)** アプリケーションのアクセス許可を付与する

1. Citrix マルチテナント AAD アプリケーションに同意し、Citrix Gateway が AAD ドメインで認証できるようにします。Azure グローバル管理者は、次の URL にアクセスして同意する必要があります。

   「https://login.windows.net/common/adminconsent?client_id=b6a53a76-5d50-499e-beb3-c8dbdad5c40b&redirect_uri=https://www.citrix.com&state=consent」を参照してください。

2. Citrix マルチテナント AAD アプリケーションに同意し、モバイルアプリケーションが Citrix Gateway のマイクロ VPN で認証できるようにします。このリンクは、Azure グローバル管理者が [ユーザーがアプリケーションを登録できる] の既定値を [はい] から [いいえ] に変更した場合にのみ必要です。
   この設定は、Azure ポータルの [**Active Directory] > [**ユーザー**] > [**ユーザー設定**]** の下にあります。
   Azure グローバル管理者は、次の URL にアクセスして同意する必要があります (テナント ID を追加)https://login.microsoftonline.com/%5Btenant_id%5D/adminconsent?client_id=9215b80e-186b43a1-8aed-9902264a5af7。

マイクロ **VPN** 用の **Citrix Gateway** の構成

Intune で Micro VPN を使用するには、Citrix Gateway で Azure Active Directory が認証されるように設定する必要があります。このユースケースでは、既存の Citrix Gateway 仮想サーバーは利用できません。
まず、Azure AD がオンプレミスの Active Directory と同期するように設定します。この手順は、Intune と Citrix Gateway との間の認証を適切に行うために必要です。

ダウンロードスクリプト**:** .zip ファイルには、スクリプトを実装するための指示を含む readme が含まれています。スクリプトに必要な情報を手動で入力し、Citrix Gateway でスクリプトを実行してサービスを構成する必要があります。スクリプトファイルは、シトリックスのダウンロードページからダウンロードできます。

> 重要: Citrix Gateway の構成を完了した後、「完了」以外の OAuth ステータスが表示された場合は、「トラブルシューティング」セクションを参照してください。

マイクロソフトのエッジブラウザーの構成

1. https://portal.azure.com/にサインインし、[**Intune**] **>** ［モバイルアプリ］の順に移動します。
2. 通常どおりに Edge App を公開し、アプリ構成ポリシーを追加します。
3. ［管理］の ［アプリ構成ポリシー］をクリックします。
4. ［追加］をクリックし、作成するポリシーの名前を入力します。[デバイスの登録の種類] で、[管理対象アプリ] を選択します。
5. [関連付けられたアプリ**]** をクリックします。
6. ポリシーを適用するアプリ (Microsoft Edge または Intune 管理対象ブラウザー) を選択し、[**OK**] をクリックします。
7. ［構成設定］をクリックします。
8. [**Name**] フィールドに、次の表に示すいずれかのポリシーの名前を入力します。
9. ［値］フィールドに、対象のポリシーに適用する値を入力します。フィールドの外をクリックすると、ポリシーがリストに追加されます。ポリシーは複数追加できます。
10. [**OK**］をクリックしてから ［追加］をクリックします。

ポリシーのリストにポリシーが追加されます。

名前（iOS または Android）	値	説明
MvpnGatewayAddress	`https://external.companyname.com`	Citrix Gateway の外部 URL
MvpnNetworkAccess	MvpnNetworkAccessTunneledWebSSO Unrestricted	MvpnNetworkAccessTunneledWebSSO は、トンネリングのデフォルトです。
MvpnExcludeDomains	除外するドメイン名のコンマ区切りリスト	オプションです。Default=blank

> 注**:** Web SSO は、設定の「Secure Browse」の名前です。動作は同じです。

- **Mvpn** ネットワークアクセス -Mvpn ネットワークアクセストンネル WebSSO は、Citrix Gateway を介した HTTP/HTTPS リダイレクトを有効にします。これは、トンネリングされた Web SSO とも呼ばれます。Gateway は HTTP 認証チャレンジにインラインで応答し、シングルサインオン (SSO) エクスペリエンスを提供します。Web SSO を使用するには、このポリシーを **Mvpn** ネットワークアクセストンネル **WebSSO** に設定します。フルトンネルリダイレクションは現在サポートされていません。マイクロ VPN トンネリングをオフにしておくには、[**Unlimited**] を使用します。
- **MvpnExcludeDomains** -Citrix Gateway リバース Web プロキシ経由のルーティングから除外されるホストまたはドメイン名のコンマ区切りリスト。Citrix Gateway で構成されたスプリット DNS 設定によってドメインまたはホストが選択される場合がありますが、ホスト名またはドメイン名は除外されます。

  > 注**:** このポリシーは、**MvpnNetworkAccessTunnedWebSSO** 接続に対してのみ適用されます。MvpnNetworkAccess が **[**制限なし**]** の場合、このポリシーは無視されます。

トラブルシューティング

一般的な問題

問題	解像度
アプリを開くと、「ポリシーの追加が必要です」というメッセージが表示されます。	Microsoft Graph API でポリシーを追加する
ポリシーの競合があります	1 つのアプリにつき 1 つのポリシーのみ許可されます。
アプリをラップすると、「アプリをパッケージ化できませんでした」というメッセージが表示されます。完全なメッセージについては、以下を参照してください。	アプリは Intune SDK と統合されています。Intune でアプリをラップする必要はありません。
アプリが内部リソースに接続できない	正しいファイアウォールポートが開いていること、テナント ID が正しいことを確認します。

アプリのエラーメッセージをパッケージ化できませんでした**:**

Failed to package app. com.microsoft.intune.mam.apppackager.utils.AppPackagerException: This app already has the MAM
SDK integrated.
com.microsoft.intune.mam.apppackager.AppPackager.packageApp(AppPackager.java:113)
com.microsoft.intune.mam.apppackager.PackagerMain.mainInternal(PackagerMain.java:198)
com.microsoft.intune.mam.apppackager.PackagerMain.main(PackagerMain.java:56)
The application cannot be wrapped.

Citrix Gateway の問題

問題	解像度
Azure の Gateway アプリ用に構成するために必要なアクセス許可は使用できません。	適切な Intune ライセンスが利用可能かどうかを確認します。管理. ウィンドウサズ ure.comポータルを利用して、権限を追加できるかどうかを試してください。問題が解決しない場合は、Microsoft のサポートにお問い合わせください。
Citrix Gateway はlogin.microsoftonline.comandgraph.windows.netにアクセスできません。	NS シェルから、次の Microsoft Web サイトにアクセスできるかどうかを確認します。curl-v-khttps://login.microsoftonline.com。次に、Citrix Gateway で DNS が構成されているかどうかを確認します。また、ファイアウォール設定が正しいことを確認します（DNS 要求がファイアウォールされている場合）。
OAuthAction を設定すると、ns.log にエラーが記録される。	Intune のライセンスが有効であること、および Azure Gateway アプリに適切な権限のセットが設定されているかを確認します。
Sh OAuthAction コマンドで OAuth のステータスが完了と表示されない。	DNS 設定と Azure Gateway アプリに設定されている権限を確認します。
Android または iOS デバイスで 2 要素認証のプロンプトが表示されない。	2 要素デバイス ID ログオンスキーマが認証仮想サーバーにバインドされているかを確認します。

Citrix Gateway の **OAuth** ステータスとエラー状態

ステータス	エラー状態
AADFORGRAPH	シークレットが無効、URL が未解決、接続タイムアウト
MDMINFO	*manage.microsoft.comがダウンしているか、到達不能です。
GRAPH	グラフエンドポイントがダウンしており到達不能
CERTFETCH	DNS エラーのためトークンエンドポイント：https://login.microsoftonline.comと通信できない。この構成を検証するには、shell に移動し、curl https://login.microsoftonline.comと入力します。このコマンドは検証が必要です。

注**:** OAuth ステータスが成功すると、ステータスは COMPLETE と表示されます。

UDP トラフィックに対するサービスサポートのタイプ

March 26, 2020

UDP のタイプオブサービス（ToS）のサポートにより、送信者が UDP パケットに対して ToS 値が構成されると、Citrix Gateway はそのパケットが宛先に到達するまで値を保持します。設定された値と宛先ネットワークの設定に基づいて、宛先ネットワークは UDP パケットを優先順位付けされた発信キューに配置します。

> 注：ToS 情報
> を使用すると、各 IP パケットに優先順位を割り当て、高スループット、高信頼性、低遅延などの特定の処理を要求できます。

Citrix Gateway でのアウトバウンドプロキシのプロキシ自動構成サポート

March 26, 2020

プロキシ自動構成（PAC）をサポートするように Citrix Gateway アプライアンスを構成すると、PAC ファイルの URL がクライアントブラウザーにプッシュされます。クライアントからのトラフィックは、PAC ファイルで定義された条件に従ってそれぞれのプロキシにリダイレクトされます。

次に、アウトバウンドプロキシの PAC の一般的な使用例を示します。

- クライアントトラフィックを処理する複数のプロキシサーバーを構成する。
- サブネット間でプロキシトラフィックをロードバランシングする。

コマンドラインインターフェイスを使用して、送信プロキシの PAC をサポートするように Citrix Gateway グローバルパラメータを構成するには、次の操作を行います。

コマンドプロンプトで、次のように入力します。

```
1 ```
2 set vpn parameter -proxy BROWSER -autoProxyUrl <URL>
3 <!--NeedCopy--> ```
```

セッションプロファイルで PAC をサポートするように Citrix Gateway を構成するには

コマンドプロンプトで、次のように入力します。

```
1 ```
2 add vpn sessionAction <name> -proxy BROWSER -autoProxyUrl <URL>
3 <!--NeedCopy--> ```
```


値

- URL — プロキシサーバーの URL
- 名前：VPN セッションアクションの名前

Citrix ADC GUI を使用して、送信プロキシの PAC をサポートするように Citrix Gateway グローバルパラメータを構成するには、次の操作を行います。

1. [** 構成] ** > **Citrix Gateway** > [** グローバル設定] ** に移動します。
2. [グローバル設定**]** ページで、[グローバル設定の変更] をクリックし、[クライアントエクスペリエンス**]** タブを選択します。
3. [クライアントエクスペリエンス] タブで、[詳細設定**]** を選択し、[プロキシ**]** タブを選択します。
4. [プロキシ**]** タブで、**[**ブラウザ] を選択し、[自動構成を使用] を選択します。
5. [自動プロキシ設定ファイルへの **URL]** フィールドに、必要な PAC ファイルの URL を入力します。
6. [作成] をクリックします。

