NetScaler Gateway 13.1

Machine translated content

Disclaimer

Contents

NetScaler Gateway リリースノート

February 1, 2024

リリースノートには、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既知の問題が記載されています。

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機能強化とその他の変更。
- 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。
- 注意点: ビルドを使用する際に留意すべき重要な点です。
- 制限事項: ビルドに存在する制限事項。

> 重要： NetScaler Gateway のリリースノートは、ADC リリースノートの一部として記載されています。NetScaler Gateway 13.1 の拡張機能、既知の問題、およびバグ修正の詳細については、リリースノートのページを参照してください 。

注:

- 問題の説明の下にある［# XXXXXX］ラベルは、NetScaler チームが内部的に使用する追跡 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。セキュリティ関連の修正と勧告のリストについては、セキュリティ速報を参照してください。

NetScaler Gateway について

April 1, 2024

NetScaler Gateway は導入が簡単で、管理も簡単です。最も一般的な展開構成は、DMZ に NetScaler Gateway アプライアンスを配置することです。ネットワーク内に複数の NetScaler Gateway アプライアンスをインストールして、より複雑な展開環境を実現することができます。

NetScaler Gateway を初めて起動するときに、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設定を実行できます。IP アドレス、サブネットマスク、デフォルトゲートウェイ 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、NetScaler Gateway 操作に固有の設定を構成します。

NetScaler 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で展開の計画に関する情報を確認してください。展開計画には、アプライアンスを設置する場所の決定、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。NetScaler 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またはソフトウェアを変更することなく、任意の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。NetScaler 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の他のネットワーク製品をサポートしています。

NetScaler Gateway を構成する前に、インストール前チェックリストに設定を書いて、手元に置くことができます。

NetScaler Gateway アプライアンス	NetScaler 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	確認する計画情報と、NetScaler Gateway をネットワークにインストールする前に完了する必要が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、DMZ のない安全なネットワーク、および負荷分散とフェイルオーバーをサポートするための他のアプライアンスとの NetScaler Gateway の展開に関する情報を提供します。また、Citrix Virtual Apps and Desktops を使用した NetScaler Gateway の展開に関する情報も記載されています。
Licensing	アプライアンスにライセンスをインストールする方法について説明します。また、複数の NetScaler Gateway アプライアンスにライセンスをインストールする方法についても説明しています。

NetScaler Gateway アーキテクチャ

NetScaler Gateway のコアコンポーネントは次のとおりです。

- 仮想サーバー。NetScaler 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。単一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 NetScaler Gateway アプライアンスで、認証およびリソースアクセスの要件が異なる複数のユーザーコミュニティにサービスを提供することができます。
- 認証、承認、監査。認証、承認、およびアカウンティングを構成して、セキュリティ保護されたネットワーク内の NetScaler Gateway または LDAP や RADIUS などの認証サーバーのいずれかで認識される資格情報を使

用して、ユーザーが NetScaler Gateway にログオンできるようにします。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されるリソースを決定します。認証と承認について詳しくは、「認証と承認の構成」を参照してください。監査サーバーは、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、NetScaler 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、NetScaler Gateway または外部サーバーに保存されます。監査について詳しくは、「NetScaler Gateway での監査の設定」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 NetScaler Gateway にログオンできます。
  - Windows 向け Citrix Secure Access クライアントは、Windows ベースのコンピューター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 Secure Access クライアント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 Secure Access クライアントでログオンします。Citrix Workspace アプリと Citrix Secure Access クライアント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 Secure Access クライアントを追加します。
  - macOS 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 macOS X 用の Citrix Secure Access クライアント。Windows 向け Citrix Secure Access クライアントと同じ特徴と機能を備えています。このプラグインバージョンのエンドポイント分析サポートを提供するには、NetScaler Gateway 10.1、ビルド 120.1316.e をインストールします。
  - 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可能にする Citrix Workspace アプリ。
  - Citrix Workspace アプリ、Secure Hub、WorxMail、および WorxWeb。ユーザーは、Citrix Endpoint Management でホストされている Web および SaaS アプリケーション、iOS および Android モバイルアプリ、および ShareFile データにアクセスできます。
  - ユーザーは、NetScaler Gateway 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、NetScaler 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 デバイスの 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、NetScaler Gateway 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、グローバルに、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、接続が NetScaler Gateway 経由で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。

NetScaler Gateway を構成するときに、ユーザーのログオン方法を構成するポリシーを作成できます。また、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 NetScaler Gateway を介して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。
- 仮想アダプター。NetScaler Gateway 仮想アダプターは、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 Secure Access クライアント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、NetScaler 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 Secure Access クライアントは、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。

  NetScaler 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を介して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インターセプトする場合、仮想アダプタは A および AAAA レコードタイプの DNS クエリをインターセプトし、他のすべての DNS クエリ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。インターネットとプライベート LAN (LAN) 接続はオープンで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

ユーザーは、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リモートの場所から接続できます。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 Secure Access クライアント
- Citrix Workspace アプリ
- WorxMail と WorxWeb
- Android と iOS のモバイルデバイス

Citrix Secure Access クライアントとの接続

Citrix Secure Access クライアントでは、次の手順で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ます。

1. ユーザーは、Web ブラウザーに Web アドレスを入力して、NetScaler Gateway に初めて接続します。ログオンページが表示され、ユーザーはユーザー名とパスワードの入力を求められます。外部認証サーバーが構成

されている場合、NetScaler 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、NetScaler 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 macOS X コンピューターの Web ブラウザーに NetScaler Gateway Web アドレスを入力すると、NetScaler Gateway は、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適用されているかどうかを確認します。セキュリティチェックは、ユーザーデバイスが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の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すると、NetScaler 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、ユーザーはログオン資格情報を入力できます。NetScaler Gateway 10.1、ビルド 120.1316.e をインストールすると、macOS 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. NetScaler Gateway がユーザーを正常に認証すると、NetScaler Gateway は VPN トンネルを開始します。NetScaler Gateway は、Windows 用 Citrix Secure Access クライアントまたは macOS X 用 Citrix Secure Access クライアントをダウンロードしてインストールするようにユーザーに求めます。
4. 認証後スキャンを構成すると、ユーザーが正常にログオンした後、NetScaler 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すると、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、ネットワークリソースへのユーザー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 NetScaler Gateway 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。NetScaler Gateway に含まれているホームページは、Access Interface と呼ばれます。ユーザーが Windows 向け Citrix Secure Access クライアント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、ユーザーデバイスは接続が確立されたことを示すメッセージが表示されます。ユーザーは、Microsoft Outlook を開いて電子メールを取得するなど、Access Interface を使用せずにネットワーク内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すると、NetScaler 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にある NetScaler Gateway アイコンを右クリックし、［ログオフ］をクリックすることで、アクティブなセッションを閉じることができます。また、非アクティブが原因でセッションが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、ブラウザーに NetScaler Gateway 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、Access Interface が表示され、そこからログオフできます。

注： Citrix Endpoint Management を内部ネットワークに展開する場合、内部ネットワークの外部から接続するユーザーは、最初に NetScaler 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 Citrix Endpoint Management でホストされている Web アプリケーション、SaaS アプリケーション、Android および iOS モバイルアプリ、および 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を介して、または Citrix Workspace アプリまたは Secure Hub を使用して、Citrix Secure Access クライアントに接続できます。

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。遠隔地から接続するには、ユーザーはデバイスに Citrix Secure Access クライアントもインストールします。Citrix Workspace アプリは、Citrix Secure Access クライアントをプラグインのリストに自動的に追加します。ユーザーが Citrix Workspace アプリにログオンすると、Citrix Secure Access クライアントにもログオンできます。また、ユーザーが Citrix Workspace アプリにログオンしたときに、Citrix Secure Access クライアントへのシングルサインオンを実行するように NetScaler Gateway を構成することもできます。

iOS および **Android** デバイスと接続する

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 で 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と、接続は NetScaler 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、接続はマイクロ VPN を自動的に使用します。さらに、
Secure Mail と WorxWeb は、マイクロ VPN を使用して、NetScaler Gateway を介した接続を確立します。NetScaler Gateway でマイクロ VPN を構成する必要はありません。

一般的な **NetScaler Gateway** の展開

February 1, 2024

NetScaler Gateway を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、内部ネットワークのリソースにアクセスする前に、NetScaler Gateway に接続する必要があります。

NetScaler 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内

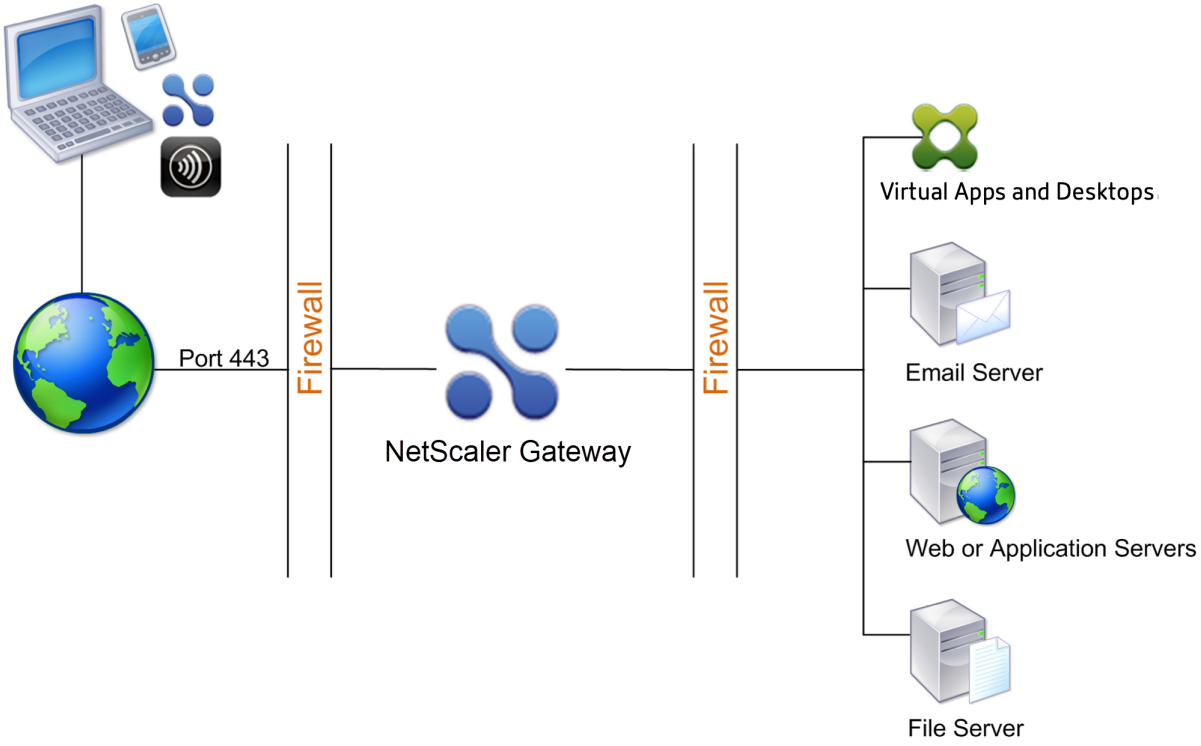
また、Citrix Virtual Desktops、Citrix Virtual Desktops、StoreFront、および Citrix Endpoint Management とともに NetScaler Gateway を展開して、ユーザーが Windows、Web、モバイル、および SaaS アプリケーションにアクセスできるようにすることもできます。展開環境に Citrix Virtual Apps、StoreFront、およびデスクトップ 7 が含まれている場合は、NetScaler Gateway をシングルホップまたはダブルホップ DMZ 構成で展開できます。ダブルホップ展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

NetScaler Gateway インストールをこれらのソリューションやその他のサポートされている NetScaler ソリューションで拡張する方法の詳細については、「NetScaler 製品との統合」トピックを参照してください 。

DMZ に NetScaler Gateway を展開する

多くの組織は DMZ で内部ネットワークを保護しています。DMZ は、組織のセキュア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 Windows 用の Citrix Secure Access または Citrix Workspace アプリに接続します。

図 1: DMZ に展開された NetScaler Gateway



前の図に示す構成では、DMZ に NetScaler 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 NetScaler Gateway 接続

DMZ に NetScaler 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 NetScaler 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。ユーザ接続が内部ネットワークに到達できるようにするには、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。

NetScaler Gateway は、ユーザーデバイスからの SSL 接続を復号化し、ユーザーに代わって 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

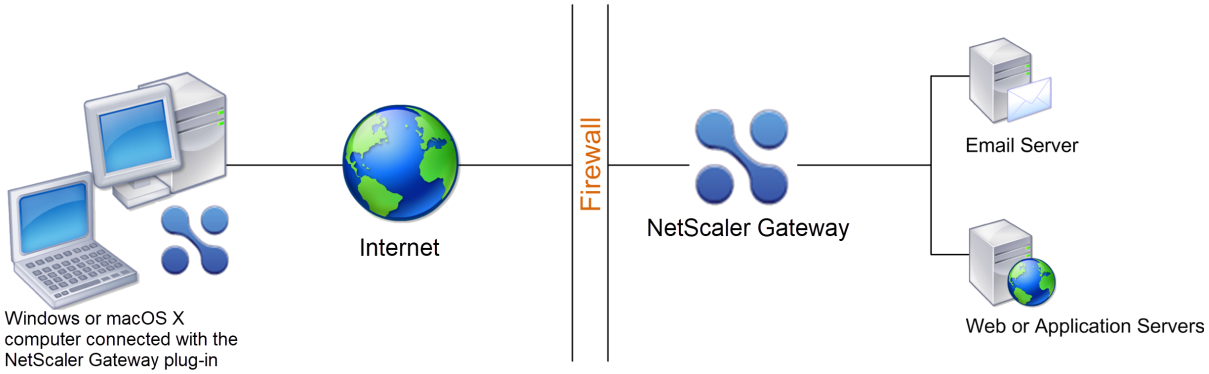
るポートは、外部ユーザーにアクセスを許可するネットワークリソースによって異なります。

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。NetScaler Gateway は、外部ユーザーデバイスに代わって、第 2 のファイアウォールを介して、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。

NetScaler Gateway を安全なネットワークに展開する

NetScaler 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立っています。NetScaler 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、ファイアウォールの内部に常駐します。

図 1: セキュリティで保護されたネットワークに展開された NetScaler Gateway



NetScaler 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ときは、NetScaler Gateway 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。NetScaler Gateway をセキュリティで保護されたネットワークに配置すると、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ます。この構成にはファイアウォールが 1 つしかないため、リモートロケーションから接続するユーザーの展開の安全性が低下します。NetScaler 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、トラフィックはユーザーが認証される前に安全なネットワークに入ります。NetScaler Gateway を DMZ に展開すると、ネットワークトラフィックがセキュリティで保護されたネットワークに到達する前にユーザーが認証されます。

NetScaler Gateway がセキュリティで保護されたネットワークに展開されている場合、Citrix Secure Access for Windows 接続は、NetScaler Gateway に接続するためにファイアウォールを通過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要件

April 1, 2024

NetScaler Gateway は、Citrix Secure Access クライアントを使用したユーザー接続をサポートします。ユーザ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 Secure Access クライアントを使用すると、ユーザーはアクセスを許可したネットワークリソースに接続できます。

エンドポイントポリシーが NetScaler Gateway 上で構成されている場合、NetScaler Gateway は、ユーザーがログオンしたときに Citrix EPA クライアントをユーザーデバイスに自動的にダウンロードしてインストールします。

Citrix Secure Access クライアントのシステム要件

Citrix Secure Access クライアントは、クライアントマシンから NetScaler 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、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ている。Web ブラウザーで NetScaler Gateway アプライアンスのセキュア URL を認証すると、プラグインがマシンに自動的にダウンロードされ、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の admin/root 権限が必要です。
> - Citrix Secure Access クライアントをサポートするブラウザは、クライアントレス VPN もサポートしています。

デスクトップアプリとしての Citrix Secure Access クライアントは、以下のオペレーティングシステムと Web ブラウザ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 リリース 30 以降、Mozilla Firefox リリース 30 以降
Windows 11	Google Chrome リリース 30 以降; Mozilla Firefox リリース 24 以降; Chromium 版 Edge
Windows 10 (x86 と x64)	Google Chrome リリース 30 以降; Mozilla Firefox リリース 24 以降; Chromium 版 Edge
Linux; Ubuntu 18.04 LTS、20.04 LTS、22.04 LTS。	Mozilla Firefox リリース 44 以降。Google Chrome 50 以降

> 注:
>
> 現在、Citrix Secure Access クライアントと Ubuntu 用 Citrix EPA クライアントは、デフォルトの GNOME ディスプレイマネージャーのみをサポートしています。

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 Secure Access クライアントは、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 7.0 以降
iOS	iOS 12.0 以降

> 注:
>
> macOS 14/iOS 17 以降などの最新の Apple OS バージョンを使用している場合は、Citrix Secure Access クライアント/Citrix SSO バージョン 23.09.1 以降にアップグレードすることをお勧めします。

エンドポイント分析の要件

NetScaler Gateway は、Citrix EPA クライアントをユーザーデバイスにインストールします。Citrix EPA クライアントは、NetScaler Gateway で構成し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します。要件には、オペレーティングシステム、ウイルス対策、Web ブラウザのバージョンなどの情報が含まれます。

ユーザーがブラウザーを使用して NetScaler Gateway に初めて接続すると、ポータルは Citrix EPA クライアントのインストールを要求します。その後ログオンを試みると、Citrix EPA クライアントはアップグレード制御構成を検証して、Citrix EPA クライアントのアップグレードが必要かどうかを確認します。必要に応じて、最新の Citrix EPA クライアントをダウンロードしてインストールするように求めるプロンプトがユーザーに表示されます。Windows 用 Citrix EPA クライアントは 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。macOS 向け Citrix EPA クライアントは、64 ビットアプリケーションとしてインストールされます。Citrix EPA クライアントのインストールまたは使用には、EPA を使用してデバイス証明書にアクセスする場合を除き、特別な権限は必要ありません。デバイス証明書認証に EPA を使用する方法の詳細については、「デバイス証明書を認証に使用する」を参照してください。

管理 UI コンソールのツールチップには、スキャンの詳細が説明されています。EPA ライブラリの詳細については、https://www.citrix.com/en-in/downloads/citrix-gateway/epa-libraries/を参照してください。

> 重要:
>
> - EPA をサポートするブラウザは、クライアントレス VPN もサポートしています。
> - 事前認証エンドポイント分析では、ユーザーが Endpoint Analysis プラグインをインストールしないか、スキャンをスキップした場合、ユーザーは Citrix Secure Access クライアントにログオンできません。
> - 認証後のエンドポイント分析では、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。
> - OPSWAT 関連のスキャンでは、クライアントマシンにバイナリパッケージ`epaPackage.exe`をインストールする必要があります。

Endpoint Analysis プラグインを使用するには、ユーザーデバイスで次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
macOS (10.9 以降)	Safari 7.1 以降、Google Chrome リリース 30 以降、Mozilla Firefox リリース 30 以降
Windows 11	Google Chrome リリース 30 以降; Mozilla Firefox リリース 24 以降; Chromium 版 Edge
Windows 10	Google Chrome リリース 30 以降; Mozilla Firefox リリース 24 以降; Chromium 版 Edge
Linux; Ubuntu 18.04 LTS、20.04 LTS、22.04 LTS。	Mozilla Firefox リリース 44 以降。Google Chrome 50 以降

注:

- 前述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。
- Windows 10 と Windows 11 の S モードはサポートされていません。
- Windows エディションの場合は、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。
- Mozilla Firefox バージョンでは、エンドポイント分析をプラグイン対応にする必要があります。最低限必要なバージョンは 3.0 です。

NetScaler Gateway と NetScaler 製品の互換性

April 1, 2024

次の表は、NetScaler Gateway 13.1 と互換性のある NetScaler 製品およびバージョンを示しています。

> 注:
>
> NetScaler Gateway の機能は、NetScaler VPX で利用できます。

NetScaler 製品およびサポート対象バージョン

NetScaler 製品	リリースバージョン
Citrix SD-WAN	10.2, 11.0
NetScaler プラットフォーム	FIPS 準拠のアプライアンスを含む、現行のすべての MPX および VPX モデル。
StoreFront	現在サポートされているすべての StoreFront バージョン。
Citrix Virtual Apps and Desktops	7.15、1808、1811、1903、1906、1909、2003、2009、2112、1912 LTSR、2203 LTSR
XenMobile	10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12

Citrix Workspace アプリ、**Citrix** 業務用モバイル アプリ、プラグイン

* 各ソフトウェアリリースで最初にサポートされているビルドを次の表に示します。特に指定がない限り、以降のビルドはすべてサポートされます。リリースライフサイクルの詳細については、「製品マトリックス」を参照し てください。

Citrix Workspace アプリまたはプラグイン	最低サポートバージョン *
macOS X 用 Citrix Secure Access クライアント	3.1.8
Windows 用 Citrix Secure Access クライアント	12.0
iOS 用 Citrix Secure Access クライアント	3.1.4
Android 用 Citrix Secure Access クライアント	2.0.14
Android 向け Citrix Workspace アプリ	3.11
iOS 向け Citrix Workspace アプリ	7.1.3
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

Citrix Workspace アプリまたはプラグイン	最低サポートバージョン *
Chrome 向け 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

> 注:
>
> - 各 VPN クライアントでサポートされている一般的に使用される機能について詳しくは、「NetScaler Gateway VPN クライアントとサポートされる機能」を参照してください。

NetScaler Gateway ライセンス

February 1, 2024

NetScaler Gateway をインストールすると、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 Citrix から取得できます。Citrix 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ある場合は、NetScaler Gateway にアップロードします。Citrix ライセンスについて詳しくは、「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設定してから、アプライアンスを再起動してください。

ライセンスを取得するには、NetScaler ライセンスのアクティベーション、アップグレード、および管理 Web ページにアクセスしてください 。このページでは、新しいライセンスを取得し、NetScaler ライセンスのアクティベーション、アップグレード、管理を行うことができます。

重要:

> - NetScaler Gateway にライセンスをインストールする必要があります。アプライアンスは NetScaler ライセンスサーバーからライセンスを取得しません。
> - 受け取ったすべてのライセンスファイルのローカルコピーを保持する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。NetScaler 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。

NetScaler 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、NetScaler Gateway を再起動します。セットアップウィザードを使用して、ホスト名を設定します。NetScaler Gateway のユニバーサルライセンスを生成すると、ホスト名がライセンスで使用されます。

NetScaler Gateway ライセンスの種類

NetScaler 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 プロキシを使用した Citrix Virtual Apps、Citrix Virtual Desktops、または StoreFront への接続を無制限に許可します。Citrix Secure Access クライアント、SmartAccess ログオンポイント、または Secure Hub、WorxWeb、または Secure Mail からネットワークへの 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。NetScaler 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、次の NetScaler Gateway バージョンでサポートされています。

- NetScaler 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
- NetScaler VPX

> 重要：受信するすべてのライセンスファイルのローカルコピーを保持する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。NetScaler 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 Citrix Virtual Desktops への無制限のユーザー接続を許可します。Citrix Receiver を使用した接続では、NetScaler Gateway ユニバーサルライセンスは使用されません。これらの接続には、Platform ライセンスのみが必要です。プラットフォームライセンスは、物理または仮想を問わず、すべての新しい NetScaler Gateway 注文とともに電子的に提供されます。保証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、Citrix 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。

ユニバーサル・ライセンス

NetScaler Gateway ユニバーサルライセンスは、同時ユーザーセッションの数を購入したライセンスの数に制限します。100 個のライセンスを購入した場合、いつでも 100 の同時セッションを使用できます。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に対して解放されます。複数のコンピューターから NetScaler 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、管理者が構成ユーティリティを使用してセッションを終了するまで、追加の接続を開くすることはできません。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ます。

NetScaler 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。

- ライセンスアクセスコード (ライセンスキー) が電子メールで届きます。
- セットアップウィザードを使用して、ホスト名で NetScaler Gateway を構成します。
- NetScaler Gateway のライセンスは、Citrix の Web サイトから割り当てます。割り当てプロセス中にホスト名を使用して、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 NetScaler Gateway にインストールします。

ユニバーサルライセンスは、次の機能をサポートしています。

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

ユニバーサルライセンスの取得　ユニバーサルライセンスの Citrix Web サイトにアクセスする前に、次の情報が必要です。

- Citrix アカウントのユーザー ID とパスワード。

  Citrix Web サイト（https://www.citrix.com/welcome/create-account/）で登録して、ユーザー ID とパスワードを受け取ります。
  注：ライセンスコードまたはユーザー ID とパスワードが見つからない場合は、Citrix カスタマーサービスに連絡してください。

- NetScaler Gateway のホスト名

  Citrix Web サイトのこの名前の入力フィールドでは大文字と小文字が区別されるため、NetScaler ADC アプライアンスで構成されているとおりにホスト名をコピーしてください。

- ライセンスファイルに含めるライセンスの数

使用できるライセンスのすべてを一度にダウンロードする必要はありません。たとえば、100 ライセンスを購入した場合は、50 ライセンスをダウンロードできます。残りは後で別のライセンスファイルに割り当てることができます。
NetScaler Gateway には複数のライセンスファイルをインストールできます。

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

ユニバーサルライセンスを取得するには

1. Citrix の資格情報を使用して Citrix Web サイト（https://www.citrix.com/en-in/account/）にログインします。
2.「**Citrix Manage Licenses** はここにあります」で、指示に従ってライセンスファイルを取得します。

ユニバーサルライセンスのインストール　ライセンスをインストールするには、「ライセンスのインストール」を参照してください。インストール後、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ます。

ユニバーサルライセンスのインストールの確認　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ます。

CLI 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、NetScaler ADC アプライアンスへの SSH 接続を開きます。
2. 管理者の資格情報を使用して NetScaler ADC アプライアンスにログオンします。
3. show license コマンドを使用して、「SSL VPN = YES」と最大ユーザ数が 5 から予想される同時ユーザ数に増加していることを確認します。

GUI 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. Web ブラウザーで、NetScaler アプライアンスの IP アドレス（`http://192.168.100.1`など）を入力します。
2. [User Name] ボックスと [Password] ボックスに管理者資格情報を入力します。
3. ナビゲーションペインで、[System] を展開し、[Licenses] をクリックします。
4. [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 NetScaler Gateway ユーザーの最大数] フィールドには、NetScaler ADC アプライアンスでライセンスされている同時ユーザーセッションの数が表示されます。

関連情報

- Citrix ライセンスシステム

- NetScaler データシート
- NetScaler ADC および NetScaler Gateway ライセンスの種類

NetScaler Gateway にライセンスをインストールする

February 1, 2024

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、NetScaler 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 NetScaler Gateway の初期設定を構成した場合は、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、追加の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. 詳細ペインで、[**Manage Licenses**] 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、NetScaler Gateway を再起動する必要があることを示す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

アプライアンスにライセンスをインストールしたら、アプライアンスへの接続を許可す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、[**NetScaler 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は、ライセンスファイルに含まれているライセンスの数に対応しています。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総数以下である必要があります。たとえば、100 ユーザーライセンスを含むライセンスと 400 ユーザーライセンスを含むもう一つのライセンスをインストールするとします。ライセンスの総数は 500 になります。その場合、ログオンできるユーザーの最大数は 500 人以下です。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と、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を確認する

先に進む前に、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。

GUI 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、NetScaler 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 NetScaler 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ている同時ユーザーセッションの数が表示されます。

CLI 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、; と入力します。

```
1 show license
2 <!--NeedCopy-->
```

SSL VPN パラメータが Yes に等しく、最大ユーザ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。

NetScaler Gateway ライセンスに関するよくある質問

February 1, 2024

トライアルライセンスまたはデモライセンスのサポートを受けるにはどうすればよいですか

現在、NetScaler 製品の多くは、専門家による包括的でプライベートな 1 対 1 のデモ体験として提供されています。Citrix エキスパートが、お客様のニーズ、ユースケース、アクティブなプロジェクトに合わせてデモをカスタマイズします。ダウンロード、ライセンス、インストールは不要です。インスタントデモを見るには最小限の設定が必要です。デモの後、サービスに適用される Citrix ソリューションの概念実証または試用を進めるには、Citrix 専門家にお問い合わせください。デモの場合は、https://demo.citrix.com/をクリックします。

ライセンスをインストールするには

ライセンスのインストールについて詳しくは、「NetScaler Gateway にライセンスをインストールするには」を参照してください。

Gateway ライセンスにはどのような種類がありますか

プラットフォームライセンスでは、ICA プロキシを使用した Citrix Virtual Apps、Citrix Virtual Desktops、または StoreFront への接続を無制限に許可します。
ユニバーサルライセンスは、NetScaler ADC プラットフォームライセンスの上にあるアドオンライセンスです。これにより、Citrix Secure Access クライアント、SmartAccess ログオンポイント、または Secure Hub、Secure Web、または Secure Mail からネットワークへの VPN 接続が可能になります。詳しくは、「NetScaler Gateway ライセンスの種類」を参照してください。

サポートされる同時ユーザーセッションはいくつありますか

サポートされるセッションは、ゲートウェイライセンスタイプによって異なります。詳しくは、「NetScaler Gateway ライセンスの種類」を参照してください。

考慮すべきもう 1 つの要素は、基盤となるハードウェア自体の容量です。パフォーマンスに関する考慮事項については、NetScaler MPX/SDX データシートまたは CitrixADC VPX データシートを参照してください 。

現在の同時ユーザーセッションのライセンスを確認するにはどうすればよいですか**?**

構成ユーティリティの [構成] タブで、[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、NetScaler 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 **NetScaler 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ている同時ユーザーセッションの数が表示されます。

ライセンスされたスループット制限に達しているかどうかを確認する方法

リアルタイムスループットは、newnslogを使用して抽出できます。たとえば、ライセンススループットが 500 Mbps の場合、次のコマンドを使用して 500 を超えるリアルタイムスループットを抽出できます。

```
1 nsconmsg -K newnslog -g mbits -d past -s disptime=1 -s ratecount=500 |
     more
2 <!--NeedCopy-->
```



```
reltime:mili second between two records Mon Feb  5 13:47:13 2018
 Index    rtime totalcount-val      delta rate/sec symbol-name&device-no&time
    12     7000      801130681       3701      528 allnic_tot_rx_mbits  Mon Feb  5 13:47:55 2018
    13        0      460776045       3682      526 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:47:55 2018
    14     7000      801134437       3756      536 allnic_tot_rx_mbits  Mon Feb  5 13:48:02 2018
    15        0      460779784       3739      534 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:02 2018
    16     7000      801138166       3729      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:09 2018
    17        0      460783497       3713      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:09 2018
    18     7000      801141896       3730      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:16 2018
    19        0      460787213       3716      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:16 2018
    20     7000      801145623       3727      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:23 2018
    21        0      460790929       3716      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:23 2018
    22     7000      801149353       3730      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:30 2018
    23        0      460794646       3717      531 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:30 2018
    24     7000      801153067       3714      530 allnic_tot_rx_mbits  Mon Feb  5 13:48:37 2018
    25        0      460798342       3696      528 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:37 2018
```

ライセンススループットに達するとパケットがドロップされるかどうかを確認する方法

次のコマンドを使用して、パケットがドロップされているかどうかを確認できます。

```
nsconmsg -K newnslog -d current -g nic_err_rl_pkt_drops -s disptime=1 |
    more
<!--NeedCopy-->
```

```
reltime:mili second between two records Fri Feb  2 00:12:38 2018
 Index    rtime     totalcount-val      delta rate/sec symbol-name&device-no&time
     0 1966993        23723602        478       68 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:38 2018
     1        0        48048402        465       66 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:38 2018
     2        0      8307679782     145475    20782 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:38 2018
     3     7000        23723933        331       47 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:45 2018
     4        0        48048712        310       44 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:45 2018
     5        0      8307787105     107323    15331 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:45 2018
     6     7000        23723941          8        1 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:52 2018
     7        0        48048735         23        3 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:52 2018
     8        0      8307811163      24058     3436 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:52 2018
```

NetScaler ADC アプライアンスのライセンスされたスループットはどのようにして調べることができますか**?**

CLI から`show license`コマンドを実行し、モデル番号を使用して、ADC またはゲートウェイ MPX、SDX、および VPX のデータシートからスループットを取得します。


```
> sh license
        License status:
                              Web Logging: YES
                        Surge Protection: YES
                          Load Balancing: YES
                       Content Switching: YES
                       Cache Redirection: YES
                             Sure Connect: YES
                     Compression Control: YES
                       Delta Compression: NO
                        Priority Queuing: YES
                          SSL Offloading: YES
           Global Server Load Balancing: YES
                          GSLB Proximity: YES
                    Http DoS Protection: YES
                        Dynamic Routing: YES
                      Content Filtering: YES
                     Integrated Caching: YES
                                SSL VPN: YES   (Maximum users = 5)   (Maximum ICA u
sers = 0)
                                    AAA: YES
                             OSPF Routing: YES
                              RIP Routing: YES
                              BGP Routing: YES
                                  Rewrite: YES
                IPv6 protocol translation: YES
                     Application Firewall: YES
                                Responder: YES
                           HTML Injection: YES
                           NetScaler Push: YES
                    Web Interface on NS: YES
                                AppFlow: YES
                              CloudBridge: YES
                         Model Number ID: 5500
 Done
> 
```

CITRIX

Citrix NetScaler | Datasheet

NetScaler platform	MPX 9500	MPX 7500	MPX 5500	VPX 10/200/1000/3000
Platform attributes				
Processor	Intel Xeon L5410 (4 cores total)	Intel Xeon L5410 (4 cores total)	Intel Xeon E5205 (2 cores total)	Minimum Server Req.:[1] Dual core server with Intel® VTx or AMD-V™
Memory	8 GB	8 GB	4 GB	
Ethernet ports	8x 10/100/1000 BASE-T OR 4x 10/100/1000 BASE-T AND 4x 1000BASE-X SFP (fiber or copper)	8x 10/100/1000 BASE-T OR 4x 10/100/1000 BASE-T AND 4x 1000BASE-X SFP (fiber or copper)	4x 10/100/1000 BASE-T	• Citrix® XenServer® 5 (update 3 or better) • Windows Server 2008 R2 with Hyper-V role • VMWare ESX/ESXi 3.5 or higher • 4G RAM/20 GB hard drive • Hypervisor supported NIC
Transceivers support	SX, LX	SX, LX		
Software upgradable performance		Upgrade option to MPX 9500		Upgrade options to VPX 200, VPX 1000 and VPX 3000
Platform performance				
System throughput, Gbps	3	1	0.5	Up to 3.0[2]
HTTP requests/sec	200,000	100,000	50,000	Up to 100,000
SSL transactions/sec	20,000	10,000	5,000	Up to 500
SSL throughput, Gbps	3	1	0.5	Up to 1.0
Compression throughput, Gbps	2	1	0.5	Up to 0.75
SSL VPN: concurrent users	10,000	10,000	5,000	Up to 300[3]

既存の **Gateway** ライセンスにユーザーを追加するにはどうすればよいですか**?**

追加のユニバーサルライセンスをインストールできます。たとえば、100 のユーザライセンスを含む 1 つのユニバーサルライセンスをインストールしたとします。400 のユーザライセンスを含む 2 つ目のユニバーサルライセンスをインストールすると、ユーザライセンスの総数は 500 になります。

開始する前に

April 1, 2024

NetScaler 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、ユーザーが接続でき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があります。

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。NetScaler Gateway は、以下の NetScaler 製品と互換性があります。

- Citrix Endpoint Management
- Citrix Virtual Apps
- Citrix Virtual Desktops
- StoreFront
- Web Interface
- Citrix SD-WAN

NetScaler Gateway の展開について詳しくは、「[一般的な展開と NetScaler 製品との統合](/ja-jp/netscaler-gateway/13-1/common-deployments.html)」を参照してください。

アクセス戦略を準備するには、次の予備的な手順を実行します。

- リソースを特定する。リスク分析で定義した 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、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開発する。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 Secure Access クライアントで完全な VPN アクセスを提供し、ユーザーは Citrix Workspace アプリまたは Secure Hub を使用してログオンするか、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、ユーザーが公開アプリケーションを使用してドキュメントを変更できるか、ファイル共有に接続してドキュメントを変更できるかを指定できます。

- 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。NetScaler 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された条件を満たすときに適用されます。条件は、作成したアクセスシナリオに基づいて決定します。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り、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。

このセクションでは、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ています。
- 必要になる可能性がある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。
- NetScaler 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チェックリスト。

NetScaler Gateway をインストールするための前提条件

NetScaler 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。

- NetScaler 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。NetScaler Gateway は、DMZ またはファイアウォールの背後にある内部ネットワークに展開されています。また、ダブルホップ DMZ で NetScaler 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。
- NetScaler Gateway をデフォルトゲートウェイまたは内部ネットワークへの静的ルートで構成し、ユーザーがネットワーク内のリソースにアクセスできるようにします。NetScaler 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。
- 認証と認可に使用される外部サーバは設定され、実行されています。詳細については、「認証と承認」を参照してください。
- ネットワークには、正しい NetScaler Gateway ユーザー機能を提供するための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 Secure Access クライアントとのユーザー接続用のユニバーサルライセンスを Citrix の Web サイトからダウンロードしました。これで、ライセンスを NetScaler Gateway にインストールする準備ができました。
- NetScaler Gateway には、信頼できる認証局（CA）によって署名された証明書があります。詳しくは、「Installing and Managing Certificates」を参照してください。

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

セキュリティの計画

NetScaler Gateway の展開を計画するときは、証明書、および認証と承認に関連する基本的なセキュリティ問題を理解する必要があります。

セキュアな証明書管理を構成する

デフォルトでは、NetScaler Gateway には、アプライアンスが SSL ハンドシェイクを完了できるようにする自己署名セキュアソケットレイヤー（SSL）サーバー証明書が含まれています。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、NetScaler では本番環境での使用は推奨していません。NetScaler Gateway を実稼働環境に展開する前に、既知の認証局（CA）から署名付き SSL サーバー証明書を要求して受信し、NetScaler Gateway にアップロードすることをお勧めします。

NetScaler Gateway が SSL ハンドシェイクでクライアントとして動作する必要がある環境（別のサーバーとの暗号化された接続を開始する）に NetScaler Gateway を展開する場合は、NetScaler Gateway にも信頼されたルート証明書をインストールする必要があります。たとえば、Citrix Virtual Apps と Web Interface を備えた NetScaler Gateway を展開する場合、NetScaler 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、NetScaler Gateway に信頼されたルート証明書をインストールする必要があります。

認証サポート

ユーザーを認証し、内部ネットワーク上のネットワークリソースに対するユーザーのアクセス（または承認）のレベルを制御するように NetScaler Gateway を構成できます。

NetScaler Gateway を展開する前に、ネットワーク環境に次の認証タイプのいずれかをサポートするためのディレクトリと認証サーバーが配置されている必要があります。

- 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 構成の RSA
- SAML 認証

環境がこれら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人口が少ない場合は、NetScaler Gateway でローカルユーザーのリストを作成できます。次に、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 NetScaler Gateway を構成できます。この構成では、ユーザーアカウントを別の外部ディレクトリに保持する必要はありません。

NetScaler Gateway 展開環境のセキュリティ保護

展開が異なれば、セキュリティに関する考慮事項も異なる場合があります。NetScaler の安全な導入ガイドラインは、特定のセキュリティ要件に基づいて適切な安全な導入を決定するのに役立つ一般的なセキュリティガイダンスを提供します。

詳しくは、「NetScaler 安全な展開ガイドライン」を参照してください。

ゲートウェイのインストール前チェックリスト

February 1, 2024

チェックリストは、NetScaler 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リストで構成されています。

各タスクを完了してメモを作成すると、各タスクをチェックオフできる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 NetScaler 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。

NetScaler Gateway をインストールおよび構成する手順については、「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 Secure Access 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特定します。注: 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。

NetScaler 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。

- NetScaler Gateway 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た署名付きサーバー証明書に含まれています。
- Citrix Web サイトからユニバーサルライセンスを取得する
- 証明書署名要求 (CSR) を生成し、認証局 (CA) に送信します。CSR を認証局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。NetScaler Gateway に付属するデフォルトのパスワードは`nsroot`です。
- NetScaler Gateway がセキュリティで保護されたユーザー接続をリッスンするポート番号を書き留めます。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で開いている必要があります。
- デフォルトゲートウェイの 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 サーバを直接追加する場合は、アプライアンスで ICMP（ping）も設定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）。

NetScaler 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 NetScaler Gateway を介して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
- Citrix Secure Access クライアントを使用して NetScaler Gateway 経由で接続するときに、ユーザーがアクセスする必要の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

2 つの NetScaler Gateway アプライアンスがある場合は、1 つの NetScaler Gateway が接続を受け入れて管理し、2 番目の NetScaler Gateway が最初のアプライアンスを監視する高可用性構成でそれらを展開できます。最初の NetScaler Gateway が何らかの理由で接続の受け入れを停止した場合、2 番目の NetScaler 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。

- NetScaler Gateway ソフトウェアのバージョン番号を書き留めます。
- バージョン番号は、両方の NetScaler Gateway アプライアンスで同じである必要があります。
- 管理者パスワードを書き留めます (`nsroot`)。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 NetScaler Gateway 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 NetScaler Gateway 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します。
- RPC ノードのパスワードを書き留めます。

認証と承認

NetScaler Gateway は、さまざまな組み合わせで使用できるいくつかの異なる認証および承認タイプをサポートしています。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 サーバが含まれている場合は、認証に LDAP を使用できます。

- 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、デフォルトのポートは 389 です。LDAP サーバーへの接続を SSL で暗号化する場合、デフォルトのポートは 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構成できます。

- 管理者バインド DN を書き留めます。

  LDAP サーバーで認証が必要な場合は、NetScaler Gateway が LDAP ディレクトリにクエリを実行するときに認証に使用する必要がある管理者 DN を入力します。例として、cn= 管理者、cn=Users、dc=ace、dc=com がある。

- 管理者パスワードを書き留めます。

  パスワードは、管理者バインド DN に関連付けられています。

- ベース DN を書き留めます。

  ユーザが配置されている DN（またはディレクトリレベル）。たとえば、ou=users、dc=ace、dc=com などです。

- サーバ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 ディレクトリのユーザーオブジェクト属性を入力します。デフォルトは sAMAccountName です。Active Directory を使用していない場合、この設定の一般的な値は 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 認証の設定を参照してください。

- グループ属性を書き留めます。
  ユーザが属するグループを指定する LDAP ディレクトリの Person 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、NetScaler 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。

- サブ属性名を書き留めます。

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、SafeWord、Gemalto Protiva 製品が含まれる。

- 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ディングのタイプ（PAP、CHAP、MS-CHAP v1、MSCHAP v2）を書き留めます。

SAML 認証

セキュリティアサーションマークアップ言語 (SAML) は、ID プロバイダ (IdP) とサービスプロバイダ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。

- NetScaler Gateway にセキュアな IdP 証明書を取得してインストールします。
- リダイレクト URL を書き留めます。
- ユーザー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てポートを開く（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 NetScaler 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 NetScaler 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** の間のファイアウォール上

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

- 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。NetScaler 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セキュリティで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。

  NetScaler 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 のポートを書き留めます。
- NetScaler Gateway を Citrix Virtual Apps and Desktops で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

NetScaler Gateway を展開して、Web Interface または StoreFront を介して Citrix Virtual Apps and Desktops へのアクセスを提供する場合は、次のタスクを実行します。この展開では、Citrix Secure Access クライアントは必要ありません。ユーザーは、Web ブラウザーと Citrix Receiver のみを使用して、NetScaler Gateway を介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。

- 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 インターフェイスの場合のみ）。

Citrix Endpoint Management

内部ネットワークに Citrix Endpoint Management を展開する場合は、次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、および SaaS アプリにアクセスする前に NetScaler Gateway に接続する必要があります。

- Endpoint Management 完全修飾ドメイン名または 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

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ために、ダブルホップ DMZ 構成で 2 つの NetScaler Gateway アプライアンスを展開する場合は、次のタスクを実行します。

最初の DMZ の NetScaler 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セキュリティ保護されてい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 から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 NetScaler Gateway に接続します。最初の DMZ に NetScaler 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 NetScaler Gateway のこのチェックリストの「NetScaler Gateway の基本ネットワーク接続」セクションの項目を完了します。

  これらの項目を完了すると、インターフェイス 0 はこの NetScaler 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 NetScaler Gateway を 2 番目の DMZ の NetScaler 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。

  NetScaler Gateway をダブルホップ DMZ の最初のホップとして構成するには、最初の DMZ のアプライアンスの 2 番目の DMZ で NetScaler 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で NetScaler Gateway プロキシが構成されるタイミングを指定したら、NetScaler 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書き留めます。

  NetScaler Gateway をダブル DMZ の最初のホップとして構成するには、2 番目の DMZ の NetScaler Gateway が接続をリッスンする接続プロトコルと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 を使用した SOCKS（デフォルトポート 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く必要があります。

2 番目の **DMZ** の **NetScaler Gateway**

2 番目の DMZ は、内部のセキュア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 NetScaler 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 NetScaler Gateway のこのチェックリストの「NetScaler Gateway 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 は、最初の DMZ でこの NetScaler Gateway を NetScaler Gateway に接続します。インターフェイス 1 は、この NetScaler Gateway をセキュリティで保護されたネットワークに接続します。

NetScaler Gateway アプライアンスのインストールと構成

February 1, 2024

NetScaler 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、指示に従ってサーバラックが配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、アプライアンスをネットワーク、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後、初期設定を行い、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。

NetScaler VPX 仮想アプライアンスをインストールするときは、まず仮想アプライアンスイメージを取得し、ハイパーバイザー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。

NetScaler Gateway アプライアンスを構成する前に、設定を記録できるように、NetScaler Gateway インストール前チェックリストのトピックを使用することをお勧めします 。チェックリストには、NetScaler 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。

ウィザードを使用して **NetScaler Gateway** アプライアンスを構成する

April 1, 2024

NetScaler Gateway には、アプライアンスの設定を構成するために使用できる次の 6 つのウィザードがあります。

- NetScaler 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。
- クイック構成ウィザードを使用すると、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。
- NetScaler Gateway ウィザードでは、NetScaler Gateway 固有の設定を構成できます。
- セットアップウィザードを使用すると、NetScaler Gateway の基本的な設定を初めて構成できます。
- Citrix Endpoint Management の統合構成は、NetScaler Gateway および Citrix Endpoint Management 環境の構成に役立ちます。
- 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

NetScaler Gateway アプライアンスの初期設定のインストールと構成を完了し、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をインストールしていない。
- サブネットまたはマッピング IP アドレスが設定されていません。
- アプライアンスのデフォルトの IP アドレスが 192.168.100.1 の場合。

初回セットアップウィザードで **NetScaler Gateway** を構成する

NetScaler 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用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 NetScaler 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ます。NetScaler Gateway アドレスと 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します。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、NetScaler Gateway アプライアンスの次の基本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 サーバのアドレスを指定すると、ローカルコンピュータ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）またはライセンスキー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ー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、NetScaler Gateway でアプライアンスを再起動するように求められます。アプライアンスに再度ログオンすると、他のウィザードおよび構成ユーティリティを使用して他の設定を構成できます。

クイック構成ウィザード

クイック構成ウィザードを使用すると、NetScaler Gateway で複数の仮想サーバーを構成できます。仮想サーバを追加、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すると、次の展開をシームレスに構成できます。

- Secure Ticket Authority（STA）の複数のインスタンスを構成できる、Citrix Virtual Apps and Desktops への Web Interface 接続
- Citrix Endpoint Management のみ
- StoreFront のみ
- Citrix Endpoint Management と StoreFront を一緒に

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、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ト
- LDAP サーバ
- RADIUS サーバー
- 証明書
- DNS サーバー
- Citrix Endpoint Management および Citrix Virtual Apps and Desktops

  注：SSO を有効にするには、セッションアクションの［**NetScaler Gateway** セッションプロファイルの作成］**>**［クライアントエクスペリエンス］タブの［**Web** アプリケーションへのシングルサインオン］オプションを手動で有効にする必要があります。

NetScaler Gateway は、Citrix Endpoint Management への直接ユーザー接続をサポートしています。これにより、ユーザーは ShareFile へのアクセスとともに、Web、SaaS、およびモバイルアプリにアクセスできます。また、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と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。

- Receiver、Receiver for Web、Citrix Secure Access クライアント、および Program Neighborhood Agent のポリシーとプロファイルを含むセッションポリシー
- クライアントレスアクセス
- LDAP および RADIUS 認証

クイック構成ウィザードで設定を構成する

NetScaler Gateway の設定を構成して、Citrix Endpoint Management、StoreFront、または Web Interface との通信を有効にするには、クイック構成ウィザードを使用します。構成が完了すると、ウィザードにより、NetScaler Gateway、Endpoint Management、StoreFront、または Web Interface 間の通信に関する正しい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、ポリシーは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、NetScaler 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、モバイルアプリにアクセスできます。その後、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、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ト
- 証明書
- LDAP サーバ
- 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認証をサポートしています。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、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、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、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属性**]** フィールドで **samAccountName** を使用するポリシーを **1** つ構成し、**[**** サーバーログオン名属性] フィールドでユーザープリンシパル名 (UPN) を使用する 2 つ目の 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、NetScaler 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。詳細については、LDAP 認証の設定を参照してください。

次の方法を使用して、NetScaler Gateway の証明書をクイック構成ウィザードで構成できます。

- 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。

- NetScaler Gateway のログオンページを表示し、［展開の種類］で［**NetScaler 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した場合、[ホーム] タブは表示されません。
- Citrix **Gateway** の詳細ペインの［**NetScaler Gateway** の作成/監視］リンクから。このリンクは、NetScaler ADC 機能を有効にするライセンスをインストールすると表示されます。アプライアンスのライセンスを NetScaler Gateway 専用にした場合、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、ウィザードをもう一度実行して、さらに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 NetScaler 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ものと同じ IP アドレスは使用できません。たとえば、ポート番号が 80 の IP アドレス 192.168.10.5 の仮想サーバーがあるとします。クイック構成ウィザードを実行して、ポート番号 443 の IP アドレス 192.168.10.5 を持つ 2 番目の仮想サーバーを作成します。設定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、次のいずれかを実行します。
   a) アプライアンスに NetScaler 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 NetScaler ADC 機能を含めるための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［**NetScaler Gateway** ］をクリックし、詳細ペインの［はじめに］の下の［エンタープライズストアの **NetScaler Gateway** の構成］をクリックします。
2. ダッシュボードで、［新しい **NetScaler Gateway** の作成］をクリックします。
3. **NetScaler Gateway** 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に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] の [キーの選択] で、[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。

ネットワーク設定と認証設定の構成が完了したら、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の設定を構成する　NetScaler Gateway は、Web、SaaS、モバイルアプリ、および ShareFile へのユーザーアクセスを Endpoint Management 経由でのみサポートしています。StoreFront または Web Interface も展開する場合、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 一緒に
- Web インターフェイスのみ

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 統合設定] ページから開始します。

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 の設定を変更することはできません。

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、ウィザードは設定を構成せずに Web インターフェイスを自動的に選択します。この状況が発生した場合、Web Interface を構

成するための仮想サーバーの詳細を編集できますが、Citrix Endpoint Management に切り替えることはできません。切り替えるには、新しい仮想サーバーを作成する必要があり、構成中にウィザードをキャンセルしてはいけません。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** 完全修飾ドメイン名] 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 Path** では、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. 安全なユーザー接続には **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 の公開アプリケーションまたは Citrix Virtual Desktops の仮想デスクトップへのアクセスを提供する場合は、[**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 NetScaler Gateway を介して StoreFront に接続すると、ユーザーは Receiver for Web または Receiver のいずれかからアプリケーションおよび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. [アプリコントローラーの **FQDN**] に、Endpoint Management の FQDN を入力します。
3. [完了] をクリックします。

Web インターフェイスの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** インターフェイス] を選択し、次の項目を構成します。
    a) **Citrix Virtual Apps** サイト **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 Services** サイト **URL**」に、**Citrix Workspace** アプリパスを含む **Web** インターフェイスの完全な **IP** アドレスまたは完全修飾ドメイン名（FQDN）を入力します。デフォルト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] に、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。

NetScaler Gateway ウィザード

NetScaler 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ー
- 認証
- 承認
- ポートリダイレクト
- 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

NetScaler Gateway ウィザードを使用して設定を構成する

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

NetScaler 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、NetScaler Gateway ウィザードを使用するときに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。NetScaler Gateway をユーザーに公開する前に、署名付き証明書を取得することをお勧めします。

注：NetScaler Gateway ウィザード内から証明書署名要求（CSR）を作成できます。NetScaler 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、証明機関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。証明書の詳細については、「証明書のインストールと管理」を参照してください。

仮想サーバーを構成するときに、NetScaler 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。ユーザー接続に IPv6 を使用する方法の詳細については、「ユーザー接続用の IPv6 の構成」を参照してください。

NetScaler 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［NetScaler Gateway］をクリックします。
2. 詳細ペインの［はじめに］で、［NetScaler 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。

セットアップウィザード

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
- マップされた 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 Web サイトからライセンスをダウンロードしてください。詳しくは、「
NetScaler Gateway のライセンス」を参照してください。

公開アプリケーションウィザード

公開アプリケーションウィザードを使用して、内部ネットワークで Citrix Virtual Apps and Desktops を実行しているサーバーに接続するように NetScaler 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。

- サーバーファームに接続する仮想サーバーを選択します。
- 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 NetScaler Gateway を構成する方法の詳細については、「Web Interface を介した公開アプリケーションおよび仮想デスクトップへのアクセスの提供」を参照してください。

統合された **Citrix Endpoint Management** 構成

Citrix Endpoint Management MDM を使用して NetScaler Gateway を展開すると、スケーリング、アプリの高可用性の確保、セキュリティの維持が可能になります。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、次の項目が作成されます。

- デバイスマネージャ用の負荷分散サーバー。
- 電子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 の負荷分散サーバー。

統合 Citrix Endpoint Management 構成を使用した設定の作成について詳しくは、「Citrix Endpoint Management 環境の設定を構成する」を参照してください

NetScaler Gateway の構成

February 1, 2024

NetScaler 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含まれます。

- 仮想サーバー。NetScaler Gateway で複数の仮想サーバーを構成できます。これにより、実装する必要が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、グループのメンバー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、ユーザーを内部ネットワークのネットワークリソースに制限できます。次の方法を使用して、仮想サーバーを作成できます。
  - クイック構成ウィザード
  - NetScaler 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 NetScaler Gateway アプライアンスを展開すると、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セッションに影響を与えることなく引き継ぐことができます。
- 証明書。証明書を使用して、NetScaler 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。NetScaler Gateway は、ローカル LDAP、RADIUS、SAML、クライアント証明書、TACACS+ など、いくつかの認証タイプをサポートしています。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 を使用する場合は、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可能性のある制限を決定できます。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、および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 Access Interface 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 NetScaler 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。
- エンドポイント分析。NetScaler Gateway では、ユーザーのログオン時にユーザーデバイスのソフトウェア、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を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になるため、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

構成ユーティリティを使用すると、ほとんどの NetScaler Gateway 設定を構成できます。Web ブラウザを使用して、構成ユーティリティにアクセスします。

構成ユーティリティにログオンします

1. Web ブラウザーで、NetScaler Gateway のシステム IP アドレス（`http://192.168.100.1`など）を入力します。
   注：NetScaler Gateway は、
   デフォルトの IP アドレス 192.168.100.1、
   サブネットマスクが 255.255.0.0 であらかじめ構成されています。
2. [ユーザー名] と [パスワード] に次のように入力します。`nsroot`.
3. ［展開の種類］で［NetScaler 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 の設定を構成することもできます。

NetScaler 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。
- Configuring Settings with the Quick Configuration Wizard
- NetScaler Gateway ウィザードを使用した設定の構成

仮想サーバーを作成する

April 2, 2024

仮想サーバは、ユーザ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。仮想サーバーは、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ています。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)

- NetScaler 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

NetScaler 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。次の方法で、より多くの仮想サーバーを構成できます。

- 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ペインにあります。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。Citrix Endpoint Management、StoreFront、または Web Interface を環境に展開する場合は、クイック構成ウィザードを使用して、展開に必要な仮想サーバーと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、RADIUS などの特定の認証タイプを使用できるようにする場合は、仮想サーバを設定し、サーバに一意の IP アドレスを割り当てることができます。ユーザーがログオンすると、仮想サーバーに転送され、RADIUS 資格情報の入力を求められます。

また、ユーザーが NetScaler 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。

仮想サーバーを作成するには

仮想サーバーを追加、変更、有効化、無効化、および削除するには、NetScaler Gateway GUI またはクイック構成ウィザードを使用します。クイック構成ウィザードを使用した仮想サーバーの構成の詳細については、「クイック構成ウィザードを使用した設定の構成」を参照してください。

> 注:
>
> VPN 仮想サーバーは、デフォルトで DTLS バージョン 1.0 をサポートしています。DTLS バージョン 1.2 を有効にするには、「SSL VPN 仮想サーバーを使用した DTLS VPN 仮想サーバーの設定」を参照してください。

GUI を使用して仮想サーバーを作成するには

1. 「**NetScaler Gateway**」**>**「仮想サーバー」に移動します。
2. 詳細ペインで、[追加] をクリックします。
3. 要件に従って設定を構成します。
4. [**Create**] をクリックしてから、[**Close**] をクリックします。

CLI を使用して仮想サーバーを作成するには

コマンドプロンプトで次を入力します:


```
add vpn vserver <name> <serviceType> [<IPAddress> [<port>]
<!--NeedCopy-->
```

例:

```
add vpn vserver gatewayserver SSL 1.1.1.1 443
<!--NeedCopy-->
```

ネットプロファイルを **VPN** 仮想サーバーにバインドする際の注意点

ネットプロファイル（ネットワークプロファイル）を作成して、指定した送信元 IP アドレスを使用するようにアプライアンスを設定し、ネットプロファイルを VPN 仮想サーバーにバインドできます。ただし、ネットプロファイルを VPN 仮想サーバーにバインドする場合は、次の点に注意してください。

- ネットプロファイルを NetScaler Gateway 仮想サーバーにバインドすると、ネットプロファイルは、バックエンドサーバーへのトラフィック用に仮想サーバーまたはサービスによって使用される特定の SNIP を選択しません。代わりに、Gateway Appliance はネットプロファイルバインディングを無視し、ラウンドロビン方式を使用して SNIP を選択します。
- ネットプロファイルは、動的に生成されたサービス（STA、SF モニタ）では機能しません。STA およびその他の動的に生成されるサービスの場合、ネットプロファイルをそれらのモニタに直接バインドでき、その時点でそれらのモニタが使用されます。ただし、同じアプライアンスに複数のゲートウェイがある場合、すべてのゲートウェイは、設定されたモニタに対して同じネットプロファイルを使用します。

ネットプロファイルの詳細については、バックエンド通信に指定されたソース IP を使用するを参照してください。

仮想サーバ上の現在のユーザーと接続しているユーザーの総数

現在のユーザー**:** 特定の仮想サーバーにログオンしているユーザーの数。CCU を追跡するために現在のユーザを監視することをお勧めします。

接続しているユーザーの合計**:** 特定の仮想サーバーを介して 1 つ以上のアクティブな接続を持つユーザーの数。接続しているユーザーの総数は、主に ICA プロキシで使用されます。

接続ユーザーの合計数カウンタは、次のシナリオで使用できます。

- ICA 接続は確立されているが、対応する認証、承認、および監査セッションが確立されていないとします。このシナリオでは、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してブラウザを閉じ、起動したアプリケーションまたはデスクトップで作業を続行します。認証、承認、および監査セッションはタイムアウトしますが、接続はまだアクティブです。接続しているユーザーの合計数を使用して、まだ接続しているユーザーを識別できます。

- HDX 最適ルーティングでは、認証ゲートウェイと ICA ゲートウェイを異なるアプライアンス上に置くことができます。この場合の接続ユーザーの合計は、ICA ゲートウェイ上の接続ユーザーの数を識別するために使用できます。

注意事項:

- アクティブなセッションがある（まだタイムアウトしていない）が、これらのセッションにアクティブな接続がない場合、現在のユーザは合計接続ユーザ数を超えています。たとえば、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してすぐに閉じたものの、認証、承認、および監査セッションからログアウトしなかった場合などです。
- 認証、承認、および監査セッションがタイムアウトしても、ICA 接続がアクティブな場合、接続しているユーザーの合計が現在のユーザーを超えています。
- 純粋な VPN 設定（ICA は関与しない）では、現在のユーザー数と接続ユーザーの総数は等しくなります。

仮想サーバーで接続タイプを構成する

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せずに、Citrix Virtual Apps and Desktops にのみ接続します。
- Citrix Secure Access クライアントと SmartAccess との接続。これにより、SmartAccess、エンドポイント分析、および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 NetScaler 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しないように、接続は 1 つのセッションに移行されます。

ユーザがユーザソフトウェアなしでログオンできるようにする場合は、クライアントレスアクセスポリシーを設定し、それを仮想サーバにバインドできます。

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

1. [**NetScaler Gateway** ］に移動し、[仮想サーバー］をクリックします。
2. 詳細ペインで、[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 Secure Access** クライアント、および **SmartAccess** を使用してユーザーがログオンできるようにするには、「**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ー用のリッスンポリシーを構成する

NetScaler Gateway 仮想サーバーを構成して、仮想サーバーが特定の VLAN でリッスンする機能を制限できます。指定された VLAN 上のトラフィックの処理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。

設定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、仮想サーバーの作成後に名前を変更することはできません。名前は 127 文字を超えることはできません。また、最初の文字は数字または文字である必要があります。また、アットマーク (@)、アンダースコア (_)、ダッシュ (-)、ピリオド (.)、コロン (:)、シャープ記号 (#)、およびスペースを使用することもできます。
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。
種類	サービスの動作。選択肢は、HTTP、SSL、FTP、TCP、SSL_TCP、UDP、SSL_BRIDGE、NNTP、DNS、ANY、SIP-UDP、DNS-TCP、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 の範囲で指定する必要があります。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。
リスニング優先度	リッスンポリシーに割り当てられている優先順位。プライオリティは逆の順序で評価されます。数字が小さいほど、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必要がある VLAN の識別に使用するポリシールール。ルールは次のとおりです。 CLIENT.VLAN.ID.EQ (<ipaddressat>) <ipaddressat>の場合は、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. ナビゲーションペインで［**NetScaler Gateway**］を展開し、［仮想サーバー］をクリックします。
2. 詳細ペインで、[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 [構成] をクリックします。
9. 「式の作成」ダイアログで、「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。

NetScaler Gateway で **IP** アドレスを構成する

February 1, 2024

構成ユーティリティにログオンし、ユーザー接続用の IP アドレスを構成できます。NetScaler Gateway は、管理アクセス用のデフォルト IP アドレス 192.168.100.1、サブネットマスク 255.255.0.0 で構成されています。デフォルトの IP アドレスは、システム IP (NSIP) アドレスのユーザーが構成した値が存在しない場合に使用されます。

- 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 NetScaler Gateway の管理 IP アドレス。NetScaler Gateway は、認証に NSIP アドレスも使用します。
- デフォルトゲートウェイ。セキュリティで保護されたネットワークの外部から NetScaler 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ってユーザデバイスを表す IP アドレス。

SNIP アドレスは、ポート 1024 ～64000 を使用します。

NetScaler Gateway が **IP** アドレスを使用する方法

NetScaler Gateway は、発生している機能に基づいて IP アドレスからトラフィックをソースします。次のリストでは、一般的なガイドラインとして、いくつかの機能と、NetScaler 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。NetScaler Gateway が使用する IP アドレスは、認証サーバーの種類によって異なります。
  - LDAP/RADIUS/TACACS サーバ。AAAD が認証仮想サーバーと直接通信する場合、NSIP アドレスが使用されます。

  - ロードバランサをプロキシとして使用する場合、ロードバランサは認証に SNIP アドレスを使用します。AAAD は NSIP アドレスを使用してロードバランサと通信します。NetScaler ADC が使用する IP アドレスは、認証仮想サーバーと通信しているエンティティによって異なります。
  - SAML/OAUTH/WEBAUTH サーバー: これらのサーバーは SNIP アドレスを使用して通信します。

- ホームページからのファイル転送。NetScaler Gateway は SNIP アドレスを使用します。
- **DNS** および **WINS** クエリ。NetScaler Gateway は SNIP アドレスを使用します。
- セキュリティで保護された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。NetScaler Gateway は、NetScaler Gateway の構成に応じて、SNIP アドレスまたは IP プールを使用します。
- **ICA** プロキシ設定。NetScaler Gateway は SNIP アドレスを使用します。

サブネット **IP** アドレス

サブネット IP アドレスを使用すると、ユーザーは別のサブネット上にある外部ホストから NetScaler 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、サブネットに追加された最初の 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、NetScaler Gateway の初期構成時にサブネット IP アドレスを指定することは必須ではありません。

マッピング IP アドレスとサブネット IP アドレスは、ポート 1024 ～64000 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. 詳細ペインで、[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 の種類] 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。

ユーザー接続用の **IPv6** を構成する

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 NetScaler 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 アドレスを入力できます。

- 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
- NetScaler 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
- 高可用性セットアップ
- 高可用性のためのルートモニターのバインド/バインド解除
- 仮想サーバー (負荷分散)

NetScaler Gateway 仮想サーバーが IPv6 アドレスでリッスンするように構成すると、ユーザーは Citrix Workspace アプリでのみ接続できます。Citrix Secure Access クライアントとのユーザー接続は、IPv6 ではサポートされていません。

NetScaler 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 と Web Interface。ユーザー接続用に IPv6 を構成し、IPv6 を使用するマッピング IP アドレスがある場合、Citrix Virtual Apps および Web Interface サーバーも IPv6 を使用できます。Web Interface は、NetScaler 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 NetScaler 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。
- 仮想サーバー。NetScaler Gateway ウィザードを実行すると、仮想サーバーの IPv6 を構成できます。NetScaler Gateway ウィザードの［仮想サーバー］ページで、［IPv6］をクリックして IP アドレスを入力します。仮想サーバーの IPv6 アドレスを構成するには、NetScaler Gateway ウィザードを使用する必要があります。
- その他。ICA プロキシ、認証、監査、および高可用性用に IPv6 を構成するには、ダイアログボックスで [IPv6] チェックボックスをオンにし、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** サーバーを解決する

February 1, 2024

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。この問題は、次の手順で解決できます。

- 既知の完全修飾ドメイン名 (FQDN) に解決されるカスタム DNS モニターを使用して DNS サービスを作成する。
- NetScaler Gateway 上に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します。

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のみです。
- アプライアンスに NetScaler ADC 負荷分散ライセンスをインストールすると、ナビゲーションペインに［仮想サーバーとサービス］ノードが表示されません。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ペインで、[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. 詳細ペインで、［Add］をクリックします。
3. [名前] 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] を選択し、[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]、[閉じる] の順にクリックします。

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

DNS サービスを **DNS** 仮想サーバーにバインドするには

1. [仮想サービスの構成 (負荷分散)] 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]、[閉じる] の順にクリックします。

DNS 仮想サーバーを構成する

February 1, 2024

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。NetScaler 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、この IP アドレスは、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、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。また、DNS ポートを指定します。

注：アプライアンスに NetScaler ADC 負荷分散ライセンスをインストールすると、ナビゲーションペインに［仮想サーバーとサービス］ノードが表示されません。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。詳細については、NetScaler 製品ドキュメントの NetScaler ドキュメント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ペインで、[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. 詳細ペインで、［Add］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 NetScaler Gateway に関連付けます。

- サーバーを NetScaler 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 仮想サーバーをグローバルに展開すると、すべてのユーザーがそのサーバー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して、ユーザーを制限できます。

ネームサービスプロバイダーの設定

April 1, 2024

NetScaler Gateway 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。

NetScaler Gateway ウィザードを実行すると、DNS サーバーまたは WINS サーバーのいずれかを構成できます。構成ユーティリティを使用して、他の 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。

NetScaler Gateway に **DNS** 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、［NetScaler 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、[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]、[閉じる] の順にクリックします。
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 **NetScaler 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、［NetScaler 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、[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 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。NetScaler Gateway 仮想サーバーと同様に、仮想サーバーには IP アドレスを割り当てる必要があります。ただし、この IP アドレスは、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、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。

名前解決のために DNS サーバーと WINS サーバーを構成する場合は、NetScaler 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度を指定するには

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［NetScaler Gateway］をクリックします。
2. 詳細ペインの［はじめに］で、［NetScaler Gateway ウィザード］をクリックします。
3. ［次へ］をクリックして、［ネームサービスプロバイダ］ページが表示されるまで現在の設定を受け入れます。
4. [名前の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。

サーバー起動接続を構成する

April 1, 2024

IP アドレスが有効な NetScaler Gateway にログオンしたユーザーごとに、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、ユーザの IP アドレスではなく DNS 名をユーザに提供するのに役立ちます。

IP アドレスがユーザーのセッションに割り当てられると、内部ネットワークからユーザーのデバイスに接続できます。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) クライアントを使用して接続しているユーザーは、問題のあるアプリケーションを診断するためにユーザーデバイスにアクセスできます。また、リモートでログオンしている内部ネットワーク IP アドレスを持つ 2 人の NetScaler Gateway ユーザーが、NetScaler Gateway を介して相互に通信することも可能です。アプライアンスでログオンしているユーザーの内部ネットワーク IP アドレスの検出を許可すると、この通信が補助されます。

リモートユーザーは、次の ping コマンドを使用して、NetScaler 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。


```
ping \<username.domainname\>
```

サーバーは、次のさまざまな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、内部ネットワーク内の外部システム、または NetScaler Gateway にログオンしている別のコンピューターから発生します。NetScaler 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 アドレスは、これらの接続に使用されます。NetScaler Gateway がサポートするさまざまな種類のサーバー起動接続について説明します。
  TCP または UDP サーバー起動接続の場合、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予備知識を持ち、それに接続します。NetScaler Gateway はこの接続を傍受します。

  次に、ユーザーデバイスはサーバーへの初期接続を行い、サーバーは、既知または最初に構成されたポートから派生したポートで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、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、サーバーとポートと IP アドレスを交換します。これにより、NetScaler 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。
- Port 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。NetScaler Gateway は、内部ネットワーク IP アドレスを使用した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 NetScaler Gateway を使用する 2 つの NetScaler Gateway ユーザーデバイスが相互に接続を開始できます。このタイプの例としては、Office Communicator や Yahoo! メッセンジャー。

ユーザーが NetScaler Gateway からログオフし、ログオフ要求がアプライアンスに到達しなかった場合、ユーザーは任意のデバイスを使用して再度ログオンし、以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展開で役立つ場合があります。

ユーザーが NetScaler Gateway に初めてログオンすると、セッションが作成され、IP アドレスがユーザーに割り当てられます。ユーザーがログオフしてもログオフ要求が失われた場合、またはユーザーデバイスがクリーンログオフを実行できない場合、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、認証が成功すると、［ログオン転送］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の転送を選択すると、NetScaler Gateway 上の以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 2 分間だけアクティブになります。複数のデバイスから同時にログオンを試みた場合は、最後のログオン試行で元のセッションが置き換えられます。

サーバーが開始する接続のプライベートポート範囲の設定

Citrix Secure Access クライアントのリリース 23.10.1.7 以降、サーバー開始接続（SIC）用に 49152 から 64535 までのプライベートポートを構成できます。プライベートポートを構成することで、ポートを使用して Citrix Secure Access クライアントとクライアントマシン上のサードパーティアプリとの間でソケットを作成するときに発生する可能性のある競合を回避できます。これは WFP ドライバが使用されている場合にのみ適用されます。

SicBeginPort Windows VPN レジストリを使用してプライベートポートを構成できます。または、NetScaler の VPN プラグインカスタマイズ JSON ファイルを使用してプライベートポート範囲を構成することもできます。

サーバーが接続を開始すると、Citrix Secure Access クライアントはSicBeginPort Windows VPN レジストリから始まる最初の 1000 個のポートを使用してソケットを作成します。レジストリがクライアントマシン上で構成されている場合、レジストリ設定は NetScaler JSON 設定よりも優先されます。

以下は、NetScaler 上の VPN プラグイン JSON 構成の例です:

```
root@ADC# cat /var/netscaler/gui/vpn/pluginCustomization.json

{
 "SicBeginPort" : 51000 }

<!--NeedCopy-->
```

レジストリ設定について詳しくは、「NetScaler Gateway Windows VPN クライアントのレジストリキー」を参照してください。

> 注:
>
> ソケットの作成に使用されるデフォルトのポート範囲は 62500 ～63500 です。

NetScaler Gateway でルーティングを構成する

April 1, 2024

内部ネットワークリソースへのアクセスを提供するために、NetScaler Gateway はデータを内部の安全なネットワークにルーティングします。デフォルトでは、NetScaler Gateway は静的ルートを使用します。

NetScaler Gateway がデータをルーティングできるネットワークは、NetScaler Gateway ルーティングテーブルの構成方法と、NetScaler Gateway に指定するデフォルトゲートウェイによって決まります。

NetScaler Gateway 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が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。

NetScaler Gateway は、次のルーティングプロトコルをサポートしています。

- ルーティング情報プロトコル（RIP v1 および v2）
- Open Shortest Path First (OSPF)
- ボーダーゲートウェイプロトコル (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、NetScaler 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] を展開し、[ルート] をクリックします。
2. 詳細ペインの [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、[作成] 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。

   他のデバイスと正常に通信している場合、メッセージは、同じ数のパケットが送受信され、ゼロのパケットが失われたことを示します。

   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は、受信されたパケットがゼロで、すべてのパケットが失われたことを示します。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。

オートネゴシエーションの設定

April 1, 2024

デフォルトでは、アプライアンスは自動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、NetScaler Gateway がネットワークトラフィックを両方向同時に送信し、適切なアダプタ速度を決定します。
デフォルト設定を自動ネゴシエーションのままにすると、NetScaler Gateway は全二重操作を使用します。この動作では、ネットワークアダプターは双方向に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、NetScaler Gateway は半二重操作を使用します。この動作では、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一方向または他方のみを使用できます。

初回のインストールでは、アプライアンスに接続されているポートに自動ネゴシエーションを使用するように NetScaler Gateway を構成することをお勧めします。最初にログオンして NetScaler Gateway を構成したら、自動ネゴシエーションを無効にすることができます。オート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。

オート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ウィンドウで、[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. 詳細ウィンドウで、インターフェイスを選択し、[開く] をクリックします。
3.「インタフェースを設定」**(Configure Interface**) ダイアログボックスで次のいずれかを実行します:

    - オートネゴシエーションを有効にするには、［オートネゴシエーション］の横にある［はい］をクリックし、［**OK**］をクリックします。
    - オートネゴシエーションを無効にするには、［オートネゴシエーション］の横にある［いいえ］をクリックし、［**OK**］をクリックします。

NetScaler Gateway でホスト名と **FQDN** を構成する

April 1, 2024

ホスト名は、ライセンスファイルに関連付けられている NetScaler 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 NetScaler 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た署名付き証明書に含まれています。NetScaler Gateway では FQDN を構成しません。1 つのアプライアンスは、証明書を使用して NetScaler Gateway で構成された各仮想サーバーに割り当てられた一意の FQDN を持つことができます。

証明書の FQDN は、証明書の詳細を表示することで確認できます。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. 詳細ウィンドウで、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 がリストに表示されます。

NetScaler Gateway のポリシーとプロファイル

April 1, 2024

NetScaler Gateway のポリシーとプロファイルを使用すると、指定されたシナリオまたは条件の下で構成設定を管理および実装できます。個々のポリシーは、指定された条件セットが満たされたときに有効になる構成設定を指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。

ポリシーの仕組み

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コレクションで構成されます。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が決定されます。

プロファイルは、特定のパラメータを使用する設定の集まりです。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。

ポリシーは、設定され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、またはグローバルにバインドできます。ポリシーは、制御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と、ユーザーがログオンしたままにできる時間を制御できます。

NetScaler Gateway を Citrix Virtual Apps で使用している場合、NetScaler Gateway ポリシー名はフィルターとして Citrix Virtual Apps に送信されます。NetScaler Gateway を Citrix Virtual Apps および SmartAccess と互換性があるように構成する場合は、Citrix Virtual Apps で次の設定を構成します。

- アプライアンスに構成されている仮想サーバーの名前。この名前は、NetScaler Gateway ファーム名として Citrix Virtual Apps に送信されます。
- 事前認証ポリシー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。

NetScaler Gateway を Citrix EndpointManagement と互換性を持たせるための構成について詳しくは、「Citrix Endpoint Management 環境の設定を構成する」を参照してください。

NetScaler Gateway を Citrix Virtual Apps and Desktops と互換性を持たせるための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 の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。

条件付きポリシー

ポリシーを設定するときは、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文字列
- ネットワーク情報
- HTTP ヘッダーとクッキー
- 一日の時間

- クライアント証明書の値

また、ユーザーデバイスが特定の条件 (SmartAccess のセッションポリシーなど) を満たす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構成するもう 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ー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 Secure Access クライアントに接続するユーザーには LDAP による認証を要求し、WAN 経由で接続するユーザーは RADIUS を使用して認証するように要求できます。

注: ポリシー・ルールがセッション・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。

ポリシーの優先順位

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および評価されます。

次の 2 つの方法により、ポリシーのプライオリティが決まります。

- ポリシーがバインドされるレベル（グローバル、仮想サーバー、グループ、またはユーザー）。ポリシーレベルは、次のように最高から最低にランク付けされます。
  - ユーザー (最優先度)
  - グループ
  - 仮想サーバー
  - グローバル (最低優先度)
- 数値のプライオリティは、ポリシーがバインドされているレベルに関係なく優先されます。グローバルにバインドされたポリシーのプライオリティ番号が 1 で、ユーザにバインドされた別のポリシーのプライオリティ番号が 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。

NetScaler Gateway でポリシーを作成する

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、ポリシーを適切なレベル（ユーザー、グループ、仮想サーバー、グローバル）にバインドします。ポリシーをこれらのレベルのいずれかにバインドすると、ポリシー条件が満たされると、ユーザーはプロファイル内の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環境の設定を構成できます。ウィザードの詳細については、「クイック構成ウィザードを使用した設定の構成」を参照してください。

システム式の設定

April 1, 2024

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間に適用されます。セッションポリシーの式は、ユーザーが認証されて NetScaler Gateway にログオンした後に評価され、適用されます。

NetScaler Gateway での式は次のとおりです。

- NetScaler Gateway への接続を確立する際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表現です。たとえば、以下を参照してください:
  - セッションポリシー
- 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表現。たとえば、以下を参照してください:
  - エンドポイントポリシー
- 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。たとえば、以下を参照してください:
  - トラフィックポリシー
  - 承認ポリシー

NetScaler Gateway は、NetScaler ADC アプライアンスとしても使用できます。アプライアンス上のいくつかの式は、NetScaler ADC により適用されます。一般的な式とネットワークベースの式は、NetScaler ADC で一般的に使用され、NetScaler Gateway では一般的に使用されません。クライアントセキュリティ式は、NetScaler Gateway で使用され、ユーザーデバイスに正しいアイテムが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

式はポリシーの構成要素です。式は、リクエストまたはレスポンス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

NetScaler Gateway での証明書管理

February 1, 2024

NetScaler 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、接続の一端にサーバー証明書が必要です。接続のもう一方の端には、サーバ証明書を発行した認証局 (CA) のルート証明書が必要です。

- 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。NetScaler Gateway には、このタイプ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、サーバ証明書に署名した CA を識別します。ルート証明書は認証局に属します。ユーザーデバイスは、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を必要とします。

ユーザーデバイス上の Web ブラウザとのセキュアな接続を確立すると、サーバーは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 ブラウザーは、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 ブラウザはユーザに証明書を受け入れるか拒否するかを尋ねます（事実上、サイトへのアクセス権限を承認または拒否します）。

NetScaler 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。NetScaler 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。
- 証明書と秘密キーの格納または転送に使用される 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、NetScaler Gateway にインストールされます。

Thawte や Verisign など、信頼できる 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。

証明書署名要求を作成する

April 1, 2024

SSL または TLS を使用してセキュリティで保護された通信を提供するには、NetScaler Gateway でサーバー証明書が必要です。証明書を NetScaler Gateway にアップロードする前に、証明書署名要求（CSR）と秘密キーを生成する必要があります。NetScaler 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。証明書要求の作成により、署名用に認証局（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が作成されます。CA が証明書に署名し、指定した電子メールア

ドレスに証明書を返します。署名付き証明書を受け取ったら、NetScaler 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、証明書と秘密キーをペアにします。

重要：NetScaler 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 が署名付き証明書を送信するのを待つ必要があります。証明書を受け取ったら、NetScaler 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。NetScaler Gateway ウィザードについて詳しくは、「NetScaler 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。

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

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 [**NetScaler**Gateway] をクリックします。
2. 詳細ペインの [はじめに] で、[**NetScaler 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、NetScaler Gateway 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ーに保存し、[閉じる] をクリックします。
6. 設定を保存せずに NetScaler Gateway ウィザードを終了します。

NetScaler GUI を使用して **CSR** を作成する

また、NetScaler Gateway ウィザードを実行せずに、NetScaler 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 CA に証明書を電子メールで送信します。

詳細な手順については、「証明書署名要求の作成」を参照してください。

NetScaler Gateway に署名付き証明書をインストールする

認証局（CA）から署名付き証明書を受け取ったら、それをアプライアンスの秘密キーとペアにして、NetScaler Gateway に証明書をインストールします。

GUI を使用して、署名付き証明書と秘密キーをペアリングします

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 NetScaler Gateway のフォルダー 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ペインで、[**SSL] > [**証明書] を展開します。
3. [**SSL** 証明書] ページで、[開始する] をクリックします。
4. 詳細ペインで、[インストール] をクリックします。
5. [証明書とキーのペア名**]** に、証明書の名前を入力します。
6. [証明書ファイル名] で、[アプライアンス] をクリックします。
7. 証明書に移動し、[選択] をクリックし、[開く] をクリックします。
8. [キーファイル名] で、[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。秘密キーは、NetScaler Gateway の\ nsconfig\ ssl ディレクトリにあります。
9. 秘密キーを選択し、[開く] をクリックします。
10. 証明書が PEM 形式の場合は、[パスワード] に秘密鍵のパスワードを入力します。
11. 証明書の有効期限が切れるときの通知を構成する場合は、[期限切れ時に通知] を選択します。
12. [通知期間] に日数を入力し、[作成] をクリックし、[閉じる] をクリックします。

GUI を使用して証明書と秘密キーを仮想サーバーにバインドする

証明書と秘密キーのペアを作成してリンクしたら、それ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の［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］**>**［仮想サーバー］の順に展開します。
2. 詳細ペインで仮想サーバーを選択して、［**Open**］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」をクリックして、「**OK**」をクリックします。

CLI を使用して、証明書と秘密キーを仮想サーバーにバインドします

コマンドプロンプトで次を入力します:

```
1 bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
     Mandatory | Optional )
2 <!--NeedCopy-->
```

例**:**

```
1 bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA -
     ocspCheck Mandatory
2 <!--NeedCopy-->
```

注**:** デバイス証明書に OCSP チェックが必要ない場合、oscpCheck はオプションです。

GUI を使用して仮想サーバーからテスト証明書をバインド解除します

署名付き証明書をインストールしたら、仮想サーバーにバインドされているすべてのテスト証明書をバインド解除します。構成ユーティリティを使用して、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、［**NetScaler Gateway**］**>**［仮想サーバー］の順に展開します。
2. 詳細ペインで仮想サーバーを選択して、［**Open**］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。

中間証明書を構成する

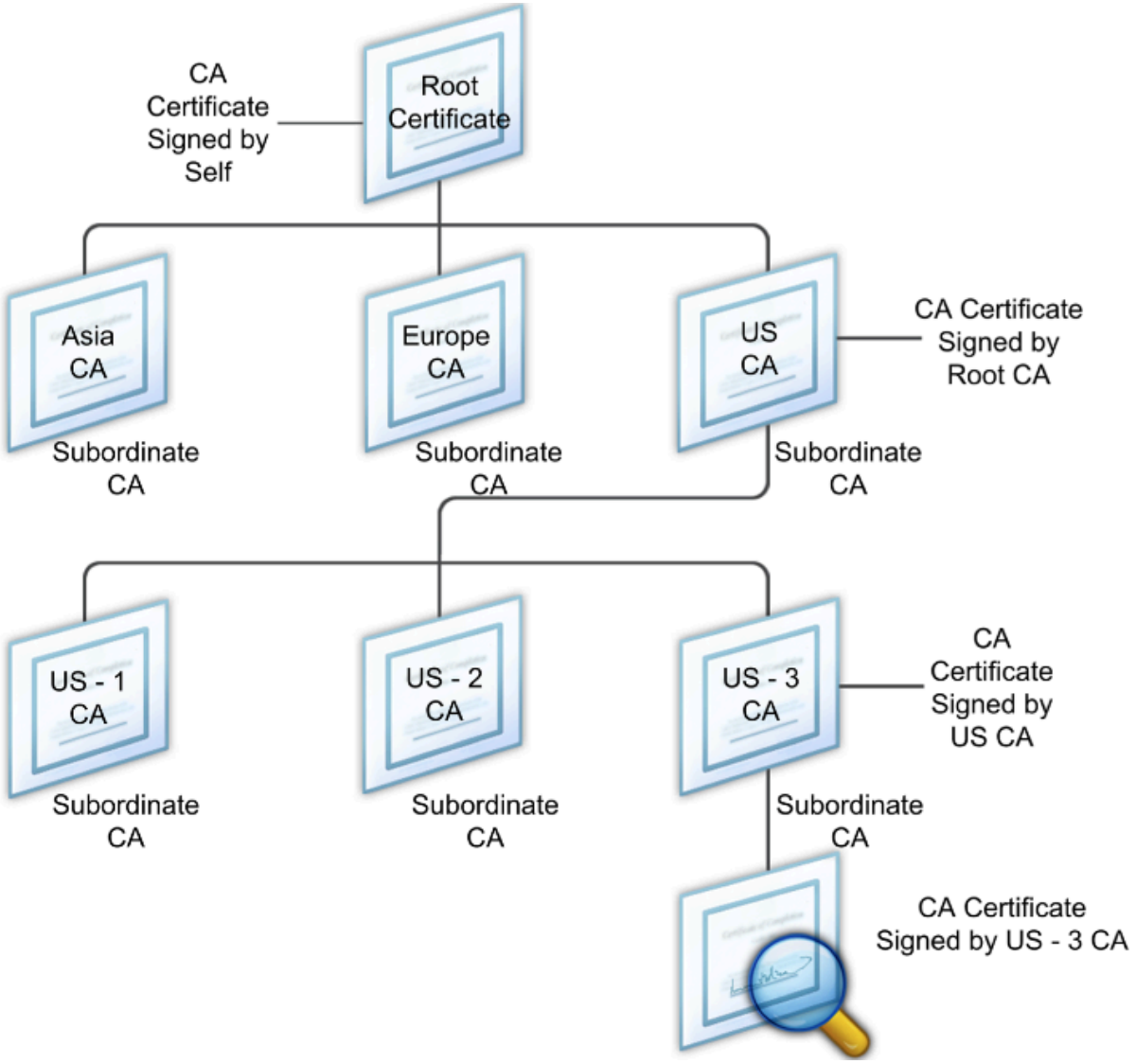
February 1, 2024

中間証明書は、NetScaler Gateway（サーバー証明書）とルート証明書（ユーザーデバイスにインストールされている）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、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ています。

証明書の発行責任は、下位の認証局 (CA) を設定することで委任できます。CA は、独自の証明書（自己署名）に署名することも、別の認証局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、認証局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、ルート認証局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 の下にある 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：典型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使用して 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認証局という 2 つの証明書で構成されます。ユーザー証明書またはサーバー証明書が中間認証局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）と中間認証局の証明書（この順序で）であることを示しています。中間認証局の証明書の後には、その認証局の証明書が続きます。このリストは、リストの最後の証明書がルート認証局の証明書になるまで続きます。チェーン内の各証明書は、以前の証明書の 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

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、一覧から [ローカル] または [アプライアンス] を選択します。
5. コンピューター（ローカル）または NetScaler Gateway（アプライアンス）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。

NetScaler Gateway に中間証明書をインストールするときは、秘密キーまたはパスワードを指定する必要はありません。

証明書をアプライアンスにインストールしたら、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

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] の横にあるリスト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

February 1, 2024

NetScaler 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、従来のまたは高度なエンドポイント分析 (EPA) ポリシーの一部として構成できます。クラシック EPA ポリシーでは、デバイス証明書は事前認証 EPA に対してのみ構成できます。

NetScaler Gateway は、エンドポイント分析スキャンの実行前、またはログオンページが表示される前に、デバイス証明書を検証します。エンドポイント分析を設定すると、エンドポイントスキャンが実行され、ユーザーデバイスが検証されます。デバイスがスキャンに合格し、NetScaler Gateway がデバイス証明書を検証すると、ユーザーは NetScaler Gateway にログオンできます。

> 重要:
>
> - デフォルトでは、Windows はデバイス証明書にアクセスするための管理者権限を義務付けています。
> - 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、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。
> - 複数の CA 証明書をゲートウェイに追加し、デバイス証明書を検証できます。
> - NetScaler 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、ユーザーは NetScaler 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の実行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。
> - 中間 CA によって発行されたデバイス証明書がある場合は、中間 CA 証明書とルート CA 証明書の両方をバインドする必要があります。
> - EPA クライアントは、ユーザーがマシン証明書ストアにアクセスできるローカル管理者権限を持っている必要があります。これがまれにしか発生しないため、回避策として、ローカルストアにアクセスできる完全な NetScaler Gateway プラグインをインストールします。

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。

- Microsoft Web サイトの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) 。
- Apple サポート Web サイトの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 証明機関に証明書を要求する方法 。
- iPad/iPhone 証明書の発行 Microsoft サポートブログの「ディレクトリサービスチームに尋ねる」を参照してください。
- Windows IT Pro の Webサイトでネットワークデバイス登録サービスをセットアップします 。
- Configuration Manager の PKI 証明書の展開のステップバイステップの例:Windows Server 2008 証明機関 を Microsoft System Center の Web サイトから入手してください。

デバイス証明書を構成する手順

デバイス証明書を設定するには、次の手順を完了する必要があります。

- デバイス証明書発行者の証明機関証明書を NetScaler Gateway にインストールします。詳しくは、「NetScaler 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。

- デバイス証明書発行者の証明機関証明書を NetScaler Gateway 仮想サーバーにバインドし、OCSP チェックを有効にします。詳しくは、「NetScaler 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。
- デバイス証明書発行者の認証局証明書に OCSP（レスポンダ）を作成し、バインドします。詳細については、「OCSP による証明書ステータスの監視」を参照してください。

仮想サーバーでデバイス証明書のチェックを有効にし、デバイス証明書発行者の認証局証明書をデバイス証明書のチェックリストに追加します。詳細については、クラシック EPA ポリシーの仮想サーバーでのデバイス証明書チェックの有効化を参照してください。

Windows マシンでクライアント側の設定とデバイス証明書の検証を完了します。詳細については、「Windows マシンでのデバイス証明書の検証」を参照してください。

> 注:
>
> デバイス証明書 EPA チェックを利用するすべてのクライアントでは、マシンのシステム証明書ストアにデバイス証明書がインストールされている必要があります。

クラシック **EPA** ポリシーの仮想サーバーでデバイス証明書チェックを有効にする

デバイス証明書を作成したら、NetScaler 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、NetScaler Gateway に証明書をインストールします。

1. ［構成］タブで、［**NetScaler Gateway**］**>**［仮想サーバー］に移動します。
2. **NetScaler 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」ページの「基本設定」セクションで、「編集」をクリックします。
4. 認証を無効にするには、[認証を有効にする] チェックボックスをオフにします。
5. [デバイス証明書を有効にする] ボックスを選択して、デバイス証明書を有効にします
6. [追加] をクリックして、使用可能なデバイス証明書発行者の CA 証明書名をリストに追加します。
7. CA 証明書を仮想サーバーにバインドするには、[デバイス証明書の **CA]** セクションの **[CA** 証明書] をクリックし、[追加] をクリックして証明書を選択し、[**+**] をクリックします。

> 注:
>
> 高度な 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。

Windows マシンでのデバイス証明書の検証

1. ブラウザーを開き、NetScaler Gateway FQDN にアクセスします。
2. Citrix エンドポイント分析（EPA）クライアントの実行を許可します。EPA がインストールされていない場合は、EPA をインストールします。

Citrix EPA はデバイス証明書を実行して検証し、デバイス証明書 EPA チェックに合格すると認証ページにリダイレクトされ、合格しなかった場合は EPA エラーページにリダイレクトされます。他の EPA チェックがある場合、EPA スキャンの結果は、設定された EPA チェックによって異なります。

クライアントでさらにデバッグするには、クライアントで次の EPA ログを調べます。
C:\Users<User name>\ AppData\ Local\ Citrix\ AGEE\ nsepa.txt

注:

> CRL によるデバイス証明書の検証はサポートされていません。

既存の証明書をインポートしてインストールする

April 1, 2024

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ー、または Secure Gateway を実行しているコンピューター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、必ず秘密キーもエクスポートしてください。秘密キーをエクスポートできないことがあります。つまり、NetScaler Gateway に証明書をインストールできません。この場合は、証明書署名要求 (CSR) を使用して証明書を作成します。詳細については、「証明書署名要求の作成」を参照してください。

Windows から証明書と秘密キーをエクスポートすると、コンピューターは個人情報交換 (.pfx) ファイルを作成します。このファイルは、PKCS #12 証明書として NetScaler Gateway にインストールされます。

Secure Gateway を NetScaler Gateway に置き換える場合は、Secure Gateway から証明書と秘密キーをエクスポートできます。Secure Gateway から NetScaler 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 を廃棄し、NetScaler Gateway に証明書をインストールして、構成をテストします。Secure Gateway と NetScaler Gateway が同じ FQDN を持つ場合、ネットワーク上で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 管理コンソール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はデフォルト値のままにし、パスワードを定義して、.pfx ファイルをコンピュータに保存します。証明書がエクスポートされたら、NetScaler Gateway にインストールします。

NetScaler Gateway に証明書と秘密キー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［**NetScaler**Gateway］をクリックします。

2. 詳細ペインの［はじめに］で、［**NetScaler 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)** ファイルのインストール」を選択します。
5. [**PKCS #12** ファイル名] で、[参照] をクリックし、証明書に移動して、[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 NetScaler Gateway ウィザードを終了します。

証明書が NetScaler Gateway にインストールされると、構成ユーティリティの［**SSL**］**\ >**［証明書］ノードに証明書が表示されます。

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ペインで、[**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. [キーファイル名] に、秘密キーの名前を入力するか、[参照] をクリックして既存のファイルに移動します。
4. [キーのサイズ **(**ビット**)**] に、秘密キーのサイズを入力します。
5.「公開指数値」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. [キーフォーマット] で、[PEM] または [DER] を選択します。証明書には PEM 形式を推奨します。
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] と [パスフレーズの確認] 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、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、**[Create DSA Key**] をクリックし、RSA 秘密キーを作成する手順に従います。

証明書失効リスト

April 1, 2024

認証局 (CA) は、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 Corporation を離れたとします。会社は、Ann の証明書を CRL に配置して、彼女がそのキーでメッセージに署名するのを防ぐことができます。

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は、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。

NetScaler Gateway は、次の 2 つの CRL タイプをサポートしています。

- 失効した証明書または無効になった証明書を一覧表示する CRL
- Online Certificate Status Protocol (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、次の手順を実行します。

NetScaler 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にローカルに保存されていることを確認します。高可用性セットアップの場合、CRL ファイルは両方の NetScaler 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: NetScaler ADC に追加される CRL の名前。最大 31 文字です。
- CRL ファイル: NetScaler ADC に追加される CRL ファイルの名前。NetScaler ADC は、デフォルトで/var/netscaler/ssl ディレクトリで CRL ファイルを検索します。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
- 日数: 最大 31

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. 詳細ペインで、［Add］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。

GUI で **LDAP** または **HTTP** を使用して **CRL** 自動更新を設定するには、次の手順を実行します。

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。NetScaler Gateway アプライアンスの 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。

NetScaler Gateway アプライアンスは、Web の場所または 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 ロケーションまたは LDAP サーバを指定する場合、コマンドの実行時に CRL がローカルハードディスクドライブに存在してい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の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 を格納するためのデフォルトのパスは /var/netscaler/SSL です。

CRL リフレッシュパラメータ

- **CRL** 名

  NetScaler Gateway で更新される CRL の名前。

- **CRL** 自動更新を有効にする

  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。NetScaler 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。可能な値:HTTP、LDAP。デフォルト:HTTP。

- 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。指定した範囲が
  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 の取得元の 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 サーバが通信するポート番号。

- **URL**

  CRL の取得元の 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 証明書の発行者名の代わりにベース DN 属性を使用することをお勧めします。Issuer-Name フィールドは、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**

  バインド DN 属性は、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ます。バインド DN 属性は、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。

- 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される管理者パスワード。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、パスワードが必要です。

- 間隔

  CRL リフレッシュを実行する必要がある間隔。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.