Citrix ADC GUI を使用して、セッションプロファイルの PAC をサポートするように Citrix Gateway を構成するには

1. [設定] **>** [**Citrix Gateway**] > [ポリシー] > [** セッション **] に移動します。
2. Citrix Gateway セッションポリシーとプロファイルページで、Citrix Gateway セッションプロファイルを作成します。

Citrix Gateway セッションプロファイルを作成するには、[セッションプロファイル] タブを選択し、[追加] をクリックして名前を入力します。

1. [クライアントエクスペリエンス] タブで、[詳細設定**]** を選択し、[プロキシ] タブを選択します。
2. [プロキシ] タブで、[ブラウザ] を選択し、[自動構成を使用] を選択します。
3. [自動プロキシ設定ファイルへの **URL]** フィールドに、必要な PAC ファイルの URL を入力します。
4. [作成] をクリックします。

アウトバウンド **ICA** プロキシのサポート

March 26, 2020

Citrix Gateway のアウトバウンド ICA プロキシのサポートにより、ネットワーク管理者は Receiver と Citrix Gateway が異なる組織に展開されている場合でも、SmartControl 機能を利用できます。

次のシナリオは、アウトバウンド ICA プロキシソリューションの使用を示しています。

Receiver と Citrix Gateway を異なる組織に展開する場合は、ネットワーク管理者が ICA セッション関連の機能を制御する必要があります。

アウトバウンド **ICA** プロキシのサポートについて：

企業組織に SmartControl 機能をもたらすために, 会社 A, これは、Receiver を持っています, 私たちは、LAN プロキシとして機能する Citrix ADC アプライアンスを追加する必要があります. Citrix ADC LAN プロキシは SmartControl を強制し、B 社の Citrix Gateway にトラフィックをプロキシします。この展開シナリオでは、Receiver は Citrix ADC LAN プロキシにトラフィックを転送します。これにより、A 社のネットワーク管理者が SmartControl を強制することができます。展開を次の図に示します。

このシナリオでは、LAN プロキシと Citrix Gateway 間のトラフィックは SSL 経由です。

> 注:
> クライアント証明書ベースの認証は、Citrix Gateway で有効にしないでください。

アウトバウンド **ICA** プロキシの構成

March 26, 2020

CLI を使用してアウトバウンド ICA プロキシを構成するには、次の手順に従います。

1. キャッシュリダイレクト Vserver を追加します。

   add cr vserver <name> <serviceType> <IPAddress> <port> -**cacheType** <cacheType>

   サービスは HDX である必要があります

   キャッシュタイプはフォワードでなければなりません

   例:

   add cr vserver CR_LAN_Proxy HDX 10.217.208.197 8080 -cacheType FORWARD

2. ICA スマートコントロールプロファイルを追加します。

   add ica accessprofile <name> -**ConnectClientLPTPorts** (DEFAULT | DISABLED) **ClientAudioRedirection** (DEFAULT | DISABLED) -**LocalRemoteDataSharing** (DEFAULT | DISABLED) -**ClientClipboardRedirection** (DEFAULT | DISABLED) -**ClientCOMPortRedirection** (DEFAULT |DISABLED) -**ClientDriveRedirection** (DEFAULT | DISABLED) -**ClientPrinterRedirection** (DEFAULT |DISABLED) -**Multistream** (DEFAULT | DISABLED) -**ClientUSBDriveRedirection** (DEFAULT | DISABLED)

   例:

   ```
   add ica accessprofile disableCDM -ConnectClientLPTPorts DEFAULT -
       ClientAudioRedirection DEFAULT  - LocalRemoteDataSharing DEFAULT
        -ClientClipboardRedirection DEFAULT -ClientCOMPortRedirection
       DEFAULT  - ClientPrinterRedirection DEFAULT -Multistream DEFAULT
        -ClientUSBDriveRedirection DEFAULT
   ```


3. ICA アクションを追加する:

   add ica action <name> **-accessProfileName** <string>

   例:

```
add ica action disableCDM\_action -accessProfileName disableCDM
```

4. ICA ポリシーを追加します。

   add ica policy <name> **-rule** <expression> **-action** <string> **-comment** <string> **-logAction** <string>

5. ICA ポリシーを仮想サーバーまたはグローバルにバインドします。

   a. 仮想サーバーにバインド

```
**bind cr vserver** \<name\> **-policyName** \<string\> **-
   priority** \<positive\_integer\>
```

   例:

```
bind cr vserver CR\_LAN\_Proxy  - policyname disableCDM\_pol  -
   priority 10
```

   b. グローバルにバインド

```
**bind ica global -policyName** \<string\> -**priority** \<
   positive\_integer\>
```

   例:

```
bind ica global  - policyName disableCDM\_pol  - priority 10
```

> 注
>
> [Secure ICA ポート] の設定: この値は、LAN プロキシがアウトバウンド接続を行う Citrix Gateway のポート番号です。デフォルトでは 443 に設定されています。ポートを変更するには、次のコマンドを使用します。
>
> **set ns param -secureicaPorts**<port>
>
> 例:
>
> set ns param -secureicaPorts 8443

Citrix Gateway と Citrix Virtual Apps and Desktops の統合

March 26, 2020

公開リソースおよびデータへのアクセスを管理するには、StoreFront サーバーを展開および構成します。リモートアクセスの場合は、Citrix Gateway を StoreFront の前に追加することをお勧めします。

> 注:
> Citrix Virtual Apps and Desktops を Citrix Gateway と統合する構成手順については、StoreFront のドキュメントを参照してください。

次の図は、Citrix Gateway を含む Citrix の簡易展開の例を示しています。Citrix Gateway は StoreFront と通信して、Citrix Virtual Apps and Desktops が配信するアプリやデータを保護します。ユーザーデバイスは Citrix Workspace アプリを実行してセキュリティで保護された接続を構築し、アプリ、デスクトップ、ファイルにアクセスします。

認証のネイティブ **OTP** サポート

March 26, 2020

Citrix Gateway では、サードパーティのサーバーを使用せずに、ワンタイムパスワード（OTP）をサポートしています。ワンタイムパスワードは、生成される番号またはパスコードがランダムであるため、セキュリティで保護されたサーバに対して認証を行うための非常に安全なオプションです。以前は、ランダムな数字を生成する特定のデバイスを備えた RSA などの専門企業によって OTP が提供されていました。このシステムは、サーバーが期待する数値を生成するために、クライアントと常に通信する必要があります。

この機能は、設備コストと運用コストの削減に加えて、Citrix ADC アプライアンスの構成全体を維持することで、管理者の管理を強化します。

> 注
>
> サードパーティ製サーバーが不要になったため、Citrix ADC 管理者は、ユーザーデバイスを管理および検証するためのインターフェイスを構成する必要があります。

ユーザーが OTP ソリューションを使用するには、Citrix Gateway 仮想サーバーに登録されている必要があります。登録は、一意のデバイスごとに 1 回だけ必要で、特定の環境に制限できます。登録ユーザーの設定と検証は、追加の認証ポリシーの設定に似ています。

ネイティブ **OTP** サポートの利点

- Active Directory に加えて認証サーバに追加のインフラストラクチャを使用する必要がなくなるため、運用コストが削減されます。
- 構成を Citrix ADC アプライアンスにのみ統合し、管理者に優れた制御を提供します。
- クライアントが期待する数値を生成するために、追加の認証サーバーへのクライアントの依存を排除します。

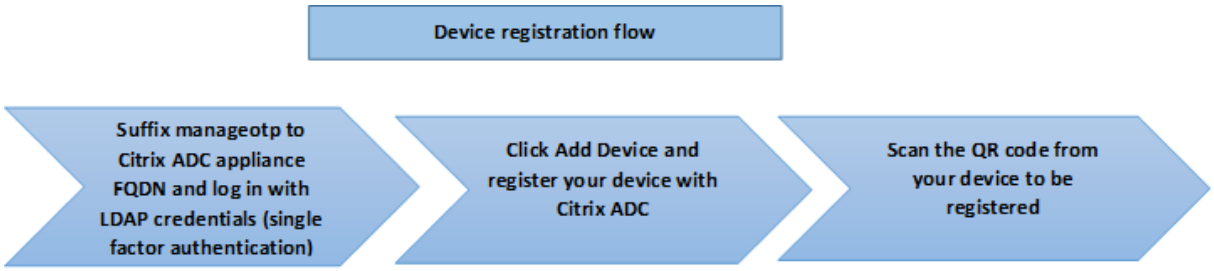
ネイティブ **OTP** ワークフロー

ネイティブ OTP ソリューションは 2 つ折りプロセスであり、ワークフローは次のように分類されます。

- デバイス登録
- エンドユーザーログイン

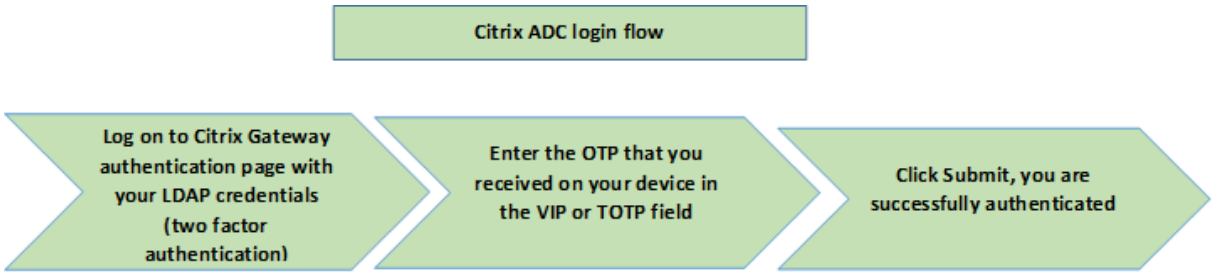
> 重要
>
> サードパーティ製のソリューションを使用している場合や、Citrix ADC アプライアンス以外のデバイスを管理している場合は、登録プロセスをスキップできます。追加する最後の文字列は、Citrix ADC で指定された形式である必要があります。

次の図は、OTP を受信する新しいデバイスを登録するためのデバイス登録フローを示しています。



> 注
>
> デバイスの登録は、任意の数の要因を使用して行うことができます。デバイス登録プロセスを説明する例として、1 つのファクタ（前の図を参照）を使用します。

次の図は、登録されたデバイスを介した OTP の検証を示しています。



前提条件

ネイティブ OTP 機能を使用するには、次の前提条件が満たされていることを確認します。

- Citrix ADC 機能のリリースバージョンは 12.0 ビルド 51.24 以降です。
- 高度なエディションまたはプレミアムエディションのライセンスが Citrix Gateway にインストールされている。
- Citrix Gateway には管理 IP が設定されており、管理コンソールにはブラウザーとコマンドラインの両方を使用してアクセスできます。

- Citrix ADC は、ユーザーを認証するための認証、承認、監査仮想サーバーで構成されています。
- Citrix ADC アプライアンスは Unified Gateway で構成され、認証、承認、監査プロファイルが Gateway 仮想サーバーに割り当てられます。
- ネイティブ OTP ソリューションは、nFactor 認証フローに制限されています。ソリューションを構成するには、高度なポリシーが必要です。詳細については、記事CTX222713を参照してください。

また、Active Directory については、次の点を確認してください。

- 256 文字の属性の最小長。
- 属性タイプは、ユーザーパラメータなどの ‘ディレクトリ文字列’ である必要があります。これらの属性は文字列値を保持できます。
- デバイス名が英語以外の文字である場合、属性文字列タイプは Unicode である必要があります。
- Citrix ADC LDAP 管理者は、選択した AD 属性への書き込みアクセス権を持っている必要があります。
- Citrix ADC アプライアンスとクライアントマシンは、共通のネットワークタイムサーバーに同期する必要があります。

GUI を使用したネイティブ OTP の設定

ネイティブ OTP 登録は、単要素認証ではありません。次のセクションでは、シングルファクタ認証と 2 番目のファクタ認証の設定について説明します。

最初の要素のログインスキーマの作成

1. [セキュリティ **AAA] > [**アプリケーショントラフィック**] > [**ログインスキーマ] に移動します。
2. [プロファイル] に移動し、[追加] をクリックします。
3.「認証ログイン・スキーマの作成」ページで、「名前」フィールドに **lschema_first_factor** と入力し、「**noschema** 」の横にある 「編集」をクリックします。
4. [**LoginSchema**] フォルダをクリックします。
5. 下にスクロールして **SingleAuth.xml** を選択し、[選択] をクリックします。
6. [作成] をクリックします。
7. [ポリシー] をクリックし、[追加] をクリックします。
8. [認証ログインスキーマポリシーの作成] 画面で、次の値を入力します。

   名前**:** lschema_first_factor
   プロファイル**:** リストから lschema_first_factor を選択します。
   ルール**:** HTTP. 要求. クッキー. 値 (「NSC_TASS」) .EQ (「管理」)

認証、承認、監査仮想サーバーの構成

1. [セキュリティ**] > [AAA] > [**アプリケーショントラフィック**] > [**認証仮想サーバ] に移動します。既存の仮想サーバーを編集する場合にクリックします。
2. 右側のペインの [詳細設定**]** の [ログインスキーマ] の横にある [**+**] アイコンをクリックします。
3. 「ログインスキーマなし」を選択します。
4. 矢印をクリックして、**lschema_first_factor** ポリシーを選択します。
5. **lschema_first_factor** ポリシーを選択し、[選択] をクリックします。
6. [バインド] をクリックします。
7. 上にスクロールし、[高度な認証ポリシー**]** の下の **[**認証ポリシー**]** を **1** つ選択します。
8. **nFactor** ポリシーを右クリックし、[バインディングの編集**]** を選択します。
9. [次の係数の選択**]** の下にある **[**+**] アイコンをクリックし、** [次の係数] を作成して [バインド] をクリックします。
10. 「認証ポリシーラベルの作成」画面で次のように入力し、「続行」をクリックします。

    名前: OTP 管理ファクター

    ログインスキーマ: Lschema_Int
11. 「認証ポリシーラベル」画面で、「**+** 」アイコンをクリックしてポリシーを作成します。
12. [認証ポリシーの作成] 画面で、次のように入力します。

    名前. otp_manage_ldap
13. [アクションタイプ] リストを使用して、アクションタイプを選択します。
14. 「アクション」フィールドで、「**+** 」アイコンをクリックしてアクションを作成します。
15. 「認証 **LDAP** サーバーの作成」ページで、「サーバー **IP** 」ラジオ・ボタンを選択し、「認証」の横にあるチェック・ボックスの選択を解除し、次の値を入力して「接続のテスト」を選択します。

    名前: LDAP_no_auth

    IP アドレス: 192.168.10.11

    ベース **DN**: DC = トレーニング、DC = ラボ

    管理者: Administrator@training.lab

    パスワード: xxxxx
16. [その他の設定**]** セクションまで下にスクロールします。ドロップダウンメニューを使用して、次のオプションを選択します。

    「サーバー・ログオン名」属性として「新規」と入力し、「
    ユーザープリンシパル名」と入力します。

17. ドロップダウンメニューを使用して、「新規」として「**SSO** 名属性」を選択し、「**userprincipalname** 」と入力します。
18. 「**OTP** シークレット」フィールドに「ユーザーパラメータ」と入力し、「詳細」をクリックします。
19. 次の属性を入力します。

    属性 **1** = メール
    属性 **2** = オブジェクト GUID
    属性 **3** = 変更不可能 ID
20. [**OK**] をクリックします。
21. [認証ポリシーの作成] ページで、[式] を **true** に設定し、[作成] をクリックします。
22. 「認証ポリシーの作成」ラベルページで、「バインド」をクリックし、「完了」をクリックします。
23. [ポリシーのバインド] ページで、[バインド] をクリックします。
24. [認証ポリシー] ページで、[閉じる] をクリックし、[完了] をクリックします。

> 注
>
> 認証仮想サーバーは RFWebUI ポータルテーマにバインドする必要があります。サーバー証明書をサーバーにバインドします。サーバー IP '1.2.3.5' には、後で使用するために otpauth.server.com という対応する FQDN が必要です。

第 **2** 要素 **OTP** のログインスキーマの作成

1. [セキュリティ**] > [AAA** アプリケーショントラフィック**] > [**仮想サーバ] に移動します。編集する仮想サーバを選択します。
2. 下にスクロールして、[ログインスキーマ**]** を **1** つ選択します。
3. [バインドを追加**]** をクリックします。
4. [ポリシーのバインド] セクションで、[**+**] アイコンをクリックしてポリシーを追加します。
5. [認証ログインスキーマポリシーの作成] ページで、「名前」に OTP と入力し、[**+**] アイコンをクリックしてプロファイルを作成します。
6. 「認証ログイン・スキーマの作成」ページで、「名前」に「OTP」と入力し、「noschema」の横のアイコンをクリックします。
7. [**LoginSchema**] フォルダーをクリックし、[**DualAuth.xml**] を選択し、[選択] をクリックします。
8. [作成] をクリックします。
9. [ルール] セクションで、**True** と入力します。[作成] をクリックします。
10. [バインド] をクリックします。
11. 認証の 2 つの要素に注目してください。[閉じる] をクリックし、[完了] をクリックします。

OTP を管理するためのコンテンツスイッチングポリシーを構成する

Unified Gateway を使用する場合は、次の設定が必要です。

1. [トラフィック管理] **>** [コンテンツの切り替え] **>** [ポリシー] に移動します。コンテンツスイッチングポリシーを選択し、右クリックして [編集] を選択します。
2. 式を編集して次の OR ステートメントを評価し、[**OK**] をクリックします。

is_vpn_url	HTTP.REQ.URL.CONTAINS(“manageotp”)

CLI を使用したネイティブ **OTP** の設定

OTP デバイス管理ページを設定するには、次の情報が必要です。

- 認証仮想サーバに割り当てられた IP
- 割り当てられた IP に対応する FQDN
- 認証用サーバー証明書仮想サーバー

> 注
>
> ネイティブ OTP は、Web ベースのソリューションのみです。

OTP デバイスの登録および管理ページを構成するには

認証仮想サーバーの作成

```
> add authentication vserver authvs SSL 1.2.3.5 443
> bind authentication vserver authvs -portaltheme RFWebUI
> bind ssl vserver authvs -certkeyname otpauthcert
```

> 注
>
> 認証仮想サーバーは RFWebUI ポータルテーマにバインドする必要があります。サーバー証明書をサーバーにバインドする必要があります。サーバー IP ‘1.2.3.5’ には、後で使用するために otpauth.server.com という対応する FQDN が必要です。

LDAP ログオンアクションを作成するには

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP
> - serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
ldapBindDnPassword <PASSWO> -ldapLoginName <USER FORMAT>
```

例:

```
add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4 -
    serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
    administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
    ldapLoginName userprincipalname
```


LDAP ログオンの認証ポリシーを追加するには

```
add authentication Policy auth_pol_ldap_logon -rule true -action
    ldap_logon_action
```

ログインスキーマを使用して **UI** を表示するには

ログオン時にユーザー名のフィールドとパスワードフィールドをユーザーに表示する

```
add authentication loginSchema lschema_single_auth_manage_otp -
    authenticationSchema "/nsconfig/loginschema/LoginSchema/
    SingleAuthManageOTP.xml"
```

デバイスの登録と管理ページを表示する

デバイスの登録と管理画面を表示するには、URL またはホスト名の 2 つの方法があります。

- **URL** を使用する

  URL に'/manageotp' が含まれている場合

  - add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_url -rule "http.req.cookie.value("NSC_TASS").contains("manageotp")"-action lschema_single_auth_manage_otp
  - bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_url -priority 10 -gotoPriorityExpression END

- ホスト名の使用

  ホスト名が「alt.server.com」の場合。

  - add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_host -rule "http.req.header("host").eq("alt.server.com")"-action lschema_single_auth_manage_otp
  - bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_hos -priority 20 -gotoPriorityExpression END

CLI を使用してユーザログインページを設定するには

[ユーザーログオン] ページを構成するには、次の情報が必要です。

- 負荷分散仮想サーバの IP
- 負荷分散仮想サーバーの対応する FQDN
- 負荷分散仮想サーバーのサーバー証明書

> 注
>
> 2 要素認証に既存の認証仮想サーバー (authvs) を再利用します。

負荷分散仮想サーバーを作成するには

```
> add lb vserver lbvs_https SSL 1.2.3.162 443 -persistenceType NONE -
    cltTimeout 180 -  AuthenticationHost otpauth.server.com -
    Authentication ON -authnVsName authvs
> bind ssl vserver lbvs_https -certkeyname lbvs_server_cert
```

ロードバランシングにおけるバックエンドサービスは、次のように表されます。

```
> add service iis_backendsso_server_com 1.2.3.210 HTTP 80
> bind lb vserver lbvs_https iis_backendsso_server_com
```

OTP パスコード検証アクションを作成するには

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP> -
serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -ldapBindDnPassword
 <PASSWORD> -ldapLoginName <USER FORMAT> -authentication DISABLED -OTPSecret
 <LDAP ATTRIBUTE>
```