- 日数

  CRL リフレッシュを実行する必要がある日。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。

- 時間

  CRL リフレッシュを実行する必要がある正確な時刻（24 時間形式）。

- 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。可能な値: はい、いいえ。デフォルト: いいえ。

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: 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
   - スコープ
   - サーバー IP
   - ポート *
   - URL
   - ベース DN*
   - バインド DN

- パスワード
- 間隔
- 日数
- 時間

5. ［Create］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 で証明書のステータスを監視する

Online Certificate Status Protocol (OCSP) は、クライアント SSL 証明書の状態を判断するために使用されるインターネットプロトコルです。NetScaler Gateway は RFC 2560 で定義されているように OCSP をサポートしています。OCSP には、タイムリーな情報の点で、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、多額の資金や高額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。NetScaler Gateway の OCSP の実装には、要求のバッチ処理と応答のキャッシュが含まれます。

OCSP の **NetScaler Gateway** 実装

NetScaler Gateway アプライアンスでの OCSP 検証は、NetScaler Gateway が SSL ハンドシェイク中に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、NetScaler Gateway は OCSP 要求を作成し、OCSP レスポンダーに転送します。そのために、NetScaler Gateway は、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、ローカルで構成された URL を使用します。NetScaler 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一時停止状態になります。サーバーからの応答が構成された時間を超えて遅延し、他のレスポンダーが構成されていない場合、NetScaler Gateway は、OCSP チェックをオプションまたは必須に設定したかどうかに応じて、トランザクションを許可するかエラーを表示します。NetScaler Gateway は、OCSP 要求のバッチ処理と OCSP 応答のキャッシュをサポートして、OCSP レスポンダーの負荷を軽減し、応答を高速化します。

OCSP リクエストのバッチング

NetScaler 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避けるために、NetScaler Gateway は同じ要求で複数のクライアント証明書の状態を照会できます。リクエストのバッチ処理を効率的に実行するには、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、ユーザへの応答が速くなり、OCSP レスポンダの負荷が軽減されます。OCSP レスポンダーからクライアント証明書の失効ステータスを受信すると、NetScaler Gateway は

事前定義された時間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、NetScaler Gateway はまずローカルキャッシュでこの証明書のエントリを確認します。まだ有効な（キャッシュタイムアウト制限内で）エントリが見つかると、その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、NetScaler Gateway は OCSP レスポンダーに要求を送信し、構成された期間応答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

オンライン証明書状態プロトコル (OCSP) を構成するには、OCSP レスポンダの追加、OCSP レスポンダを認証局 (CA) からの署名付き証明書にバインドし、証明書と秘密キーを Secure Sockets Layer (SSL) 仮想サーバーにバインドします。構成済みの 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、まずレスポンダーをバインド解除してから、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. 詳細ペインで、［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 文字を超えることはできません。
5. OCSP 応答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、NetScaler Gateway が応答を保持する分数を入力します。
6. [要求バッチ処理] で、[有効にする] をクリックします。
7. [バッチング遅延] で、OCSP 要求のグループをバッチ処理する時間をミリ秒単位で指定します。

   指定できる値は 0 ～10000 です。デフォルトは 1 です。
8. ［時間スキューで生成される時間］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ときに NetScaler 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場合は、[応答の検証] で [応答を信頼する] を選択します。

   信頼応答を有効にする場合は、ステップ 8 とステップ 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 が応答の検証に使用されます。
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も含まれます。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、リクエストは署名されません。
13. 一度使用した番号を有効にするには(nonce)extension、[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。

NetScaler Gateway の構成設定の管理

February 1, 2024

NetScaler 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。

- 設定を保存しました。NetScaler Gateway に保存した設定を表示できます。
- 実行構成。構成したが、NetScaler Gateway の保存済み構成として保存していないアクティブな設定（仮想サーバーや認証ポリシーなど）を表示できます。
- 実行構成と保存済み構成の比較。NetScaler Gateway で実行されている構成と保存されている構成を並べて比較できます。

NetScaler Gateway の構成設定をクリアすることもできます。

重要：NetScaler Gateway の設定をクリアすると、証明書、仮想サーバー、および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。

NetScaler Gateway 構成を保存する

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

NetScaler Gateway で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。

NetScaler Gateway で構成ファイルを表示して保存するには

保存される構成は、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、NetScaler Gateway のログファイルに保存される設定です。

NetScaler Gateway で設定を構成すると、コンピューター上のファイルにその設定を保存できます。NetScaler 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 NetScaler 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、ファイルを NetScaler 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. 詳細ウィンドウの [構成の表示] で、[保存された構成] をクリックします。
3. [保存された設定] 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て、[保存] をクリックします。
   注：ns.conf というファイル名を使用して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

NetScaler Gateway への変更を保存せずに行われた変更は、実行構成と呼ばれます。これらの設定は NetScaler Gateway でアクティブになりますが、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、または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。

保存済み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、[保存した仮想環境の実行] をクリックします。

NetScaler Gateway の構成をクリアする

NetScaler Gateway の構成設定をクリアできます。次の 3 つのレベルからクリアする設定を選択できます。

重要：NetScaler 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。

- ベーシック。システム IP アドレス、デフォルトゲートウェイ、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、および機能およびモード設定を除くアプライアンス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。設定を工場出荷時の設定に復元します。ただし、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は除きます。

設定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、NetScaler Gateway に保存されている証明書、ライセンスなどの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ーに保存します。構成を保存すると、NetScaler Gateway で ns.conf ファイルを復元できます。ファイルをアプライアンスに復元して NetScaler 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されません。

高可用性ペアがある場合、両方の NetScaler 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、変更は 2 番目のアプライアンスに伝播されます。

NetScaler 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。

NetScaler Gateway での証明書管理

February 1, 2024

NetScaler 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、接続の一端にサーバー証明書が必要です。接続のもう一方の端には、サーバ証明書を発行した認証局 (CA) のルート証明書が必要です。

- 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。NetScaler Gateway には、このタイプ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、サーバ証明書に署名した CA を識別します。ルート証明書は認証局に属します。ユーザーデバイスは、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を必要とします。

ユーザーデバイス上の Web ブラウザとのセキュアな接続を確立すると、サーバーは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 ブラウザーは、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 ブラウザはユーザに証明書を受け入れるか拒否するかを尋ねます（事実上、サイトへのアクセス権限を承認または拒否します）。

NetScaler 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。NetScaler 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。
- 証明書と秘密キーの格納または転送に使用される 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、NetScaler Gateway にインストールされます。

Thawte や Verisign など、信頼できる 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。

証明書署名要求を作成する

April 1, 2024

SSL または TLS を使用してセキュリティで保護された通信を提供するには、NetScaler Gateway でサーバー証明書が必要です。証明書を NetScaler Gateway にアップロードする前に、証明書署名要求（CSR）と秘密キーを生成する必要があります。NetScaler 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。証明書要求の作成により、署名用に認証局（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が作成されます。CA が証明書に署名し、指定した電子メールアドレスに証明書を返します。署名付き証明書を受け取ったら、NetScaler 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、証明書と秘密キーをペアにします。

重要：NetScaler 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 が署名付き証明書を送信するのを待つ必要があります。証明書を受け取ったら、NetScaler 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。NetScaler Gateway ウィザードについて詳しくは、「NetScaler 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。

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

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［**NetScaler**Gateway］をクリックします。
2. 詳細ペインの［はじめに］で、［**NetScaler 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、NetScaler Gateway 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ーに保存し、[閉じる] をクリックします。
6. 設定を保存せずに NetScaler Gateway ウィザードを終了します。

NetScaler GUI を使用して **CSR** を作成する

また、NetScaler Gateway ウィザードを実行せずに、NetScaler 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 CA に証明書を電子メールで送信します。

詳細な手順については、「証明書署名要求の作成」を参照してください。

NetScaler Gateway に署名付き証明書をインストールする

認証局（CA）から署名付き証明書を受け取ったら、それをアプライアンスの秘密キーとペアにして、NetScaler Gateway に証明書をインストールします。

GUI を使用して、署名付き証明書と秘密キーをペアリングします

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 NetScaler Gateway のフォルダー 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ペインで、[**SSL] > [**証明書] を展開します。
3. [**SSL** 証明書] ページで、[開始する] をクリックします。
4. 詳細ペインで、[インストール] をクリックします。
5. [証明書とキーのペア名**]** に、証明書の名前を入力します。
6. [証明書ファイル名] で、[アプライアンス] をクリックします。
7. 証明書に移動し、[選択] をクリックし、[開く] をクリックします。
8. [キーファイル名] で、[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。秘密キーは、NetScaler Gateway の\ nsconfig\ ssl ディレクトリにあります。
9. 秘密キーを選択し、[開く] をクリックします。
10. 証明書が PEM 形式の場合は、[パスワード] に秘密鍵のパスワードを入力します。
11. 証明書の有効期限が切れるときの通知を構成する場合は、[期限切れ時に通知] を選択します。
12. [通知期間] に日数を入力し、[作成] をクリックし、[閉じる] をクリックします。

GUI を使用して証明書と秘密キーを仮想サーバーにバインドする

証明書と秘密キーのペアを作成してリンクしたら、それ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の［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］**>**［仮想サーバー］の順に展開します。
2. 詳細ペインで仮想サーバーを選択して、［**Open**］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」をクリックして、「**OK**」をクリックします。

CLI を使用して、証明書と秘密キーを仮想サーバーにバインドします

コマンドプロンプトで次を入力します:

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
   Mandatory | Optional )
<!--NeedCopy-->
```

例**:**

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA -
   ocspCheck Mandatory
<!--NeedCopy-->
```

注**:** デバイス証明書に OCSP チェックが必要ない場合、oscpCheck はオプションです。

GUI を使用して仮想サーバーからテスト証明書をバインド解除します

署名付き証明書をインストールしたら、仮想サーバーにバインドされているすべてのテスト証明書をバインド解除します。構成ユーティリティを使用して、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、［**NetScaler Gateway**］**>**［仮想サーバー］の順に展開します。
2. 詳細ペインで仮想サーバーを選択して、［**Open**］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。

中間証明書を構成する

February 1, 2024

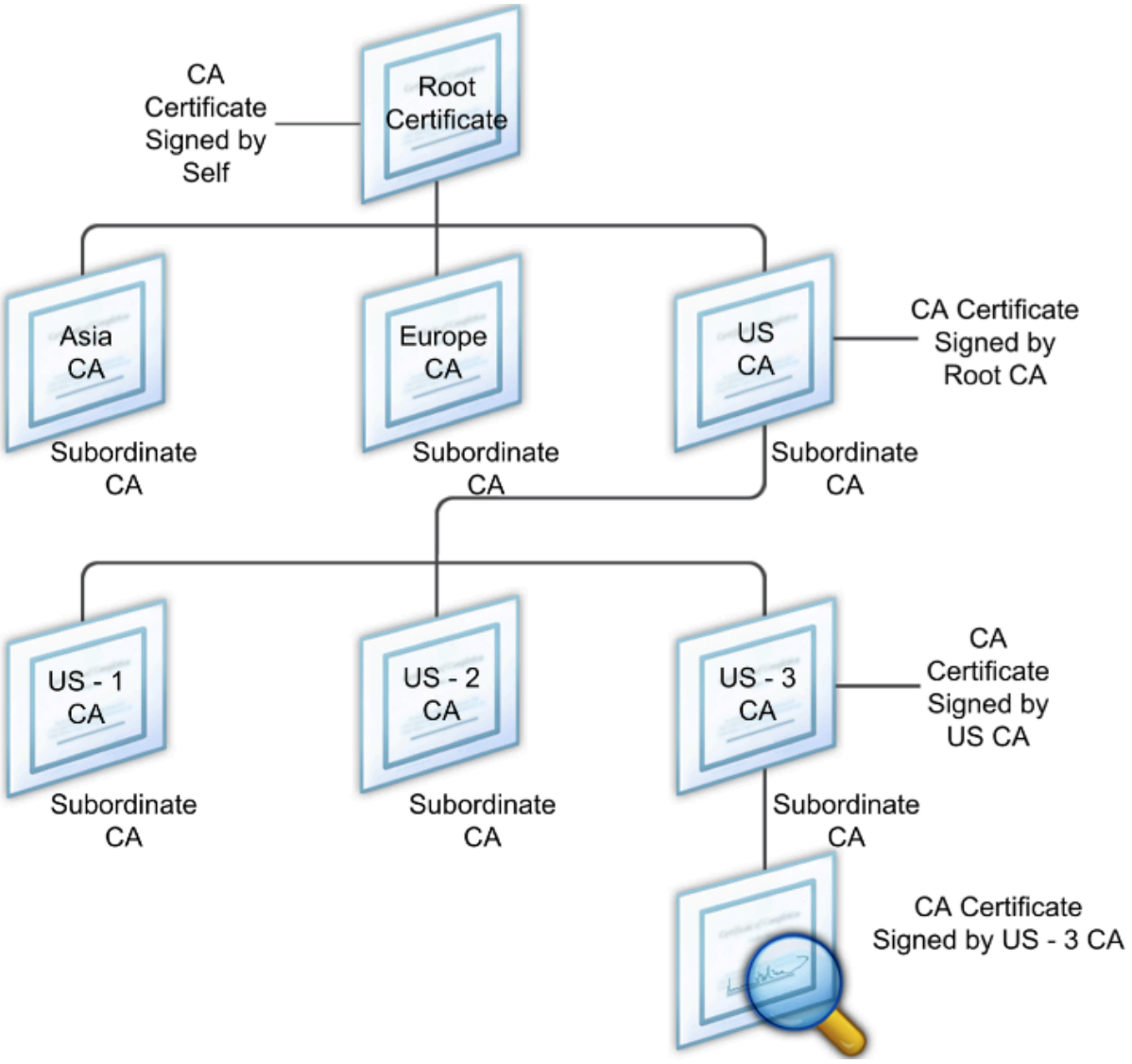
中間証明書は、NetScaler Gateway（サーバー証明書）とルート証明書（ユーザーデバイスにインストールされている）の間にある証明書です。中間証明書はチェーンの一部です。

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、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ています。

証明書の発行責任は、下位の認証局 (CA) を設定することで委任できます。CA は、独自の証明書（自己署名）に署名することも、別の認証局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、認証局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、ルート認証局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 の下にある 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：典型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使用して 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認証局という 2 つの証明書で構成されます。ユーザー証明書またはサーバー証明書が中間認証局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）と中間認証局の証明書（この順序で）であることを示しています。中間認証局の証明書の後には、その認証局の証明書が続きます。このリストは、リストの最後の証明書がルート認証局の証明書になるまで続きます。チェーン内の各証明書は、以前の証明書の 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

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、一覧から [ローカル] または [アプライアンス] を選択します。
5. コンピューター（ローカル）または NetScaler Gateway（アプライアンス）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。

NetScaler Gateway に中間証明書をインストールするときは、秘密キーまたはパスワードを指定する必要はありません。

証明書をアプライアンスにインストールしたら、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

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] の横にあるリスト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

February 1, 2024

NetScaler 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、従来のまたは高度なエンドポイント分析 (EPA) ポリシーの一部として構成できます。クラシック EPA ポリシーでは、デバイス証明書は事前認証 EPA に対してのみ構成できます。

NetScaler Gateway は、エンドポイント分析スキャンの実行前、またはログオンページが表示される前に、デバイス証明書を検証します。エンドポイント分析を設定すると、エンドポイントスキャンが実行され、ユーザーデバイスが検証されます。デバイスがスキャンに合格し、NetScaler Gateway がデバイス証明書を検証すると、ユーザーは NetScaler Gateway にログオンできます。

> 重要:
>
> - デフォルトでは、Windows はデバイス証明書にアクセスするための管理者権限を義務付けています。
> - 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、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。
> - 複数の CA 証明書をゲートウェイに追加し、デバイス証明書を検証できます。
> - NetScaler 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、ユーザーは NetScaler 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の実行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。
> - 中間 CA によって発行されたデバイス証明書がある場合は、中間 CA 証明書とルート CA 証明書の両方をバインドする必要があります。
> - EPA クライアントは、ユーザーがマシン証明書ストアにアクセスできるローカル管理者権限を持っている必要があります。これがまれにしか発生しないため、回避策として、ローカルストアにアクセスできる完全な NetScaler Gateway プラグインをインストールします。

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。

- Microsoft Web サイトの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) 。
- Apple サポート Web サイトの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 証明機関に証明書を要求する方法 。
- iPad/iPhone 証明書の発行 Microsoft サポートブログの「ディレクトリサービスチームに尋ねる」を参照してください。
- Windows IT Pro の Webサイトでネットワークデバイス登録サービスをセットアップします 。
- Configuration Manager の PKI 証明書の展開のステップバイステップの例:Windows Server 2008 証明機関 を Microsoft System Center の Web サイトから入手してください。

デバイス証明書を構成する手順

デバイス証明書を設定するには、次の手順を完了する必要があります。

- デバイス証明書発行者の証明機関証明書を NetScaler Gateway にインストールします。詳しくは、「NetScaler 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。

- デバイス証明書発行者の証明機関証明書を NetScaler Gateway 仮想サーバーにバインドし、OCSP チェックを有効にします。詳しくは、「NetScaler 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。
- デバイス証明書発行者の認証局証明書に OCSP（レスポンダ）を作成し、バインドします。詳細については、「OCSP による証明書ステータスの監視」を参照してください。

仮想サーバーでデバイス証明書のチェックを有効にし、デバイス証明書発行者の認証局証明書をデバイス証明書のチェックリストに追加します。詳細については、クラシック EPA ポリシーの仮想サーバーでのデバイス証明書チェックの有効化を参照してください。

Windows マシンでクライアント側の設定とデバイス証明書の検証を完了します。詳細については、「Windows マシンでのデバイス証明書の検証」を参照してください。

> 注:
>
> デバイス証明書 EPA チェックを利用するすべてのクライアントでは、マシンのシステム証明書ストアにデバイス証明書がインストールされている必要があります。

クラシック **EPA** ポリシーの仮想サーバーでデバイス証明書チェックを有効にする

デバイス証明書を作成したら、NetScaler 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、NetScaler Gateway に証明書をインストールします。

1. ［構成］タブで、［**NetScaler Gateway**］**>**［仮想サーバー］に移動します。
2. **NetScaler 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」ページの「基本設定」セクションで、「編集」をクリックします。
4. 認証を無効にするには、[認証を有効にする] チェックボックスをオフにします。
5. [デバイス証明書を有効にする] ボックスを選択して、デバイス証明書を有効にします
6. [追加] をクリックして、使用可能なデバイス証明書発行者の CA 証明書名をリストに追加します。
7. CA 証明書を仮想サーバーにバインドするには、[デバイス証明書の **CA]** セクションの **[CA** 証明書] をクリックし、[追加] をクリックして証明書を選択し、[**+**] をクリックします。

> 注:
>
> 高度な 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。

Windows マシンでのデバイス証明書の検証

1. ブラウザーを開き、NetScaler Gateway FQDN にアクセスします。
2. Citrix エンドポイント分析（EPA）クライアントの実行を許可します。EPA がインストールされていない場合は、EPA をインストールします。

Citrix EPA はデバイス証明書を実行して検証し、デバイス証明書 EPA チェックに合格すると認証ページにリダイレクトされ、合格しなかった場合は EPA エラーページにリダイレクトされます。他の EPA チェックがある場合、EPA スキャンの結果は、設定された EPA チェックによって異なります。

クライアントでさらにデバッグするには、クライアントで次の EPA ログを調べます。
C:\Users<User name>\ AppData\ Local\ Citrix\ AGEE\ nsepa.txt

注:

> CRL によるデバイス証明書の検証はサポートされていません。

既存の証明書をインポートしてインストールする

April 1, 2024

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ー、または Secure Gateway を実行しているコンピューター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、必ず秘密キーもエクスポートしてください。秘密キーをエクスポートできないことがあります。つまり、NetScaler Gateway に証明書をインストールできません。この場合は、証明書署名要求 (CSR) を使用して証明書を作成します。詳細については、「証明書署名要求の作成」を参照してください。

Windows から証明書と秘密キーをエクスポートすると、コンピューターは個人情報交換 (.pfx) ファイルを作成します。このファイルは、PKCS #12 証明書として NetScaler Gateway にインストールされます。

Secure Gateway を NetScaler Gateway に置き換える場合は、Secure Gateway から証明書と秘密キーをエクスポートできます。Secure Gateway から NetScaler 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 を廃棄し、NetScaler Gateway に証明書をインストールして、構成をテストします。Secure Gateway と NetScaler Gateway が同じ FQDN を持つ場合、ネットワーク上で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 管理コンソール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はデフォルト値のままにし、パスワードを定義して、.pfx ファイルをコンピュータに保存します。証明書がエクスポートされたら、NetScaler Gateway にインストールします。

NetScaler Gateway に証明書と秘密キー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［**NetScaler**Gateway］をクリックします。

2. 詳細ペインの［はじめに］で、［**NetScaler 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)** ファイルのインストール」を選択します。
5. [**PKCS #12** ファイル名] で、[参照] をクリックし、証明書に移動して、[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 NetScaler Gateway ウィザードを終了します。

証明書が NetScaler Gateway にインストールされると、構成ユーティリティの［**SSL**］**\ >**［証明書］ノードに証明書が表示されます。

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ペインで、[**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. [キーファイル名] に、秘密キーの名前を入力するか、[参照] をクリックして既存のファイルに移動します。
4. [キーのサイズ **(**ビット**)**] に、秘密キーのサイズを入力します。
5.「公開指数値」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. [キーフォーマット] で、[PEM] または [DER] を選択します。証明書には PEM 形式を推奨します。
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] と [パスフレーズの確認] 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、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、**[Create DSA Key**] をクリックし、RSA 秘密キーを作成する手順に従います。

証明書失効リスト

April 1, 2024

認証局 (CA) は、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 Corporation を離れたとします。会社は、Ann の証明書を CRL に配置して、彼女がそのキーでメッセージに署名するのを防ぐことができます。

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は、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。

NetScaler Gateway は、次の 2 つの CRL タイプをサポートしています。

- 失効した証明書または無効になった証明書を一覧表示する CRL
- Online Certificate Status Protocol (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、次の手順を実行します。

NetScaler 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にローカルに保存されていることを確認します。高可用性セットアップの場合、CRL ファイルは両方の NetScaler 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: NetScaler ADC に追加される CRL の名前。最大 31 文字です。
- CRL ファイル: NetScaler ADC に追加される CRL ファイルの名前。NetScaler ADC は、デフォルトで/var/netscaler/ssl ディレクトリで CRL ファイルを検索します。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
- 日数: 最大 31

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. 詳細ペインで、［Add］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。

GUI で **LDAP** または **HTTP** を使用して **CRL** 自動更新を設定するには、次の手順を実行します。

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。NetScaler Gateway アプライアンスの 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。

NetScaler Gateway アプライアンスは、Web の場所または 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 ロケーションまたは LDAP サーバを指定する場合、コマンドの実行時に CRL がローカルハードディスクドライブに存在してい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の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 を格納するためのデフォルトのパスは /var/netscaler/SSL です。

CRL リフレッシュパラメータ

- **CRL** 名

  NetScaler Gateway で更新される CRL の名前。

- **CRL** 自動更新を有効にする

  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。NetScaler 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。可能な値:HTTP、LDAP。デフォルト:HTTP。

- 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。指定した範囲が
  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 の取得元の 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 サーバが通信するポート番号。

- **URL**

  CRL の取得元の 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 証明書の発行者名の代わりにベース DN 属性を使用することをお勧めします。Issuer-Name フィールドは、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**

  バインド DN 属性は、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ます。バインド DN 属性は、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。

- 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される管理者パスワード。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、パスワードが必要です。

- 間隔

  CRL リフレッシュを実行する必要がある間隔。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.

- 日数

  CRL リフレッシュを実行する必要がある日。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。

- 時間

  CRL リフレッシュを実行する必要がある正確な時刻（24 時間形式）。

- 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。可能な値: はい、いいえ。デフォルト: いいえ。

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: 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
   - スコープ
   - サーバー IP
   - ポート *
   - URL
   - ベース DN*
   - バインド DN

- パスワード
- 間隔
- 日数
- 時間

5. ［Create］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 で証明書のステータスを監視する

Online Certificate Status Protocol (OCSP) は、クライアント SSL 証明書の状態を判断するために使用されるインターネットプロトコルです。NetScaler Gateway は RFC 2560 で定義されているように OCSP をサポートしています。OCSP には、タイムリーな情報の点で、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、多額の資金や高額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。NetScaler Gateway の OCSP の実装には、要求のバッチ処理と応答のキャッシュが含まれます。

OCSP の **NetScaler Gateway** 実装

NetScaler Gateway アプライアンスでの OCSP 検証は、NetScaler Gateway が SSL ハンドシェイク中に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、NetScaler Gateway は OCSP 要求を作成し、OCSP レスポンダーに転送します。そのために、NetScaler Gateway は、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、ローカルで構成された URL を使用します。NetScaler 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一時停止状態になります。サーバーからの応答が構成された時間を超えて遅延し、他のレスポンダーが構成されていない場合、NetScaler Gateway は、OCSP チェックをオプションまたは必須に設定したかどうかに応じて、トランザクションを許可するかエラーを表示します。NetScaler Gateway は、OCSP 要求のバッチ処理と OCSP 応答のキャッシュをサポートして、OCSP レスポンダーの負荷を軽減し、応答を高速化します。

OCSP リクエストのバッチング

NetScaler 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避けるために、NetScaler Gateway は同じ要求で複数のクライアント証明書の状態を照会できます。リクエストのバッチ処理を効率的に実行するには、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、ユーザへの応答が速くなり、OCSP レスポンダの負荷が軽減されます。OCSP レスポンダーからクライアント証明書の失効ステータスを受信すると、NetScaler Gateway は

事前定義された時間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、NetScaler Gateway はまずローカルキャッシュでこの証明書のエントリを確認します。まだ有効な（キャッシュタイムアウト制限内で）エントリが見つかると、その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、NetScaler Gateway は OCSP レスポンダーに要求を送信し、構成された期間応答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

オンライン証明書状態プロトコル (OCSP) を構成するには、OCSP レスポンダの追加、OCSP レスポンダを認証局 (CA) からの署名付き証明書にバインドし、証明書と秘密キーを Secure Sockets Layer (SSL) 仮想サーバーにバインドします。構成済みの 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、まずレスポンダーをバインド解除してから、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. 詳細ペインで、［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 文字を超えることはできません。
5. OCSP 応答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、NetScaler Gateway が応答を保持する分数を入力します。
6. [要求バッチ処理] で、[有効にする] をクリックします。
7. [バッチング遅延] で、OCSP 要求のグループをバッチ処理する時間をミリ秒単位で指定します。

   指定できる値は 0 ～10000 です。デフォルトは 1 です。
8. ［時間スキューで生成される時間］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ときに NetScaler 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場合は、[応答の検証] で [応答を信頼する] を選択します。

   信頼応答を有効にする場合は、ステップ 8 とステップ 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 が応答の検証に使用されます。
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も含まれます。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、リクエストは署名されません。
13. 一度使用した番号を有効にするには(nonce)extension、[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。

NetScaler Gateway の構成をテストする

April 1, 2024

NetScaler 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。

NetScaler 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 Secure Access クライアント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 Secure Access クライアントをインストールして正常に接続すると、Access Interface が表示されます。Access Interface は、NetScaler Gateway のデフォルトのホームページです。

GUI を使用してユーザアカウントを作成する

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、[**NetScaler Gateway] > [**ユーザー管理] を展開し、[**AAA** ユーザー] をクリックします。
2. 詳細ペインで、[Add] 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、NetScaler 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] に、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に問題がある場合は、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 NetScaler Gateway にインストールされています。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、対応するルート証明書がユーザーデバイスにあることを確認します。
- 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、および 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。また、ホスト名が署名付き証明書の IP アドレスと一致しないという問題もあります。構成された証明書の共通名が、構成された仮想サーバの 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、または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。

NetScaler Gateway ソフトウェアをアップグレードする

April 1, 2024

新しいリリースが利用可能になったら、NetScaler Gateway にあるソフトウェアをアップグレードできます。アップデートは、Citrix Web サイトで確認できます。新しいリリースにアップグレードできるのは、アップデートのリリース時に NetScaler Gateway ライセンスが Subscription Advantage プログラムの下にある場合のみです。Subscription Advantage はいつでも更新できます。詳細については、NetScaler サポート Web サイトを参照してください 。

アップグレードパスと互換性のある製品情報は、『Citrix アップグレードガイド』にも記載されています。

最新の NetScaler Gateway メンテナンスリリースの詳細については、Citrix ナレッジセンターを参照してください。

ソフトウェアアップデートの確認

1. Citrix の Web サイトに移動します。
2. [**My Account**] をクリックしてログオンします。
3. [**Downloads**] をクリックします。
4. [ダウンロードの検索] で [**NetScaler Gateway**] を選択します
5. 「ダウンロード・タイプの選択」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、NetScaler 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. NetScaler Gateway ページで、[**NetScaler Gateway**] または [アクセスゲートウェイ] 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。

ソフトウェアがコンピュータにダウンロードされたら、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 **NetScaler Gateway** をアップグレードする

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、[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 **NetScaler Gateway** をアップグレードする

1. ソフトウェアを NetScaler Gateway にアップロードするには、WinSCP などのセキュア 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. NetScaler Gateway にログオンします。
5. コマンドプロンプトで、次のように入力します。`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. ソフトウェアをアンパックするには、tar –xvzf build_x_xx.tgz と入力します。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、NetScaler Gateway を再起動します。

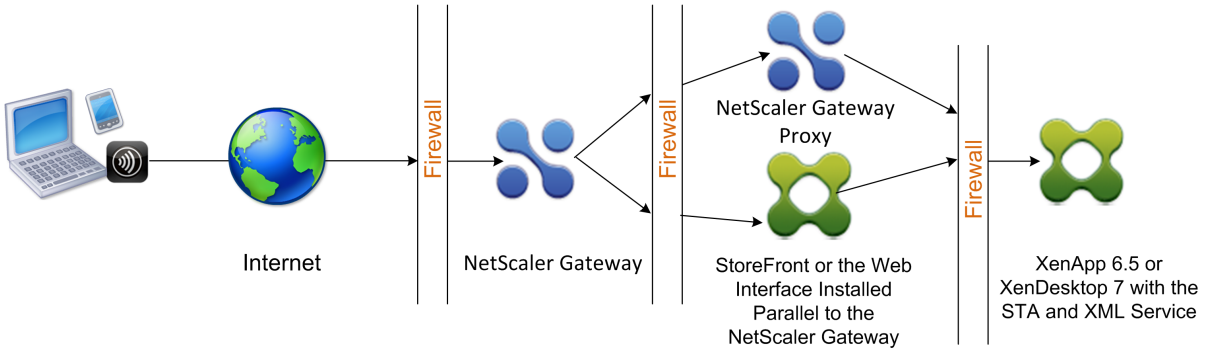
NetScaler Gateway の再起動後、インストールが正常に完了したことを確認するには、構成ユーティリティを起動します。アプライアンス上の NetScaler Gateway のバージョンが右上隅に表示されます。

NetScaler Gateway をダブルホップ **DMZ** に展開する

April 1, 2024

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 に展開された NetScaler Gateway アプライアンス



> 注:
>
> 上記の例では、説明のために、StoreFront、Web Interface、Citrix Virtual Apps で 3 つのファイアウォールを使用するダブルホップ構成について説明しています。ただし、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があるダブルホップ DMZ を使用することもできます。DMZ に 1 つのアプライアンスとセキュアネットワークに 1 つのアプライアンスを持つダブルホップ構成を設定する場合、第 3 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 を構成して、Citrix StoreFront または NetScaler Gateway プロキシと並行してインストールされた Web Interface をサポートできます。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 NetScaler Gateway を展開すると、Citrix Workspace アプリ用の電子メールベースの自動検出は機能しません。

ダブルホップ展開の仕組み

NetScaler 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。ダブルホップ展開の接続は、次のように発生します:

- 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して、最初の DMZ で NetScaler Gateway に接続します。
- Citrix Workspace アプリがユーザーデバイスで起動します。ユーザーは NetScaler Gateway に接続して、セキュリティで保護されたネットワーク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: Secure Hub と Windows 向け Citrix Secure Access クライアントは、ダブルホップ DMZ 展開ではサポートされません。Citrix Workspace アプリのみがユーザー接続に使用されます。

- 最初の DMZ の NetScaler 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 NetScaler Gateway は、ユーザー接続を暗号化し、ユーザーの認証方法を決定し、内部ネットワークのサーバーへのアクセスを制御します。
- 2 番目の DMZ の NetScaler Gateway は、NetScaler Gateway プロキシデバイスとして機能します。この NetScaler Gateway を使用すると、ICA トラフィックが 2 番目の DMZ を通過してサーバーファームへのユーザー接続を完了できます。最初の DMZ の NetScaler 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 NetScaler Gateway を介してプロキシされます。

NetScaler Gateway は、IPv4 接続と 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サポートを示します。

ICA 機能	ダブルホップサポート
SmartAccess	はい
SmartControl	はい
Enlightened Data Transport（EDT）	はい
HDX Insight	はい
ICA セッション信頼性 (ポート 2598)	はい
ICA セッションの移行	はい
ICA セッションタイムアウト	はい
マルチストリーム ICA	はい (TCP のみ)
Framehawk	いいえ
UDP オーディオ	いいえ

ダブルホップ **DMZ** 展開の準備

ダブルホップ DMZ 展開を設定する場合は、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たいですか?
- ファイアウォールではどのポートを開けますか?
- SSL 証明書はいくつ必要ですか?
- 展開を開始する前に必要なコンポーネントは何ですか?

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のに役立つ情報が含まれています。

展開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 NetScaler Gateway アプライアンス（DMZ ごとに 1 つ）が使用可能である必要があります。
- Citrix Virtual Apps を実行するサーバーは、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 NetScaler Gateway に 1 つの 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。この証明書により、Web ブラウザーと NetScaler Gateway へのユーザー接続が暗号化されます。

  ダブルホップ DMZ 展開内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** 展開での通信フロー

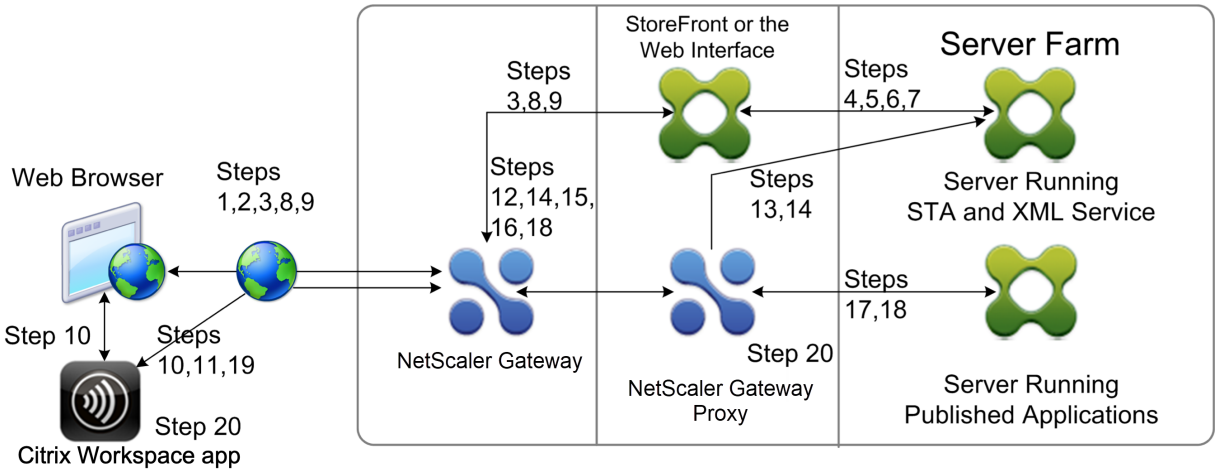
February 1, 2024

ダブルホップ DMZ 展開に関連する構成の問題を理解するには、ダブルホップ DMZ 展開内のさまざまな NetScaler Gateway および Citrix Virtual Apps コンポーネントがユーザー接続をサポートするためにどのように通信するかについての基本的な理解が必要です。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 つの連続したフローで行われますが、このプロセスには次の高レベルのステップが含まれます。

- ユーザーを認証する
- セッションチケットを作成する
- Citrix Workspace アプリを起動する
- 接続を完了する

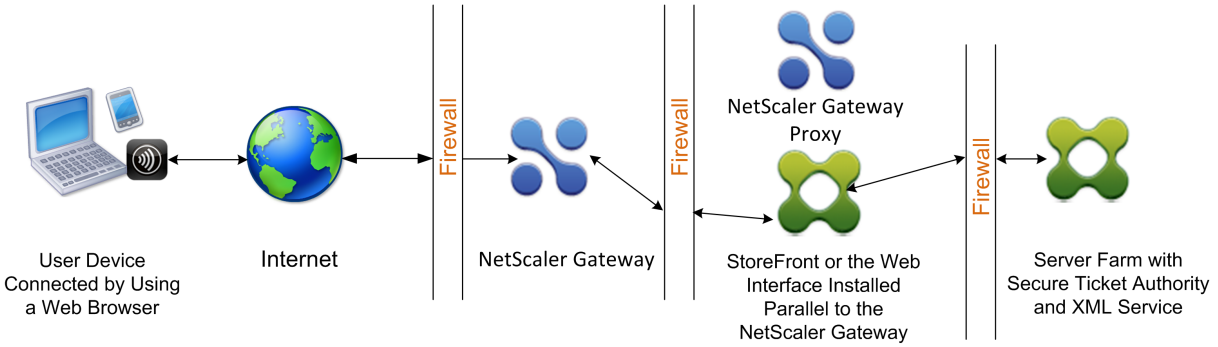
次の図は、StoreFront または Web Interface へのユーザー接続プロセスで発生する手順を示しています。セキュリティで保護されたネットワークでは、Citrix Virtual Apps を実行しているコンピューターは、Secure Ticket Authority（STA）、XML サービス、および公開アプリケーションも実行しています。



接続プロセス

ユーザの認証は、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、この展開でのユーザー接続プロセスを示しています。



ユーザー認証段階では、次の基本プロセスが発生します。

1. ユーザーが NetScaler Gateway のhttps://www.ng.wxyco.comなどのアドレスを Web ブラウザーで入力して、最初の DMZ で NetScaler Gateway に接続します。NetScaler Gateway でログオンページ認証を有効にした場合、NetScaler Gateway はユーザーを認証します。
2. 最初の DMZ の NetScaler Gateway が要求を受信します。
3. NetScaler Gateway は、Web ブラウザー接続を 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 サービスにユーザー資格情報を送信します。
5. Citrix 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。

   注:

- NetScaler Gateway で認証を有効にすると、アプライアンスは NetScaler 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情報を入力すると、アプライアンスがユーザーを認証します。その後、NetScaler Gateway はユーザーの資格情報を Web Interface に返します。
- 認証を有効にしない場合、NetScaler Gateway は認証を実行しません。アプライアンスは Web インターフェイスに接続し、Web インターフェイスのログオンページを取得し、Web インターフェイスのログオンページをユーザーに送信します。ユーザーは Web Interface のログオンページで認証資格情報を入力し、NetScaler Gateway はユーザーの資格情報を Web Interface に返します。

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接続プロセスの第 **2** 段階です。

セッションチケットの作成段階では、次の基本プロセスが発生します。

7. Web Interface は、内部ネットワーク内の XML サービスおよび 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ごとに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。
8. 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。次に、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ていますが、実際の IP アドレスは含まれません。
9. 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 によって発行されたチケットが含まれています。次に、Web Interface は、公開アプリケーションへのリンクの一覧を Web ページを作成して入力し、この Web ページをユーザーデバイス上の Web ブラウザに送信します。

   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。

10. ユーザーが 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 ブラウザーに 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 NetScaler 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）名も含まれています。

11. Web ブラウザで Receiver が起動し、ユーザーは ICA ファイル内の NetScaler Gateway 名を使用して、最初の DMZ で NetScaler Gateway に接続します。最初の SSL/TLS ハンドシェークは、NetScaler Gateway を実行しているサーバーのアイデンティティを確立するために発生します。

    接続の完了は、ダブルホップ **DMZ** 展開におけるユーザ接続プロセスの第 **4** 段階であり、最後の段階です。

    接続完了段階では、次の基本プロセスが発生します。

    - ユーザーが 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 ブラウザーは、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 NetScaler Gateway への ICA 接続を開始します。
- 最初の DMZ の NetScaler Gateway は、内部ネットワーク内の Secure Ticket Authority（STA）と通信して、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ーの実際の IP アドレスに解決します。この通信は、NetScaler 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 NetScaler 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 NetScaler Gateway アプライアンスを介して、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。

12. 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 で NetScaler Gateway に送信します。
13. 最初の DMZ の NetScaler 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、NetScaler Gateway は、2 番目の DMZ の NetScaler Gateway プロキシへの SSL 接続を備えた SOCKS または SOCKS を確立します。
14. 2 番目の DMZ の NetScaler Gateway プロキシは、内部ネットワークの STA にチケット検証要求を渡します。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ーにチケットをマッピングします。
15. STA は、2 番目の DMZ の NetScaler Gateway プロキシに応答を送信します。この応答は、最初の DMZ で NetScaler Gateway に渡されます。この応答により、チケットの検証が完了し、公開アプリケーションをホストするコンピュータの IP アドレスが含まれます。
16. 最初の DMZ の NetScaler 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 NetScaler Gateway プロキシに送信します。
17. 2 番目の DMZ の NetScaler Gateway プロキシは、接続パケットで指定されたサーバーに接続要求を行います。
18. サーバーは、2 番目の DMZ の NetScaler Gateway プロキシに応答します。2 番目の DMZ の NetScaler Gateway プロキシは、この応答を最初の DMZ の NetScaler Gateway に渡して、最初の DMZ のサーバーと NetScaler Gateway の間の接続を完了します。
19. 最初の DMZ の NetScaler 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。
20. ICA トラフィックは、ユーザーデバイスとサーバーの間で、最初の DMZ の NetScaler Gateway、2 番目の DMZ の NetScaler Gateway プロキシを介して流れます。

ダブルホップ **DMZ** での **NetScaler Gateway** のインストールと構成

April 1, 2024

ダブルホップ DMZ に NetScaler Gateway を展開するには、いくつかの手順を完了する必要があります。手順には、両方の DMZ へのアプライアンスのインストールと、アプライアンスのユーザーデバイス接続の設定が含まれます。

最初の **DMZ** に **NetScaler Gateway** をインストールする

最初の DMZ に NetScaler Gateway をインストールするには、「ハードウェアのインストール」の手順に従います。

最初の DMZ に複数の NetScaler 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 **NetScaler Gateway** を構成する

ダブルホップ DMZ 展開では、最初の DMZ の各 NetScaler Gateway を構成して、2 番目の DMZ の StoreFront または Web Interface のいずれか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、NetScaler Gateway 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実行されます。NetScaler Gateway を介して Web Interface に接続するには、Web Interface へのリダイレクトが有効になっている NetScaler Gateway ユーザーグループにユーザーを関連付ける必要があります。

第 **2** の **DMZ** に **NetScaler Gateway** をインストールする

2 番目の DMZ の NetScaler Gateway アプライアンスは、ICA および Secure Ticket Authority（STA）トラフィックを 2 番目の DMZ でプロキシするため、NetScaler Gateway プロキシと呼ばれます。
ハードウェアをインストールして、 各 NetScaler Gateway アプライアンスを 2 番目の 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 番目の DMZ に他のアプライアンスをインストールできます。

2 番目の DMZ に NetScaler 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。

- NetScaler Gateway プロキシで仮想サーバーを構成します。
- 第 1 および第 2DMZ の NetScaler 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 番目の DMZ の NetScaler Gateway をグローバルに、または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。

NetScaler Gateway プロキシの仮想サーバーの設定を構成する

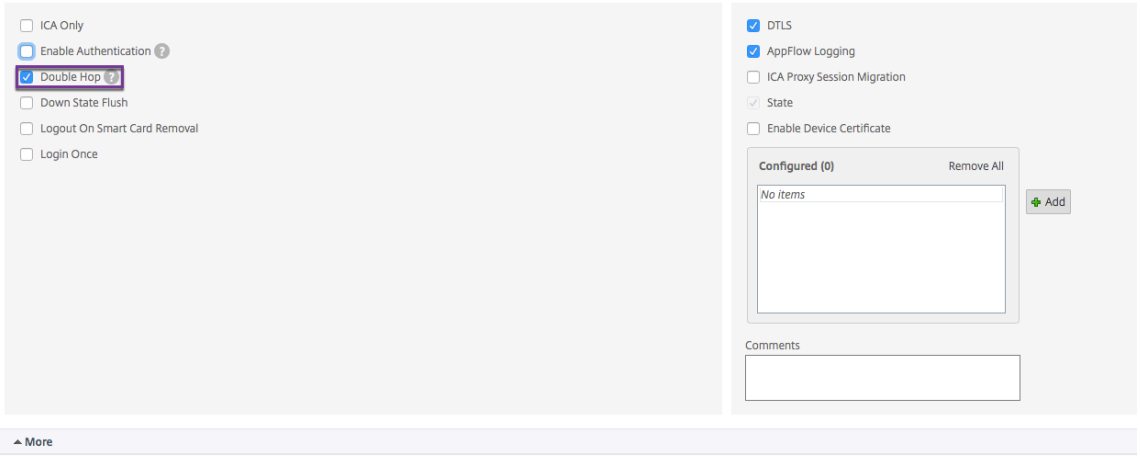
April 1, 2024

NetScaler Gateway アプライアンス間の接続を許可するには、NetScaler 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、NetScaler 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 NetScaler Gateway で、2 番目の DMZ の NetScaler Gateway と通信するように仮想サーバーを構成します。NetScaler Gateway プロキシで認証またはポリシーを構成しないでください。仮想サーバーで認証を無効にすることをお勧めします。

GUI を使用して NetScaler 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

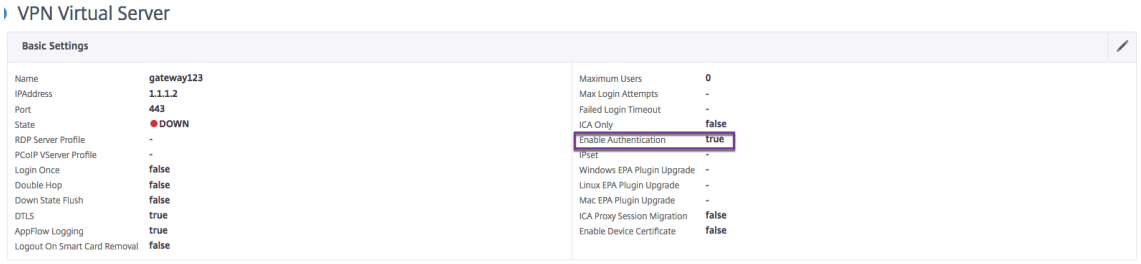
1. 構成 **> NetScaler Gateway >** 仮想サーバーに移動します。
2. 仮想サーバを選択し、[編集（Edit）] をクリックします。
3. [基本設定] セクションで、[編集] アイコンをクリックし、[詳細] をクリックします。
4. [ダブルホップ] を選択します。



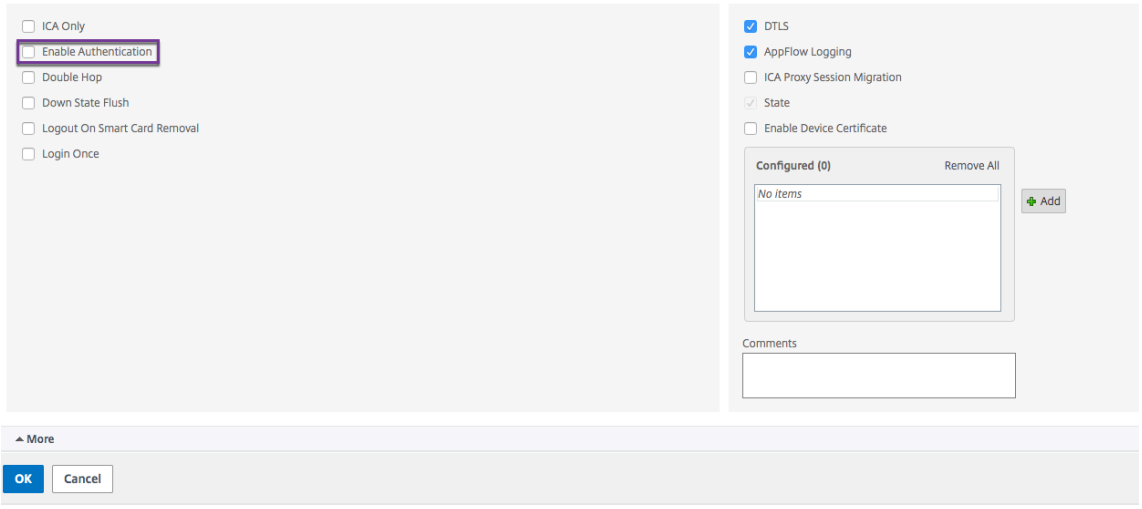
5. [**OK**] をクリックします。

GUI を使用して NetScaler Gateway プロキシ上の仮想サーバーで認証を無効にするには

1. 構成 **> NetScaler Gateway >** 仮想サーバーに移動します。
2. 仮想サーバを選択し、[編集（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、[詳細] 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ようにアプライアンスを設定する

February 1, 2024

ダブルホップ DMZ に NetScaler Gateway を展開する場合は、最初の DMZ で NetScaler Gateway を構成して、2 番目の DMZ の NetScaler Gateway プロキシと通信する必要があります。

2 番目の DMZ に複数のアプライアンスを展開する場合は、最初の DMZ の各アプライアンスが 2 番目の DMZ のすべてのプロキシアプライアンスと通信するように設定します。

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、[NetScaler Gateway] > [リソース] の順に展開し、[
ネクストホップサーバー] をクリックします。次の手順の手順に従って、[
IPv6] チェックボックスをオンにします。

NetScaler Gateway プロキシと通信するように **NetScaler Gateway** を構成するには

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［リソース］の順に展開し、［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、［Add］をクリックします。
3. [名前] に、最初の NetScaler Gateway の名前を入力します。
4. [IP アドレス] に、2 番目の DMZ にある NetScaler Gateway プロキシの仮想サーバー 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 などのセキュアな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ている各 NetScaler Gateway を、2 番目の DMZ にインストールされているすべての NetScaler 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。

NetScaler Gateway プロキシの設定を構成したら、NetScaler Gateway グローバルのネクストホップサーバーまたは仮想サーバーにポリシーをバインドします。

NetScaler 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、［NetScaler Gateway］>［リソース］の順に展開し、［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、ネクストホップサーバーを選択し、[操作] で [グローバルバインド] を選択します。
3. ［ネクストホップサーバー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ー名］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。

NetScaler Gateway 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、［NetScaler Gateway］を展開し、［仮想サーバー］をクリックします。
2. 詳細ペイン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 および **ICA** トラフィックを処理するように **NetScaler Gateway** を構成する

April 1, 2024

ダブルホップ DMZ に NetScaler Gateway を展開する場合は、最初の DMZ で NetScaler 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 をグローバルに設定してバインドするには、次の手順を実行します。

1. GUI の［構成］タブで、［**NetScaler 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** サーバーのバインド/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 を実行しているサーバーへのパス (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

1. GUI の［構成］タブで、［**NetScaler Gateway** ］を展開し、［仮想サーバー］をクリックします。
2. 詳細ペイン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 を実行しているサーバーへのパス (http://mycompany.comまたはhttp://ipAddressなど) を入力し、[作成] をクリックします。

注:

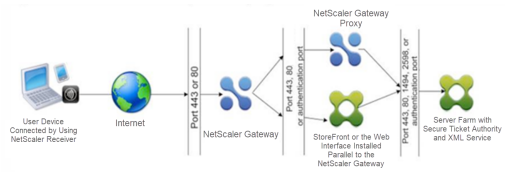
VPN 仮想サーバーが同じネクストホップ仮想サーバーと STA サーバーを共有している場合、同じネクストホップ仮想サーバーを共有する仮想サーバーから共通 STA サーバーがバインド解除されると、接続がリセットされます。

ファイアウォールの適切なポートを開きます

February 1, 2024

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。接続プロセスの詳細については、ダブルホップ DMZ 展開での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 展開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、その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	使用ポート
インターネットからの Web ブラウザは、最初の DMZ で NetScaler Gateway に接続します。注: NetScaler Gateway には、ポート 80 で確立された接続をセキュアポートにリダイレクトするオプションがあります。NetScaler 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を介してポート 80 を開くことができます。ユーザーがポート 80 で NetScaler Gateway に暗号化されていない接続を行うと、NetScaler Gateway は自動的に安全なポートに接続をリダイレクトします。	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。
インターネットからの Citrix Workspace アプリは、最初の DMZ で NetScaler 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。

次の表は、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ています。

第 2 ファイアウォール経由の接続	使用ポート
最初の DMZ の NetScaler 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介したセキュアな接続の場合は TCP ポート 443 を開きます。
最初の DMZ の NetScaler Gateway は、2 番目の DMZ の NetScaler 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安全な SOCKS 接続を確立します。
最初の DMZ で NetScaler 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る場合があります。	認証サーバが接続をリッスンする TCP ポートを開きます。例としては、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、第 3 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。

第 3 ファイアウォール経由の接続	使用ポート
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。	セキュアでない接続の場合はポート 80 を、3 番目のファイアウォールを介したセキュアな接続にはポート 443 を開きます。
2 番目の DMZ の StoreFront または 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。	セキュアでない接続の場合はポート 80 を、3 番目のファイアウォールを介したセキュアな接続にはポート 443 を開きます。

第 3 ファイアウォール経由の接続	使用ポート
2 番目の DMZ の NetScaler Gateway は、セキュアネットワークに存在する STA に接続します。	セキュアでない接続の場合はポート 80 を、3 番目のファイアウォールを介したセキュアな接続にはポート 443 を開きます。
2 番目の DMZ の NetScaler Gateway は、内部ネットワーク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への ICA 接続を確立します。	TCP ポート 1494 を開いて、第 3 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 で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 NetScaler 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る場合があります。	認証サーバが接続をリッスンする TCP ポートを開きます。例としては、RADIUS 用のポート 1812、LDAP 用のポート 389 などがあります。

システムのメンテナンスとモニタリング

February 1, 2024

NetScaler 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。次の方法でこれを行うことができます。

- NetScaler Gateway を最新バージョンのソフトウェア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、NetScaler Gateway ダウンロードサイトに移動してソフトウェアをダウンロードできます。メンテナンスビルドの Readme は、Citrix ナレッジセンターで参照できます。
- NetScaler Gateway の構成タスクと管理タスクを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、個人にアクセスレベルを割り当てて、NetScaler Gateway での特定のタスクの実行を制限できます。
- NetScaler Gateway 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済み構成を比較できます。NetScaler Gateway から構成を消去することもできます。
- NetScaler Gateway 構成ユーティリティでは、ユーザーセッションを表示、更新、およびエンドユーザーセッションできます。
- NetScaler Gateway でログを構成できます。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。

委任管理者の構成

February 1, 2024

NetScaler Gateway には、デフォルトの管理者ユーザー名とパスワードがあります。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。

さらに管理者アカウントを作成し、各アカウントに NetScaler Gateway への異なるアクセスレベル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、委任管理者と呼ばれます。たとえば、NetScaler Gateway の接続とログを監視する担当者が 1 人、NetScaler Gateway の特定の設定を構成する別の担当者が割り当てられているとします。最初の管理者は読み取り専用アクセス権を持ち、2 番目の管理者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、およびシステムユーザーとグループを使用します。

委任管理者を設定する場合、構成プロセスは次のとおりです。

- 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、所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。コマンドポリシーを使用すると、ユーザーまたはグループがアクセスおよび変更できる NetScaler 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、および管理者とグループが設定できるその他の要素などのコマンドを制御することもできます。
- 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、NetScaler Gateway が優先するポリシーを判断できるようにします。

NetScaler Gateway には、デフォルトの拒否システムコマンド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。ポリシーをシステム管理者（ユーザー）またはグループに直接バインドします。ユーザーおよび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、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、NetScaler 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設定して、ユーザー権利の割り当てに関する詳細レベルをより詳細に定義できます。たとえば、セッションポリシーを NetScaler Gateway に追加する権限をあるユーザーに付与し、そのユーザーに他の構成の実行を許可することはできません。

委任管理者のコマンドポリシーの設定

April 1, 2024

NetScaler Gateway には、委任管理に使用できる 4 つの組み込みコマンドポリシーがあります。

- 読み取り専用では、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が許可されます。

- **Operator** は読み取り専用アクセスを許可し、サービスでコマンドを有効または無効にするアクセスも許可します。このポリシーでは、サービスおよびサーバーを「アクセスダウン」に設定するためのアクセスも許可します。
- ネットワークは、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。
- スーパーユーザは、デフォルトの管理者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、システムユーザー、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。

NetScaler 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. 詳細ペインで、[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] フィールドと [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、「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 **>** アクション **>** 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」をクリックします。

管理グループの作成

管理グループには、NetScaler Gateway の管理権限を持つユーザーが含まれます。構成ユーティリティで管理グループを作成できます。

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. 詳細ペインで、[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 [操作] で、[挿入] をクリックし、1 つまたは複数のポリシーを選択し、[**OK**]、[作成]、[閉じる] の順にクリックします。

委任管理者用のカスタムコマンドポリシーの設定

April 1, 2024

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。コマンド仕様により、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 コマンドを使用する権限を拒否するとします。ポリシーを設定するときは、アクションを deny に設定し、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ときは、NetScaler Gateway や認証などのアプライアンス上のコンポーネントを構成します。詳細ポリシーを設定するときは、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、そのグループで管理者が実行できるコマンドを選択します。

簡単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. 詳細ペインで、[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. [コマンド仕様] 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 [単純] 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. 詳細ペインで、[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. [コマンド仕様] 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. [**Entity Group**] 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**]**、 [閉じる] の順にクリックします。

   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. [作成**]** をクリックし、 [閉じる] 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**]**、 [閉じる] の順にクリックします。

「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「コマンド仕様」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、一覧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。

NetScaler Gateway での監査の構成

February 1, 2024

NetScaler 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、および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保存される場所を決定する設定を構成できます。

NetScaler Gateway は現在、ローカルログ用の独自のログ形式と、syslog サーバーで使用する syslog 形式の 2 つのログ形式をサポートしています。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。ログのエントリは、NetScaler Gateway が使用できなくなる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	NetScaler Gateway が正しく機能しない可能性があるが、その操作にとって重要ではない問題をログに記録します。NetScaler Gateway で重大な問題が発生するのを防ぐために、できるだけ早く是正措置を講じることができます。
クリティカル	NetScaler Gateway の操作を制限しないが、より大きな問題にエスカレートする可能性のある重大な状態を記録します。
エラー	NetScaler Gateway で失敗した操作の結果として生じるエントリを記録します。
警告	エラーまたは重大なエラーにつながる可能性のある潜在的な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記録しますが、通知と同じ目的を果たします。
情報	NetScaler Gateway によって実行されたアクションを記録します。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 圧縮を構成した場合、NetScaler Gateway 監査ログには、NetScaler Gateway の圧縮統計も格納されます。異なるデータに対して達成された圧縮率は、各ユーザーセッションのログファイルに格納されます。

NetScaler Gateway はログ署名セッション ID を使用します。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。ユーザが同じユーザデバイスから同じ IP アドレスを持つ 2 つのセッションを確立する場合、各セッションは一意の sessionID を持ちます。

> 重要**:** カスタムログ解析スクリプトを作成した場合は、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。

NetScaler Gateway でのログの構成

April 1, 2024

NetScaler Gateway でログを構成するときは、監査ログを NetScaler Gateway に保存するか、syslog サーバーに送信するかを選択できます。構成ユーティリティを使用して、監査ポリシーを作成し、監査ログを格納するための設定を構成します。

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、［**NetScaler 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 は、ログを Syslog サーバに送信する場合に使用します。
   - `Nslog`で NetScaler Gateway にログを保存します。
     > 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. 詳細ペインで、[追加] をクリックします。
5. ログが保存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. [作成] をクリックし、[閉じる] をクリックします。

監査ポリシーを作成したら、次の任意の組み合わせにポリシーをバインドできます。

- グローバルに
- 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、［**NetScaler Gateway** ］ > ［ポリシー］ > ［監査］の順に展開します。
2. **`Syslog`**または**`Nslog`**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、［**NetScaler Gateway** ］ > ［ポリシー］ > ［監査］の順に展開します。
2. **Syslog**または**Nslog**を選択します。
3. 詳細ウィンドウで、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

NetScaler 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、［**NetScaler Gateway** ］ > ［ポリシー］ > ［監査］の順に展開します。
2. [**Syslog**] または [**Nslog**] を選択します。
3. 詳細ウィンドウで、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

February 1, 2024

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記録するように NetScaler 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、有効にしたロギングのタイプ（syslog または nslog）に応じて、syslog またはnslogファイルのいずれかに保存されます。

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 に一致する場合、最初のパケットの詳細だけがロギングされます。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、次のパラメータに対して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
- Destination port
- 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はない場合、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、カウンタは増加します）。

> **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。

次の表に、拡張 ACL のルールレベルで ACL ロギングを設定するためのパラメータを示します。

パラメーター名	説明
Logstate	ACL のロギング機能の状態。有効な値: 有効および無効。 デフォルト: 無効。
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、NetScaler 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。

NetScaler Gateway で **ACL** または **TCP** の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、[**NetScaler Gateway**] > [ポリシー] > [監査] の順に展開します。
2. syslog またはnslog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 Secure Access ログの有効化

April 1, 2024

Citrix Secure Access クライアントは、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記録するように構成できます。ユーザーは、Citrix Secure Access クライアントを構成して、ユーザーデバイスへのログレベルを設定して特定のユーザーアクティビティを記録できます。ユーザーがログを構成すると、プラグインはユーザーデバイスに次の 2 つのファイルを作成します。

- hooklog\ .txt は、Citrix Secure <num\ > Access クライアントが生成するインターセプト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。Citrix では、ファイルを定期的に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 (すべてのユーザー): %SystemDrive%:\Documents and Settings\All Users\Application Data\Citrix\AGEE
- Windows XP (ユーザー固有): %SystemDrive%:\Documents and Settings\%username%\Local Settings\Application Data\Citrix\AGEE
- Windows Vista (すべてのユーザー): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows Vista (ユーザー固有): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE
- Windows 7 (すべてのユーザー): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows 7 (ユーザー固有): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE
- Windows 8（すべてのユーザー）: %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows 8（ユーザー固有）: %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE

これらのログファイルを使用して、Citrix Secure Access クライアント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、ユーザーは Citrix Secure Access クライアント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 Secure Access クライアントの統計情報を記録する
- 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

Windows 向け Citrix Secure Access クライアントのログ機能について詳しくは、「Windows クライアントのログ収集の改善」を参照してください。

ICA 接続を監視するには

February 1, 2024

サーバーファームのアクティブなユーザーセッションは、[
ICA 接続] ダイアログボックスを使用して監視できます。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］**>**［**NetScaler**Gateway］に移動します。
2.「モニター接続」セクションで、「**ICA** 接続」をクリックします。

ICA セッションログ

ns.logファイルには、ICA セッションログが次の形式で印刷されます:

```
1 May  2 09:29:02 <local0.info> 10.106.40.223  05/02/2023:09:29:02 GMT
     0-PPE-1 : default ICA Message 141327 0 :  "[Remote ip =
     10.10.99.86:514] [EDT] [CGP][ICAUUID=0006ab3454-d7de-1450-9678-
     c6333447a76] Received response from STA server {
2  sta-server=10.11.40.222:80,type=ResponseData }
3  "
4 <!--NeedCopy-->
```

リリースバージョン 13.1 ビルド 50.x 以降、ICA ログに次の拡張が加えられました:

- TCP、EDT、CGP、SOCKS などの接続タイプを表示します。
- ICA ユニバーサルユニーク識別子 (UUID) を表示します。
- すべての STA ログは情報レベルのログとして表示されます。

認証と承認

February 1, 2024

NetScaler Gateway は、NetScaler Gateway のユーザー認証を広範囲に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、サーバーでユーザーを認証するように NetScaler Gateway を構成できます。NetScaler Gateway 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しています。NetScaler 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。

NetScaler Gateway 認証には、ローカルユーザーと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。この設計は、構成する認証手順を制御するためのポリシーの使用を中心にしています。作成したポリシーは、

NetScaler Gateway グローバ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を設定するために使用できます。

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

NetScaler Gateway には、次の認証タイプがサポートされています。

- ローカル
- ライトウェイトディレクトリアクセスプロトコル（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）

NetScaler Gateway は、RSA SecurID、ジェムアルト・プロティバ、SafeWord もサポートしています。これらの認証の種類を構成するには、RADIUS サーバーを使用します。

認証によってユーザーは NetScaler Gateway にログオンして内部ネットワークに接続できますが、承認はユーザーがアクセスできるセキュアネットワーク内のリソースを定義します。LDAP ポリシーと RADIUS ポリシーを使用して認可を設定します。

デフォルトのグローバル認証タイプの設定

April 1, 2024

NetScaler Gateway をインストールして NetScaler 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、NetScaler Gateway グローバルレベルに自動的にバインドされます。NetScaler Gateway ウィザードで構成する認証タイプがデフォルトの認証タイプです。NetScaler Gateway ウィザードを再度実行してデフォルトの認証タイプを変更するか、構成ユーティリティでグローバル認証設定を変更できます。

追加の認証の種類を追加する必要がある場合は、NetScaler 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 NetScaler 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、優先度を設定して、優先する認証タイプを定義できます。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。

ログオンページを NetScaler Gateway のインメモリキャッシュから配信するか、NetScaler 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ことを選択した場合、NetScaler Gateway からのログオンページの配信は、HTTP サーバーからの配信よりも大幅に高速

です。インメモリキャッシュからログオンページを配信するように選択すると、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 アドレスを設定することもできます。この IP アドレスは認証用に固有のもので、NetScaler Gateway のサブネット、マップ、または仮想 IP アドレスではありません。この設定はオプションです。

注：NetScaler 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認証を構成できます。ウィザードを実行すると、NetScaler Gateway で構成されている既存の LDAP 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、［NetScaler Gateway］を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウの [設定] で、[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、認証用の一意の 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] を選択すると、ログオンページが高速に配信されます。
6. 認証が失敗した場合にユーザーにメッセージを表示するには、[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、パスワードエラー、アカウントが無効またはロックされている、またはユーザーが見つからない、などが含まれます。
7. [既定の認証タイプ] で、認証タイプを選択します。
8. 認証タイプの設定を構成し、[OK] をクリックします。

認可なしの認証の設定

February 1, 2024

承認は、ユーザーが NetScaler Gateway を介して接続できるリソースを定義します。式を使用して承認ポリシーを構成し、ポリシーを許可または拒否するように設定します。NetScaler Gateway は、承認なしで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、NetScaler 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設定したポリシーは、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

February 1, 2024

承認は、ユーザーが NetScaler Gateway にログオンした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。承認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。

NetScaler Gateway での承認は、承認ポリシーと式を使用して構成します。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承認ポリシーをバインドできます。

承認ポリシーの構成

April 1, 2024

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。

CLIENT.IP.DST.IN_SUBNET (10.3.0.0/16)

承認ポリシーは、ユーザーおよびグループに適用されます。ユーザーが認証されると、NetScaler 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することにより、グループ認証チェックを実行します。ユーザーがグループ情報にアクセスできる場合、NetScaler 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確認します。

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する場合は、サブディレクトリパスだけを使用でき、ルートディレクトリは使用できません。たとえば、fs.path には「\\ rootdir\\ dir1\\ dir2」が含まれているのではなく、fs.path には「\\ dir1\\ dir2」が含まれています。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、仮想サーバにバインドされたポリシーに対して最初に検証され、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する場合は、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 0 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プライオリティ番号が 1 で、ユーザ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。

> 重要:
>
> - 従来の認可ポリシーは、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は、すべてのタイプのトラフィックに適用できます (TCP/UDP/ICMP/DNS).
>   - To apply policy on UDP/ICMP/DNS traffic, policies must be bound at type UDP_REQUEST, ICMP_REQUEST, and DNS_REQUEST respectively.
>   - While binding, if “type” is not explicitly mentioned or “type” is set to REQUEST, the behavior does not change from earlier builds, that is these policies are applied only to TCP traffic.
>   - The policies bound at UDP_REQUEST do not apply for DNS traffic. For DNS, policies must be explicitly bound to DNS_REQUEST TCP_DNS is similar to other TCP requests.

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

承認ポリシー表現の例

権限付与ポリシーの表現例を以下に示します。

- `add authorization policy athzPol1 "HTTP.REQ.USER.IS_MEMBER_OF(\"allowedGroup\")"ALLOW`
- `add authorization policy athzPol2 "CLIENT.IP.DST.BETWEEN(10.102.75.10,10.1 "DENY`
- `add authorization policy athzPol3 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv")|| CLIENT.IP.DST.IN_SUBNET(10.102.75.0/25)"ALLOW`

GUI を使用して認可ポリシーを設定するには

1. **NetScaler Gateway >** ポリシー **>** 承認に移動します。
2. 詳細ペインで、[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. 「エクスプレッション」で、「エクスプレッションエディタ」をクリックします。
6. 式の設定を開始するには、[選択] をクリックし、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. [**Create**] をクリックします。

GUI を使用して認可ポリシーをユーザにバインドするには

1. ［**NetScaler 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. [ポリシーのバインド] 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」でリクエストのタイプを選択し、「**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. ［**NetScaler 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. [ポリシーのバインド] 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」でリクエストのタイプを選択し、「**OK**」をクリックします。

デフォルトのグローバル認証の設定

April 1, 2024

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介して、関連付けられた認可ポリシーをまだ持っ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を上書きします。デフォルトの認可アクションが [拒否（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許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、セキュリティの向上に役立ちます。

デフォルトのグローバル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］タブのナビゲーションペインで、［NetScaler 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、[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 [デフォルトの承認アクション] 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

February 1, 2024

展開で認証が不要な場合は、認証を無効にできます。認証を必要としない仮想サーバーごとに、認証を無効にできます。

重要：認証は慎重に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、ローカルユーザーとグループを作成して、NetScaler Gateway でユーザーを認証できるようにします。認証を無効にすると、NetScaler 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 Web アドレスを入力して NetScaler Gateway に接続すると、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、［NetScaler Gateway］を展開し、［仮想サーバー］をクリックします。
2. 詳細ペイン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。

特定の時刻の認証の設定

April 1, 2024

認証ポリシーを設定して、ユーザが特定の時間（通常の勤務時間内など）に内部ネットワークにアクセスできるようにすることができます。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 NetScaler Gateway にログオンするタイミングを制限するには、認証ポリシー内に式を作成し、それを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設定するには

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［ポリシー］［認証］を展開します。
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。

   - TIME は、ユーザーがログオンできない時間を設定します。
   - DATE: ユーザーがログオンできない日付を設定します。
   - DAYOFWEEK は、ユーザーがログオンできない日を設定します。

   例: 時間:2020-10-12-02:30:00 GMT 日付:2020-10-12 DAYOFWEEK: Monday
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にある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

認証ポリシーの仕組み

February 1, 2024

ユーザーが NetScaler Gateway にログオンすると、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、NetScaler Gateway の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設定し、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して、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、NetScaler Gateway がユーザー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 値に設定した場合、ユーザーのログオン時に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、ポリシーをグローバルレベルまたは仮想サーバにバインドします。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と、グローバル認証タイプの優先順位が仮想サーバーにバインドされたポリシーよりも高い場合を除き、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された認証ポリシーは使用されません。

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

- 仮想サーバは、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、NetScaler Gateway はグローバル認証ポリシーを確認します。
- 認証ポリシーが仮想サーバまたはグローバルにバインドされていない場合、ユーザはデフォルトの認証タイプで認証されます。

LDAP および RADIUS 認証ポリシーを構成し、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、構成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構成することもできます。

認証プロファイルの設定

April 1, 2024

認証プロファイルは、NetScaler Gateway ウィザードまたは構成ユーティリティを使用して作成できます。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ています。プロファイルは、認証ポリシーの作成時に設定します。

NetScaler 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。NetScaler Gateway ウィザードについて詳しくは、「NetScaler 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、［NetScaler Gateway］>［ポリシー］［認証］を展開します。
2. ナビゲーションペインの [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、[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、認証タイプの設定を構成し、[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]、[作成]、[閉じる] の順にクリックします。
   注: 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、認証タイプを変更することはできません。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、設定済みの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、［NetScaler Gateway］>［ポリシー］［認証］を展開します。
2. ナビゲーションペインの [認証] で、認証の種類を選択します。
3. 詳細ウィンドウの [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、対応する認証ポリシーを NetScaler Gateway から削除します。

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［ポリシー］［認証］を展開します。
2. ナビゲーションペインの [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

February 1, 2024

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。いずれかの構成ユーティリティを使用して、認証ポリシーをバインドできます。

GUI 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

1. 構成ユーティリティの［構成］タブで、［**NetScaler Gateway**］**>**［ポリシー］［認証］を展開します。
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] の [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、NetScaler Gateway によって式が自動的に真値に設定されます。

GUI 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

1. 構成ユーティリティの［構成］タブで、［**NetScaler Gateway**］**>**［ポリシー］［認証］を展開します。
2. 「ポリシー」タブの「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」タブで、「ポリシー名」でポリシーを選択し、「ポリシーをバインド解除」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度の設定

April 1, 2024

デフォルトでは、認証ポリシーは、仮想サーバにバインドされたポリシーに対して最初に検証され、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 0 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プライオリティ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、［NetScaler Gateway］>［ポリシー］［認証］を展開します。
2.「ポリシー」タブの「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［プライマリ］タブまたは［セカンダリ］タブの［優先度］に番号を入力し、［OK］をクリックします。

仮想サーバー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、［NetScaler 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。

ローカルユーザの設定

April 1, 2024

NetScaler 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、NetScaler 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 [**NetScaler Gateway**] **>** [ユーザー管理] を展開して、[**AAA** ユーザー] をクリックします。
2. 詳細ペインで、[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**:LDAP** や **RADIUS** などの外部認証サーバに対してユーザを認証するには、**[**外部認証**]** を選択します。NetScaler Gateway がローカルユーザーデータベースに対して認証されるようにするには、このチェックボックスをオフにします。
5. [パスワード] と [パスワードの確認] に、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。

ユーザー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するか、外部認証サーバーに対して認証されるユーザーアカウントを構成できます。

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 [**NetScaler Gateway**] **>** [ユーザー管理] を展開して、[**AAA** ユーザー] をクリックします。
2. 詳細ウィンドウで、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

ローカル認証用に設定されているユーザがいる場合は、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 [**NetScaler Gateway**] **>** [ユーザー管理] を展開して、[**AAA** ユーザー] をクリックします。
2. 詳細ウィンドウで、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

NetScaler 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 [**NetScaler Gateway**] **>** [ユーザー管理] を展開して、[**AAA** ユーザー] をクリックします。
2. 詳細ウィンドウで、ユーザーを選択し、[削除] をクリックします。

NetScaler Gateway からユーザーを削除すると、関連付けられてい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。

グループの設定

February 1, 2024

NetScaler Gateway には、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持つことができます。認証に外部サーバーを使用している場合、NetScaler Gateway 上のグループは、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 NetScaler Gateway 上のグループの設定を継承します。

グループを設定したら、認可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、およびユーザがアクセスできるファイル共有およびサーバの 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、NetScaler Gateway で構成されているグループに追加します。その後、ユーザはそのグループの設定を継承します。

重要: ユーザーが AcActive Directory グループのメンバーである場合、NetScaler 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。

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［NetScaler 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、[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

NetScaler 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［NetScaler 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

April 1, 2024

グループの作成時または後で、グループにユーザーを追加できます。複数のグループにユーザーを追加すると、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 [**NetScaler Gateway**] **>** [ユーザー管理] を展開して、[AAA ユーザー] 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

February 1, 2024

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、NetScaler Gateway で構成されているグループに追加します。その後、ユーザ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・ボックスでは、ユーザー・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順位を設定する必要があります。

たとえば、group1 がホームページ www.homepage1.com で設定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。Group2 は、ホームページ www.homepage2.com で設定されたセッションポリシーにバインドされ

ています。これらのポリシーが、優先度番号のない、または同じ優先度番号を持つ各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に低い優先度の番号を設定すると、両方のグループに属するユーザーがホームページ www.homepage1.com を受信できるようになります。

セッションポリシーにプライオリティ番号が割り当てられていない場合、またはプライオリティ番号が同じ場合、precedence は次の順序で評価されます。

- ユーザー
- グループ
- 仮想サーバー
- 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、またはポリシーのプライオリティ番号が同じ場合、評価の順序はポリシーのバインド順序に従います。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。

ユーザーが複数のグループにバインドされ、各グループに IIP がバインドされている場合、そのユーザーはバインドされたグループから自由な IP を取得できます。

LDAP 認証の構成

February 1, 2024

1 つまたは複数の LDAP サーバーでユーザーアクセスを認証するように NetScaler Gateway を構成できます。

LDAP 認証には、Active Directory、LDAP サーバー、および NetScaler 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・レイヤー・セキュリティ (TLS) を使用して安全です。セキュア LDAP 接続には 2 つのタイプがあります。1 つのタイプでは、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。ユーザが SSL 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
- 636 セキュアな LDAP 接続の場合
- Microsoft のセキュアでない LDAP 接続の場合は 3268
- Microsoft のセキュア LDAP 接続の場合は 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。NetScaler 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と、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、NetScaler 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、このアプローチはパフォーマンスに影響す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 サーバのユーザ属性フィールドの例を示します。

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

次の表に、ベース DN の例を示します。

LDAP サーバ	ベース DN
Microsoft Active Directory サーバー	DC=citrix、DC= ローカル
Novell eDirectory	ou=users、ou=dev
IBM Directory Server	cn=users
Lotus Domino	OU=City、O=Citrix、C=US
Sun ONE ディレクトリ (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	バインド DN
Microsoft Active Directory サーバー	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

LDAP サーバ	バインド DN
Sun ONE ディレクトリ (旧 iPlanet)	uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot

注:LDAP サーバー設定の詳細については、
LDAP ディレクトリ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

February 1, 2024

1. **NetScaler Gateway** > ポリシー > 認証に移動します。
2. **LDAP** をクリックします。
3. 詳細ペインの [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. [タイプ] で、Active Directory の場合は **AD** 、**Novell** ディレクトリサービスの場合は **NDS** のいずれかを選択します。
9. [接続設定**]** で、以下を完了します。

   a) [ベース **DN (**ユーザーの場所**)**] に、ユーザーが配置されているベース 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。ベース DN の構文の例は次のとおりです。

   ```
   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 の構文の例は次のとおりです。

   ```
   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=groupname として指定されたグループ名が必要です。NetScaler 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。

その他の LDAP ディレクトリでは、グループ名は必要ないか、必要に応じて ou=groupname として指定します。

NetScaler 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。ユーザーを特定した後、NetScaler Gateway は管理者の資格情報をバインド解除し、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. その他の 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 と 13 に進みます。それ以外の場合は、ステップ 14 に進みます。

11. [その他の設定] の [サーバーログオン名の属性] に、構成する LDAP サーバーのユーザーログオン名を NetScaler Gateway が検索するときに使用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、1 つまたは複数の Active Directory 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:
    >
    > 前の例を使用して、特定の AD グループのメンバーにのみ NetScaler Gateway アクセスを制限できます。

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、属性を使用している LDAP サーバタイプの属性に変更します。この属性により、NetScaler 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. ユーザに LDAP パスワードの変更を許可するには、[パスワードの変更を許可] を選択します。

    注:

    - セキュリティの種類として **PLAINTEXT** を選択した場合、ユーザーがパスワードを変更できるようにすることはサポートされません。
    - セキュリティのために **PLAINTEXT** または **TLS** を選択する場合は、ポート番号 389 を使用します。**SSL** を選択する場合は、ポート番号 636 を使用します。

LDAP ディレクトリ内の属性を決定する

April 1, 2024

NetScaler Gateway で認証設定を構成できるように、LDAP ディレクトリ属性の決定についてサポートが必要な場合は、Softerra の無償の LDAP ブラウザーを使用して簡単に検索できます。

LDAP ブラウザは、Softerra LDAP アドミニストレータの Web サイトからダウンロードできます。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 ブラウザーによって提供される情報は、NetScaler Gateway でこの設定を構成する必要があるベース DN を決定するのに役立ちます。
- 匿名バインドチェックは、LDAP サーバーに接続するためにユーザー資格情報が必要かどうかを判断します。LDAP サーバがクレデンシャルを必要とする場合は、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

February 1, 2024

2 要素認証を使用している場合、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、NetScaler 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、NetScaler 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 NetScaler Gateway 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度を設定します。

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 グループ抽出がユーザオブジェクトから直接動作する仕組み
- LDAP グループ抽出がグループオブジェクトから間接的に動作する仕組み

LDAP グループ抽出がユーザオブジェクトから直接動作する仕組み

February 1, 2024

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、NetScaler Gateway 認証をサポートします。

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、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 サーバーはどちらも、NetScaler Gateway グループの抽出をサポートしています。

たとえば、IBM Directory Server では、静的グループ、動的グループ、および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を、IBM-AllGroups 属性を使用して返すことができます。Sun ONE では、管理対象、フィルタ処理、ネストを含むすべてのロールは 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動作する仕組み

February 1, 2024

グループオブジェクトから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、NetScaler Gateway 認証と互換性がありません。

Lotus Domino などの一部の LDAP サーバーでは、グループ・オブジェクトのみがユーザーに関する情報を格納できます。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含めることができないため、NetScaler Gateway グループ抽出と互換性がありません。この LDAP サーバータイプでは、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の検索が実行されます。

LDAP 認可グループ属性フィールド

February 1, 2024

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 サーバー	memberOf

LDAP サーバ	LDAP 属性
Novell eDirectory	groupMembership
IBM Directory Server	ibm-allGroups
Sun ONE ディレクトリ (旧 iPlanet)	nsRole