例:

```
add authentication ldapAction ldap_otp_action -serverIP 1.2.3.4 -
    serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
    administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
    ldapLoginName userprincipalname -authentication DISABLED -OTPSecret
    userParameters
```

> 重要
>
> LDAP ログオンと OTP アクションの違いは、認証を無効にし、新しいパラメータ「OTPSecret」を導入する必要があることです。AD 属性値を使用しないでください。

OTP パスコード検証の認証ポリシーを追加するには

```
> add authentication Policy auth_pol_otp_validation -rule true -action
    ldap_otp_action
```


LoginSchema を使用して **2** 要素認証を表示するには

2 要素認証用の UI を追加します。

```
1 > add authentication loginSchema lscheme_dual_factor -
    authenticationSchema "/nsconfig/loginschema/LoginSchema/DualAuth.xml
    "
2
3 > add authentication loginSchemaPolicy lpol_dual_factor -rule true -
    action lscheme_dual_factor
```

ポリシーラベルを使用してパスコード検証係数を作成するには

次の要素の管理 OTP フローポリシーラベルを作成する（最初の要素は LDAP ログオン）

```
1 > add authentication loginSchema lschema_noschema -authenticationSchema
     noschema
2
3 > add authentication policylabel manage_otp_flow_label -loginSchema
    lschema_noschema`
```

OTP ポリシーをポリシー・ラベルにバインドするには

```
1 bind authentication policylabel manage_otp_flow_label -policyName
    auth_pol_otp_validation -priority 10 -gotoPriorityExpression NEXT
```

UI フローをバインドするには

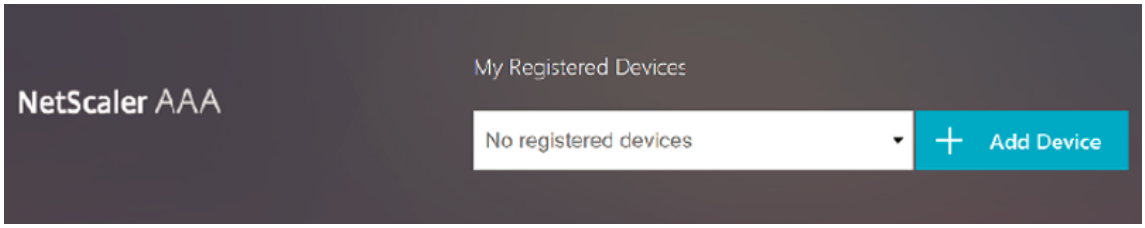
LDAP ログオンに続いて OTP 検証を認証仮想サーバーとバインドします。

```
1 > bind authentication vserver authvs -policy auth_pol_ldap_logon -
    priority 10 -nextFactor  manage_otp_flow_label -
    gotoPriorityExpression NEXT
2
3 > bind authentication vserver authvs -policy lpol_dual_factor -priority
     30 -gotoPriorityExpression END
```

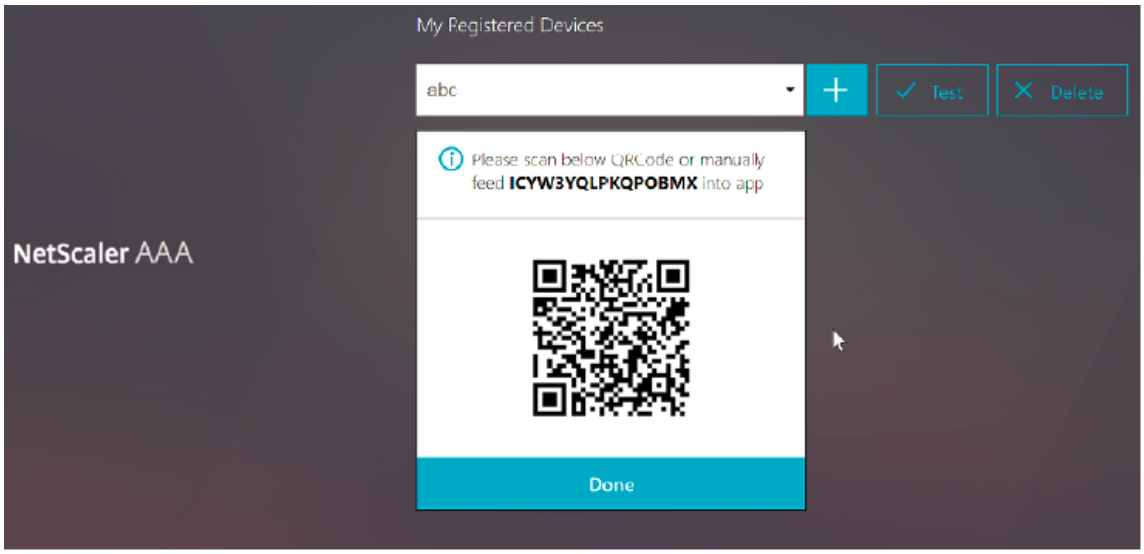
Citrix ADC でデバイスを登録する

1. /manageotp というサフィックスが付いた、Citrix ADC FQDN（最初のパブリック IP アドレス）に移動します。たとえば、ユーザーの資格情報でhttps://otpauth.server.com/manageotp にログインします。

2. [**+**] アイコンをクリックして、デバイスを追加します。

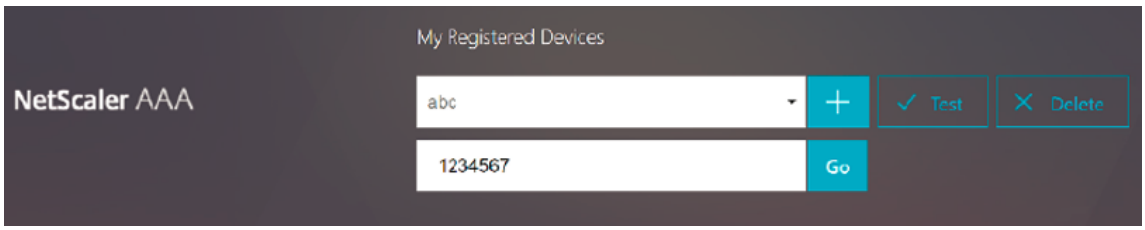


3. デバイス名を入力し、**Go** キーを押します。バーコードが画面に表示されます。
4. [セットアップの開始] をクリックし、[バーコードのスキャン] をクリックします。
5. デバイスのカメラを QR コードの上に置きます。必要に応じて、16 桁のコードを入力できます。



> 注:
>
> 表示されている QR コードは 3 分間有効です。

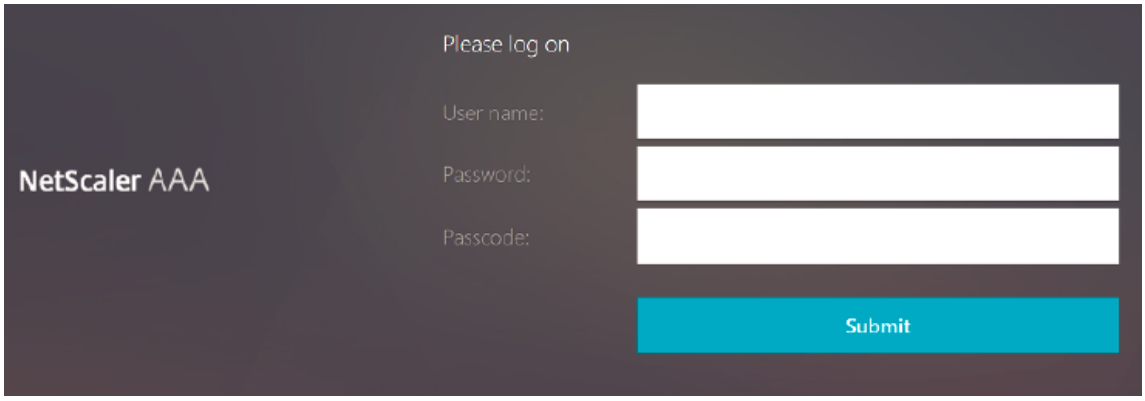
6. スキャンに成功すると、ログインに使用できる 6 桁の時間依存コードが表示されます。



7. テストするには、QR 画面で [完了] をクリックし、右側の緑色のチェックマークをクリックします。
8. プルダウンメニューから端末を選択し、Google Authenticator からコード（赤ではなく青でなければならない）を入力し、[**Go**] をクリックします。
9. ページの右上隅にあるドロップダウンメニューを使用してログアウトしてください。

OTP を使用して **Citrix ADC** にログインします

1. 最初の公開 URL に移動し、Google Authenticator から OTP を入力してログオンします。
2. Citrix ADC スプラッシュページへの認証を行います。



OTP のプッシュ通知

April 9, 2020

Citrix Gateway は、OTP のプッシュ通知をサポートしています。ユーザーは、Citrix Gateway にログインするために、登録されたデバイスで受信した OTP を手動で入力する必要はありません。管理者は、プッシュ通知サービスを使用してユーザーの登録デバイスにログイン通知が送信されるように Citrix Gateway を設定できます。ユーザーが通知を受け取ったら、通知の [許可] をタップするだけで Citrix Gateway にログインできます。Gateway は、ユーザーからの確認応答を受信すると、要求の送信元を識別し、そのブラウザ接続に応答を送信します。

タイムアウト時間（30 秒）内に通知応答が受信されない場合、ユーザーは Citrix Gateway のログインページにリダイレクトされます。その後、ユーザは OTP を手動で入力するか、[再送信（**Resend Notification**）] をクリックして、登録されたデバイスで再度通知を受信できます。

管理者は、プッシュ通知用に作成されたログインスキーマを使用して、プッシュ通知認証をデフォルト認証として行うことができます。

> 重要：プッシュ通知機能は、Citrix ADC Premium エディションライセンスで利用できます。

プッシュ通知の利点

- プッシュ通知は、より安全な多要素認証メカニズムを提供します。ユーザーがログイン試行を承認するまで、Citrix Gateway への認証は成功しません。
- プッシュ通知は、管理と使用が簡単です。ユーザーは、Citrix SSO モバイルアプリをダウンロードしてインストールする必要があります。管理者による支援は必要ありません。
- ユーザーはコードをコピーしたり覚えておく必要はありません。認証を受けるには、デバイスをタップするだけで済みます。

- ユーザーは複数のデバイスを登録できます。

プッシュ通知の動作

プッシュ通知ワークフローは、次の 2 つのカテゴリに分類できます。

- デバイス登録
- エンドユーザーログイン

プッシュ通知を使用するための前提条件

- Citrix Cloud のオンボーディングプロセスを完了します。
  1. Citrix Cloud の企業アカウントを作成するか、既存のアカウントに参加します。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。
  2. https://citrix.cloud.comにログインし、顧客を選択します。
  3. 「メニュー」から「ID」と「アクセス管理」を選択し、「API Access」タブに移動して、顧客のクライアントを作成します。
  4. ID、シークレット、カスタマー ID をコピーします。この ID とシークレットは、Citrix ADC でプッシュサービスを「ClientID」と「ClientSecret」として構成するために必要です。

> 重要:
>
> - 同じ API 認証情報を複数のデータセンターで使用できます。
> - オンプレミスの Citrix ADC アプライアンスは、サーバーアドレスの mfa.cloud.com と trust.citrixWorkspacesapi.net を解決できる必要があり、アプライアンスからアクセスできる必要があります。これは、ポート 443 を介してこれらのサーバに対してファイアウォールまたは IP アドレスブロックがないことを保証するためです。

- iOS デバイスと Android デバイス用のアプリストアと Play ストアから Citrix SSO モバイルアプリをダウンロードします。プッシュ通知は、2.3.5 から Android 上のビルド 1.1.13 から iOS でサポートされています。
- Active Directory について次のことを確認します。
  - 属性の最小長は 256 文字以上にする必要があります。
  - 属性タイプは、ユーザーパラメータなどの ‘ディレクトリ文字列’ である必要があります。これらの属性は文字列値を保持できます。
  - デバイス名が英語以外の文字である場合、属性文字列タイプは Unicode である必要があります。
  - Citrix ADC LDAP 管理者は、選択した AD 属性への書き込みアクセス権を持っている必要があります。
  - Citrix ADC とクライアントマシンは、共通のネットワークタイムサーバーに同期する必要があります。

プッシュ通知の設定

プッシュ通知機能を使用するには、次の手順を完了する必要があります。

- Citrix Gateway 管理者は、ユーザーを管理および検証するためのインターフェイスを構成する必要があります。

  1. プッシュ・サービスを構成します。
  2. OTP 管理とエンドユーザーログイン用に Citrix Gateway を構成します。

     Citrix Gateway にログインするには、デバイスを Gateway に登録する必要があります。
  3. デバイスを Citrix Gateway に登録します。
  4. Citrix Gateway にログインします

プッシュ・サービスの作成

1. [セキュリティ] > [**AAA** アプリケーショントラフィック] > [ポリシー] > [認証] > [高度なポリシー] > [アクション] > [プッシュサービス] に移動し、[追加] をクリックします。
2.「名前」に、プッシュ・サービスの名前を入力します。
3.「クライアント **ID**」に、クラウド内の Citrix Push サーバーと通信するための証明書利用者の一意の ID を入力します。
4. [クライアントシークレット] に、クラウド内の Citrix Push サーバーと通信するための証明書利用者の一意のシークレットを入力します。
5. [顧客 **ID**] に、クライアント ID とクライアントシークレットのペアを作成するために使用するクラウド内のアカウントの顧客 ID または名前を入力します。

OTP 管理とエンドユーザーログインのための **Citrix Gateway** の構成

OTP 管理とエンドユーザログインを行うには、次の手順を実行します。

- OTP 管理用のログインスキーマの作成
- 認証、承認、監査仮想サーバーの構成
- VPN または負荷分散仮想サーバーの構成
- ポリシー・ラベルの構成
- エンド・ユーザー・ログイン用のログイン・スキーマの作成

設定の詳細については、ネイティブ OTP サポートを参照してください。

重要: プッシュ通知の場合、管理者は以下を明示的に設定する必要があります。

- プッシュ・サービスを作成します。
- OTP 管理用のログインスキーマを作成するときは、必要に応じて SingleAuthManageOTP.xml ログインスキーマまたは同等のログインスキーマを選択します。
- エンドユーザーログイン用のログインスキーマを作成するときは、必要に応じて DualAuthOrPush.xml ログインスキーマまたは同等のログインスキーマを選択します。

デバイスを **Citrix Gateway** に登録する

プッシュ通知機能を使用するには、デバイスを Citrix Gateway に登録する必要があります。

1. Web ブラウザで、Citrix Gateway の FQDN を参照し、FQDN に **/manageotp** という接尾辞を付けます。

   認証ページが読み込まれます。
   例：https://gateway.company.com/manageotp

2. 必要に応じて、LDAP クレデンシャルまたは適切な 2 要素認証メカニズムを使用してログインします。
3. ［デバイスを追加］をクリックします。
4. デバイスの名前を入力し、［実行］をクリックします。

   Citrix Gateway のブラウザページに QR コードが表示されます。

5. 登録するデバイスから Citrix SSO アプリを使用して、この QR コードをスキャンします。

   Citrix SSO は QR コードを検証し、プッシュ通知でゲートウェイに登録します。登録プロセスにエラーがない場合、トークンはパスワードトークンページに正常に追加されます。

6. 追加/管理するデバイスがない場合は、ページの右上隅にあるリストを使用してログアウトします。

ワンタイムパスワード認証のテスト

1. OTP をテストするには、リストからデバイスをクリックし、[**Test**] をクリックします。
2. デバイスで受信した OTP を入力し、[**Go**] をクリックします。

   「OTP 検証に成功しました」というメッセージが表示されます。

3. ページの右上隅のリストを使用してログアウトします。

注：OTP 管理ポータルを使用して、認証のテスト、登録済みデバイスの削除、または追加のデバイスの登録をいつでも行うことができます。

Citrix Gateway にログインします

Citrix Gateway にデバイスを登録すると、ユーザーはプッシュ通知機能を使用して認証を行うことができます。

1. Citrix Gateway 認証ページに移動します（例：https://gateway.company.com）。

   ログインスキーマの構成に応じて、LDAP 認証情報のみを入力するように求められます。

2. LDAP ユーザー名とパスワードを入力し、[**Submit**] を選択します。

   登録済みのデバイスに通知が送信されます。

   注意**:** OTP を手動で入力する場合は、「クリックして OTP を手動で入力する」を選択し、「**TOTP** 」フィールドに OTP を入力する必要があります。

3. 登録したデバイスで Citrix SSO アプリを開き、［許可］をタップします。

注:

- 認証サーバは、設定されたタイムアウト時間が経過するまで、プッシュサーバ通知応答を待機します。タイムアウト後、Citrix Gateway はログインページを表示します。その後、ユーザは OTP を手動で入力するか、[再送信（**Resend Notification**）] をクリックして、登録されたデバイスで再度通知を受信できます。選択したオプションに基づいて、Gateway は入力した OTP を検証するか、登録済みのデバイスに通知を再送信します。
- ログイン失敗に関する通知は、登録されたデバイスに送信されません。

障害状態

- 次の場合、デバイスの登録が失敗することがあります。
  - サーバー証明書がエンドユーザーのデバイスによって信頼されていない可能性があります。
  - OTP の登録に使用された Citrix Gateway は、クライアントからアクセスできません。
- 通知は、次の場合に失敗することがあります。
  - ユーザーデバイスがインターネットに接続されていません
  - ユーザーデバイス上の通知がブロックされる
  - ユーザーがデバイス上の通知を承認しない

このような場合、認証サーバは、設定されたタイムアウト時間が経過するまで待機します。タイムアウト後、Citrix Gateway にはログインページが表示され、手動で OTP を入力するか、登録済みのデバイスに通知を再送信するかを選択できます。選択したオプションに基づいて、さらに検証が行われます。

iOS での **Citrix SSO** アプリケーションの動作 **—** 注意すべきポイント

通知のショートカット

Citrix SSO iOS アプリには、ユーザーエクスペリエンスを向上させるためのアクション可能な通知のサポートが含まれています。iOS デバイスで通知を受信した後、デバイスがロックされているか、Citrix SSO アプリケーションがフォアグラウンドになっていない場合、ユーザーは通知に組み込まれたショートカットを使用してログイン要求を承認または拒否できます。

通知のショートカットにアクセスするには、デバイスのハードウェアに応じて、強制的にタッチ（3D タッチ）または長押しする必要があります。[ショートカットの許可] アクションを選択すると、Citrix ADC にログイン要求が送信されます。認証、承認、および監査仮想サーバーでの認証ポリシーの構成方法に応じて、

- ログイン要求は、アプリをフォアグラウンドで起動したり、デバイスのロックを解除したりすることなく、バックグラウンドで送信されることがあります。
- アプリは、アプリがフォアグラウンドで起動される余分な要素として、Touch-ID/Face-ID/パスコードを要求することがあります。

Citrix SSO からのパスワードトークンの削除

1. Citrix SSO アプリでプッシュ用に登録されたパスワードトークンを削除するには、以下の手順を実行する必要があります。
2. Gateway 上の iOS/Android デバイスを登録解除（削除）します。デバイスから登録を削除するための QR コードが表示されます。
3. Citrix SSO アプリを開き、削除するパスワードトークンの情報ボタンをタップします。
4.「トークンの削除」をタップし、QR コードをスキャンします。

注:

- QR コードが有効な場合、トークンは Citrix SSO アプリから正常に削除されます。
- 端末がすでに Gateway から削除されている場合は、QR コードをスキャンすることなく、「強制削除」をタップしてパスワードトークンを削除できます。強制削除を行うと、Citrix Gateway からデバイスが削除されていない場合でも、デバイスが通知を受信し続けることがあります。

サーバ名表示拡張の設定

March 26, 2020

Citrix Gateway アプライアンスは、バックエンドサーバーに送信される SSL「client hello」パケットにサーバー名表示（SNI）拡張子を含めるように構成できるようになりました。SNI 拡張は、バックエンドサーバが SSL ハンドシェイク中に要求されている FQDN を識別し、それぞれの証明書で応答するのに役立ちます。

> 注
>
> 複数の SSL ドメインが同じサーバーでホストされている場合、SNI サポートを有効にします。

GUI を使用して **SNI** をサポートするように **Citrix Gateway** を構成するには:

1. NetScaler の GUI で、「構成」**>**「**Citrix NetScaler>**「グローバル設定」の順に選択します。
2. [グローバル設定の変更**]** リンクをクリックし、[バックエンドサーバ **SNI**] ドロップダウンから [有効] を選択します。

コマンドラインインターフェイスを使用して **SNI** をサポートするように **Citrix Gateway** を構成するには、コマンドプロンプトで次のように入力します。

```
1 set vpn parameter backendServerSni <ENABLED><DISABLED>
```


SSL ハンドシェイク中のサーバー証明書の検証

March 26, 2020

Citrix Gateway アプライアンスは、SSL ハンドシェイク中にバックエンドサーバーによって提供されたサーバー証明書を検証するように構成できるようになりました。