LDAP 認証を設定するには

April 1, 2024

認証ポリシーで LDAP 認可を設定するには、グループ属性名とサブ属性を設定します。

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［ポリシー］［認証］を展開します。
2. [認証] で、認証の種類をクリックします。
3. 詳細ペインで、［Add］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. [サブ属性名] 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・ボックスの「名前付き表現」の横にある式を選択し、「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。

LDAP ネストされたグループ抽出の設定

April 1, 2024

NetScaler Gateway は、LDAP グループにクエリを実行し、認証サーバーで構成した祖先グループからグループおよび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。ユーザーがグループ 3 に属している場合、NetScaler Gateway は、ネストされたすべての祖先グループ（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。クエリが実行されると、NetScaler 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、［**NetScaler Gateway**］**>**［ポリシー］**>**［認証**/**承認］**>**［認証］の順に展開し、［**LDAP**］をクリックします。
2. 詳細ペインの [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、NetScaler Gateway がチェックするレベルの数を入力します。
9. **[**グループ名識別子] に、LDAP サーバ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。例：`memberOf`。
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**]** に、クエリ文字列を入力します。たとえば、フィルタは`&(samaccountname=test)(objectClass=\*)`です。
13. [作成] をクリックし、[閉じる] 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の [名前付き式] の横で式を選択し、[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。

複数ドメインの **LDAP** グループ抽出の設定

February 1, 2024

認証に複数のドメインがあり、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 NetScaler Gateway を構成できます。

Active Directory では、ネットワーク内のドメインごとに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、グループおよび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、NetScaler Gateway 上の複数のドメインの LDAP グループ抽出を構成します。

複数のドメインのグループ抽出用に NetScaler Gateway を構成するには、ネットワーク内のドメインの数と同じ数のセッションポリシーと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 という名前の 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、NetScaler Gateway でグループを作成し、セッションポリシーをグループにバインドします。次に、認証ポリシーを仮想サーバーにバインドします。

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。

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

グループ抽出のためのセッションポリシーの作成

April 1, 2024

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 インターフェイス 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の [構成] タブのナビゲーションペインで、**[NetScaler 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「グローバル上書き」をクリックし、「オン」を選択します。
    b) [**Web** インターフェイスアドレス] の横にある [グローバル上書き] をクリックし、Web インターフェイスの 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 [グローバルを上書き] 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 (Child など) を入力します。
6. [シングルサインオンドメイン] の横で、最初の Windows 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、[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の [構成] タブのナビゲーションペインで、**[NetScaler 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 [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.「リクエスト・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 [一般] 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。

複数ドメインの **LDAP** 認証ポリシーの作成

April 1, 2024

NetScaler 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検索フィルタです。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、次に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用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、［NetScaler 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. 詳細ペインで、[サーバー] タブをクリックし、[追加] をクリックします。
4. [**Name**] に、最初のドメインの名前 (Sampaなど) を入力します。
5. LDAP サーバーの設定を構成し、[作成] 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、[閉じる（**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、［**NetScaler Gateway**］**>** ［ポリシー］［認証］を展開します。
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 [一般] 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。

複数ドメインの **LDAP** グループ抽出のためのグループおよびバインディングポリシーの作成

April 1, 2024

認証ポリシーを作成したら、NetScaler 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。

NetScaler Gateway でグループを作成するには

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、［**NetScaler 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、[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 NetScaler 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。グループ名で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が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、［**NetScaler Gateway** ］を展開し、［仮想サーバー］をクリックします。
2. 詳細ペインで仮想サーバーを選択して、［**Open**］をクリックします。
3. [認証] タブで [プライマリ] をクリックし、[ポリシー名] で [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。
4.「ポリシー名」で、「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。

LDAP 認証のための 14 日間のパスワード有効期限通知

February 1, 2024

NetScaler Gateway アプライアンスは、LDAP ベースの認証に対して 14 日間のパスワード有効期限切れ通知をサポートしています。この機能を使用すると、管理者はパスワードの有効期限のしきい値を日単位でエンドユーザに通知できます。詳細については、LDAP 認証の 14 日間のパスワード有効期限切れ通知を参照してください。

クライアント証明書認証の構成

February 1, 2024

NetScaler Gateway 仮想サーバーにログオンするユーザーは、仮想サーバーに提示される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、LDAP や RADIUS などの他の認証タイプと一緒に使用して、2 要素認証を提供することもできます。

クライアント側の証明書属性に基づいてユーザーを認証するには、仮想サーバーでクライアント認証を有効にし、クライアント証明書を要求する必要があります。さらに、NetScaler 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 NetScaler 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。認証は、次の場合に失敗します。

- セキュアソケットレイヤー (SSL) ハンドシェイク中にユーザーが有効な証明書を提供しない場合。
- ユーザー名の抽出が失敗し、認証が失敗します。

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。

GUI を使用して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するには

1. ［構成］ **>** ［**NetScaler Gateway**］ の順に選択し、［グローバル設定］ をクリックします。
2. 詳細ウィンドウの [認証設定**]** で、**[**認証 **CERT** 設定の変更] をクリックします。
3. 要件に従って証明書を使用して 2 要素認証を有効にするには、[オン] を選択します。
4. [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。
5. [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。
6. [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

NetScaler 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。認証が成功すると、証明書からユーザー名またはユーザーのユーザー名とグループ名が抽出されます。また、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

April 1, 2024

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、［**NetScaler Gateway**］**>** ［ポリシー］［認証］を展開します。
2. ナビゲーションペインの [認証] で、[**CERT**] をクリックします。
3. 詳細ペインで、[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** 要素］の横にある ［オフ］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：以前に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 [
   ユーザ名（User Name）] フィールドと [
   グループ名（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・ボックスの「名前付き表現」の横にある式を選択し、「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。

クライアント証明書ポリシーを仮想サーバー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認証ポリシーを構成したら、そのポリシー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、［**NetScaler Gateway** ］を展開し、［仮想サーバー］をクリックします。
2. 詳細ペインで仮想サーバーをクリックし、[開く] をクリックします。
3. **NetScaler 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] で、[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、［**NetScaler 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] 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」または「必須」を選択し、「OK」を 2 回クリックします。同じ仮想サーバーで他の認証タイプを許可し、クライアント証明書の使用を必要としない場合は、[オプション] を選択します。

> 注
>
> - コールバック URL について詳しくは、「NetScaler Gateway のインポート」を参照してください。
> - 証明書の詳細については、「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

February 1, 2024

最初にユーザを認証し、次に LDAP や RADIUS などのセカンダリ認証タイプでログオンするようにユーザに要求するようにクライアント証明書を設定できます。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。次に、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できます。Secure Sockets Layer (SSL) 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取ることができます。

- ユーザー名もグループも証明書から抽出されません。ログオンページがユーザーに表示され、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。NetScaler Gateway は、通常のパスワード認証の場合と同様に、ユーザーの資格情報を認証します。
- ユーザー名とグループ名は、クライアント証明書から抽出されます。ユーザー名のみが抽出された場合、ログオン名が存在するユーザーに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。

NetScaler Gateway が 2 回目の認証ラウンド中に抽出したグループ情報は、NetScaler 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

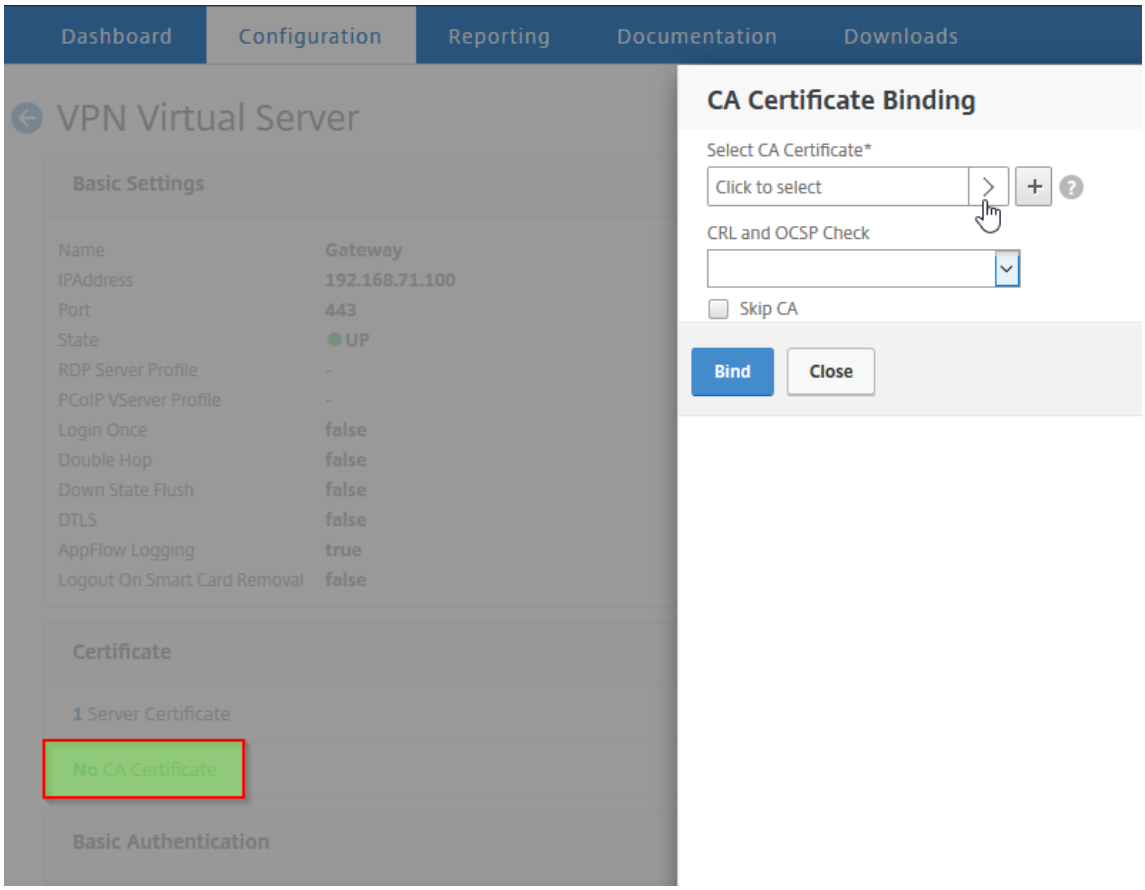
April 1, 2024

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 NetScaler Gateway を構成できます。

NetScaler Gateway で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。詳細については、「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 NetScaler Gateway に追加します。詳しくは、「To install a root certificate on NetScaler Gateway」を参照してください。

  重要：スマートカード認証のためにルート証明書を仮想サーバーに追加する場合は、[**CA** 証明書の選択] リストから証明書を選択する必要があります。



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**]** タブのドメインを`mydomain`の代わりに`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、値を 1 に設定するコマンド`wi-sso-split-upn`を実行した場合。この例では、userPrincipalName 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すると、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、NetScaler 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 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。

セキュアな **ICA** 接続を使用したスマートカード認証の構成

NetScaler 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、個人識別番号（PIN）の入力を求められることがあります。

- ログオン時、および公開リソースを起動しようとしたとき。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た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、プロセスまたはセキュアソケットレイヤー（SSL）接続を Web ブラウザーと共有しません。したがって、ICA 接続が NetScaler Gateway との SSL ハンドシェイクを完了すると、クライアント証明書がもう一度必要になります。

ユーザーに 2 つ目の 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 仮想サーバーでのクライアント認証は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。

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

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、［NetScaler 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. 構成ユーティリティを使用して、[構成] 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:

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、NetScaler Gateway にログオンします。

RADIUS 認証の構成

February 1, 2024

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 NetScaler 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 NetScaler 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 の使用を有効にすると、アプライアンスは、RADIUS 接続の確立に使用されるソース 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 RADIUS サーバと通信するために NAS IP を使用して設定された NAS ID を無視します。

ジェムアルトプロティバの設定

Protiva は、Gemalto のスマートカード認証の長所を利用するために開発した、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るユーザー名、パスワード、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。Gemalto Protiva を NetScaler Gateway と互換性があるように構成するには、次のガイドラインを使用します。

- Protiva サーバーをインストールします。
- 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 Microsoft IAS RADIUS サーバーに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。
- NetScaler 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。

セーフワードを構成する

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 は直ちにパスコードを無効にし、再度使用することはできません。SafeWord サーバーを構成するときは、次の情報が必要です。

- NetScaler Gateway の IP アドレス。IP アドレスは、RADIUS サーバクライアントの設定で設定した IP アドレスと同じ IP アドレスである必要があります。NetScaler 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。2 つのアプライアンスを高可用性に設定する場合は、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

April 1, 2024

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［ポリシー］［認証］を展開します。
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 [秘密キー] と [秘密キーの確認] に、RADIUS サーバーシークレットを入力します。
10. [NAS ID] に ID 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・ボックスの「名前付き表現」の横にある式を選択し、「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。

RADIUS 認証プロトコルの選択

February 1, 2024

NetScaler Gateway は、ユーザー認証に次のようないくつかのプロトコルを使用するように構成された RADIUS の実装をサポートしています。

- パスワード認証プロトコル (PAP)
- チャレンジハンドシェイク認証プロトコル (CHAP)
- Microsoft のチャレンジハンドシェイク認証プロトコル (MS-CHAP バージョン 1 およびバージョン 2)

NetScaler Gateway の展開環境が RADIUS 認証を使用するように構成されており、RADIUS サーバーが PAP を使用するように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、および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 文字の長さです。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 共有シークレットを判別します。

RADIUS トラフィックをさらに保護するには、各 NetScaler Gateway アプライアンスまたは仮想サーバー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秘密を割り当てることもできます。その場合は、RADIUS 認証を使用する各 NetScaler 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 NetScaler 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

April 1, 2024

RADIUS サーバーから IP アドレスを抽出するように NetScaler 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ているフレーム付き IP アドレスを返します。フレーム付き IP アドレスは、アクセス要求では RADIUS 属性 8 フレームド IP アドレスとも呼ばれます。

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、NetScaler Gateway にログオンしたユーザーの内部ネットワークから IP アドレスを提供できるようにします。
- **ipaddress** タイプを使用する任意の RADIUS 属性（ベンダーエンコードされた属性を含む）の設定を許可します。

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 と属性タイプを設定します。ベンダー ID と属性は、RADIUS クライアントと RADIUS サーバ間の関連付けを作成するために使用されます。

- ベンダー識別子（ID）により、RADIUS サーバは、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 応答の属性です。ゼロの値は、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。
- 属性タイプは、RADIUS 応答のリモート IP アドレス属性です。最小値は 1 で、最大値は 255 です。

一般的な設定は、RADIUS 属性フレームの **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 に設定されます。

GUI を使用して **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. [**NetScaler Gateway] > [**ポリシー**] > [**認証] に移動し、[**RADIUS**]
2. 詳細ペインの [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の [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.「グループ属性タイプ」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

February 1, 2024

RADIUS 許可は、グループ抽出と呼ばれる方式を使用して設定できます。グループ抽出を構成すると、NetScaler Gateway にユーザーを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 許可を設定するには、認証ポリシーを使用し、グループベンダー ID（ID）、グループ属性タイプ、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にバインドするか、仮想サーバにバインドします。

Windows Server 2003 での **RADIUS** の設定

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、NetScaler Gateway の構成中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。
- Type 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。デフォルトの名前は ctxUserGroups=

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 のスナップインをインストールします。ウィザードの指示に従って、次の設定を選択してください。

- [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 チャレンジハンドシェイク認証プロトコルバージョン 2（MS-CHAP v2）
  - Microsoft チャレンジハンドシェイク認証プロトコル（MS-CHAP）
  - チャレンジハンドシェイク認証プロトコル (CHAP)
  - 暗号化されていない認証 (PAP、SPAP)
- [ベンダー固有属性] を選択します。

  ベンダー固有属性は、サーバー上のグループで定義したユーザーと NetScaler 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 NetScaler Gateway に送信します。必ず [RADIUS = 標準] を選択してください。
- RADIUS のデフォルトは 0 です。この番号をベンダーコードに使用します。
- ベンダー割り当ての属性番号は 0 です。

  これは、[User Group] 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。

  アクセスゲートウェイの場合、属性値は ctxUserGroups=GroupName です。売上と財務などの 2 つのグループが定義されている場合、属性値は ctxUserGroups=Sales; finance になります。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ら、NetScaler 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 Server 2008 での認証用の RADIUS の設定

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 の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、ネットワークの RADIUS 設定を構成するには、[スタート] メニューの [管理サービス] から NPS を起動します。NPS を開くと、NetScaler 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。

- ベンダー名には、[RADIUS 標準] を選択します。
- NetScaler 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ておきます。

RADIUS グループの場合、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構成します。

- 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、NetScaler 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設定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ときに、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、条件を設定します。

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 [暗号化された認証 (CHAP)] と [暗号化されていない認証 (PAP と SPAP)] を選択します。
- [ベンダー固有属性] に [RADIUS 標準] を選択します。

  デフォルトの属性番号は 26 です。この属性は、RADIUS 認可に使用されます。

  NetScaler Gateway には、サーバー上のグループで定義されたユーザーと NetScaler 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 NetScaler 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。

  NetScaler Gateway の場合、属性値は ctxUserGroups= グループ名です。売上と財務などの 2 つのグループが定義されている場合、属性値は ctxUserGroups=Sales; finance になります。各グループはセミコロンで区切ります。
- 区切り文字は、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に NPS で使用した区切り文字です。

IAS でのリモートアクセスポリシーの構成が完了したら、NetScaler 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

April 1, 2024

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［ポリシー］［認証］を展開します。
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・ボックスの「名前付き表現」の横にある式を選択し、「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。

RADIUS ユーザアカウンティングの設定

April 1, 2024

NetScaler 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で送信されるメッセージには、RFC2866 で定義されている属性のサブセットが含まれます。表 1 に、サポートされている属性と、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 NetScaler Gateway イベントを示します。

表 1. サポートされている RADIUS 属性

属性	意味	RAD_START	RAD_STOP
User-Name	セッションに関連付けられているユーザーの名前。	X	X
セッション ID	NetScaler セッション ID。	X	X
Acct-Session-Time	セッション継続時間 (秒)。		X
Acct-Terminate-Cause	アカウント終了の理由。		X

表 2. RADIUS 終了の原因

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
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
その他	RAD_TERM_NAS_ERROR

RADIUS ユーザアカウンティングの設定には、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の送信先となる 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、次の手順を実行する必要があります。

1. RADIUS ポリシーを作成して、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することができます。
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、NetScaler Gateway 仮想サーバーにバインドして、その仮想サーバーを通過す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のナビゲーションペインで、［NetScaler 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. 詳細ペインの [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、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. ［Create］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のナビゲーションペインで、［NetScaler 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（Accounting Policy）] メニューで、前に作成した RADIUS ポリシーを選択します。
9. ［Create］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. ［Create］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のナビゲーションペインで、［NetScaler 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、[グローバルバインド] を選択します。
4. ［Bind］をクリックします。
5. [ポリシー] ペインで、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（Policies）] リストで、セッションポリシーの [Priority] 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 **NetScaler 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のナビゲーションペインで、［NetScaler Gateway］ノードを展開し、［仮想サーバー］を選択します。

2. メインの詳細ペインで、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. [Bind] をクリックします。
7. [ポリシー] ペインで、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

April 1, 2024

セキュリティアサーションマークアップ言語 (SAML) は、ID プロバイダ (IdP) とサービスプロバイダ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。NetScaler 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。これは、IdP の秘密キーに対応するパブリックキーです。
- 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。
- ユーザーフィールド。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。この設定はオプションです。
- 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 NetScaler Gateway サーバーの秘密キーです。証明書名を設定しない場合、アサーションは署名されずに送信されるか、認証要求が拒否されます。
- 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。issuer フィールドには、アサーションの送信元の機関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、ユーザが認証される認証サーバー上のグループです。
- 2 要素。この設定では、2 要素認証を有効または無効にします。
- 署名なし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、NetScaler Gateway はユーザー認証を拒否します。

NetScaler Gateway は HTTP ポスト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、必要な情報を含むフォーム自動投稿を含む 200 OK でユーザーに返信します。具体的には、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`SAMLResponse`、`SAMLRequest`という名前の 2 つの非表示フィールドを含める必要があります。このフォームには RelayState も含まれます。RelayState は、送信側によって処理されない任意の情報を送信するために使用される状態または情報です。依存側が情報を送り返すので、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ことができます。RelayState を暗号化または難読化することをお勧めします。

> 注
>
> - NetScaler Gateway を Citrix Cloud への IdP として使用する場合、NetScaler Gateway で **RelayState** ルールを構成する必要はありません。
> - IdP チェーンの場合は、最初の SAML ポリシーでのみ **RelayState** ルールを設定すれば十分です。このコンテキストでは、IdP チェーンとは、設定された SAML アクションが、別の SAML アクションを含む認証仮想サーバー IdP を参照するシナリオです。

Active Directory フェデレーションサービス **2.0** の構成

Active Directory フェデレーションサービス (AD FS) 2.0 は、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 または Windows Server 2012 コンピューターで構成できます。ADFS サーバーを NetScaler Gateway と互換性があるように構成する場合は、Windows Server 2008 または Windows Server 2012 の証明書利用者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 のパラメーター:

- 依存パーティ信頼。NetScaler Gateway 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。vserver.fqdn.com は、NetScaler 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記載されています。
- 承認規則。証明書利用者へのユーザーのアクセスを許可または拒否できます。

Windows Server 2012 年の変数:

- 依存パーティ信頼。NetScaler Gateway 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。vserver.fqdn.com は、NetScaler 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記載されています。
- 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。NetScaler 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。NetScaler 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、NetScaler Gateway アプライアンスのアサーションコンシューマサービス URL です。これは定数パラメーターであり、NetScaler Gateway はこの URL で SAML レスポンスを期待します。
- 証明書利用者信頼識別子。NetScaler Gateway という名前を入力します。これは、`https://netscalerGateway.virtualServerName.com/adfs/services/trust`などの証明書利用者を識別する URL です。

- 承認規則。証明書利用者へのユーザーのアクセスを許可または拒否できます。
- 要求ルールを構成します。LDAP 属性の値は、発行トランスフォームルールを使用して構成できます。また、[LDAP 属性を要求として送信] テンプレートを使用できます。次に、以下を含む 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、リレーパーティのプロパティを選択し、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、リレーパーティの証明書失効リスト（CRL）を無効にします。このチェックを無効にしない場合、AD FS は CRL で証明書を検証しようとします。

  CRL を無効にするには、次のコマンドを実行します。set-adfwRelayingPartyTrust-signingCertfiCateRvocatonNone-TargetName NetScaler

設定を構成したら、リレーパーティの信頼ウィザードを完了する前に、証明書利用者データを確認します。NetScaler Gateway 仮想サーバー証明書をエンドポイント URL（`https://vserver.fqdn.com/cgi/samlauth`など）で確認します。

リレー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、構成済みの信頼を選択し、プロパティを編集します。以下の手順に従います:

- セキュアハッシュアルゴリズムを SHA-1 に設定します。

  注：NetScaler は SHA-1 のみをサポートしています。
- 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。
- 次の項目を含む要求ルールを編集します。
  - トランスフォームルールの選択
  - クレームルールの追加
  - 要求規則テンプレートの選択:LDAP 属性を要求として送信する
  - 名前を挙げて
  - 属性ストアの選択:Active Directory
  - LDAP 属性を選択:<Active Directory parameters>
  - 「名前 ID」として「アウトゴーイングクレームルール」を選択します

  注: 属性名の 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、次のとおりである必要があります。


```
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、NetScaler 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、NetScaler Gateway で SAML 認証を構成できます。

SAML 二要素認証の設定

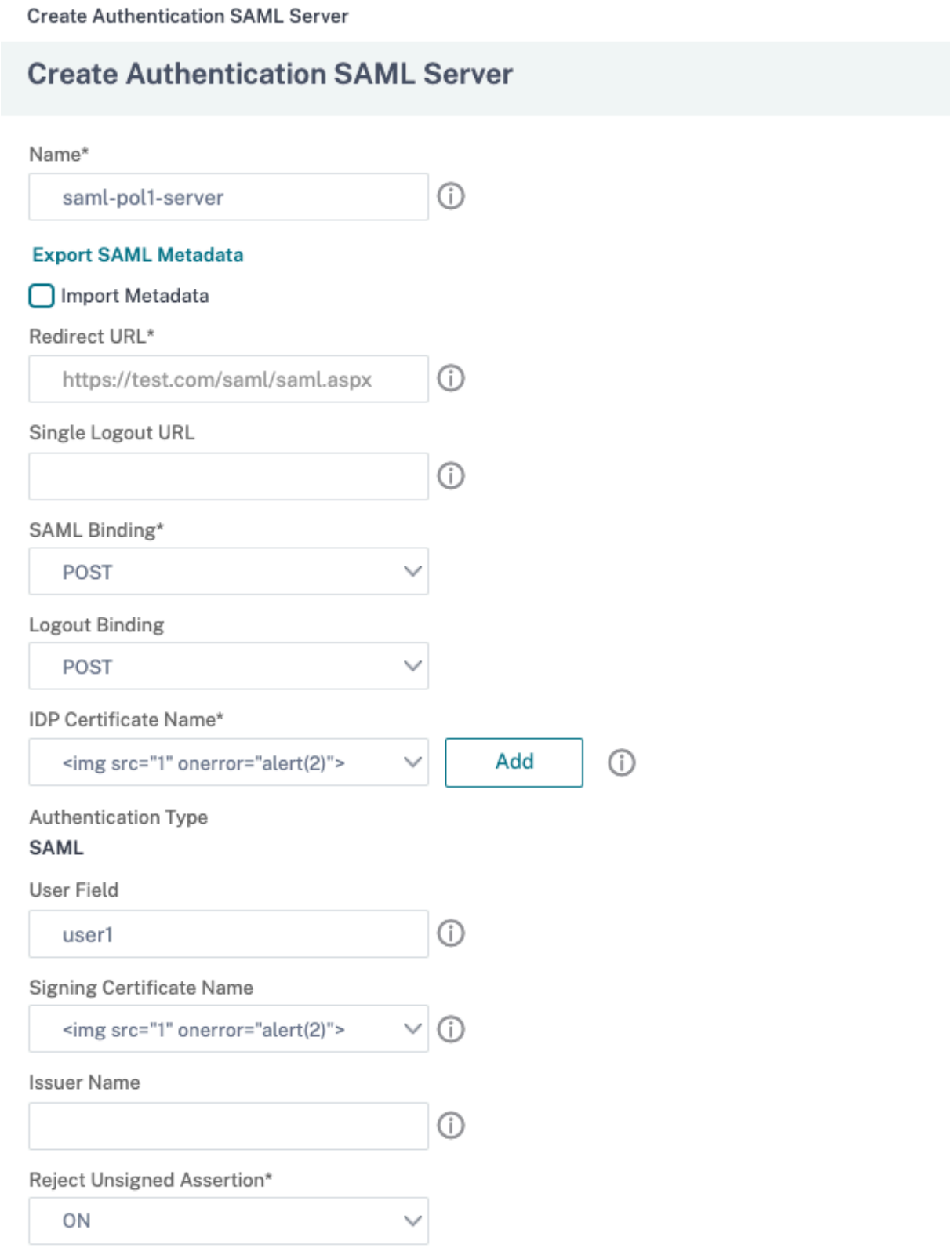
SAML の 2 要素認証を設定できます。LDAP 認証を使用した SAML 認証を設定する場合は、次のガイドラインに従ってください。

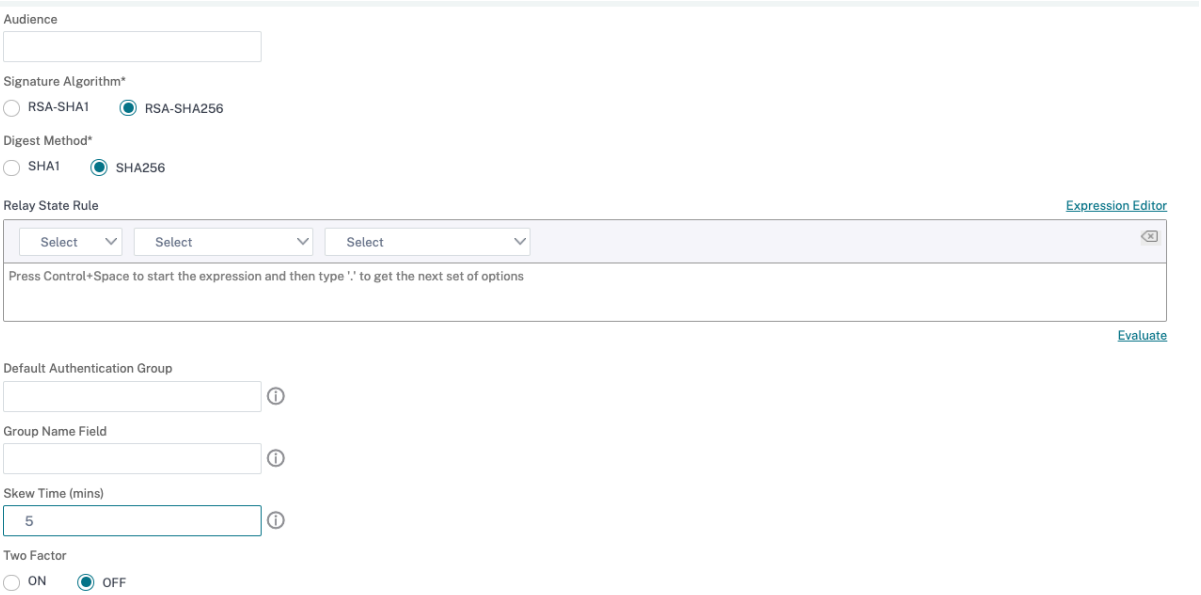
- SAML がプライマリ認証タイプの場合、LDAP ポリシーで認証を無効にし、グループ抽出を設定します。次に、LDAP ポリシーをセカンダリ認証タイプとしてバインドします。
- SAML 認証はパスワードを使用せず、ユーザー名のみを使用します。また、SAML 認証は、認証が成功した場合にのみユーザーに通知します。SAML 認証が失敗した場合、ユーザーには通知されません。失敗応答は送信されないため、SAML はカスケードの最後のポリシーであるか、唯一のポリシーである必要があります。
- 不透明な文字列ではなく、実際のユーザー名を構成することをお勧めします。
- SAML をセカンダリ認証タイプ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

April 1, 2024

1. 構成ユーティリティの［構成］タブで、［**NetScaler Gateway**］**>** ［ポリシー］［認証］を展開します。
2. ナビゲーションペインで、[**SAML**] をクリックします。
3. 詳細ペインで、[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。





1. 「サーバー」の横にある「新規」をクリックします。
2. [名前] に、サーバープロファイルの名前を入力します。
3. [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 または IdP サーバーにインストールされる証明書です。

   [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、「Installing and Managing Certificates」を参照してください。
4. [リダイレクト **URL**] に、認証 ID プロバイダ (IdP) の URL を入力します。

   これは、SAML サーバーへのユーザーログオンの URL です。これは、NetScaler Gateway が最初の要求をリダイレクトするサーバーです。
5. [シングルログアウト **URL**] で、サインアウトプロセスを完了するためにクライアントを IdP に返送するタイミングをアプライアンスが認識できるように、URL を指定します。
6. [**SAML** バインディング] で、クライアントを SP から IdP に移動するために使用する方法を選択します。これは、IdP でクライアントがどのように接続するかを理解できるように、IdP で同じである必要があります。アプライアンスが SP として動作する場合、POST、REDIRECT、および ARTIFACT バインディングをサポートします。
7. 「ログアウトバインド」で「リダイレクト」を選択します。
8. [**IDP** 証明書名] で、SAML 署名証明書の下にある IdPCert 証明書 (Base64) を選択します。

   > 注:
   >
   > [メタデータのインポート] をクリックして、メタデータ構成が格納されている URL を選択することもできます。
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、アプライアンスが IdP への認証要求に署名するために使用する SAML SP 証明書（秘密キーを含む）を選択します。IdP が認証要求署名を検証できるように、同じ証明書（秘密キーなし）を IdP にインポートする必要があります。このフィールドは、ほとんどの IdP では必要ありません。

    これは、NetScaler Gateway 仮想 IP アドレスにバインドされている証明書です。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. 発行者名に、アプライアンスが初期認証（GET）要求を送信する負荷分散または NetScaler Gateway 仮想 IP アドレスの FQDN を入力します。
12. [署名されていないアサーションを拒否する] で、IdP からのアサーションに署名を要求するかどうかを指定します。アサーションのみを署名する (ON) か、アサーションと IdP からの応答の両方に署名する (STRICT) 必要があります。
13. [オーディエンス] に、IdP によって送信されたアサーションを適用できるオーディエンスを入力します。これは通常、サービスプロバイダーを表すエンティティ名または URL です。
14. 「署名アルゴリズム」で、「RSA-SHA256」を選択します。
15. ダイジェスト方式で、SHA256 を選択します。
16. [デフォルト認証グループ（Default Authentication Group）] に、抽出されたグループに加えて、認証が成功した場合に選択されるデフォルトグループを入力します。
17. [グループ名（Group Name）] に、ユーザグループを含むアサーション内のタグの名前を入力します。
18. [**Skew Time (mins)**] に、サービスプロバイダーが着信アサーションで許可する許容クロックスキューを分単位で指定します。
19. [作成**]** をクリックし、 [閉じる] をクリックします。
20. [認証ポリシーの作成] ダイアログボックスの [名前付き式] の横にある [一般] を選択し、[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、[閉じる] をクリックします。

参照ドキュメント

- SAML サービスプロバイダーとしての NetScaler
- SAML IdP としての NetScaler
- SAML でサポートされる追加機能

SAML 認証を使用して NetScaler Gateway にログインする

February 1, 2024

SAML 認証を使用して、VPN クライアントとワークスペースアプリを使用して NetScaler Gateway にログインできます。プラグインは、認証仮想サーバーにバインドされた高度な SAML ポリシー、つまり nFactor 認証による SAML 認証のみをサポートします。

重要：SAML ポリシーが VPN 仮想サーバーに直接バインドされている場合、プラグインは SAML 認証、つまり非 nFactor 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

次の表に、NetScaler Gateway にログインするための 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を示します。

Product	バージョン
NetScaler 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 ビルド 49.37 以降。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
ワークスペース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** 認証の設定

高度な SAML ポリシーを使用した SAML 認証の構成について詳しくは、SAML IdP としての NetScaler ADC を参照してください。

SAML 認証の改善

April 1, 2024

この機能を使用するには、この情報を使用するには、SAML の知識、基本的な認証の習熟度、および FIPS の理解が必要です。

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およびサーバーでは、次の NetScaler ADC 機能を使用できます。

- SAML サービスプロバイダー (SP)
- SAML アイデンティティプロバイダ (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) を許可します。SAML SP 機能は、IdP からのユーザクレーム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 NetScaler ADC アプライ

アンスにすることができます。SAML IdP 機能は、ユーザーログオンをアサートし、SP によって消費されるクレームを提供するために使用されます。

SAML サポートの一環として、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、およびこれらの 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実行します。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 NetScaler ADC では、SSL 証明書の秘密キーはパケットエンジンまたはユーザー空間で利用できないため、今日の 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。署名の検証は、公開鍵が利用可能であるため、ソフトウェアで行われます。

解決策

SAML 機能セットは、シグニチャオフロードに SSL API を使用するように拡張されました。影響を受けるこれらの SAML サブ機能の詳細については、NetScaler 製品のドキュメント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/レスポンス/両方の署名
3. SAML SP シングルログアウトシナリオ—SP 開始モデルでのログアウトリクエストの署名と IdP 開始モデルでのログアウトレスポンスの署名
4. SAML SP アーティファクトバインディング—ArtifactResolve リクエストの署名
5. SAML SP リダイレクトバインディング—認証リクエストの署名
6. SAML IdP リダイレクトバインディング—レスポンス/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 プラットフォームで自動的に実行されます。

ただし、SSL 秘密キーは FIPS ハードウェアのユーザー空間では使用できないため、FIPS ハードウェアでの SSL 証明書の作成には若干の構成変更があります。

設定情報は次のとおりです。

- `add ssl fipsKey fips-key`

  CSR を作成し、CA サーバで使用して証明書を生成します。その後、その証明書を/nsconfig/sslにコピーできます。ファイルが fips3cert.cer だと仮定しましょう。

- `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します。

- `set samlAction <name> -samlSigningCertName fips-cert`

  同様に、SAML IdP モジュールのsamlIdpProfileでこれを使用します。

- `set samlidpprofile fipstest -samlIdpCertName fips-cert`

最初は、FIPS キーは使用できません。FIPS キーがない場合は、「FIPS キーを作成する」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>
<!--NeedCopy-->
```

TACACS+ 認証の設定

February 1, 2024

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 NetScaler Gateway を構成するには、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、使用中のサーバーポート番号がデフォルトのポート番号である 49 以外の場合のみです。

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、［**NetScaler Gateway**］**>** ［ポリシー］［認証］を展開します。
2. [**TACACS**] をクリックします。
3. 詳細ペインで、[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 サーバに変更を加えます。
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. [**Port**] で、デフォルトのポート番号 49 を使用します。

9. [**TACACS Key**] 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、同じキーを入力して確認します。
10. [詳細] クリックします。
11. [認証] で、[オン] 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]、[閉じる] の順にクリックします。

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-->
```

NetScaler 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、グローバルまたは仮想サーバレベルのいずれかでバインドできます。認証ポリシーのバインドの詳細については、「認証ポリシーのバインド」を参照してください。

設定のクリアベーシック **TACACS** の設定をクリアしてはならない

February 1, 2024

このトピックでは、clear config コマンドの実行時に、RBA（ロールベースアクセス）関連の設定をすべてクリア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：

- 基本
- 拡張
- フル

レベルに基づいて、NetScaler ADC 構成はクリアされ、工場出荷時のデフォルトにリセットされます。

使用されるコマンドは、

```
clear ns config [-force] <level>
```



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

新しいコマンドは、すべての RBA 関連設定の削除を許可または拒否するノブを追加します。

新しいコマンド

RBA 設定のクリア機能について説明します。

1. はい/いいえノブ。デフォルト: はい。

   管理者は、RBA 構成を保持するかどうかを決定します。

2. クリアコンフィグ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。

   - システムユーザー/グループを追加/バインドします。
   - cmd ポリシーを追加します。
   - TACACS コマンド（TACACS アクション/ポリシーの追加）
   - システムグローバルをバインドする

   注**:** TACACS 関連の設定（アクション/ポリシー）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、またはクリアされた場合に保持されます。

CLI 構成

使用されるコマンドは、

```
clear config [ - force] <level> [-RBAconfig]
<!--NeedCopy-->
```

デフォルトでは YES に設定され、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:

- /bind システムユーザー /グループの追加
- システムグローバルをバインドする
- TACACS 関連コマンド（TACACS アクション/ポリシーの追加）
- cmd ポリシーの追加

多要素認証の設定

February 1, 2024

NetScaler Gateway では、次の 2 種類の多要素認証を構成できます。

- 認証優先度レベルを設定するカスケード認証
- 2 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

複数の認証サーバーがある場合は、認証ポリシーの優先順位を設定できます。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の小さいポリシーは、番号が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 トークンのコードを使用して認証します。

カスケード認証の設定

April 1, 2024

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。カスケードを設定すると、システムはカスケードされたポリシーの定義に従って各認証サーバを走査して、ユーザのクレデンシャルを検証します。優先順位付けされた認証ポリシーは昇順でカスケードされ、1 ～9999 の範囲のプライオリティ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、ユーザーがログオンすると、最初に仮想サーバーがチェックされ、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の両方の認証ポリシーに属している場合は、最初に仮想サーバのポリシーが適用され、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に受信させる場合は、ポリシーのプライオリティを変更します。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、仮想サーバーにバインドされた 3 つの認証ポリシーがあり、各ポリシーの優先順位を設定できます。

ユーザがプライマリカスケードのポリシーに対する認証に失敗した場合、またはそのユーザがプライマリカスケードのポリシーに対する認証に成功しても、セカンダリカスケード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プライオリティを設定するには

1. 構成ユーティリティの［構成］タブで、［**NetScaler Gateway**］**>** ［ポリシー］［認証］を展開します。

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］に番号を入力し、［**OK**］をクリックします。

仮想サーバー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、［**NetScaler Gateway**］を展開し、［仮想サーバー］をクリックします。
2. 詳細ペインで仮想サーバーを選択して、［**Open**］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. 認証ポリシーの横にある [優先順位] に番号を入力し、[**OK**] をクリックします。

2 要素認証の設定

April 1, 2024

NetScaler Gateway は 2 要素認証をサポートしています。通常、ユーザーを認証するとき、NetScaler Gateway は、構成された認証方法のいずれかを使用してユーザーを正常に認証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、あるサーバーでユーザーを認証し、別のサーバーからグループを抽出する必要がある場合があります。たとえば、ネットワークで RADIUS サーバに対してユーザーを認証するが、RSA SecurID トークン認証も使用しており、ユーザー・グループがそのサーバに格納されている場合、グループを抽出するために、そのサーバに対するユーザーの認証が必要になることがあります。

ユーザが 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である場合、2 番目の認証方法として証明書認証ポリシーを構成できます。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。ユーザーがユーザー名とパスワードでログオンすると、ネットワークリソースにアクセスできます。

2 要素認証を構成する場合、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、［NetScaler Gateway］> ［ポリシー］［認証］を展開します。
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、ステップ 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

April 1, 2024

NetScaler 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の［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］**>**［ポリシー］**>**［セッション］の順に展開します。
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変更するには、[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」タブの「認証情報インデックス」の横にある「グローバル上書き」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変更する場合は、「**OK**」をクリックします。

クライアント証明書と **LDAP** の **2** 要素認証の設定

April 1, 2024

LDAP でのスマートカード認証の使用など、LDAP 認証および承認で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すると、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。ポリシーのプライオリティを設定する場合、クライアント証明書認証ポリシーには、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認証局 (CA) が、Active Directory を実行しているのと同じ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 認証および承認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をユーザーデバイスにインストールし、対応するルート証明書を NetScaler Gateway に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。

- 仮想サーバーを作成します。
- LDAP サーバの 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 を使用した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、［**NetScaler 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の [認証] で、[証明書] をクリックします。
3. 詳細ペインで、［Add］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 因子] 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]、[作成]、[閉じる] の順にクリックします。

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。

NetScaler 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、CA から Base64 形式でルート証明書を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 NetScaler 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。

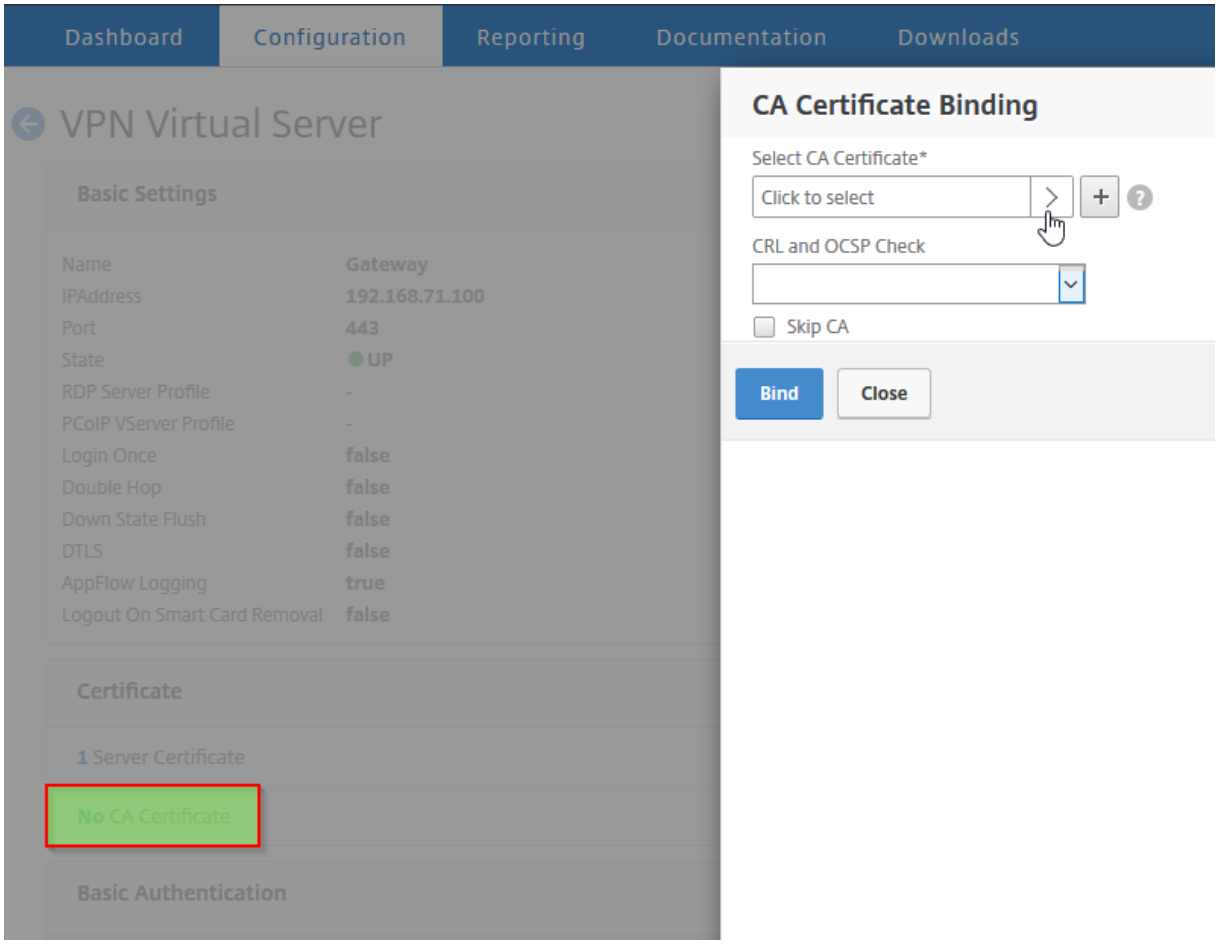
2. 詳細ペインで、[Install] をクリックします。
3. [証明書-キーペア名] に、証明書の名前を入力します。
4. 「証明書ファイル名」で「参照」をクリックし、リストから「アプライアンス」または「ローカル」を選択します。
5. ルート証明書に移動し、[開く]、[インストール] の順にクリックします。

ルート証明書を仮想サーバーに追加するには

NetScaler 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のため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**]** リスト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、［NetScaler Gateway ］を展開し、［仮想サーバー］をクリックします。
2. 詳細ペイン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］の横の一覧で［CA］をクリックし、［OK］をクリックします。
4. ステップ 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 Secure Access クライアントを使用して NetScaler 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名が表示されない場合は、LDAP ディレクトリ内のユーザアカウントとグループを確認します。NetScaler Gateway で定義されているグループは、LDAP ディレクトリ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が正しく読み取られないことがあります。

ユーザーおよびグループがドメインルートレベルにない場合、NetScaler 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」という名前のフォルダーがあり、証明書には CN=Users と記載されています。ログオンページの [ユーザー名] に [ユーザー] という単語が表示されます。

グループおよび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、NetScaler 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

February 1, 2024

Windows、Web アプリケーション（SharePoint など）、ファイル共有、および Web Interface へのシングルサインオンをサポートするように NetScaler Gateway を構成できます。シングルサインオンは、ユーザーが Access Interface のファイル転送ユーティリティまたは通知領域の NetScaler 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、ユーザーは資格情報をもう一度入力しなくても、自動的に再ログオンされます。

Windows でのシングルサインオンの構成

April 1, 2024

ユーザーは、デスクトップから Citrix Secure Access クライアントを起動して接続を開きます。シングルサインオンを有効にすることで、ユーザーが Windows にログオンしたときに Citrix Secure Access クライアントが自動的に起動するように指定できます。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認証のために NetScaler Gateway に渡されます。Citrix Secure Access クライアント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、ユーザーデバイスでの操作が容易になります。

シングルサインオンは、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有効にします。シングルサインオンが有効で、ドメインに存在しないデバイスからユーザーが接続した場合、ユーザーはログオンするように求められます。

Windows でのシングルサインオンは、グローバルに、または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、［**NetScaler 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、[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の［構成］タブのナビゲーションペインで、［NetScaler 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. 「リクエストプロファイル」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［グローバルを上書き］、［**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 [一般] を選択し、[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、[閉じる] 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の構成

April 1, 2024

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 NetScaler Gateway を構成できます。シングルサインオンを使用すると、ユーザーを SharePoint サイトなどのカスタムホームページや Web Interface にリダイレクトできます。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 ブラウザに入力した Web アドレスから、Citrix Secure Access クライアントを介して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。ユーザーが NetScaler Gateway または外部認証サーバーによって認証されると、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、ユーザはユーザ名とパスワードの入力を求める認証プロンプトを受け取ります。

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、［NetScaler 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、[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の [構成] タブのナビゲーションペインで、[NetScaler 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 [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・ボックスの「リクエスト・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

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、NetScaler 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、［NetScaler 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、[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、[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、ユーザーデバイス接続にクライアントレスアクセスを使用するか、Citrix Secure Access クライアントを使用するかに関係なく、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

April 1, 2024

シングルサインオンを構成し、ユーザーが username@domain.com 形式のユーザープリンシパル名 (UPN) を使用してログオンすると、既定ではシングルサインオンが失敗し、ユーザーは 2 回認証する必要があります。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、この形式のユーザー名を受け入れるように LDAP 認証ポリシーを変更します。

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、［**NetScaler Gateway**］**>** ［ポリシー］［認証］を展開します。
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の [サーバー] の横にある [変更] をクリックします。
4. [接続設定**]** 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。ここで、domainname.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** 名属性] に、ユーザーがログオンするときの形式を入力し、[**OK**] を 2 回クリックします。この値は`SamAccountName`または`UserPrincipalName`です。

ドメインへのシングルサインオンの設定

April 1, 2024

ユーザーが Citrix Virtual Apps を実行しているサーバーに接続して SmartAccess を使用する場合は、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への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の [構成] タブのナビゲーションペインで、[NetScaler 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 [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・ボックスの「リクエスト・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設定」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、「Override Global」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 を使用した NetScaler Gateway の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 のシングルサインオンの構成

February 1, 2024

次のセクションでは、NetScaler 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 Access (OWA) 2010 用の SSO は、次の条件では機能しません。

- Microsoft Exchange 2010 でのフォームベースの認証を使用する。
- 認証、承認、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負荷分散。

> 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仮想サーバの負荷分散でのみ機能します。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、NetScaler 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適宜変更します。
- logon.aspx リクエストで PBack Cookie 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 Cookie を設定し、[送信（Submit）] 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、NetScaler Gateway によってフォーム要求が生成されます。クッキーはフォーム送信リクエストに添付されません。
- OWA サーバーは、フォーム送信要求で PBack Cookie を期待します。書き換えポリシーは、フォーム送信リクエストに PBack Cookie 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、および監査の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します。

   - `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`

代替リライト構成

まれに、Microsoft Outlook が OWA セッションクッキーを発行せず、Pback クッキーも挿入されないことがあります。この問題は、前述のコマンドを実行して書き換え設定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

February 1, 2024

トークン個人識別番号（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 NetScaler 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度入力できません。

ワンタイムパスワードの使用を含む製品には、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 を使用するように構成します。詳細については、RADIUS 認証の設定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ように、RADIUS でワンタイムパスワードを使用するように NetScaler Gateway で認証を構成すると、NetScaler 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、NetScaler Gateway に変更を加えたとき、または Citrix Secure Access クライアントと NetScaler Gateway 間の接続が中断されてから復元された場合に行われます。

再認証の試行は、接続が Citrix Workspace アプリを使用するように構成されており、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発生する可能性があります。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、NetScaler 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 SecurID 認証の設定

February 1, 2024

RSA SecureID 認証用に RSA/ACE サーバを設定する場合は、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。

- NetScaler Gateway アプライアンスの名前を指定します。
- 説明を入力します (必須ではありません)。
- システム IP アドレスを指定します。
- NetScaler 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。

- NetScaler 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る）。FQDN を入力したら、[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 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。
- NetScaler Gateway を介した認証を許可されているすべてのユーザーまたはユーザーのセットをインポートするように構成します。

まだ設定されていない場合は、次の情報を含む RADIUS サーバのエージェントホストエントリを作成します。

- RSA サーバの FQDN を入力します。

  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 アドレスを指定します。

- 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、または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、仮想サーバまたはグローバルにバインドします。詳細については、「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

April 1, 2024

ドメインパスワードは、トークンが RADIUS サーバから生成する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 NetScaler Gateway にログオンすると、トークンの暗証番号（PIN）とパスコードを入力します。NetScaler Gateway が資格情報を検証すると、RADIUS サーバーはユーザーの Windows パスワードを NetScaler Gateway に返します。NetScaler 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シングルサインオンに使用します。RADIUS 機能によるこのパスワードの返却により、ユーザに Windows パスワードを思い出す必要なく、シングルサインオンを設定できます。

ユーザーがパスワードを返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、［パスワードベンダー識別子］パラメーターと［パスワード属性タイプ］パラメーターを使用して、NetScaler Gateway で RADIUS 認証ポリシーを構成します。これらの 2 つのパラメーターは、ユーザーの Windows パスワードを NetScaler Gateway に返します。

NetScaler Gateway は Imprivata OneSign をサポートしている。Imprivata OneSign の最低必要バージョンは、サービスパック 3 で 4.0 である。Imprivata OneSign のデフォルトのパスワードベンダー識別子は 398 です。Imprivata OneSign のデフォルトのパスワード属性タイプコードは 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。ユーザのシングルサインオンパスワードをベンダー固有の属性値のペアで返すように RADIUS サーバを設定します。NetScaler 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］パラメーターと［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 Web サイトにあります。たとえば、RSA セキュリティのベンダー識別子は 2197、Microsoft では 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 は、ベンダー固有属性のリストを Microsoft ベンダー固有の RADIUS 属性で公開しています。

ベンダー固有の属性を選択して、ベンダーの RADIUS サーバ上のユーザのシングルサインオンパスワードを保存できます。ユーザーパスワードが RADIUS サーバーに格納されているベンダー識別子と属性を使用して NetScaler Gateway を構成すると、NetScaler Gateway は、RADIUS サーバーに送信されるアクセス要求パケットの属性の値を要求します。RADIUS サーバが access-accept パケット内の対応する属性と値のペアで応答する場合、使用する RADIUS サーバに関係なく、パスワードの返却は機能します。

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、次の手順を実行します：

1. 構成ユーティリティの［構成］タブで、［**NetScaler 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. 詳細ペインで、[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 サーバーから返されるベンダー ID 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. [パスワード属性タイプ**]** に、ベンダー固有の AVP コードで RADIUS サーバから返される属性タイプを入力します。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の [名前付き式**]** の横で式を選択し、[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。

Configuring SafeWord Authentication

February 1, 2024

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、そのパスコードは SafeWord によって無効になり、再度使用することはできません。

セキュアゲートウェイおよび Web Interface 展開でアクセスゲートウェイが Secure Gateway を置き換える場合は、アクセスゲートウェイで認証を構成せず、Web Interface が着信 HTTP トラフィックに対して SafeWord 認証を提供することを引き続き許可することができます。

アクセスゲートウェイは、次の製品の SafeWord 認証をサポートしています。

- SafeWord 2008
- SafeWord プレミアアクセス
- SafeWord for Citrix
- SafeWord リモートアクセス

次の方法で、Access Gateway を SafeWord 製品を使用して認証するように構成できます。

- SafeWord PremierAccess の一部としてインストールされている PremierAccess RADIUS サーバーを使用するように認証を構成し、認証を処理できるようにします。
- SafeWord リモートアクセス、SafeWord for Citrix、および SafeWord PremierAccess 4.0 のコンポーネントである SafeWord IAS エージェントを使用するように認証を構成します。
- SafeWord Web Interface エージェントをインストールして、Citrix Web Interface をサポートします。Access Gateway で認証を構成する必要はなく、Citrix Web Interface でこれを処理できます。この構成では、PremierAccess RADIUS サーバーまたは SafeWord IAS エージェントは使用されません。

SafeWord RADIUS サーバーを構成する場合は、次の情報が必要です。

- アクセスゲートウェイの IP アドレス。RADIUS サーバでクライアント設定を構成する場合は、アクセスゲートウェイ 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 プロティバ認証の設定

February 1, 2024

Protiva は、Gemalto のスマートカード認証の長所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 認証サーバに送信され、パスワードは検証または拒否されます。

NetScaler Gateway をサポートするように Gemalto Protiva を構成するには、次のガイドラインを使用します。

- Protiva サーバーをインストールします。
- 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 Microsoft IAS RADIUS サーバーに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。

ゲートウェイ認証用の nFactor

April 1, 2024

nFactor 認証は、認証に関するまったく新しい可能性を可能にします。nFactor を使用する管理者は、仮想サーバーの認証要素を設定する際に、認証、承認、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 つの要因により、管理者は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できます。以前の要素に基づいて、nFactor は認証方法を決定します。動的ログインフォームと障害発生時のアクションは、nFactor を使用することで可能です。

> 重要
>
> - リリース 13.0 ビルド 67.x 以降、nFactor 認証はゲートウェイ/VPN 仮想サーバーでのみ標準ライセンスでサポートされ、認証仮想サーバーではサポートされません。Standard ライセンスでは、nFactor ビジュアライザー GUI を使用して nFactor フローで EPA を作成することはできません。また、ログインスキーマを編集することはできませんが、既成のログインスキーマをそのまま使用する必要があります。
> - NetScaler ADC が nFactor 認証をサポートするには、アドバンスドライセンスまたはプレミアムライ

> センスが必要です。NetScaler での nFactor 認証について詳しくは、「nFactor 認証」を参照してください。

認証、認可、監査機能のライセンス要件

次の表に、使用可能な認証、承認、および監査機能のライセンス要件を示します。

	標準ライセンス	上級ライセンス	プレミアムライセンス
ローカル認証	はい	はい	はい
LDAP 認証	はい	はい	はい
RADIUS 認証	はい	はい	はい
TACACS 認証	はい	はい	はい
Web 認証	はい	はい	はい
クライアント証明書認証	はい	はい	はい
認証のネゴシエート	はい	はい	はい
SAML 認証	はい	はい	はい
OAuth 認証	いいえ	はい	はい
ネイティブ **OTP**	いいえ	はい	はい
メール **OTP**	いいえ	はい	はい
OTP のプッシュ通知	いいえ	いいえ	はい
ナレッジベースの質問と回答 **(KBA** 認証**)**	いいえ	はい	はい
セルフサービスパスワードリセット **(SSPR)**	いいえ	はい	はい
nFactor ビジュアライザー	はい	はい	はい

> 注
>
> - NetScaler 標準ライセンスで nFactor を構成する手順については、NetScaler 標準ライセンスで

> nFactor 認証用のゲートウェイ仮想サーバーを作成するセクションを参照してください。
> - NetScaler Standard ライセンスのゲートウェイ/VPN 仮想サーバーにバインドできるのは、アドレス指定できない認証、承認、および監査仮想サーバーのみです。
> - NetScaler ADC 標準ライセンスでは、ログインスキーマのカスタマイズは許可されていません。nFactor のサポートは基本で、アプライアンスに付属するデフォルトおよびすでに追加されているログインスキーマのみがあります。管理者は設定で使用できますが、ログインスキーマを追加することはできません。したがって、GUI オプションは無効になります。

使用例

nFactor 認証は、ユーザプロファイルに基づいて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、フローがユーザーに対してシンプルで直感的になることがあります。それ以外の場合は、Active Directory または他の認証サーバのセキュリティ保護と組み合わせることができます。次に、Gateway に固有の要件をいくつか示します:

1. 動的なユーザー名とパスワードの選択。従来、クライアント（ブラウザとレシーバを含む）は、Active Directory（AD）のパスワードを最初のパスワードフィールドとして使用していました。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、まず OTP を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実行できます。
2. マルチテナント認証エンドポイント。組織によっては、証明書ユーザーと証明書以外のユーザーに異なる 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 NetScaler ADC アプライアンスによって異なります。ゲートウェイは、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。組織によっては、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できます。
4. 認証の副要因。場合によっては、異なる認証ポリシーのペアを使用して、異なるユーザーセットを認証することがあります。ペアポリシーを提供すると、効果的な認証が向上します。従属ポリシーは、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は、効率を高め、複雑さを軽減する独自のフローになります。

認証レスポンスの処理

NetScaler Gateway コールバックレジスタは、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 に適切なアクションを実行するように指示します。

クライアントサポート

次の表に、設定の詳細を示します。

Client	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	はい	VPN	はい
ゲートウェイプラグイン	はい	VPN	はい

注:

- Citrix Workspace アプリは、以下のバージョンのサポートされているオペレーティングシステムで nFactor 認証をサポートしています。
  - Windows 4.12
  - Linux 13.10
  - Mac 1808
  - iOS 2007
  - Android 1808
  - HTML5: ストアウェブを通じてサポート
  - Chrome: ストアウェブでサポート

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。属性としての仮想サーバ名は、このモデルに必要な唯一の設定です。

```
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。AuthnvsName 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。

相互運用性の課題

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 によって送信される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想

定されています。これらのクライアントは、「pwcount」「NSC_CERT」などのさまざまなゲートウェイ Cookie にも依存しています。

エンドポイント分析 **(EPA)**

nFactor の EPA は、NetScaler 認証、承認、および監査モジュールではサポートされていません。したがって、NetScaler Gateway 仮想サーバーは 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 は認証後処理を続行し、ユーザー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、ユーザクレデンシャルを 1 回だけ送信します。Gateway は、ログイン要求でクライアントから 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、これらの要素に使用されます。ただし、nFactor では、設定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、設定されたファクタに対して（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、ファクタで再使用されるパスワードが実際にそのファクタに適用可能であることを確認する必要があります。

クライアントの定義

この構成オプションは、NetScaler 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別するのに役立ちます。

管理者がすべてのクライアントのパターンを構成できるように、ns_vpn_client_useragents というパターンセットが提供されています。

同様に、「Citrix Receiver」文字列を上のpatsetにバインドして、ユーザーエージェントに「Citrix Receiver」を含むすべてのクライアントを無視します。

ゲートウェイの **nFactor** を制限する

次の条件が存在する場合、ゲートウェイ認証の nFactor は発生しません。

1. 認証プロファイルが NetScaler Gateway に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にバインドされません。同じ認証仮想サーバについては、authnProfileを参照してください。
3. HTTP 要求のユーザーエージェント文字列は、patset ns_vpn_client_useragent 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は、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。

User-Agent またはその一部が前述のpatset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、次のコマンドはすべてのブラウザの設定を制限します (すべてのブラウザで user-agent 文字列に「Mozilla」が含まれていると仮定します)。

```
1 bind patset ns_vpn_client_useragents Mozilla
2 <!--NeedCopy-->
```

ログインスキーマ

LoginSchema は、ログオンフォームの論理表現です。XML 言語によって定義されています。LoginSchema の構文は、Citrix の共通形式プロトコル仕様に準拠しています。

LoginSchema はプロダクトの「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。ログインスキーマには、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または失敗のメッセージを提供できます。

次のコマンドを使用して、ログインスキーマを設定します。

```
1 add authentication loginSchema <name> -authenticationSchema <string> [-
     userExpression <string>] [-passwdExpression <string>] [-
     userCredentialIndex <positive_integer>]
2 [-passwordCredentialIndex <positive_integer>] [-authenticationStrength
     <positive_integer>] [-SSOCredentials ( YES | NO )]
3 <!--NeedCopy-->
```

パラメータの説明

- name-新しいログインスキーマの名前。これは必須の議論です。最大長：127
- AuthenticationSchema-ログインページ 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。このファイルには、ログインフォームをレンダリングするための Citrix Forms 認証プロトコルに基づく要素の xml 定義が含まれています。管理者がユーザーに他の資格情報の入力を求めるのではなく、以前に取得した資格情報で続行する場合は、noschema を引数として与えることができます。これは、ユーザー定義ファクターで使用される LoginSchema にのみ適用され、仮想サーバーファクターには適用されません。

これは必須の議論です。最大長：255

- userExpression-ログイン時にユーザー名を抽出するための式。これは、関連する高度なポリシー式であればどれでも使用できます。最大長：127
- PasswdExpression-ログイン時のパスワード抽出の式。これは、関連する高度なポリシー式であればどれでも使用できます。最大長：127

- userCredentialIndex-ユーザーが入力したユーザー名のインデックスがセッションに格納されている必要があります。最小値:1、最大値:16
- PasswordCredentialIndex-ユーザーがパスワードを入力したインデックスは、セッションに格納する必要があります。最小値:1、最大値:16
- 認証強度-現在の認証の重み最小値:0、最大値:65535
- `SSOCredentials` -このオプションは、現在の要素認証情報がデフォルトの SSO (singleSignOn) 資格情報であるかどうかを示します。可能な値: はい、いいえ。デフォルト値:NO

ログインスキーマと **nFactor** の知識が必要

事前構築されたログインスキーマファイルは、次の Citrix **ADC** の場所**/nsConfig/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ており、必要に応じてわずかなバリエーションに変更できます。

また、カスタマイズがほとんどない単一要素のユースケースのほとんどは、ログインスキーマの設定を必要としません。

管理者は、NetScaler ADC が要因を検出できるようにする他の構成オプションについては、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設定して、認証ファクタを柔軟に選択して処理できます。

loginSchema を使用せずに二要素認証を構成する

NetScaler ADC は、構成に基づいて二重要素の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で最初のポリシー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、NetScaler ADC がユーザーにアクセスせずに既存の資格情報セット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」ファクターを使用することで、管理者はプログラムで認証フローを駆動できます。管理者は、nFactor の仕様書または展開ガイドで詳細を読むことをお勧めします。
マルチファクター (nFactor) 認証を参照してください。

ユーザ名とパスワードの表現

ログイン認証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 のカスタマイズがほとんどないシングルファクタまたはデュアルファクタのユースケースでは、XML 定義を指定する必要はありません。LoginSchema には、ユーザーが提示するユーザー名またはパスワードを変更するために使用できる userExpression や passwdExpression などの他のプロパティがあります。

ログインスキーマ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も使用できます。これは、次の例に示すように、**-AuthenticationSchema** にパラメータの文字列を追加することで実現できます。

以下は、ユーザー名とパスワードのユーザー入力をそれぞれ変更する例です。

- ユーザ名のユーザ入力をusername@citrix.comからusername@xyz.comに変更します。

```
1   add authentication loginSchema user_schema -authenticationSchema
       LoginSchema/DualAuth.xml -userExpression "AAA.LOGIN.USERNAME.
       BEFORE_STR("@").APPEND("@xyz.com")"
2   <!--NeedCopy-->
```

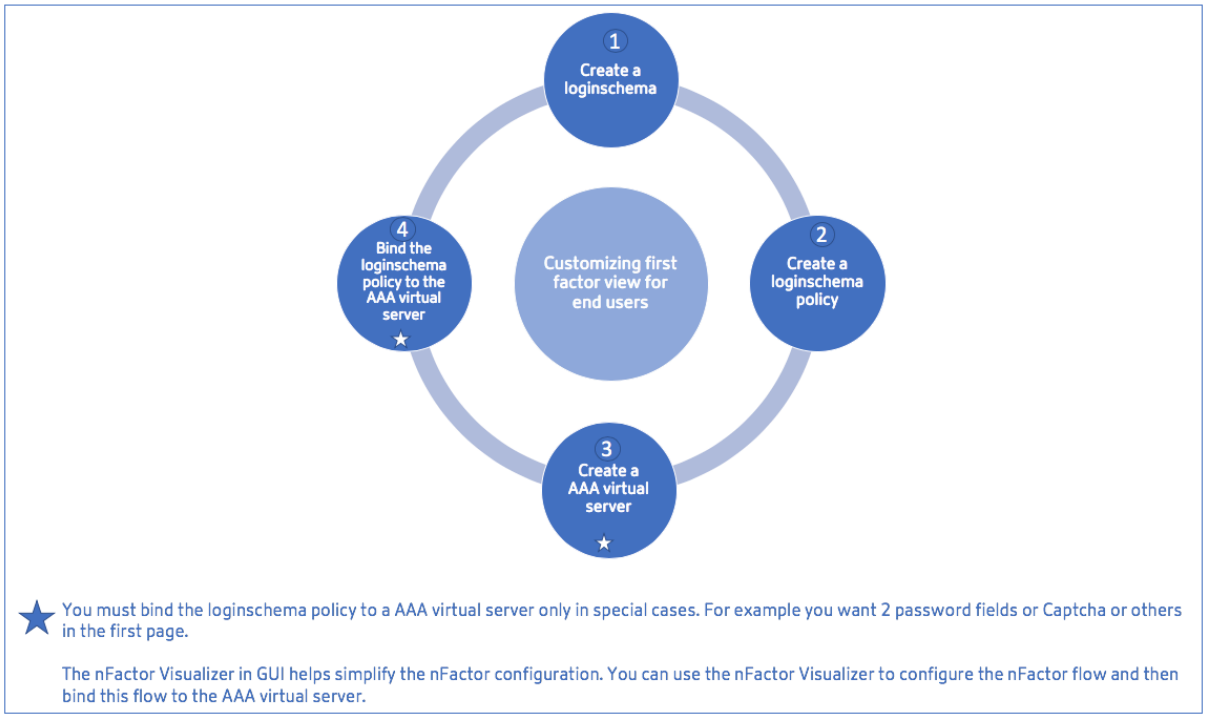
- 構成されたログインスキーマの一部として、ユーザーが第 1 要素にパスワードとパスコードを入力するシナリオを考えてみましょう。最初の要素でユーザーによって提供されたパスコードを使用し、2 番目の要素でパスワードを使用するには、次のコマンドを使用して既存のログインスキーマを変更できます。

```
1   add authentication loginSchema user_schema -authenticationSchema
       LoginSchema/DualAuth.xml -passwdExpression "AAA.LOGIN.
       PASSWORD2"
2   <!--NeedCopy-->
```

```
1   add authentication loginSchema user_schema_second -
       authenticationSchema noschema  -passwdExpression "AAA.LOGIN.
       PASSWORD"
2   <!--NeedCopy-->
```

nFactor 構成のハイレベルな手順

次の図は、nFactor の設定に関連する高レベルの手順を示しています。



GUI 構成

このセクションでは、次のトピックについて説明します。

- 仮想サーバーを作成する
- 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 認証サーバーを追加する
- LDAP 認証ポリシーを追加する
- 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

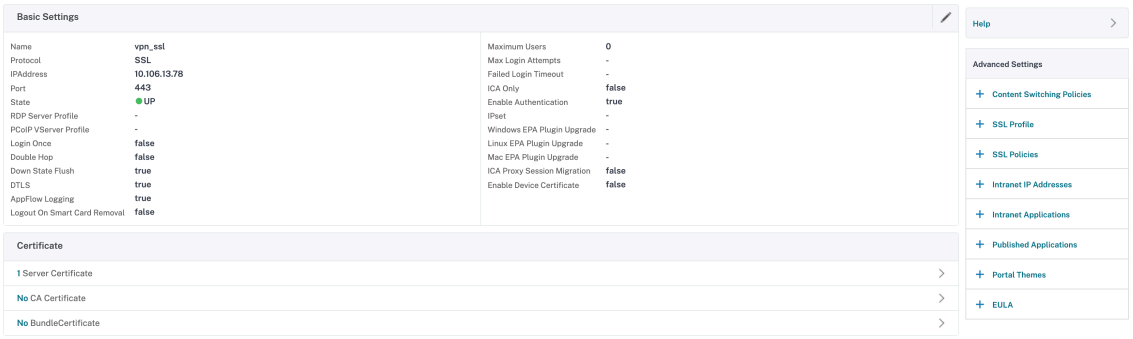
1. 「**NetScaler Gateway**」**>**「仮想サーバー」に移動します。
2. [**Add**] ボタンをクリックして、ゲートウェイ仮想サーバーを作成します。
3. 次の情報を入力し、「**OK**」をクリックします。

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。	NetScaler Gateway 仮想サーバーの名前。ASCII アルファベット文字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 (@)、等号 (=)、およびハイフン (-) のみを含める必要があります。仮想サーバーの作成後に変更できます。次の要件は、NetScaler 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（たとえば、「マイサーバー」または「マイサーバー」）。
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。

パラメーター名	パラメータの説明
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機器に割り当てられた数値ラベルです。
仮想サーバー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。	仮想サーバ上の認証プロファイルエンティティ。このエンティティは、多要素 (nFactor) 認証のために、認証、承認、および監査仮想サーバーに認証をオフロードするために使用できます。
RDP サーバプロファイルを入力します。	仮想サーバに関連付けられている RDP サーバプロファイルの名前。
[最大ユーザー数] を入力します。	この仮想サーバー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総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。	ログオン試行の最大回数。
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を入力します。	Linux のプラグインアップグレード動作を設定するオプション。
MAC EPA プラグインのアップグレードに入る	Mac のプラグインアップグレード動作を設定するオプション。
一度ログイン	このオプションは、この仮想サーバーのシームレス SSO を有効または無効にします。

パラメーター名	パラメータの説明
ICA のみ	［オン］に設定すると、ユーザーは Citrix Workspace アプリまたはブラウザーのいずれか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 Secure Access クライアントを使用して接続することはできず、エンドポイントスキャンを構成することもできません。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、ユーザーは Citrix Workspace アプリ、ブラウザ、または Citrix Secure Access クライアントのいずれかを使用してログオンできる SmartAccess モードになります。管理者は、クライアントシステム上でエンドポイントスキャンを実行するように構成し、その結果を使用して公開アプリ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 およびクライアントレス VPN）でゲートウェイに接続できます。ログインしてリソースにアクセスできるユーザーの数は、このモードの CCU ライセンスによって制限されます。
認証を有効にする	NetScaler Gateway に接続するユーザーに認証を要求します。
ダブルホップ	NetScaler 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強化します。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配置できます。
ダウンステートフラッシュ	仮想サーバーが DOWN とマークされたら、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、場合によっては過負荷の負荷分散セットアップの回復が高速化されます。この設定は、接続がダウンしているときに接続を安全に閉じることができるサーバーで有効にします。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 状態のフラッシュを有効にしないでください。

パラメーター名	パラメータの説明
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 ロギング	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、標準の NetFlow または IPFIX 情報を含む 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、応答ステータスコード、サーバー応答時間、待機時間などのアプリケーションレベルの情報を含むレコードも記録します。
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	仮想サーバの現在の状態（UP、DOWN、BUSY など）。
デバイス証明書を有効にする	EPA の一部としての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. [サーバー証明書の選択**]** の **[****] 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. [**Bind**] 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。

認証仮想サーバーを作成する

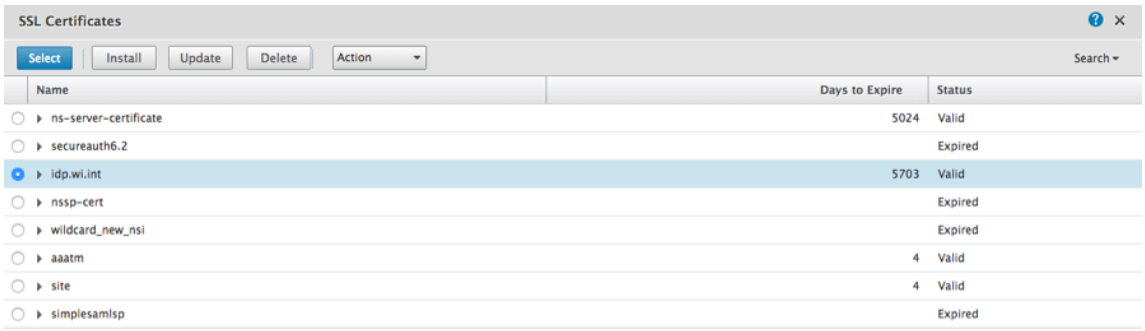
1. [** セキュリティ] > [NetScaler AAA ―アプリケーショントラフィック] **[仮想サーバー] に移動します

2. [追加] をクリックします。
3. 次の基本設定を完了して、認証仮想サーバーを作成します。

   注**:** 設定名の右側にある * 記号は、必須フィールドを示します。

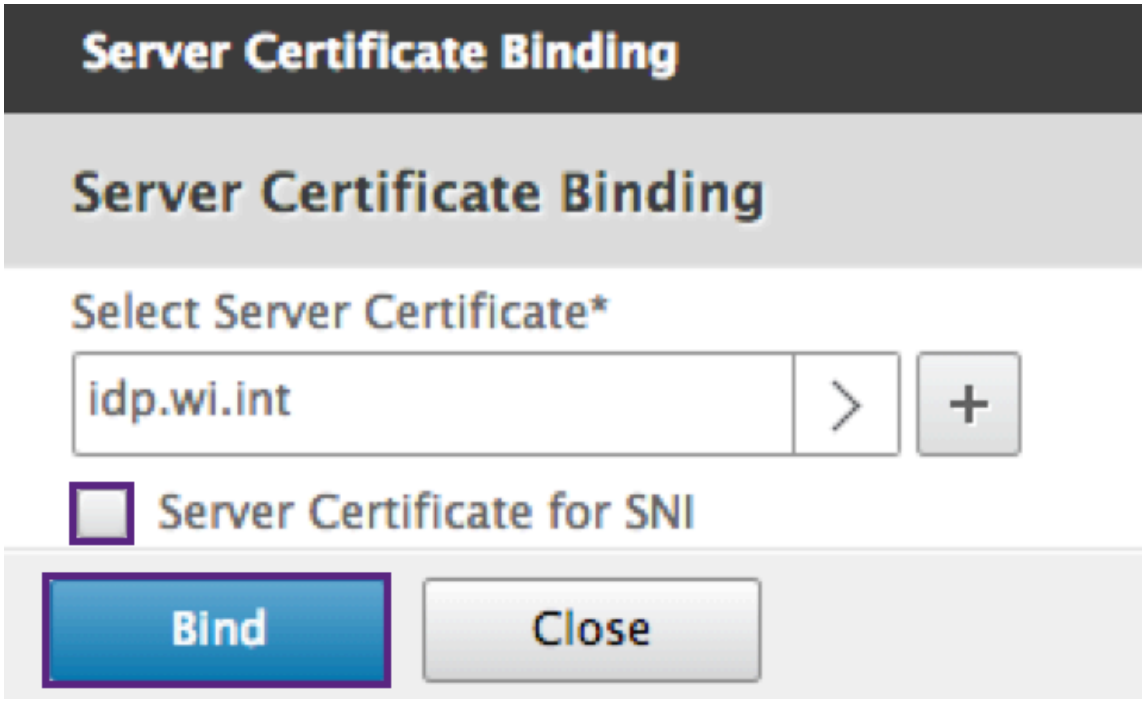
   - 新しい認証仮想サーバの [**Name**] を入力します。
   - **IP** アドレスタイプを入力します。IP アドレスタイプは、アドレス指定不可として設定できます。
   - **IP** アドレスを入力します。IP アドレスはゼロでもよい。
   - 認証仮想サーバのプロトコルタイプを入力します。
   - 仮想サーバが接続を受け付ける **TCP** ポートを入力します。
   - 認証仮想サーバによって設定された認証 Cookie のドメインを入力します。
4. [**OK**] をクリックします。
5. [サーバー証明書なし] をクリックします。
6. リストから目的のサ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、証明書がバインドされている必要はありません。



8. サーバ証明書バインディングを設定します。

   - **SNI** 処理に使用される **1** つ以上の証明書キーをバインドするには、**[SNI** のサーバー証明書] 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**]-> [NetScaler 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**]-> [**証明書**]** 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。設定名の右にある * 記号は、必須フィールドを示します。
   - **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―この場合、2 要素認証オプションは NOOP です。
   - 「ユーザー名フィールド」―ユーザー名の抽出元となる client-cert フィールドを入力します。”Subject “または”Issuer”(両方の二重引用符を含む) のいずれかに設定する必要があります。
   - グループ名フィールド -グループが抽出されるクライアント証明書フィールドを入力します。”Subject “または”Issuer”(両方の二重引用符を含む) のいずれかに設定する必要があります。
   - デフォルト認証グループ -これは、抽出されたグループに加えて認証が成功した場合に選択されるデフォルトのグループです。
4. [**Create**] をクリックします。

認証ポリシーを作成する

> 注:
>
> AAA.login を使用してポリシールールで第 1 要素ポリシーを構成する場合、Citrix Workspace アプリが nFactor 展開をサポートするには、次の式を OR 条件で構成する必要があります。
>
> ```
> || HTTP.REQ.URL.CONTAINS("/cgi/authenticate")
> ```

1. [セキュリティ**]-> [NetScaler AAA** —アプリケーショントラフィック**]-> [**ポリシー**]-> [**認証**]-> [**詳細ポリシー**]-> [**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。設定名の右にある * 記号は、必須フィールドを示します。

   a) [名前] —高度な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、およびハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等号 (=)、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、NetScaler 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（たとえば、「認証ポリシー」または「認証ポリシー」）。

   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される認証アクションの名前を入力します。

   d) ログアクション -要求がこのポリシーに一致した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 -認証サーバーでユーザーを認証するかどうかを決定するためにポリシーが使用する NetScaler ADC 名前付きルールの名前またはデフォルトの構文式を入力します。

   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を入力します。
4. ［作成］をクリックします

LDAP 認証サーバーを追加する

1. [セキュリティ**]-> [NetScaler 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. [サーバ] タブを選択し、[追加] ボタンを選択して LDAP ** サーバを追加します ** 。

LDAP 認証ポリシーを追加する

1. セキュリティ **> NetScaler AAA-**アプリケーショントラフィック **>** ポリシー **>** 認証 **>** 詳細ポリシー **>** ポリシーに移動します。

2. [**Add**] 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。設定名の右にある * 記号は、必須フィールドを示します。

   a) 名前 -高度な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、およびハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等号 (=)、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、NetScaler 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（たとえば、「認証ポリシー」または「認証ポリシー」）。

   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**： リクエストがこのポリシーに一致したときに使用するメッセージログアクションの名前。

   e）式 -認証サーバーでユーザーを認証するかどうかを決定するためにポリシーが使用する NetScaler ADC 名前付きルールの名前、またはデフォルトの構文式。

   f) コメント -このポリシーに関する情報を保存するためのコメント。
4. 「作成」をクリックします。

RADIUS 認証サーバーを追加する

1. [セキュリティ**] > [NetScaler 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。設定名の右にある * 記号は、必須フィールドを示します。

   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 **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] の値を数秒で入力します。NetScaler ADC アプライアンスは、構成されたタイムアウト値が期限切れになるまで、RADIUS サーバーからの応答を待ちます。

   e) RADIUS サーバーと Citrix **ADC** アプライアンス間で共有される秘密キーを入力します。秘密キーは、NetScaler 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) 秘密キーを確認します。
4. 「作成」をクリックします。

RADIUS 認証ポリシーを追加する

1. セキュリティ **> NetScaler AAA-**アプリケーショントラフィック **>** ポリシー **>** 認証 **>** 詳細ポリシー **>** ポリシーに移動します。
2. [**Add**] 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。設定名の右にある * 記号は、必須フィールドを示します。

   a) **Name**： 高度な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、およびハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等号 (=)、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、NetScaler 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（たとえば、「認証ポリシー」または「認証ポリシー」）。

   a) アクションタイプ -認証アクションのタイプ。

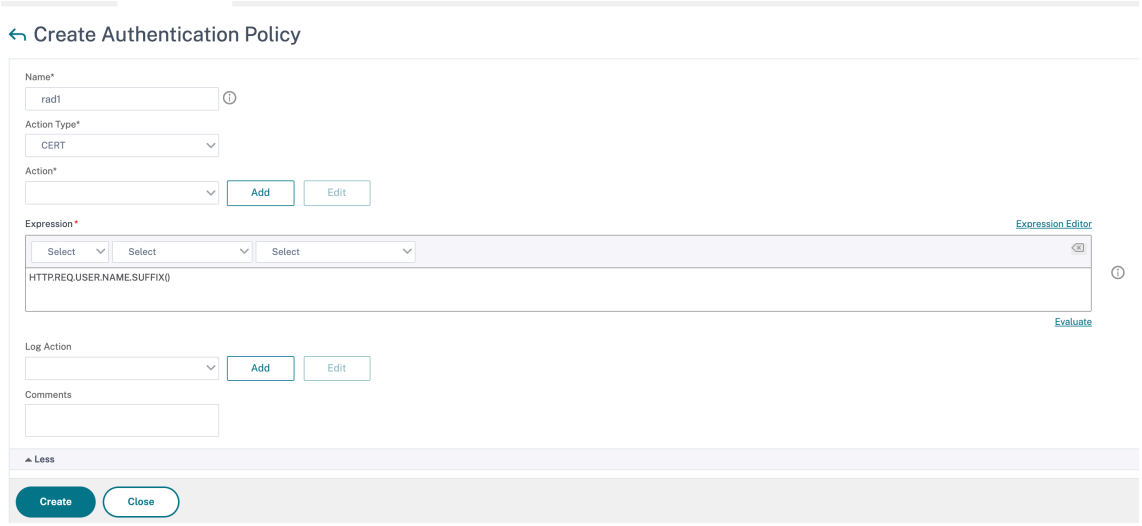
   b) **Action**： ポリシーが一致した場合に実行される認証アクションの名前。

   c) ログアクション -リクエストがこのポリシーに一致する場合に使用するメッセージログアクションの名前。

   d) 式 -認証サーバーでユーザーを認証するかどうかを決定するためにポリシーが使用する NetScaler ADC 名前付きルールの名前、またはデフォルトの構文式。

   e) コメント -このポリシーに関する情報を保存するための任意のコメント。

4. 「**OK**」をクリックします。作成した認証ポリシーがポリシーの一覧に表示されます。



認証ログインスキーマの作成

1. [セキュリティ**] > [NetScaler 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. 次のフィールドに入力して、認証ログインスキーマを作成します:

   a)「名前を入力」—新しいログインスキーマの名前です。

   b) 認証スキーマの入力 -ログインページ UI に送信される認証スキーマを読み取るファイルの名前。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には、Citrix Forms 認証プロトコルに従って要素の XML 定義が含まれている必要があります。管理者がユーザにさらなるクレデンシャルを要求せず、以前に取得したクレデンシャルで続行する場合は、”noschema“を引数として与えることができます。これは、ユーザー定義ファクタで使用される loginSchemas にのみ適用され、仮想サーバーファクタには適用されません

   c) ユーザー式の入力 -ログイン時にユーザー名を抽出するための式

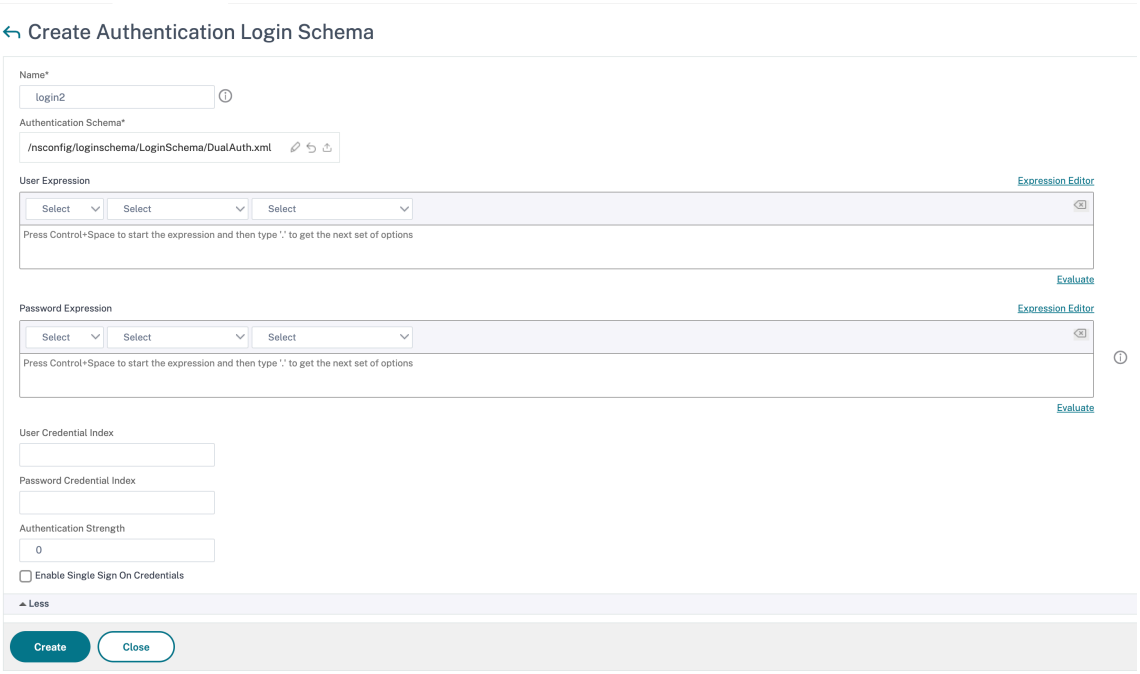
   d) パスワード式の入力 -ログイン時のパスワード抽出の式

   e) ユーザー資格情報インデックスの入力 -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。

   f) パスワード認証情報インデックスの入力 -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必要があるインデックス。

   g) 認証強度 -現在の認証の重みを入力します。

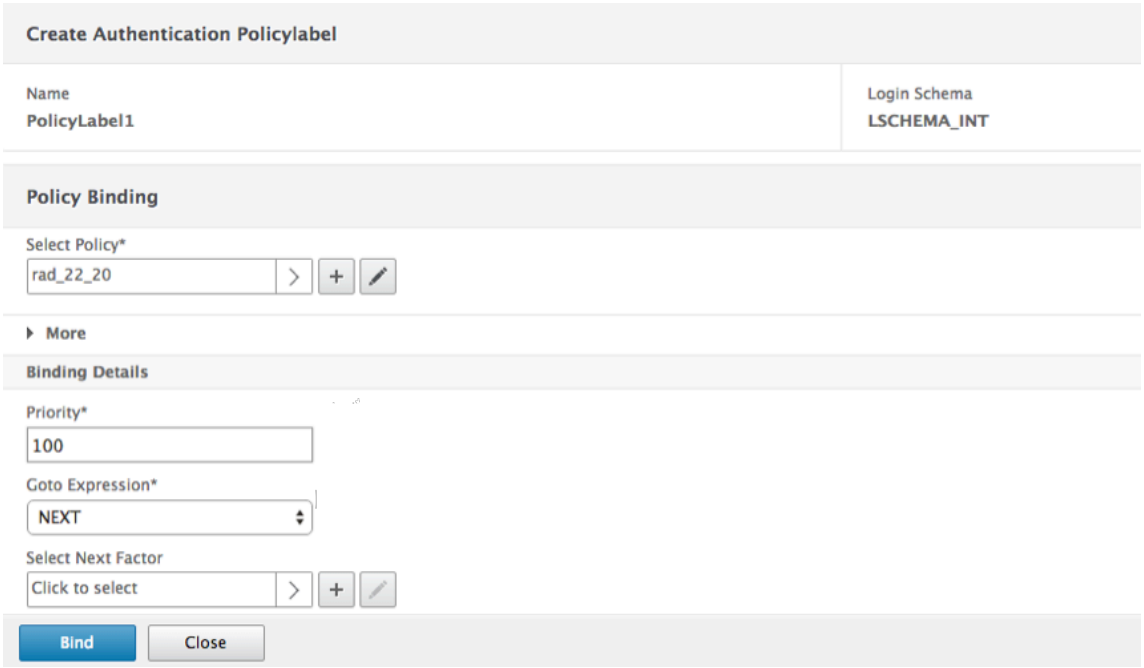
4.「作成」をクリックします。作成したログインスキーマプロファイルが、ログインスキーマプロファイルリストに表示されている必要があります。



ポリシーラベルを作成する

ポリシーラベルは、特定のファクタ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 **> NetScaler AAA-**アプリケーショントラフィック **>** ポリシー **>** 認証 **>** 詳細ポリシー **>** 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. 次のフィールドに入力して、認証ポリシーラベルを作成します：
   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** 式を入力します。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度を指定します。



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 認証の設定を再キャプチャする

NetScaler ADC リリース 12.1 ビルド 50.x 以降、NetScaler 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アクション「CaptchaAction」をサポートします。キャプチャはファーストクラスアクションであるため、独自の要素になる可能性があります。キャプチャは nFactor フローのどこにでも挿入できます。

以前は、RfWebUI に変更を加えたカスタム WebAuth ポリシーも作成する必要がありました。CaptchaAction の導入により、JavaScript を変更する必要はありません。

> 重要
>
> スキーマでユーザー名またはパスワードフィールドと一緒に Captcha が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。

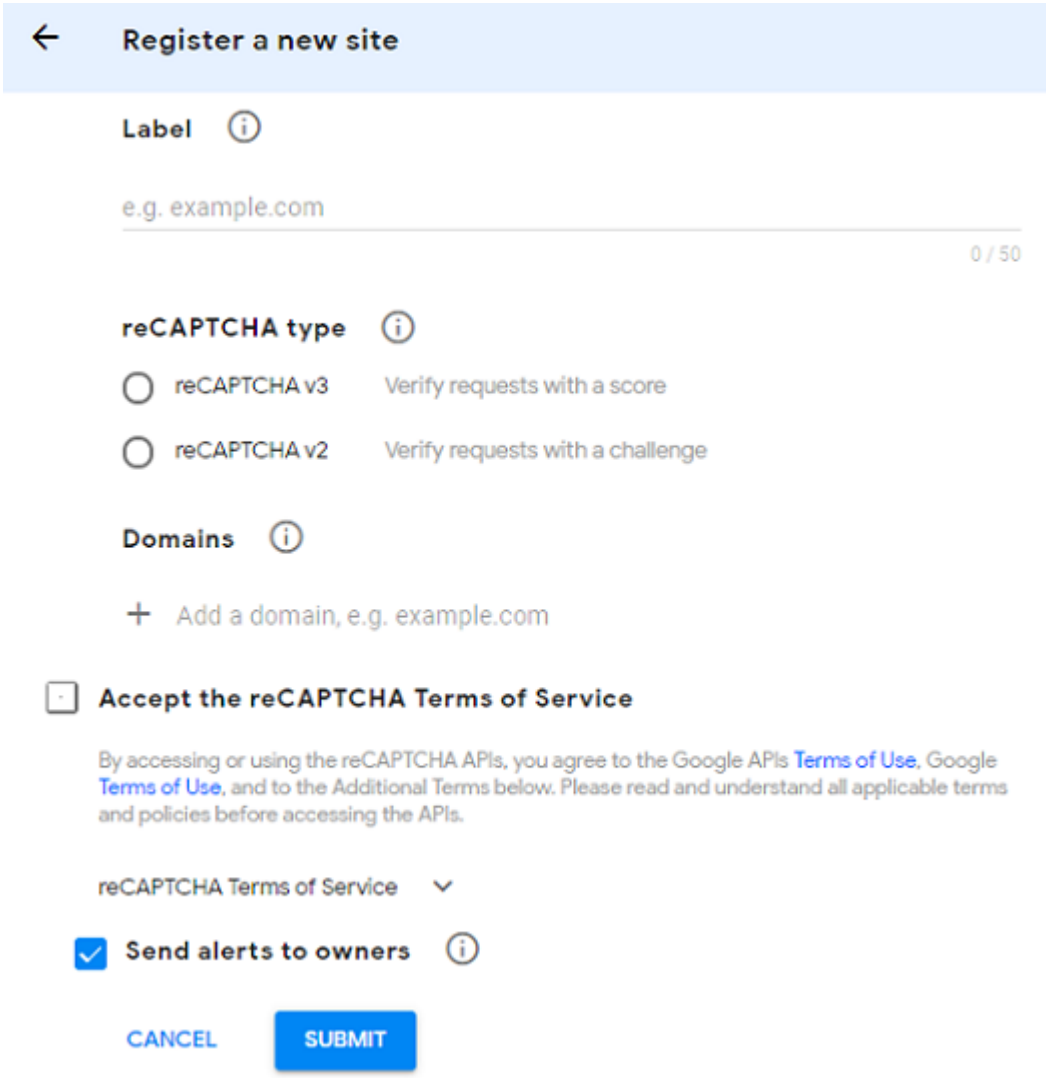
キャプチャの設定

キャプチャの設定には 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 の設定。
2. ログインフローの一部としてキャプチャを使用するように NetScaler ADC アプライアンスの構成。

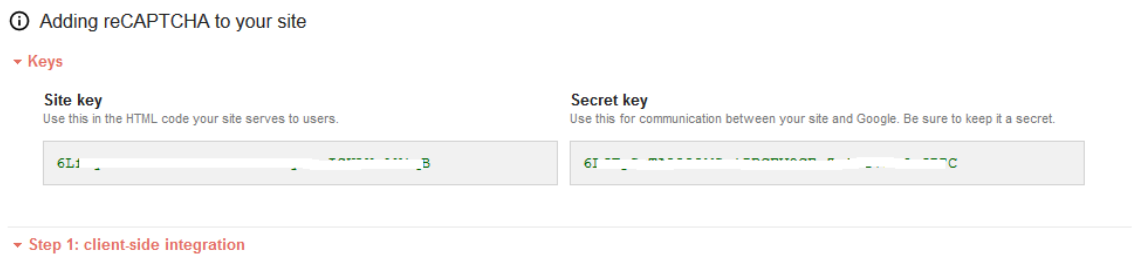
グーグルでのキャプチャの設定　`https://www.google.com/recaptcha/admin#list`でキャプチャのドメインを登録します。

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 のみを使用します。見えないreCAPTCHAはまだプレビュー中です。

2. ドメインが登録されると、「SiteKey」と「secretKey」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。

NetScaler ADC アプライアンスのキャプチャ構成　NetScaler 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
- キャプチャレスポンスを Google サーバーに投稿する
- 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 SingleAuthCaptcha.xml は、NetScaler ADC アプライアンスの/nsconfig/loginSchema/LoginSchema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 Factor（ユーザー名やパスワードなし）のみが必要な場合や、Captcha との二重認証が必要な場合などです。
> - カスタムの変更を実行したり、ファイルの名前を変更したりする場合は、すべてのログインスキーマを/nsConfig/loginSchema/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

```
1 -  add authentication loginSchema singleauthcaptcha -
     authenticationSchema /nsconfig/loginschema/SingleAuthCaptcha.xml
2
3 -  add authentication loginSchemaPolicy singleauthcaptcha -rule true -
     action singleauthcaptcha
4
5 -  add authentication vserver auth SSL <IP> <Port>
6
7 -  add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to
     -key-file>
8 -  bind ssl vserver auth -certkey vserver-cert
9 -  bind authentication vserver auth -policy singleauthcaptcha -priority
      5 -gotoPriorityExpression END
10 <!--NeedCopy-->
```

キャプチャレスポンスを **Google** サーバーに投稿する　ユーザーに表示する必要がある Captcha を設定した後、管理者は Google サーバーに設定をポストして、ブラウザからの Captcha 応答を確認します。

ブラウザから **Captcha** レスポンスを確認するには

```
1 -  add authentication captchaAction myrecaptcha -sitekey <sitekey-
     copied-from-google> -secretkey <secretkey-from-google>
```



```
2
3  -  add authentication policy myrecaptcha -rule true -action myrecaptcha
4  -  bind authentication vserver auth -policy myrecaptcha -priority 1
5  <!--NeedCopy-->
```

AD 認証が必要かどうかを設定するには、次のコマンドが必要です。それ以外の場合は、この手順は無視してかまいません。

```
1  -  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
2
3  -  add authenticationpolicy ldap-new -rule true -action ldap-new
4  <!--NeedCopy-->
```

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 Captcha の後に行われ、2 番目の要素に追加します。

```
1  -  add authentication policylabel second-factor
2  -  bind authentication policylabel second-factor -policy ldap-new -
      priority 10
3  -  bind authentication vserver auth -policy myrecaptcha -priority 1 -
      nextFactor second-factor
4  <!--NeedCopy-->
```

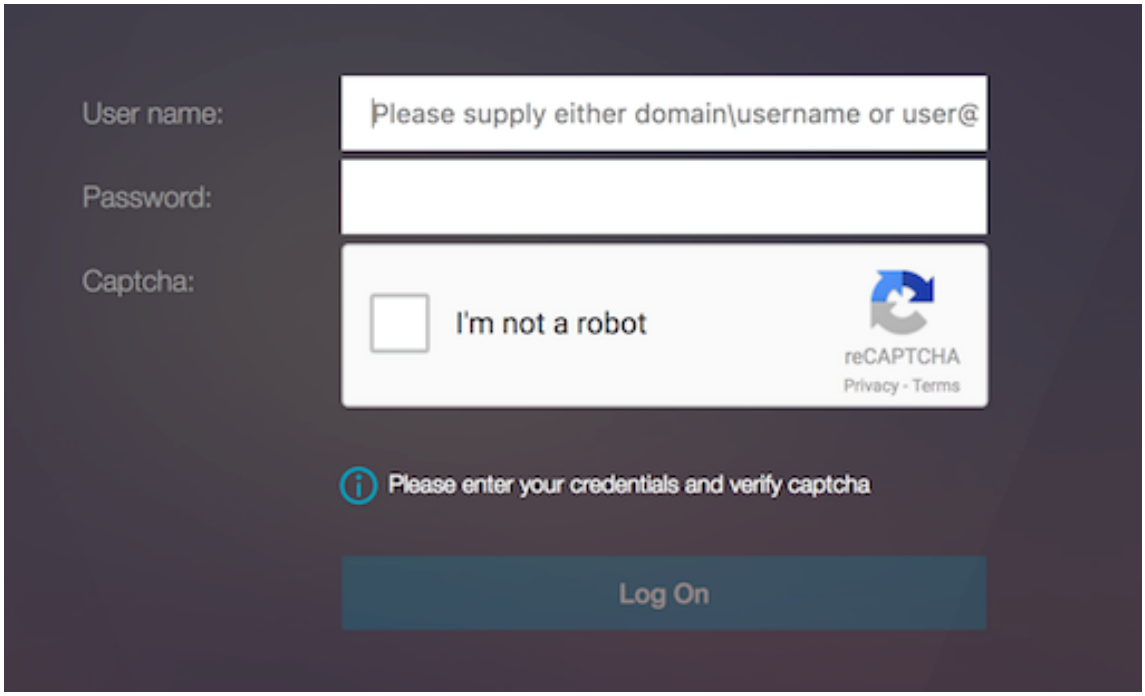
管理者は、アクセスに負荷分散仮想サーバーと NetScaler Gateway アプライアンスのどちらを使用するかに応じて、適切な仮想サーバーを追加する必要があります。負荷分散仮想サーバーが必要な場合は、管理者が次のコマンドを構成する必要があります。

```
1  add lb vserver lbtest HTTP <IP> <Port> -authentication ON -
      authenticationHost nssp.aaatm.com`
2  <!--NeedCopy-->
```

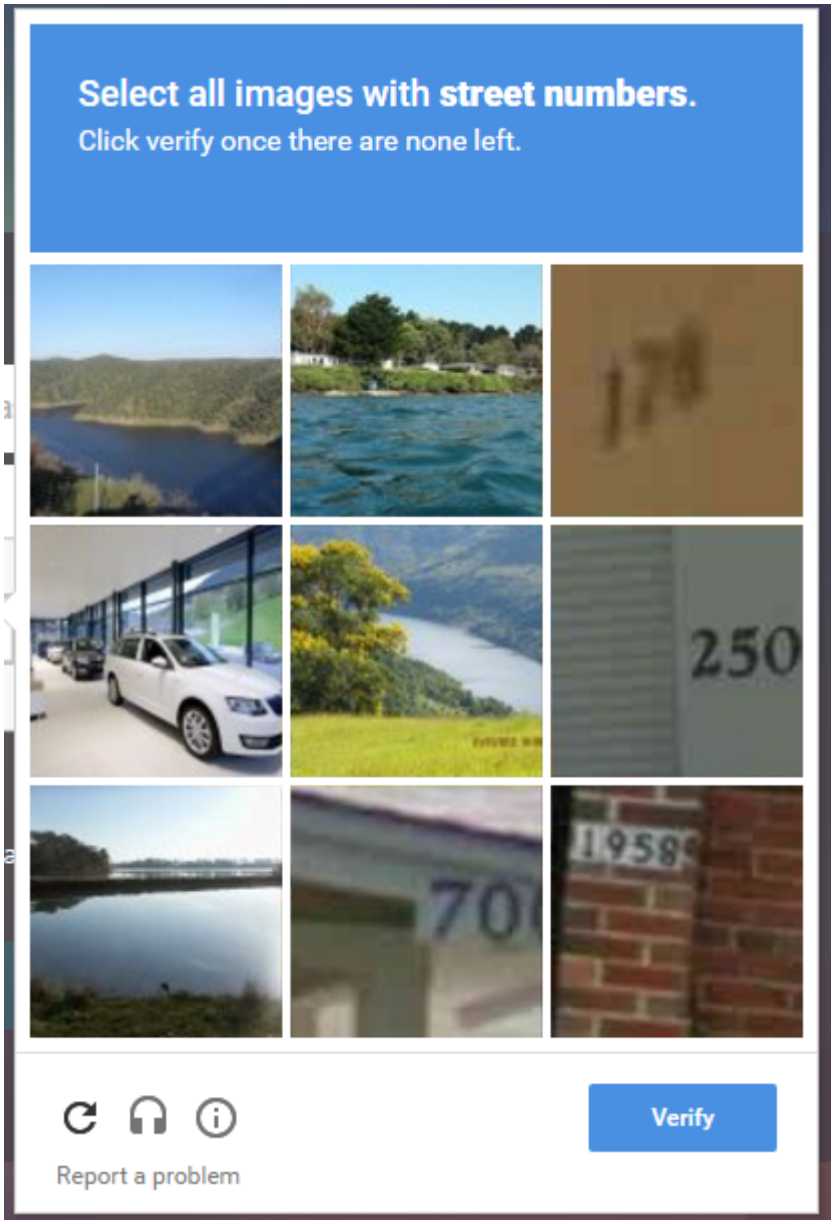
nssp.aaatm.com —認証仮想サーバに解決されます。

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、前述のユーザインターフェイスの画面キャプチャを参照してください。

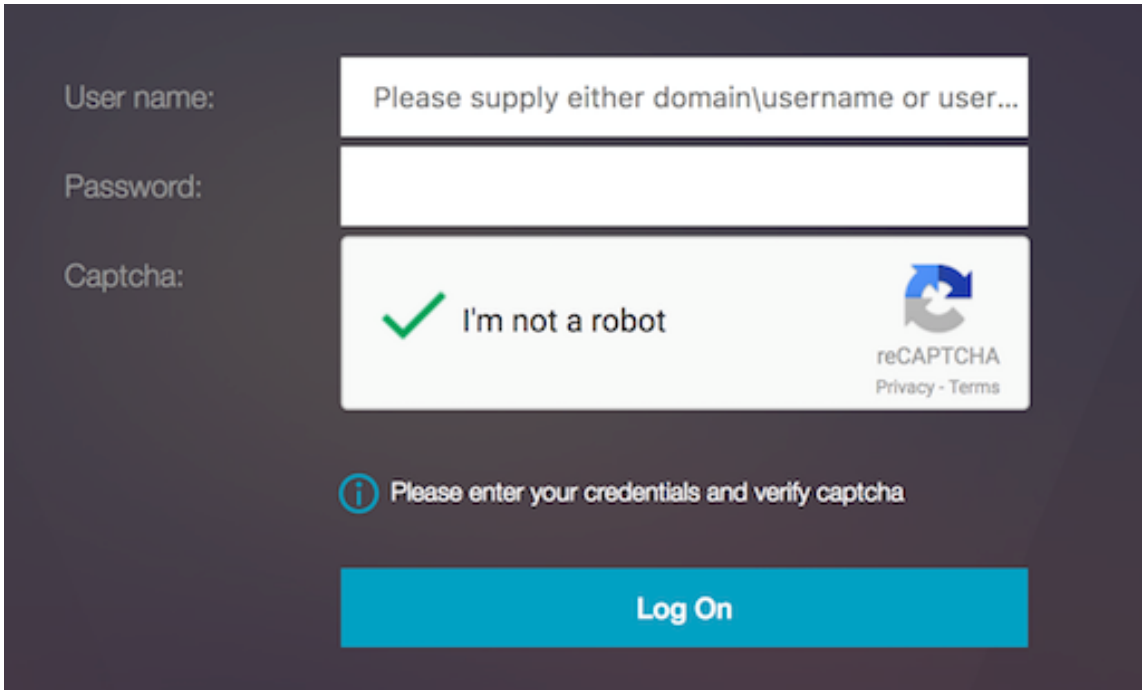
1. 認証仮想サーバーがログインページをロードすると、ログオン画面が表示されます。ログオンは、キャプチャが完了するまで無効になります。



2. [私はロボットではない] 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、一連のキャプチャイメージ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。

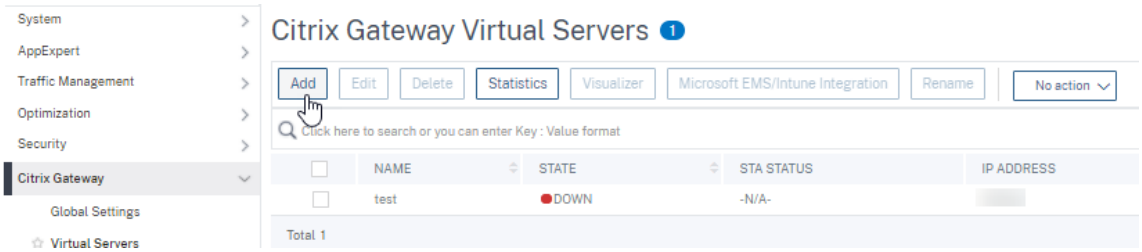


注:

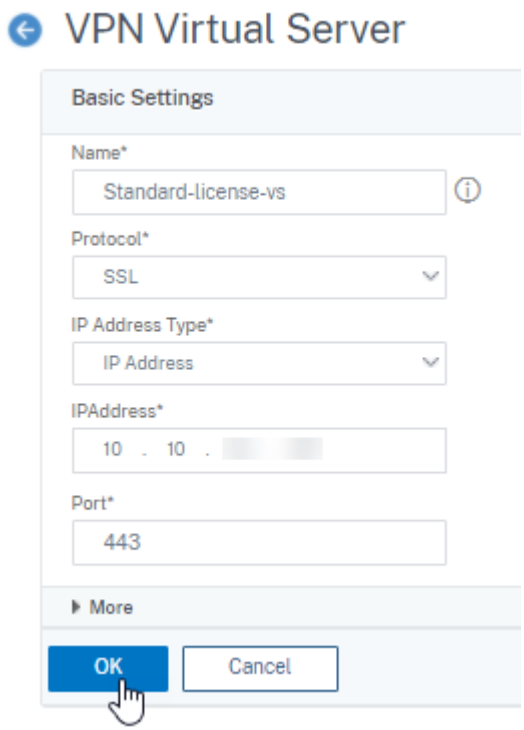
- AD 認証で Captcha を使用する場合、認証情報の [送信] ボタンは、キャプチャが完了するまで無効になります。
- キャプチャは独自の要素で発生します。したがって、AD のような後続の検証は Captcha の`nextfactor`で行われなければなりません。

NetScaler ADC 標準ライセンスで **nFactor** 認証用のゲートウェイ仮想サーバーを作成する

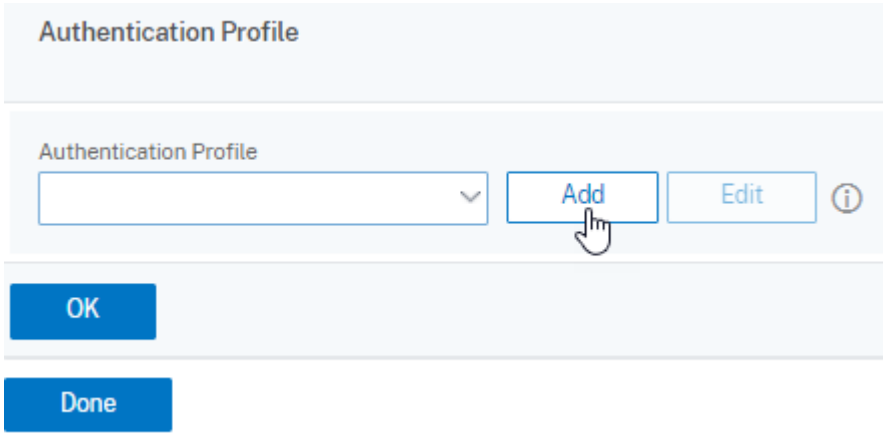
1. [**NetScaler Gateway**] **>** [仮想サーバー] に移動します。
2. [**NetScaler Gateway** 仮想サーバー] ページで、[追加] をクリックします。



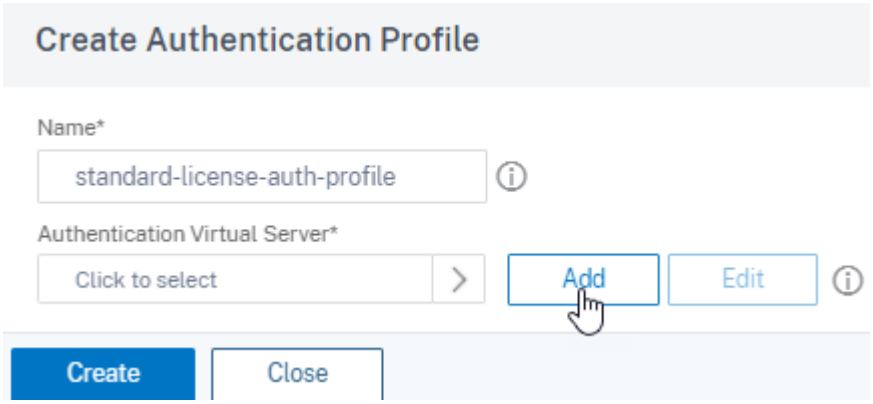
3. 「**VPN** 仮想サーバー」ページで次の詳細を入力し、「**OK**」をクリックし、「続行」をクリックします。
   - 名前: NetScaler Gateway 仮想サーバーの名前
   - プロトコル- **SSL** を選択
   - IP アドレス-NetScaler Gateway 仮想サーバーの IP アドレス
   - ポート-443 と入力します。



4. [**VPN** 仮想サーバ] ページで、[認証プロファイル] の横にあるプラスアイコンをクリックします。
5. [**Add**] をクリックして、認証プロファイルを設定します。

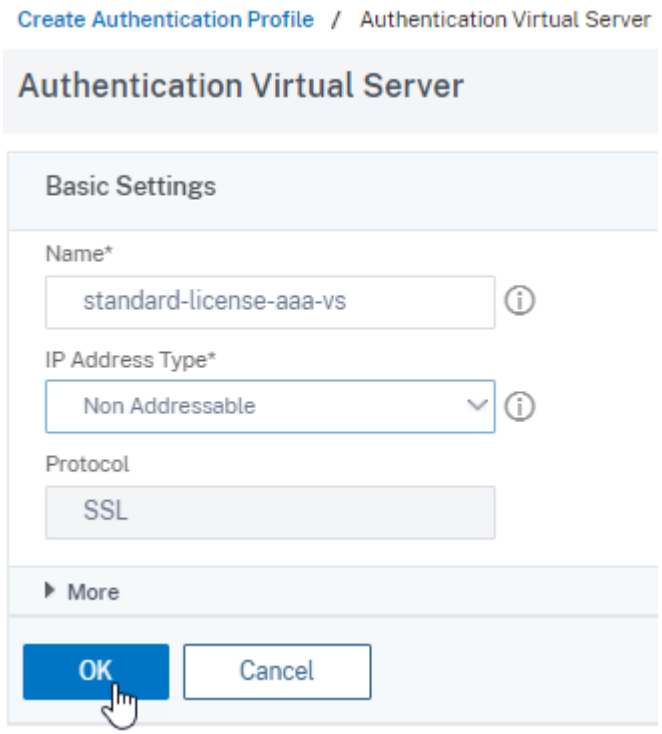


6. 認証プロファイルの名前を入力し、[**Add**] をクリックします。



7. 「**VPN** 仮想サーバー」ページで次の詳細を入力し、「**OK**」をクリックし、「続行」をクリックします。

   - Name: 認証、承認、および監査する仮想サーバの名前
   - プロトコル-[アドレス指定不可] を選択します。NetScaler Standard ライセンスのゲートウェイ/VPN 仮想サーバーにバインドできるのは、アドレス指定できない認証、承認、および監査仮想サーバーのみです。



> 注:
>
> - NetScaler Standard ライセンスでは、ポリシーを作成する手順は、サポートされているポリシータイプのプレミアムライセンスと同じです。
> - NetScaler Standard ライセンスでは、nFactor 構成での新しいログインスキーマの追加はサポートされていません。

参照ドキュメント

エンドツーエンド nFactor の設定例については、nFactor 認証の設定を参照してください。

Unified Gateway ビジュアライザー

April 1, 2024

Unified Gateway ビジュアライザは、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 ビジュアライザは、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。

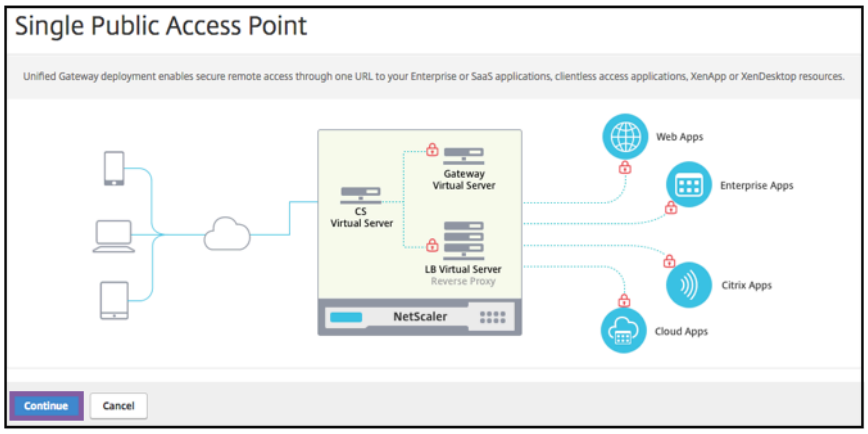
Unified Gateway ビジュアライザには、次の情報が表示されます。

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 仮想サーバー	XA/XD アプリ
ウェブアプリ	SaaS アプリ

Unified Gateway 展開により、エンタープライズまたは 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単一の URL を介した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 証明書を含む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 アプリケーションの URL または Citrix Virtual Apps and Desktops サーバーの詳細)。
3. [続行] ボタンをクリックします。

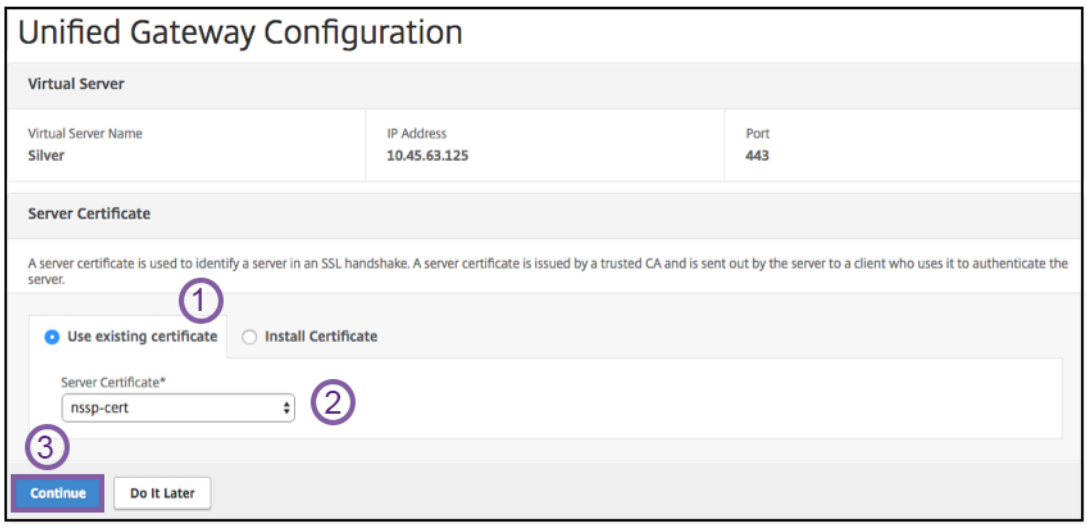


Unified Gateway 構成仮想サーバーを作成します。

1. 仮想サーバの設定名を入力します。
2. **Unified Gateway** 展開用のパブリック向けユニ **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。

次の情報を入力してサーバー証明書を指定します。

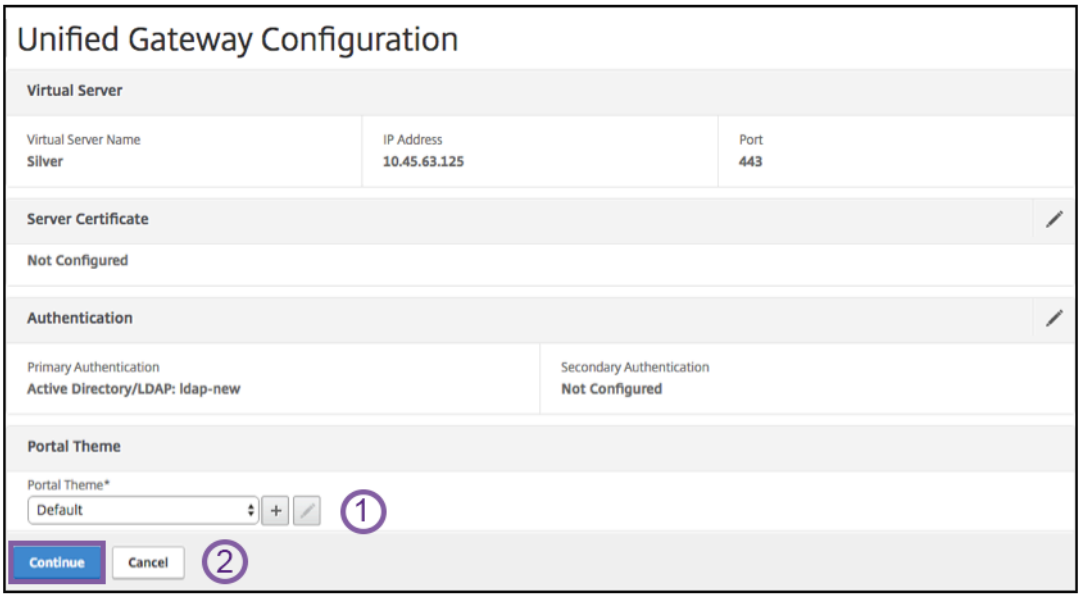
1. [既存の証明書を使用] または **[**** 証明書のインストール **] ラジオボタンを選択します。
2. メニューからサーバー証明書を選択します。
3. [続行] ボタンをクリックします。



認証を指定するには、次の情報を入力します。

1. メニューから [プライマリ] 認証方法を選択します。
2. [既存のサーバを使用] または [新しいサーバの追加] 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。
4. メニューから [ポータルのテーマ] を選択します。

5. [続行] をクリックします。
6. [**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。
7. [続行] をクリックします。



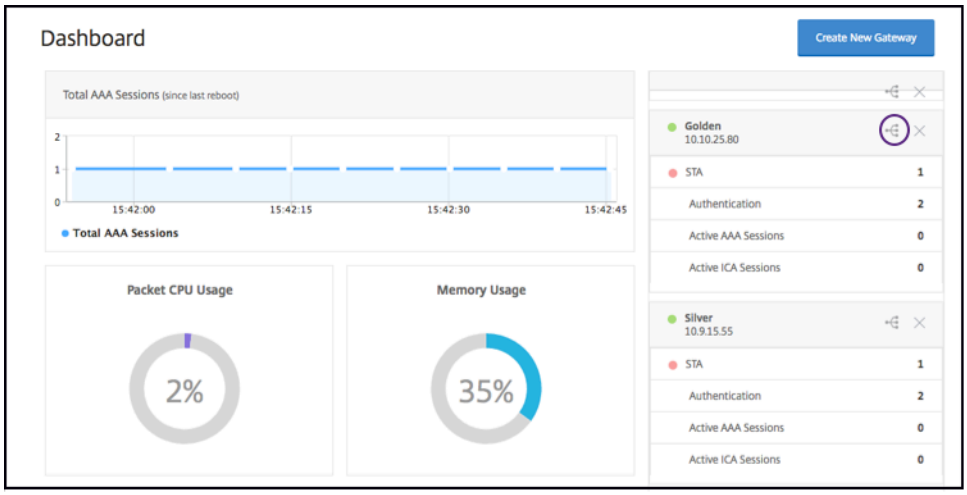
アプリケーションを選択

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。

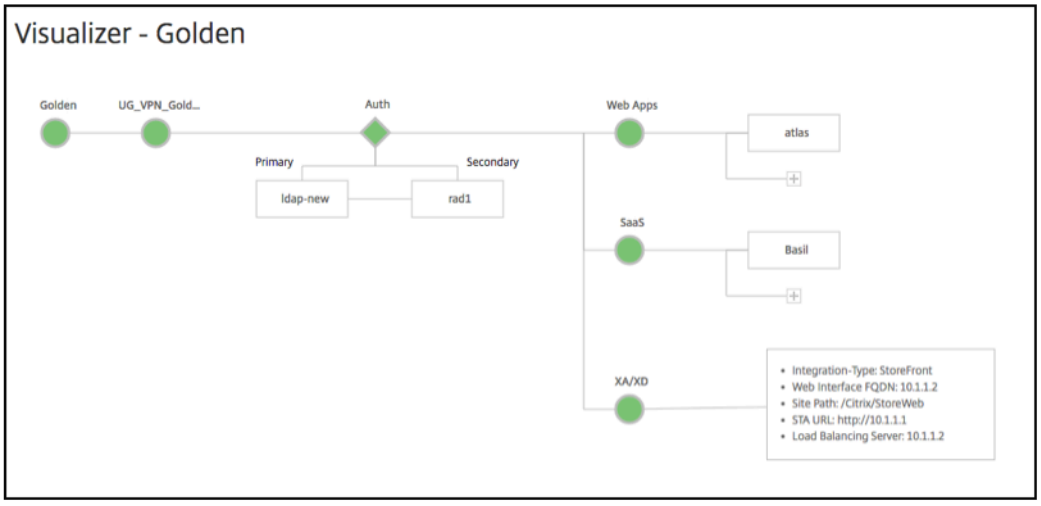
1. ブックマークリンクの [名前] を入力します。
2. VPN URL が表すアプリケーションのタイプを選択します。指定できる値は以下のとおりです:
   - イントラネットアプリケーション
   - クライアントレスアクセス
   - SaaS
   - この NetScaler ADC で事前構成されたアプリケーション
3. このチェックボックスをオンにすると、このアプリケーションに Unified Gateway URL からアクセスできるようになります。
4. ブックマークリンクの URL を入力します。
5. アイコン URL から、アイコンファイルを取得するファイルを選択します。最大長 = 255
6. [続行] ボタンをクリックします。
7. [完了] をクリックします。
8. [続行] をクリックします。
9. [完了] をクリックします。

GUI 構成

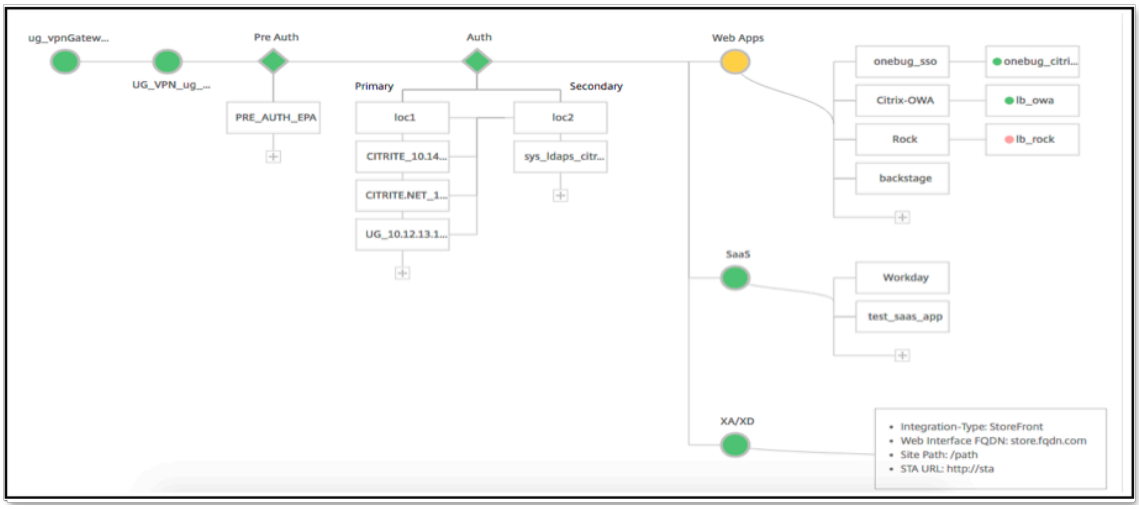
1. メニューから [Unified Gateway] を選択します。
2. [**Unified Gateway** ビジュアライザ] アイコンをクリックして、設定された Gateway インスタンスにアクセスします。



Unified Gateway ビジュアライザは、次の図に示すようなフロー図のように見えます。



Unified Gateway ビジュアライザには、PreAuth、`Auth`、および [アプリケーション] 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、`pre-auth` だけが Unified Gateway ビジュアライザに表示されます。



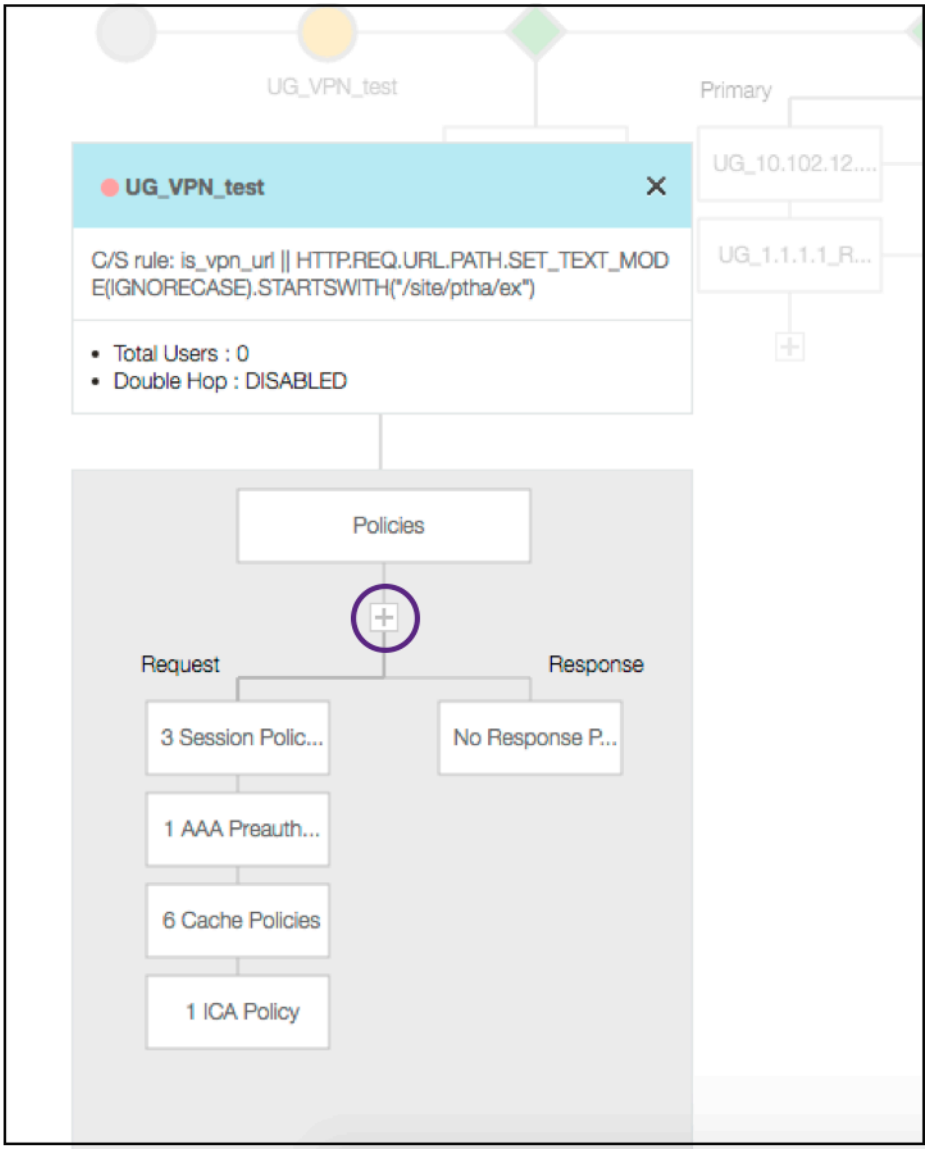
Unified Gateway ビジュアライザは、負荷分散および VPN 仮想サーバの状態を示すために色分けスキームを使用します。

色	説明
赤	は、サーバーがダウンしていることを意味します。
灰色	WebApps/Citrix Virtual Apps が構成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正常であることを意味します。
オレンジ	は、負荷分散仮想サーバサービスのいずれかを意味します。はダウンしていますが、それでも正常に機能しています。

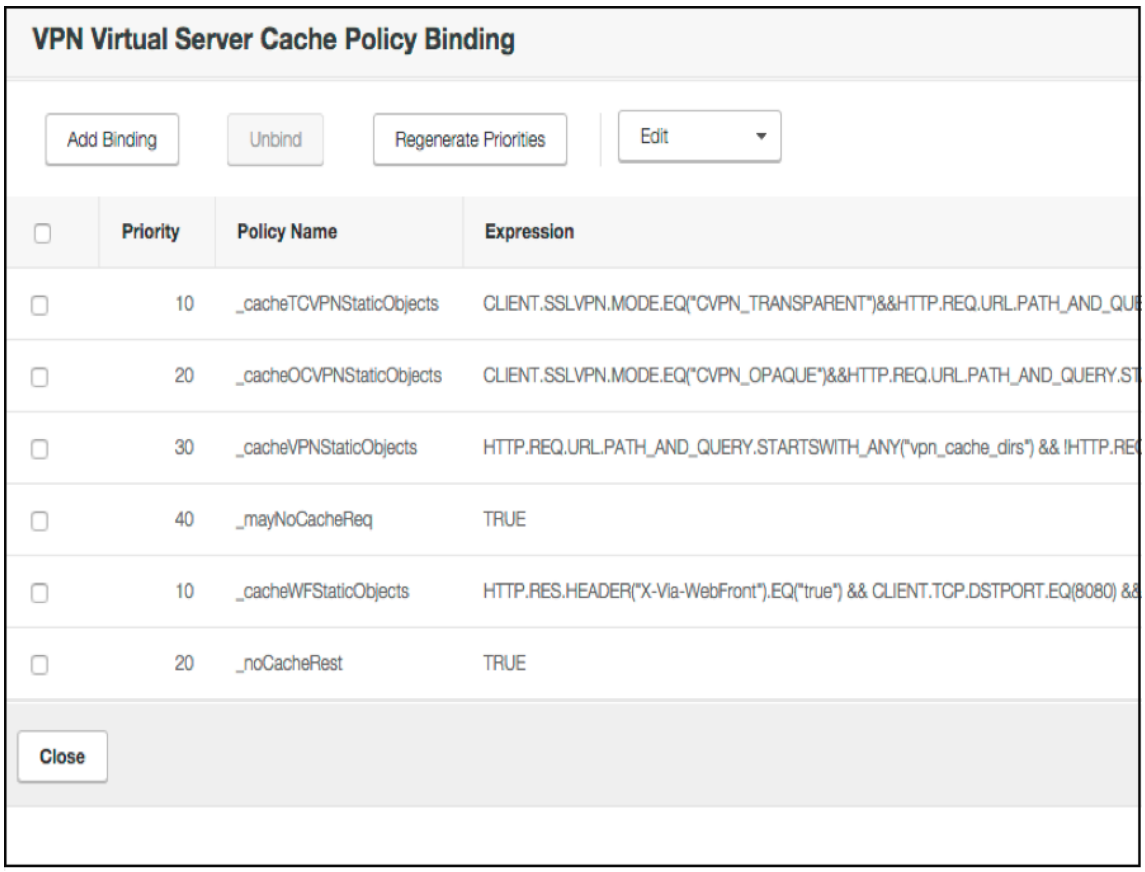
VPN 仮想サーバーの詳細

VPN 仮想サーバーの詳細を取得するには、[**VPN** 仮想サーバー] 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。

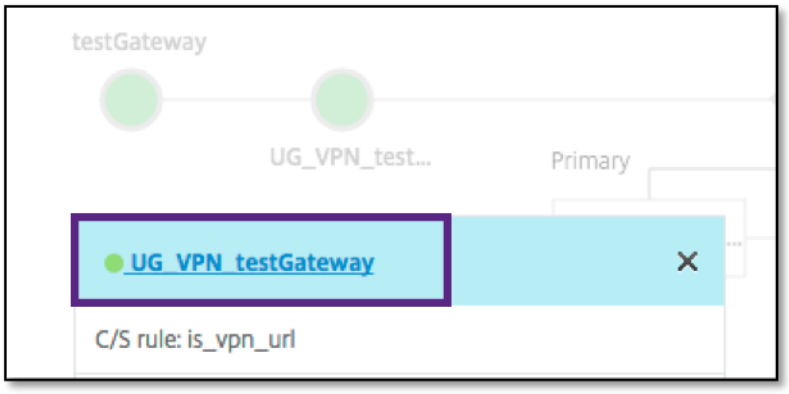
1. (+) アイコンをクリックして、VPN エンティティにポリシーを追加します。



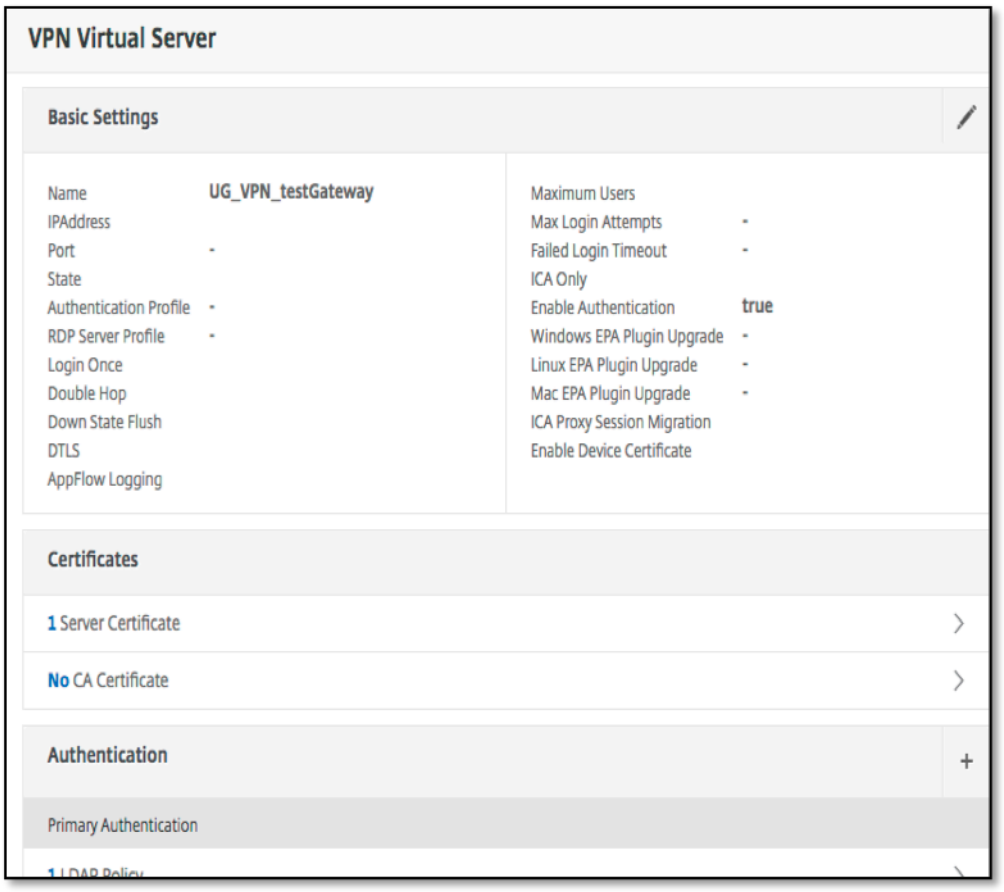
2. 目的のノードをクリックすると、設定済みのポリシーの詳細が表示されます。



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説明する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。



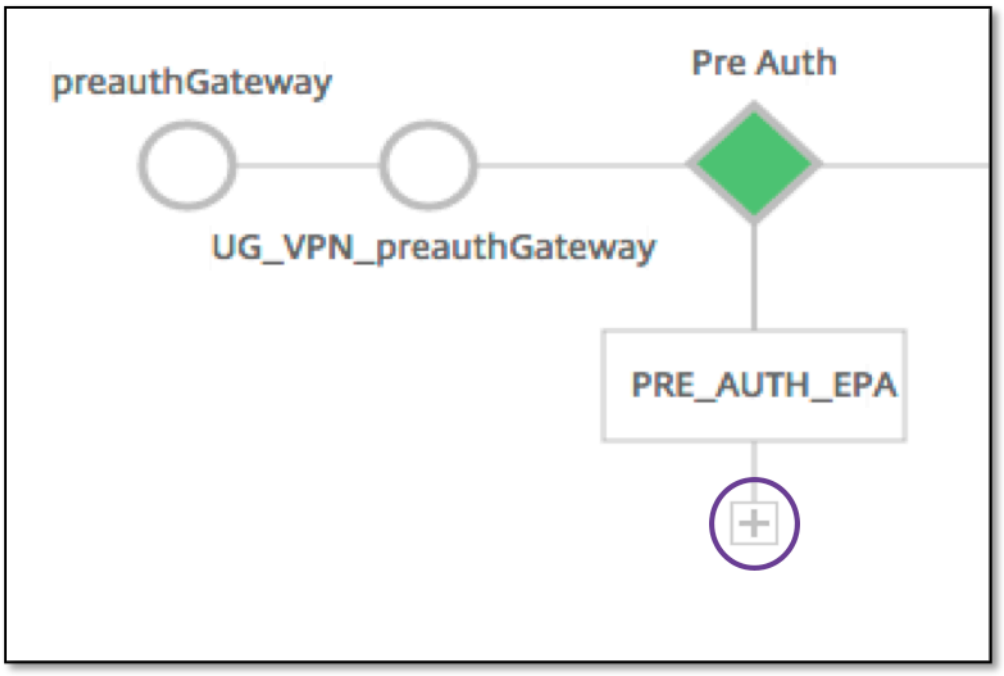
VPN サーバーの詳細はここに示されています。



The Pre Auth Block

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 Visualizer は`Pre Auth`ブロックを表示します。`Pre Auth`ブロックにはポリシーが表示され、事前認証ポリシーを VPN に追加するオプションが提供されます。

1. [**+**] をクリックして`preauth`ポリシーを追加します。

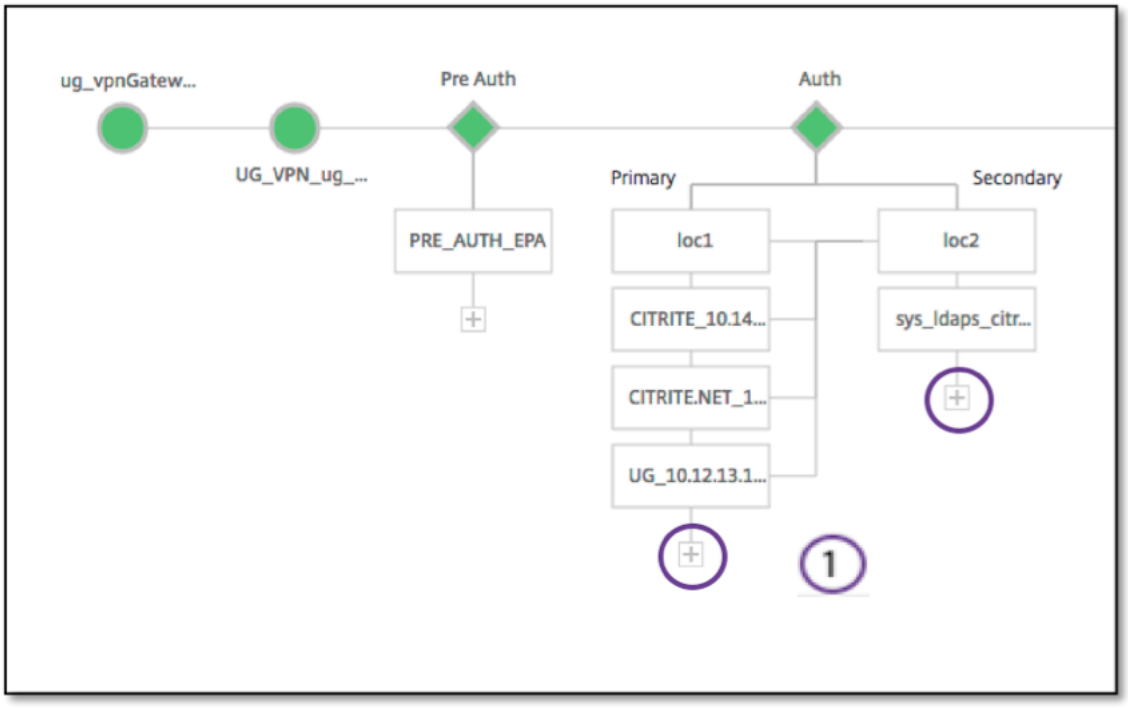


事前認証ポリシーが関連付けられていなければ、このブロックはビューから隠されます。

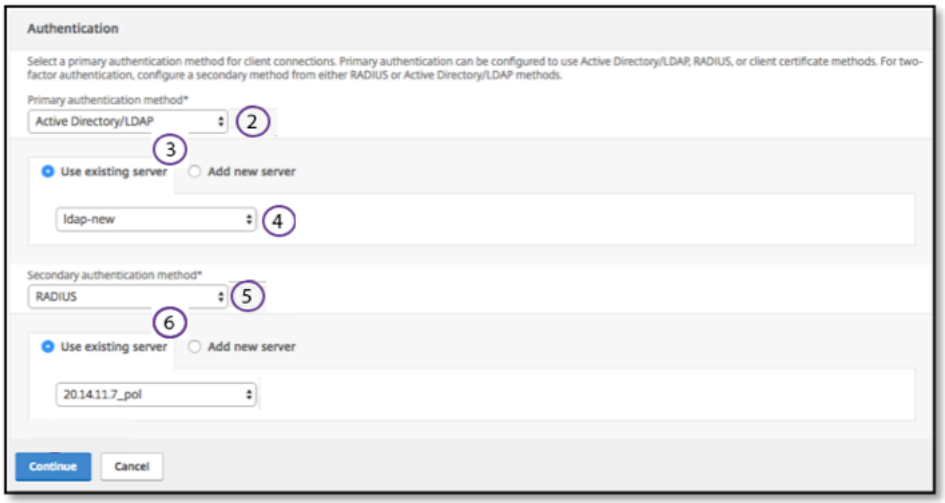
The Auth Block

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ブロックは、ポリシーを追加するオプションを提供します。

1. [プライマリ] リストの [**+**] をクリックしてプライマリ認証バインディングを追加するか、[セカンダリ] リストの [+] をクリックしてセカンダリ認証バインディングを追加します。

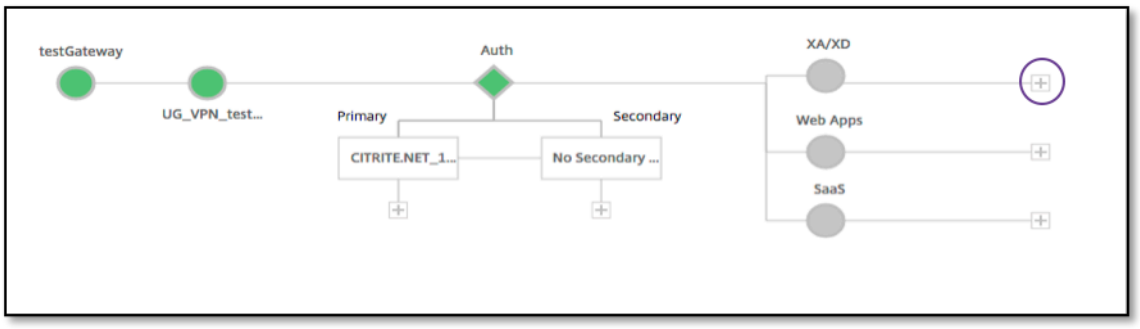


2. [プライマリ認証方法] メニューからオプションを選択します。
3. ラジオボタンを選択して、** 既存のサーバまたは新しいサーバを追加するかどうかを指定します ** 。
4. [**LDAP** ポリシー名] メニューからオプションを選択します。
5. [セカンダリ認証方法] メニューから [**RADIUS**] を選択します。
6. ラジオボタンを選択して、既存のサーバを使用するか、新しいサーバを追加するかを指定します。
7. [続行] をクリックします。



StoreFront の追加

1. XA/XD の近くにある [**+**] をクリックすると、「XA/XD」アプリを追加します。



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、次のフィールドに入力します。必須の情報を必要とするフィールドは、* で示されます。

** フィールド **	** 説明 **
–	–
StoreFront FQDN*	StoreFront サーバーの完全修飾ドメイン名を入力します。最大長:255 文字。例://storefront.xendt.net
サイトパス *	StoreFront ですでに構成されている Web サイトの Receiver へのパスを入力します。
`Single Sign-on Domain`*	ユーザー認証のデフォルトドメインを入力します
ストア名 *	StoreFront モニター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。StoreFront モニターに適用されます。最大長:31
Secure Ticket Authority Server	*Secure Ticket Authority URL* を入力します。通常は *Delivery Controller* 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 *	Unified Gateway 展開用のパブリック向け IP アドレスを入力します。

2. [続行] をクリックします。

SaaS を追加する

1. [**+**] をクリックして SaaS アプリを追加します。[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。必須情報を必要とするフィールドには、* が付いています。

フィールド	説明
名前 *	ブックマーク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。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 NetScaler ADC 上の事前構成済みアプリケーション
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。
ファイルを選択	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 を入力します。最大長 = 255

ウェブアプリの追加

1. [**+**] をクリックして Web アプリを追加します。[Web アプリの追加] ページに移動します。Web アプリケーションを構成するには、次のフィールドに入力します。必須情報を必要とするフィールドには、* が付いています。

フィールド	説明
名前 *	ブックマーク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。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 NetScaler ADC 上の事前構成済みアプリケーション
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。
ファイルを選択	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 URL を介して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負荷分散サーバーの詳細にアクセスできます。

(+) をクリックすると新しいポリシーを追加できます。また、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。

ロードバランサー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。新しいサービスをロードバランサーに追加できます。

ロードバランサの詳細については、ポップアップのタイトルがクリック可能で、負荷分散仮想サーバーの詳細ページに表示されます。

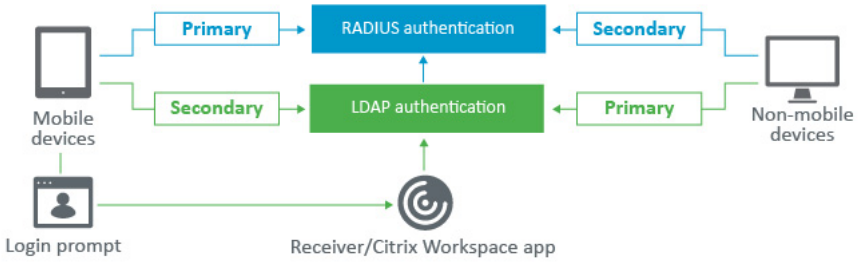
モバイル/タブレットデバイスで **RADIUS** および **LDAP** 認証を使用するように **NetScaler Gateway** を構成する

April 1, 2024

このセクションでは、モバイルデバイス/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 NetScaler Gateway アプライアンスを構成する方法について説明します。

の項で説明した設定でも、他のすべての接続で LDAP を最初に使用し、次に 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場合は、LDAP を最初に設定し、2 番目の資格情報として RADIUS を配置します。管理者の観点から見ると、モバイル以外の構成とは別の構成です。



モバイルデバイス/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 NetScaler 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。

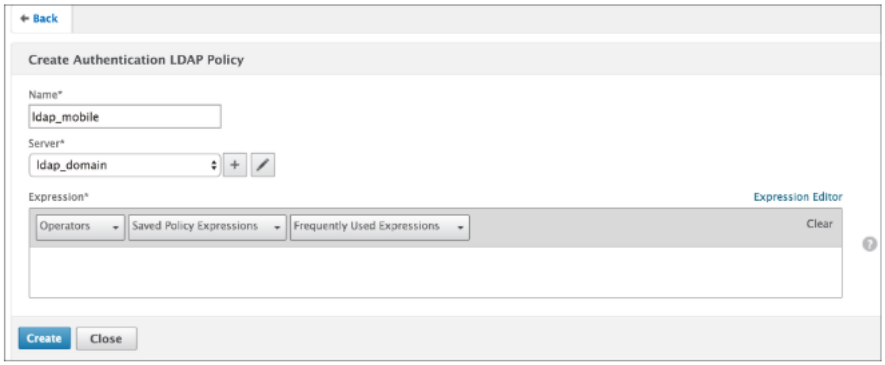
1. 構成ユーティリティで、[**NetScaler Gateway**] **>** [ポリシー] [認証] の順に選択し、モバイルデバイスおよび非モバイルデバイス用の LDAP および RSA の認証ポリシーを作成します。これは、ユーザが RADIUS 認証をバイパスできる論理条件を回避するために必要です。
2. LDAP の [サーバ] タブの下にある [追加] オプションをクリックした後、LDAP サーバの詳細を入力します。
3. 必要な LDAP サーバを選択して、モバイルデバイスの LDAP ポリシーを作成します。

   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:

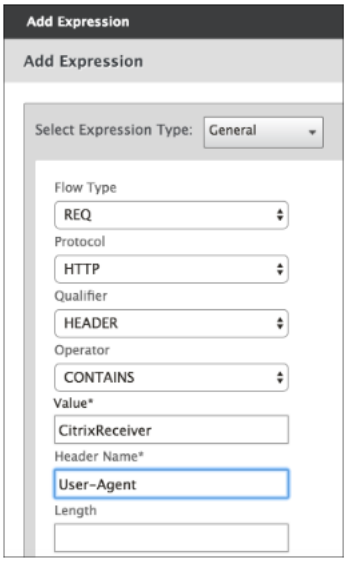
   ```
   1 REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
   ```

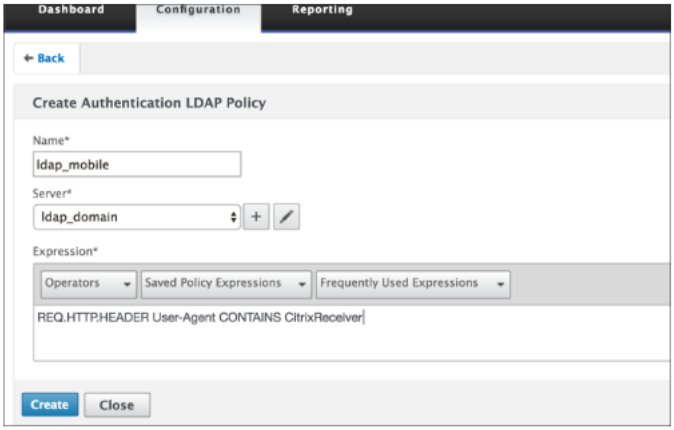
   対応する拡張式は以下のとおりです。

   ```
   1 HTTP.REQ.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:

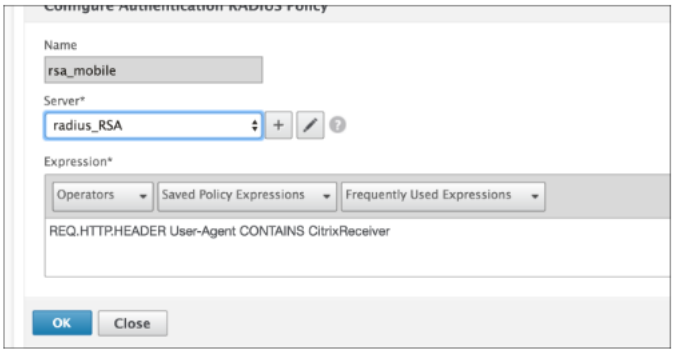




5. モバイルデバイス用の RADIUS ポリシーと RADIUS サーバを作成します。

   - [**NetScaler Gateway**] > [ポリシー] > [認証] > [**RADIUS**] の順に選択します。「サーバー」タブの「追加」をクリックします。
   - 必要な詳細を追加します。RADIUS 認証のデフォルトポートは 1812 です。

- 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:

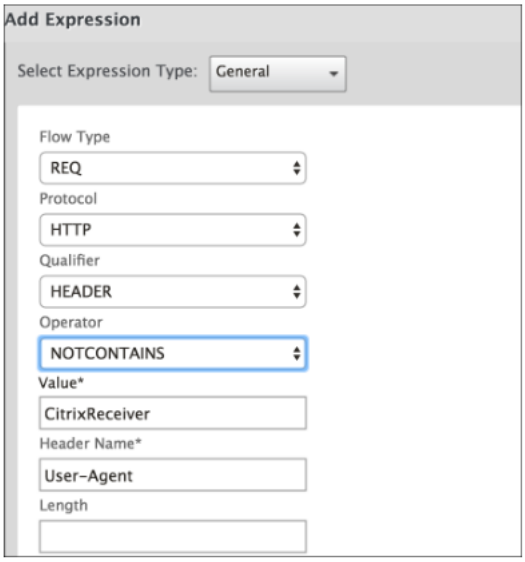


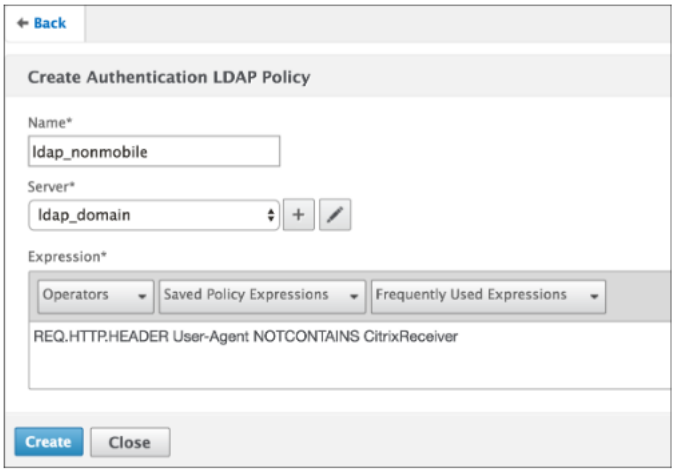
6. 同じ手順に従って、モバイルデバイス以外の LDAP ポリシーを作成します。このポリシーを非モバイルデバイスのみにバインドするには、次の式を使用します:

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

対応する拡張式は以下のとおりです。

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

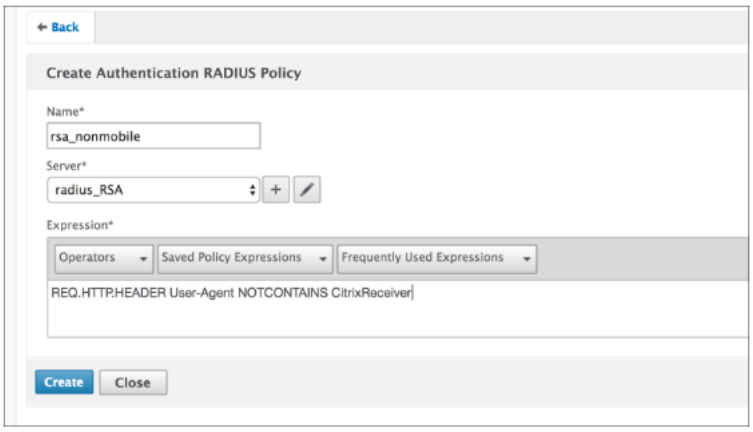


7. モバイルデバイス以外の RADIUS ポリシーを作成します。このポリシーを非モバイルデバイスのみにバインドするには、次の式を使用します:

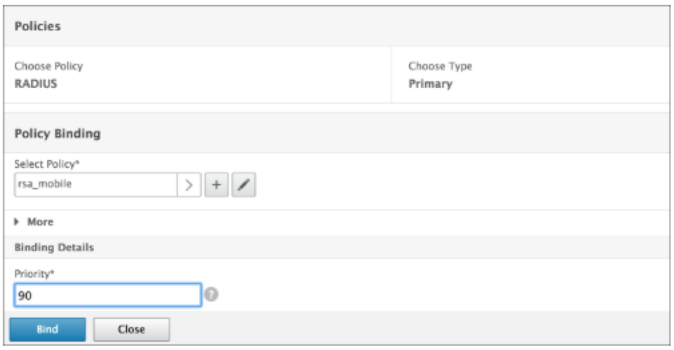
```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

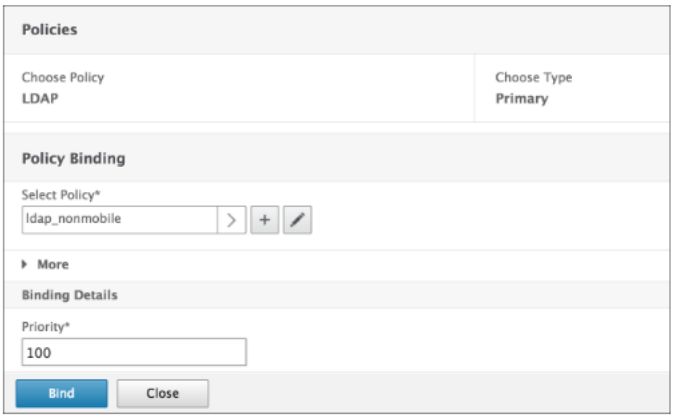
対応する拡張式は以下のとおりです。

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

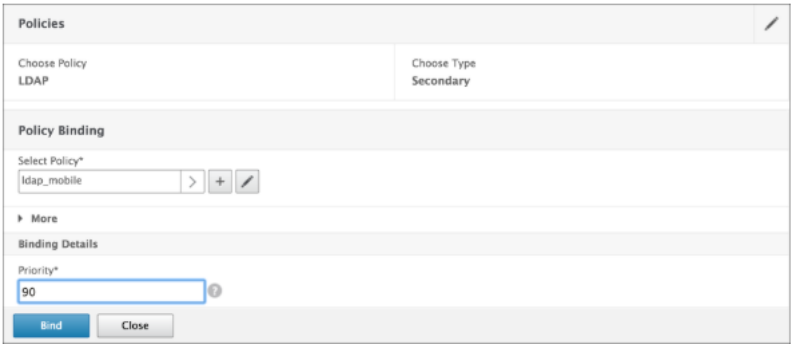



8. NetScaler Gateway 仮想サーバーの［プロパティ］に移動し、［認証］タブをクリックします。[プライマリ認証ポリシー] で、RSA_Mobile ポリシーを最優先として、LDAP_NonMobile ポリシーをセカンダリプライオリティとして追加します:





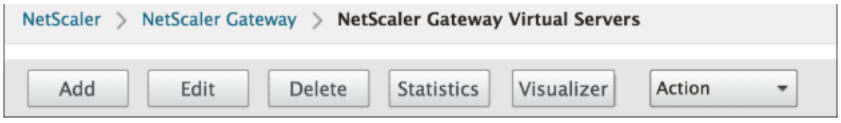
9. セカンダリ認証ポリシーで、LDAP_Mobile ポリシーを最優先として追加し、次に RSA_NonMobile ポリシーをセカンダリプライオリティとして追加します。

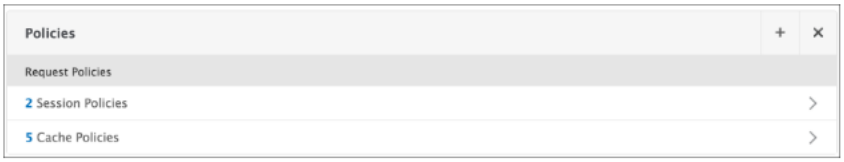


> セッションポリシーには、正しいシングルサインオン資格情報インデックスが必要です。つまり、LDAP 資格情報である必要があります。モバイルデバイスの場合、[セッションプロファイル] **>** **[**クライアントエクスペリエンス] の [資格情報インデックス] を [セカンダリ] に設定する必要があります。これは LDAP です。

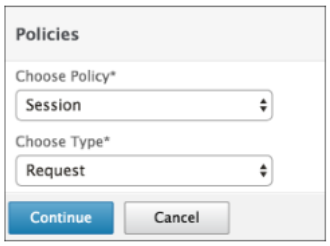
したがって、モバイルデバイス用と非モバイルデバイス用の 2 つのセッションポリシーが必要です。

- モバイルデバイスの場合、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のように表示されます。
  セッションポリシーを作成するには、目的の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:





- メニューから [セッション] オプションを選択します。



- 目的のセッションポリシー名を入力し、[+] をクリックしてプロファイルを作成します。モバイルデバイスの場合、[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。

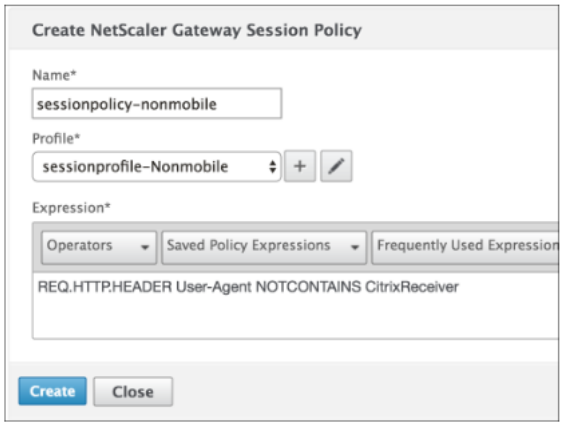
- モバイルデバイス以外の場合も、同じ手順に従います。[セッションプロファイル] **>** **[** クライアントエクスペリエンス] の資格情報インデックスは、LDAP である [プライマリ] に設定する必要があります。

式を次のように変更する必要があります。

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

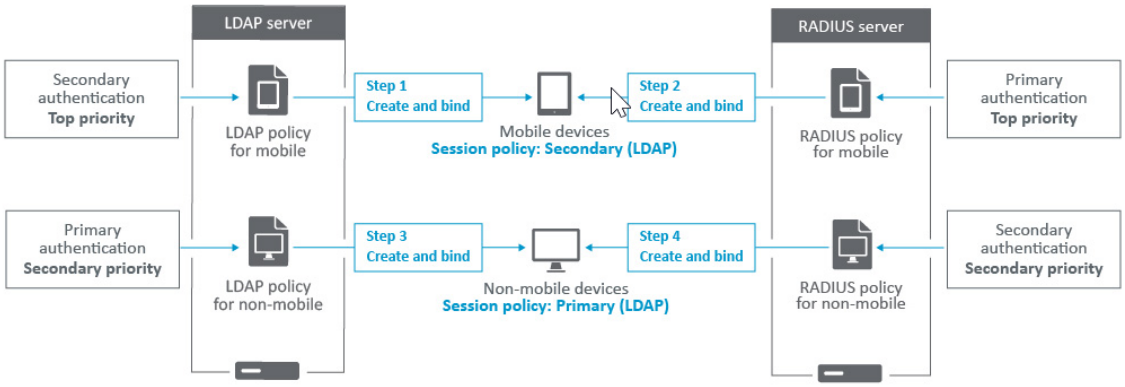
対応する拡張式は以下のとおりです。

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```



- モバイル以外のユーザーのプロファイルを作成するには、[+ 記号] をクリックします。

10. 次の図は、必要な仮想サーバの下にあるポリシーとプロファイルを示します。
11. また、StoreFront では、NetScaler 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。



1 つの Active Directory y グループのメンバーに対する NetScaler Gateway へのアクセスを制限する

April 1, 2024

NetScaler Gateway は、ログオンアクセスを制限する 2 つの方法をサポートしています。

- LDAP 検索フィルター-LDAP 検索フィルター（Active Directory グループメンバーシップなど）に一致するユーザー名のみが NetScaler Gateway にログオンできます。
- NetScaler Gateway セッションポリシーまたはプロファイルでのログオンを許可するグループ-この方法では、複数の Active Directory グループがサポートされます。詳しくは、https://support.citrix.com/article/CTX125797を参照してください。

この資料では、LDAP 検索フィルタ方式について説明します。

概要

ユーザーが NetScaler Gateway 仮想サーバーのログオンページで資格情報を入力し、Enter キーを押すと、アプライアンスはまず Active Directory（LDAP）でユーザー名を検索します。LDAP 検索フィルタが LDAP ポリシーまたはサーバで定義されていない場合、アプライアンスはすべての Active Directory ユーザ名を検索します。一致が見つかると、アプライアンスはユーザーの完全な識別名（DN）をプルし、ユーザーの DN とパスワードを使用して Active Directory への認証を行います。

LDAP 検索フィルタが定義されている場合は、LDAP 検索フィルタに一致するユーザ名のみが検索され、ユーザ名の一致が検索されます。たとえば、LDAP 検索フィルタが Active Directory グループのメンバーのみを検索するように構成されている場合、ユーザーが入力したユーザー名は、グループのメンバーと一致する必要があります。

前提条件

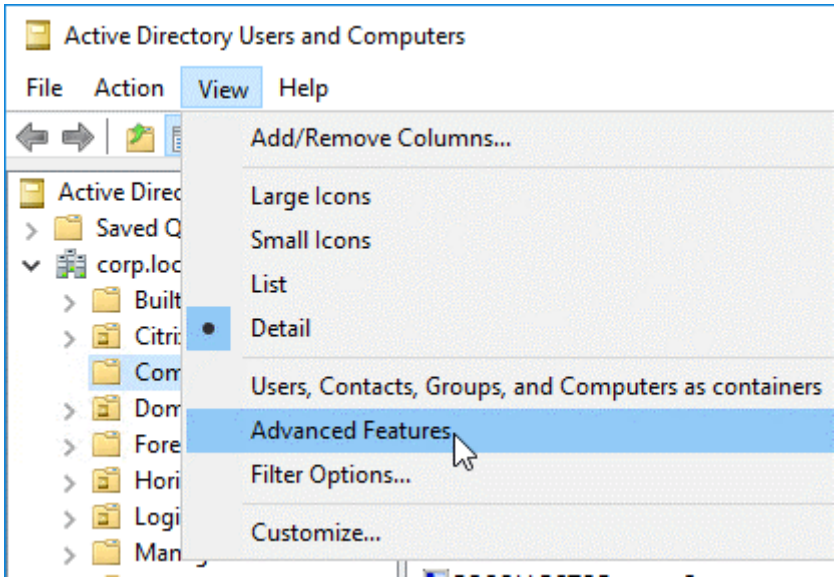
NetScaler Gateway 仮想サーバーは、LDAP 認証用に構成されている必要があります。

1 つの Active Directory グループのメンバーに対して LDAP 検索フィルタを構成する手順

1. アクセス許可を持つ Active Directory グループを特定し、その完全な識別名を取得します。

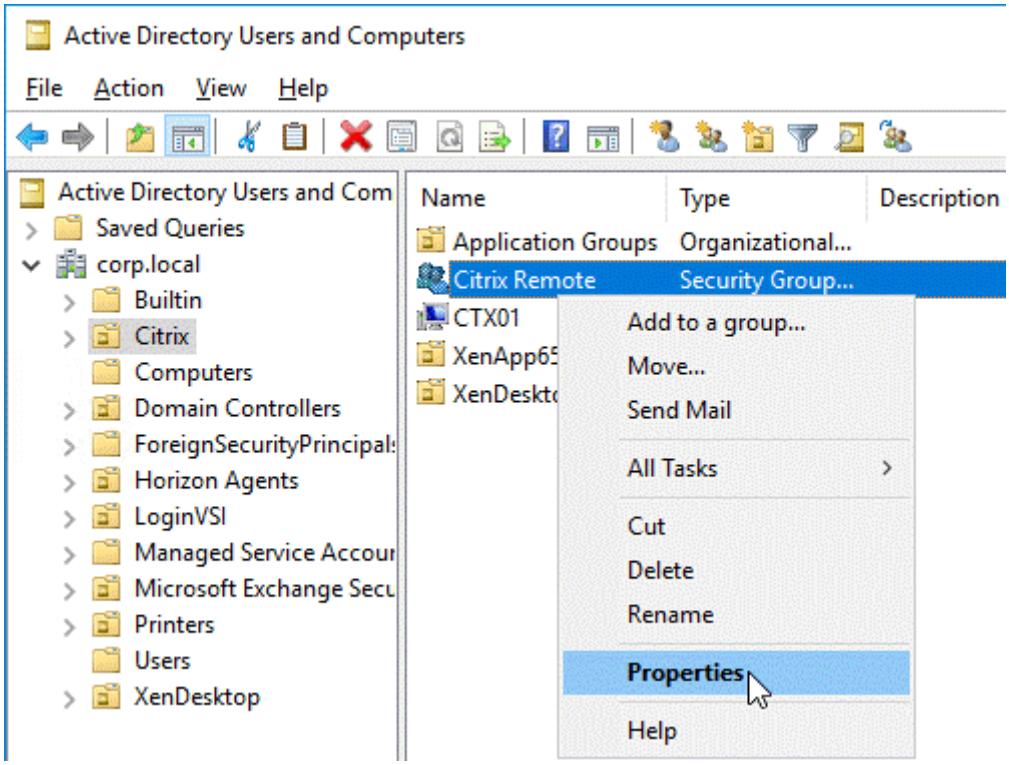
   グループの完全な識別名を取得する簡単な方法は、Active Directory ユーザーとコンピュータを使用することです。

2. [Active Directory ユーザーとコンピュータ] で、[表示] メニューの [高度な機能] を有効にします。

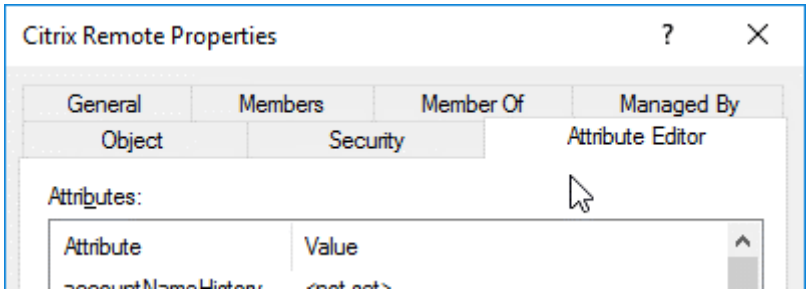


3. ツリーでグループオブジェクトを参照し、右クリックして、[プロパティ] をクリックします。

   注**:** 「検索」(**Find**) は使用できません。代わりに、ツリー内を移動してオブジェクトを見つける必要があります。

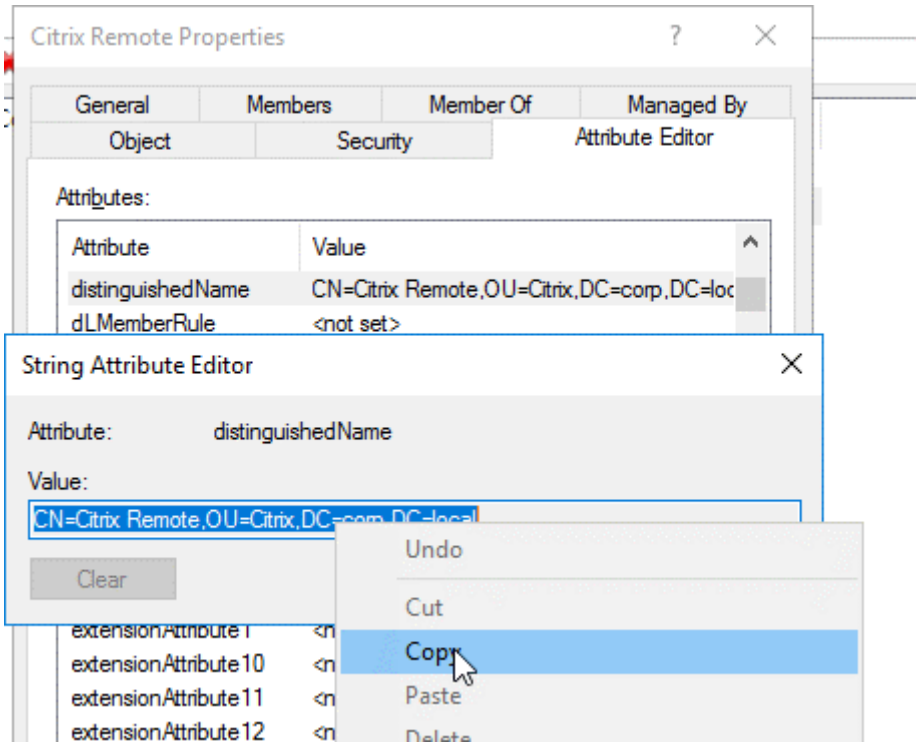


4. 右側で、属性エディタ **(Attribute Editor)** タブに切り替えます。

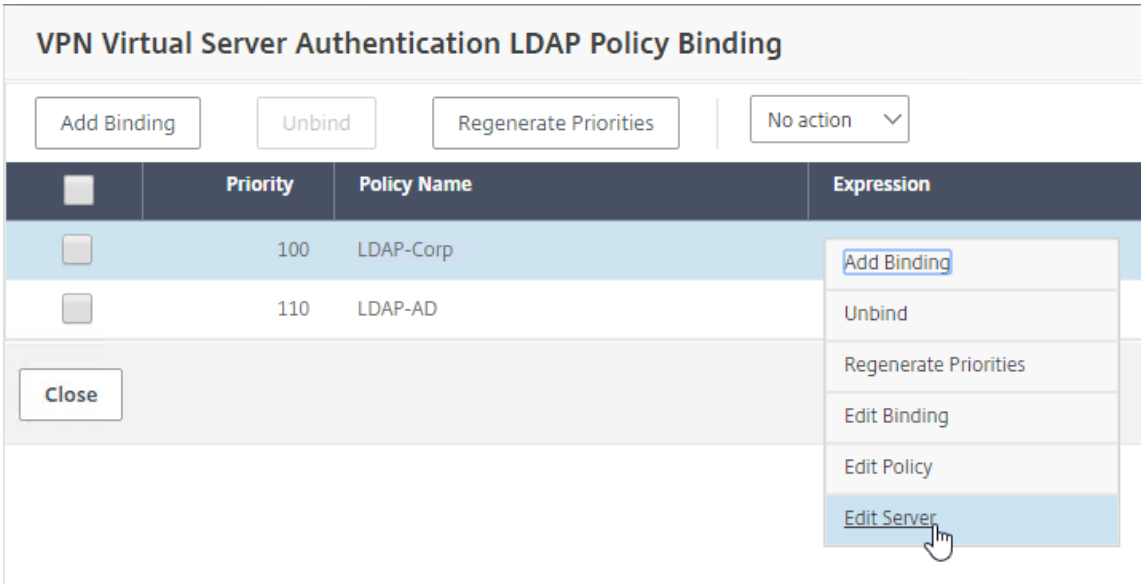


このタブは、高度な機能が有効になっていて、検索機能を使用していない場合にのみ表示されます。

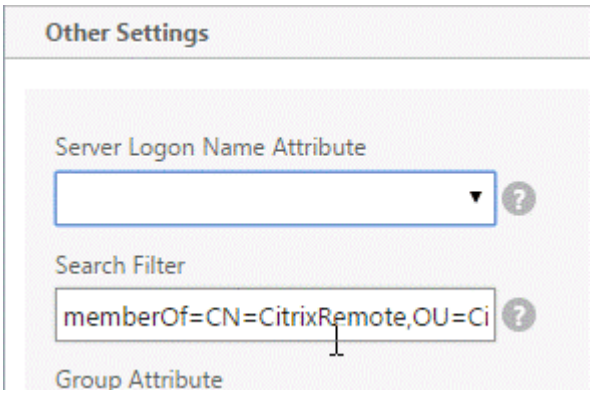
5. [**DinguishedName**] まで下にスクロールし、ダブルクリックして、クリップボードにコピーします。