構成ユーティリティを使用して送信プロキシの PAC をサポートするように Citrix Gateway グローバルパラメーターを構成するには

CA 証明書のバインド

1. [構成] **>** [**Citrix Gateway**] > [**Citrix Gateway** ポリシーマネージャー] > [証明書バインディング] の順に選択します。**
2. [証明書のバインド] 画面で、[**+**] アイコンをクリックします。
3. [**CA** 証明書のバインド] 画面で、[バインド の追加] をクリックし、[インストール] をクリックします。
4. 「証明書 ファイル名」フィールドで証明書ファイル名を選択し、「インストール」をクリックします。
5. [**CA** 証明書のバインド] 画面で、証明書を選択し、[バインド] をクリックします。
6. [完了] をクリックします。

証明書検証の有効化:

1. [**Citrix Gateway**] **>** [グローバル設定] に移動します。
2. [グローバル設定の変更] をクリックします。**
3. [バックエンドサーバ証明書の検証] ドロップダウンメニューから [有効] を選択し、[**OK**] をクリックします。

コマンドラインでサーバー証明書をサポートするように Citrix Gateway グローバルパラメーターを構成するには

コマンドプロンプトで、次のコマンドを入力します。

```
1     bind vpn global cacert DNPGCA1
2
3     set vpn parameter backendcertValidation ENABLED
4 <!--NeedCopy-->
```

アドバンスポリシーを使用した VPN ポリシーの作成

April 9, 2020

クラシックポリシーエンジン（PE）とアドバンスポリシーインフラストラクチャ（PI）は、Citrix ADC が現在サポートしている 2 つの異なるポリシー構成と評価フレームワークです。

アドバンス・ポリシー・インフラストラクチャは、非常に強力な表現言語で構成されています。式言語は、ポリシーのルールを定義したり、アクションのさまざまな部分を定義したり、サポートされているその他のエンティティを定

義したりするために使用できます。式言語は、リクエストまたはレスポンスのどの部分でも解析でき、ヘッダーとペイロードを深く調べることもできます。同じ式言語が展開され、Citrix ADC がサポートするすべての論理モジュールを介して機能します。

> 注:
> ポリシーの作成には、高度なポリシーを使用することをお勧めします。

従来のポリシーから高度なポリシーに移行する理由

高度なポリシーには、豊富な式セットがあり、クラシックポリシーよりも柔軟性に優れています。Citrix ADC は多種多様なクライアントに対応するため、高度なポリシーを大幅に上回る表現をサポートすることが不可欠です。詳しくは、「ポリシーと式」を参照してください。

以下は、アドバンスポリシーのために追加された機能です。

- メッセージの本文にアクセスする機能。
- 多くの追加プロトコルをサポートします。
- システムの多くの追加機能にアクセスします。
- 基本的な関数、演算子、およびデータ型のより多くの数を持っています。
- HTML、JSON、および XML ファイルの解析に利用できます。
- 高速な並列マルチストリングマッチング (パッチセットなど) を容易にします。

これで、アドバンスポリシーを使用して、次の VPN ポリシーを設定できます。

- セッションポリシー
- 承認ポリシー
- 交通政策
- トンネルポリシー
- 監査ポリシー

また、エンドポイント分析（EPA）は、認証機能の nFactor として構成できます。EPA は、Gateway アプライアンスに接続しようとするエンドポイントデバイスのゲートキーパーとして使用されます。エンドポイントデバイスに [Gateway] ログオンページが表示される前に、Gateway 管理者が設定した適格基準に応じて、デバイスのハードウェアおよびソフトウェアの最小要件がチェックされます。Gateway へのアクセスは、実行されたチェックの結果に基づいて付与されます。以前は、EPA はセッションポリシーの一部として設定されていました。nFactor にリンクできるようになり、いつ実行できるかについて柔軟性が高まります。EPA の詳細については、「エンドポイントポリシーの仕組み」を参照してください。nFactor の詳細については、「n ファクタ認証」を参照してください。

ユースケース:

高度な **EPA** を使用した事前認証 **EPA**

認証前 EPA スキャンは、ユーザーがログオン資格情報を入力する前に実行されます。認証要素の 1 つとして事前認証 EPA スキャンを使用した nFactor 認証用の Citrix Gateway の構成については、CTX224268トピックを参照してください。

高度な **EPA** を使用した認証後の **EPA**

認証後 EPA スキャンは、ユーザーの資格情報が確認された後に行われます。従来のポリシーインフラストラクチャでは、認証後の EPA がセッションポリシーまたはセッションアクションの一部として構成されました。[高度なポリシーインフラストラクチャ] では、EPA スキャンを N ファクタ認証の EPA ファクタとして構成します。認証後の EPA スキャンを認証要素の 1 つとして使用して n 要素認証を行うための Citrix Gateway の構成については、CTX224303トピックを参照してください。

高度なポリシーを使用した事前認証および認証後の **EPA**

EPA は、認証前および認証後で実行できます。事前認証および認証後の EPA スキャンを使用した nFactor 認証用の Citrix Gateway の構成については、CTX231362トピックを参照してください。

nFactor 認証の要素としての定期的な **EPA** スキャン

クラシックポリシーインフラストラクチャでは、定期的な EPA スキャンがセッションポリシーアクションの一部として構成されました。高度なポリシーインフラストラクチャでは、N ファクタ認証の EPA ファクタの一部として構成できます。

nFactor 認証の要素として定期的な EPA スキャンを構成する方法の詳細については、CTX231361トピックをクリックしてください。

トラブルシューティング:

トラブルシューティングの際は、次の点に留意してください。

- 同じタイプのクラシックポリシーとアドバンスポリシー（セッションポリシーなど）は、同じエンティティ/バインドポイントにバインドできません。
- すべての PI ポリシーでは、プライオリティは必須です。
- VPN のアドバンスポリシーは、すべてのバインドポイントにバインドできます。
- 同じ優先度を持つアドバンスポリシーは、単一のバインドポイントにバインドできます。
- 設定された認可ポリシーがいずれもヒットしない場合は、VPN パラメータで設定されたグローバル認可アクションが適用されます。
- 認可ポリシーでは、認可規則が失敗しても、認可アクションは取り消されません。

クラシックポリシーでよく使用される高度なポリシーの等価式**:**

従来のポリシー表現	アドバンスポリシー式
ns_true	true
ns_false	false
REQ.HTTP	HTTP.REQ
RES.HTTP	HTTP.RES

従来のポリシー表現	アドバンスポリシー式
HEADER “foo”	HEADER(“foo”)
CONTAINS ”bar”	.CONTAINS(“bar”) [Note use of “.”.]
REQ.IP	CLIENT.IP
RES.IP	SERVER.IP
SOURCEIP	SRC
DESTIP	DST
REQ.TCP	CLIENT.TCP
RES.TCP	SERVER.TCP
SOURCEPORT	SRCPORT
DESTPORT	DSTPORT
STATUSCODE	STATUS
REQ.SSL.CLIENT.CERT	CLIENT.SSL.CLIENT_CERT

テンプレートを使用した簡略化された **SaaS** アプリケーション設定

March 26, 2020

Citrix Gateway でのシングルサインオンによる SaaS アプリケーションの構成は、一般的な SaaS アプリケーションのテンプレートドロップダウンメニューを Provisioning することで簡素化されます。設定する SaaS アプリは、メニューから選択できます。このテンプレートは、アプリケーションの構成に必要な多くの情報をあらかじめ入力しています。ただし、お客様に固有の情報を提供する必要があります。

注：以下のセクションでは、テンプレートを使用してアプリケーションを構成および公開するために **Citrix Gateway** で実行する手順について説明します。アプリケーションサーバーで実行する設定手順については、以降のセクションで説明します。

テンプレートを使用したアプリケーションの構成と公開**-Citrix Gateway** 固有の構成

以下の設定では、テンプレートを使用してアプリケーションを設定および発行する例として **AWS** コンソールアプリケーションを使用します。

開始する前に、次のものが必要です。

- AWS コンソールの管理者アカウント

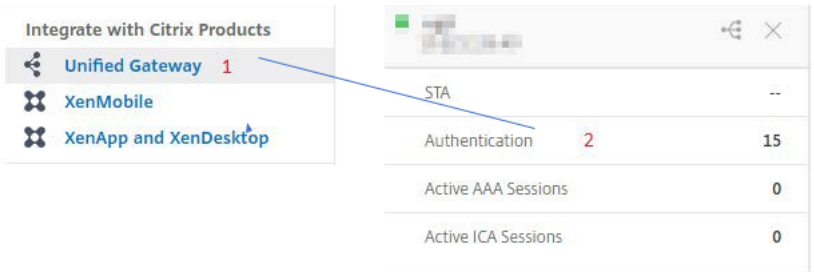
- Citrix Gateway の管理者アカウント

AWS コンソールの設定手順は次のとおりです。

1. アプリケーションカタログを使用して AWS コンソールを設定します。
2. Citrix ADC から AWS コンソールの IdP メタデータをエクスポートします。
3. AWS コンソールで IdP を設定します。

ステップ **1:** アプリケーションカタログで AWS コンソールを設定する

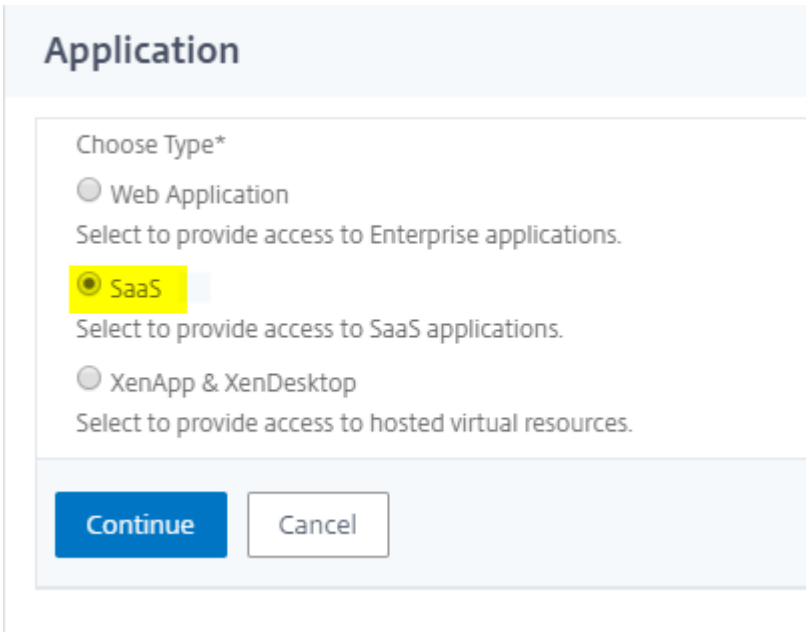
1. [**Unified Gateway] > [**認証**]** をクリックします。