6. NetScaler Gateway GUI で、[**NetScaler Gateway**] **>** [仮想サーバー] に移動します。
7. 既存の NetScaler Gateway 仮想サーバーを選択し、[編集] をクリックします。
8. [基本認証] セクションで、[**LDAP** ポリシー] をクリックします。
9. 既存の LDAP ポリシーを右クリックし、[サーバの編集] をクリックします。



10. [その他の設定] セクションの **[**検索フィルタ] フィールドに **memberOf=** と入力し、等号 (=) の後に Active Directory グループの識別名を貼り付けます。



検索フィルターの例は次のとおりです。
memberOf=CN=Citrix リモート、OU=Citrix 、DC=Corp、
DC= ローカル注：デフォルトでは、NetScaler は Active Directory グループの直接のメンバーであるユーザー名のみを検索します。ネストされたグループを検索する場合は、Microsoft OID⊠ を LDAP 検索フィルタに追加します。OID は memberOf と = の間に挿入されます。

例： memberof: 1.2.840.113556.1.4.1941: =CN=Citrix Remote、OU=Citrix、DC=Corp、DC=Local

11. [**OK**] をクリックします。

高可用性の使用

February 1, 2024

2 つの NetScaler Gateway アプライアンスの高可用性展開は、あらゆるトランザクションで中断のない操作を提供できます。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付けてサーバを管理し、セカンダリノードがプライマリを監視します。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。

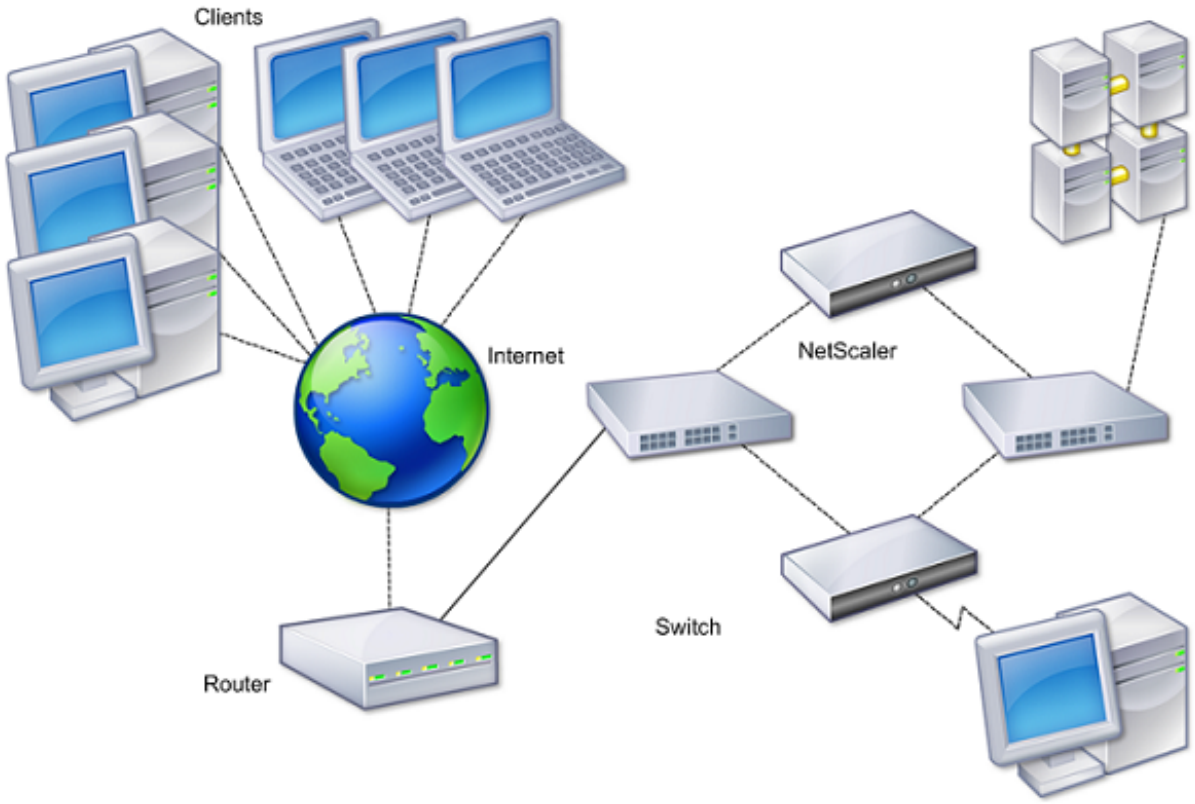
セカンダリノードは、プライマリノードが接続を受け付けているかどうかを判断するために、定期的なメッセージ（ハートビートメッセージまたはヘルスチェックとも呼ばれます）を送信してプライマリを監視します。ヘルスチェックが失敗した場合、セカンダリノードは指定された期間接続を再試行し、その後、プライマリノードが正常に機能していないと判断します。次に、セカンダリノードがプライマリ（フェールオーバーと呼ばれるプロセス）を引き継ぎます。

フェイルオーバー後、すべてのクライアントは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パーシステンスを有効にすると、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。ロギングパーシステンスを有効にするには、ログサーバーの設定で log.conf ファイルに両方のシステムのエントリが含まれている必要があります。

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：高可用性構成の NetScaler 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. 両方のノードを同じサブネットに配置して、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はない状況を回避します。
6. NetScaler Gateway gratuitous 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、異なるサブネットに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

February 1, 2024

高可用性ペアで NetScaler Gateway を構成すると、セカンダリ NetScaler Gateway は、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定期的なメッセージを送信して、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することにより、最初のアプライアンスを監視します。ヘルスチェックが失敗した場合、セカンダリ NetScaler 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、指定され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 NetScaler Gateway がプライマリ NetScaler Gateway を引き継ぎます。これはフェールオーバーと呼ばれます。

次のポートは、NetScaler Gateway アプライアンス間の高可用性に関する情報を交換するために使用されます。

- UDP ポート 3003 は、間隔のステータスを通信するための hello パケットの交換に使用されます。
- TCP ポート 3010 は、高可用性設定の同期に使用されます。
- TCP ポート 3011 は、構成設定の同期に使用されます。

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する必要があります。

- 各 NetScaler Gateway アプライアンスは、同じバージョンの NetScaler 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の上部にあります。
- NetScaler Gateway は、2 つのアプライアンス間でパスワードを自動的に同期しません。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 NetScaler Gateway を構成できます。

- プライマリとセカンダリの両方の NetScaler Gateway 上の構成ファイル ns.conf のエントリは、次の例外を除いて一致する必要があります。
  - プライマリおよびセカンダリの NetScaler Gateway アプライアンスは、それぞれ固有のシステム IP アドレスで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 NetScaler Gateway のシステム IP アドレスを構成または変更します。
  - 高可用性ペアでは、NetScaler Gateway ID と関連する IP アドレスが他の NetScaler Gateway を指している必要があります。

    たとえば、AG1 と AG2 という名前の 2 つのアプライアンスがある場合は、AG2 の一意の NetScaler Gateway ID と IP アドレスを使用して AG1 を構成する必要があります。AG1 の一意の NetScaler Gateway ID と IP アドレスを使用して AG2 を構成する必要があります。

    注：各 NetScaler Gateway アプライアンスは、常にノード 0 として識別されます。各アプライアンスを一意のノード ID で構成します。
- 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・インタフェースを直接使用しない方法 (SSL 証明書のインポートや起動スクリプトへの変更など) 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、構成ファイルをもう一方のノードにコピーするか、同じものを作成する必要があります。そのノード上のファイルです。
- 高可用性ペアを設定するときは、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両方のマッピングされた IP アドレスとデフォルトゲートウェイ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。

高可用性の設定の構成

April 1, 2024

高可用性構成を設定するには、2 つのノードを作成します。各ノードは、もう一方の NetScaler Gateway IP アドレスをリモートノードとして定義します。まず、高可用性を構成する 2 つの NetScaler ADC アプライアンスのいずれかにログオンし、ノードを追加できます。他のアプライアンスの NetScaler 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、他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 NetScaler 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。

アプライアンスを設定する前に、高可用性ノードを追加します。このノードは、高可用性ペアの第 1 または第 2 の NetScaler Gateway を表します。高可用性を構成するには、最初にノードを作成し、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ペインで、[システム**] > [**高可用性] を展開します。
2. 詳細ペインの [ノード] タブで、[追加] をクリックします。
3. ［**HA** ノードの作成］ページの［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 NetScaler ADC NSIP アドレスを入力します。NetScaler Gateway 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、[高可用性セットアップに参加するようにリモートシステムを構成する] 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、現在設定しているノードを追加する必要があります。
5. [ダウンしている **HA** モニタインターフェイス**/**チャネルをオフにする**]** を有効にする時にクリックします。
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、[リモートシステムのログオン資格情報] で、[リモートシステムのログイン資格情報がセルフノードと異なる] 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無効または有効にできます。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するため、プライマリノードはセカンダリノードのステータスをチェックできなくなります。ノードを有効にすると、その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ペインで、[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. [高可用性ノードの構成] ダイアログボックスの [高可用性ステータス] で、[有効 (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ペインで、[システム**] > [**高可用性] を展開します。
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 Configure Node**] 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を変更する

April 1, 2024

他の NetScaler Gateway アプライアンスと通信するには、各アプライアンスには、NetScaler Gateway での認証方法など、他のアプライアンスの知識が必要です。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 NetScaler Gateway には 1 つの RPC ノードが存在し、他の NetScaler 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を格納します。別の NetScaler Gateway と接続する NetScaler Gateway は、RPC ノード内のパスワードをチェックします。

NetScaler Gateway では、高可用性ペアの両方のアプライアンスで RPC ノードのパスワードが必要です。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。プライマリアプライアンスはセカンダリ RPC ノードのパスワードを認識している必要があり、セカンダリアプライアンスはプライマリ RPC ノードのパスワードを認識している必要があります。最初は、各 NetScaler Gateway は同じ RPC ノードパスワードで構成されます。セキュリティを強化するには、デフォルトの 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、ノードを追加するとき、またはグローバルサーバー負荷分散 (GSLB) サイトを追加するとき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保護する必要があります。[**Secure**] チェックボックスをオンにして、RPC ノードのパスワードを構成するときに、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てセキュアな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. [ソース **IP** アドレス］に、他の NetScaler 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. 「セキュア」をクリックし、「**OK**」をクリックします。

> 注:
>
> [セキュア（Secure）] 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 ノードに送信される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設定

February 1, 2024

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 NetScaler Gateway 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ペインで、[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。

通信間隔の設定

February 1, 2024

NetScaler Gateway を高可用性ペアとして構成すると、セカンダリ NetScaler Gateway が特定の間隔（ミリ秒（ミリ秒）でリッスンするように構成できます。これらのインターバルは、hello インターバル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い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 間隔を設定する場合は、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の値は 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 **NetScaler 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ペインで、[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の操作を行います。
    - 「Hello 間隔 (msec)」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。デフォルトの設定は 3 秒です。

NetScaler Gateway アプライアンスの同期

April 1, 2024

高可用性ペアでの NetScaler 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に変更を加え、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。同期はポート 3010 を使用します。

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。

同期を無効にできます。これにより、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 NetScaler Gateway がその構成をプライマリ NetScaler Gateway と同期しないようにできます。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ペインで、[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、次のいずれかを実行します。
   - 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設定を取得する] 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設定を取得する] 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。ステータスバーに、ノード構成が成功したことを示すメッセージが表示されます。

アプライアンス間で同期を強制するには

自動同期に加えて、NetScaler Gateway は、高可用性ペアの 2 つのノード間の強制同期をサポートします。

プライマリとセカンダリの両方の NetScaler Gateway アプライアンス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、NetScaler Gateway は警告を表示します。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ペインで、[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の設定ファイルの同期

April 1, 2024

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設定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

- Mode

  実行する同期のタイプ。次の説明では、オプションを指定するコマンドライン引数を、かっこで囲んで説明します。

- ライセンスと **rc.conf (**すべて**)** 以外のすべて。システム構成、NetScaler 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、およびアプリケーションファイアウォール 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 (bookmarks)。すべての NetScaler Gateway 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 (all_plus_misc)** を含むすべて。システム構成、NetScaler 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 NetScaler 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］メニューで、適切な同期の種類（［ライセンスと rc.conf 以外のすべて］など）を選択し、［**OK**］をクリックします。

コマンド伝播の設定

April 1, 2024

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自動的に伝達され、セカンダリノードで実行されます。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。コマンドの伝播では、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、コマンドの伝播を有効または無効にできます。プライマリノードでコマンドの伝播を無効にすると、コマンドはセカンダリノードに伝播されません。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: 伝播を再度有効にした後は、同期を強制することを忘れないでください。

注：伝播を無効にしているときに同期が発生した場合、伝播の無効化が有効にな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ペインで、[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:
    - 高可用性伝播を無効にするには、[プライマリノードが設定をセカンダリに伝播する] チェックボックスをオフにします。
    - 高可用性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播する] 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

February 1, 2024

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示します。

- ネットワーク接続はアクティブではありません。コマンドの伝達が失敗した場合は、プライマリとセカンダリの NetScaler Gateway アプライアンス間のネットワーク接続を確認します。
- セカンダリ NetScaler Gateway にリソースがありません。コマンドの実行がプライマリ NetScaler Gateway で成功したが、セカンダリ NetScaler Gateway への伝達に失敗した場合は、セカンダリ NetScaler Gateway でコマンドを直接実行してエラーメッセージを表示します。このエラーは、コマンドで必要なリソースがプライマリ NetScaler Gateway に存在し、セカンダリ NetScaler Gateway では使用できないために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していることを確認します。

  たとえば、すべてのセキュアソケットレイヤー（SSL）証明書が各 NetScaler 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 NetScaler 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。

フェイルセーフモードを構成する

February 1, 2024

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失敗したときに、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がアクティブになり、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、各ノードで個別に構成します。

次の表に、フェイルセーフのケースをいくつか示します。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	フェイルセーフ対応の高可用性動作	説明
NOT_UP (最後に失敗した)	NOT_UP (最初に失敗した)	A (二次)、B (二次)	A (プライマリ)、B (セカンダリ)	両方のノードが次々に障害が発生した場合、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 (最初に失敗した)	NOT_UP (最後に失敗した)	A (二次)、B (二次)	A (セカンダリ)、B (プライマリ)	両方のノードが次々に障害が発生した場合、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。
上へ	上へ	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。
上へ	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)	セカンダリノードだけに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。

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	フェイルセーフ対応の高可用性動作	説明
NOT_UP	上へ	A (セカンダリ)、B (プライマリ)	A (セカンダリ)、B (プライマリ)	プライマリだけに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 (STAYSECONDARY)	A (二次)、B (二次)	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ペインで、[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［フェールセーフモード］で、［両方のノードが正常でない場合でもプライマリノードを 1 つ維持する］を選択し、［OK］をクリックします。

仮想 **MAC** アドレスの設定

February 1, 2024

仮想 MAC アドレスは、高可用性セットアップのプライマリおよびセカンダリ NetScaler Gateway アプライアンスで共有されます。

高可用性セットアップでは、プライマリ NetScaler 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。このプロトコルは、これらの 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 テーブルは、フローティング IP アドレスとプライマリ NetScaler 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 NetScaler Gateway が新しいプライマリ NetScaler Gateway として引き継ぎます。次に、gratuitous Address Resolution Protocol（GARP; 無償アドレス解決プロトコル）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、NetScaler Gateway によって生成された GARP メッセージを受け入れません。その結果、一部の外部デバイスは、古いプライマリ NetScaler Gateway によってアドバタイズされた古い IP から MAC へのマッピングを保持します。この状況では、サイトが利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 NetScaler 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 NetScaler Gateway アプライアンスが同じ MAC アドレスを持つことを意味します。その結果、フェイルオーバーが発生しても、セカンダリ NetScaler Gateway の MAC アドレスは変更されず、外部デバイスの 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。高可用性セットアップでは、ユーザ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。汎用仮想 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、それを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 進数表現です。1 ～254 の範囲の 255 個の仮想ルータ 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

February 1, 2024

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 IPv4 パケットはすべて、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、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 アドレスは 00:00:5 e: 00:01:\ <VRID\ > の形式になります。たとえば、値が 60 の VRID を作成し、それをインターフェイスにバインドすると、生成される仮想 MAC アドレスは 00:00:5 e: 00:01:3 c になります。ここで、3c は VRID の 16 進数表現です。1 ～255 の値で 255 個の VRIDs を作成できます。

IPv4 仮想 MAC アドレスの作成または変更

April 1, 2024

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 アドレスの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。可能な値:1 ～255

- `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. [システム**] > [**ネットワーク] に移動し、[**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、その仮想 MAC アドレスが構成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 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. [システム**] > [**ネットワーク**]** に移動し、[**VMAC**] をクリックします。
2. 詳細ペインで項目を選択し、[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、NetScaler 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できますが、NetScaler Gateway で MAC アドレスは構成したままにしておきます。

1. [システム**] > [**ネットワーク] に移動し、[**VMAC**] をクリックします。
2. 詳細ウィンドウで、アイテムを選択し、[開く] をクリックします。
3. [構成済みのインターフェイス] 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

February 1, 2024

NetScaler Gateway は、IPv6 パケットの仮想 MAC アドレスをサポートしています。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 用の仮想 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

February 1, 2024

IPv6 仮想 MAC アドレスに IPv6 仮想ルータ ID を割り当てて、IPv6 仮想 MAC アドレスを作成します。次に、仮想 MAC アドレスをインターフェイスにバインドします。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 アドレスの設定を確認するには、仮想 MAC アドレスおよび仮想 MAC アドレスにバインドされたインターフェイスを表示および確認します。

IPv6 用の仮想 MAC アドレスを設定するためのパラメータ

- `Virtual Router ID`

  仮想 MAC アドレスを識別する仮想ルータ ID。可能な値:1 ～255

- `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 アドレスを構成するには

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、[追加（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 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] をクリックします。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ー 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

February 1, 2024

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ある場合です。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ある 2 つの NetScaler 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での高可用性設定の違いの一覧を示します。

リンク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 NetScaler Gateway 機能は、クロスネットワークの高可用性構成で役立ちます。これらの機能は、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、各 NetScaler Gateway で使用されるヘルスチェックプロセスもカバーします。

独立したネットワーク構成の仕組み

NetScaler Gateway アプライアンスは、2 つの異なるネットワーク上の R3 および R4 と呼ばれる異なるルーター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、接続がアクティブであることを確認する一定の間隔で発生する信号です。この構成を拡張して、任意の数のインターフェイスを含む展開に対応できます。

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に存在する場合、セカンダリ NetScaler 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 NetScaler 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 NetScaler Gateway アプライアンスが異なる構成可能なパラメーターを持つこのタイプの構成は、独立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。

次の表に、独立したネットワーク構成の構成可能なパラメーターをまとめ、各 NetScaler Gateway でパラメーターを設定する方法を示します。

設定可能なパラメータ	動作
IP アドレス	NetScaler Gateway 固有。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	NetScaler Gateway 固有。そのアプライアンスでのみアクティブです。
ルート	NetScaler Gateway 固有。そのアプライアンスでのみアクティブです。リンク負荷分散（LLB）ルートはフローティングです。
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	NetScaler Gateway 固有。そのアプライアンスでのみアクティブです。セカンダリ NetScaler 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。
リバースネットワークアドレス変換 (NAT)	NetScaler Gateway 固有。NAT IP アドレスがフローティングであるため、仮想 IP アドレスを持つリバース NAT。

> 注:
>
> INC モードの IPSET は、パブリック IP アドレスでサポートされます。詳細については、「Azure ロードバランサーを使用した NetScaler ADC 高可用性フロントエンド IP 検証済みリファレンスデザイン」を参照してください。

リモートノードの追加

April 1, 2024

高可用性ペアの 2 つのノードが異なるサブネットに存在する場合、各ノードのネットワーク構成は異なる必要があります。したがって、2 つの独立したシステムを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ときは、接続されていない、またはトラフィックに使用されていない各インターフェイスの高可用性モニタを無効にする必要があります。

独立ネットワークコンピューティングモード用の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ペインで、[システム**] > [**高可用性] を展開します。
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 NetScaler 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クリックします。
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、[高可用性セットアップに参加するようにリモートシステムを構成する] 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 モニタのクリアが有効になります。
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場合にクリックします。
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ペインで、[システム**] > [**高可用性] を展開します。
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]、[はい] の順にクリックします。

ルートモニタの設定

February 1, 2024

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、高可用性ステート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て、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。

NetScaler 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、静的ルートの監視対象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

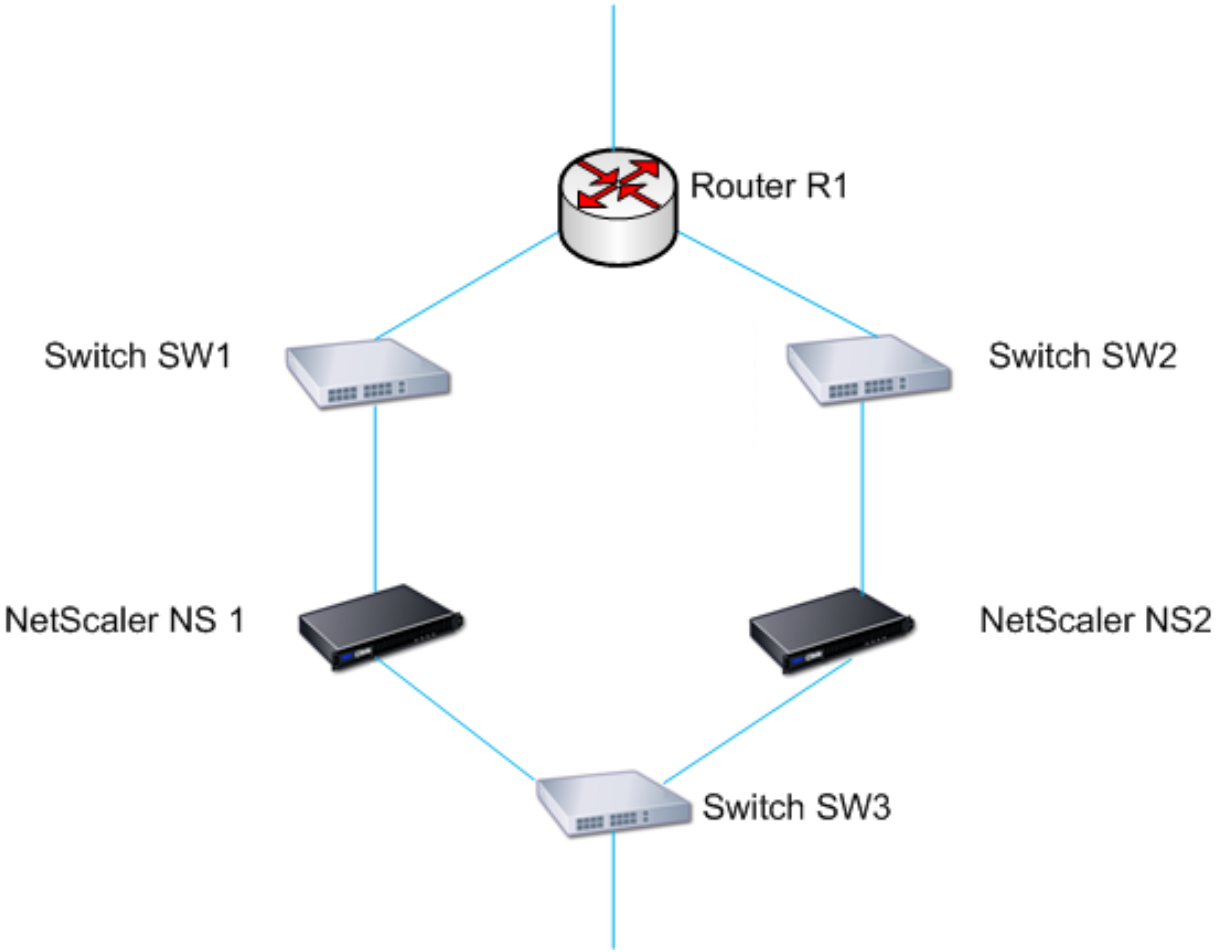
ィックルートは、到達不能なスタティックルートを内部ルーティングテーブルから削除します。スタティックルートでモニタ対象スタティックルートを無効にすると、到達不能なスタティックルートが内部ルーティングテーブルに残り、ルートモニタの目的が失われます。

ルートモニタは、[独立ネットワーク構成] 設定を有効または無効にした場合にサポートされます。次の表に、高可用性セットアップのルートモニタと、独立ネットワーク構成を有効または無効にした場合の動作を示します。

無効になっている独立ネットワーク構成モードで高可用性のルートモニタ	有効な独立ネットワーク構成モードで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達され、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。
NetScaler 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かかわらず、ルートモニターの状態を常に UP として表示します。	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、NetScaler Gateway アプライアンスは、ルートモニターの状態をダウンとして表示します。
ルートモニターは、次の場合にルートの監視を開始し、NetScaler Gateway が動的ルートを学習できるようにします。これには最大 180 秒かかる場合があります：再起動、フェイルオーバー、v6 ルートの route6 コマンドの設定、`msr` v4 ルートのルート有効/無効コマンド、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ゲートウェイ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、NetScaler 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、および SW3 を持つツーアームトポロジの高可用性セットアップで、独立した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 に到達できないときはいつでも、高可用性セットアップをフェールオーバーします。各ノードにルートモニタ（それぞれ RM1 と RM2）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、NS1 の内部ルーティングテーブルを監視し、ルータ R1 のルートエントリの存在を確認します。NS1 と NS2 は、スイッチ 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し、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 と NS2 は、スイッチ SW3 を介してハートビートメッセージを定期的に交換します。
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。R1 へのルートが NS1 と NS2 の両方からダウンしている場合、アプライアンスの 1 つが R1 に到達して接続を復元できるようになるまで、180 秒ごとにフェイルオーバーが実行されます。

ルートモニタの追加または削除

February 1, 2024

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ある場合、NetScaler 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 NetScaler 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 NetScaler 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ペインで、[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 [ルートモニター] タブで、[アクション]、[構成] の順にクリックします。
3. ［ルートモニターの指定］の［ネットワーク］に、他の NetScaler 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]、[OK] の順にクリックします。

この手順が完了すると、ルートモニターは NetScaler Gateway にバインドされます。

注：ルートモニターが NetScaler 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の状態は、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ペインで、[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] タブで、[操作]、[構成] の順にクリックします。
3. ［構成済みルートモニタ］でモニタを選択し、［削除］、［OK］の順にクリックします。

リンク冗長性の設定

February 1, 2024

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、他の機能しているインターフェイスを持つ NetScaler Gateway の 1 つのネットワークインターフェイスの障害によるフェールオーバーを防ぎます。プライマリ NetScaler 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と、2 つのインターフェイスをフェー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 NetScaler

Gateway のすべてのインターフェイスが機能しない限り、単一のリンクの障害によってセカンダリ NetScaler Gateway へのフェールオーバーが発生するの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保持します。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 NetScaler Gateway で有効で高可用性の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、フェールオーバーがトリガーされるためです。

リンク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ペインで、[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. [インターフェイス] 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ついてステップ 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ペインで、[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、NetScaler 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ペインで、[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を理解する

February 1, 2024

次のイベントは、高可用性構成でフェールオーバーを引き起こす可能性があります。

1. セカンダリノードが、セカンダリノードで設定されたデッドインターバルを超える期間、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。デッドインターバルの設定の詳細については、「通信インターバルの設定」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。
    - ネットワーク構成に問題があると、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障害が発生し、その原因でフリーズする（ハング）、リブートしたり、ハートビートパケットの処理や転送を停止したりします。
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、ネットワークインターフェイス上で 3 秒間ハートビートパケットを受信しません。
4. プライマリノードで、フェールオーバーインターフェイスセット (FIS) またはリンクアグリゲーション (LA) チャネルの一部ではなく、高可用性モニタ (HAMON) が有効になっているネットワークインターフェイスは失敗します。インターフェイスは有効になっていますが、DOWN 状態になります。
5. プライマリノードでは、FIS 内のすべてのインターフェイスで障害が発生します。インターフェイスは有効になっていますが、DOWN 状態になります。
6. プライマリノードで、HAMON が有効になっている LA チャネルで障害が発生します。インターフェイスは有効になっていますが、DOWN 状態になります。
7. プライマリノードでは、すべてのインターフェイスで障害が発生します。この場合、フェールオーバーは HAMON の設定に関係なく発生します。
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 の設定に関係なく発生します。
9. いずれかのノードで force failover コマンドを発行して、フェールオーバーを強制します。
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がダウンします。

ノードからのフェイルオーバーの強制

February 1, 2024

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は、フェールオーバーを強制的に実行できます。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強制的にフェールオーバーできます。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。強制フェイ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できます。

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のままになるように設定されます。

NetScaler Gateway アプライアンスは、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、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、続行する前に確認を要求します。

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

February 1, 2024

プライマリノードでフェー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。強制フェールオーバーは、プライマリノードがセカンダリノードが稼働中であ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ダウンしている場合、force failover コマンドは次のエラーメッセージを返します。「ピアの状態が無効なため、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。`"Operation not possible now. Please wait for system to stabilize before retrying."`

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ヘルス状態が良好で、ノードがセカンダリ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。

セカンダリノードがプライマリノードになれない場合、またはセカンダリノードがセカンダリのままになるように設定されている場合（STAYSECONDARY オプションを使用）、ノードは次のエラーメッセージを表示します。「自分の状態が無効であるため、操作はできません。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ペインで、[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 [強制フェイルオーバー] 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のままにする

February 1, 2024

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 NetScaler Gateway を強制的にプライマリのままにすることができます。この設定は、スタンドアロンの NetScaler 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 NetScaler 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保つには

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、[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、[プライマリに維持する] をクリックし、[OK] をクリックします。

この設定は、次のコマンドを使用することによってのみクリアできます。

```
clear configuration full
```

次のコマンドは、NetScaler Gateway の高可用性構成を変更しません。

```
clear configuration basic
```

```
clear configuration extended
```

セカンダリノードを強制的にセカンダリに維持する

April 1, 2024

高可用性セットアップでは、プライマリ NetScaler Gateway の状態に関係なく、セカンダリ NetScaler Gateway を強制的にセカンダリのままにすることができます。NetScaler Gateway をセカンダリのままにするように構成すると、プライマリ NetScaler Gateway に障害が発生してもセカンダリのままになります。

たとえば、既存の高可用性セットアップで、プライマリ NetScaler 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された時間がかかるとします。アップグレード中、プライマリ NetScaler Gateway が使用できなくなる場合がありますが、セカンダリ NetScaler Gateway が引き継ぐことは望ましくありません。プライマリ NetScaler Gateway で障害が検出された場合でも、セカンダリ NetScaler Gateway のままにします。

高可用性ペアの NetScaler 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、高可用性ステートマシンの移行には参加しません。NetScaler Gateway のステータスは、構成ユーティリティの［ノード］タブで確認できます。

この設定は、スタンドアロンとセカンダリ NetScaler Gateway の両方で機能します。

高可用性ノードを設定すると、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 NetScaler Gateway のみに影響します。

セカンダリノードを強制的にセカンダリに保つには

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、[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、[セカンダリを維持 (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。

NetScaler 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ペインで、[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、プライマリノードとして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

February 1, 2024

NetScaler Gateway をクラスタ構成に展開して、VPN クライアントトラフィックに高スループット、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、NetScaler Gateway アプライアンスまたは仮想マシンのグループが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。NetScaler Gateway クラスターは、クラスターノードとして構成された最小 2 台および最大 32 台の NetScaler Gateway アプライアンスまたは仮想マシンを使用して構築できます。

NetScaler Gateway クラスターの構成を開始する前に、NetScaler ADC クラスタリングのドキュメントをお読みください。こ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。

- 使用する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、クラスタリングの仕組みを参照してください。
- 展開を計画し、環境に関連する可能性のあ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。

NetScaler Gateway クラスターは、スポッティングされた VIP 構成タイプの NetScaler ADC クラスターとして動作します。

> 重要:
>
> **XenApp** および **XenDesktop** ウィザードはクラスタリングをサポートしていないため、**GUI >** ナビゲーショ

> ンペイン **NetScaler 製品との統合セクションに XenApp および XenDesktop ウィザードは表示されません ** 。

クラスタリングの構成

April 1, 2024

NetScaler Gateway クラスタリングをセットアップする際の主なタスクは次のとおりです。

1. 構成コーディネーターとなる NetScaler Gateway アプライアンスまたは仮想マシンを決定し、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まだ存在しない場合）。
2. NetScaler 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 NetScaler 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。

NetScaler 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 **NetScaler Gateway** クラスターインスタンスを作成するには

展開の詳細を整理したら、構成コーディネーターである NetScaler 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設定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。クラスタで使用される既存の設定は、クラスタの確立後に構成コーディネータに再適用できます。

1. NSIP アドレスで NetScaler 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、[クラスタ] サブノードの順に展開します。
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) クラスターインスタンス ID を入力します。クラスターインスタンス ID 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。クラスタ IP アドレスは、クラスタの構成コーディネータの IP アドレスで、クラスタの管理 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、クラスタノード間の通信に使用するこの NetScaler Gateway インターフェイスです。
5. ［Create］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が表示されたら、[はい] をクリックします。
7. ノードが起動し、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 認証情報を変更します。RPC ノードの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のを待ちます。使用可能になったら、手順 4 (2) で設定したクラスタ IP アドレスで構成ユーティリティにログオンします。

注: [システム情報] 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ーとして報告されます。これにより、ベースクラスターインスタンスが動作中であることを確認します。

構成コーディネーターのローカルノードは、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。

NetScaler 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 NetScaler Gateway ノードをクラスターに追加できます。

NetScaler Gateway システムをクラスターに追加するには、構成ユーティリティを使用して、クラスターノードの作成およびクラスターへの参加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、NetScaler Gateway 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やり直す必要がある場合に、NetScaler Gateway 構成を繰り返す必要はありません。

1. クラスター IP アドレスで NetScaler 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、次に「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. [クラスタノード] 詳細ペインで、[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 NetScaler 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 NetScaler Gateway システムの NetScaler 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の資格情報] ウィンドウで、ローカルの承認済みユーザーのパスワードを入力します。
9. [**Create**] 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、リモートの NetScaler Gateway のウォームリブートを実行します。
11. ノードが起動し、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 認証情報を変更します。RPC ノードの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 NetScaler Gateway システムごとに、手順 4 から 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、必要なすべてのノードがリストされるまで、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. クラスター IP アドレスで NetScaler 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、次に「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. 詳細ペインで、[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. NetScaler Gateway 仮想サーバーの種類をサポートするには、［スティッキー］オプションを選択します。
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した。構成ユーティリティのこの領域を離れる前に、ローカル NetScaler 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します

NetScaler Gateway クラスター構成はスポットタイプであるため、ノードグループにバインドできるノードは 1 つのみです。次の手順は、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、クラスター内の任意のノードをこのバインドに使用できます。

1. [詳細設定] ペインで、[クラスタノード] 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. [クラスタノードの設定] 画面で、[バインド] をクリックします。
4. この NetScaler 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. [挿入] 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。

これで、クラスターにデータが入力され、次のタスクで構成されたとおりに NetScaler Gateway 仮想サーバーを共有する準備が整いました。

NetScaler Gateway 仮想サーバーをクラスターノードグループにバインドする

クラスターが確立されたら、クラスター展開が機能する NetScaler Gateway 構成の構築に進むことができます。構成をクラスターに関連付けるには、NetScaler Gateway 仮想サーバーを作成し、スティッキータイプに設定されて

いる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。仮想サーバーがクラスターノードグループにバインドされたら、NetScaler Gateway の構成を続行できます。

複数の NetScaler Gateway 仮想サーバーが構成されている場合は、それらも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。

注： NetScaler Gateway 仮想サーバーがまだ構成されていない場合は、最初に［システム］**>**［設定］**>**［基本機能の構成］で **NetScaler Gateway** および認証、承認、および監査機能を有効にする必要があります。

1. クラスター IP アドレスで NetScaler 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、次に「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. [ノードグループ] ペインで、目的のノードグループ名を選択し、[編集] 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. ［**Bind**］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、それを選択し、「挿入」、「**OK**」の順にクリックします。
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。NetScaler ADC 仮想サーバーの構成に進みます。最低限必要なのは、仮想サーバーを作成してクラスターノードグループにバインドできるようにすることだけです。
10. ［NetScaler Gateway 仮想サーバー］ボックスの一覧で仮想サーバーが使用可能になったら、それを選択し、［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 NetScaler Gateway 仮想サーバーが構成されている場合は、これと同じ方法でそれらも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。

Unified Gateway

April 1, 2024

Unified Gateway を備えた **NetScaler ADC**：**1** つの **URL**

Unified Gateway を搭載した NetScaler 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に、単一の URL を介したあらゆるアプリケーションへの簡素化された安全なアクセスが可能になります。この単一の URL の背後には、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、および制御を一元的に管理できます。

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/ログアウトの操作性が向上しました。

これを実現するために、Gateway を備えた NetScaler ADC は、NetScaler ADC のコンテンツスイッチング機能と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 を通じて組織のサイトとアプリへのアクセスを提供します。また、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 Secure Access クライアントを搭載した Linux、PC、または Mac システムを使用して、どこにいても Unified Gateway URL に統一的にアクセスできます。

Unified Gateway 展開では、次のカテゴリのアプリケーションへの単一の 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
- NetScaler ADC によって提供される事前構成されたアプリケーション
- Citrix Virtual Apps and Desktops 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 ベースの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、セキュアなエンタープライズネットワーク内に存在するクライアントレスアプリケーションの Unified Gateway は、Outlook Web Access と 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使用する必要がある専用のクライアントソフトウェアを使用せずに、Exchange 電子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、一般にクラウドアプリケーションとも呼ばれ、組織が依存している ShareFile、Salesforce、NetSuite などの外部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、それを提供する SaaS アプリケーションでサポートされています。

一部の組織では、**NetScaler ADC** 負荷分散構成で展開された **NetScaler ADC** サーバーアプリケーションを事前に構成し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。Unified Gateway は、展開用の仮想サーバーが同じ NetScaler ADC Unified Gateway インスタンスまたはアプライアンスに存在する場合、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、Unified 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。

公開された **Citrix Virtual Apps and Desktops** の公開アプリケーションは、Unified Gateway URL を通じて利用可能にすることができます。SmartAccess および SmartControl ポリシーは、オプションで、これらのリソースに対する詳細なポリシーとアクセス制御に適用できます。

Unified Gateway 構成ウィザード

Unified Gateway 展開で NetScaler ADC を構成するための推奨される方法は、Unified 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展開を管理し、その動作を監視できます。

> 注:
>
> Unified Gateway 構成ウィザードでは、システムの初期設定は実行されません。NetScaler Gateway アプライアンスまたは VPX インスタンスは、Unified Gateway を構成する前に基本インストールを完了している必要があります。基本構成を完了するには、「初回セットアップウィザードを使用した NetScaler Gatewayの構成」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設定される Unified Gateway 要素は次のとおりです。

- Unified Gateway プライマリ仮想サーバ
- Unified Gateway 仮想サーバの SSL サーバ証明書
- プライマリ認証および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
- Unified Gateway ポータルを介してアクセスされるユーザアプリケーション

これらの各要素について、構成情報を提供する必要があります。基本的な Unified Gateway 展開では、次の情報が必要です。

- プライマリ Unified Gateway 仮想サーバの場合、展開のパブリック IP アドレスと IP ポート番号。これは、DNS で Unified Gateway URL のホスト名に解決される IP アドレスです。たとえば、Unified Gateway 展開の URL が`https://mycompany.com/`の場合、IP アドレスは mycompany.com に解決される必要があります。

- 展開用の署名付き SSL サーバ証明書。NetScaler 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ている認証システムは、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 認証設定も作成される場合があります。認証サーバの IP アドレスは、関連する管理者クレデンシャルまたはディレクトリ属性とともに指定する必要があります。証明書認証の場合、デバイス証明書属性と CA 証明書を指定する必要があります。

- ポータル・テーマが選択されている場合があります。カスタマイズまたはブランド化されたポータル設計が必要な場合は、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では、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使用する Web アプリケーションの場合、ユーティリティは、他のオプションの SAML パラメータとともにアサーションコンシューマサービス URL を収集します。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 Virtual Apps and Desktops の公開リソースを Unified Gateway 展開環境で使用できるようにするには、統合ポイント（StoreFront、Web Interface、または NetScaler ADC 上の Web Interface）を指定する必要があります。この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) サーバーの URL、および統合ポイントのタイプに応じてその他が必要です。

追加の構成管理

代替 SSL 設定やセッションポリシーなど、Unified 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、NetScaler Gateway 構成ユーティリティで必要な設定を管理できます。これらの設定は、Unified 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 仮想サーバで変更できます。

コンテンツスイッチング仮想サーバー

これは、展開のメイン IP アドレスと URL の背後にある NetScaler ADC 構成エンティティです。SSL サーバ証明書とパラメータは、この仮想サーバで管理されます。この仮想サーバー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 サーバーの応答と RHI の状態をこの仮想サーバーで変更できます。コンテンツスイッチ仮想サーバーは、[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 [構成] タブにあります。

> 重要:
>
> Unified Gateway 環境をリリース 13.0 ビルド 58.x 以降にアップグレードすると、ゲートウェイまたは VPN 仮想サーバーの前に構成されているコンテンツスイッチング仮想サーバーで DTLS ノブが無効になります。アップグレード後、コンテンツスイッチング仮想サーバーで DTLS ノブを手動で有効にします。設定にウィザードを使用している場合は、DTLS ノブを有効にしないでください。

VPN 仮想サーバー

Unified Gateway 構成のその他すべての VPN パラメータ、プロファイル、およびポリシーバインディングは、メイン認証構成を含め、この仮想サーバで管理されます。このエンティティは、[**NetScaler 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、Unified 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付けられた名前が含まれます。

> 注:
>
> Unified Gateway 展開用に作成された VPN 仮想サーバはアドレス指定できず、0.0.0.0 IP アドレスが割り当てられます。

Unified Gateway に関するよくある質問

April 1, 2024

Unified Gateway とは何ですか

Unified Gateway は、NetScaler 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る）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 Unified Gateway 仮想サーバーにバインドされている仮想サーバーに内部的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（Unified Gateway 仮想サーバに関連付けられた）単一の IP アドレスまたは URL 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、NetScaler Gateway 展開の構成を簡素化できます。

各 Unified Gateway 仮想サーバーは、フォーメーションの一部として、ゼロ個以上の負荷分散仮想サーバーとともに、1 つの NetScaler Gateway 仮想サーバーをフロントエンドにすることができます。Unified Gateway は、NetScaler ADC アプライアンスのコンテンツスイッチング機能を使用して機能します。

Unified Gateway の展開の例をいくつか示します:

- Unified Gateway 仮想サーバー-> [1 台の NetScaler Gateway 仮想サーバー]
- Unified Gateway 仮想サーバー-> [1 つの NetScaler Gateway 仮想サーバー、1 つの負荷分散仮想サーバー]
- Unified Gateway 仮想サーバー-> [NetScaler 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-> [NetScaler 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負荷分散サーバーであればどれでもかまいません。

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（Unified Gateway 仮想サーバに関連付けられた）単一の IP アドレスまたは URL を使用して複数のサービスにアクセスできます。管理者にとっての利点は、IP アドレスを解放し、NetScaler Gateway 展開の構成を簡素化できることです。

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ーは、トラフィックを受信し、内部的に適切な仮想サーバーに誘導する仮想サーバーであるため、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ーは、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。その使用方法は **Unified Gateway** とも呼ばれますか

複数の仮想サーバーのトラフィックを受信するためのコンテンツスイッチ仮想サーバーの使用は、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、NetScaler Gateway 仮想サーバーにトラフィックを転送することはできません。

11.0 の拡張により、コンテンツスイッチング仮想サーバーは、NetScaler 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用の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 NetScaler Gateway 仮想サーバーを指定するために使用されます。例:

   ```
   add cs action UG_CSACT_MyUG -targetVserver UG_VPN_MyUG
   ```

   NetScaler Gateway 構成ユーティリティでは、コンテンツスイッチングアクションに新しいオプション「ターゲット仮想サーバー」が追加されました。このオプションは、NetScaler Gateway 仮想サーバーを参照できます。

2. 新しい高度なポリシー式 is_vpn_url を使用して、NetScaler Gateway および認証固有のリクエストを照合できます。

Unified Gateway で現在サポートされていない **NetScaler 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、軽微な問題（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 NetScaler Gateway アクセス方法に対してのみトリガーされ、NetScaler AAA TM アクセスではトリガーされません。NetScaler Gateway 仮想サーバーで認証が行われているにもかかわらず、ユーザーが NetScaler ADC 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。その場合は、認証またはシームレス SSO のいずれかが行われます。

Unified Gateway のライセンス要件は何ですか

Unified Gateway は、アドバンスドライセンスおよびプレミアムライセンスでのみサポートされます。NetScaler Gateway のみのライセンスエディションまたはスタンダード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 **NetScaler 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 NetScaler Gateway 仮想サーバーの場合、NetScaler Gateway 仮想サーバーで IP/ポート/SSL 構成は必要ありません。ただし、RDP プロキシ機能の場合、同じ SSL/TLS サーバー証明書を NetScaler Gateway 仮想サーバーにバインドできます。

NetScaler Gateway 仮想サーバー上にある **SSL/TLS** 証明書を、**Unified Gateway** 仮想サーバーで使用するために再プロビジョニングする必要がありますか

NetScaler Gateway 仮想サーバーに現在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 証明書を自由に再利用し、それらを Unified Gateway 仮想サーバーにバインドできます。

単一の **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 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能力を指します。この制限は、証明書のサブジェクトに FQDN が入力された SSL/TLS サーバ証明書を Unified Gateway が使用する場合に存在します。例:ug.citrix.com

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) 機能を備えた SSL/TLS 構成です。例: auth.citrix.com、auth.citrix.de、auth.citrix.co.uk、auth.citrix.co.jp

単一ホストと複数ホストは、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 Web サイトが一般的にホストされる方法に似ています。単一のホストがある場合は、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場合と同様に、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。

Unified Gateway ではどのような認証メカニズムを使用できますか

NetScaler Gateway と互換性のある既存の認証メカニズムはすべて、Unified Gateway とも互換性があります。

これには、LDAP、RADIUS、SAML、Kerberos、証明書ベースの認証などが含まれます。

アップグレード前に NetScaler Gateway 仮想サーバーで構成されている認証メカニズムは、NetScaler Gateway 仮想サーバーが Unified Gateway 仮想サーバーの背後に配置されたときに自動的に使用されます。アドレス指定不可能な IP アドレス（0.0.0.0）を NetScaler 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。

「**selfAuth**」認証とは何ですか

selfAuth は、それ自体で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 設定には、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 は、Unified Gateway 仮想サーバと同じドメインにないリソースにアクセスするために使用できます。この設定は、ブックマークを構成するときに構成ユーティリティで確認できます。

「**StepUp**」認証」って何ですか

NetScaler AAA TM リソースにアクセスするために、より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 authenticationLevel パラメーターを設定します。例:

```
1 add authentication authnProfile AuthProfile -authnVsName AAATMVserver -
     AuthenticationHost auth.citrix.lab -AuthenticationDomain citrix.lab
     **-**AuthenticationLevel 100
2 <!--NeedCopy-->
```

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 **NetScaler ADC AAA TM** 仮想サーバーでサポートされていますか

はい、サポートされています。

login once/logout once って何ですか

Login Once: VPN ユーザーは、NetScaler AAA TM または NetScaler Gateway 仮想サーバーのいずれかに一度ログインします。それ以降、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。ユーザは再認証される必要はありません。ただし、再認証は、NetScaler AAA TM StepUp などの特殊なケースに対して行われます。

`Logout Once`: 最初の NetScaler ADC AAA TM または NetScaler Gateway セッションが作成された後、そのユーザーの後続の NetScaler ADC AAA TM または NetScaler Gateway セッションを作成するために使用されます。これらのセッションのいずれかがログアウトすると、NetScaler 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。

負荷分散仮想サーバーレベルで **NetScaler ADC AAA TM** 負荷分散仮想サーバー固有の認証バインドを使用して、共通の認証ポリシーを **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を教えてください

Unified Gateway の背後にある NetScaler ADC AAA TM 仮想サーバーに個別の認証ポリシーを指定する必要がある場合は、個別のアドレス指定可能な認証仮想サーバーが必要です（通常の NetScaler ADC AAA TM 構成と同様）。負荷分散仮想サーバーの認証ホスト設定は、この認証仮想サーバーを指し示す必要があります。

バインドされた **NetScaler ADC AAA TM** 仮想サーバーが独自の認証ポリシーを持つように、**Unified Gateway** をどのように構成しますか

このシナリオでは、負荷分散サーバーで、NetScaler AAA TM 仮想サーバーを指すように認証 FQDN オプションを設定する必要があります。NetScaler AAA TM 仮想サーバーは、独立した IP アドレスを持っており、NetScaler 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。

NetScaler AAA TM 認証仮想サーバーは、**Unified Gateway** 仮想サーバーを介して来るユーザーを認証するために必要ですか**?**

なし NetScaler Gateway 仮想サーバーは、NetScaler AAA TM ユーザーも認証します。

NetScaler Gateway 認証ポリシーは、**Unified Gateway** 仮想サーバーまたは **NetScaler Gateway** 仮想サーバーでどこで指定しますか

認証ポリシーは、NetScaler 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ーの背後にある **NetScaler ADC AAA TM** 仮想サーバーで認証を有効にするにはどうすればよいですか

NetScaler 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。

コンテンツスイッチの後ろに **TM** 仮想サーバーを追加する方法 **(**単一の **URL** とマルチホスト**)**

単一の URL に対して NetScaler ADC AAA TM 仮想サーバーを追加することと、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。

仮想サーバーが **Unified Gateway** 仮想サーバーの背後に移動された場合、**NetScaler AAA TM** 負荷分散仮想サーバー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、NetScaler 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の必要性さえあります)。認証ホストを Unified Gateway 仮想サーバーの FQDN を指すようにすることで、NetScaler Gateway 仮想サーバーによって認証が行われることが保証されます。認証ホストに Unified Gateway のコンテンツスイッチングをポイントし、まだ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、認証ホストを独立したアドレス指定可能な認証仮想サーバーを指す場合、バインドされた認証ポリシーが有効になります。

NetScaler AAA TM セッションのセッションポリシーをどのように構成しますか**?**

Unified Gateway で、NetScaler 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、NetScaler AAA TM セッションは NetScaler Gateway セッションポリシーを継承します。認証仮想サーバーが指定されている場合、その仮想サーバーにバインドされた NetScaler ADC AAA TM セッションポリシーが適用されます。

NetScaler 11.0 の **NetScaler Gateway** ポータルの変更点は何ですか**?**

11.0 より前の NetScaler ADC リリースでは、グローバルレベルで単一のポータルのカスタマイズを設定できます。特定の NetScaler ADC アプライアンス内のすべてのゲートウェイ仮想サーバーは、グローバルポータルのカスタマイズを使用します。

NetScaler 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。

NetScaler 11.0 は **NetScaler 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して、新しいポータル・テーマ機能を使用して、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。さまざまな画像をアップロードしたり、配色を設定したり、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、独自のポータル設計で NetScaler Gateway 仮想サーバーをカスタマイズできます。

ポータル・テーマは、**NetScaler ADC** の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、NetScaler ADC の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。

カスタマイズは、**NetScaler 11.0** アップグレードプロセスの一環として移行されますか**?**

なし 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た NetScaler Gateway ポータルページに対する既存のカスタマイズは、NetScaler 11.0 へのアップグレード時に自動的に移行されません。

NetScaler 11.0 のポータルテーマの準備をする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、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、[デフォルト] 設定を割り当てる必要があることです:

1. ［構成］**>**［**NetScaler 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] をクリックし、[**UI** テーマ] リストから [デフォルト] を選択します。

rc.conf または **rc.netscaler** によって呼び出される **NetScaler ADC** インスタンスに保存されているカスタマイズがあります。ポータル・テーマに移動するにはどうすればよいですか

Citrix ナレッジセンターの記事 CTX126206 には 、10.0 ビルド 73.5001.e までの NetScaler ADC 9.3 および 10.0 リリースのこのような構成について詳しく説明しています。NetScaler 10.0 ビルド 10.0 73.5002.e（10.1 および 10.5 を含む）以降、UITHEME CUSTOM パラメータを使用して、再起動後もカスタマイズを保持できるようになりました。カスタマイズが NetScaler ADC ハードドライブに保存されており、これらのカスタマイズを引き続き使用する場合は、11.0 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。ポータルの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**]** で **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、DEFAULT または GREENBUBBBLE 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。

NetScaler 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 **NetScaler 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ファイルは、ディスク上に保存され、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 NetScaler ADC 11.0 カーネルおよびカーネルの一部である他の GUI ファイルと完全に互換性があるとは限りません。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はありません。SSH または WinSCP などのファイル転送ユーティリティを使用して、NetScaler ADC インスタンスからファイルを削除します。

ポータル・テーマは、**NetScaler 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、NetScaler AAA TM 仮想サーバーでサポートされています。

NetScaler Gateway 11.0 の **RDP** プロキシ機能の変更点は何ですか**?**

NetScaler 10.5.e 拡張リリース以降、RDP プロキシに多くの機能強化が加えられました。NetScaler 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

NetScaler 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ド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

NetScaler 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。NetScaler 11.0 では、有効コマンドが追加されました。

```
enable feature rdpproxy
<!--NeedCopy-->
```

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。

RDP プロキシのその他の変更

サーバプロファイルの事前共有キー（PSK）属性が必須になりました。

RDP プロキシ用の既存の NetScaler ADC 10.5.e 構成を NetScaler ADC 11.0 に移行するには、次の詳細を理解し、対処する必要があります。

管理者が既存の RDP プロキシ構成を選択した Unified Gateway 展開に追加する場合は、次の手順を実行します:

- NetScaler 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 フォーメーションの一部である NetScaler Gateway 仮想サーバーにバインドする必要があります。

NetScaler 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 **NetScaler ADC 11.0** にどのように移行しますか

オプション 1：プレミアムライセンスまたはアドバンスドライセンスを使用して、RDP プロキシ構成の既存の NetScaler Gateway 仮想サーバーをそのまま維持します。

オプション 2：RDP プロキシ構成で既存の NetScaler Gateway 仮想サーバーを移動し、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 NetScaler Gateway 仮想サーバーを既存の Standard Edition アプライアンスに追加します。

NetScaler 11.0 リリースを使用して、**RDP** プロキシ構成用に **NetScaler 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 NetScaler Gateway 仮想サーバーを使用する。これには、NetScaler Gateway 仮想サーバーに対して外部から見える IP アドレス/FQDN が 1 つ必要です。このオプションは、NetScaler 10.5.e で利用可能なものです。
2. Unified Gateway 仮想サーバーを使用して、NetScaler Gateway 仮想サーバーをフロントエンドにします。

オプション 2 では、NetScaler Gateway 仮想サーバー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、独自の IP アドレス/FQDN を必要としません。

HDX Insight は **Unified Gateway** と互換性がありますか

NetScaler Gateway を Unified Gateway で展開する場合は、次の条件を満たす必要があります。

- NetScaler 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。
- HDX Insight のレポートを作成するために、NetScaler ADM で AppFlow レコードを生成するには、NetScaler Gateway 仮想サーバーが稼働状態になっている必要があります。

既存の **HDX Insight** 構成を移行するにはどうすればよいですか

移行は必要ありません。NetScaler Gateway 仮想サーバーが Unified Gateway ゲートウェイ仮想サーバーの背後に配置されている場合、NetScaler Gateway 仮想サーバーにバインドされた AppFlow ポリシーが引き継がれます。

NetScaler Gateway 仮想サーバーの NetScaler ADM 上の既存のデータについては、次の 2 つの可能性があります。

- NetScaler 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 Unified Gateway ateway 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、NetScaler Gateway 仮想サーバーからの 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ではありません。

NetScaler Gateway アプライアンスでの **VPN** 構成

April 1, 2024

> 重要**:**
>
> このセクションのスクリーンキャプチャは、次の理由によりグレースケールスキームで維持されます。
>
> - 視覚障害のある読者、特に色覚障害や色覚障害のある読者を支援します。
> - グレースケールイメージの使用は、ユーザーのブラウザやオペレーティングシステムで行われた可能性のあるカラーコーディングのカスタマイズの影響を示さない一般的な形式でイメージを表します。

ユーザーは、次の方法を使用して、NetScaler Gateway を介して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、および ShareFile にユーザーが接続できるようにする Web 向け Citrix Workspace アプリ。
- Secure Hub: ユーザーが iOS および Android デバイスから Secure Mail、WorxWeb、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します。
- Windows、macOS X、または Linux 用の Citrix Secure Access クライアント。
- iOS および Android 向けの NetScaler Gateway アプリ。
- クライアントレスアクセス。ユーザソフトウェアをインストールしなくても、ユーザに必要なアクセス権をユーザに提供します。
- Citrix SD-WAN プラグインとの相互運用性。

ユーザーが Citrix Secure Access クライアントをインストールしてから、Citrix Virtual Apps 6.5 for Windows Server 2008（Feature Pack および Feature Pack 2 を含む）、Citrix Virtual Desktops 7.0 以降から Citrix Workspace アプリをインストールすると、Citrix Workspace アプリは自動的に Citrix Secure Access クライアントを追加します。ユーザーは、Web ブラウザまたは Citrix Workspace アプリから Citrix Secure Access クライアントに接続できます。

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。スマートアクセスの詳細については、「SmartAccess 構成」を参照してください。

NetScaler Gateway は、iOS および Android モバイルデバイス向けの Citrix Endpoint Management 業務用モバイルアプリをサポートしています。NetScaler 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 NetScaler Gateway に接続できる Secure Browse が含まれています。Secure Hub に接続する Android デバイスは、マイクロ VPN トンネルを自動的に確立し、内部ネットワークのリソースへの Web およびモバイルアプリケーションレベルの安全なアクセスを提供します。ユーザーが業務用モバイルアプリを搭載した Android デバイスから接続する場合は、NetScaler 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 デバイスの 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。

ユーザーが **Citrix Secure Access** クライアントに接続する方法

April 1, 2024

NetScaler Gateway は以下のように動作する。

- 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 Secure Access クライアントは組織の内部ネットワーク宛のすべてのネットワークトラフィックを暗号化し、パケットを NetScaler Gateway に転送します。
- NetScaler 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、その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。NetScaler Gateway は、セキュリティで保護されたトンネルを介してリモートコンピューターにトラフィックを戻します。

ユーザーが Web アドレスを入力すると、ログオンページが表示され、そこで資格情報を入力してログオンします。資格情報が正しい場合、NetScaler 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。詳細については、「ユーザー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 Secure Access クライアント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した場合、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

ユーザーが Citrix Secure Access クライアント、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 NetScaler Gateway で構成されている任意のポート）を介して安全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、NetScaler Gateway は Citrix Secure Access クライアント、Secure Hub、または Citrix Workspace アプリに、保護するネットワークを説明し、アドレスプールを有効にしている場合は IP アドレスを含む構成情報を送信します。

セキュアな接続を介してプライベートネットワークトラフィックをトンネルする

Citrix Secure Access クライアントが起動して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のすべてのネットワークトラフィックがキャプチャされ、安全なトンネルを介して NetScaler Gateway にリダイレクトされます。ユーザーがログオンしたときにセキュアトンネルを介して接続を確立するには、Citrix Workspace アプリが Citrix Secure Access クライアントをサポートしている必要があります。

Secure Hub、Secure Mail、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。

NetScaler Gateway は、ユーザーデバイスが行うすべてのネットワーク接続をインターセプトし、Secure Sockets Layer（SSL）を介して NetScaler Gateway に多重化します。NetScaler Gateway では、トラフィックが逆多重化され、接続が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の対象となります。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/サブネットペアの範囲）を指定します。

Citrix Secure Access クライアントは、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。

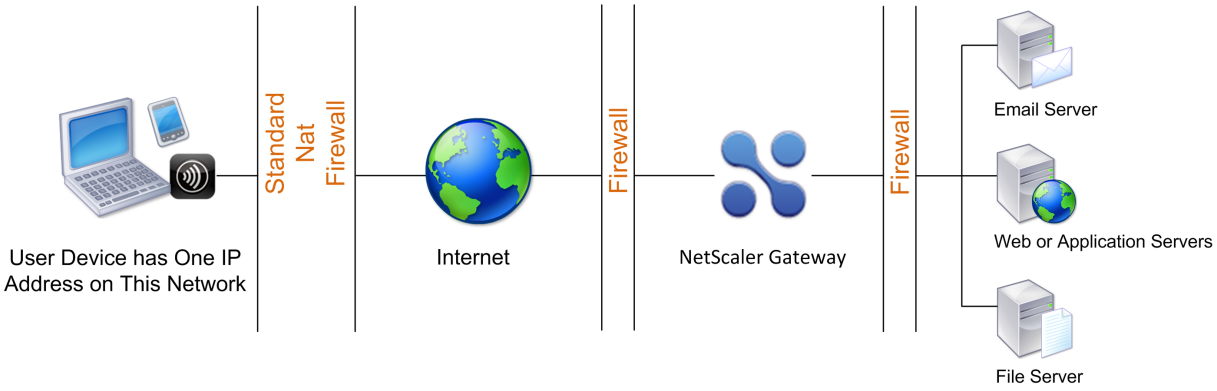
- TCP (すべてのポート)
- UDP (すべてのポート)
- ICMP（タイプ 8 および 0-エコー要求/応答）

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、NetScaler Gateway に安全にトンネリングされ、NetScaler Gateway はターゲットサーバーへの接続を再確立します。ターゲットサーバーは、プライベートネットワーク上のローカル NetScaler Gateway からの接続として認識し、ユーザーデバイスを隠します。これは、リバース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、送信元の場所にセキュリティが追加されます。

ローカルでは、SYN-ACK、PUSH、ACK、FIN パケットなどのすべての接続関連トラフィックが、Citrix Secure Access クライアントによってユーザーデバイス上で再作成され、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経由で接続する

Citrix Secure Access クライアントのユーザーは、次の図に示すように、別の組織のファイアウォールの内側にいる場合があります。



NAT ファイアウォールは、NetScaler Gateway からユーザーデバイスに安全なパケットをルーティングできるようにするテーブルを保持します。回線指向接続の場合、NetScaler Gateway はポートマップされたリバース NAT 変換テーブルを保持します。リバース NAT 変換テーブルを使用すると、NetScaler Gateway は接続を照合し、正しいポート番号を持つユーザーデバイスにパケットをトンネル経由で送信し、パケットが正しいアプリケーションに返されるようにします。

Citrix Secure Access クライアントのアップグレードを制御

システム管理者は、NetScaler ADC プラグインのバージョンが NetScaler Gateway リビジョンと一致しない場合の NetScaler ADC プラグインの実行方法を制御します。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、NetScaler ADC アプライアンスの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

要件

- Windows EPA および VPN プラグインのバージョンは 11.0.0.0 より大きくなければなりません
- 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:
>
> NetScaler ADC アプライアンスを 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、以前のアップグレード制御設定が尊重されます。

プラグインビヘイビア

NetScaler Gateway では、クライアントの種類ごとに、次の 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。

- いつも

エンドユーザーのプラグインのバージョンが NetScaler ADC アプライアンス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。

- 必須 (およびセキュリティ)

プラグインは、必要であると判断された場合にのみアップグレードされます。アップグレードは、次の 2 つの状況で必要であるとみなされます。

- インストールされているプラグインは、現在の NetScaler ADC アプライアンスのバージョンと互換性がありません。
- インストールされているプラグインは、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したいが、プラグインのセキュリティアップデートを見逃したくない場合は、このオプションを選択します。

- 決して

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

NetScaler 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 および 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、NetScaler Gateway は windowsInPluginUpgrade と macPluginUpgrade という名前の 2 つのセッションプロファイルパラメーターをサポートしています。

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、[常時]、[必須]、または [なし] の値を指定できます。これらのパラメータの詳細については、「プラグインビヘイビア」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

NetScaler 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、NetScaler Gateway は windowsEpaPluginUpgrade および macePAPluginUpgrade という名前の 2 つの仮想サーバーパラメーターをサポートしています。

パラメータは、仮想サーバレベルで使用できます。各パラメータには、[常時]、[必須]、または [なし] の値を指定できます。これらのパラメータの詳細については、「プラグインビヘイビア」を参照してください

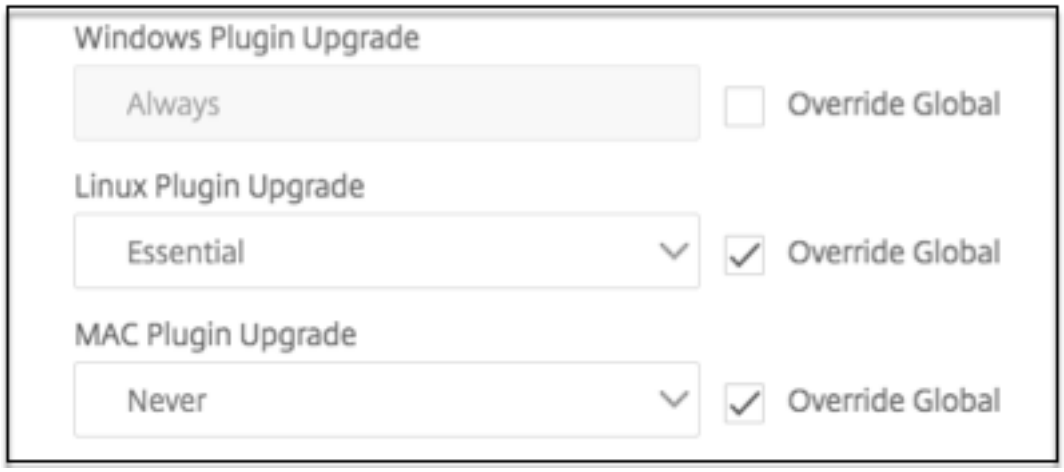
VPN 構成

Windows、Linux、および Mac プラグインの **VPN** 構成については、以下の手順に従ってください。

1. [**NetScaler] > [**ポリシー**] > [**セッション**]** に移動します。
2. 目的のセッションポリシーを選択し、[編集] をクリックします。
3. [クライアントエクスペリエンス] タブを選択します。
4. 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。

   - いつも
   - エッセンシャル
   - 決して

   デフォルトは [常時] です。
5. 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、および 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. [**NetScaler Gateway**] **>** [仮想サーバー] に移動します。
2. サーバを選択し、[**Edit**] 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。以下の種類から選択できます。

    - いつも
    - エッセンシャル
    - 決して

NetScaler Gateway での完全 **VPN** のセットアップ

April 1, 2024

このセクションでは、NetScaler Gateway アプライアンスで完全 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、ネットワーキング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 証明書をインストールし、VPN 仮想サーバーにバインドします。
    - 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と一致する信頼できる CA 証明書に置き換える方法
  - NetScaler ドキュメント -証明書とキーのペアを SSL ベースの仮想サーバーにバインドする

- NetScaler Gateway の認証プロファイルを作成します。
  - 詳細については、NetScaler のドキュメント「外部ユーザー認証の設定」を参照してください。
  - 詳細については、「チェックリスト: 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」を参照してください。
- VPN クライアントをダウンロードします。
- 完全な VPN 接続を許可するセッションポリシーを作成します。

ユーザーが Citrix Secure Access クライアント、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 NetScaler Gateway で構成されている任意のポート）を介して安全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、NetScaler Gateway は、セキュリティで保護するネットワークを説明する構成情報を Citrix Secure Access クライアント、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 を有効にすると、この情報には IP アドレスも含まれます。

ユーザーデバイス接続を構成するには、内部ネットワークでユーザーが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、次の作業が含まれます。

- 分割トンネリング
- アドレスプール (イントラネット IP) を含むユーザーの IP アドレス
- 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されるドメインの定義
- タイムアウト設定
- シングルサインオン
- NetScaler Gateway を介して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

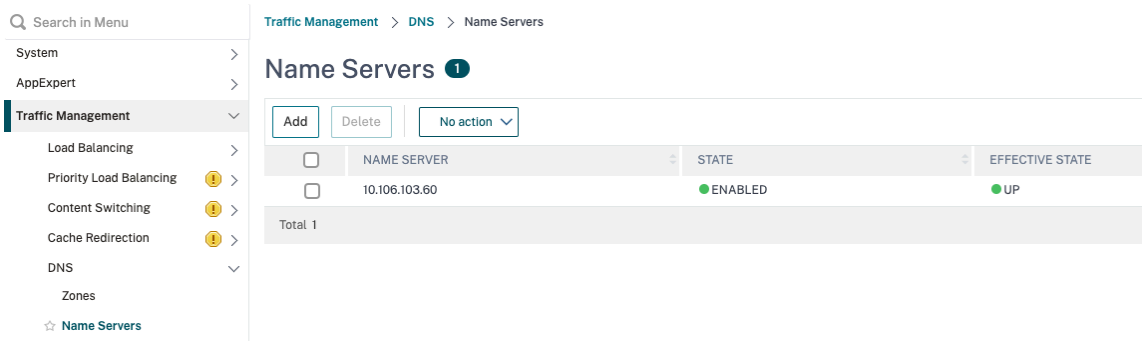
ほとんどのユーザーデバイス接続は、セッションポリシーの一部であるプロファイルを使用して構成します。また、認証ごとのポリシー、トラフィックポリシー、および認可ポリシーを使用して、ユーザーデバイスの接続設定を定義することもできます。また、イントラネットアプリケーションを使用して構成することもできます。

NetScaler Gateway アプライアンスで完全 **VPN** セットアップを構成する

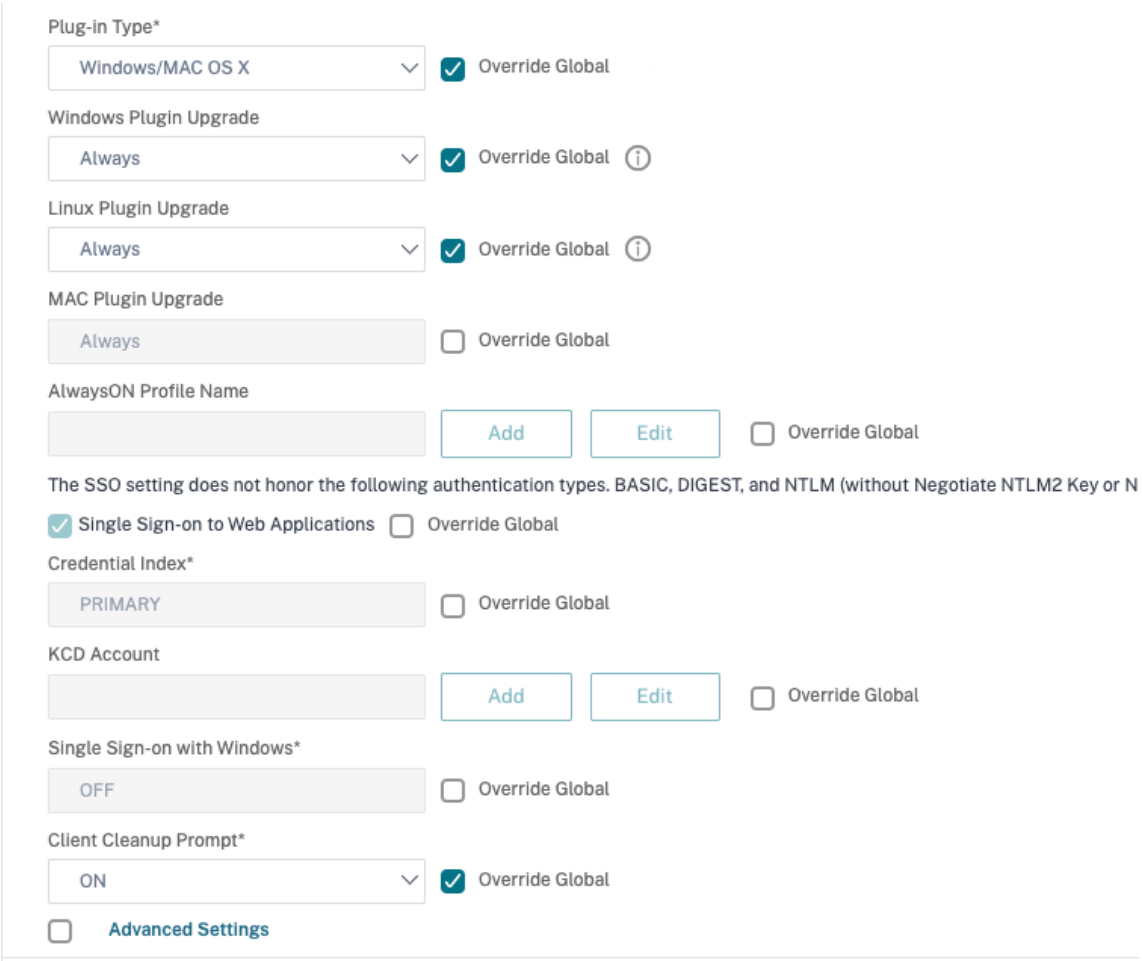
NetScaler Gateway アプライアンスで VPN セットアップを構成するには、次の手順を実行します。

1. [トラフィック管理**] > [DNS**] に移動します。

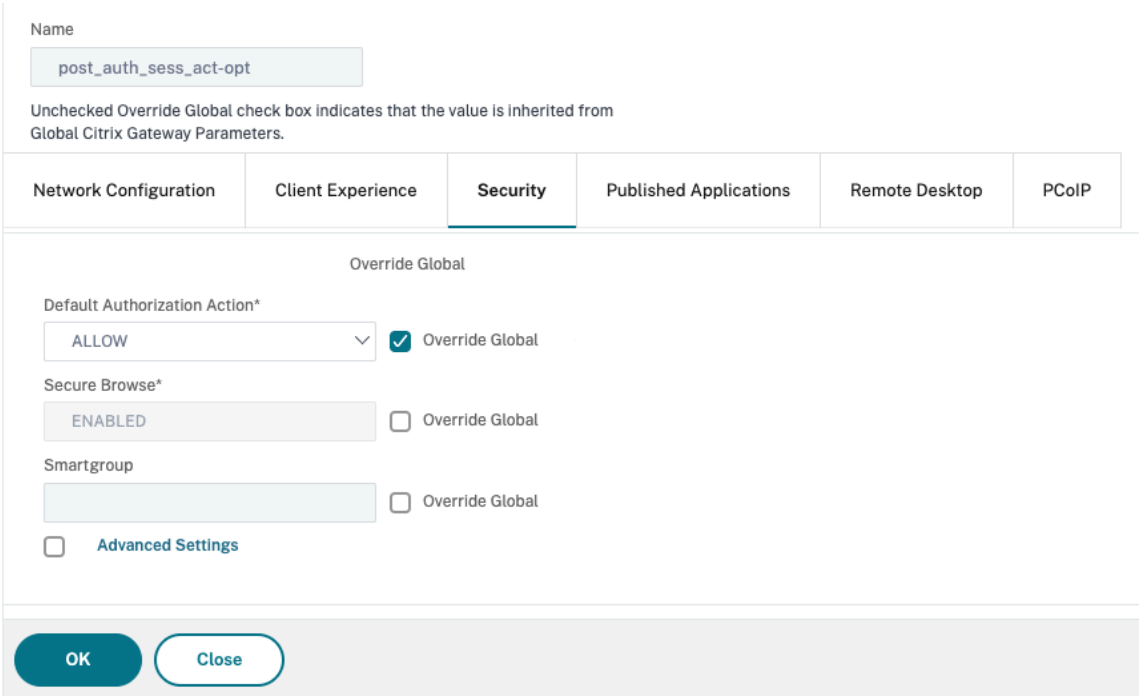
2. 次のスクリーンショットに示すように、[ネームサーバー] ノードを選択します。DNS ネームサーバーが一覧表示されていることを確認します。使用できない場合は、DNS ネームサーバーを追加します。



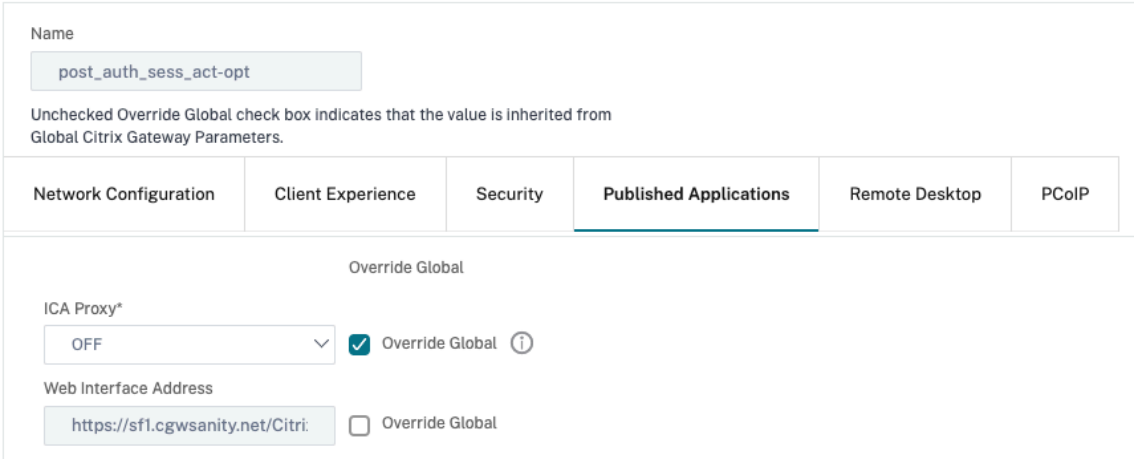
3. **NetScaler Gateway >** ［ポリシー］を展開
4. [セッション] ノードを選択します。
5. [NetScaler Gateway セッションポリシーとプロファイル] ページで、[プロファイル] タブをクリックし、[追加］をクリックします。
   [NetScaler Gateway セッションプロファイルの構成］ダイアログボックスで構成する各コンポーネントについて、それぞれのコンポーネントの［グローバルを上書き］オプションを選択します。
6. [クライアントエクスペリエンス] タブをクリックします。
7. ユーザが VPN にログインするときに任意の URL を表示する場合は、[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. [分割トンネル（Split Tunnel）] リストから目的の設定を選択します。
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。



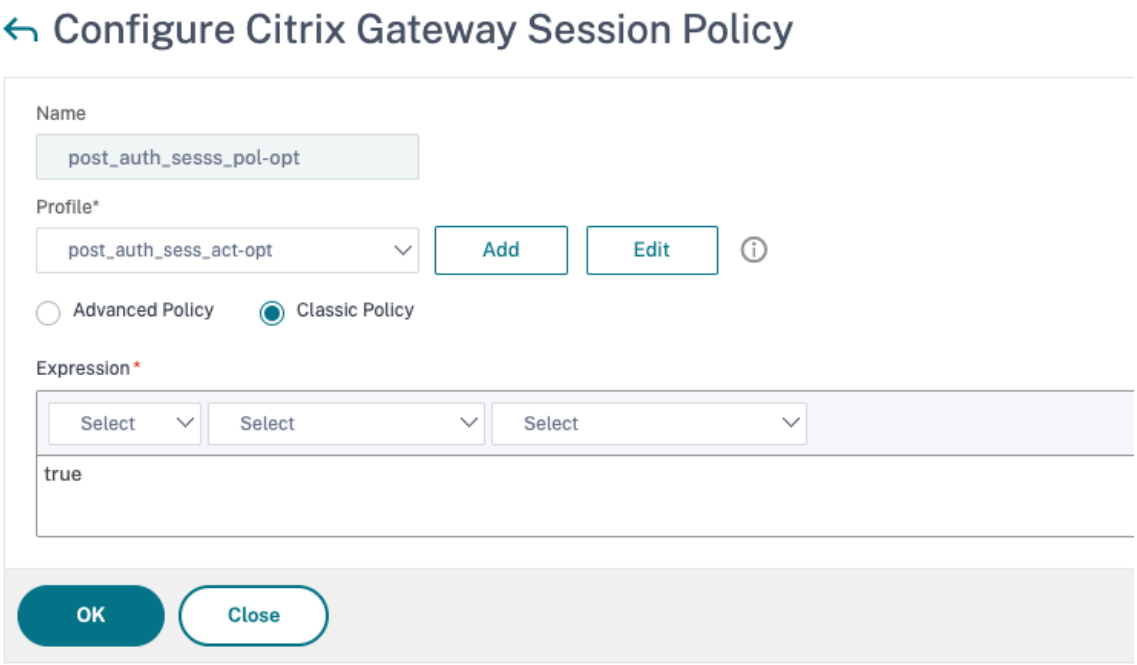
13. ［セキュリティ］タブをクリックします。
14. 「デフォルト認証アクション」リストから「許可」が選択されていることを確認します。



15. [**Published Applications**] タブをクリックします。
16. [公開アプリケーション] オプションの [**ICA** プロキシ] リストで [**OFF**] が選択されていることを確認します。



17. [**Create**] をクリックします。
18. [閉じる] をクリックします。
19. 仮想サーバーの [**NetScaler 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] タブをクリックするか、必要に応じてグループ/ユーザー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、必須の式または true を使用してセッションポリシーを作成します。