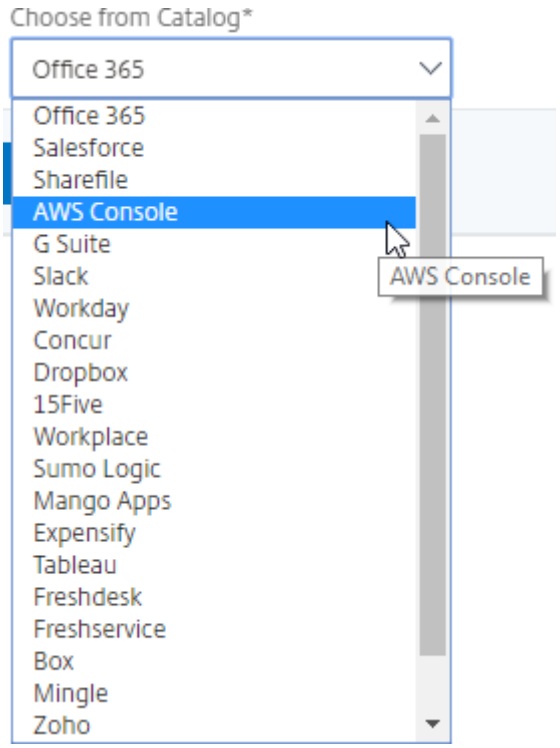
[Unified Gateway の設定] 画面が表示されます。

2. [アプリケーション] セクションで、[編集] アイコンをクリックします。さて、プラスアイコンをクリックします。[アプリケーション] ウィンドウが表示されます。

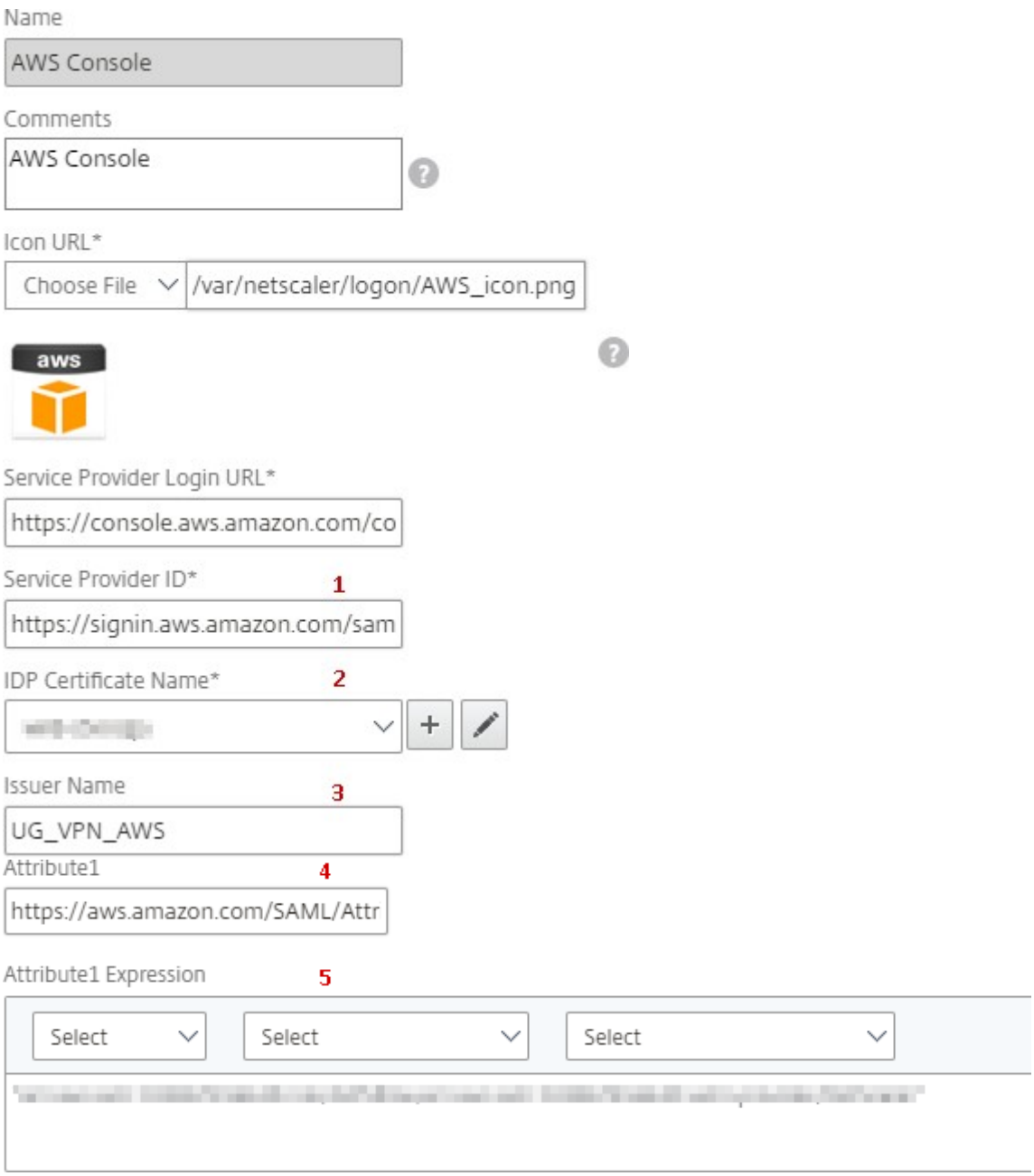
3. [アプリケーションタイプ] から [**SaaS**] を選択します。



4. ドロップダウンリストから [**AWS** コンソール] を選択します。



5. アプリケーションテンプレートに適切な値を入力します。



6. 次の SAML 設定の詳細を入力し、[**Continue**] をクリックします。

   サービスプロバイダ **ID** —https://signin.aws.amazon.com/saml

   署名証明書名 — IdP 証明書を選択する必要があります。

   発行者名 -発行者名は、あなたの選択に従って記入することができます

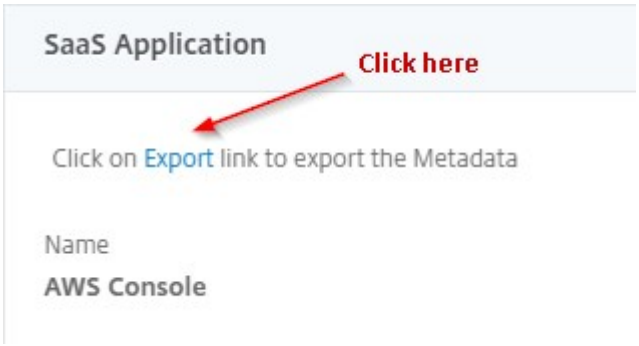
   属性 **1** —`https://aws.amazon.com/SAML/Attributes/Role`

   属性 **1** の式 — ステップ 3 に示すように、ロール ARN、IdP ARN

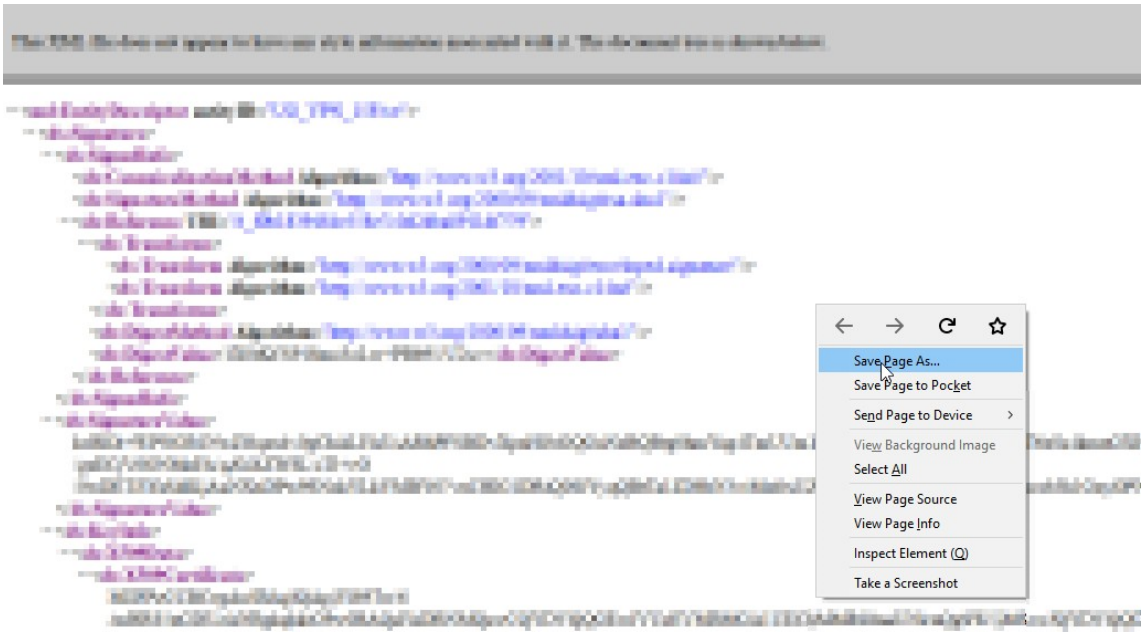
7. [完了] をクリックします。

ステップ **2:** Citrix Gateway から AWS コンソールの IdP メタデータをエクスポートします。

1. [**Unified Gateway] > [**認証**]** をクリックします。
2. 下にスクロールして、**AWS** コンソールテンプレートをクリックします。[SaaS アプリケーション] ウィンドウが表示されます。[エクスポート] リンクをクリックします。



3. メタデータが別のウィンドウで開きます。**IdP** メタデータ・ファイルの保存



ステップ **3:** AWS コンソールへの IdP の設定 .