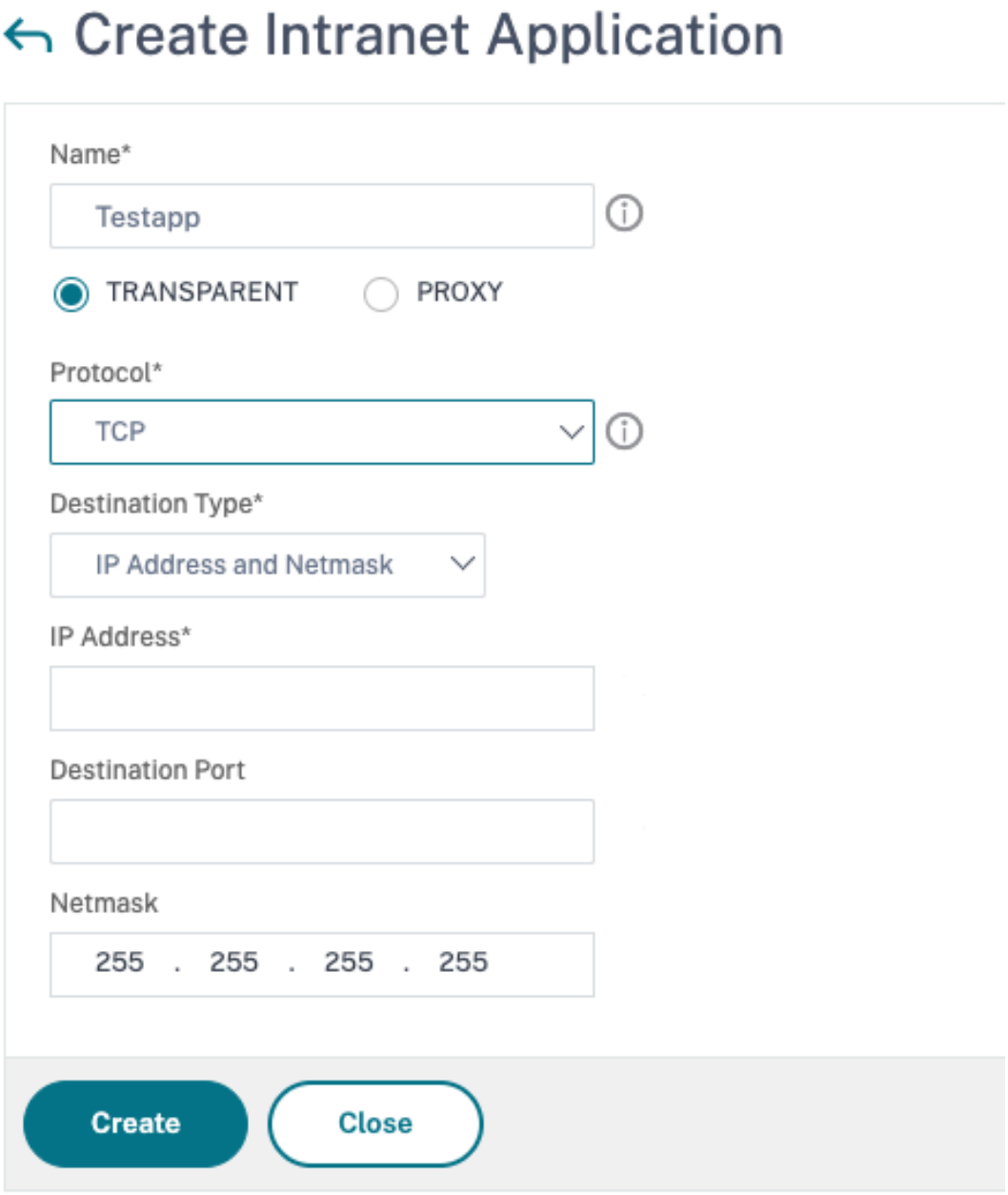


21. セッションポリシーを VPN 仮想サーバーにバインドします。詳細については、「バインドセッションポリシー」を参照してください。

    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。イントラネットアプリケーションについて詳しくは、「Citrix Secure Access クライアントのイントラネットアプリケーションの構成」を参照してください。

    a) [**NetScaler Gateway**] > [リソース] > [イントラネットアプリケーション] に移動します。

    b) イントラネットアプリケーションを作成します。Windows クライアントを使用した FullVPN の場合は、[透明] を選択します。許可するプロトコル (TCP、UDP、または ANY)、宛先タイプ (IP アドレスとマスク、IP アドレス範囲、またはホスト名) を選択します。



c) 必要に応じて、次の式を使用して iOS と Android の VPN の新しいポリシーを設定します。

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixVPN")&&HTTP.
REQ.HEADER("User-Agent").CONTAINS("NSGiOSplugin")&&HTTP.REQ.
HEADER("User-Agent").CONTAINS("Android")
```

d) 必要に応じて、ユーザー/グループ/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。

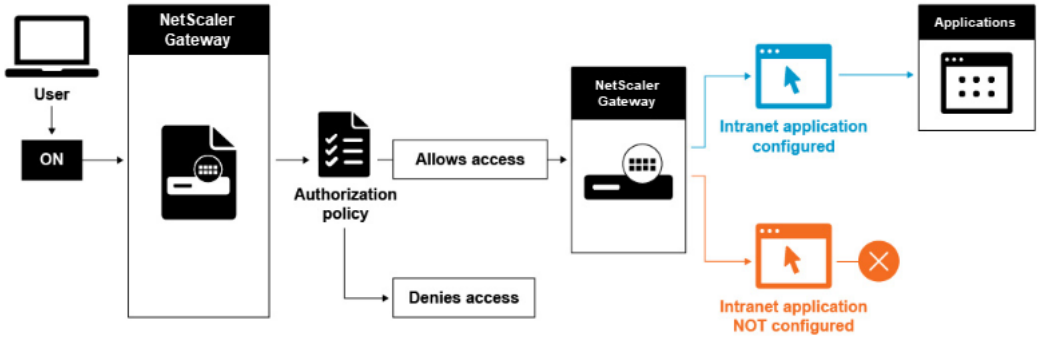
分割トンネリングの設定

1. ［構成］>［**NetScaler Gateway**］**>**［ポリシー］［セッション］に移動します。
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、[編集] 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［グローバルオーバーライド］を選択し、オプションを選択して［**OK**］をクリックします。

   分割トンネリングおよび認可の設定

   NetScaler 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オンに設定されており、NetScaler Gateway 経由でネットワークトラフィックを送信するようにイントラネットアプリケーションを構成していない。NetScaler Gateway にこの種類の構成がある場合、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た場合、Citrix Secure Access クライアントは NetScaler Gateway にトラフィックを送信しますが、次の条件ではリソースへのアクセスは拒否されます。

- 分割トンネリングが ON に設定されている。
- イントラネットアプリケーションは、ネットワークトラフィックを NetScaler Gateway 経由でルーティングするように構成されている

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
- 承認ポリシーの構成
- デフォルトのグローバル認証の設定

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 > **NetScaler Gateway >** リソース **>** イントラネットアプリケーションの順に移動します。
2. 詳細ペインで、[追加] をクリックします。

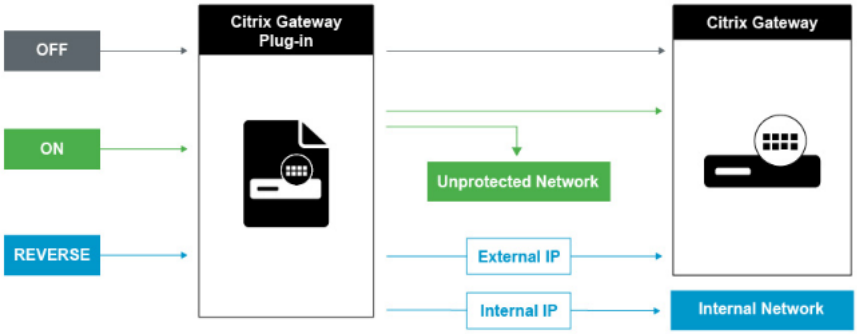
3. ネットワークアクセスを許可するためのパラメータを入力し、[作成]、[閉じる] の順にクリックします。

VPN ユーザーのイントラネット IP を設定しない場合、ユーザーはトラフィックを NetScaler Gateway VIP に送信し、そこから NetScaler ADC アプライアンスは内部 LAN 上の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作成します。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けて発信されます。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）への応答を試みます。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送信します。

イントラネット IP アドレスが使用されると、ユーザーはトラフィックを NetScaler Gateway VIP に送信し、そこから NetScaler ADC アプライアンスはクライアント IP をプールの構成されたイントラネット IP の 1 つにマップします。NetScaler ADC アプライアンスはイントラネット IP プールを所有することになるため、これらの範囲を内部ネットワークで使用しないでください。NetScaler ADC アプライアンスは、DHCP サーバーが行うように、着信 VPN 接続にイントラネット IP を割り当てます。NetScaler ADC アプライアンスは、ユーザーがアクセスする LAN 上の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けて発信されます。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（イントラネット IP）への応答を試みます。この場合、応答パケットは、イントラネット IP が配置されている NetScaler ADC アプライアンスにルーティングする必要があります（NetScaler ADC アプライアンスはイントラネット 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 SNIP のいずれかを指すイントラネット IP へのルートを持っている必要があります。非対称トラフィックを回避するために、パケットが NetScaler ADC アプライアンスを最初に送信するルートを保持する SNIP にトラフィックをポイントバックすることをお勧めします。

分割トンネリングオプション

次に、さまざまな分割トンネリングオプションを示します。



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 Secure Access クライアントはユーザーデバイスから発信されるすべてのネットワークトラフィックをキャプチャし、そのトラフィックを VPN トンネルを介して NetScaler Gateway に送信します。つまり、VPN クライアントは、クライアント PC から NetScaler Gateway VIP を指す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がトンネルを介して送信されるため、許可ポリシーは、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されるか、拒否されるかを決定する必要があります。

「オフ」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の場合は、NetScaler ADC アプライアンス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、プロキシサーバーを介して接続し、内部ネットワークにアクセスすることもできます。
NetScaler 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、NetScaler Gateway でこれらの設定を指定する必要があります。NetScaler Gateway 上のプロキシサーバーで使用される 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その後のすべての接続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。

- ユーザー接続のプロキシサポートの有効化

分割トンネル **ON**

分割トンネリングを有効にすると、Citrix Secure Access クライアントが不必要なネットワークトラフィックを NetScaler Gateway に送信するのを防ぐことができます。分割トンネルが有効になっている場合、Citrix Secure Access クライアントは、NetScaler Gateway によって保護されているネットワーク（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 Secure Access クライアントは、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 NetScaler Gateway に送信しません。Citrix Secure Access クライアントは起動すると、NetScaler 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ているサブネットごとにルートを確立します。Citrix Secure Access クライアントは、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、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（VPN 接続の開始時に作成されたルーティングテーブル）と比較します。パケット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 Secure Access クライアントは VPN トンネルを介して NetScaler 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既定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。

リバース分割トンネル

NetScaler Gateway は、NetScaler Gateway が傍受しないネットワークトラフィックを定義するリバース分割トンネリングもサポートしています。分割トンネリングをリバースに設定すると、イントラネットアプリケーションは、NetScaler 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。リバース分割トンネリングを有効にすると、内部 IP アドレスに向けられたすべてのネットワークトラフィックは VPN トンネルをバイパスし、他のトラフィックは NetScaler Gateway を経由します。リバース分割トンネリングを使用して、すべての非ローカル LAN ト

ラフィックをログに記録できます。たとえば、ユーザーが自宅のワイヤレスネットワークを使用して Citrix Secure Access クライアントでログオンしている場合、NetScaler Gateway はワイヤレスネットワーク内のプリンターや別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。

> 注:
>
> Windows 向け Citrix Secure Access クライアントは、Citrix Secure Access バージョン 22.6.1.5 以降の FQDN ベースのリバース分割トンネルもサポートしています。

注意事項　**IP** ベースのリバース分割トンネリング**:**

- IP アドレスベースのルールの数は 1024 に制限されています。
- DNE ドライバーと WFP ドライバーの両方でサポートされています。

ホスト名ベースのリバース分割トンネリング**:**

- VPN セッション中にアクセスできるホスト名の数は、FQDN スプーフィング範囲で指定された使用可能な IP アドレスの数によって制限されます。これは、すべてのホスト名が FQDN スプーフィング範囲から 1 つの IP アドレスを占めるためです。IP 範囲がなくなると、最後に割り当てられた IP アドレスが次の新しいホスト名に再利用されます。
- DNS サフィックスを設定する必要があります。

  > 注:
  >
  > Windows クライアントの場合、ホスト名ベースのリバース分割トンネリングは WFP ドライバーでのみサポートされます。「EnableWFP」レジストリ値を1に設定して、WFP ドライバモードを有効にします。詳しくは、「Windows フィルタリングプラットフォームを使用する Windows Citrix Secure Access クライアント」を参照してください。

IP ベースおよびホスト名ベースのリバース分割トンネリング**:**

- WFP ドライバーでのみサポートされます。IP ベースのリバース分割トンネリングとホスト名ベースのリバース分割トンネリングに記載されているその他のガイドラインはすべて適用されます。

ネームサービス解決を構成する

NetScaler Gateway のインストール中に、NetScaler 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その他の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。NetScaler Gateway ウィザードでは、次の操作も実行できます。

- DNS サーバーまたは WINS サーバーを構成する
- DNS ルックアップの優先度を設定する
- サーバーへの接続を再試行する回数を設定します。

NetScaler Gateway ウィザードを実行すると、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、別の DNS サーバーと WINS サーバーを NetScaler Gateway に追加できます。その後、ウィザードで最初に構成した名前解決サーバーとは異なる名前解決サーバーに接続するようにユーザーおよびグループに指示できます。

NetScaler Gateway で別の DNS サーバーを構成する前に、名前解決用の 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 サーバーまたは 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 > [**NetScaler Gateway**] **>** [ポリシー] **>** [セッション]
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 **Server 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。

参照ドキュメント

- 分割トンネリング
- ユーザーが Citrix Secure Access クライアントに接続する方法
- NetScaler Gateway について
- ユーザーのアクセス方法を選択します

ユーザーのアクセス方法を選択します

February 1, 2024

次のシナリオでユーザー接続を提供するように NetScaler Gateway を構成できます。

- Citrix Workspace アプリを使用したユーザー接続。Citrix Workspace アプリは、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する、StoreFront または Web Interface と互換性があります。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 Citrix Workspace アプリを Windows ベースまたは Mac ベースのコンピューターにインストールすると、Citrix Workspace アプリには、ユーザー接続用の Citrix Secure Access クライアントを含むすべてのプラグインが含まれます。NetScaler Gateway は、Android 向け Citrix Workspace アプリおよび 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 を介して、仮想デスクトップおよび Windows ベース、ウェブ、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 で構成されたモバイル、ウェブ、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。ユーザーが Secure Hub にログオンすると、WorxMail と WorxWeb、および 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 テクノロジを使用して、NetScaler Gateway を介して接続を確立します。
- Citrix Secure Access クライアントをスタンドアロンアプリケーションとして使用することによるユーザー接続。Citrix Secure Access クライアントは、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内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では、Citrix Secure Access クライアントや Citrix Workspace アプリなどのソフトウェアをユーザーデバイスに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、Citrix Virtual Apps で公開されているアプリケーション、Citrix Virtual Apps and Desktops からの仮想デスクトップ、および Access Interface を介したセキュリティで保護されたネットワーク内のファイル共有などの限定された Web リソースセットへの接続が可能になります。ユーザーは、Web ブラウザーに NetScaler Gateway Web アドレスを入力して接続し、選択肢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、アクセスシナリオフォールバックと呼ばれます。アクセスシナリオ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 Secure Access クライアントから 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 アプリを介して NetScaler Gateway にログオンすると、事前認証スキャンは機能しません。認証後スキャンは、NetScaler 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、次の方法で Citrix Secure Access クライアント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 NetScaler Gateway に接続する。
- NetScaler Gateway 接続を受け入れるように構成されている StoreFront に接続しています。
- 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。
- NetScaler ADC プラグインをマーチャンダイジングサーバーにアップロードする。

ユーザーアクセス用の **Citrix Secure Access** クライアントを導入

February 1, 2024

NetScaler 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 用 Citrix Secure Access クライアント
- Mac 用 Citrix Secure Access クライアント

ユーザーが NetScaler Gateway に初めてログオンすると、Web ページから Citrix Secure Access クライアント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 NetScaler Gateway アイコンをクリックしてログオンします。macOS X コンピュータでは、ユーザは **Dock** 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。NetScaler 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、Citrix Secure Access クライアントはユーザーデバイス上で自動的に更新されます。

MSI インストーラーパッケージを使用して **Citrix Secure Access** クライアントを展開します

Citrix Secure Access クライアントは、Microsoft AActive Directory インフラストラクチャまたは Windows Server Update Services などの標準のサードパーティ MSI 展開ツール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を使用して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

- セキュリティ要件に準拠する能力。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します。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。
- スケーラビリティ。一元化された展開戦略は、より多くのユーザーをサポートするように簡単に拡張できます。
- ポジティブなユーザーエクスペリエンス。このプロセスにユーザを関与させることなく、インストール関連の問題の展開、テスト、および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利用できる場合は、このオプションをお勧めします。

詳しくは、「Active Directory から Citrix Secure Access クライアントを展開する」を参照してください。

展開するソフトウェアプラグインを決定する

NetScaler Gateway 展開環境がユーザーデバイスにソフトウェアプラグインを必要としない場合、展開はクライアントレスアクセスを提供すると見なされます。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 ブラウザだけを必要とします。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 Secure Access** クライアントを選択してください

April 1, 2024

NetScaler 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 用 Citrix Secure Access クライアント
- macOS 向け Citrix Secure Access クライアント

セッションポリシーを作成し、その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て、構成を完了します。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、プラグインタイプとして Windows または macOS X 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、またはセッションプロファイルとポリシーで定義されているプラグインを受け取ります。プラグインタイプ用に個別のプロファイルを作成します。

プラグインをグローバルに構成する

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、［NetScaler 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、[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/macOS 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 **macOS** のプラグインタイプを構成する

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、**[NetScaler Gateway] > [**ポリシー**]** を展開し、**[**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：
   - セッションポリシーを作成する場合は、詳細ペインで [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、[開く] をクリックします。
3. 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、次のいずれかを実行します：
   - 「リクエストプロファイル」の横にある「新規」をクリックします。
   - 「リクエストプロファイル」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、[プラグインの種類] の横にある [グローバルを上書き] をクリックし、[**Windows/macOS X**] を選択します。
5. 次のいずれかを行います：

- プロファイルを作成する場合は、[作成] 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、[作成]、[閉じる] の順にクリックします。
- 既存のプロファイルを変更する場合は、選択後、「OK」を 2 回クリックします。

Windows 用 Citrix Secure Access クライアント

ユーザーが NetScaler Gateway にログオンすると、Citrix Secure Access クライアントをユーザーデバイスに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、初回の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権は必要ありません。

ユーザーが NetScaler 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。

- NetScaler Gateway 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た場合、Citrix Secure Access クライアント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:

- ユーザーが自分のコンピューター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でブロックされないように、ファイアウォールの設定を変更する必要があります。Citrix Secure Access クライアントは、Windows XP のインターネット接続ファイアウォールと Windows XP Service Pack 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。
- NetScaler 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、パッシブ転送を実行するように FTP アプリケーションを設定する必要があります。パッシブ転送とは、FTP サーバーからリモートコンピューターへのデータ接続が確立されるのではなく、リモートコンピューターが FTP サーバーへのデータ接続を確立することを意味します。
- 接続を介して X クライアントアプリケーションを実行したいユーザーは、コンピュータ上で X サーバ (など XManager) を実行する必要があります。
- Receiver for Windows または Receiver for Mac をインストールしたユーザーは、Receiver から、または Web ブラウザーを使用して Citrix Secure Access クライアントを起動できます。Receiver または Web ブラウザを使用して Citrix Secure Access クライアントにログオンする方法について、ユーザーに説明してください。

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 NetScaler 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 Secure Access クライアントをコンピューターにダウンロードしてインストールできます。

Windows 用 **Citrix Secure Access** クライアントのインストール

1. Web ブラウザーで、NetScaler 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 Secure Access クライアントが接続し、Windows ベースのコンピューターの通知領域にメッセージを表示します。

ユーザーが Web ブラウザーを使用せずに Citrix Secure Access クライアントに接続できるようにするには、**Windows** ベースのコンピューターの通知領域にある **NetScaler Gateway** アイコンを右クリックしたときにログオンダイアログボックスを表示するか、[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 向け **Citrix Secure Access** クライアントのログオンダイアログボックスの構成

ログオンダイアログボックスを使用するように Citrix Secure Access クライアントを構成するには、ユーザーがログオンしてこの手順を完了する必要があります。

1. Windows ベースのコンピューターでは、通知領域で NetScaler Gateway アイコンを右クリックし、[NetScaler 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、[ログオンに Citrix Secure Access クライアントを使用する] をクリックします。
   注：Receiver 内から [NetScaler 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。

Windows 向け **Citrix Secure Access** クライアントのインターセプトモードを設定します

Windows 向け Citrix Secure Access クライアントを構成する場合は、インターセプトモードを構成して透過モードに設定する必要もあります。

1. 構成ユーティリティで、[構成] タブをクリックし、[**NetScaler 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. 詳細ペインで、[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「任意」を選択します。
6. [宛先タイプ] で、[**IP** アドレス**]** と **[**ネットマスク] 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を入力し、[作成**]**、 [閉じる] の順にクリックします。

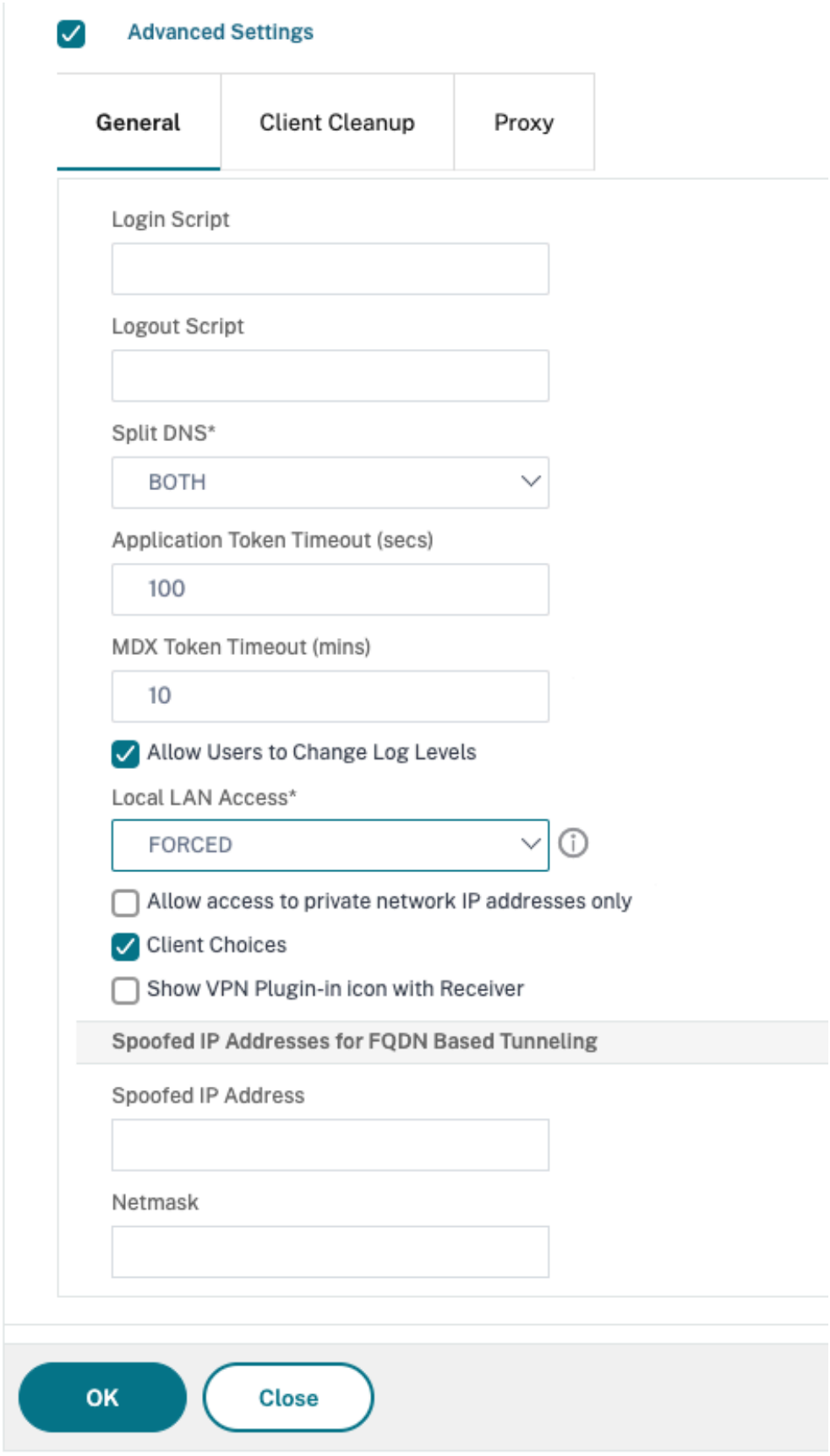
ADC 構成に基づいてエンドユーザーにローカル **LAN** アクセスを強制する

管理者は、エンドユーザーがクライアントマシンのローカル LAN アクセスオプションを無効にすることを制限できます。既存のローカル LAN アクセスパラメータ値に、FORCED という新しいオプションが追加されました。ローカル LAN アクセス値が FORCED に設定されている場合、クライアントマシンのエンドユーザーはローカル LAN アクセスが常に有効になります。エンドユーザーは、Citrix Secure Access クライアント UI を使用してローカル LAN 設定を無効にすることはできません。

管理者は、ローカル LAN アクセスパラメータを ON に設定することで、エンドユーザーがクライアントマシン上のローカル LAN リソースにアクセスできるようにすることができます。エンドユーザーがクライアントマシン上のローカル LAN リソースにアクセスできないようにするには、管理者はローカル LAN アクセスパラメーターを OFF に設定できます。エンドユーザー構成の詳細については、「macOS のローカル LAN アクセス 」と「iOS のローカル LAN アクセス」を参照してください。

GUI を使用して **[**強制**]** オプションを有効にするには**:**

1. ［**NetScaler Gateway**］**>** ［グローバル設定］**>** ［グローバル設定の変更］に移動します。
2. [クライアントエクスペリエンス] タブをクリックし、[詳細設定] をクリックします。
3. [ローカル **LAN** アクセス] で [強制] を選択します



CLI を使用して **Forced** オプションを有効にするには、次のコマンドを実行します。

```
set vpn parameter -localLanAccess FORCED
<!--NeedCopy-->
```

メモ:

- macOS/iOS 向け Citrix Secure Access クライアントとそれ以降のバージョンは、NetScaler Gateway のローカル LAN アクセス機能をサポートしています。
- Windows 23.10.1.7 向け Citrix Secure Access クライアント以降、ローカル LAN アクセスパラメーターが「NetScaler Gateway で強制」に設定されている場合、ローカル LAN アクセスはマシンレベルのトンネルでサポートされます。

Windows Citrix Secure Access の **Microsoft Edge WebView** サポート—プレビュー

Windows Citrix Secure Access の Microsoft Edge WebView サポートにより、エンドユーザーエクスペリエンスが強化されます。詳細については、「Windows Citrix Secure Access の Microsoft Edge WebView サポート」を参照してください。

Windows フィルタリングプラットフォームを使用する **Windows Citrix Secure Access** クライアント

Windows Filtering Platform (WFP) は、ネットワークフィルタリングアプリケーションを作成するためのプラットフォームを提供する API およびシステムサービスのセットです。WFP は、DNE ドライバーで使用されていたネットワークドライバーインターフェイス仕様 (NDIS) フィルターという、以前のパケットフィルター技術を置き換えるように設計されています。WFP モードは、Windows Citrix Secure Access クライアントの 22.6.1.5 ビルドでサポートされています。

WFP ビルドをインストールする

WFP ビルドは、次のいずれかの方法でインストールできます。

- DNE と WFP の両方のドライバーで VPN プラグインをインストールします (既定の方法)

  プラグインが DNE と WFP の両方のドライバーと共にインストールされている場合、管理者はレジストリノブを介して WFP または DNE ドライバーをトンネリングに使用できます。デフォルトでは、DNE ドライバーはトンネリングに使用されます。

- WFP ドライバーだけで VPN プラグインをインストールする (DNE ドライバーのインストールをスキップ)

  DNE ドライバーは、使用していないときでも一部のサードパーティ製アプリケーションではサポートされていません。これらの展開では、管理者はこのインストールタイプを使用できます。DNE ドライバーはインストールされていないため、トンネリングには WFP ドライバーのみが使用されます。

DNE ドライバーの代わりに **WFP** ドライバーを選択する

DNE ドライバーの代わりに WFP ドライバーを選択するには、次の手順を実行します。

> 注:
>
> これは、既定のインストール方法でのみ機能します。

1. WFP がサポートする VPN プラグインビルドをダウンロードし、新しい VPN プラグインをインストールします。
2. デフォルトでは、DNE ドライバーはトラフィックのトンネリングに使用されます。WFP ドライバーをトンネリングに使用するには、管理者は次のレジストリエントリを作成する必要があります。
   - REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
     - REG_TYPE - REG_DWORD
     - REG_NAME - EnableWFP
     - REG_VALUE —WFP を使用する場合は値を 1 に設定し、DNE を使用する場合は 0 に設定します (このレジストリ値が存在しない場合、または 0 に設定されている場合は、デフォルトで DNE が有効になります)

> 注:
>
> トンネリングモードを DNE から WFP に、またはその逆に切り替えた後、変更を適切に有効にするには、システムを再起動する必要があります。

DNE のインストールを完全にスキップする

DNE のインストールをスキップするには、次の手順を実行します。

1. VPN プラグインのクリーンアンインストールを実行します。
   a) マシンに現在存在する VPN プラグインをアンインストールし、マシンを再起動します。
   b) 次のいずれかのオプションを使用して、DNE ドライバーがアンインストールされているかどうかを確認します。
      - 管理者特権のコマンドプロンプト (または PowerShell) を開きます。次のコマンドを実行します (出力例は、DNE ベースのドライバーがシステムにインストールされていることを示しています)

```
PS C:\Users\Administrator> sc qc cag
[SC] QueryServiceConfig SUCCESS
SERVICE_NAME: cag
TYPE               : 1  KERNEL_DRIVER
START_TYPE         : 2   AUTO_START
ERROR_CONTROL      : 1   NORMAL
BINARY_PATH_NAME   : ??\C:\Program Files\Common Files\
    Deterministic Networks\Common Files\cag.sys
LOAD_ORDER_GROUP   :
```



```
TAG                : 0
DISPLAY_NAME       : Citrix cag plugin for Access Gateway
DEPENDENCIES       :
SERVICE_START_NAME :
PS C:\Users\Administrator> sc qc dne
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: dne
TYPE               : 1  KERNEL_DRIVER
START_TYPE         : 1   SYSTEM_START
ERROR_CONTROL      : 1   NORMAL
BINARY_PATH_NAME   : \SystemRoot\system32\DRIVERS\dnelwf64.sys
LOAD_ORDER_GROUP   : NDIS
TAG                : 38
DISPLAY_NAME       : DNE LightWeight Filter
DEPENDENCIES       :
SERVICE_START_NAME :
<!--NeedCopy-->
```

ドライバがインストールされていない場合は、次の出力が表示されます。

```
The specified service does not exist as an installed service.
```

DNE ドライバー（dnelwf64.sys）は他のベンダーでも使用されているため、Citrix Secure Access クライアントがシステムにインストールされていない場合でも存在する可能性があります。一方、CAG プラグインは Citrix Secure Access クライアントでのみ使用されます。

- DNE の存在は、CAG と DNE ドライバを起動しようとすることによっても確認できます。管理者権限を使用してコマンドプロンプトを開き、次のコマンドを実行します。

```
net start cag
net start dne
<!--NeedCopy-->
```

  - 出力メッセージに、サービスが見つからない (サービス名が無効である) ことが示されている場合、プラグインおよびドライバコンポーネントは正常にアンインストールされます。この場合は、手順 2 に進みます。
  - プラグインおよびドライバコンポーネントが正常にアンインストールされない場合は、https://citrix.sharefile.com/d-s829800c3821a4a8f869ad324de6f0332に記載されている手順に従って、クライアントマシンでクリーンアップユーティリティを実行します。
    * クリーンアップユーティリティを解凍し、フォルダにコピーします。
    * コマンドプロンプトから nsRmSAC.exe を実行します。
    * クライアントマシンを再起動します。

2. 次のレジストリエントリを作成します。

- REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - REG_TYPE - REG_DWORD

  - REG_NAME - SkipDNE
  - REG_VALUE-DNE がマシンにインストールされていないことを確認するには 1 に設定します
- REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - REG_TYPE - REG_DWORD
  - REG_NAME - EnableWFP
  - REG_VALUE-WFP を有効にする場合は 1 に設定します (DNE インストールをスキップする場合は、このエントリを作成する必要があります)

> 注:
>
> - インストール前にレジストリエントリが作成されていない場合は、デフォルトで DNE がインストールされます。また、VPN ログファイルをチェックして、WFP と DNE のどちらが使用されているかを検証できます。
> - DNE インストールをスキップする場合は、EnableWFP を 1 に設定する必要があります。この場合、Citrix Secure Access クライアントを再インストールしない限り、DNE ベースのプラグインに切り替えることはできません。

3. 新しい VPN プラグインをインストールします。
4. WFP ドライバーがシステムにインストールされているかどうかを確認します。管理者特権のコマンドプロンプトを開き、次のコマンドを実行します。サンプル出力は、WFP ドライバーがシステムにインストールされていることを示しています。

```
PS C:\Users\Administrator> sc qc ctxsgwcallout
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: ctxsgwcallout
    TYPE               : 1  KERNEL_DRIVER
    START_TYPE         : 1   SYSTEM_START
    ERROR_CONTROL      : 0   IGNORE
    BINARY_PATH_NAME   : ??\C:\Program Files\Citrix\Secure Access
       Client\ctxsgwcallout.sys
    LOAD_ORDER_GROUP   :
    TAG                : 0
    DISPLAY_NAME       : Citrix Secure Access Callout Driver
    DEPENDENCIES       :
    SERVICE_START_NAME :
<!--NeedCopy-->
```

ドライバがインストールされていない場合は、次の出力が表示されます。

```
The specified service does not exist as an installed service.
```

1. クライアントマシンを再起動します。

WFP の利点

スタンドアロン WFP ドライバーのインストールがクライアントで実行される場合の WFP の利点の一部を以下に示します。

- **FQDN** ベースのリバース分割トンネルのサポート**:** WFP ドライバーは、FQDN ベースの REVERSE 分割トンネリングのサポートを可能にします。DNE ドライバーではサポートされていません。詳細については、分割トンネリングオプションを参照してください。
- **Wireshark** のサポート**:** DNE は Ethernet/Wi-Fi アダプタとリンクしているため、クライアントマシンで双方向トラフィックをキャプチャできません。これは新しい WFP ドライバーの問題ではありません。トラフィックキャプチャ（一方向または双方向）はすべて暗号化され、復号化するには SSL キーが必要です。
- **NMAP** サポート**:** 新しい WFP ドライバーは NMAP スキャンをサポートしますが、VPN プラグインはトラフィックをトンネリングするのに対し、DNE は NMAP スキャンを許可しませんが、VPN プラグインはトラフィックのトンネリングに使用されます。
- ネットワーク速度**:** 一部のシナリオでは、クライアントマシンに DNE がインストールされている場合、ダウンロードとアップロードの速度が影響を受けますが、これは WFP には当てはまりません。
- **nslookup** パフォーマンスの向上**:** DNE では、`nslookup`がより少ない試行回数で応答できないことがあり、WFP では同じことが見られません。
- **UDP** 上の **iperf** パフォーマンスの向上**:DNE** では、**iperf over UDP** を使用したスケーラビリティテスト中にパケット損失が観察されました。WFP ではパケットロスは発生しません。

Active Directory から **Citrix Secure Access** クライアントを展開する

April 2, 2024

ユーザーに Citrix Secure Access クライアントをユーザーデバイスにインストールする管理者権限がない場合は、Active Directory Directory からユーザーにプラグインを展開できます。この方法を使用して Citrix Secure Access クライアントを展開すると、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 Secure Access クライアントパッケージを割り当てる。

  注：Active Directory からの Citrix Secure Access クライアントの配布は、Windows 7、Windows 8、および Windows 10 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 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 Secure Access** クライアント **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 Secure Access クライアントで、「**Windows** 用 **NetScaler 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:

   - 64 ビットコンピュータでは、Agee_setup.exe ファイルを Windows サーバに保存する必要があります。
   - ［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 キーを押して［**Windows** 向け **Citrix Secure Access** クライアントのダウンロード］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。

   ```
   nsvpnc_setup /c
   <!--NeedCopy-->
   ```

   これにより、ファイル agee.msi が抽出されます。

   注**:** 64 ビットコンピュータでは、**Agee_setup.exe** を保存したフォルダに移動して、次のように入力します。

   ```
   Agee_setup.exe /c
   <!--NeedCopy-->
   ```

   これにより、ファイル agee64.msi 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。

ファイルを展開したら、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 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 Secure Access クライアントを公開する場合、Citrix で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およびアクセラレーション (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権限で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. ［ネットワークロケーション］画面で［変更］をクリックし、Citrix Secure Access クライアント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。

抽出したパッケージをネットワーク共有に配置したら、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 Secure Access クライアント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、次回のユーザーデバイスの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たら、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 Secure Access クライアントがインストール中であるというメッセージがユーザーに表示されます。

Active Directory を使用して **Citrix Secure Access** クライアントを管理する

February 1, 2024

Citrix Secure Access クライアントの各リリースは、パッチとしてではなく、製品全体の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 Secure Access クライアントがプラグインの新しいバージョンを検出すると、プラグインは自動的にアップグレードされます。Citrix Secure Access クライアントを展開して、Active Directory を使用してアップグレードすることもできます。

そのためには、Citrix Secure Access クライアント用のディストリビューションポイントを作成します。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そのオブジェクトに割り当てます。次に、新しいパッケージと既存のパッケージの間にリンクを作成します。リンクを作成すると、Citrix Secure Access クライアントが更新されます。

Citrix Secure Access クライアントをユーザーデバイスから削除します

Citrix Secure Access クライアントをユーザーデバイスから削除するには、割り当てられたパッケージをグループポリシーオブジェクトエディターから削除します。

プラグインがユーザーデバイスから削除されると、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ユーザーに表示されます。

Active Directory を使用した **Citrix Secure Access** クライアントのインストールに関するトラブルシューティング

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:

ソフトウェアインストール設定の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、ソフトウェアインストールポリシーのアプリケーションが次のログオンまで遅延しました。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機能を呼び出す必要があります。

このエラーは、Windows XP の高速ログオンの最適化が原因で、オペレーティングシステムが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初期化する前にユーザーがログオンできることが原因です。ポリシーによっては、有効にするために複数の再起動が必要な場合があります。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 インストーラーログを有効にすることをお勧めします。

Citrix Secure Access クライアントを **Citrix Workspace** アプリと統合する

February 1, 2024

NetScaler 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システムは、次のコンポーネントで構成されています。

- Windows 3.4 以降向けの Citrix Workspace アプリ
- 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 またはそれ以降
- Endpoint Management 2.8 以降または Citrix Endpoint Management 10
- Citrix Web サイトでホストされている Citrix更新サービス

NetScaler Gateway と NetScaler 製品の互換性について詳しくは、「NetScaler 製品との互換性」を参照してください。

NetScaler Gateway は、ユーザーがアプライアンスにログオンしたときに、Citrix Secure Access クライアントが Web ブラウザーを開き、Citrix Workspace アプリのホームページへのシングルサインオンを可能にするように構成できます。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 NetScaler Gateway 経由でルーティングできます。

- Endpoint Management に直接アクセスする
- StoreFront に直接アクセスする
- Endpoint Management で MDX モバイルアプリを構成しない場合は、StoreFront、Endpoint Management の順に指定します。
- Endpoint Management で MDX モバイルアプリを構成する場合は、Endpoint Management と StoreFront の順に指定します

> 注:
>
> Endpoint Management に直接ルーティングされる接続は、Endpoint Management 2.0、Endpoint Management 2.5、Endpoint Management 2.6、Endpoint Management 2.8、および Endpoint Management 2.9 でのみサポートされます。ネットワークに Endpoint Management 1.1 を展開している場合、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。

ユーザーが **Citrix Workspace** アプリに接続する方法

February 1, 2024

ユーザーは、Citrix Workspace アプリから次のアプリケーション、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 で公開されている Windows ベースのアプリケーションと仮想デスクトップ
- 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。

- Citrix Workspace アプリ（Web）
- 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 向け Citrix Workspace アプリでログオンできます。

ユーザーが任意のバージョンの Citrix Workspace アプリでログオンすると、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ーまたは Citrix Workspace アプリウィンドウに表示されます。

Citrix Workspace アプリのアイコンを切り離す

April 1, 2024

Citrix Secure Access クライアントを Citrix Workspace アプリと統合して Citrix Virtual Apps and Desktops 環境を構成すると、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 Secure Access** アイコンは、通常、Windows のシステムトレイまたは macOS 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 Secure Access クライアント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 Secure Access クライアントのコントロールが表示されます。macOS X ユーザーの場合、統合後に Citrix Secure Access クライアントを制御することはできません。

一部の統合展開では、基盤となる機能の統合を維持しながら、プラグイン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、次の CLI コマンドまたは NetScaler ADC 構成ユーティリティタスクを使用して、VPN クライアントのアイコン統合を切り替えます。

CLI を使用したアイコン統合の設定

コマンドプロンプトで次を入力します:

```
set vpn parameter [-iconWithReceiver (ON/OFF)]

<!--NeedCopy-->
```

GUI を使用したアイコン統合の設定

1. ［構成］タブで、［**NetScaler 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** を構成する

April 1, 2024

NetScaler Gateway は、ICA 接続の IPv6 アドレスをサポートしています IPv6 を使用した Web Interface または StoreFront への接続は、IPv4 接続と同様に機能します。ユーザーが NetScaler Gateway Web アドレスを使用して接続すると、NetScaler 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 NetScaler Gateway またはダブルホップ DMZ に展開された NetScaler Gateway の IPv6 を構成できます。

NetScaler 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 NetScaler 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ていません。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 NetScaler Gateway を構成する必要があります。

ネットワークに複数の IPv6 サブネットを展開する場合は、NetScaler Gateway で、ネットワーク内のサブネットごとに複数の 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。

CLI を使用して **ICA** プロキシの **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、NetScaler Gateway にログオンします。コマンドプロンプトで次を入力します:

```
enable ns feature IPv6PT. This enables IPv6.

enable ns mode USNIP.

set dns parameter  -resolutionOrder AAAAThenAQuery AThenAAAAQuery
   OnlyAAAAQuery OnlyAQuery

set vpn parameter -wihome `http://XD_domain/Citrix/StoreWeb`

<!--NeedCopy-->
```

各項目の意味は次のとおりです StoreFront のドメイン名または IP アドレスのいずれかです。

例:

```
set vpn parameter -wihome `http://storefront.domain.com/Citrix/StoreWeb
   `.
<!--NeedCopy-->
```

または

```
set vpn parameter -wihome `http://[1000:2000::3000]/Citrix/StoreWeb`
<!--NeedCopy-->
```

> 注:

> IPv6 アドレスを使用してこのパラメータを設定する場合は、IP アドレスを括弧で囲む必要があります。

NetScaler Gateway で Citrix Workspace アプリのホームページを構成する

April 1, 2024

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。NetScaler Gateway を介して StoreFront を認識しない Citrix Workspace アプリを Web およびそれ以前のバージョンの Citrix Workspace アプリ用に構成する場合は、2 つの別々のセッションプロファイルを作成する必要があります。ユーザーが正常にログオンできるように、Citrix Workspace アプリのホームページのフィールドには、各プロファイルの正しい Web アドレスが必要です。

NetScaler Gateway を介して StoreFront を認識する Citrix Workspace アプリの場合、Web 向け 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 向け Citrix Workspace アプリのセッションプロファイルと、他のすべての Citrix WorkCitrix 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構成するには

Citrix Workspace アプリのホームページ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、［NetScaler 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、[グローバル設定の変更] をクリックします。
3. ［グローバル NetScaler 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 向け Citrix Workspace アプリのホームページの 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の [構成] タブのナビゲーションペインで、**[NetScaler 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、[追加] をクリックします。
3. ［**NetScaler 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** 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 向け Citrix Workspace アプリのホームページの Web アドレスを入力し、［作成］をクリックします。

Citrix Workspace アプリのテーマを NetScaler Gateway のログオンページに適用する

April 1, 2024

NetScaler Gateway UI を使用して、Citrix Workspace アプリテーマを NetScaler Gateway のログオンページに適用できます。Citrix Workspace アプリテーマと作成したカスタムテーマを切り替えることができます。カスタムテーマを作成したら、ブラウザーのキャッシュをクリアして、キャッシュされたページが表示されないようにします。

デフォルトでは、NetScaler Gateway のログインページは、StoreFStoreFront で使用される統合 UI のスタイルと一致する RfWebUI ビジュアルテーマを使用します。Citrix Workspace プラットフォームまたはオンプレミスの StoreFront [を新しい Workspace ユーザーインターフェイスで使用している場合は](https://docs.citrix.com/ja-jp/citrix-workspace/get-started/user-experience)、このサポート記事に記載されている手順に従ってください。または、独自のカスタムテーマを作成することもできます。詳しくは、「NetScaler Gateway ログオンページのカスタムテーマの作成」を参照してください。

NetScaler Gateway ポータルテーマが VPN 仮想サーバーにバインドされていることを確認します。詳細については、「ポータルテーマを VPN 仮想サーバーにバインドする」を参照してください。

NetScaler Gateway ログオンページのカスタムテーマを作成する

February 1, 2024

GUI を使用して、NetScaler 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のままにすることも、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、NetScaler 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、GUI 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、NetScaler Gateway グローバル設定を使用して構成します。

この機能は、次のバージョンの NetScaler Gateway で使用できます。

- NetScaler Gateway 10.1
- アクセスゲートウェイ 10、ビルド 73.5002.e（Endpoint Management 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）
- アクセスゲートウェイ 10、ビルド 71.6104.e

CLI を使用したカスタムテーマの作成と展開

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. NetScaler Gateway 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.gz 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/media 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 NetScaler 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ついて手順 3 と 4 を繰り返します。

NetScaler Gateway Windows VPN クライアントのレジストリキー

April 1, 2024

VPN クライアントのレジストリキーは、**HKEY_LOCAL_MACHINE\ SOFTWARE\ Citrix\ Secure Access Client** の下にあります。次の表に、NetScaler Gateway VPN クライアントのレジストリキー、値、および各値の簡単な説明を示します。

レジストリキー	レジストリタイプ	値と説明
AlwaysOnService	REG_DWORD	1 => マシンレベルのトンネルを確立するが、ユーザーレベルのトンネルは確立しない。2 => マシンレベルのトンネルとユーザーレベルのトンネルを確立する。
AlwaysOnURL	REG_SZ	ユーザーが接続する NetScaler Gateway 仮想サーバーの URL。例: *https://xyz.companyDomain.com*

レジストリキー	レジストリタイプ	値と説明
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。0 => 位置検出を無効にする。
suffixList	REG_SZ	イントラネットドメインのセミコロンリスト。位置検出が有効な場合に使用されます。
AlwaysOnAllowlist	REG_SZ	常時接続の厳密モードでドライバーによって許可される IP アドレスまたは FQDN のセミコロン区切りのリスト。
ProductVersion	REG_SZ	Citrix Secure Access クライアントにインストールされている現在のバージョン。
InstallDir	REG_SZ	Citrix Secure Access クライアントがインストールされている場所。
userCertCAList	REG_SZ	常時接続サービスのコンテキストで使用され、カスタマーはクライアント証明書の選択元となる CA のリストを指定できます。
addedRoutes/modifiedRoutes	REG_SZ	内部プラグイン通信用に作成されます。ユーザーはこのキーを変更してはなりません。
ProductCode	REG_SZ	このキーは内部で使用されます。ユーザーはこのキーを変更してはならない
EnableAutoUpdate	REG_DWORD	クライアント側からプラグインアップデート機能を制御するために使用されます。0 に設定すると、自動更新機能が無効になります。1 に設定すると、ADC 構成が考慮されます。
Connected	REG_DWORD	接続に成功すると、このキーは 1 に設定され、それ以外の場合は 0 に設定されます。このキーは内部で使用されます。ユーザーはこのキーを変更してはなりません。

レジストリキー	レジストリタイプ	値と説明
EnableVA	REG_DWORD	IIP が存在する場合に Citrix 仮想アダプタを有効にする必要がある場合。このキーは内部で使用されます。ユーザーはこのキーを変更してはなりません。
DisableGA	REG_DWORD	1 に設定すると、Google Analytics が無効になります。
DisableCredProv	REG_DWORD	[ユーザーログオン前に常時接続] が有効になっている場合、Windows VPN プラグインは、ログオン画面にトンネルの状態を表示するための資格情報プロバイダーを追加します。この追加機能が必要ない場合は、このレジストリを作成し、1 に設定します。
ClientControl	REG_DWORD	1 => ユーザーがログアウトしたり、他のゲートウェイに接続したりすることを許可します。0 => ユーザーがログアウトしたり、他のゲートウェイに接続したりすることをブロックします。
ForcedLogging	REG_DWORD	デバッグロギングを有効にするには、このキーを 1 に設定します。
NoDHCPRoute	REG_DWORD	1 に設定すると、DHCP サーバールートは追加されません。
DisableIntuneDeviceEnrollment	REG_DWORD	1 に設定すると、Intune デバイスの登録は実行されません。
HttpTimeout	REG_DWORD	HTTP タイムアウトは秒単位で設定されます。タイムアウトが設定されていない場合、デフォルトのタイムアウトが使用されます。デフォルトのタイムアウト値は 100 秒で、Windows 標準に基づいています。

レジストリキー	レジストリタイプ	値と説明
secureDNSUpdate	REG_DWORD	0 => VPN プラグインは非セキュア DNS の更新のみを試行します。1 => VPN プラグインは先にセキュアでない DNS の更新を試みます。セキュアでない DNS アップデートが失敗すると、VPN プラグインはセキュア DNS アップデートを試みます。これは 21.3.1.2 Windows プラグインビルド以降のデフォルトの動作です。2 => VPN プラグインはセキュア DNS の更新のみを試行します。
DisableIconHide	REG_DWORD	1 => Citrix Workspace アプリとゲートウェイプラグインがタスクバーに表示されます。0 => ゲートウェイプラグインアイコンは、Windows 向け Citrix Workspace アプリと統合されています。完全な VPN セッションを実行している場合、ゲートウェイプラグインはタスクバーに表示されません。
SecureChannelResetTimeoutSeconds	REG_DWORD	デフォルトでは、このレジストリ値は設定も追加もされません。「SecureChannelResetTimeoutSeconds」の値が 0xFFFFFFFF であるか、レジストリに存在しない場合、VPN プラグインは SecureChannelReset () API 呼び出しが完了するのを待ってから、データトラフィックのトンネリングを開始します。これはデフォルトの動作です。API 呼び出しが完了するまで指定された時間待ってからデータトラフィックのトンネリングを開始するには、管理者がクライアントにこのレジストリを設定して、VPN プラグインがデータトラフィックのトンネリングを開始する必要があります。

レジストリキー	レジストリタイプ	値と説明
DisableDNSRoutes	REG_DWORD	デフォルト値 0 => VPN Plug-in は、DNS サーバーのルートが物理インターフェイスのデフォルトゲートウェイと異なる場合、ルートを追加します。ただし、Windows クライアントマシンのトポロジーによっては、DNS サーバールートが必ずしも必要ではない場合があります。1 に設定すると、VPN プラグインは DNS サーバーに明示的なルートを追加しません。
IPv6 DNS ドロップをオーバーライド	REG_DWORD	1 => IPv6 DNS トラフィックが VPN 経由で流れることを許可します。0 => IPv6 DNS トラフィックフローを制限します。
DisallowCaptivePortals	REG_DWORD	1 => VPN プラグインは、VPN セッションを開始する前に Microsoft Connect テストページへの接続を試行してキャプティブポータルを確認します 。0 => VPN プラグインはキャプティブポータルのチェックをスキップします。
EnableWFP	REG_DWORD	デフォルト値 0 => デフォルトでは DNE は有効になっています。1 => VPN プラグインは WFP を使用します。0 => VPN プラグインは DNE を使用します。

レジストリキー	レジストリタイプ	値と説明
コンフィグサイズ	REG_DWORD	Windows クライアントは、デフォルトで 64 KB の構成ファイルサイズをサポートします。このレジストリを使用して、構成ファイルのサイズを増やします。構成ファイルのサイズがデフォルト値 (64 KB) より大きい場合は、64 KB を追加するたびに ConfigSize レジストリ値を (バイトに変換後) 5 x 64 KB に設定する必要があります。たとえば、64 KB を追加する場合は、レジストリ値を 64 x 1024 x 5 = 327680 に設定する必要があります。同様に、128 KB を追加する場合は、レジストリ値を 64 x 1024 x (5+5) = 655360 に設定する必要があります。
SecureAccessLogInScript	REG_SZ	Citrix Secure Access サービスは、Citrix Secure Private Access サービスに接続するときに、このレジストリキーを使用してログインスクリプト構成にアクセスします。詳細については、「ログインとログアウトのスクリプト設定レジストリ」を参照してください。
SecureAccessLogOutScript	REG_SZ	Citrix Secure Access サービスは、Citrix Secure Private Access サービスに接続するときに、このレジストリキーを使用してログアウトスクリプト構成にアクセスします。詳細については、「ログインとログアウトのスクリプト設定レジストリ」を参照してください。
EnableKerberosAuth	REG_DWORD	0 => デフォルト値。1 => VPN クライアントは自動ログオンに Kerberos 認証方法を使用します。

レジストリキー	レジストリタイプ	値と説明
SicBeginPort	REG_DWORD	ポートを使用して Citrix Secure Access クライアントとクライアントマシン上のサードパーティアプリとの間でソケットを作成するときに発生する可能性のある競合を回避します。許容範囲は 49152 から 64535 (16 進数形式では C000 から FC17) です。VPN クライアントは、`EnableWFP`が1に設定されている場合のみ、`SicBeginPort`から始まる最大 1000 個のポートを使用します。

> 重要:
>
> - 展開に基づいてレジストリキーを適用できます。たとえば、AlwaysOnService レジストリキーは常時接続サービスにのみ適用されますが、ClientControl レジストリキーは常時接続サービスには適用されません。詳しくは、それぞれの展開に関するドキュメントを参照してください。
> - `secureDNSUpdate` は、ドメインに参加しているクライアントデバイスにのみ適用されます。
> - Windows 23.1.1.8 以降のバージョンの Citrix Secure Access クライアントの場合、レジストリキー名は`overrideIPV6DnsDrop`です。Windows 22.10.1.9 以前のバージョン用の Citrix Secure Access クライアントの場合、レジストリキー名は`overrideIP6DnsDrop`です。

認証 **Cookie** に **HttpOnly** フラグを強制する

April 1, 2024

NetScaler Gateway リリース 13.1-37.x 以降では、VPN シナリオの認証 Cookie、つまり NSC_AAAC および NSC_TMASCookie で HttpOnly フラグが使用できるようになりました。NSC_TMAS 認証 Cookie は nFactor 認証時に使用され、NSC_AAAC Cookie は認証セッションに使用されます。Cookie の HttpOnly フラグは、JavaScript ドキュメント Cookie オプションを使用して Cookie アクセスを制限します。これにより、クロスサイトスクリプティングによる Cookie の盗難を防ぐことができます。

対応シナリオ

HttpOnly フラグは nFactor 認証でサポートされています。

NetScaler AAA パラメータの **HTTPOnlyCookie** ノブを **tmsession** の **HTTPOnlyCookie** ノブとともに使用したときの動作:

- 認証、承認、および監査パラメータの HTTPOnlyCookie ノブが有効になっていて nFactor 認証が使用されている場合、認証、承認、および監査パラメータの HTTPOnlyCookie ノブは TM セッションの HTTPOnlyCookie ノブよりも優先されます。また、NSC_TMAS と NSC_AAAC はどちらも、セッションタイプ（VPN セッション、TM セッション、または nFactor 認証中）に関係なく、HTTPOnly とマークされます。
- HTTPOnlyCookie ノブを無効にすると、VPN セッションに HTTPOnly フラグは設定されません。認証、承認、および監査シナリオでは、HttpOnly フラグは TM セッションノブの値に基づいて設定されます。

CLI を使用して **HTTPOnly** 機能を設定します

- HTTPOnly フラグを有効にする

```
set aaa parameter -httpOnlyCookie ENABLED
<!--NeedCopy-->
```

- HttpOnly 機能のステータスを確認してください

```
show aaa parameter
<!--NeedCopy-->
```

制限事項

- HttpOnly 機能を有効にすると、Citrix Secure Access クライアントの［ホームページ］ボタンが機能しません。
- HttpOnly フラグは従来の認証では設定されていません。

VPN ユーザー用のユーザーポータルをカスタマイズする

April 1, 2024

VPN ユーザーにポータルを提供する NetScaler Gateway インストールには、ポータルテーマを選択して、ポータルページのカスタマイズされたルックアンドフィールを作成するオプションが含まれています。提供されているテーマのセットから選択することも、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設定されたポータルを構築することもできます。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・デザインのその他のさまざまな属性を追加して、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ています。Web ブラウザー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表示されます。

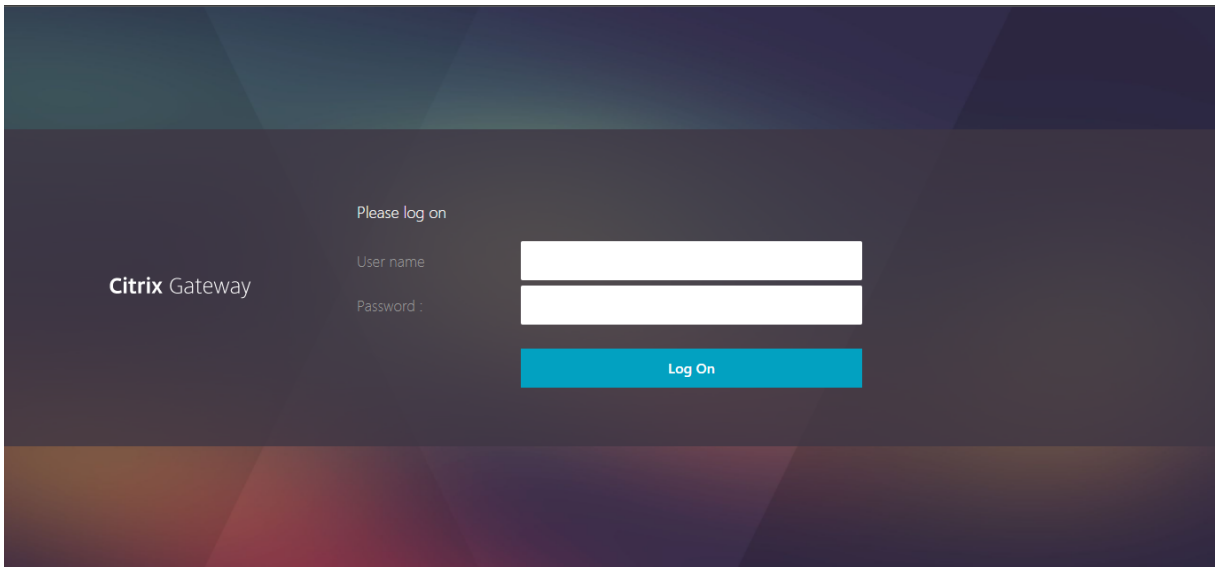
VPN ユーザーがサインインを許可される前に VPN ユーザーに提示されるカスタム EULA を作成できます。EULA 機能は、ロケール固有のバージョンの EULA をサポートします。これは、Web ブラウザーで報告されたロケールに基づいてユーザーに提示されます。

ポータル・テーマと EULA 構成はどちらも、VPN 仮想サーバーと VPN グローバル・レベルで個別にバインドできます。

> 重要:
>
> NetScaler は、コードの変更を必要とするカスタマイズをサポートしていません。また、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。

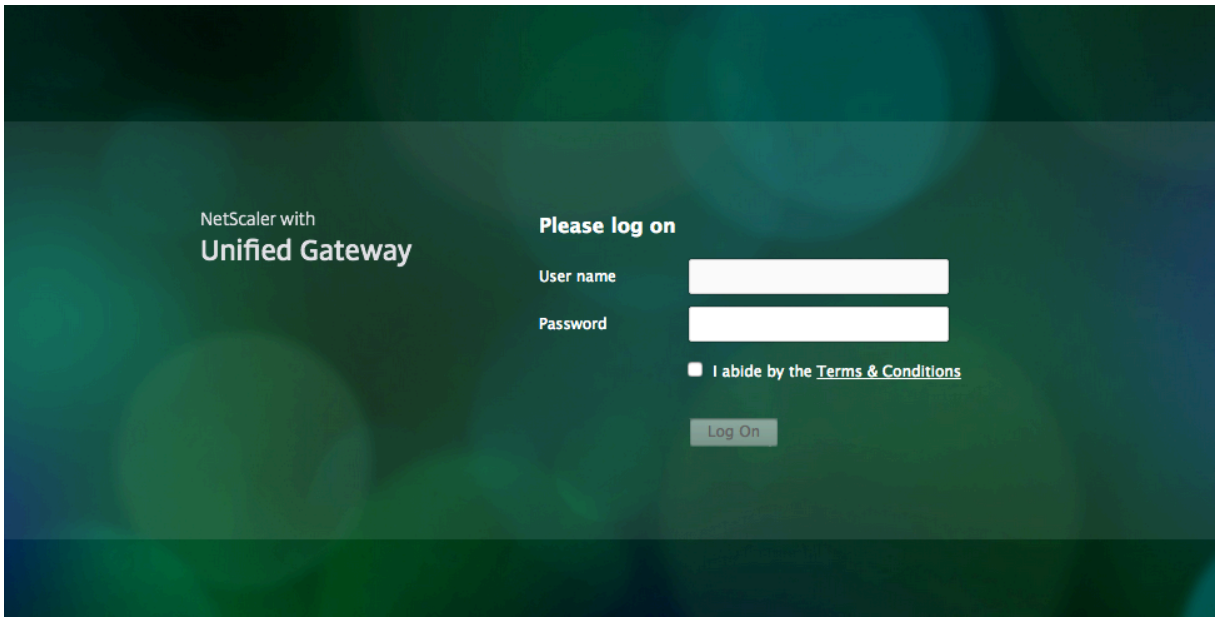
ポータル・テーマの適用

リリース 13.0 ビルド 67.43 以降、VPN ポータルはデフォルトで RfWebUI テーマを使用するように設定されます。以前は、`Caxton theme` がデフォルトのテーマでした。緑の吹き出しと X1 のテーマを適用することもできます。

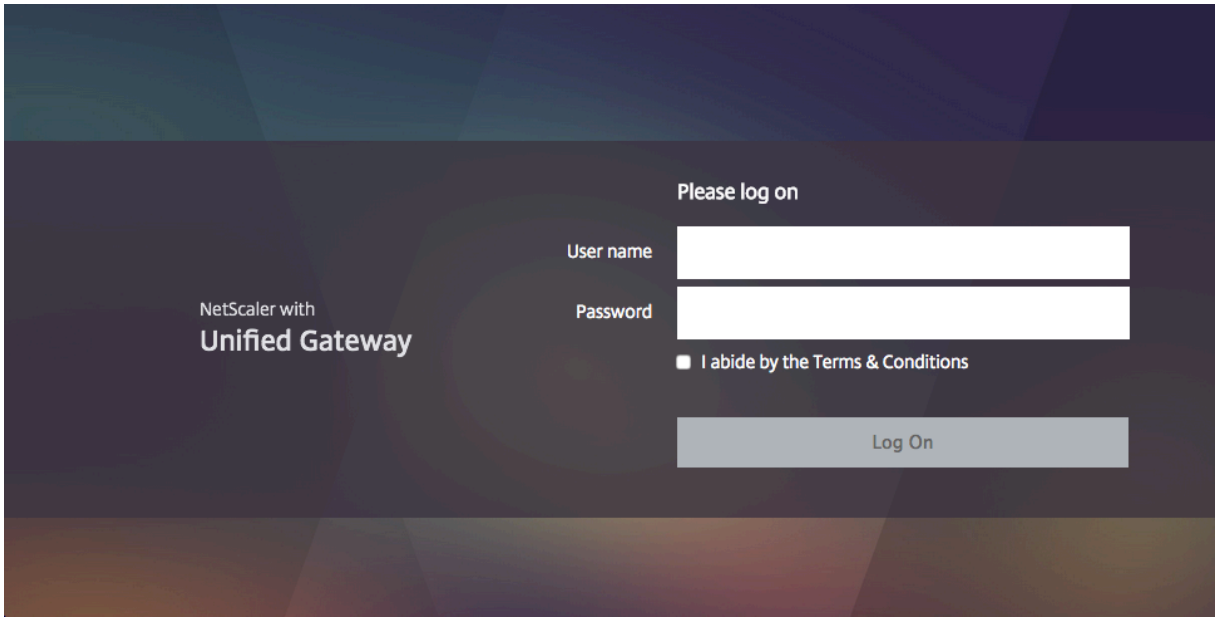


キャクストンのテーマ

グリーンバブルのテーマ



X1 のテーマ



提供されているテーマは、VPN 仮想サーバー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。

ポータル・テーマを **VPN** 仮想サーバーにバインドする

ポータル・テーマは、既存の仮想サーバー上にバインドすることも、新しい仮想サーバーを作成する場合にもバインドできます。

CLI を使用してポータル・テーマを **VPN** 仮想サーバーにバインドする

コマンドプロンプトで次を入力します:

```
bind vpn vserver <name> - portaltheme <name>
<!--NeedCopy-->
```

GUI を使用してポータル・テーマを **VPN** 仮想サーバーにバインドする

1. [構成] タブで、[**NetScaler 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、詳細ウィンドウの [詳細設定] の下にある [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] オプションは詳細ウィンドウですでに展開されています。

4. 詳細ウィンドウの [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・テーマのバインド] ウィンドウを展開します。
5. Click クリックして選択します。
6. [ポータルのテーマ] 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. [**Bind**] 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] 編集ペインで手順 3 から始まる前の手順の手順に従って、ポータル・テーマをバインドできます。

ポータル・テーマを **VPN** グローバルにバインドする

CLI を使用してポータルテーマを **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:

```
bind vpn global portaltheme <name>
<!--NeedCopy-->
```

GUI を使用してポータルテーマを **VPN** グローバルにバインドする

1. [構成] タブで、[**NetScaler Gateway**] に移動します。
2. メインの詳細ペインで、[**NetScaler 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、[ポータルのテーマ] 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、「バインドを追加」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. [ポータルのテーマ] 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. [**Bind**] 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:
>
> 変更を行った後、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、変更が NetScaler ADC 構成ファイルに保存されていることを確認します。

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。

ストックポータル・テーマをカスタム・ポータル・テーマのテンプレートとして使用する

ポータル・テーマを作成するには、構成ユーティリティまたはコマンドラインを使用してテーマ・エンティティを作成します。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。

CLI 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-->
```

GUI を使用したポータル・テーマの作成

1. ［構成］タブで、［**NetScaler Gateway**］に移動し、［ポータルのテーマ］をクリックします。
2. メインの詳細ペインで、[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て、「**OK**」をクリックします。
4. この時点で、ポータル・テーマの編集ウィンドウが初めて表示されます。［**OK**］をクリックして終了します。

初回表示で新しいポータル・テーマのカスタマイズに進むことができます。

新しいテーマを作成したら、それを VPN 仮想サーバーまたは VPN グローバルにバインドできます。新しいテーマは、作成直後またはカスタマイズの完了後にバインドできます。

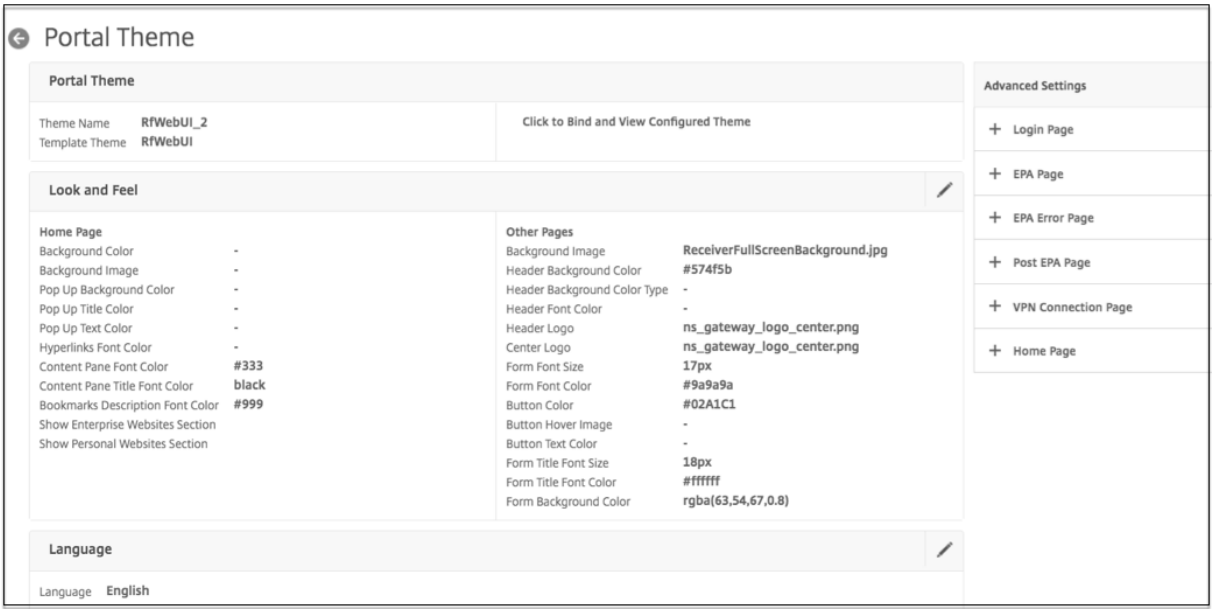
ポータル・テーマのカスタマイズ

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 Portal Theme インターフェースを使用します。最良の結果を得るには、このインターフェイスのさまざまな要素を理解してから使用する必要があります。

ポータル・テーマ・インターフェースについて

NetScaler 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［**NetScaler 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ことも、メインの詳細ペインで既存のテーマを選択して「編集」をクリックすることもできます。

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 つの主要コンポーネント・ペイン（「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、「言語」ペイン）があります。



ページ上部の [**Portal** Theme] ペインには、編集用にロードされているテーマと、そのベースになっているテンプレートテーマが表示されます。この表示オプションを使用すると、ユーザ接続で VPN にアクセスしなくても、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 仮想サーバーにバインドする必要があり、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 [**Look & Feel**] ペインを使用して、ヘッダー、背景色とイメージ、フォントプロパティ、ロゴなど、テーマの一般的なプロパティを構成します。このウィンドウが編集モードの場合、属性の凡例を使用して、ポータルページでのルックアンドフィール属性の使用場所に関するガイダンスとして使用できます。

[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含まれています。ページのコンテンツを編集用に読み込むには、一覧表示されたページの 1 つをクリックします。ページコントロールは、他の中央ペインの下に開きます。ページが変更されていない限り、ポータル・テーマの編集全体にわたって [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。

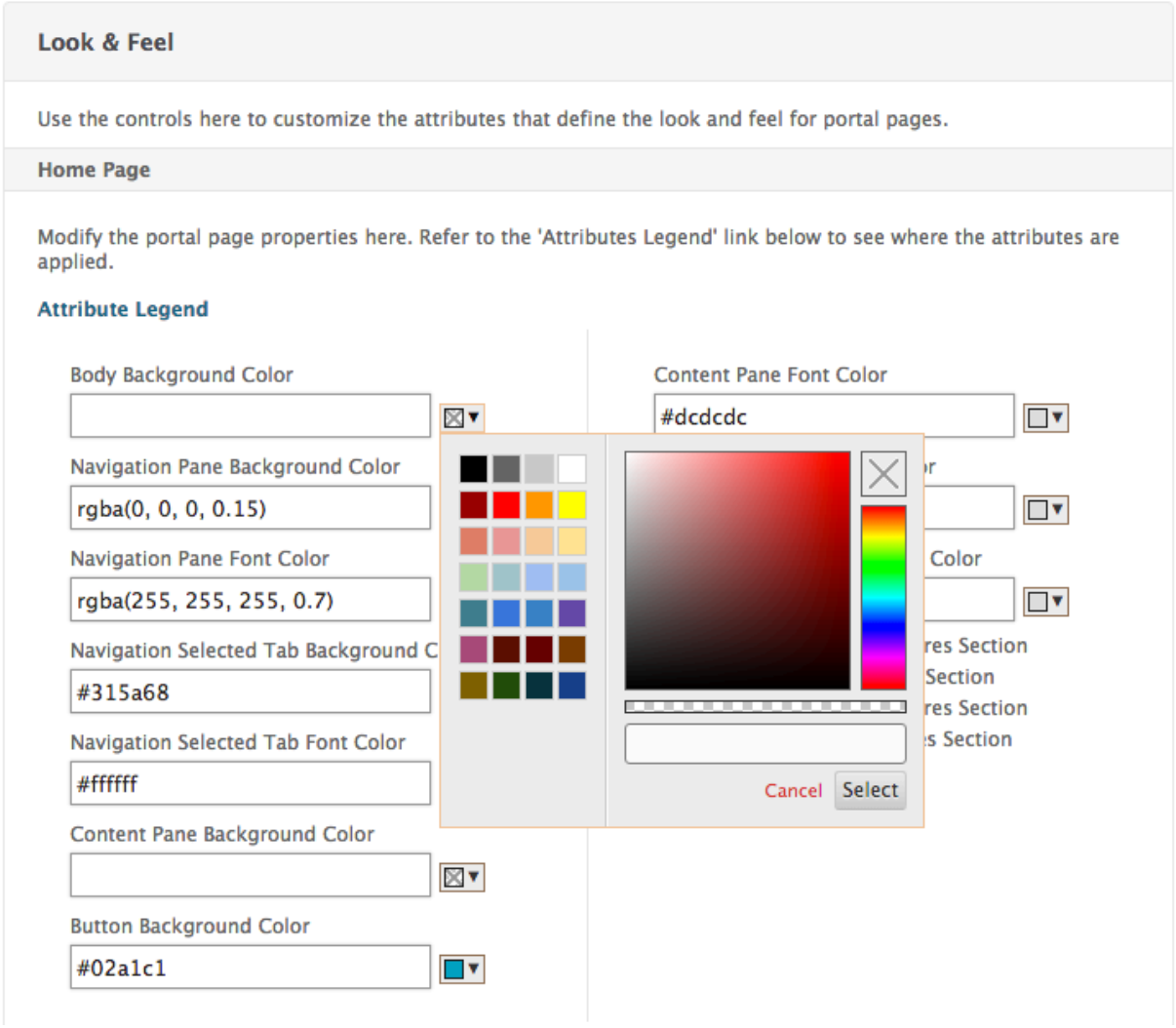
[言語] ペインでは、[詳細設定] ペインで編集対象としてページを選択したときにロードされる言語を選択できます。デフォルトでは、英語のページが読み込まれます。

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・インター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グラフィカル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]

ポータルのデザインは、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、選択したアイテム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 フォーマット、HTML 16 進トリプレットフォーマット、および X11 カラー名で入力できます。カラーピッカーは、属性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と、適用可能な任意のカラー属性でアクセスできます。



Fonts

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。これらの各属性について、ポータルの設計によって決定されるように、各属性で使用できるサイズがメニューに表示されます。

イメージ

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、推奨サイズおよびその他の要件が示されます。説明は、ページ上の属性の位置とその機能によって異なります。PNG または JPEG の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の場所を参照します。

ラベル

[詳細設定] セクションでは、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。ページのデフォルトの英語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便宜上提供されていますが、カスタマイズを行う場合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、別の言語を選択するまでその言語で表示されます。

> 重要
>
> 高可用性展開またはクラスター展開では、ポータルテーマがプライマリまたは構成コーディネーターの NetScaler ADC エンティティでそれぞれ作成された場合にのみ、共有構成全体にポータルテーマが分散されます。

古いポータルのカスタマイズ

11.0 より前の NetScaler Gateway または Access Gateway リリースで作成されたカスタムポータルデザインを手動で変更してインストールする場合、NetScaler 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始めることを強くお勧めします。それができない場合は、カスタマイズを手動で適用できますが、そのための直接的な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・バインディングで上書きすることはできません。この場合、構成ユーティリティまたはコマンドラインを使用して VPN 仮想サーバー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、高可用性およびクラスタ構成の場合、NetScaler ADC ファイルシステム上の基礎となるファイルは自動共有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カスタマイズを実行する必要があります。

カスタムポータル構成を手動で作成する

NetScaler Gateway 11.0 へのアップグレード後に古いカスタマイズされた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 NetScaler ADC ファイルシステムに配置し、****UITHEME** パラメーターとして **CUSTOM** 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、NetScaler ADC ファイルシステムにファイルを転送できます。

1. NetScaler Gateway 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/customthem 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

    - 緑の泡のテーマをカスタマイズする場合は、**cp-r** `Greenbubble` **Custom** と入力して、緑の泡の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** にコピーし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/media** 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 ファイルへの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ものを作成できます。

6. すべてのカスタマイズの変更が完了したら、プロンプトで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
>
> 前の手順でテーマディレクトリをコピーする場合、NetScaler ADC シェルインターフェイスでは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ー名は「カスタム」と正確に入力する必要があります。ディレクトリ名を正確に入力しないと、**UITHEME** 設定が **CUSTOM** に設定されているときに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します

手動でカスタマイズされたポータル構成が完了し、NetScaler ADC ファイルシステムにコピーされたら、NetScaler Gateway 構成に適用する必要があります。これは、UITHEME パラメーターを CUSTOM に設定することで実行され、コマンドラインまたは構成ユーティリティで完了できます。

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 **UIPHEME** パラメーターを設定します。

```
1 set vpn parameter UITHEME CUSTOM
2 <!--NeedCopy-->
```

構成ユーティリティを使用して 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、[**NetScaler 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。

手動でカスタマイズしたポータルが、VPN ユーザーに提示されるポータル設計になりました。

EULA を作成する

VPN ポータルシステムには、ポータル構成に EULA を適用するオプションが用意されています。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 NetScaler Gateway 構成にバインドされると、VPN ユーザーは VPN への認証を許可される前に、利用規約としての EULA に同意する必要があります。

ポータルのテーマと同様に、ユーザーには、Web ブラウザーによって報告されるロケールに基づいて、言語固有の EULA が提供されます。ロケールがサポートされている言語のいずれとも一致しない場合、提供される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。翻訳済みのコンテンツは、ポータル・テーマのような EULA 構成には提供されません。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、ユーザーは 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、構成ユーティリティの［構成］タブの［NetScaler Gateway］**>** ［グローバル設定］**>** [**EULA**] または［**NetScaler Gateway**］［リソース］**>** ［**EULA**］のいずれかのコントロールを使用できます。[**Global Settings**] ペインのコントロールは、VPN グローバル EULA バインディングの管理に使用され、[リソース**] > [EULA**] ノードのコントロールは、EULA 設定に関する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、［**NetScaler 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。

CLI を使用して **EULA** エンティティを作成する

コマンドプロンプトで次を入力します:

```
add vpn eula <name>
<!--NeedCopy-->
```

GUI を使用して **EULA** エンティティを作成する

1. [**NetScaler Gateway >** ［リソース］**>** ［**EULA**］に移動します
2. [追加] 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。プレーンテキストまたは HTML タグを使用して、改行を追加する
タグを含め、コンテンツの書式を設定することができます。
5. [**Create**］をクリックします。

EULA エンティティが作成されると、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。

CLI 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:

```
bind vpn global eula <name>
<!--NeedCopy-->
```

GUI を使用して **EULA** を **VPN** グローバルにバインドする

1. [構成] タブで、[**NetScaler Gateway**] **>** [グローバル設定] に移動します。
2. メインの詳細ウィンドウで、[エンドユーザー使用許諾契約書の構成] をクリックします。
3. [**Add Binding**] 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. [**Bind**] をクリックします。
7. [閉じる] をクリックします。

CLI 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-->
```

GUI を使用して **EULA** を **VPN** 仮想サーバーにバインドする

1. [構成] タブで、[**NetScaler 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、[編集] をクリックします。
3. ページの右側にある [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. `Click` クリックして選択します。
6. EULA エンティティを選択し、[選択] をクリックします。
7. [**Bind**] をクリックします。
8. [完了] をクリックします。

カスタムページを作成して、古いブラウザまたはサポートされていないブラウザをアップグレードするようにユーザに促す

February 1, 2024

クライアントが SSLv3 などの安全でない暗号を使用して NetScaler VIP アドレスに接続すると、クライアントはカスタムページにリダイレクトされ、Internet Explorer、Firefox、Chrome、または Safari の最新バージョンにアップグレードするように求められます。

注**:** インターネット技術タスクフォース (ITEF) の RFC6176 によると、TLS サーバーは SSLv2 をサポートしてはなりません。したがって、NetScaler アプライアンスはリリース 12.1 以降の SSLv2 をサポートしていません。

SSL に基づいてサポートされていない古いブラウザをアップグレードするようにユーザーに促すカスタムページを作成する方法

- ルール`client.ssl.version.eq()`を使用して NetScaler レスポンダーポリシーを作成します。バージョンは SSL プロトコルのバージョンを返します。
  - トランザクションが SSL ベースでない場合は 0 を返します。
  - トランザクションが SSLv2 の場合は 0x002 を返します。
  - トランザクションが SSLv3 の場合は 0x300 を返します。
  - トランザクションが TLSv1 の場合は 0x301 を返します。
- レスポンダーポリシーをトリガーするには、SSLv3（またはその他の以前のバージョン）を有効にする必要があります。

  たとえば、NetScaler アプライアンスで SSLv3 が無効になっていて、SSLv3 を使用する古いブラウザーを使用しているクライアントが接続を試みると、アクセスは拒否されます。
- 導入環境で SSLv3 またはそれ以前のバージョンを指定期間（1 か月または 2 か月）に必要とする場合は、次の設定を行います:
  - SSLv3 プロトコルを有効にします。
  - カスタムページを更新して、指定した期間が過ぎると、ブラウザがアプライアンスに接続できないという情報を含めます。

NetScaler Gateway でクライアントレス **VPN** アクセスを構成する

April 1, 2024

クライアントレスアクセスにより、ユーザーは Citrix Secure Access クライアントや 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には、次の手順を実行します。

- グローバルに、またはユーザー、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てから、それを有効にするセッションポリシーを作成します。

NetScaler 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するかどうかを選択できます。ウィザードの設定はグローバルに適用されます。NetScaler 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 Secure Access クライアント。ユーザーは、Citrix Secure Access クライアントのみを使用してログオンできます。
- Citrix Secure Access クライアントを使用して、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 Secure Access クライアントを使用して NetScaler Gateway にログオンします。ユーザ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、ユーザはクライアントレスアクセスを使用してログオンすることが許可されます。これが発生すると、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は制限されます。

クライアントレス **VPN** アクセスポリシーの仕組み

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、構成ユーティリティで構成できます。クライアントレスアクセスポリシーは、ルールとプロファイルで構成されます。NetScaler Gateway に付属する事前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。また、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。

NetScaler Gateway には、次の事前構成されたポリシーが用意されています。

- Outlook Web Access と Outlook Web アプリケーション
- SharePoint 2007
- その他すべての Web アプリケーション

> 注**:**
>
> OWA 2016 および SharePoint 2016 は、高度なクライアントレスアクセスを使用する場合にのみサポートされます。

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留意してください。

- これらは自動的に設定され、変更できません。
- 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、NetScaler Gateway で構成する書き換えポリシー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 Citrix Secure Hub 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 デバイス上で動作する Citrix Secure Hub 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 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 デバイスに接続しない場合は、Secure Browse を有効にする必要はありません。

クイック設定ウィザードは、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構成します。クイック構成ウィザードを実行して、StoreFront および Citrix Endpoint Management への接続に関する正しい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、カスタムポリシーを作成して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対して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、カスタムポリシーのプライオリティ番号を事前設定されたポリシーよりも小さくします。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。

クライアントレス **VPN** アクセスを有効にする

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。NetScaler 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することができます。

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。

- オン。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 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。

- オフ。クライアントレスアクセスは、デフォルトでは有効になっていません。クライアントレスアクセスは、ユーザーが Citrix Secure Access クライアントでログオンした後に有効になります。クライアントの選択を無効にし、StoreFront を構成または無効にしない場合、ユーザーは Citrix Secure Access クライアントでログオンします。ユーザがログオンしたときにエンドポイント分析が失敗した場合、ユーザには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。
- 無効。クライアントレスアクセスは無効です。[無効（Disabled）] を選択すると、ユーザ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は選択ページに表示されません。

NetScaler 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い場合は、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、［NetScaler 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、[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［オン］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、または仮想サーバのグループ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またはクリアします。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、ユーザー、グループ、または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、［**NetScaler Gateway**］**>**［ポリシー］**>**［セッション］の順に展開します。
2. 詳細ペインの [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.「リクエストプロファイル」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. [クライアントエクスペリエンス] タブの **[**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 [一般] を選択し、[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、 [閉じる] をクリックします。
8. [作成**]** をクリックし、 [閉じる] 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、ユーザー、グループ、または仮想サーバーにバインドします。

Web アドレスをエンコードする

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しておくかを選択できます。設定は次のとおりです。

- あいまい。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、ユーザがログオンし、ブックマークを使用して再度 Web アドレスに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 Access Interface 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 アドレスエンコーディングをグローバルに構成する

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、［NetScaler 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、[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］の横にあるエンコーディングレベルを選択し、［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構成する

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、［**NetScaler 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 [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.「リクエストプロファイル」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「グローバルオーバーライド」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 [一般] を選択し、[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、[閉じる] をクリックします。

クライアントレスアクセスポリシーの作成

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たいが、ポリシーを仮想サーバにバインドする場合は、デフォルトのポリシーをコピーして、ポリシーの新しい名前を指定できます。構成ユーティリティを使用して、デフォルト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クライアントレスアクセスポリシーを作成する

1. 構成ユーティリティのナビゲーションペインで、[**NetScaler 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

ポリシーを作成したら、そのポリシー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の［構成］タブのナビゲーションペインで、［NetScaler Gateway ］を展開し、［仮想サーバー］をクリックします。
2. 詳細ペインで仮想サーバーを選択し、[開く] をクリックします。
3. ［NetScaler 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、リスト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、[**NetScaler 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ら、[作成] をクリックします。

NetScaler Gateway を使用した高度なクライアントレス VPN アクセス

April 1, 2024

クライアントレス VPN は、クライアントマシンに VPN クライアントアプリケーションを使用せずに、NetScaler Gateway を介して企業のイントラネットリソースへのリモートアクセスを提供する方法を認識します。クライアントレス VPN は、クライアント側の Web ブラウザを使用して、エンタープライズ 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。
高度なクライアントレス VPN ソリューションにより、クライアントレス VPN に関する次の制限が排除されます。

- 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-Respones/Web ページに存在する相対 URL を書き換えるのではなく、新しいユニークな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ー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、高度なクライアントレス VPN を設定するための前提条件を示します。

- ワイルドカードサーバー証明書 -高度なクライアントレス VPN は独自の方法で URL を書き換えます。この一意性は、ユーザーごとのすべての URL で維持されます。たとえば、Web アプリケーションが`https://webapp.customer.com`でホストされ、VPN 仮想サーバが`https://vpn.customer.com`でホストされている場合、高度なクライアントレス VPN はそれを`https://cvpneqwerty.vpn.customer.com`として書き換えます。つまり、すべての URL は VPN 仮想サーバーのサブドメインとして書き換えられます。この新しい URL では、`cvpneqwerty`を`https://webapp.customer.com`に復号化できます。文字列`cvpneqwerty`は動的であるため、SSL の場合は、ワイルドカード証明書を使用して VPN 仮想サーバをバインドする必要があります。

  サーバがでホストされている場合 `https://vpn.customer.com`、サーバ証明書には、証明書 CN または SAN（CN= 共通名、SAN= サブジェクト代替名）の一部として（vpn.customer.com および.vpn.customer.com）のエントリが必要です。この証明書をバインドするプロセスは、NetScaler Gateway でも同じです。
  注**:** ワイルドカード証明書は、1 レベル (つまり、..customer.com は許可されていません)。すでにワイルドカード証明書（*.customer.com 用）を使用して`https://vpn.customer.com`をホスティングし

ている場合、これは高度なクライアントレス VPN では機能しません。*.vpn.customer.comで新しい証明書を取得する必要があります。

- ワイルドカード **DNS** エントリ -クライアント（Web ブラウザ）は、高度なクライアントレス VPN アプリケーションの FQDN を解決する必要があります。NetScaler Gateway サーバーをセットアップするときに、vpn.customer.com を解決するために DNS エントリを構成しておく必要があります。これにより、ブラウザは vpn.customer.com を VPN 仮想サーバーの IP アドレスに解決できます。https://cvpnqwerty.vpn.customer.comのような URL を同じ IP (VPN) 仮想サーバーの IP アドレスに解決するには、vpn.customer.comのメインの新しいレコードを追加する必要があります。DNS サーバーでドメイン設定を見つけ、以前と同じ IP アドレスを持つ「*」の新しいホストレコードを追加します。ホストレコードを追加したら、https://cpvnanything.vpn.customer.comの正常な ping 応答を確認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高度なクライアントレス VPN モード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-->
```

NetScaler GUI を使用して高度なクライアントレス **VPN** アクセスを構成するには:

1. NetScaler GUI で、[構成] > [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、「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] リストで、[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] リストで、[有効] をクリックします。
   [高度なクライアントレス **VPN** モード］の一覧から［**STRICT** ］を選択すると、NetScaler ADC アプライアンスは従来のクライアントレス VPN 形式の StoreFront URL にのみ応答し、他のすべての従来のクライアントレス VPN 要求をブロックします。このオプションは、内部 Web リソースを配信するための、アプライアンスのより安全な設定を提供します。

> 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、［**NetScaler Gateway** セッションプロファイルの構成］ページの［****** クライアントエクスペリエンス］タブから、そのセッションアクションの［高度なクライアントレス **VPN** モード ******］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。
> - 高度なクライアントレス VPN 機能は、セッションレベルでも設定できます。

注意事項

高度なクライアントレス VPN 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 をシングルオクテット（クライアントレス VPN）にエンコードするため、サブドメインの関係が失われます。その結果、エンタープライズ WebApp を CORS で設定すると、高度なクライアントレス VPN 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を構成する

April 1, 2024

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。NetScaler 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るか除外する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。除外リストは、ユーザーがアクセスを許可されていない特定のリソースセットを引用しています。ユーザーは、除外リストに含まれるドメインには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を挙げています。ユーザーは、リストに表示されていないドメインには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 に接続する場合は、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、NetScaler Gateway が StoreFront および Endpoint Management の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。

NetScaler 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［NetScaler Gateway］をクリックします。
2. 詳細ペインの［はじめに］で、[NetScaler Gateway ウィザード］をクリックします。
3. [次へ] をクリックし、[クライアントレスアクセスの設定] 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. [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、次のいずれかを実行します。
   - 除外するドメインのリストを作成するには、[ドメインを除外] をクリックします。
   - 含まれるドメインのリストを作成するには、[ドメインを許可] 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. リストに追加するドメインごとにステップ 5 を繰り返し、完了したら OK をクリックします。
7. NetScaler 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、ドメインリスト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、［NetScaler 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リストを作成するには、[ドメインを除外] をクリックします。
   - 含まれるドメインのリストを作成するには、[ドメインを許可] 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ステップ 4 を繰り返し、完了したら OK をクリックします。

SharePoint 2003、**SharePoint 2007**、および **SharePoint 2013** のクライアントレス **VPN** アクセス

April 1, 2024

NetScaler Gateway は、1 つ以上の SharePoint 2003、SharePoint 2007、SharePoint 2013 サイトのコンテンツを書き換えて、Citrix Secure Access クライアントを必要とせずにユーザーがコンテンツを利用できるようにします。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 NetScaler Gateway を構成する必要があります。

NetScaler 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。

NetScaler 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。

NetScaler 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。

> 重要:
>
> クラシッククライアントレスアクセスは、SharePoint 2013 と OWA 2013 までのバージョンをサポートしています。アドバンストクライアントレスアクセスは、SharePoint 2016 と OWA 2016、およびそれ以降のバージョンをサポートします。

NetScaler 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

1. **NetScaler 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、完了したら 「**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

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. [**NetScaler Gateway**] **>** [ポリシー] に移動し、[セッション] をクリックします。
2. 詳細ペインで、[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. 「リクエストプロファイル」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 [グローバルを上書き**]** 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 [一般] を選択し、[**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、[閉じる] をクリックします。

セッションポリシーを完了したら、ユーザー、グループ、仮想サーバーに、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

SharePoint 2007 サーバーは、構成されたサーバー名をホスト名としてさまざまな URL 内の応答の一部として送信します。構成された SharePoint サーバー名が完全修飾ドメイン名（FQDN）でない場合、NetScaler Gateway は SharePoint サーバー名を使用して IP アドレスを解決できず、一部のユーザー関数はエラーメッセージ「HTTP: 1.1 Gateway Timeout」でタイムアウトします。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、ワークスペースの表示、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が含まれます。

この問題を解決するには、次のいずれかを試してください。

- 名前解決の前に SharePoint ホスト名が FQDN に変換されるように、NetScaler 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、NetScaler Gateway のローカル DNS エントリを構成します。
- すべての SharePoint サーバー名を変更して、完全修飾ドメイン名を使用します。たとえば、SharePoint の代わりに SharePoint.intranetDomain のように、

DNS サフィックスを構成する

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、[DNS] を展開し、[**DNS** サフィックス] をクリックします。
2. 詳細ペインで、[追加] をクリックします。
3. [**DNS** サフィックス] に、サフィックスとしてイントラネットドメイン名を入力し、[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。

NetScaler Gateway 上のすべての SharePoint サーバー名のローカル 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. 詳細ペインで、[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、アプライアンスに重複した A レコードが存在することはできません。

クライアントレス **VPN** アクセスパーシステント **Cookie** を有効にする

April 1, 2024

永続的なクッキーは、SharePoint サーバーでホストされている Microsoft Word、Excel、および PowerPoint ドキュメントを開いて編集するなど、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 Cookie はユーザーデバイス上に残り、HTTP 要求ごとに送信されます。NetScaler Gateway は、永続 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、Cookie を定期的に更新します。セッションが終了すると、Cookie は古くなります。

NetScaler Gateway ウィザードでは、管理者は永続クッキーをグローバルに有効にすることができます。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] はパーシステント 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、ユーザーは SharePoint に保存されている Microsoft ドキュメントを開いたり編集したりできなくなります。
- [プロンプト] 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にユーザーに求めます。

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 **VPN** アクセス用の永続クッキーを構成する

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。

パーシステント **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、［NetScaler 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、[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永続的 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パーシステント **Cookie** 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、［**NetScaler 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 [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.「リクエストプロファイル」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. [クライアントエクスペリエンス] タブで、[クライアントレスアクセス永続的 Cookie] の横にある [グローバルを上書き] 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。

モバイルデバイス用の **Citrix SSO VPN** クライアント

February 1, 2024

Citrix SSO は、モバイルデバイス（macOS、iOS、iOS）用の VPN クライアントです。Citrix SSO は、macOS、iOS、および Android で完全なモバイルデバイス管理（MDM）サポートを提供します。MDM サーバーを使用すると、管理者はデバイスレベルの VPN プロファイルとアプリごとの VPN プロファイルをリモートで構成および管理できます。
Citrix SSO は、一般的に使用される機能のほとんどもサポートしています。

参照ドキュメント

- Citrix Secure Access クライアント
- NetScaler Gateway VPN クライアントとサポートされる機能

[クライアントの選択] ページの設定

April 1, 2024

NetScaler Gateway を構成して、ユーザーに複数のログオンオプションを提供できます。クライアント選択ページを構成すると、ユーザーは 1 つの場所から次の選択肢を使用してログオンできます。

- Windows 用 Citrix Secure Access クライアント
- macOS X 用 Citrix Secure Access クライアント
- StoreFront
- Web Interface
- クライアントレスアクセス

ユーザーは、NetScaler 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 NetScaler 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と、ユーザーが受け取るログオンの選択肢を決定できます。NetScaler Gateway の構成方法に応じて、［クライアントの選択］ページには、次のログオンの選択肢を表す最大 3 つのアイコンが表示されます。