テンプレートを使用したアプリの構成と公開**-**アプリサーバー固有の構成

以下は、テンプレートを使用して一般的な SaaS アプリを構成および公開するためのアプリサーバー固有の構成に関するガイダンスを持っている pdf のリンクです。

- 15Five
- Absorb
- Accompa

- Adobe Captivate Prime
- Adobe Creative Cloud
- Aha
- Alertops
- Allocadia
- Ariba
- Assembla
- AWS コンソール
- BambooHR
- Base CRM
- BitaBIZ
- Bluejeans
- Blissbook
- Bonusly
- Box
- Bugsnag
- Buildkite
- CakeHR
- Cardboard
- Cedexis
- Celoxis
- Cisco Meraki
- ClearSlide
- CloudCheckr
- ConceptShare
- Concur
- Confluence
- Contactzilla
- Convo

- Criconus
- Dashlane
- Datadog
- Deskpro
- Deputy
- DigiCert
- Docusign
- Domo
- Dropbox
- Duo
- efront
- Ekarda
- Envoy
- ERP
- Expensify
- EZOfficeInventory
- EZRentOut
- Favro
- Federated Directory
- Feedly
- Fivetran
- Flatter Files
- Flowdock
- Freshdesk
- Front
- G-Suite
- GitHub
- GlassFrog
- GotoMeeting

- Happyfox
- Helpjuice
- Help Scout
- Hoshinplan
- Humanity
- Igloo
- Illumio
- Image Relay
- iMeet Central
- InteractGo
- iQualify One
- Jira
- Kanban Tool
- Keeper Security
- Kentik
- Kentik
- Kissflow
- KnowBe4
- KnowledgeOwl
- Kudos
- LaunchDarkly
- Lifesize
- Litmos
- LiquidPlanner
- LogDNA
- Mango
- Manuscript
- Marketo
- Mingle

- Mixpanel
- MuleSoft
- MyWebTimesheets
- New Relic
- Nmbrs
- Nuclino
- Office365
- OneDesk
- OpsGenie
- Orginio
- Pagerduty
- Panorama9
- ParkMyCloud
- Peakon
- People HR
- Pingboard
- Pipedrive
- PlanMyLeave
- PlayVox
- Podio
- ProdPad
- Proto.io
- Proxyclick
- PurelyHR
- Quandora
- Rackspace
- RealtimeBoard
- Remedyforce
- Robin

- Rollbar
- Salesforce
- Samanage
- Samepage
- Sentry
- ServiceDesk Plus
- ServiceNow
- Shufflrr
- Skeddly
- Skills Base
- Slack
- Slemma
- Sli.do
- Smartsheet
- Spoke
- Spotinst
- SproutVideo
- StatusCast
- Status Hero
- Statushub
- Statuspage
- Sumologic
- Supermood
- Syncplicity
- Tableau
- Targetprocess
- Teamphoria
- Testable
- TestFairy

- TextExpander
- TextMagic
- ThousandEyes
- Thycotic Secret server
- Tinfoil Security
- Trisotech
- Trumba
- TwentyThree
- Unifi
- UserEcho
- UserVoice
- Velpic
- VictorOps
- Vidizmo
- Visual Paradigm
- Weekdone
- Wepow
- When I Work
- Workday
- Workpath
- Workplace
- Workstars
- Workteam
- XaitPorter
- Ximble
- XMatters
- Yodeck
- Zendesk
- Zivver

- Zoho-one
- Zivver
- Zoom

EPA コンポーネントとしての nFactor でのデバイス証明書

March 26, 2020

デバイス証明書は、nFactor で EPA コンポーネントとして設定できます。デバイス証明書は、EPA の一部として任意の要素として表示できます。

以下は、EPA コンポーネントとして nFactor でデバイス証明書を構成する利点です。

- デバイス証明書の検証に失敗しても、ログオンエラーは発生しません。構成に基づいて、ログオンを続行し、アクセスを制限されたグループの下にユーザーを配置することができます。
- デバイス証明書のチェックはポリシーによって決定されるため、デバイス証明書の認証に基づいて、社内のイントラネットリソースへのアクセスを選択的に許可またはブロックできます。たとえば、デバイス証明書認証は、企業で管理されているラップトップ上でのみの Office 365 アプリケーションへの条件付きアクセスを提供するために使用できます。

デバイス証明書の検証を定期的な EPA スキャンに含めることはできません。

> 重要**:** Windows では、デフォルトで、デバイス証明書にアクセスするための管理者権限が義務されています。管理者以外のユーザーのデバイス証明書チェックを追加するには、デバイスに EPA プラグインと同じバージョンの VPN プラグインをインストールする必要があります。

デバイス証明書を NFactor で EPA コンポーネントとして構成する

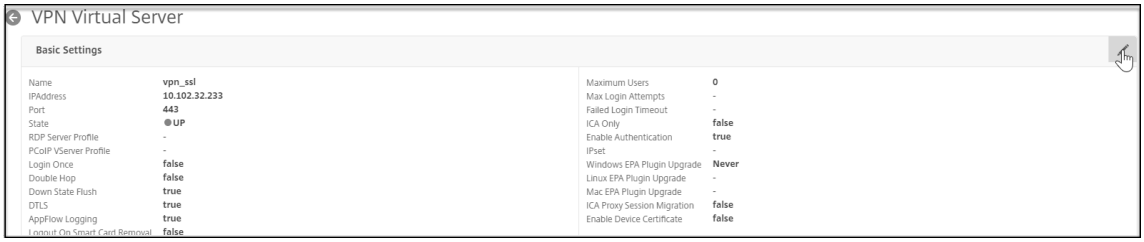
コマンドラインインターフェイスを使用して **nFactor** のデバイス証明書を **EPA** コンポーネントとして構成するには、コマンドプロンプトで次のように入力します。

```
1 add authentication epaAction epa-act -csecexpr sys.client_expr("device-
      cert_0_0") -defaultgroup epa_pass -quarantine_group epa_fail
2
3 <!--NeedCopy-->
```

Citrix ADC GUI を使用して、**VPN** 仮想サーバーの **EPA** コンポーネントとして **nFactor** のデバイス証明書を構成するには:

1. NetScaler GUI で、「構成」**>**「**Citrix Gateway**」**>**「仮想サーバー」の順に選択します。
2. [**Citrix Gateway** 仮想サーバー] ページで、変更する仮想サーバーを選択し、[編集] をクリックします。

3. [**VPN** 仮想サーバー] ページで、[編集] アイコンをクリックします。



4. [詳細] をクリックします。

5. [デバイス証明書の CA] セクションの横にある [追加] をクリックし、[OK] をクリックします。

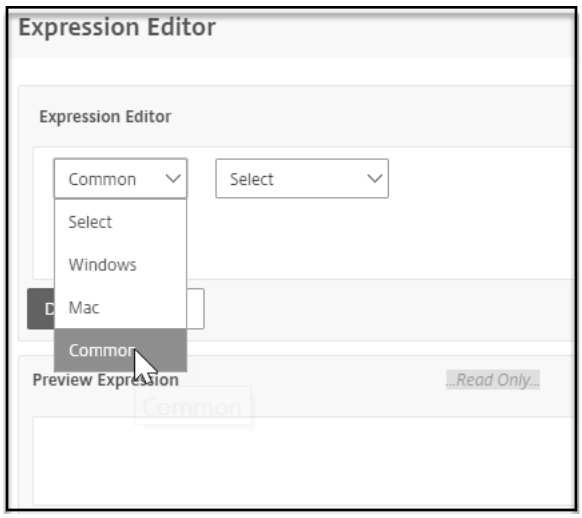
> [デバイス証明書を有効にする] チェックボックスは選択しないでください。これを有効にすると、従来の EPA でデバイス証明書の検証が有効になります。

6. NetScaler GUI で、「構成」**>**「セキュリティ」**>**「**AAA**」**—**「アプリケーショントラフィック」**>**「ポリシー」**>**「認証」**>**「高度なポリシー」**>**「アクション」**>**「**EPA>**」の順に選択します。

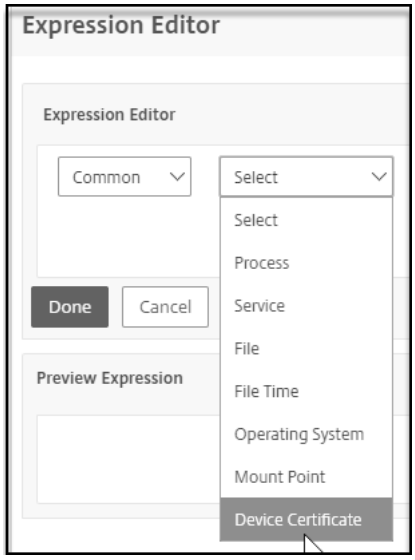
7. [認証 **EPA** アクション] ページで、[追加] をクリックします。[**Edit**] をクリックすると、既存の EPA アクションを編集できます。

8. [認証 **EPA** アクションの作成] ページで、認証 EPA アクションを作成するために必要なフィールドの値を入力し、[**EPA** エディタ] リンクをクリックします。

9. [式エディタ**]** リストから **[**** 共通]** を選択します。



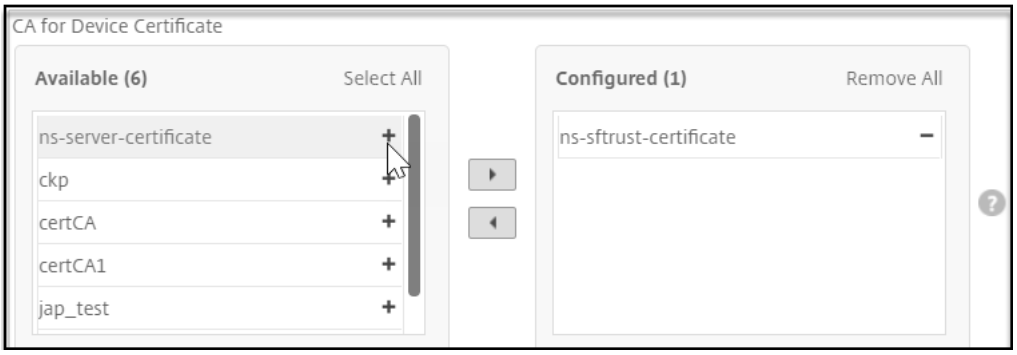
10. 表示される次のリストから [デバイス証明書] を選択し、[完了] をクリックして設定を完了します。



Citrix ADC GUI を使用して、**nFactor** でデバイス証明書を **AAA** 仮想サーバの **EPA** コンポーネントとして構成するには、次の手順を実行します。

1. Citrix DC GUI で、「セキュリティ」**>**「**AAA** アプリケーショントラフィック」**>**「仮想サーバー」の順に選択します。
2. [**Citrix Gateway** 仮想サーバー] ページで、変更する仮想サーバーを選択し、[編集] をクリックします。
3. [認証仮想サーバー] ページで、[編集] アイコンをクリックします。
4. [詳細] をクリックします。
5. [デバイス証明書の **CA**] セクションの横にある [追加] をクリックします。

6. 追加する証明書を選択し、[**OK**] をクリックして構成を完了します。



7. 前のセクションで示 した手順 **6** ～**10** を繰り返して、設定を完了します。

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