- 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 NetScaler 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。ダウンロードとインストールが完了すると、Access Interface が表示されます。NetScaler Gateway の新しいバージョン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、Windows 向け Citrix Secure Access クライアントはアプライアンス上のバージョンにサイレントにアップグレードまたはダウングレードします。ユーザーが Mac 用 Citrix Secure Access クライアントを使用して接続した場合、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にアップグレードされます。このバージョンのプラグインは、サイレントにダウングレードしません。
- Web Interface または StoreFront。ユーザーがログオンする Web インターフェイスを選択すると、[Web インターフェイス（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、ユーザーはアプリケーションとデスクトップにアクセスできます。
  注：StoreFront をクライアントの選択肢として構成した場合、アプリケーションとデスクトップは Access Interface 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、Access Interface 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。Access Interface では、ユーザーはファイル共有、Web サイトに移動したり、Outlook Web Access を使用したりできます。

Secure Browse を使用すると、ユーザーは iOS デバイスから NetScaler Gateway 経由で接続できます。Secure Browse を有効にすると、ユーザーが Secure Hub を使用してログオンすると、Secure Browse によってクライアント選択ページが無効になります。

ログオン時に [クライアントの選択] ページを表示する

クライアント選択オプションを有効にすると、NetScaler Gateway への認証が成功すると、ユーザーは 1 つの Web ページから Citrix Secure Access クライアント、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。ログオンが成功すると、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。

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 NetScaler 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 Client Security 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 が構成されている場合、選択肢ページには 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、グローバルに設定するか、セッションプロファイルとポリシーを使用して設定します。

> 重要:
>
> クライアントの選択肢を構成するときは、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、検疫され、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じように扱われるユーザーデバイス。

クライアントの選択肢オプションをグローバルに有効にする

1. GUI の［構成］タブのナビゲーションペインで［**NetScaler 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、[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肢を有効にする

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、それをユーザー、グループ、および仮想サーバーにバインドすることもできます。

1. GUI の［構成］タブのナビゲーションペインで、［**NetScaler 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、[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.「リクエストプロファイル」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［クライアントの選択］の横にある［グローバル上書き］、［クライアントの選択］、［**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 [一般] を選択し、[**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、[閉じる] をクリックします。

クライアント選択オプションの設定

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の選択を有効にすることに加えて、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、ユーザーに Citrix Secure Access クライアント、StoreFront、Web Interface のいずれか、またはクライアントレスアクセスのいずれかを使用してログオンさせたいとします。3 つのオプションとクライアントの選択肢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た式を True 値に設定した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、ユーザーの認可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

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［**NetScaler Gateway**］**>**［ユーザー管理］の順に選択し、［**AAA** グループ］をクリックします。
2. 詳細ペインで、[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、それぞれの [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。

以下の手順は、Citrix Secure Access クライアント、StoreFront、およびクライアントレスアクセスでクライアントを選択するためのセッションプロファイルの例です。

クライアント選択用のセッションプロファイルを作成する

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、［**NetScaler Gateway**］**>**［ポリシー］**>**［セッション］の順に展開します。
2. 詳細ペインで、[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「グローバル上書き」をクリックし、「ホームページを表示」をオフにします。これにより、Access Interface 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 [グローバルを上書き] をクリックし、[オフ] を選択します。
    c) [プラグインの種類] の横にある [グローバルを上書き] 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、[クライアントの選択] の横にある [グローバル上書き] をクリックし、[クライアントの選択] をクリックします。

5.「セキュリティ」タブの「デフォルト承認アクション」の横にある「グローバル上書き」をクリックし、「許可」を選択します。
6. [セキュリティ] タブの [詳細設定] をクリックします。
7. [認証グループ] で [グローバルを上書き] 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 [グローバル上書き] をクリックし、[オフ] を選択します。
    b) [**Web Interface** アドレス］の横にある［グローバル上書き］をクリックし、StoreFront の Web アドレス（など）を入力します http://ipAddress/Citrix/。
    c) [**Web Interface** ポータルモード] の横にある [グローバルを上書き] 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. [作成] をクリックし、[閉じる] をクリックします。

Citrix Secure Access クライアント for Java をクライアントの選択肢として使用する場合は、［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、傍受モードを [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 値に設定します。

StoreFront をクライアントの選択肢として使用するには、NetScaler 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ています。

> 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設定する

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［**NetScaler 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** サーバーのバインド**/**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 サーバーをさらに追加し、「**OK**」をクリックします。

STA を仮想サーバにバインドする

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、［**NetScaler Gateway** ］を展開し、［仮想サーバー］をクリックします。
2. 詳細ペインで仮想サーバーを選択して、［**Open**］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**］の下の［アクティブ］で、STA サーバーを選択し、［**OK**］をクリックします。

STA サーバーは、[公開アプリケーション] タブでも追加できます。

アクセスシナリオのフォールバックの設定

April 1, 2024

SmartAccess を使用すると、NetScaler 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判断できます。アクセスシナリオフォールバックは、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 Secure Access クライアントから 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、NetScaler Gateway へのログオン時にユーザーが別のアクセス方法を受け取るかどうかを決定する認証後ポリシーを構成します。この認証後ポリシーは、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、プロファイルは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、NetScaler 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選択が無効になっている場合、ユーザーは Web Interface または StoreFront にのみアクセスできるグループに隔離されます。
- NetScaler Gateway でクライアントレスアクセスと Web Interface または StoreFront が有効になっていて、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フォールバックします。
- 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フォールバックします。

クライアントレスアクセスが無効になっている場合は、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 インターフェイスのホームページを定義します。
- クライアントの選択肢を無効にします。
- ユーザーデバイスがクライアントセキュリティチェックに失敗すると、ユーザーは、Web Interface または StoreFront および公開アプリケーションへのアクセスのみを許可する検疫グループに配置されます。

アクセスシナリオフォールバックのポリシーの作成

アクセスシナリオのフォールバック用に NetScaler Gateway を構成するには、次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が配置される検疫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されるグローバル 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、その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。

- クライアント選択またはアクセスシナリオフォールバックを使用するには、すべてのユーザーに 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した場合、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、NetScaler Gateway 10.1、ビルド 120.1316.e で削除されました
- 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。ユーザーは引き続き、Citrix Secure Access クライアントまたは Citrix Workspace アプリを使用して、Web Interface または StoreFront にログオンできます。
  注：クライアントの選択を有効にする場合は、検疫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隔離されます。
- 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配置された場合、検疫グループにバインドされたポリシーは、検疫グループにバインドされたポリシーと同等またはそれ以下の優先度番号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です。
- Access Interface と、Web Interface または StoreFront に異なる 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 Secure Access クライアントでは Access Interface ホームページが優先され、Web Interface ユーザーには Web Interface 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

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、［**NetScaler 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、[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、ユーザーが所属する可能性のあ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セキュリティスキャンに合格しても、ユーザーは隔離されます。

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 NetScaler Gateway を構成します。

ユーザー接続を検疫するための設定を構成する

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、［NetScaler 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、[グローバル設定の変更] をクリックします。
3. ［グローバル **NetScaler 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［オフ］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検疫グループにバインドします。

アクセス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

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、**[NetScaler 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.「リクエストプロファイル」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] タブで、[**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 [一般] を選択し、[**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、 [閉じる] をクリックします。

セッションポリシーを作成したら、ポリシーを検疫グループにバインドします。

セッションポリシーを検疫グループにバインドします

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、［**NetScaler 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. [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。

NetScaler 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

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、［NetScaler 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、[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 [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。システム式の構成の詳細については、「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構成](/ja-jp/netscaler-gateway/13-1/vpn-user-config/endpoint-policies/ng-endpoint-expressions-compound-con.html)」を参照してください
5.「検疫グループ」で、グループ手順で設定したグループを選択し、「**OK**」をクリックします。

Citrix Secure Access クライアントの接続を設定する

April 1, 2024

ユーザーデバイス接続を構成するには、内部ネットワークでユーザーが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されるドメインを定義する。
- アドレスプール (イントラネット IP) を含む、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の設定。
- クライアント代行受信の設定。
- 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設定。
- NetScaler Gateway を介して接続するためのユーザーソフトウェアの構成。
- モバイルデバイスのアクセスを設定する。

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、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。
>
> REG_DWORD タイプのレジストリ「HKLM\ ソフトウェア\ Citrix\ Secure Access Client\ DisableGA」を 1 に設定します。

ユーザセッション数の設定

April 1, 2024

特定の時点で NetScaler Gateway に接続できるユーザーの最大数を、グローバルレベルまたは仮想サーバーレベルごとに構成できます。アプライアンスに接続するユーザーの数が構成した値を超えると、NetScaler Gateway でセッションは作成されません。ユーザー数が許可した数を超えると、ユーザーはエラーメッセージを受け取ります。

グローバルユーザー制限を設定するには

ユーザー制限をグローバルに設定すると、この制限は、システム上の異なる仮想サーバーとのセッションを確立するすべてのユーザーに適用されます。ユーザーセッション数が設定した値に達すると、NetScaler Gateway に存在する仮想サーバーで新しいセッションを確立できなくなります。

NetScaler 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、［NetScaler Gateway］を展開し、［グローバル設定］をクリックします。
2. 詳細ウィンドウの [設定] で、[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。

仮想サーバーあたり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にユーザ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と、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、［NetScaler Gateway ］を展開し、［仮想サーバー］をクリックします。
2. 詳細ペイン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」にユーザー数を入力し、「OK」をクリックします。

タイムアウト設定を構成する

April 1, 2024

指定した分数の間接続にアクティビティがない場合、強制的に切断するように NetScaler Gateway を構成できます。セッションがタイムアウト (切断) する 1 分前に、ユーザーはセッションの終了を示すアラートを受信します。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。

次のタイムアウトオプションを使用できます。

- 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 NetScaler Gateway によってセッションが切断されます。タイムアウト間隔が過ぎても接続が切断されないようにする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 Secure Access クライアント、Citrix Workspace アプリ、Secure Hub、または Web ブラウザーを介して接続するユーザーに適用されます。最小値は 1 で、最大値は 65535 です。
- 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いと、NetScaler Gateway によってセッションが切断されます。この設定は、Citrix Secure Access クライアント、Citrix Workspace アプリ、Citrix Secure Hub、または Web ブラウザーを介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。最小値は 1 で、最大値は 65535 です。
- アイドルセッションのタイムアウト。指定した時間間隔でマウス、キーボード、タッチなどによるユーザー操作がない場合に、Citrix Secure Access クライアントがアイドルセッションを終了するまでの時間です。この設定は、Citrix Secure Access クライアントに接続するユーザーにのみ適用されます。最小値は 1 で、最大値は 9999 です。

1 ～65536 の値を入力して、タイムアウト間隔の分を指定することで、任意のタイムアウト設定を有効にできます。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、ユーザーデバイス接続は閉じられます。

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、その設定はすべてのユーザセッションに適用されます。

> 注:
>
> - Always On（サービスモードまたはユーザモード）では、VPN クライアントはすべてのタイムアウトを無視します。強制タイムアウトとセッションタイムアウトの決定は NetScaler ADC アプライアンスで行われるため、これらのタイムアウトは意図したとおりに機能します。このようなタイムアウトが発生すると、VPN プラグインは自動認証を実行しようとします。
>
>   Always On では、ユーザデバイスは常に VPN トンネルを介して接続する必要があるため、強制タイムアウトまたはクライアントアイドルタイムアウトを設定しないでください。ただし、セッションタイムアウトを設定して、古いセッションを取り除くことができます。
>
> - 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電子メールサーバーに自動的に送信します。アイドルセッションタイムアウトとセッションタイムアウトを構成して、ユーザーデバイス上で無人状態のセッションが妥当な時間内にタイムアウトするようにすることをお勧めします。

強制タイムアウトを構成する

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 Secure Access クライアント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、またはセッションポリシーの一部として設定できます。

グローバル強制タイムアウトを構成する

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、［NetScaler 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、[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、[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、接続が切断される予定であることをユーザーに警告するまでの分数を入力し、［**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

強制タイムアウトを受信す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の［構成］タブのナビゲーションペインで、［NetScaler 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.「リクエストプロファイル」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. [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 [グローバルオーバーライド] 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をユーザーに警告する時間を分単位で入力します。［**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 [一般] を選択し、[**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、 [閉じる] をクリックします。

セッションタイムアウトまたはアイドルタイムアウトの設定

NetScaler GUI 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構成したり、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。

> 注**:**
>
> グローバル設定を明示的に上書きせず、[クライアントエクスペリエンス**] > [**セッションタイムアウト **(**分**)**] でセッションタイムアウトを設定すると、再ログインを必要とする認証ループが発生する可能性があります。これは、デフォルトのセッションタイムアウトが 30 分であっても発生します。

GUI 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をグローバルに設定するには

1. ［構成］タブのナビゲーションペインで、［**NetScaler 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、[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。

GUI を使用して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］タブのナビゲーションペインで［**NetScaler 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. ［**NetScaler Gateway** セッションポリシーとプロファイル］ページで、［セッションプロファイル］、［追加］の順にクリックします。
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 [グローバルを上書き] をクリックし、分数を入力して [作成] をクリックします。
   - [クライアントのアイドルタイムアウト **(**分**)**] の横にある [グローバルを上書き] をクリックし、分数を入力して [作成] をクリックします。
5. a) ［**NetScaler Gateway** セッションポリシーとプロファイル］ページで、［セッションポリシー］、［追加］の順にクリックします。
6. ［**NetScaler Gateway** セッションの作成］ポリシーで、
   - [**Name**] に、ポリシーの名前を入力します。
   - [プロファイル] で、規則の条件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を指定するプロファイルを選択します。
   - [詳細ポリシー] を選択します。
   - [**Expression**] フィールドに、ポリシーに一致するトラフィックを指定して、式または名前付き式の名前を追加します。
   - [作成] をクリックし、[閉じる] をクリックします。

内部ネットワークリソースに接続する

April 1, 2024

NetScaler Gateway を構成して、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することができます。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 NetScaler Gateway に送信され、承認ポリシーによって、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されるかどうかが決定されます。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、NetScaler Gateway に送信されます。イントラネットアプリケーションを使用して、NetScaler Gateway がインターセプトする IP アドレスを構成します。

Windows 向け Citrix Secure Access クライアントを使用している場合は、インターセプトモードを透明に設定してください。Java 向け Citrix Secure Access クライアント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てください。代行受信モードをトランスペアレントに設定すると、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

代行受信モードをプロキシに設定すると、宛先 IP アドレス、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

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、[NetScaler Gateway]、[リソース]、[イントラネットアプリケーション］の順に展開します。
2. 詳細ペインで、[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設定

April 1, 2024

分割トンネリングを有効にすると、Citrix Secure Access クライアントが不必要なネットワークトラフィックを NetScaler Gateway に送信するのを防ぐことができます。

分割トンネリングを有効にしない場合、Citrix Secure Access クライアントはユーザーデバイスから発信されるすべてのネットワークトラフィックをキャプチャし、そのトラフィックを VPN トンネルを介して NetScaler Gateway に送信します。

分割トンネリングを有効にすると、Citrix Secure Access クライアントは、NetScaler Gateway で保護されているネットワーク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 Secure Access クライアントは、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 NetScaler Gateway に送信しません。

Citrix Secure Access クライアントが起動すると、NetScaler 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 Secure Access クライアントは、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 Secure Access クライアントは VPN トンネルを介して NetScaler 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傍受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は、分割トンネリングを構成する必要はありません。

NetScaler Gateway は、NetScaler Gateway が傍受しないネットワークトラフィックを定義するリバース分割トンネリングもサポートしています。分割トンネリングをリバースに設定すると、イントラネットアプリケーションは、NetScaler 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。リバース分割トンネリングを有効にすると、内部 IP アドレスに向けられたすべてのネットワークトラフィックは VPN トンネルをバイパスし、他のトラフィックは NetScaler Gateway を経由します。リバース分割トンネリングを使用して、すべての非ローカル LAN トラフィックをログに記録できます。たとえば、ユーザーが自宅のワイヤレスネットワークを使用して Citrix Secure Access クライアントでログオンしている場合、NetScaler Gateway はワイヤレスネットワーク内のプリンターや別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、「クライアント代行受信の構成」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、［**NetScaler 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［グローバルオーバーライド］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

NetScaler 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オンに設定されており、NetScaler Gateway 経由でネットワークトラフィックを送信するようにイントラネットアプリケーションを構成していない。NetScaler Gateway にこの種類の構成がある場合、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。

承認ポリシーで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 NetScaler Gateway を介して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 Secure Access クライアントはトラフィックを NetScaler Gateway に送信しますが、リソースへのアクセスは拒否されます。

分割トンネリングオプションの詳細については、「分割トンネリングオプション」を参照してください。

クライアント傍受を構成する

April 1, 2024

NetScaler Gateway のユーザー接続の傍受ルールは、イントラネットアプリケーションを使用して構成します。デフォルトでは、アプライアンス上でシステム 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、クライアント傍受が発生する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。

GUI 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。

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、イントラネットアプリケーションで Endpoint Management および Exchange IP アドレスを構成する必要はありません。

分割トンネリング設定の詳細については、「分割トンネリングの設定」を参照してください。

Citrix Secure Access クライアント用のイントラネットアプリケーションの構成

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、以下を定義します:

- 1 つの IP アドレス
- IP アドレスの範囲
- ホスト名

NetScaler Gateway でイントラネットアプリケーションを定義すると、Windows 向け Citrix Secure Access クライアントは、リソース宛てのユーザートラフィックをインターセプトし、NetScaler Gateway を介して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ときは、次の点を考慮してください:

- 分割トンネルがオンの場合、
  - イントラネットアプリケーションを構成します。
  - イントラネットアプリケーションをすべての認証、承認、および監査グループに割り当てます。
- 分割トンネルがオフの場合、
  - すべてのトラフィックは VPN トンネルを傍受します。
  - イントラネットアプリケーションを構成する必要はありません。
- 分割トンネルが逆の場合、
  - イントラネットアプリケーションを構成します。イントラネットアプリケーションで指定されていないトラフィックは、VPN トンネルを通過します。
  - VPN から除外するイントラネットアプリケーションをすべての認証、承認、および監査グループに割り当てます。

> 重要:
>
> 分割トンネルの設定に関係なく、インターセプションは **TRANSPARENT** に設定する必要があります。

注:

- 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インターセプトモードを選択する必要があります。
- イントラネットアプリケーションをプロキシインターセプトとトランスペアレントインターセプトの両方に設定することはできません。

1 つの IP アドレ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

1. [構成] タブのナビゲーションペインで、[**NetScaler 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. 詳細ペインで、[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、「**TRANSPARENT**」を選択します。
5. [宛先タイプ] 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 アドレス範囲を設定するには

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設定できます。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］タブのナビゲーションペインで、［**NetScaler 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. 詳細ペインで、[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、「**TRANSPARENT**」を選択します。
6. [送信先の種類] で、[**IP** アドレスの範囲] を選択します。
7. [**IP Start]** に開始 IP アドレスを入力し、[IP End] 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］タブのナビゲーションペインで、［**NetScaler 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. 詳細ペインで、[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、「**TRANSPARENT**」を選択します。
5. [送信先のタイプ] で、[ホスト名] を選択します。
6. [プロトコル] で [任意] を選択し、[作成]、[閉じる] の順にクリックします。

> 重要:
>
> - リリース 13.0 ビルド 36.27 以降では、Windows VPN プラグインは、分割トンネリングのホスト名（FQDN）ベースのルールをサポートします。NetScaler ADC アプライアンスと Windows VPN プラグインの両方をリリース 13.0 ビルド 36.27 以降にアップグレードする必要があります。
> - ワイルドカードホスト名もサポートされています。たとえば、ホスト名が「*.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。
> - 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 または REVERSE に設定されている場合にのみ機能します。

ネームサービス解決を構成する

April 1, 2024

NetScaler Gateway のインストール中に、NetScaler 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その他の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。NetScaler 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 ルックアップの優先順位、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。

NetScaler Gateway ウィザードを実行すると、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、NetScaler Gateway にさらに DNS サーバーと WINS サーバーを追加できます。その後、ウィザードで最初に構成した名前解決サーバーとは異なる名前解決サーバーに接続するようにユーザーおよびグループに指示できます。

NetScaler Gateway で追加の DNS サーバーを構成する前に、名前解決用の 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** サーバーまたは **WINS** サーバーを追加する

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、［NetScaler 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 Server 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。

> 重要:
>
> VPN セッションプロファイルにアタッチされたアドレス指定不能 DNS 仮想サーバーでは、レスポンダーポリシーが評価されません。

ユーザー接続のプロキシサポートを有効にする

April 1, 2024

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。NetScaler 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、NetScaler Gateway の設定を指定します。NetScaler Gateway 上のプロキシサーバーで

使用される 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その後のすべての接続のフォワードプロキシとして使用されます。

プロキシ設定

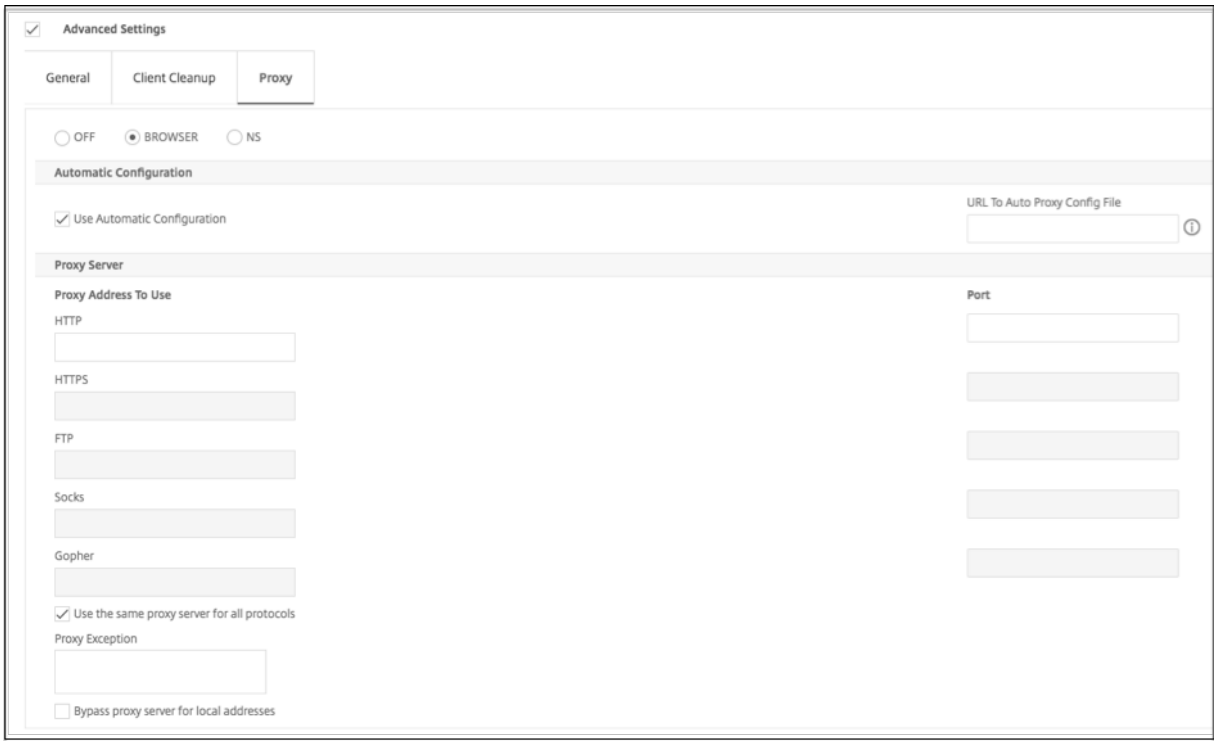
プロキシ設定は、ブラウザーまたは NetScaler ADC アプライアンスで構成できます。ブラウザーまたはアプライアンスでプロキシ設定を構成するには、［グローバル **NetScaler Gateway** 設定］**>**［クライアントエクスペリエンス］タブ **>**［詳細設定］**>**［プロキシ］の順に移動し、必要に応じて［ブラウザ］または［**NS** ］を選択します。

- ブラウザ**:** ブラウザでプロキシ設定を構成する場合、自動プロキシ設定ファイルへのリンクを提供することで、自動設定オプションを使用できます。自動構成は、手動設定を上書きする場合があります。

  また、「ブラウザ」を選択すると、プロキシ例外オプションを選択して、以前に構成したプロキシをバイパスできます。

  注**:** ブラウザプロキシの設定に関する機能は、クライアントの種類によって異なります。詳しくは、「NetScaler Gateway VPN クライアントとサポートされる機能」を参照してください。

- **NS**: NetScaler ADC アプライアンスでプロキシ設定を構成する場合、自動構成オプションは使用できません。アプライアンスでプロキシ設定を構成する場合、以前に構成したプロキシをバイパスすることはできません。



ユーザー接続のプロキシサポートを構成するには

1. ナビゲーションペインで、「**NetScaler 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、[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、[ブラウザ**]** 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:
>
> - [**NS**] を選択した場合は、セキュリティで保護された HTTP 接続と保護されていない 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。
> - NetScaler Gateway でプロキシサポートを有効にしたら、プロトコルに対応するプロキシサーバーのユーザーデバイスの構成の詳細を指定します。
>
>   プロキシサポートを有効にすると、NetScaler Gateway はプロキシサーバーの詳細をクライアントの Web ブラウザーに送信し、ブラウザーのプロキシ構成を変更します。
>
>   – When the user device connects to NetScaler Gateway, the user device can communicate with the proxy server directly for connection to the user’s network.
>   – When the user device disconnects from NetScaler Gateway, the proxy settings are restored to the previous default settings, that was present before connecting to the VPN plug-in.

NetScaler 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

1 つのプロキシサーバーを構成して、NetScaler Gateway が使用するすべてのプロトコルをサポートできます。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が提供されます。

1. ナビゲーションペインで、「**NetScaler 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、[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、[ブラウザ**]** 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［オン］に設定すると、プロキシ設定がユーザー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。

NetScaler 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伝達されないため、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。

NetScaler Gateway をプロキシサーバーとして構成するには

NetScaler Gateway をプロキシサーバーとして構成する場合、セキュリティで保護されていないセキュアな HTTP のみがサポートされるプロトコルです。

1. ナビゲーションペインで、「**NetScaler 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、[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、[**NS**] 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

April 1, 2024

状況によっては、Citrix Secure Access クライアントに接続するユーザーが NetScaler Gateway に固有の IP アドレスが必要になることがあります。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 プーリングとも呼ばれる）を有効にすると、NetScaler Gateway は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た一意の IP アドレスを使用する必要がある場合があります。

- ボイスオーバー IP
- アクティブ FTP
- インスタントメッセージング
- 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)

NetScaler 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、NetScaler Gateway を構成できます。固定 IP アドレスをユーザーに割り当てることも、IP アドレスの範囲をグループ、仮想サーバー、またはシステムにグローバルに割り当てることもできます。

NetScaler 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。内部ネットワークの IP アドレスは、リモートユーザをアドレス指定することができます。IP アドレスの範囲を使用することを選択した場合、システムはオンデマンドでその範囲の 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ときは、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確実に行うには、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 アドレスが Network Address Translation（NAT; ネットワークアドレス変換）デバイスを介して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、NetScaler 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ー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、バインドレベル内の複数のエンティティにバインドできません。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。
- NetScaler 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。

  - ユーザーのダイレクトバインディング
  - グループ割り当てアドレスプール
  - 仮想サーバ割り当てアドレスプール
  - グローバルアドレス範囲

- 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、下位レベルのエンティティにさら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には、次の範囲をバインドできます。

  - 仮想サーバー
  - グループ
  - ユーザー

- バインドされた仮想サーバーのアドレス範囲には、次のサブセットをバインドできます。

  - 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、そのアドレスはユーザーの次回のログオン用に予約されます。アドレスが使い果たされると、NetScaler Gateway は、NetScaler Gateway から最も長くログオフしたユーザーの IP アドレスを再利用します。

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、NetScaler 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、NetScaler Gateway でマップされた IP アドレスをイントラネット IP アドレスとして使用できるようにします。

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て、マシンのホスト名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。

DNS 登録を正常に行うには、次の`nsapimgr`ノブが設定されていることを確認してください。また、権限のある DNS サーバーが「非セキュア」DNS 更新を許可するように設定されていることも確認してください。

- **`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状態で VPN クライアントが DNS/WINS 要求をインターセプトすると、対応する「GET/DNS」HTTP 要求をトンネル経由で 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 NetScaler Gateway 仮想サーバーに透過的に転送します。この場合、DNS パケットは VPN トンネルを介してそのまま 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返される 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 サーバーに到達するため、NetScaler Gateway サーバーは DNS サーバーに TCP-DNS クエリを行います。
- **nsapimgr-ys enable_vpn_dnstruncate_fix=1**: 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、（受信 TCP-DNS パケットに元々存在していた DNS サーバー IP に送信しようとするのではなく）NetScaler Gateway で構成された DNS サーバーに上書きします。UDP DNS 要求の場合、デフォルトでは、DNS 解決用に設定された DNS サーバが使用されます。Windows 用 NetScaler Gateway プラグインは、セキュアな DNS アップデートと非セキュアな DNS 21.7.1.1 以降のビルドでは、セキュア DNS 更新サポートがデフォルトで存在します。

  Windows プラグインのセキュア DNS アップデートは、デフォルトでは無効になっています。有効にするには、`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access`に REG_DWORD 型の値を作成して 1 に設定します。

  - 値を 1 に設定すると、VPN プラグインはセキュリティで保護されていない DNS アップデートを最初に試みます。セキュリティで保護されていない DNS の更新が失敗した場合、VPN プラグインは安全な DNS の更新を試みます。
  - セキュリティで保護された DNS アップデートのみを試すには、値を 2 に設定します。

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。

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

1. 構成ユーティリティのナビゲーションペインで、[**NetScaler Gateway**] を展開し、次のいずれかの操作を行います。
   - 「NetScaler Gateway ユーザー管理」を展開し、「**AAA** ユーザー」をクリックします。
   - 「**NetScaler Gateway** 」>「ユーザー管理」を展開し、「**AAA** グループ」をクリックします。
   - 「**NetScaler 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 アドレスごとに手順 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

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、[**NetScaler 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 NetScaler 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] をクリックします。
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**]**、 [挿入] の順にクリックします。
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 IP アドレスごとに手順 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

セッションポリシーまたはグローバル NetScaler 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 NetScaler Gateway に割り当てる一方で、特定のユーザーグループのイントラネット IP アドレスの使用を無効にすることができます。

アドレスプールは、次の 3 つの方法のいずれかでセッションポリシーを使用して設定できます:

- **`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。使用可能なイントラネット IP アドレスをすべて使用したユーザーには、[ログオンの転送] 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、マッピング 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 IP アドレスが設定されていない場合、SNIP が使用されます。

アドレスプールを定義するには

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、［NetScaler 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 [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. 「リクエストプロファイル」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. [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 [グローバルを上書き] 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 [**Override Global**] 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、式を作成します。[作成**]** をクリックし、 [閉じる] をクリックします。

「ログオンを転送」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、NetScaler Gateway との別のセッションを確立しようとすると、［ログオン転送］ページが表示されます。ログオン転送ページでは、ユーザーは既存の NetScaler 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。

ログオンの転送ページは、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かった場合にも使用できます。例:

- ユーザーには静的イントラネット IP アドレスが割り当てられ、既存の NetScaler Gateway セッションがあります。ユーザーが別のデバイスから 2 つ目のセッションを確立しようとすると、「ログオンの転送」ページが表示され、ユーザー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、NetScaler Gateway を介して 5 つのセッションがあります。ユーザーが 6 回目のセッションを確立しようとすると、「ログオンの転送」ページが表示され、ユーザーは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を選択できます。

> メモ:
>
> - ユーザーに IP アドレスが割り当てられていないため、新しいセッションを確立できない場合、エラーメッセージが表示されます。
> - Citrix Secure Access for Android 23.12.1 以降のバージョンでは、NetScaler Gateway のログオン転送機能が常時接続 VPN モードでサポートされています。

Transfer Logon ページは、アドレスプールを設定してスピルオーバーを無効にした場合にのみ表示されます。

DNS サフィックスを構成する

ユーザーが NetScaler 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 NetScaler Gateway 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たときにユーザー名に追加するように DNS サフィックスを構成できます。これにより、ユーザは DNS 名で参照され、IP アドレスよりも覚えやすくなります。ユーザーが NetScaler 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の［構成］タブのナビゲーションペインで、［NetScaler 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 [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.「リクエストプロファイル」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」の横にある「グローバルを上書き」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 1, 2024

NetScaler 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 Secure Access クライアントに接続すると、NetScaler 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。

NetScaler Gateway は以下の VoIP ソフトフォンをサポートしています。

- Cisco Softphone
- Avaya IP Softphone

セキュアトンネリングは、IP PBX と、ユーザデバイス上で実行されているソフトフォンソフトウェアとの間でサポートされています。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 Secure Access クライアント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を介して送信される場合、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た発信コール
- 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します。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 Softphone Communication 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、「アドレスプールの構成」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、透過的な代行受信を有効にする必要があります。

Access Interface の設定

April 1, 2024

NetScaler Gateway には、ユーザーがログオンした後に表示され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 Access Interface 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設定します。

Access Interface 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 Access Interface の左側のパネルで 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。

Access Interface は、内部および外部の Web サイトへのリンク、および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。Access Interface は、次の方法でカスタマイズできます。

- Access Interface の変更。
- Access Interface リンクの作成。

ユーザーは、Web サイトやファイル共有への独自のリンクを追加して、Access Interface をカスタマイズすることもできます。ユーザーは、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、Access Interface 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、NetScaler 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 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。

Access Interface の変更

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したい場合があります。これを行うには、NetScaler 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。

カスタマイズし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 [NetScaler Gateway] をクリックします。
2. 詳細ペインの [**Access Interface** のカスタマイズ**]** で、**[**Access Interface** 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. NetScaler 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

Access Interface をカスタムホームページに置き換える

グローバル設定またはセッションポリシーおよび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て、デフォルト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。ポリシーを構成したら、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。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 Access Interface 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構成する

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、[**NetScaler 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、[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のカスタムホームページの設定

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、[NetScaler 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 [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. 「リクエストプロファイル」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 [グローバルを上書き] 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 [一般] を選択し、[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、[閉じる**]** をクリックします。

Web リンクの作成と適用

April 1, 2024

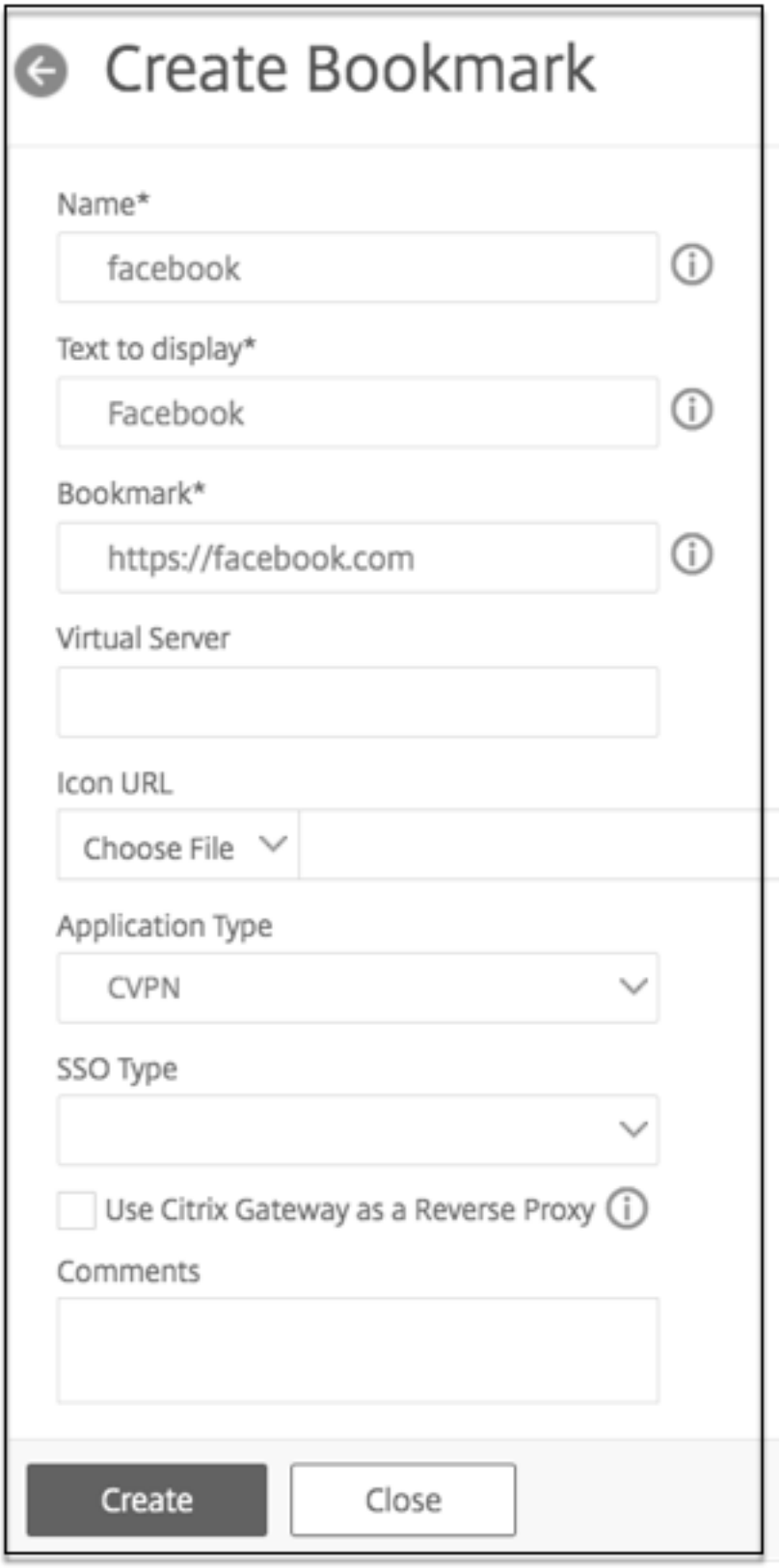
Access Interface は、ユーザが使用できる内部リソースへのリンクのセットを表示するように設定できます。これらのリンクを作成するには、最初にリンクをリソースとして定義する必要があります。次に、それらをユーザー、グループ、仮想サーバー、またはグローバルにバインドして、Access Interface でアクティブにします。作成したリンクは、[エンタープライズ ****Web** サイト] の下の [Web サイト **] ウィンドウに表示されます。

> 重要:
>
> NetScaler ADC リリース 13.0 ビルド 64.xx 以降では、NetScaler Gateway を介したファイル共有はサポートされていません。

エンタープライズブックマークの作成

セッションポリシーで **Access Interface** 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、［**NetScaler Gateway**］**>** ［リソース］の順に展開し、［ポータルブックマーク］ をクリックします。
2. 詳細ペインで、[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。説明は **Access Interface** に表示されます。
5. [ブックマーク] に、アプリケーションの Web アドレスを入力します。
6. [仮想サーバー] に、関連する負荷分散/コンテンツスイッチング仮想サーバーの名前を入力します。この情報は入力しなくても構いません。
7. **Icon URL** では、アップロードされたアイコンは、デフォルトテーマを除くすべてのテーマでサポートされています。推奨最大サイズは 70 x 70 ピクセルです。透明な画像を使用することをおすすめします。この情報は入力しなくても構いません。
8. [アプリケーションタイプ] で、URL が表すアプリケーションのタイプ（VPN、クライアントレス VPN、または SaaS）を選択します。この情報は入力しなくても構いません。
9. [**SSO** タイプ] で、ブックマークに設定する SSO タイプを選択します。SSO を設定すると、ユーザーはその後のログオン時に資格情報を入力しなくてもアプリケーションにアクセスできます。次の SSO タイプがサポートされています。

    - Unified Gateway: この SSO 設定により、単一の URL からアプリケーションの複数のリソースへの安全なリモートアクセスが可能になります。
    - 自己認証：この SSO 構成では、NetScaler Gateway ユーザーはアプリケーションにアクセスするためのログイン資格情報を入力するよう求められます。
    - SAML ベースの認証：この SSO 構成では、NetScaler Gateway は IdP を使用してユーザーの詳細を検証し、SAML アサーションを生成して SP に送信します。検証に合格すると、SSO は成功します。

    > 注:
    >
    > 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 NetScaler Gateway を経由するようにできます。たとえば、Googleのブックマークを追加したとします。「**NetScaler 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選択します。このチェックボックスをオンにすると、Web サイト要求はユーザーデバイスから NetScaler Gateway に送信され、次に Web サイトに送信されます。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た場合にのみ使用できます。

10. [作成] をクリックし、[閉じる] をクリックします。

Access Interface リンクをバインドするには

Access Interface リンクは、次の場所にバインドできます。

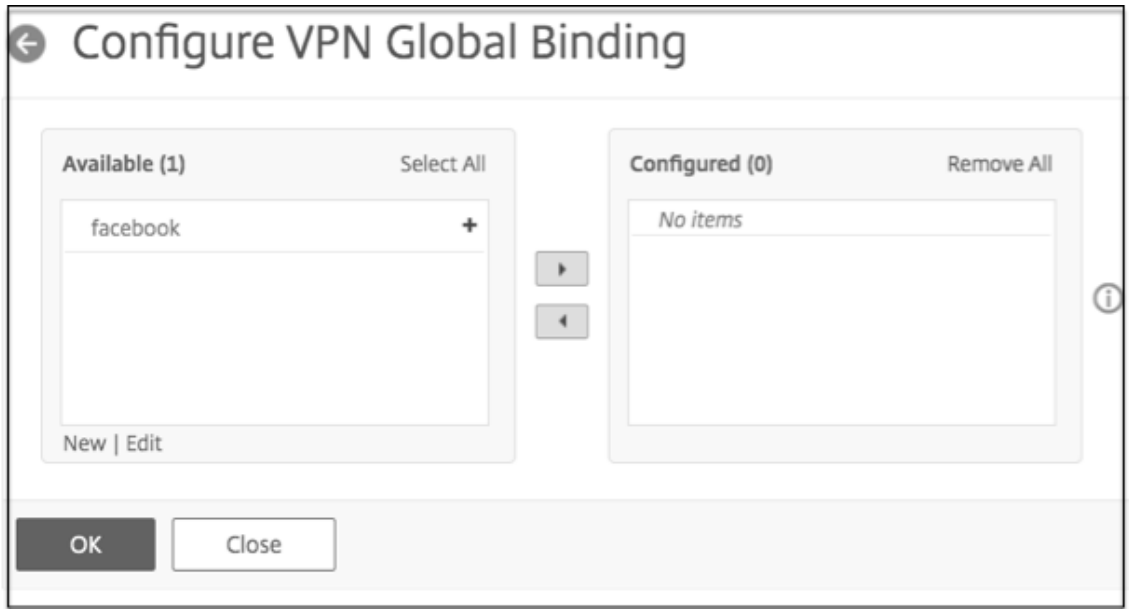
- ユーザー
- グループ
- 仮想サーバー

構成を保存すると、[ホーム] タブの [アクセスインタフェース] でユーザーが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。

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:
   - 「**NetScaler Gateway** ユーザー管理」を展開し、「**AAA** ユーザー」をクリックします。
   - ［**NetScaler Gateway** ユーザー管理］を展開し、［**AAA** グループ］をクリックします。
   - 「**NetScaler 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。
   - 仮想サーバーを選択し、[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ブックマークを［構成済みのブックマーク］の下に移動してから、［**OK**］をクリックします。

GUI を使用してブックマークをグローバルにバインドするには

1. ［構成］タブのナビゲーションペインで、［**NetScaler 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、**NetScaler Gateway** ポータルページでアクセス可能にする **HTTP** および **Windows** ファイル共有アプリケーションへのリンクの作成をクリックします。



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 つ以上のブックマークを選択し、右矢印をクリックしてブックマークを [構成済み] に移動し、次に [**OK**] の下に移動します。

CLI を使用してエンタープライズブックマークを追加するには

コマンドプロンプトで入力します:

```
add vpn url <urlName> <linkName> <actualURL>  [-ssotype <ssotype>]
<!--NeedCopy-->
```

例:

Web ブックマーク

```
add vpn url google google "https://www.google.com"
<!--NeedCopy-->
```

CLI を使用してエンタープライズブックマークをバインドするには

Enterprise ブックマークは、ユーザー、グループ、仮想サーバー、およびグローバルレベルにバインドできます。

```
bind aaa user <userName> -urlName <string>
bind aaa group <groupName> -urlName <string>
bind vpn vserver <vserverName> -urlName <string>
bind vpn global  - urlName <string>
<!--NeedCopy-->
```

例:

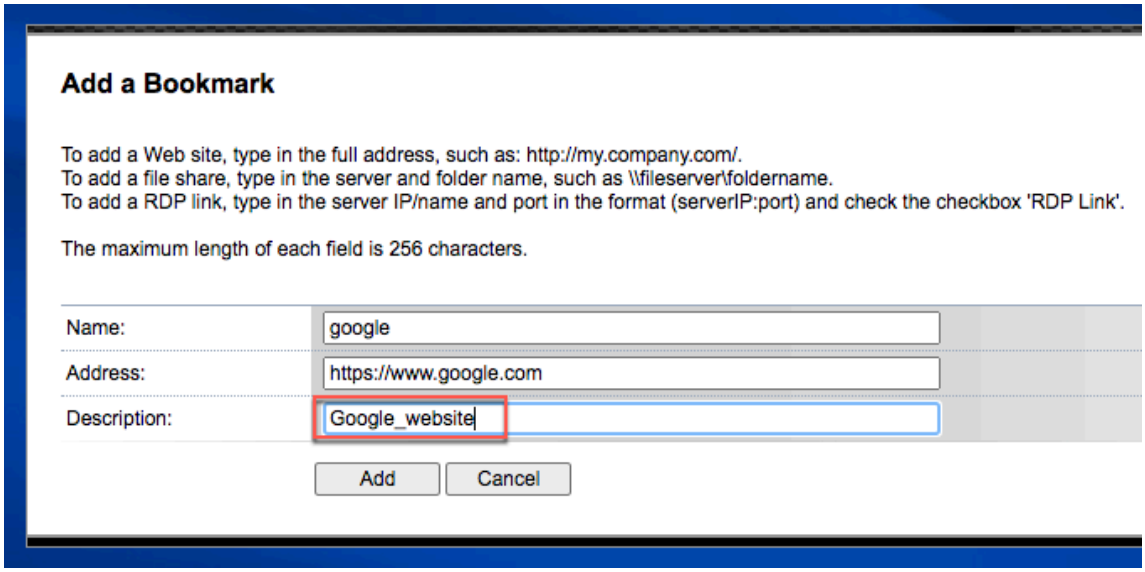
```
bind vpn global -urlName google
<!--NeedCopy-->
```

個人用ブックマークの作成

個人用 Web サイトは、VPN 仮想サーバーからのみ作成できます。個人用ブックマークを追加するための NetScaler Gateway 管理 GUI はありません。

1. VPN 仮想サーバーにログオンします。
2. [ネットワークアクセス] または [クライアントレスアクセス] をクリックして、ブックマークを追加します。
3. [追加] をクリックします。

4. Web サイト名、住所、説明などのブックマークの詳細を入力します。



5. [追加] をクリックします。

追加した Web サイトは、それぞれのタブの下に表示されます。

ブックマークでユーザー名トークンを構成する

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 を構成できます。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%\ というフォルダに、Jack という名前の従業員用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\\ EmployeeServer\ Jack\ にマップされます。ブックマークでユーザー名トークンを構成するときは、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は、プライマリ認証タイプのユーザー名が%username% トークンを置き換えるために使用されます。
- 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% トークンを置き換えます。

トラフィックポリシー

April 1, 2024

トラフィックポリシーを使用すると、ユーザー接続の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性の高いアプリケーションのタイムアウトを短縮します。
- 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ます。[TCP] を選択した場合は、特定のアプリケーションの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 Secure Access クライアントトラフィックに他の HTTP 機能を使用したい状況を特定します。
- ファイルタイプの関連付けで使用されるファイル名拡張子の定義。

トラフィックポリシーを作成する

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 Human Resources 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、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。

アプリケーションに対する 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、アクションに 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表現の例

トラフィックポリシーの表現例を次に示します。

- `add vpn trafficPolicy trafPol1 "HTTP.REQ.URL.CONTAINS(\"/Citrix/\")|| HTTP.REQ.URL.CONTAINS(\"10.102.\")")"trafAct1`

- `add vpn trafficPolicy trafPol2 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv\")|| HTTP.REQ.URL.CONTAINS(\"homePage\"))"trafAct2`
- `add vpn trafficPolicy trafPol3 true trafAct3`

GUI を使用したトラフィックポリシーの設定

1. [**NetScaler Gateway**] **>** [ポリシー] の順に展開し、[トラ
2. 詳細ペインの [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. 「リクエストプロファイル」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. [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を構成できず、この設定はプロファイルダイアログボックスで無効になります。
7. [**AppTimeout (**分**)**] に、分数を入力します。この設定では、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を制限します。
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 [オン] 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。詳細については、「
   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. ファイルの種類の関連付けを指定するには、[ファイルの種類の関連付け] で [オン] 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、Citrix SD-WAN で［オン］を選択し、［作成］、［閉じる］の順にクリックします。
11. アプライアンスで KCD を設定する場合は、[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 の構成について詳しくは、「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. [トラフィックポリシーの作成（Create Traffic Policy）] ダイアログボックスで、式を作成または追加し、[作成（**Create**）**]** をクリックし、 [閉じる（**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

フォームベースのシングルサインオンを使用すると、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 1 回ログオンできます。NetScaler 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

ーはパスワードをもう一度入力しなくても、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。詳細については、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の設定

1. [**NetScaler Gateway] > [**ポリシー**]** を展開し、 [トラフィック] をクリックします。
2. 詳細ペインで、[**Form 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、完了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] 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] 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** 成功ルールで、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説明する式を作成します。このフィールドの下にある [プレフィックス]、[追加]、および [演算子] ボタンを使用して、エクスプレッション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. [名前と値のペア] に、ユーザー名フィールドの値、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、名前 1= 値 1& 名前 2= 値 2 のようにアンパサンド (&) で区切ります。
9. [レスポンスサイズ] に、完全なレスポンスサイズに許容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/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される HTTP メソッドを選択します。デフォルトは Get です。
12. [作成**]** をクリックし、 [閉じる] をクリックします。

SAML シングルサインオンの設定

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。NetScaler 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の設定

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、［**NetScaler 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. 詳細ペインで、［Add］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. [リレーステートルール] 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) リストから選択して、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、[オン] または [オフ] を選択
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をバインドする

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 NetScaler Gateway Global にバインドできます。構成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。

GUI 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

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、［**NetScaler 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、[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. [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

いずれかの構成ユーティリティを使用して、NetScaler Gateway からトラフィックポリシーを削除できます。構成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、ポリシーがユーザー、グループ、または仮想サーバレベルにバインドされている場合は、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。

GUI を使用してトラフィックポリシーをバインド解除する

1. ［**NetScaler Gateway**］を展開し、［仮想サーバー］をクリックします。
   - 「**NetScaler Gateway**」**>**「ユーザー管理」を展開し、「**AAA** グループ」をクリックします。
   - ［**NetScaler Gateway**］**>** ［ユーザー管理］を展開し、［**AAA** ユーザー］
2. 詳細ペインで、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. ［**NetScaler 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のバインドが解除されたら、ポリシーを削除できます。

GUI を使用してトラフィックポリシーを削除する

1. **[**NetScaler 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

April 1, 2024

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 Secure Access クライアントや Mac 用の Citrix Secure Access クライアントなど、ユーザーのログオン時に使用するソフトウェアを構成するための設定を定義できます。また、ユーザーに Citrix Workspace アプリまたは Secure Hub でのログオンを要求する設定を構成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、常に設定内のグローバル設定よりも優先されます。
- 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、仮想サーバ用に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ていないその他の属性は、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を作成するための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、さまざまな構成のセッションポリシーを構成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、この設定は、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。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します。セッションポリシーを作成しなくても、プロファイルとポリシー内の設定を変更できます。さらに、すべての設定をグローバルレベルで作成し、セッションポリシーを作成してグローバル設定を上書きすることもできます。

Citrix Endpoint Management または StoreFront をネットワークに展開する場合は、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。ウィザードの実行時に、展開の設定を定義します。NetScaler Gateway は、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を作成します。

セッションポリシーを作成する

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、[NetScaler 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 [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.「リクエストプロファイル」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. 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: 式で [
   True value] を選択して、ポリシーがバインドされているレベルに常に適用されるようにします。

セッションポリシー表現の例

セッションポリシーの表現例は次のとおりです。

- `add vpn sessionPolicy sessPol1 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")|| HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixWorkspace\")"sessAct1`
- `add vpn sessionPolicy sessPol2 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT"sessAct2`
- `add vpn sessionPolicy sessPol3 true sessAct3`

セッションポリシーのバインド

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
- グローバルに

GUI を使用してセッションポリシーを仮想サーバーにバインドする

1. 「**NetScaler Gateway**」**>**「仮想サーバー」に移動します。
2. 仮想サーバを選択し、[編集（Edit）] をクリックします。新しい仮想サーバーを作成することもできます。
3. [**Policies**] セクションまで下にスクロールし、[**+**] アイコンをクリックします。
4. **[**ポリシーの選択] で [セッション] を選択します。
5. 「タイプの選択」で、「要求」を選択し、「続行」をクリックします。
6. **[**ポリシーの選択] で、この仮想サーバーにバインドするポリシーを選択します。
7. [**Priority**] に、ポリシーのプライオリティ番号を入力します。
8. [**Bind**] をクリックします。

GUI を使用して、セッションポリシーを認証、承認、および監査グループにバインドする

1. **NetScaler Gateway >** ユーザー管理 **> AAA** グループに移動します。
2. 既存の認証、承認、および監査グループを選択し、[**Edit**] をクリックします。認証、承認、および監査グループを作成することもできます。
3. [詳細設定] で、[ポリシー**]** をクリックし、 [**+**] アイコンをクリックします。
4. **[**ポリシーの選択] で [セッション] を選択し、[続行] をクリックします。
5. [**Select Policy**] で、この認証、承認、および監査グループにバインドするポリシーを選択します。
6. [**Priority**] に、ポリシーのプライオリティ番号を入力します。
7. [**Bind**] をクリックします。

GUI を使用して、セッションポリシーを認証、承認、および監査中のユーザーにバインドする

1. **NetScaler Gateway >** ユーザー管理 **> AAA** ユーザーに移動します。
2. 既存の NetScaler ADC ユーザーを選択し、[編集] をクリックします。認証、承認、および監査ユーザーを作成することもできます。
3. [詳細設定] で、[ポリシー**]** をクリックし、 [**+**] アイコンをクリックします。
4. **[**ポリシーの選択] で [セッション] を選択し、[続行] をクリックします。

5. [**Select Policy**] で、この認証、承認、および監査ユーザーにバインドするポリシーを選択します。
6. [**Priority**] に、ポリシーのプライオリティ番号を入力します。
7. [**Bind**] をクリックします。

注: 優先度の詳細については、https://support.citrix.com/article/CTX214588を参照してください。

セッションプロファイルを作成する

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ています。

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。構成ユーティリティを使用して、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。1 つの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ユーザー接続のネットワーク設定を構成する

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 (イントラネット IP アドレス) のスピルオーバー設定
- 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接続設定を構成する

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:

- Access Interface 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)
- プラグインタイプ（Windows 用 Citrix Secure Access クライアント、または macOS X 用 Citrix Secure Access クライアント）
- 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
- プラグインタイプ (Windows または Mac)

- 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 アドレスとローカル LAN アクセスへのアクセス
- クライアントの選択肢
- プロキシ設定

ユーザー接続の設定について詳しくは、「Citrix Secure Access クライアントの接続の構成」を参照してください。

セッションプロファイルでセキュリティ設定を構成する

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
- 検疫グループ
- オーソリゼーショングループ

NetScaler Gateway での承認の構成について詳しくは、「承認の構成」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** の設定の構成

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関する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
- Web インターフェイスアドレス
- Web インターフェイスポータルモード
- 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の構成について詳しくは、「Web Interface を介した公開アプリケーションおよび仮想デスクトップ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別に作成できます。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。

GUI 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の［構成］タブのナビゲーションペインで、［**NetScaler 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. プロファイルの設定を行い、[作成**]** をクリックし、[閉じる] をクリックします。

プロファイルを作成したら、そのプロファイルをセッションポリシーに含めることができます。

GUI 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、次のいずれかを実行します。
   - [**Add**] をクリックしてセッションポリシーを作成します。
   - ポリシーを選択し、[開く] をクリックします。
3.「リクエスト・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、次のいずれかを実行します。
   a) [作成**]** をクリックし、[閉じる] 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。

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

April 1, 2024

エンタープライズブックマーク (VPN URL) は高度なポリシーとして設定できます。

> メモ:
>
> - NetScaler Gateway は、エンタープライズブックマーク用の HTTP、HTTPS、および RDP プロトコルをサポートしています。
> - NetScaler Gateway は、エンタープライズブックマークの絶対 URL のみをサポートします。

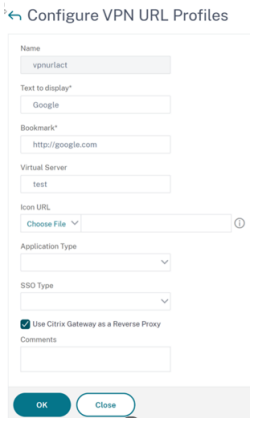
VPN URL を高度なポリシーとして設定する

GUI について

1. VPN URL プロファイルを作成します。
   - [構成**] > [NetScaler Gateway] > [**ポリシー**] > [VPN URL]** に移動します。

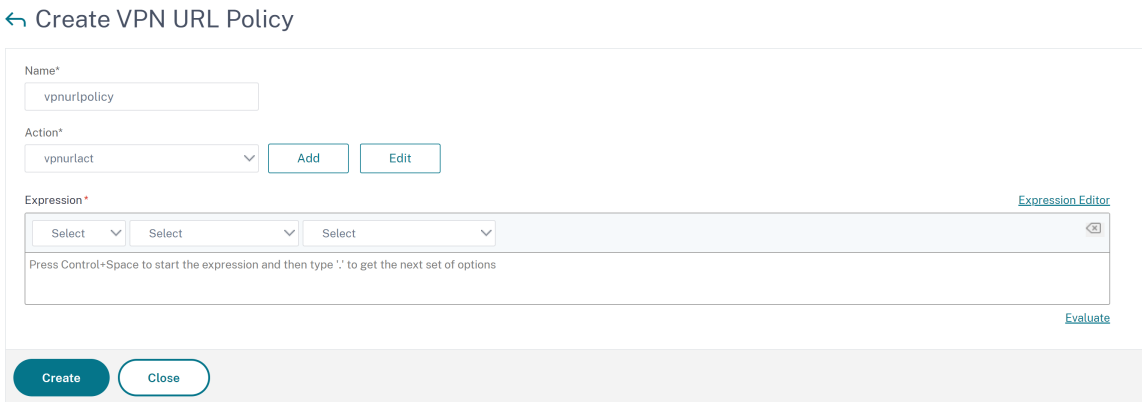
- 「**VPN URL** ポリシーとプロファイル」ページで、「**VPN URL** プロファイル」タブを選択し、「追加」をクリックします。
- 必須フィールドを更新し、「作成」をクリックします。
  - 名前:VPN URL プロファイルの名前。
  - 表示するテキスト: リンクの簡単な説明。説明は Access Interface に表示されます。
  - ブックマーク: アプリケーションの Web アドレス。
  - 仮想サーバー: 構成されている関連する負荷分散またはコンテンツスイッチング仮想サーバーの名前。この情報は入力しなくても構いません。
  - アイコン URL: このフィールドにアップロードされたアイコンは、デフォルトテーマを除くすべてのテーマでサポートされています。推奨最大サイズは 70 x 70 ピクセルです。透明な画像を使用することをおすすめします。この情報は入力しなくても構いません。
  - アプリケーションタイプ:URL が表すアプリケーションのタイプ (VPN、クライアントレス VPN、または SaaS) を選択します。この情報は入力しなくても構いません。
  - SSO タイプ: ブックマークに設定する SSO タイプ。SSO を設定すると、ユーザーはその後のログオン時に資格情報を入力しなくてもアプリケーションにアクセスできます。次の SSO タイプがサポートされています。
    - Unified Gateway: この SSO 設定により、単一の URL からアプリケーションの複数のリソースへの安全なリモートアクセスが可能になります。
    - 自己認証: この SSO 構成では、NetScaler Gateway ユーザーはアプリケーションにアクセスするためのログイン資格情報を入力するよう求められます。
    - SAML ベースの認証: この SSO 構成では、NetScaler Gateway は IdP を使用してユーザーの詳細を検証し、SAML アサーションを生成して SP に送信します。検証に合格すると、SSO は成功します。

> **Note:**
>
> If you enable clientless access, you can make sure that requests to websites go through NetScaler Gateway. For example, you added a bookmark for Google. Select the Use NetScaler Gateway as a reverse proxy check box. When you select this check box, website requests go from the user device to NetScaler Gateway and then to the website. When you clear the check box, requests go from the user device to the website. This check box is only available if you enable clientless access.



2. VPN URL ポリシーを作成します。

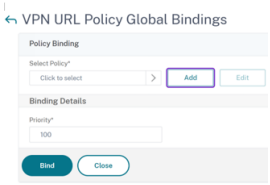
   - [構成] **> [NetScaler Gateway] > [**ポリシー**] > [VPN URL]** に移動します。
   - 「**VPN URL** ポリシーとプロファイル」ページで、「**VPN URL** ポリシー」タブを選択し、「追加」をクリックします。
   - 必須フィールドを更新し、「作成」をクリックします。
     - 名前:VPN URL ポリシーの名前。
     - アクション: 設定した VPN URL プロファイルを選択します。ドロップダウンリストにプロファイルがない場合は、[追加] をクリックして手順 1 を繰り返します。
     - 表現: 詳細なポリシー表現については、「ポリシーと表現 」を参照してください。



3. VPN URL ポリシーをバインドポイントにバインドします。

   - [構成] **> [NetScaler Gateway] > [**ポリシー**] > [VPN URL]** に移動します。
   - 「**VPN URL** ポリシーとプロファイル」ページで、「**VPN URL** ポリシー」タブを選択します。
   - 「アクションの選択」ドロップダウンリストから「グローバルバインディング」を選択します。
   - VPN URL ポリシーを選択します。ポリシーが表示されない場合は、[追加] をクリックして手順 2 を繰り返します。

- バインディングの詳細セクションで、VPN URL ポリシーに優先順位を割り当てます。



CLI で

VPN URL アクションの作成**:**

コマンドプロンプトで、次のように入力します:

```
add vpn urlAction <name> -linkName <string> -actualURL <string> \[-
    vServerName <string>] \[-clientlessAccess \( ON | OFF )] \[-comment
    <string>] \[-iconURL <URL>] \[-ssotype <ssotype>] \[-applicationtype
     <applicationtype>] \[-samlSSOProfile <string>]
```

NetScaler Gateway は、VPN URL アクションの以下の操作をサポートしています。

- **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]
```

> 注:
>
> クライアントレスアクセスをオンに設定すると、Web サイトへの要求がユーザーデバイスから NetScaler Gateway、次に Web サイトに送信されることを確認できます。

- **show**

```
show vpn urlAction [<name>]
```


- 削除

```
remove vpn urlAction <name>
```

- **rename**

```
rename vpn urlAction <name>@ <newName>@
```

VPN URL ポリシーの作成**:**

NetScaler Gateway は、VPN URL ポリシーの以下の操作をサポートしています。

- **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>]
```

- 削除

```
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 )]
```

ポリシーをバインドポイントにバインドします。

NetScaler Gateway は、VPN URL ポリシーバインディングの以下の操作をサポートしています。

- **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>
```

> 注:
>
> バインドポイントは aaauser、aaagroup、vpnvserver、vpnglobalです。

エンドポイントポリシー

April 1, 2024

Endpoint Analysis (EPA) は、ユーザーのデバイスをスキャンして、オペレーティングシステムの更新、ウイルス対策、ファイアウォール、Web ブラウザーソフトウェアの有無やバージョンレベルなどの情報を検出するプロセスです。Endpoint Analysis では、ネットワークに接続する前に、ユーザーのデバイスが要件を満たしているかどうかを判断できます。また、ユーザーが接続している間に変更がないか定期的に確認するように設定することもできます。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チェックして、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。

> 重要:
>
> - Endpoint Analysis は、事前に定められたコンプライアンス基準に照らしてユーザーデバイスを分析することを目的としており、エンドユーザーデバイスのセキュリティを強制または検証するものではありません。ローカル管理者による攻撃からデバイスを保護するには、エンドポイントセキュリティシステムを使用することをお勧めします。
> - EPA クライアントはスタンドアロンクライアントとして使用でき、Citrix Secure Access クライアントにバンドルされています。Citrix EPA クライアントと Citrix Secure Access クライアントは相互に独立しています。

エンドポイントポリシーの仕組み

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要件を満たしているかどうかを確認するように NetScaler Gateway を構成できます。これは事前認証ポリシーと呼ばれます。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 NetScaler 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ていない他の要件を確認するには、セッションポリシーを設定し、それをユーザーまたはグループにバインドできます。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基準が常に準拠していることを確認するため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、NetScaler Gateway は Endpoint Analysis プラグインをダウンロードし、ユーザーのデバイスでスキャンを実行します。ユーザーがログオンするたびに、Endpoint Analysis プラグインが自動的に実行されます。

次の 3 種類のポリシーを使用してエンドポイントポリシーを設定できます。

- Yes または No パラメータを使用する事前認証ポリシー。このスキャンでは、ユーザーデバイスが指定され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 に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デバイスチェック表現。ユーザーデバイスがクライアントデバイスチェック式の要件を満たしていない場合、ユーザーを隔離グループに入れるように構成できます。ユーザーデバイスがスキャンに合格すると、ユーザーは別のグループに配置され、他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さまざまなレベルのアクセス権限を付与できます。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。準拠していないデバイスから接続するユーザーには、より制限されたアクセスレベルを提供して、ユーザーがダウンロードせずにリモートサーバー上のドキュメントを編集できるようにすることができます。EPA を実行しているすべてのデバイスは非準拠デバイスとみなされます。

エンドポイント分析は、次の基本手順を実行します。

- 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。
- 該当するすべてのスキャンを実行します。ユーザーが接続しようとすると、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についてユーザーデバイスをチェックします。ユーザーデバイスがスキャンに合格すると、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すると、ユーザーはログオンできなくなります。

  注**:** Endpoint Analysis 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、構成済みのスキャンにリストされている目的のプロパティ値を比較します。

- 目的のプロパティ値が見つかったかどうかを確認する出力を生成します。

> 重要:
>
> 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適用できます。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、この設定は、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。

EPA 表現のサンプル

以下は、強制終了プロセス、ファイル削除、デバイス証明書などの一部の EPA コンポーネントの表現例です。

- Windows:
  - 強制終了プロセス: `sys.client_expr(\ “proc_0_perl\ “)-killProcess processToKill.exe`
  - デバイス証明書:`sys.client_expr( “device-cert_0_0” )`
  - ファイルの削除:`sys.client_expr(\ “proc_0_perl\ “)-deletefiles “C:/removefile.txt”`
- MAC
  - 強制終了プロセス: `sys.client_expr(\ “proc_0_perl\ “)-killProcess processToKill.exe`
  - デバイス証明書:`sys.client_expr( “device-cert_0_0” )`
  - ファイルの削除:`sys.client_expr(\ “proc_0_perl\ “)-deletefiles “C:/removefile.txt”`

ユーザーログオンオプションの評価

ユーザーがログオンするときに、エンドポイント分析のスキャンをスキップするように選択できます。ユーザーがスキャンをスキップすると、NetScaler 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 にアクセスするか、クライアントレスアクセスを介してのみアクセスできます。

たとえば、Citrix Secure Access クライアントを使用してユーザーにアクセスできるようにしたいとします。プラグインを使用して NetScaler 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 のみでログオンし、公開アプリケーションを使用できます。また、Outlook Web Access などの特定のアプリケーションへのアクセスを制限するクライアントレスアクセスを構成することもできます。

このログオンシナリオを実現するように NetScaler Gateway を構成するには、制限付きセッションポリシーをデフォルトポリシーとして割り当てます。次に、ユーザーデバイスが Endpoint Analysis スキャンに合格したときに、

ユーザーを特権セッションポリシーにアップグレードするように設定を構成します。その時点で、ユーザーはネットワークレイヤーにアクセスでき、Citrix Secure Access クライアントでログオンできます。

制限付きセッションポリシーを最初に強制するように **NetScaler Gateway** を構成するには、次の手順に従います。

- ICA プロキシを有効にしてグローバル設定を構成し、指定したアプリケーションがユーザーデバイス上で実行されていない場合は、他のすべての必要な設定を構成します。
- Citrix Secure Access クライアント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ルール部分に、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。(`client.application.process(symantec.exe)exists`)

  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、NetScaler 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偽と見なされます）。その結果、ユーザは Web インターフェイス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。エンドポイント分析に合格すると、NetScaler Gateway がセッションポリシーを適用し、ユーザーは Citrix Secure Access クライアントにフルアクセスできるようになります。

EPA スキャンをスキップする

EPA スキャンをスキップできるのは、認証後および事前認証のみです。Skip EPA は、サポートされているすべてのオペレーティングシステムのブラウザで利用できます。ユーザーは、ゲートウェイにアクセスするときに表示される [**Skip EPA**] ボタンをクリックする必要があります。ユーザーがスキャンをスキップすると、NetScaler 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 にアクセスするか、クライアントレスアクセスを介してのみアクセスできます。

「https://support.citrix.com/article/CTX200748」も参照してください。

Ubuntu でサポートされるエンドポイント分析スキャン

次のエンドポイント分析 (EPA) スキャンは、Ubuntu オペレーティングシステム用にインストールされた EPA プラグインでサポートされています。各スキャンを設定するためのサンプル式は、EPA スキャンとともに一覧表示されています。これらの式は、認証ポリシーで設定できます。

- ファイル
  - 存在:sys.client_expr(“file_0_/home/user/test.txt”)
  - **MD5** チェックサム:sys.client_expr (“file_0*/home/user/test.txt_md5* ce780e271debcc29f551546e8db3368f)
  - ファイル内のテキスト **(**正規表現サポート**): sys.client_expr (**(“file_0_/home/user/test.txt_search_cloud”)

- プロセス
  - 存在:sys.client_expr(“proc_0_perl”)
  - **MD5** チェックサム:sys.client_expr(“proc_0*perl_md5* c060d3a5f97e27066cef8c116785567a”)
  - パス:sys.client_expr(“proc_0*perl_path*/usr/bin/perl”)
- ファイルシステムデバイスまたはマウントポイント名:sys.client_expr(“mountpoint_0_/sys”)

高度なポリシーを使用している場合、各スキャンの式は GUI から生成できます（[セキュリティ**] > [AAA] > [**ポリシー**] > [**認証**] > [**高度なポリシー**] > [EPA**]）。

注**:** Linux クライアントの [式エディタ] ページで、[共通**]** を選択し、**[**プロセス**]**、**[**ファイル**]**、または [マウントポイント] を選択できます。

事前認証ポリシーとプロファイル

April 1, 2024

> 重要**:**
>
> エンドポイント分析は、あらかじめ決められたコンプライアンス基準に照らしてユーザーデバイスを分析することを目的としており、エンドユーザーデバイスのセキュリティを強制または検証するものではありません。ローカル管理者による攻撃からデバイスを保護するには、エンドポイントセキュリティシステムを使用することをお勧めします。

NetScaler Gateway で認証される前にユーザーのデバイスをチェックするように NetScaler Gateway を構成できます。ユーザーのデバイスが組織の要件を満たしていない場合、これを使用してアクセスを制限できます。デバイスチェックは、仮想サーバーに固有の個別のポリシーを使用して実装することも、次の 2 つの手順で説明するようにグローバルに実装することもできます。

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式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 はユーザーのデバイスで実行されています。ユーザーが NetScaler Gateway にログオンすると、テキストファイルが実行されているかどうかに応じて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がログオンできないようにするには、ユーザーがログオンする前にプロセスを停止するように事前認証プロファイルを構成できます。

事前認証ポリシーには、次の設定を構成できます。

- 式。エクスプレッションを作成するのに役立つ次の設定が含まれています。
  - 式。すべてのエクスプレッションを表示します。
  - 任意の式にマッチします。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。

- [すべての式に一致]。選択した式のリストにあるすべての式に一致するようにポリシーを設定します。
- 表形式の表現。OR (||)or AND (&&)演算子を使用して、既存のエクスプレッションを含む複合エクスプレッションを作成します。
- 高度な自由形式。エクスプレッション名とOR (||)and AND (&&)演算子を使用して、カスタム複合エクスプレッションを作成します。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。
- 追加。エクスプレッションを作成します。
- 修正。既存の式を変更します。
- 削除。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。
- 名前付き式。設定済みの名前付き式を選択します。NetScaler Gateway にすでに存在する式のメニューから名前付き式を選択できます。
- [式を追加]。選択した名前付き式をポリシーに追加します。
- エクスプレッションを置換。選択した名前付き式をポリシーに置き換えます。
- エクスプレッションをプレビュー。名前付きの式を選択すると、NetScaler Gateway で構成されている詳細な文字列が表示されます。

事前認証プロファイルの設定

GUI 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］タブの［**NetScaler Gateway**］をクリックし、［グローバル設定］をクリックします。
2. 詳細ウィンドウの [設定] 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。

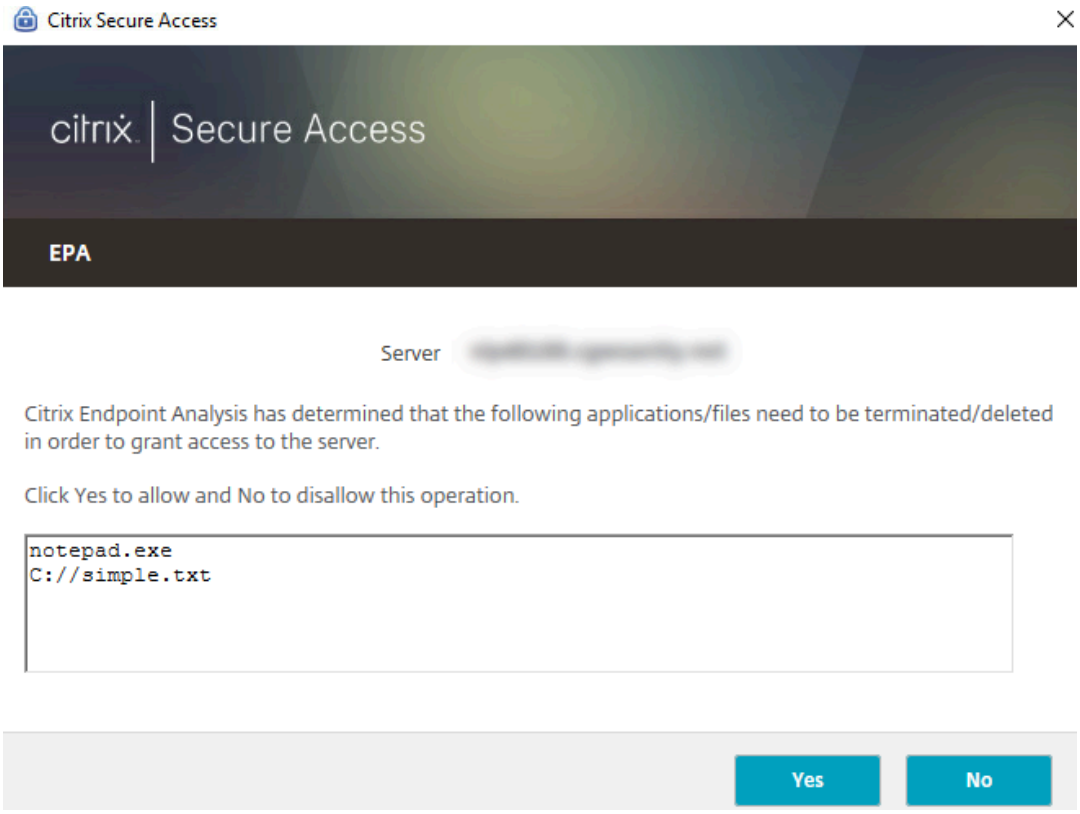
   エンドポイント分析の実行後、ユーザーのログオンを拒否または許可します。

   b)「キャンセルするプロセス」に、プロセスを入力します。

   これは、Endpoint Analysis プラグインが停止する必要があ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。

   Endpoint Analysis プラグインが削除する必要があるファイルを指定します。プロセスを削除またはキャンセルすると、エンドユーザーに通知が表示されます。

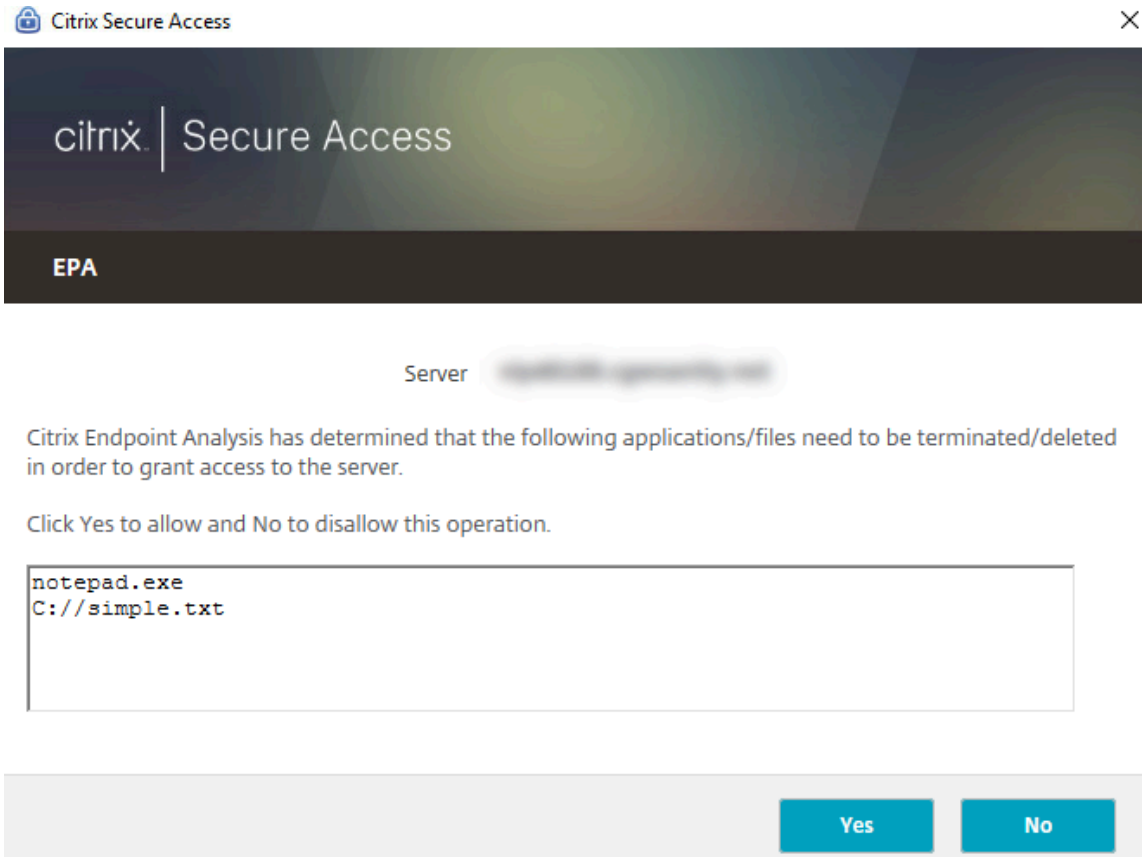


4. Expression では、ns_true という式をそのまま使用することも、ウイルス対策ソフトウェアやセキュリティソフトウェアなどの特定のアプリケーション用の式を作成して、「**OK**」をクリックすることもできます。

GUI を使用して事前認証プロファイルを設定するには

1. ［NetScaler Gateway］＞［ポリシー］＞［認証/承認］に移動し、［事前認証 EPA］をクリックします。
2. 詳細ペインの [プロファイル] タブで、[追加] をクリックします。
3. [名前] に、チェック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 [許可] 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] に、削除するファイルの名前 (c:\clientext.txt など) を入力し、[作成]、[閉じる] の順にクリックします。

   Endpoint Analysis プラグインが削除する必要があるファイルを指定します。プロセスを削除またはキャンセルすると、エンドユーザーに通知が表示されます。



GUI を使用して事前認証プロファイルを設定する場合は、[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] メニューからプロファイルを選択します。

事前設定済みの式を事前認証ポリシーに追加する

NetScaler Gateway には、名前付き式と呼ばれる事前構成された式が付属しています。ポリシーを設定するときは、ポリシーの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、更新されたウイルス定義を持つ Symantec Antivirus 10 をチェックするとします。事前認証ポリシーを作成し、次の手順の説明に従って式を追加します。

事前認証ポリシーまたはセッションポリシーを作成する場合、ポリシーの作成時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または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

1. [NetScaler Gateway] > [ポリシー] > [認証/承認] に移動し、[事前認証 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、リストからアンチウイルス製品を選択します。
4. [式の追加]、[作成**]**、 [閉じる] の順にクリックします。

カスタムエクスプレッションの設定

カスタム式は、ポリシー内に作成する式です。エクスプレッションを作成するときは、エクスプレッションのパラメータを設定します。

よく使われる文字列を参照するカスタムエクスプレッションを作成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が容易になり、設定済みの式の維持も容易になります。

たとえば、Symantec antivirus 10 用のカスタム式を作成し、ウイルス定義が 3 日以上前のものでないことを確認したいとします。ポリシーを作成し、ウイルス定義を指定する式を設定します。

次の手順は、事前認証ポリシーで式を作成する方法を示しています。セッションポリシーでも同じ手順を使用できます。

事前認証ポリシーとカスタム表現の作成

1. [**NetScaler Gateway**] **>** [ポリシー] **>** [認証**/**承認] に移動し、[事前認証 **EPA**] をクリックします。
2. 詳細ペインで、[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. 「リクエストプロファイル」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の **[**任意の式に一致する**]** 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]、[閉じる] の順にクリックします。

カスタム式を設定すると、ポリシーダイアログボックスの [式] ボックスに追加されます。

複合式の設定

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、次のウイルス対策アプリケーションのいずれかを実行することをユーザデバイスに要求するように、複合式を設定できます。

- Symantec Antivirus 10
- McAfee Antivirus 11
- Sophos Antivirus 4

OR 演算子を使用して式を設定して、前述の 3 つのアプリケーションをチェックします。NetScaler 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。[Policy] 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_10 || av_5_McAfeevirusscan_11 || av_5_sophos_4
```

複合式の詳細については、「複合式の設定」を参照してください。

事前認証ポリシーのバインド

事前認証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してバインドする

1. ［構成］タブの［**NetScaler Gateway**］をクリックし、［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設定] 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ーにバインドする

1. ［構成］タブの［**NetScaler Gateway**］をクリックし、［仮想サーバー］をクリックします。
2. 詳細ペインで仮想サーバーを選択して、［**Open**］をクリックします。
3. ［NetScaler 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

必要に応じて、NetScaler 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。

グローバル事前認証ポリシーのバインドを解除する

1. [NetScaler Gateway] > [ポリシー] > [認証/承認] に移動し、[事前認証 EPA] をクリックします。
2. 詳細ペインでポリシーを選択し、[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. [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]、[**OK**] の順にクリックします。

仮想サーバからの事前認証ポリシーのバインド解除

1. [構成] タブの [**NetScaler Gateway**] をクリックし、[仮想サーバー] をクリックします。
2. [**NetScaler 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ると、NetScaler 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

1. [**NetScaler Gateway**] **>** [ポリシー] **>** [認証/承認] に移動し、[事前認証 **EPA**] をクリックします。
2. 詳細ペインでポリシーを選択し、[削除] をクリックします。

事前認証ポリシーのプライオリティの設定

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、グローバルにバインドされている特定のウイルス対策アプリケーションをチェックするポリシーと、仮想サーバー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。グローバルにバインドされているポリシーが 2 番目に適用されます。

事前認証スキャンの発生順序を変更できます。NetScaler Gateway でグローバルポリシーを最初に適用するには、仮想サーバーにバインドされた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たポリシーよりも高い優先度を指定します。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、仮想サーバポリシーのプライオリティ番号を 2 に設定します。ユーザーがログオンすると、NetScaler Gateway は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プライオリティを変更する

1. ［構成］タブの［**NetScaler Gateway**］をクリックし、［仮想サーバー］をクリックします。
2. 詳細ペインで仮想サーバーを選択して、［**Open**］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。

認証ポリシーの投稿

April 1, 2024

> 重要:
>
> エンドポイント分析は、あらかじめ決められたコンプライアンス基準に照らしてユーザーデバイスを分析することを目的としており、エンドユーザーデバイスのセキュリティを強制または検証するものではありません。ローカル管理者による攻撃からデバイスを保護するには、エンドポイントセキュリティシステムを使用することをお勧めします。

認証後ポリシーは、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がある汎用ルールのセットです。ポリシーが失敗すると、NetScaler Gateway への接続は終了します。認証後ポリシーを構成すると、条件付きに設定できるユーザー接続の設定を構成できます。

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。

また、グループを承認グループとして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デバイスチェック式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検疫グループに入れるように、認証後ポリシーを構成することもできます。シンプルなポリシーには、クライアントデバイスのチェック表現と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 NetScaler 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、認可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 詳細については、「NetScaler Gateway での SmartAccess 構成」を参照してください。

> 注:
>
> この機能は Citrix Secure Access クライアントでのみ機能します。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。

認証後ポリシーを構成する

セッションポリシーを使用して、認証後ポリシーを設定します。シンプルなポリシーには、クライアントデバイスのチェック表現とメッセージが含まれます。

GUI を使用して認証後ポリシーを設定するには

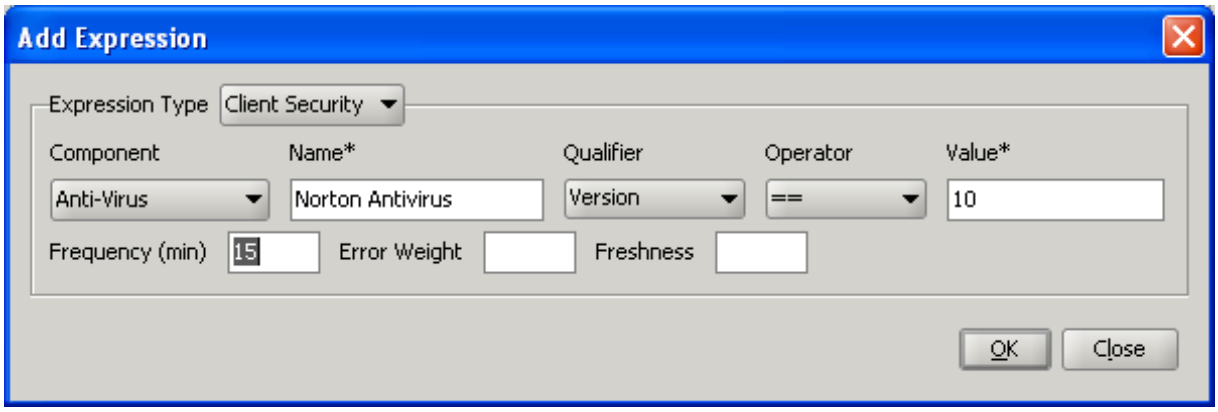
1. **NetScaler Gateway >** ポリシーを展開して、「セッション」をクリックします。
2. 詳細ペインの [ポリシー] タブで、[追加] をクリックします。
3. **[**名前] に、ポリシーの名前を入力します。
4. 「リクエストプロファイル」の横にある「新規」をクリックします。
5. **[**名前] に、プロファイルの名前を入力します。
6. [セキュリティ] タブの [詳細設定] をクリックします。
7. [クライアントセキュリティ] で、[グローバルを上書き**]** をクリックし、 [新規] をクリックします。
8. クライアントデバイスのチェック式を設定し、「作成」をクリックします。
9. [クライアントセキュリティ] の [隔離グループ] 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たいメッセージを入力します。
11. [承認グループ] で、[グローバルを上書き] をクリックし、グループを選択し、[追加]、[**OK**]、[作成] の順にクリックします。
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 [一般] を選択し、[**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、[閉じる] をクリックします。

認証後スキャンの頻度を構成する

指定した間隔で認証後ポリシーを実行するように NetScaler Gateway を構成できます。たとえば、クライアントデバイスチェックポリシーを構成し、それをユーザーデバイス上で 10 分ごとに実行したいとします。この頻度は、ポリシー内にカスタム式を作成することで設定できます。

> 注:
>
> 認証後ポリシーの頻度チェック機能は、Citrix Secure Access クライアントでのみ機能します。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。

「認証後ポリシーの設定」の手順に従って、クライアントデバイスチェックポリシーを設定する頻度（分単位）を設定できます。次の図は、「式の追加」(**Add Expression**) ダイアログボックスの頻度の値を入力できる場所を示しています。



検疫グループと承認グループ

ユーザーが NetScaler Gateway にログオンするときに、NetScaler 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するグループにユーザーを割り当てます。ユーザが認証後スキャンに失敗した場合、ユーザ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。このグループは、ネットワークリソースへのアクセスを制限します。

また、承認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、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 NetScaler Gateway で定義したデバイスチェック要件に合格すると、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。

グローバル設定またはセッションポリシーを使用して、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および承認グループを構成します。セッションポリシー内のクライアントデバイスチェック式に基づいて、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、NetScaler 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。

権限付与グループの設定

Endpoint Analysis スキャンを設定すると、ユーザーデバイスがスキャンに合格したときに、ユーザーを承認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メンバーシップをチェックする Endpoint Analysis スキャンを作成するとします。NetScaler Gateway で、ドメインに参加しているコンピューターというローカルグループを作成し、スキャンに合格したすべての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せん。ユーザーが NetScaler Gateway の別のグループのメンバーになるように構成されていない場合、承認グループを使用して、承認ポリシーのデフォルトセットを提供できます。

セッションポリシーを使用して認可グループを構成するには

1. **NetScaler Gateway >** ポリシーに移動し、「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、[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. 「リクエストプロファイル」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. [セキュリティ] タブの [詳細設定] をクリックします。
7. 「承認グループ」で、「グローバルをオーバーライド」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ます。
8. 「追加」をクリックし、「**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、[名前付き式] の横にある [一般] を選択し、[**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、[閉じる] をクリックします。

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。

グローバル権限グループを構成するには

1. **NetScaler 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、[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 [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ます。
5. 「追加」をクリックし、「**OK**」をクリックします。

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、[セキュリティ設定-詳細設定] ダイアログボックスで、一覧から承認グループを選択し、[削除] をクリックします。

検疫グループの設定

隔離グループを設定する場合、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デバイスのチェック式を設定します。

検疫グループのクライアントデバイスチェック式を設定するには

1. [**NetScaler Gateway**] **>** [ポリシー] に移動し、[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、[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. 「リクエストプロファイル」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. [セキュリティ] タブの [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、[グローバルを上書き**]** をクリックし、 [新規] をクリックします。

8. クライアントエクスプレッションダイアログボックスで、クライアントデバイスのチェックエクスプレッションを設定し、「作成」をクリックします。
9. 「隔離グループ」で、グループを選択します。
10. [エラーメッセージ] に、問題を説明するメッセージをユーザーに入力し、[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の [名前付き式] の横で [一般] を選択し、[**True value**] を選択して [式の追加] をクリックします。
12. [作成**]** をクリックし、 [閉じる] をクリックします。

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:
>
> Endpoint Analysis スキャンが失敗し、ユーザーが検疫グループに配置された場合、検疫グループにバインドされたポリシーは、検疫グループにバインドされたポリシーと同等またはそれ以下の優先度番号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です。

グローバル検疫グループを設定するには

1. **NetScaler 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、[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 [詳細設定] をクリックします。
4. **Client Security** で、クライアントデバイスのチェック式を設定します。
5. 「隔離グループ」で、グループを選択します。
6. 「エラー・メッセージ」に、問題を説明するメッセージをユーザーに入力し、「**OK**」をクリックします。

ユーザーデバイスの事前認証デバイスチェック表現

April 1, 2024

> 重要**:**
>
> エンドポイント分析は、あらかじめ決められたコンプライアンス基準に照らしてユーザーデバイスを分析することを目的としており、エンドユーザーデバイスのセキュリティを強制または検証するものではありません。ローカル管理者による攻撃からデバイスを保護するには、エンドポイントセキュリティシステムを使用することをお勧めします。

NetScaler Gateway は、ユーザーデバイスの検証に役立つさまざまなエンドポイントコンプライアンスチェックを、ユーザーログオン中またはセッション中のその他の構成時間に行います。これらのチェックに合格したユーザーデバイスのみが NetScaler Gateway セッションを確立できます。

NetScaler Gateway で構成できるユーザーデバイスのチェックの種類は次のとおりです。

- スパム対策

- 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
- オペレーティングシステム
- 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

ユーザーデバイス上でデバイスチェックが失敗した場合、次のチェックに合格するまで（定期的に行われるチェックの場合）、新しい接続は確立されません。ただし、既存の接続を経由するトラフィックは、引き続き NetScaler Gateway をトンネル経由します。

構成ユーティリティを使用して、ユーザーデバイス上で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の事前認証ポリシーまたはデバイスチェック式を設定できます。

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表現を構成する

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、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。違いは、選択した値です。たとえば、ユーザーデバイスのノートンアンチウイルスバージョン 10 と ZoneAlarm Pro をチェックする場合、セッションまたは事前認証ポリシー内に、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種類。
- 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: 値が存在するかどうか、または値と等しいかどうかを確認します。
- 値: ユーザーデバイス上のウイルス対策、ファイアウォール、インターネットセキュリティ、またはスパム対策ソフトウェアのアプリケーションバージョン。
- 頻度: 認証後スキャンが実行される頻度 (分単位)。
- エラーの重み: 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る重み。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。
- 鮮度: ウイルス定義の古さを定義します。たとえば、ウイルス定義が 3 日を超えないように式を設定できます。

クライアントデバイスチェックポリシーを事前認証ポリシー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の [構成] タブのナビゲーションペインで、**[NetScaler Gateway] > [**ポリシー**]** を展開し、**[**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、［NetScaler Gateway］>［ポリシー］>［認証/承認］を展開し、［事前認証 EPA］をクリックします。

2. 詳細ペインの [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、[**Client Security**] を選択します。
6. 次の設定を構成します。

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・デバイスのチェック文字列を入力し、「**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

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、セッションの確立時にユーザーデバイスが特定のサービスを実行していることを確認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の［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］**>**［ポリシー］を展開し、［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、［**NetScaler Gateway**］**>**［ポリシー］**>**［認証**/**承認］を展開し、［事前認証 EPA］をクリックします。

2. 詳細ペインの [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、[Client Security] を選択します。
6. 次の設定を構成します。

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) [Qualifier] での選択内容に応じて、次のいずれかを実行します。

- 空白のままの場合は、「演算子」で == または!= を選択
- 「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」、「閉じる」の順にクリックします。

Windows ベースのコンピューターで利用可能なすべてのサービスの一覧と各サービスの状態は、次の場所で確認できます:

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、リストされた名前とは異なります。[
> プロパティ] ダイアログボックスを見て、サービスの名前を確認します。

プロセスポリシーの設定

セッションポリシー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で特定のプロセスを実行するように要求する規則を定義できます。プロセスには任意のアプリケーションを使用でき、カスタマイズされたアプリケーションを含めることができます。

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リストは、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の［構成］タブのナビゲーションペインで、［**NetScaler 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、［**NetScaler Gateway**］**>** ［ポリシー］**>** ［認証**/**承認］の順に展開し、［事前認証 EPA］をクリックします。
2. 詳細ペインの [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、[Client Security] を選択します。
6. 次の設定を構成します。
   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。

Endpoint Analysis ポリシー（認証前または認証後）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、notepad.exe 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を構成する

セッションまたは事前認証ポリシーを作成すると、クライアントデバイスのチェック文字列を構成して、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、特定の Service Pack または修正プログラムをチェックするように式を構成することもできます。

Windows と Macintosh の値は次のとおりです。

オペレーティングシステム	Value
macOS X	macOS
Windows 8.1	win8.1
Windows 8	win8
Windows 7	win7
Windows Vista	ビスタ
Windows XP	winxp
Windows Server 2008	win2008
Windows Server 2003	win2003
Windows 2000 Server	win2000
Windows 64 ビットプラットフォーム	win64

GUI を使用してオペレーティングシステムポリシーを構成するには

1. 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) ［**NetScaler Gateway**］ **>** ［ポリシー］に移動し、［セッション］をクリックします。
   b) **NetScaler Gateway >** ポリシー **>** 事前認証に移動します。
2. 詳細ペインの [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. 「アクションのリクエスト」で、既存のアクションを選択するか、アクションを作成します。
5. ［**Expression Editor**］をクリックします。

6. **[**式の種類の選択**]** で、[クライアントセキュリティ] を選択します。
7. 次の設定を構成します。

    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。

    - フィールドは空白のままにします。
    - サービスパックを選択
    - 修正プログラムの選択
    - バージョンを選択 (macOS のみ)

    d) 手順 7 での選択内容に応じて、[演算子] で次のいずれかを実行します。

    - [修飾子] が空白の場合は、[演算子] で EQUAL (= =)、NOTEQUAL (!=)、EXISTS または NOTEXISTS を選択します。
    - [Service Pack] または [Hotfix] を選択した場合は、演算子を選択し、[値] に値を入力します。

8. [完了] をクリックし、[閉じる] 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している場合、［値］フィールドに数字がない場合、式が無効であるため、NetScaler Gateway はエラーメッセージを返します。

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 のチェックだけを構成できます。Service Pack 4 の存在により、以前のサービスパックが存在することが自動的に示されるためです。

レジストリポリシーを構成する

セッションポリシー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が存在し、値があるかどうかを確認できます。セッションは、特定のエントリが存在するか、設定されているか、またはより高い値を持つ場合にのみ確立されます。

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われます。

  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。

  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、スペースを示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、ユーザーがログオンしたときに Citrix Secure Access クライアントのレジストリキーを検索するレジストリ表現です。

CLIENT.REG(secureaccess).VALUE==HKEY_LOCAL_MACHINE\\\\SOFTWARE\\\\CITRIX\\\\Secure\Access\Client

> 注:
>
> レジストリキーと値をスキャンするときに、「式」ダイアログ・ボックスで「アドバンスド・フリーフォーム」を選択し、式の先頭が CLIENT.REG で始まっている必要があります。

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には、次のタイプを使用します。

- 文字列

  文字列型の場合は、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。

- 展開文字列

  バイナリやマルチストリングなどの他のタイプ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。
- <、> などの他の比較演算子、大文字と小文字を区別する比較はサポートされていません。
- レジストリ文字列の合計長は 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、ソフトウェアのバージョン、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の［構成］タブのナビゲーションペインで、［**NetScaler 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、［**NetScaler Gateway**］**>** ［ポリシー］**>** ［認証**/**承認］の順に展開し、［事前認証 EPA］をクリックします。

2. 詳細ペインの [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、[Client Security] を選択します。
6. 次の設定を構成します。

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、次のいずれかを実行します。

- 修飾子が空白のままの場合は、EXISTS または NOTEXISTS を選択します。
- [修飾子] で [値] を選択した場合は、[==] または [!==

e)［値］に、レジストリエディタに表示される値を入力し、［OK］、［閉じる］の順にクリックします。

複合クライアントデバイスチェック表現の設定

クライアントデバイスチェック文字列を組み合わせて、複合クライアントデバイスチェック式を作成できます。

NetScaler 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。

- と (&&)

または (

-
- ない (!)

精度を上げるには、括弧を使用して文字列をグループ化できます。

> 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括弧を使用してデバイスチェック式をグループ化します。かっこを使用すると、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設定

AND (&&) 演算子は、2 つのクライアントデバイスのチェック文字列を組み合わせて、両方のチェックが合格した場合にのみ複合チェックが成功するようにします。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‘&&’を使用して設定できます。

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デバイスチェックです。また、Net Logon サービスが同じコンピュータで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設定

OR (| |) 演算子は、2 つのデバイスチェック文字列を組み合わせて機能します。複合チェックは、どちらかのチェックが true の場合にパスします。式は左から右に評価され、最初のチェックに合格した場合、2 番目のチェックは実行されません。最初のチェックがパスしない場合、2 番目のチェックが実行されます。

OR (| |) 演算子は、キーワード`OR`または | | 記号を使用して設定できます。

例:

以下は、ユーザーデバイスに`c:\\file.txt`ファイルがあるのか、それとも実行中の`putty.exe`プロセスがあるのかを判断するクライアントデバイスチェックです。

```
client.file(c:\\\\\\\\\\file.txt)EXISTS)OR (client.proc(putty.exe)
EXISTS
```

この文字列は、次のように設定することもできます

```
client.file(c:\\\\\\\\\\file.txt)EXISTS)|| (client.proc(putty.exe)
EXISTS
```

NOT (!) 演算子を使用してポリシーを設定

NOT (!) または、否定演算子はクライアントデバイスのチェック文字列を無効にします。

例:

ファイル c:\sophos_virus_defs.dat ファイルが作成されてから 2 日以内であれば、次のクライアントデバイスチェックに合格します。

```
\!(client.file(c:\\\\\\\\\\sophos\\_virus\\_defs.dat).timestamp==2dy)
```

nFactor 認証の要素としての EPA スキャン

April 1, 2024

> 重要**:**
>
> エンドポイント分析は、あらかじめ決められたコンプライアンス基準に照らしてユーザーデバイスを分析することを目的としており、エンドユーザーデバイスのセキュリティを強制または検証するものではありません。ローカル管理者による攻撃からデバイスを保護するには、エンドポイントセキュリティシステムを使用することをお勧めします。

以下は、nFactor EPA の基本エンティティの一部です。

EPA アクション**:** EPA アクションは nFactor EPA に導入されたアクションタイプです。次の内容が含まれています。

- クライアントデバイスチェック式: この式は、評価のためにゲートウェイ EPA プラグインに送信されます。
- 成功グループ:EPA の結果が true の場合、このグループは (設定されている場合) ゲートウェイセッションに継承されます。
- 検疫グループ:EPA の結果が false の場合、このグループが設定されている場合、ゲートウェイセッションに継承されます。
- KillProcess: EPA プロセスが終了しなければならないプロセスの名前を表します。
- DeleteFiles: EPA プロセスで削除する必要があるファイルへのパスをカンマで区切って指定します。

グループは、セッションの存続期間中に使用して、クライアントが特定の EPA 条件を満たしているかどうかを判断できます。
特定の要因で EPA が失敗し、最後のアクションに「Quarantine Group」が含まれていない場合、そのユーザーの認証は終了します。
「隔離グループ」が存在する場合、認証は継続され、管理者はグループが制限付きアクセスを許可しているかどうかを確認できます。詳細については、「EPA の実行」を参照してください。

EPA ポリシー**:** nFactor では、すべてのポリシーが同じ構文で「認証ポリシーを追加」で追加されます。ただし、アクションのタイプによって、ポリシーが EPA ポリシーとして認定されます。

EPA ファクター： EPA ファクターは通常のポリシーラベルです。EPA ファクターと呼ばれるエンティティはありません。EPA ポリシーがファクタにバインドされると、EPA ファクタにする特定のプロパティが継承されます。

> 注:
>
> このドキュメントでは、「EPA ファクター」という用語は、EPA ポリシーが適用されるファクターを指す場合によく使用されます。

EPA —隔離**:** あるファクターですべてのアクションのすべてのクライアントデバイスチェック式が失敗し、最後のアクションに「Quarantine group」が含まれている場合、そのグループがセッションに追加され、NextFactor が調査されます。つまり、失敗にもかかわらず、「検疫グループ」の存在は、セッションを次の段階に認定します。ただし、特別なグループの継承により、管理者はセッションを制限されたアクセスまたは追加の認証ポリシー（OTP や SAML など）に降格させることができます。

最後のアクションで検疫グループが存在しない場合、認証は失敗して終了します。

nFactor の **EPA** は、次のエンティティも使用します。

- **LoginSchema :** ログオンフォームの XML 表現。ログオンフォームの「ビュー」を定義し、「ファクター」のプロパティも備えています。
- ポリシーラベルまたはポリシーファクター**:** 認証の特定の段階で試行されるポリシーの集まりです。
- 仮想サーバーラベル**:** 仮想サーバーはポリシーラベルでもあります。つまり、ポリシーを仮想サーバーにバインドできます。ただし、仮想サーバーは、ユーザーアクセスのエントリポイントであるため、さまざまなポリシーラベルの集まりです。
- 次の要素**:** 特定の認証ポリシーが成功したときに適用されるポリシーラベル/要素を指定するために使用されます。
- **NO_AUTHN** ポリシー**:** アクションが常に成功する特別なポリシー。
- パススルーファクター**:** ログインスキーマにビューが含まれていないポリシーラベル/ファクターです。これは、NetScaler ADC アプライアンスが、ユーザーの介入なしに指定された要素で認証を続行することを示します。

詳細については、nFactor の概念、エンティティ、および用語を参照してください。

EPA ファクター相互排他性

EPA ファクターには、1 つ以上の EPA ポリシーが含まれています。EPA ポリシーがファクタにバインドされると、そのファクタに対する通常の認証ポリシーは使用できません。この制限は、最高のユーザーエクスペリエンスを提供し、エンドポイント分析を明確に分離することです。この規則の唯一の例外は NO_AUTHN ポリシーです。NO_AUTHN ポリシーは「障害発生時のジャンプ」をシミュレートするために使用される特別なポリシーなので、EPA ファクターでは許可されています。

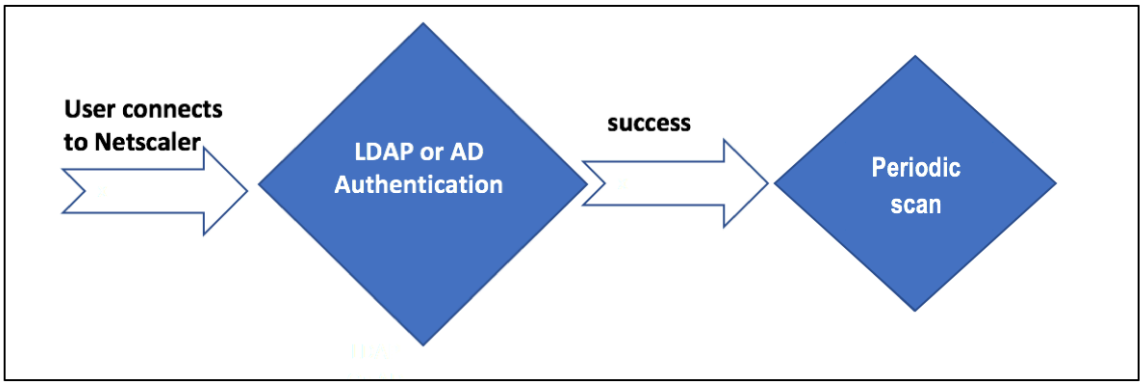
EPA の実行

任意の要素（仮想サーバーファクタを含む）で、ログオンフォームを提供する前に、NetScaler ADC アプライアンスはファクタが EPA 用に構成されているかどうかを確認します。その場合、EPA シーケンスがトリガーされるように、

特定の応答をクライアント (UI) に送信します。このシーケンスでは、クライアントがクライアントデバイスのチェック式を要求し、結果を送信します。
ファクタ内のすべてのポリシーのクライアントデバイスチェック式は、クライアントに一度に送信されます。NetScaler ADC アプライアンスで結果が得られると、すべてのアクションの各式が順番に評価されます。EPA が成功する最初のアクションはその要素を終了し、defaultGroup (構成されている場合) はセッションに継承されます。NO_AUTHN ポリシーが検出された場合、それは自動成功と見なされます。nextFactor が指定されている場合、アプライアンスはそのファクタで続行します。それ以外の場合、認証は終了します。
この条件は、第 1 因子にも当てはまります。仮想サーバーで EPA の後に認証ポリシーファクタがない場合、認証は終了します。これは、EPA の後にユーザーに常にログインページが表示される従来のポリシーの動作とは異なります。ただし、EPA ポリシーが成功しない場合、NetScaler Gateway は、そのファクタまたはカスケードの最後の EPA ポリシーに対して構成された検疫グループを検索します。最後のポリシーが検疫グループで構成されている場合、そのグループがセッションに追加され、NextFactor が検査されます。NextFactor が存在する場合、認証はその要素に進みます。それ以外の場合、認証は完了します。

認証後に実行するように **EPA** スキャンを設定

認証後に EPA スキャンを実行するように構成できます。次の例では、EPA スキャンは nFactor 認証または多要素認証の最終チェックとして使用されます。この設定では、このようなチェック中に EPA スキャンが失敗すると、セッションは終了します。



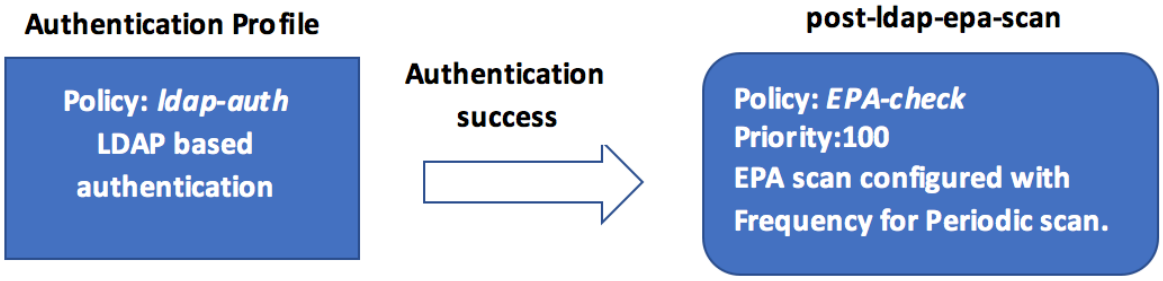
- ユーザーが NetScaler Gateway 仮想 IP に接続しようとしました。
- ユーザー名とパスワードフィールドを含むログインページがユーザーにレンダリングされ、ログイン資格情報が提供されます。これらの資格情報を使用して、LDAP または AD ベースの認証がバックエンドで実行されます。成功すると、EPA スキャンを承認するためのポップアップがユーザーに表示されます。
- ユーザーが承認すると、EPA スキャンが実行され、ユーザークライアント設定の成功または失敗に基づいて、アクセスが提供されます。
- スキャンが成功すると、EPA スキャンが定期的に実行され、設定されているデバイスチェック要件が満たされているかどうかが確認されます。
- このようなチェック中に EPA スキャンが失敗すると、セッションは終了します。

前提条件

次の設定が行われていると仮定します。

- VPN 仮想サーバ、ゲートウェイ、および認証仮想サーバの設定
- LDAP サーバの設定と関連付けられたポリシー。

次のセクションでは、必要なポリシーとポリシーラベルの設定、およびポリシーとポリシーラベルの認証プロファイルへのマッピングについて説明します。



CLI で

1. LDAP 認証の前に EPA スキャンを実行するアクションを作成し、EPA スキャンポリシーに関連付けます。

```
add authentication epaAction pre-ldap-epa-action -csecexpr "sys.client_expr ("proc_2_firefox")"

add authentication Policy pre-ldap-epa-pol -rule true -action pre-ldap-epa-action
<!--NeedCopy-->
```

   前述の式は、プロセス‘Firefox’が実行中かどうかをスキャンします。EPA クライアントは、スキャン表現の数字「2」で示されるように、2 分ごとにプロセスの存在を確認します。

2. EPA `pre-ldap-epa-label`スキャンのポリシーをホストするポリシーラベルを設定します。

```
add authentication policylabel pre-ldap-epa-label -loginSchema LSCHEMA_INT
<!--NeedCopy-->
```

   > 注:
   >
   > LSCHEMA_INT はスキーマのない組み込みスキーマです (スキーマなし)。つまり、このステップではユーザーに追加の Web ページは表示されません。

3. ステップ 1 で設定したポリシーを、ステップ 2 で設定したポリシーラベルに関連付けます。これで認証メカニズムは完了です。


```
bind authentication policylabel pre-ldap-epa-label -policyName pre
    -ldap-epa-pol -priority 100 -gotoPriorityExpression END
<!--NeedCopy-->
```

4. LDAP アクションとポリシーを設定します。

```
add authentication ldapAction ldap-act -serverIP 10.106.103.60 -
    ldapBase "dc=cgwsanity,dc=net" -ldapBindDn user1@example.net -
    ldapBindDnPassword 1.cloud -ldapLoginName samAccountName -
    groupAttrName memberOf -subAttributeName CN -passwdChange
    ENABLED

add authentication Policy ldap-pol -rule true -action ldap-act
<!--NeedCopy-->
```

5. SSO を有効にしたログインスキーマを作成します。

```
add authentication loginSchema ldap-schema -authenticationSchema "
    /nsconfig/loginschema/LoginSchema/SingleAuth.xml" -
    SSOCredentials Yes
<!--NeedCopy-->
```

6. LDAP `ldap-pol-label`認証のポリシーをホストするポリシーラベルを設定します。

```
add authentication policylabel ldap-pol-label -loginSchema ldap-
    schema
<!--NeedCopy-->
```

7. ステップ 5 で設定したログインスキーマを、ステップ 6 で設定したポリシーラベルにバインドします。

```
bind authentication policylabel ldap-pol-label -policyName ldap-
    pol -priority 100 -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

8. LDAP 認証後に EPA スキャンを実行するアクションを作成し、EPA スキャンポリシーに関連付けます。

```
add authentication epaAction post-ldap-epa-action -csecexpr "sys.
    client_expr ("proc_2_chrome")"

add authentication Policy post-ldap-epa-pol -rule true -action
    post-ldap-epa-action

add authentication policylabel post-ldap-epa-label -loginSchema
    LSCHEMA_INT

bind authentication policylabel post-ldap-epa-label -policyName
    post-ldap-epa-pol -priority 100 -gotoPriorityExpression
<!--NeedCopy-->
```

9. すべてをまとめて、`pre-ldap-epa-pol` ポリシーを認証仮想サーバーに関連付けます。次のステップでは、`ldap-pol-label` ポリシーラベルを指して EPA スキャンを実行します。


```
bind authentication vserver user.auth.test -policy pre-ldap-epa-pol -priority 100 -nextFactor ldap-pol-label -gotoPriorityExpression NEXT

bind authentication policylabel ldap-pol-label -policyName ldap-pol -priority 100 -gotoPriorityExpression NEXT -nextFactor post-ldap-epa-label
<!--NeedCopy-->
```

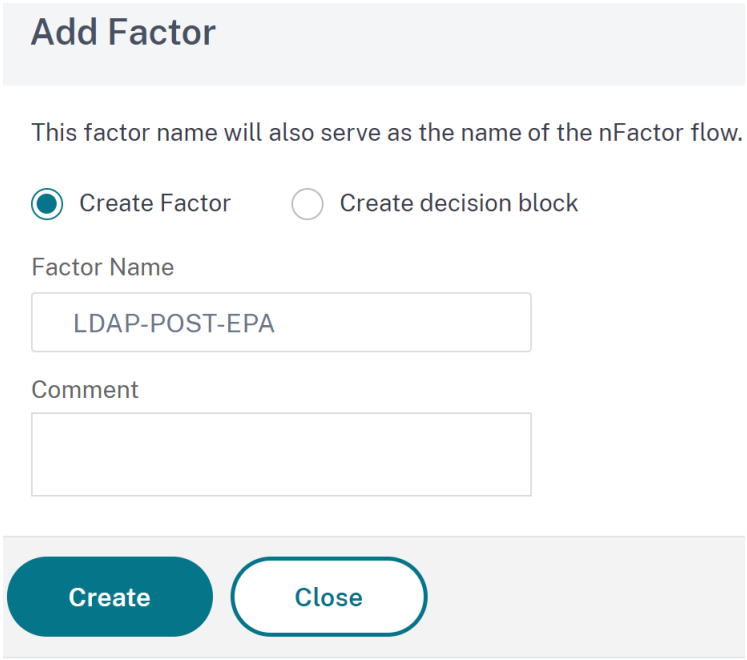
注:

- 複数のファクターとして設定された定期的な EPA では、定期的な EPA 設定による最新のファクターが考慮されます。
- 定期スキャンは EPA プラグインを使用してのみ実行でき、ブラウザでは実行できません。
- 最初の例では、EPA がスキャンでプロセス「Firefox」を検索する最初の要素です。
- EPA スキャンが成功すると、LDAP 認証が行われ、次の EPA スキャンが行われ、プロセス「Chrome」が検索されます。
- 複数の定期スキャンが異なるファクタとして設定されている場合は、最新のスキャンが優先されます。この場合、EPA プラグインは、ログインが成功してから 2 分ごとにプロセス「Chrome」をスキャンします。

GUI 上 (nFactor ビジュアライザーを使用)

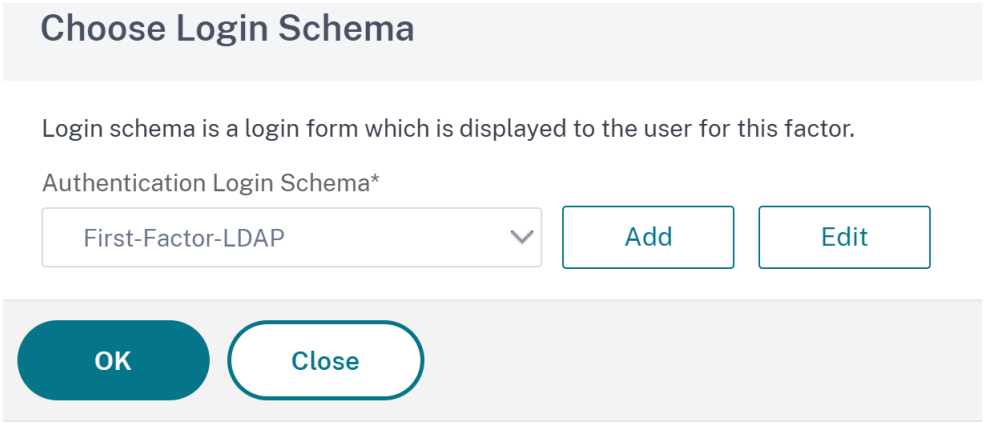
GUI の nFactor ビジュアライザーを使用して、高度な EPA スキャンをファクターとして設定できます。次の例では、最初の要素として LDAP を使用し、次の要素として EPA を使用しています。

1. nFactor フローの 1 つ目のファクターを作成します。
   - [セキュリティ] > [AAA アプリケーショントラフィック] > [nFactor ビジュアライザー] > [nFactor フロー] に移動し、[追加] をクリックします
   - + をクリックして nFactor フローを追加します。
   - 係数を追加して [作成] をクリックします。



2. 1 つ目の要素のログインスキーマとポリシーを作成します。

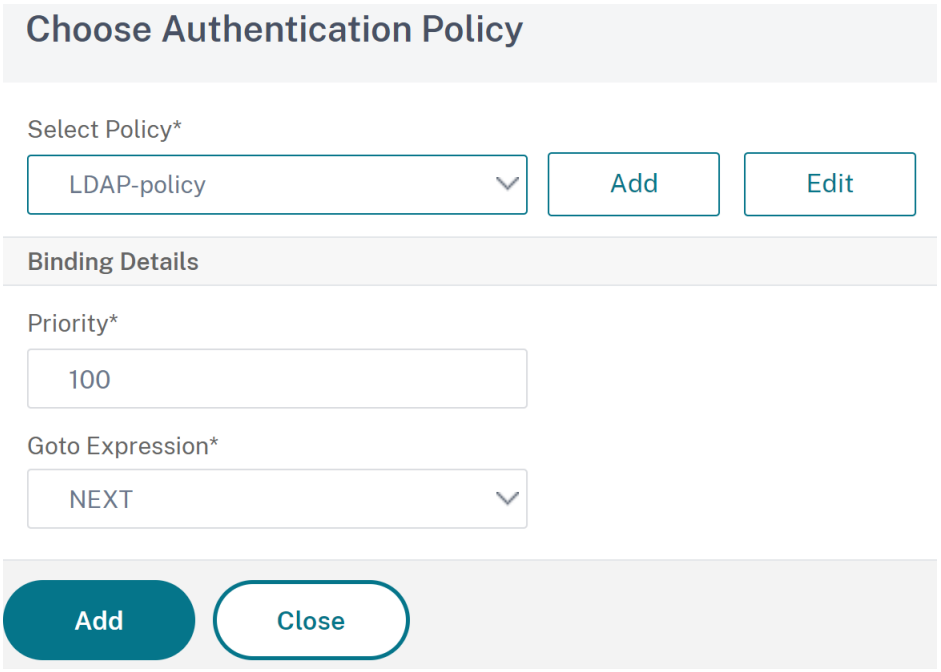
   - 最初のファクタータイルで、[スキーマの追加] をクリックしてログインスキーマを追加します。ドロップダウンリストから既存の認証ログインスキーマを選択するか、ログインスキーマを作成できます。
   - 認証ログインスキーマを作成するには、「追加」をクリックします。認証ログインスキーマの詳細については、「nFactor 認証の設定」を参照してください。

   - [ポリシーの追加] をクリックして LDAP ポリシーを追加します。LDAP ポリシーがすでに作成されている場合は、同じポリシーを選択できます。[追加] をクリックします。

     > 注:
     >
     > LDAP ポリシーが作成されていない場合は、作成できます。「ポリシーの選択」ドロップダウンリストの横にある「追加」ボタンをクリックします。「アクション」フィールドで「LDAP」を選択し

> ます。認証 LDAP サーバの追加の詳細については、を参照してください https://support.citrix.com/article/CTX123782。

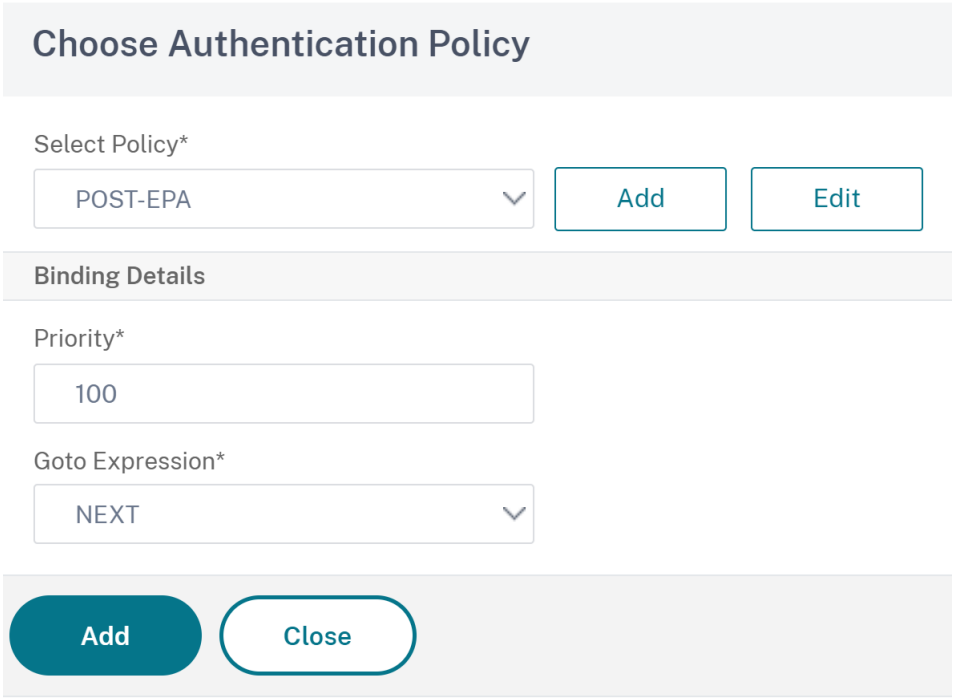


3. 次のファクターを作成し、それを最初のファクターに接続します。

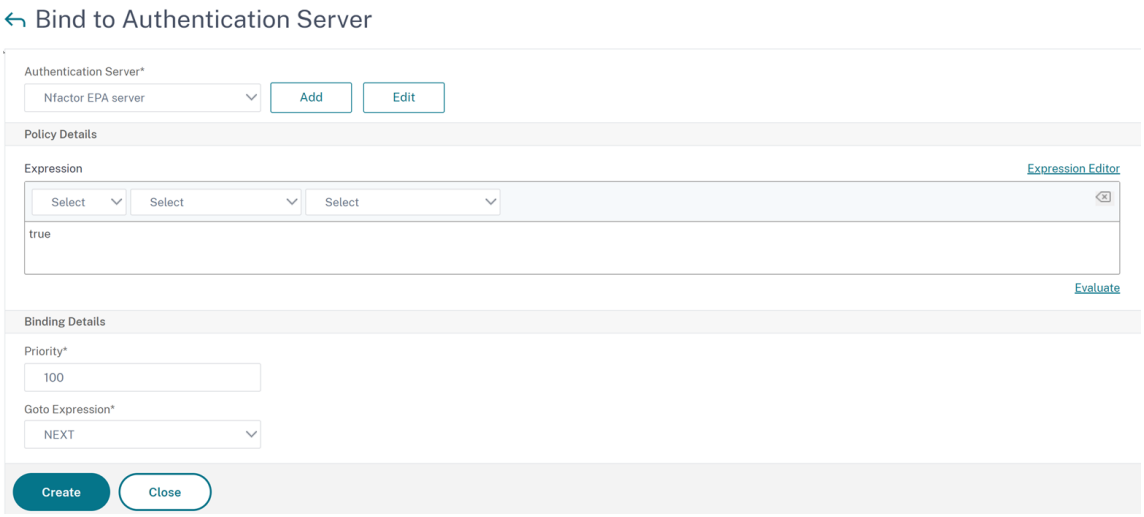
   - 緑色または赤色の「+」アイコンをクリックして、次の要素として EPA を追加します。
   - 「次の接続要素」ページで次の要素を作成します。
   - 「スキーマの追加」セクションを空白のままにすると、デフォルトではこのファクターにスキーマが適用されません。

4. 次の要素に関するポリシーを追加してください。

   - 「ポリシーを追加」をクリックして、認証後の EPA ポリシーとアクションを追加します。
   - 既存のポリシーのリストから選択するか、ポリシーを作成できます。既存のポリシーから選択するには、「ポリシーの選択」ドロップダウンリストからポリシーを選択し、バインドの詳細を入力して、「追加」をクリックします。
   - ポリシーを作成するには、「ポリシーの選択」ドロップダウンリストの横にある「追加」ボタンをクリックします。



5. nFactor フローが完了したら、[完了] をクリックします。
6. nFactor フローを認証サーバーにバインドします。
   - [セキュリティ **AAA-**アプリケーショントラフィック] **> [nFactor** ビジュアライザー] **> [nFactor** フロー] に移動します。
   - nFactor を選択し、[認証サーバーにバインド] をクリックします。



参照ドキュメント

- 多要素（nFactor）の概念、エンティティ、用語

- NetScaler Gateway で LDAP 認証を構成する方法
- LDAP 認証
- Advanced Endpoint Analysis スキャン

Windows クライアントの EPA スキャン分類タイプ

April 1, 2024

> 重要:
>
> エンドポイント分析は、あらかじめ決められたコンプライアンス基準に照らしてユーザーデバイスを分析することを目的としており、エンドユーザーデバイスのセキュリティを強制または検証するものではありません。ローカル管理者による攻撃からデバイスを保護するには、エンドポイントセキュリティシステムを使用することをお勧めします。

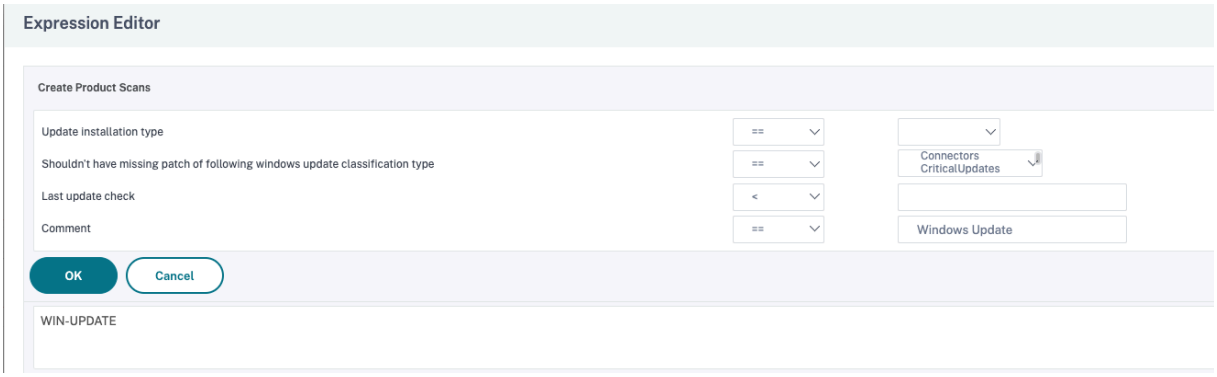
以下の新しい分類タイプが、不足しているパッチの EPA スキャンに追加されます。クライアントに次の不足しているパッチのいずれかがある場合、EPA スキャンは失敗します。

- アプリケーション
- コネクタ
- クリティカルなアップデート
- 定義更新
- developerKits
- FeaturePack
- ガイダンス
- セキュリティアップデート
- ServicePack
- ツール
- UpdateRollUps
- アップデート

> メモ:
>
> - 以前は、Windows クライアントでは、見つからないパッチの EPA スキャンは、重大度（緊急、重要、中、低）で実行されていました。
> - Citrix Secure Access for Windows 23.8.1.1 以降を使用している場合、`CLIENT.SYSTEM('WIN-UPDATE_SCAN-TIME')` スキャンは自動更新が有効になっているクライアントマシンに限定されます。自動更新が無効になっている場合、このスキャンは異なる結果を返します。

GUI を使用して EPA スキャン分類タイプを構成する

1. **NetScaler Gateway >** ポリシー **>** 事前認証に移動します。
2. 新しい事前認証ポリシーを作成するか、既存のポリシーを編集します。
3. [**OPSWAT EPA** エディタ**]** リンクをクリックします。
4. 式エディタで [ウィンドウ**] > [Windows Update**] を選択します。
5.「次のセキュリティレベルのパッチがないはずがない」で、不足しているパッチの分類タイプを選択します。
6. [**OK**] をクリックします。



お客様は、これらのオプションを使用するために OPSWAT バージョン 4.3.2744.0 にアップグレードできます。

参照ドキュメント

- Windows サーバー更新サービスの分類 GUID の詳細については、https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ff357803(v=vs.85)を参照してください。
- Microsoft ソフトウェア更新プログラムの用語の説明については、「https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/standard-terminology-software-updates」を参照してください。

Advanced Endpoint Analysis スキャン

April 1, 2024

高度なエンドポイント分析（EPA）は、NetScaler Gateway で設定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 NetScaler Gateway にアクセスしようとすると、管理者が NetScaler Gateway へのアクセスを許可する前に、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デバイスからスキャンされます。Citrix EPA クライアントのシステム要件について詳しくは、「エンドポイント分析要件」を参照してください。

高度な EPA スキャンは、NetScaler Gateway で認証セッション用に構成できるポリシーベースのスキャンです。このポリシーは、ユーザーデバイス上でレジストリチェックを実行し、評価に基づいて、NetScaler ADC ネットワークへのアクセスを許可または拒否します。

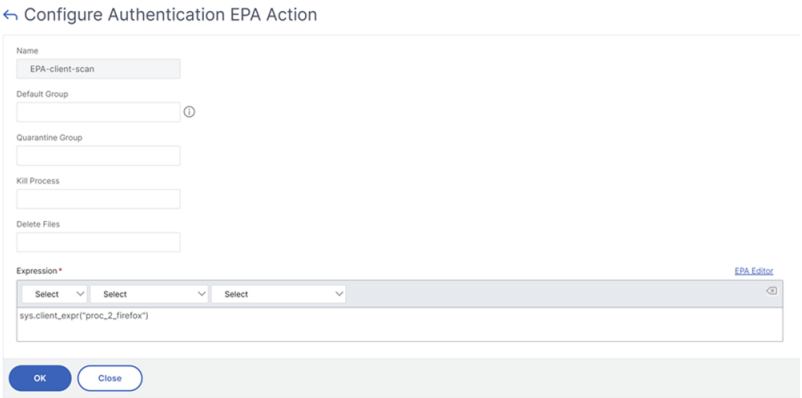
GUI または CLI を使用して高度な EPA スキャンを設定できます。

GUI について

1. EPA アクションを作成します。

   [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 **] > [**詳細ポリシー **] > [**アクション **] > [EPA**] に移動し、[追加] をクリックします。「認証 **EPA** アクションの作成」ページで、次の情報を更新し、「作成」をクリックします。

   - 名前:EPA アクションの名前。
   - デフォルトグループ:EPA チェックが成功したときに選択されるデフォルトグループ。
   - 検疫グループ:EPA チェックが失敗したときに選択される検疫グループ。
   - Kill Process: EPA プラグインによって終了されるプロセスの名前を指定する文字列。複数のプロセスはカンマで区切る必要があります。
   - ファイルの削除:EPA プラグインによって削除されるファイルのパスと名前を指定する文字列。複数のファイルはカンマで区切る必要があります。
   - 表現:EPA 表現形式については、アドバンスドエンドポイント分析ポリシー表現リファレンスを参照してください 。

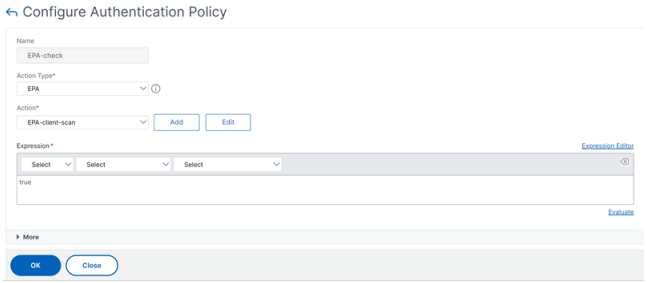
   

2. 対応する EPA ポリシーを作成します。

   [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 **] > [**詳細ポリシー **] > [**ポリシー] に移動し、[追加] をクリックします。「認証ポリシーの作成」ページで、次の情報を更新し、「作成」をクリックします。

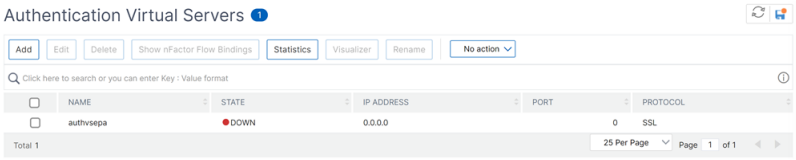
   - 名前: 詳細な EPA ポリシーの名前。
   - アクションタイプ: 認証アクションのタイプ。
   - アクション: ポリシーが一致した場合に実行される認証アクションの名前。

- 表現:EPA 表現形式については、アドバンスドエンドポイント分析ポリシー表現リファレンスを参照してください 。
- ログアクション: リクエストがこのポリシーに一致する場合に使用するメッセージログアクションの名前。最大許容長は 127 文字です。

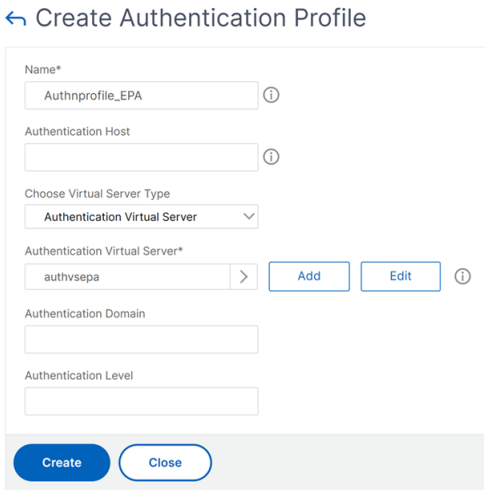


3. 認証仮想サーバーと認証プロファイルを設定します。

   - [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、[追加] をクリックします。

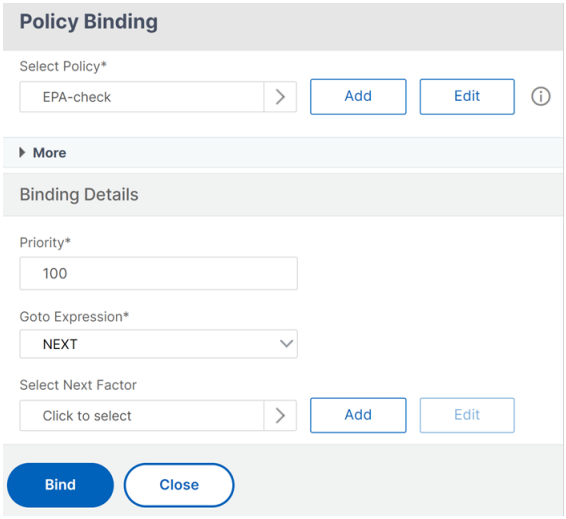


   - [セキュリティ] **> [AAA-**アプリケーショントラフィック] **> [**認証プロファイル] に移動し、[作成] をクリックします。



4. 高度な EPA ポリシーを認証仮想サーバーにバインドします。

   - [セキュリティ] **> [AAA-**アプリケーショントラフィック] **> [**認証仮想サーバー] に移動し、認証仮想サーバーを選択します。
   - 「詳細認証ポリシー」セクションでポリシーを選択します。
   - 「ポリシーバインディング」セクションの「バインド」をクリックします。



5. EPA ポリシーを nFactor フローにバインドします。

   高度な EPA ポリシーを nFactor フローの要素として追加する方法の詳細については、nFactor 認証の要素としての EPA スキャンを参照してください。

CLI で

1. EPA スキャンを実行するアクションを作成します。

```
1 add authentication epaAction EPA-client-scan -csecexpr "sys.
     client_expr ("proc_2_firefox")"
2 <!--NeedCopy-->
```

   上記の式は、プロセス「Firefox」が実行されているかどうかをスキャンします。EPA プラグインは、スキャン式の数字「2」で表される 2 分ごとにプロセスの存在をチェックします。

2. EPA アクションを高度な EPA ポリシーに関連付けます。

```
1 add authentication Policy EPA-check -rule true -action EPA-client-
     scan
2 <!--NeedCopy-->
```

3. 認証仮想サーバーと認証プロファイルを設定します。

```
1 add authentication vserver authnvsepa ssl -ip address
     10.104.130.129 -port 443
2 <!--NeedCopy-->
```

```
1 add Authnprofile_EPA -authnVsName authnvsepa
2 <!--NeedCopy-->
```

4. 高度な EPA ポリシーを認証仮想サーバーにバインドします。

```
1 bind authentication vs authnvsepa -policy EPA-check -pr 1
```



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

EPA ライブラリをアップグレードする

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:

1. ［構成］**>**［**NetScaler Gateway**］**>**［クライアントコンポーネントの更新］に移動します。
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（**Upgrade**）] をクリックします。

> 重要:
>
> - NetScaler Gateway の高可用性では、EPA ライブラリをプライマリノードとセカンダリノードの両方でアップグレードする必要があります。
> - NetScaler Gateway クラスタリングセットアップでは、すべてのクラスタノードで EPA ライブラリをアップグレードする必要があります。

NetScaler スキャン用の OPSWAT でサポートされている Windows および MAC アプリケーションのリストについては、https://support.citrix.com/article/CTX234466を参照してください。

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

Advanced Endpoint Analysis スキャンのトラブルシューティングに役立つように、クライアントプラグインはクライアントエンドポイントシステム上のファイルにログ情報を書き込みます。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\\ ローカル\\ Citrix\\ AGEE\\ nsepa.txt

Windows XP:

C:\Documents と設定\ すべてのユーザー\ アプリケーションデータ\ Citrix\ AGEE\ nsepa.txt

Mac OS X システム**:**

~/ライブラリ/アプリケーション Support/Citrix/EPAPlugin/epaplugin.log

(ここで、~ 記号は該当する macOS ユーザーのホームディレクトリパスを示します。)
(ここで、~ 記号は該当する macOS ユーザーのホームディレクトリパスを示します。)

Ubuntu:

- ~/.citrix/nsepa.txt
- ~/.citrix/nsgcepa.txt

高度なエンドポイント分析ポリシー式リファレンス

February 1, 2024

このトピックでは、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。NetScaler Gateway 構成ユーティリティは、ここに含まれる式要素を自動的に構築し、手動で構成する必要はありません。

エクスプレッションフォーマット

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とおりです:

スキャンタイプは、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 ID です。

method-name は、分析対象の製品属性またはシステム属性です。

メソッドコンパレータは、分析に選択されたコンパレータです。

method-param は、分析される 1 つまたは複数の属性値です。

例:

client.application(ANTIVIR_2600*RTP*==_TRUE)

> 注:
>
> 非アプリケーション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 になります。

エクスプレッション文字列

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は、式で一意の識別子を使用します。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

スキャンの種類	スキャンタイプの式文字列
バックアップクライアント	BACKUP
デバイスアクセス制御	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
ウェブブラウザ	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

> 注**:**
>
> macOS X 固有のスキャンの場合、式はメソッドタイプの前にプレフィックス MAC-を含みます。したがって、ウイルス対策およびフィッシング対策スキャンの場合、方法はそれぞれ MAC-ANTIVIR と MAC-ANTIPHI です。
>
> 例:
>
> client.application (MAC-ANTIVIR_2600*RTP*==_TRUE)

アプリケーションのスキャン方法

高度なエンドポイント分析式の設定では、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、式で使用可能なメソッドを列挙したものです。

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	コンパレータ	指定可能な値
VERSION*	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**	アプリケーションが本物かどうかを確認します。	==	TRUE
有効	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 (スキャンでは無視されます)。式内では [] で表されます。	==	任意のテキスト

* VERSION 文字列には、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**:**
>
> アプリケーションスキャンの種類には、汎用バージョンを選択できます。汎用スキャンを選択した場合、製品 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用意されています。汎用スキャンを使用すると、管理者はスキャンチェックを特定の製品に制限することなく、クライアントコンピュータをスキャンできます。

汎用スキャンの場合、スキャン方法は、ユーザーの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機能します。特定のスキャン方法をサポートしている製品については、NetScaler 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、指定されたスキャンの種類に固有のものです。

方法	説明	コンパレータ	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** 用: 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	コンパレータ	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	フルシステムスキャンが実行されてから何分経過したか。	<, <=, >, >=, !=, ==	任意の正数
VIRDEF-FILE-TIME	ウイルス定義ファイルが更新されてから何分経過したか（つまり、ウイルス定義ファイルのスタンプと現在のタイムスタンプの間の分数）。	<, <=, >, >=, !=, ==	任意の正数
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	コンパレータ	指定可能な値
LAST-BK-ACTIVITY	前回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。	<, <=, >, >=, !=, ==	任意の正数

表 4. データ損失防止

方法	説明	コンパレータ	指定可能な値
有効	アプリケーションが有効になっているかどうか、および時間保護がオンになっているかどうかを確認します。	==	TRUE

表 5. ヘルスチェックエージェント

方法	説明	コンパレータ	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	コンパレータ	指定可能な値
ENC-PATH	暗号化ステータスをチェックするための PATH。	NO OPERATOR	任意のテキスト
ENC-TYPE	指定したパスの暗号化タイプかどうかを確認します。	`allof`, `anyof`, `noneof`	次のオプションで一覧表示: 暗号化されていない、一部、暗号化、仮想、一時停止、保留中

表 7. Web ブラウザー

方法	説明	コンパレータ	指定可能な値
DEFAULT	デフォルト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	コンパレータ	指定可能な値

|SCAN-TIME| 前回のパッチのスキャンが実行されてから何分経過したか。|<, <=, >, >=, !=, ==| 任意の正数 |
|MISSED-PATCH| クライアントシステムには、これらのタイプのパッチがありません。|anyof, noneof| 任意の事前選択 (Patch Manager サーバで事前に選択されたパッチ)
NON|

テーブル 9. MAC アドレス

方法	説明	コンパレータ	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確認します。	anyof, noneof	編集可能なリスト

テーブル 10. ドメインメンバーシップ

方法	説明	コンパレータ	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ます。	anyof, noneof	編集可能なリスト

テーブル 11. 数値レジストリエントリ

方法	説明	コンパレータ	指定可能な値
PATH	レジストリチェックのパス。形式は次のとおりです。 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client\EnableAutoUpdate。 特殊文字のエスケープは不要です。すべてのレジストリルートキー： HKEY_LOCAL_MACHINE、 HKEY_CURRENT_USER、 HKEY_USERS、 HKEY_CLASSES_ROOT、 HKEY_CURRENT_CONFIG	NO OPERATOR	任意のテキスト

方法	説明	コンパレータ	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 リダイレクトに従います (つまり、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 リダイレクトは実行されません (つまり、32 ビットシステムと 64 ビットシステムでは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、次の記事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、REG_DWORD および REG_QWORD のレジストリタイプに対してのみ機能します。	<, <=, >, >=, !=, ==	任意の数字

MAC アドレスの EPA スキャン

April 1, 2024

NetScaler ADC リリース 13.0-88.x 以降では、許可または特定の MAC アドレスの EPA スキャン構成を構成できます。NetScaler ADC は、ポリシー式とパターンセットを使用して MAC アドレスのリストを指定します。

NetScaler リリース 13.0-88.x より前は、許可されているすべての MAC アドレスのリストを EPA 式の一部として指定する必要がありました。お客様が許可する MAC アドレスのリストが大量にある場合、すべての MAC アドレスを 1 つの式に追加するのは面倒でした。また、1 つの式に追加できる MAC アドレスの数にも制限がありました。

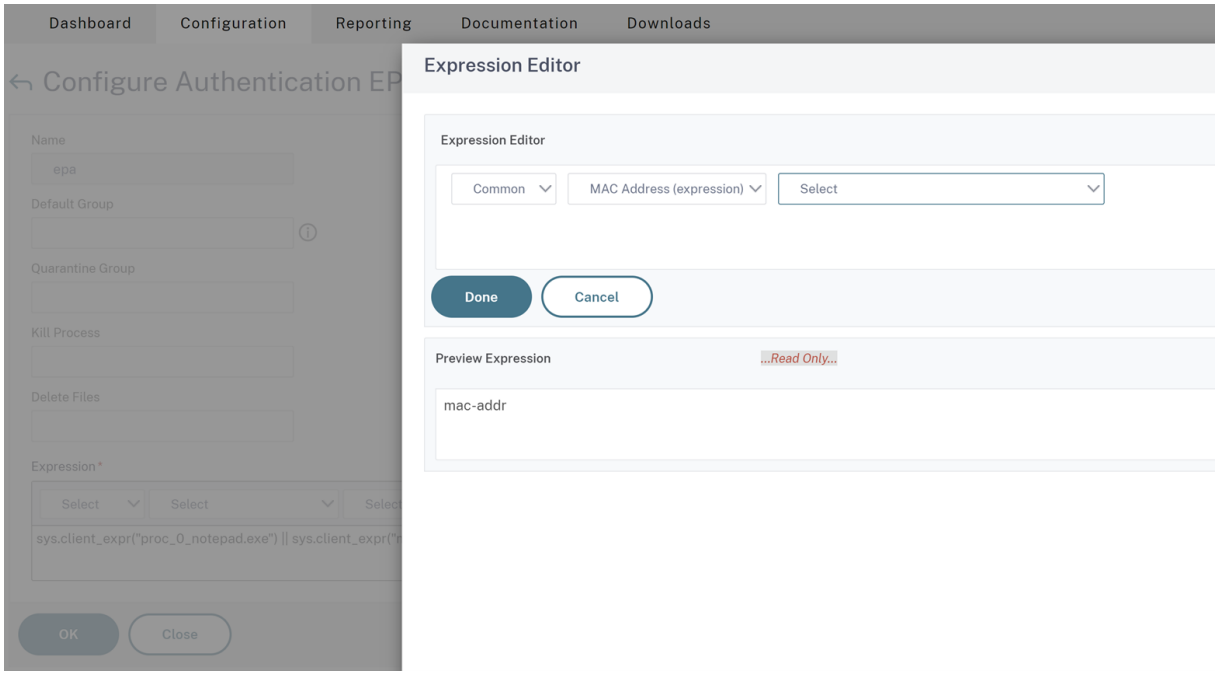
例:

```
1 add authentication epaAction epa -csecexpr q/sys.client_expr("
    proc_0_notepad.exe") || sys.client_expr("proc_0_chrome") || sys.
    client_expr("proc_0_firefox") && sys.client_expr("
    sys_0_MAC_ADDR_anyof_1AC89C83BOF7,0250F20A777C[COMMENT: MAC Address]
    ")/
2 <!--NeedCopy-->
```

GUI を使用して MAC アドレスの EPA スキャンを設定します

** 以前は **Windows** スキャンカテゴリで使用可能だった **MAC** アドレス（式）** オプションが、NetScaler **GUI** の共通スキャンカテゴリで使用できるようになりました。このオプションにより、ユーザーは許可または特定の MAC アドレスのリストの EPA スキャンを設定できます。

> 注:
>
> Citrix Secure Access Client 22.10.1 以降のバージョンでは、NetScaler ADC が GUI 上の EPA スキャン構成を処理するこの方法をサポートしています。



1. パターンセットを設定する。詳細については、「パターンセットを設定する」を参照してください。
2. パターンセットごとに、対応するポリシー式を作成します。

   エクスプレッションを設定するときに、エクスプレッションエディタで [**AAA] > [**ログイン**] > [CLIENT_MAC_ADDR] > [EQUAL_ANY (**文字列**)] > [**パターンセット**]** を選択します

   高度な式の設定について詳しくは、「ポリシーでの高度なポリシー式の構成」を参照してください。
3. 前のステップで構成した式の EPA スキャンを作成します。詳細については、高度なエンドポイント分析スキャンを参照してください。

CLI を使用して MAC アドレスの EPA スキャンを設定します

1. MAC アドレスをパターンセット内に格納します。

   コマンドプロンプトで次を入力します:

```
1 add policy patset <name> [-comment <string>]
2 <!--NeedCopy-->
```

   Example:

   ‘‘‘

   add policy patset patset1
   bind policy patset patset1 1A-C8-9C-83-BO-F7
   bind policy patset patset1 02-50-F2-0A-77-7C …and so on up to 3K entries.
   add policy patset patset2

bind policy patset patset2 1A-2B-3C-4D-5E-6A
bind policy patset patset2 1A-2B-3C-4D-5E-6B …and so on up to 3K entries.
‘‘‘

2. AAA.LOGIN.CLIENT_MAC_ADDR.equals_any() を使用して、各パターンセットに対応するポリシー式を作成します。

   コマンドプロンプトで次を入力します:

   ```
   Add policy expression <name> <value> [-comment <string>] [-
       clientSecurityMessage <string>]
   ```

   例:

   ```
   add policy expression exp1 AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("
       patset1")
   add policy expression exp2 AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("
       patset2")
   ```

3. 構成済みのポリシー式を使用して EPA スキャンを作成する

   コマンドプロンプトで次を入力します:

   ```
   add authentication epaAction <name>  -csecexpr <expression>
   ```

   例:

   ```
   add authentication epaAction epa -csecexpr q/sys.client_expr("
       proc_0_notepad.exe") || sys.client_expr("proc_0_chrome")  ||
       sys.client_expr("mac-addr_0_exp1") || sys.client_expr("mac-
       addr_0_exp2") || sys.client_expr("proc_0_firefox")/
   ```

   事前認証ポリシーを設定し、

   ```
   add authentication Policy epapol -rule true -action epa
   ```

   事前認証ポリシーをバインドし、

   ```
   bind authentication vserver <name> -policy epapol -priority 10 -
       gotoPriorityExpression NEXT
   ```

注意事項

- 許可された MAC アドレスのリストに対する EPA スキャンの設定は、nFactor 認証フローにのみ適用されます。
- 1 つのパターンセットには 3000 個以下のエントリを保存することをお勧めします。
- MAC アドレスは、1A-2B-3C-4D-5E-6F の形式で設定する必要があります。
- EPA スキャンの形式は`mac-addr_0_<policy-expression-name>`です。この形式では、`mac-addr_0_`は静的な値であり、`mac-addr_0_`後にポリシー式名を入力する必要があります。

- EPA スキャンは、記号 (||, &&) を使用して適切に分離できます。
- 1 つのパターンセットに多数の MAC アドレスを追加するには、ファイルベースのパターンセットのインポートを使用できます。最適なパフォーマンスを得るには、最大 3000 個のエントリ/パターンセットを保存することをお勧めします。
- MAC アドレスがファイル内に存在する場合、ファイルベースのパターンセットのインポートを使用し、インポート時に適切な区切り文字を指定することで、パターンセットを作成できます。

参照ドキュメント

- パターンセットを設定する。
- ファイルベースのインポートを使用してパターンセットを作成します。
  “‘

ユーザーセッションの管理

February 1, 2024

NetScaler GUI で［アクティブユーザーセッション］ダイアログボックスからユーザーセッションを管理できます。このダイアログボックスには、NetScaler Gateway 上のアクティブなユーザーセッションの一覧が表示されます。ユーザー名、グループ名、または IP アドレスを使用して、エンドユーザーまたはグループセッションを表示できます。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
- 仮想サーバーのポート番号
- ユーザーに割り当てられたイントラネット IP アドレス

GUI を使用したユーザーセッションの管理

ユーザーセッションを表示するには

1. NetScaler GUI のナビゲーションペインで、［**NetScaler 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. [アクティブユーザーセッション] で、次のタイプから選択します。

- アクティブユーザー
- アクティブグループ
- [イントラネット **IP**]-[イントラネット IP] を選択した場合は、イントラネット IP アドレスとサブネットマスクを入力する必要があります。

4. ［続行］をクリックします。

セッションリストを更新するには

NetScaler Gateway へのセッションに関する更新された情報を取得できます。

1. NetScaler GUI のナビゲーションペインで、［**NetScaler 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。

エンドユーザーまたはグループセッション、または特定のイントラネット **IP** アドレスを持つセッションを終了するには

ユーザーセッションとグループセッションを終了できます。また、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. NetScaler GUI のナビゲーションペインで、［**NetScaler 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、特定のイントラネット IP アドレスを持つユーザー、グループ、またはセッションを選択し、[終了] をクリックします。

CLI を使用してユーザセッションを管理する

次の CLI コマンドを使用して、ユーザセッション、エンドユーザ、またはグループセッションを表示できます。

- `show aaa session`-指定したユーザー、グループ、IP アドレス、または IP 範囲にバインドされているすべての NetScaler ADC 認証、承認、監査、または VPN 接続を表示します。
- `show vpn icaConnection` -ICA プロキシを使用するすべてのアクティブな接続を表示します。
- `show system session` -現在のすべてのシステムセッション、または指定されたセッションに関する情報を表示します。

常時オン

April 2, 2024

NetScaler Gateway の常時接続機能により、ユーザーは常にエンタープライズ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
>
> 常時オン機能は、NetScaler 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。

Always On をいつ使用するのか

ユーザーの位置情報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は、Always On を使用します。

次のシナリオは、Always On の使用方法を示しています。

- 従業員がエンタープライズネットワークの外部でノートパソコンを起動し、VPN 接続を確立するための支援を必要としています。
  解決方法**:** 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、Always On はシームレスにトンネルを確立し、VPN 接続を提供します。
- VPN 接続を使用している従業員は、エンタープライズネットワークに移動します。従業員は企業ネットワークに切り替えられますが、VPN トンネルへの接続は維持されますが、これは望ましい状態ではありません。
  解決方法**:** 従業員が企業ネットワークに移動すると、Always On は VPN トンネルを切断し、従業員をエンタープライズ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る（シャットダウンしない）。従業員は、ノートパソコンでの作業を再開する際に 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**:** 従業員が企業ネットワークの外に移動しても、Always On はシームレスにトンネルを確立し、VPN 接続を提供します。
- 企業は、VPN トンネルに接続していないときにユーザに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**:** 構成に応じて、Always On はアクセスを制限し、ユーザーはゲートウェイネットワークにのみアクセスできるようにします。

Always On フレームワークを理解する

Always On 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 VPN トンネルを初めて必要とするときは、ユーザーは NetScaler Gateway URL に接続してトンネルを確立する必要があります。Always On 設定がクライアントにダウンロードされた後、この設定によって後続のトンネルの確立が推進されます。

Citrix Secure Access クライアントの実行ファイルは、常にクライアントマシン上で実行されています。ユーザーがログオンするか、ネットワークが変更されると、Citrix Secure Access 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 Secure Access クライアントはトンネルを確立するか、既存のトンネルを解除します。

トンネルの確立は、ユーザーがコンピュータにログオンした後にのみ開始されます。Citrix Secure Access 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ゲートウェイサーバーを認証し、トンネルの確立を試みます。

トンネルの自動再確立

トンネルの自動再確立は、NetScaler Gateway によって VPN トンネルが切断されたときにトリガーされます。

> 注
>
> エンドポイント分析が失敗すると、NetScaler 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、NetScaler Gateway クライアントはユーザーに資格情報の入力を求めます。

シームレス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 +AD パスワード: 認証に Windows のユーザー名とパスワードを使用する場合、Citrix Secure Access 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、クライアントマシンに証明書が 1 つしかない場合、Citrix Secure Access 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は、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 Secure Access クライアントは、この優先証明書を後のトンネルに使用します。

  スマートカードがユーザー証明書を共有している場合、ストアにある証明書と比較して証明書がストアに動的にインストールされていると、自動ログオンを実行できません。
- 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、前述の認証方法を組み合わせたものです。

> 注
>
> 他のすべての認証メカニズムはサポートされますが、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。

常時オンの構成要件

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。

- ユーザーは、特定の構成のプロセス/サービスを終了できないようにする必要があります。
- 特定の構成では、ユーザーがパッケージをアンインストールできないようにする必要があります。
- ユーザーは特定のレジストリエントリを変更できないようにする

> 注
>
> 管理対象外のデバイスの場合のように、ユーザに管理特権がある場合、この機能が期待どおりに動作しない可能性があります。

常時オン機能を有効にする際の考慮事項

Always On 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分割トンネル設定に基づいて決定されます。この動作を上書きするための他の設定は提供されていません。

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、ゲートウェイサーバーへの接続時に無視されます。

> 注:
>
> NetScaler 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。システムで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。

常時オンの設定

常時接続を構成するには、NetScaler Gateway アプライアンスで常時接続プロファイルを作成し、プロファイルを適用します。

Always On プロファイルを作成するには:

1. NetScaler GUI で、［構成］**>** ［**NetScaler Gateway >** ［ポリシー］**>** ［**AlwaysOn**］に移動します
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—プロフィールの名前。
    - ** ロケーションベースの VPN (クライアント側のレジストリ名:LocationDetection) —次のいずれかの設定を選択します。
        - **Remote**： クライアントがエンタープライズネットワークにあるかどうかを検出し、エンタープライズ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。リモートはデフォルト設定です。
        - クライアントの場所に関係なく、クライアントが位置検出をスキップしてトンネルを確立できるようにするあらゆる場所
    - 「クライアント制御」—次の設定のいずれかを選択します:
        - [拒否] は、ユーザーがログオフして別のゲートウェイに接続できないようにします。[拒否] は既定の設定です。

- [許可]: ユーザーがログオフして別のゲートウェイに接続できるようにします。

- **VPN** 障害時のネットワークアクセス **(**クライアント側のレジストリ名**:alwaysOn)** —次のいずれかの設定を選択します。
  - [**Full Access**] は、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ようにします。[フルアクセス] が既定の設定です。
  - **[**ゲートウェイのみ（**Only Tto Gateway** ）] は、トンネルが確立されていないときにネットワークトラフィックがクライアントとの間で流れるのを防ぎます。ただし、ゲートウェイ IP アドレスとの間のトラフィックは許可されます。
    注: [ゲートウェイへのみ] モードでは、仮想サーバ、DNS、および DHCP トラフィックのみがブロック解除されます。他の Web サイト、IP アドレス範囲、または IP アドレスのブロックを解除するには、**AlwaysOnAllowList** レジストリに、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する必要があります。
    例えば、mycompany.com、mycdn.com,10.120.67.0-10.120.67.255,67.67.67.67

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。

Always On プロファイルを適用するには:

1. NetScaler ADC インターフェイスで、[構成] **>** [**NetScaler 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**:** セッションプロファイルでも同様の設定を行い、グループレベル、サーバレバー、またはユーザレベルでポリシーを適用できます。

IIP に関する注意事項

マシンレベルトンネルでは証明書ベースの認証が使用され、作成されるセッションには証明書の共通名がユーザー名として使用されます。そのため、デバイス証明書に一意の共通名がある場合、マシンのセッションごとにユーザー名が異なり、IIP も異なります。一意の名前を持つデバイス証明書を生成するようにしてください。デバイス証明書の共通名としてマシン名を使用するのが理想的です。

管理者ユーザーと管理者以外のユーザーの異なる設定の動作の概要

次の表は、さまざまな設定の動作をまとめたものです。また、Always On 機能に影響する可能性のある特定のユーザーアクションの可能性についても詳しく説明します。

VPN でのネットワークアクセスの失敗	クライアントコントロール	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、ネットワークからオフにできます。ユーザーは別の NetScaler 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。ユーザはログオフし、エンタープライズ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 NetScaler Gateway をポイントすることもできます。
fullaccess	拒否	トンネルは自動的に確立されます。ユーザーがログオフしたり、別の NetScaler 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 Secure Access クライアントをアンインストールするか、別の NetScaler Gateway に移動できます。
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 NetScaler 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 NetScaler 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 Secure Access クライアントをアンインストールするか、別の NetScaler Gateway に移動できます。
onlyToGateway	拒否	トンネルは自動的に確立されます。ユーザーがログオフしたり、別の NetScaler 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 Secure Access クライアントをアンインストールするか、別の NetScaler Gateway に移動できます。

「常時オン」がダウンしているときに選択した **URL** を許可する

Always On がダウンしていてネットワークがロックされている場合でも、ユーザはいくつかの Web サイトにアクセスできます。管理者は **AlwaysOnAllowList** レジストリを使用して、AlwaysOn がダウン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。

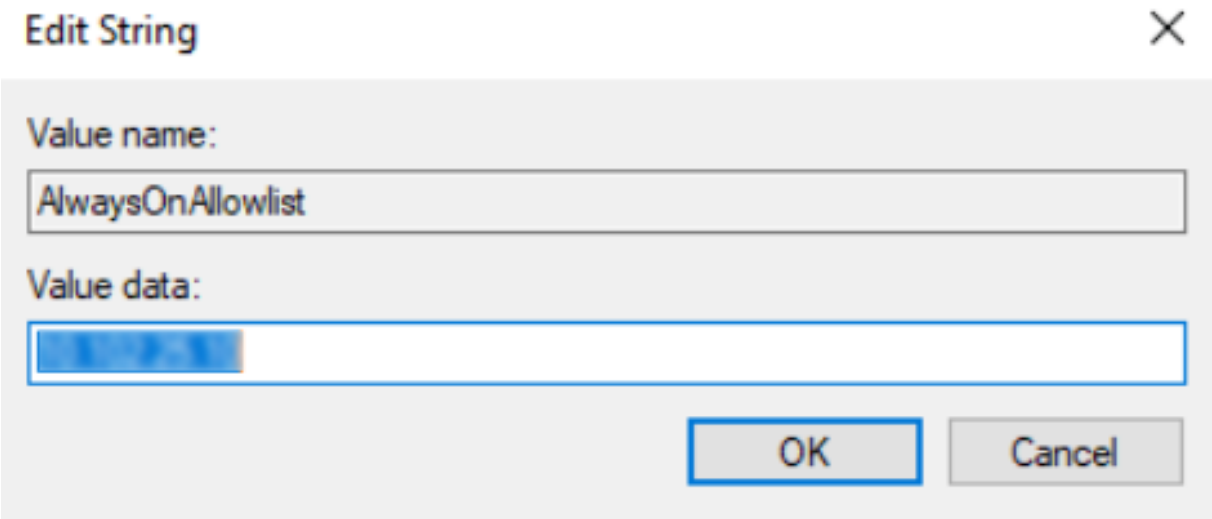
> 注:
>
> - **AlwaysOnAllowList** レジストリは、リリース 13.0 ビルド 47.x 以降でサポートされています。
> - **AlwaysOnAllowList** レジストリの場所は、Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client です。
> - ワイルドカード URL/FQDN は、**AlwaysOnAllowList** レジストリではサポートされていません。

AlwaysOnAllowList レジストリを設定するには

AlwaysOnAllowList 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: example.citrix.com; 10.103.184.156; 10.102.0.0-10.102.255.100

次の図に、**AlwaysOnAllowList** レジストリの例を示します。



Windows ログオン前に常時接続の VPN (正式には常時接続サービス)

February 1, 2024

Windows ログオン前の **AlwaysOn VPN** (正式には Always On サービス) 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あっても、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

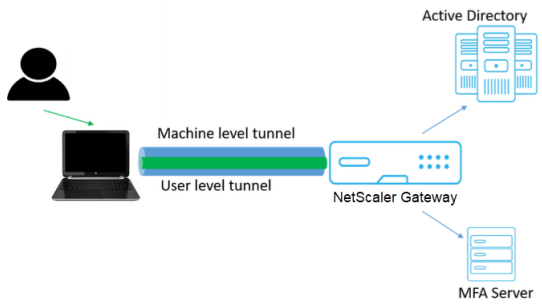
ンがシャットダウンするまでアクティブなままです。ユーザーがログオンすると、マシンレベルの VPN トンネルがユーザーレベル VPN トンネルに引き継がれます。ユーザーがログオフすると、ユーザーレベルのトンネルが破棄され、マシンレベルのトンネルが確立されます。**Windows** ログオン前の常時オン **VPN** は、高度な認証ポリシーのみを使用して構成できます。詳細については、「Windows ログオン前に常時接続 VPN を構成する」を参照してください。

Windows ログオン前に常にオン **VPN** 機能

- 管理者は、リモートで初めて作業するユーザーにワンタイムパスワードを提供できます。このワンタイムパスワードを使用して、ドメインコントローラに接続してパスワードを変更できます。
- 管理者は、ユーザーがログインする前であっても、デバイスに対する AD ポリシーをリモートで管理/適用できます。
- 管理者は、ユーザーがログオンした後のユーザーグループに基づいて、ユーザーにきめ細かなレベルの制御を提供できます。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できます。選択的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、複数のユーザーがキオスク内のマシンを面倒なく使用できます。
- リモートで作業しているユーザーは、ドメインコントローラに接続してパスワードを変更します。
- Windows マシンは、社内 Active Directory (AD) を使用してユーザーのログイン資格情報を確認でき、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。
- Windows マシンの VPN トンネルは、別のユーザーがマシンにログインまたはログアウトしても、接続されたままになります。

Windows ログオン前に常時接続の **VPN** について理解する

Windows ログオン前の常時接続 **VPN** 機能のイベントのフローを次に示します。



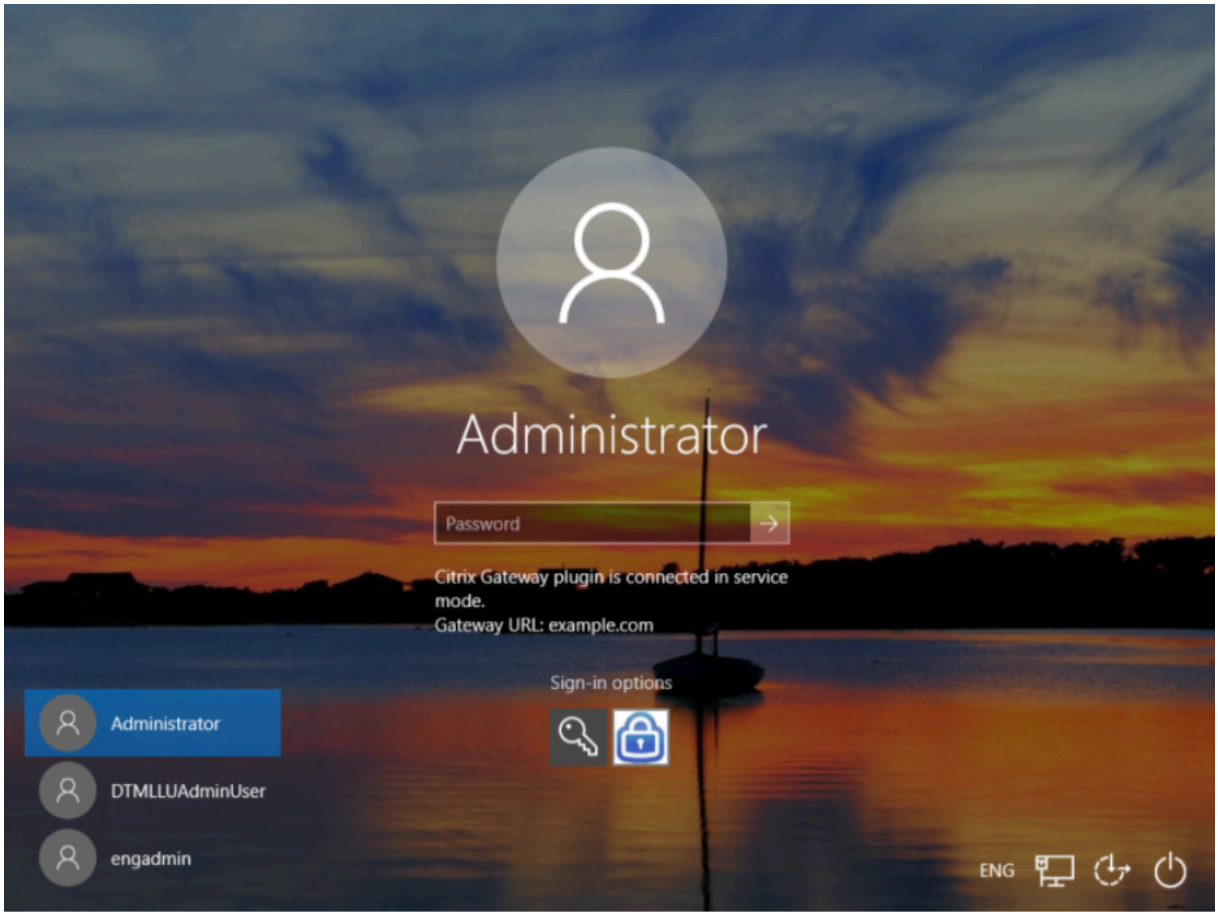
- ユーザーがラップトップの電源を入れます。デバイス証明書を ID として使用して、NetScaler Gateway に向けてマシンレベルのトンネルが確立されます。
- ユーザは AD クレデンシャルを使用してラップトップにログインします。
- ログイン後、ユーザーは MFA でチャレンジされます。
- 認証が成功すると、マシンレベルのトンネルはユーザレベルのトンネルに置き換えられます。
- ユーザがログアウトすると、ユーザレベルのトンネルはマシンレベルのトンネルに置き換えられます。

注意事項:

- NetScaler Gateway および VPN プラグインのバージョンは 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** ログオンの前に **Always On 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のを待機します。
- 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 **Always On VPN** はキャプティブポータルへのユーザ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を有効にすると、**Windows** ログオンが **VPN** トンネルを確立する前に **Always** On VPN が実行されます。
- Windows ログオン前に VPN を常時接続する機能では、NetScaler キャプティブポータルがサポートされています。
- 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は、次のシナリオでユーザーは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
- 管理者は、エンドユーザーにログオンページを表示する前に、デバイス証明書の失効ステータスを確認する必要があります。

Windows ログオン構成の前に常時接続の **VPN** の後の **Windows** 認証情報マネージャ画面

Windows ログオン前に常時オン **VPN** 機能を構成すると、**Windows** 資格情報マネージャーの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。

- NetScaler Gateway アイコンは、マシンが NetScaler 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。
  - NetScaler Gateway はサービスモードで接続されています
  - NetScaler Gateway はユーザーモードで接続されています

Windows ログオン前に常時接続の **VPN** を構成する

April 1, 2024

このセクションでは、詳細ポリシーを使用して **Windows** ログオンの前に **Always On VPN** を構成するための詳細をキャプチャします。

前提条件

- NetScaler Gateway および VPN プラグインのバージョンは 13.0.41.20 以降である必要があります。

- このソリューションが機能するには、NetScaler Advanced Edition 以上が必要です。
- この機能は、高度なポリシーを使用してのみ設定できます。
- VPN 仮想サーバーが稼働している必要があります。

大まかな設定手順

Windows ログオン前の常時接続 **VPN** の構成には、次の大まかな手順が含まれます。

1. マシンレベルトンネルのセットアップ
2. ユーザーレベルトンネルのセットアップ (オプション)
3. ユーザー認証を有効にする

    a) VPN 仮想サーバーを構成し、CA 証明書をインストールし、証明書キーを仮想サーバーにバインドします。
    b) 認証プロファイルを作成する
    c) 認証仮想サーバーを作成する
    d) 認証ポリシーの作成
    e) ポリシーを認証プロファイルにバインドします。

マシンレベルトンネル

デバイス証明書を ID として使用して、NetScaler Gateway に向けてマシンレベルのトンネルが確立されます。デバイス証明書は、クライアントマシンのマシンストアの下にインストールする必要があります。これは、[Windows ログオン前に常にオン] サービスにのみ適用されます。

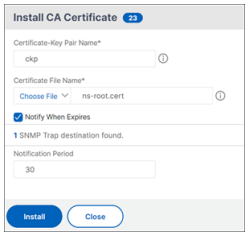
デバイス証明書について詳しくは、認証にデバイス証明書を使用するを参照してください。

> 重要:
>
> NetScaler Gateway アプライアンスの VPN 仮想サーバーが非標準ポート（443 以外）で構成されている場合、マシンレベルのトンネルは意図したとおりに機能しません。

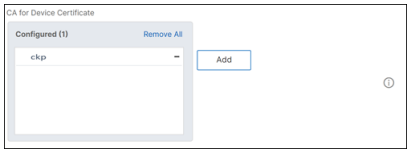
デバイス証明書を使用してマシンレベルトンネルをセットアップする

GUI を使用したデバイス証明書ベースの認証設定

1. ［構成］タブで、［**NetScaler Gateway**］**>**［仮想サーバー］に移動します。
2. **NetScaler 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. 「証明書」で、「**CA** 証明書」をクリックします。
4. 「**CA** 証明書のバインド」ページで、「CA 証明書の選択」フィールドの横にある「追加」をクリックし、必要な情報を更新して、「インストール」をクリックします。



5. **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。
6. [基本設定] セクションで、[詳細] をクリックします。
7. 「デバイス証明書用 **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。

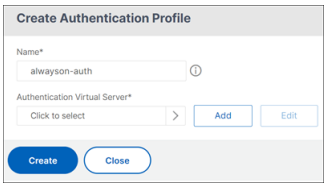
8. CA 証明書を仮想サーバーにバインドするには、[証明書] セクションの [**CA **** 証明書 **] をクリックします。[**SSL** 仮想サーバ **CA **** 証明書のバインド] ページで **[**バインドの追加 **] をクリックします。

> 注:
>
> - デバイス証明書のサブジェクトの共通名 (CN) フィールドは空にできません。デバイスが空の CN デバイス証明書でログインしようとすると、VPN セッションはユーザ名が「anonymous」として作成されます。IIP では、複数のセッションが同じユーザー名を持つ場合、以前のセッションは切断されます。したがって、IIP を有効にすると、共通名が空であるため、機能への影響に気付くでしょう。
> - クライアントに発行されたデバイス証明書に署名できる可能性のあるすべての CA 証明書（ルートおよび中間）は、手順 4 および 5 の [デバイス証明書の **CA**] セクションと、仮想サーバの [**CA** 証明書のバインド] セクションの下にバインドする必要があります。CA 証明書を中間/下位とリンクする方法の詳細については、「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。
> - 複数のデバイス証明書が設定されている場合、有効期限が最も長い証明書が VPN 接続に対して試行されます。この証明書で EPA スキャンが正常に許可されると、VPN 接続が確立されます。この証明書がスキャンプロセスで失敗すると、次の証明書が使用されます。このプロセスは、すべての証明書が試行されるまで続きます。

9. **CA** 証明書バインディングページで、証明書を選択します。
10. [**Bind**] をクリックします。
11. 認証仮想サーバーを作成します。

    a) 「**VPN** 仮想サーバー」ページで、「詳細設定」**>** 「認証プロファイル」に移動し、「追加」をクリックします。

b)「認証プロファイルの作成」ページで、認証プロファイルに名前を割り当て、「作成」をクリックします。



c) 認証仮想サーバーページで、認証仮想サーバーに名前を割り当てます。IP アドレスの種類を「アドレス指定不可」として選択し、「**OK**」をクリックします。

> 注:
>
> 認証仮想サーバーは常に DOWN 状態のままです。

12. 認証ポリシーを作成します。

a) [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] ページの [高度な認証ポリシー] セクションで、認証ポリシーを選択し、[バインドの追加] をクリックします。

b)「ポリシー・バインディング」ページで、「ポリシーの選択」フィールドの横にある「****** 追加 ****** 」をクリックします。

c)「認証ポリシーの作成」ページで。

i. 詳細認証ポリシーに名前を割り当てます。

ii. [アクションタイプ] リストから [**EPA**] を選択します。

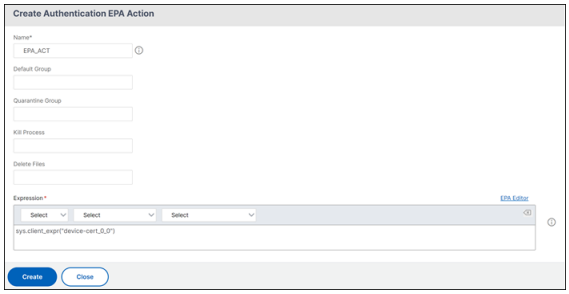
iii. [アクション] の横にある [追加] をクリックします。

d) [認証 EPA アクションの作成] ページで、

i. EPA アクションに名前を割り当てます。

ii. [式] `sys.client_expr("device-cert_0_0")` フィールドにと入力します。

iii. [**Create**] をクリックします。

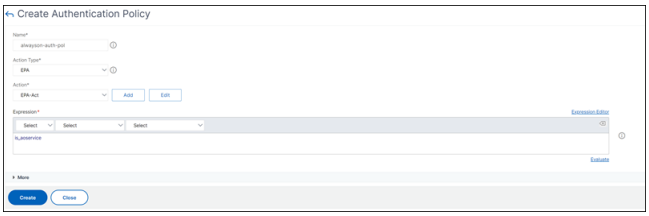


13. 「認証ポリシーの作成」ページで、

    a) 認証ポリシーに名前を割り当てます。

    b) [式] フィールドに **is_aoservice** と入力します。

    c) [**Create**] をクリックします。



14. [ポリシーのバインド] 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。

CLI を使用したデバイス証明書ベースの認証設定

1. VPN 仮想サーバーに CA 証明書をインストールします。

```
add ssl certkey ckp -cert t_CA.cer
<!--NeedCopy-->
```

2. CA 証明書を VPN 仮想サーバーにバインドします。

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
    Mandatory | Optional )
<!--NeedCopy-->
```

例

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA
    -ocspCheck Mandatory
<!--NeedCopy-->
```

3. 認証仮想サーバーを追加します。

```
add authentication authnProfile <name>  {
 -authnVsName <string> }

<!--NeedCopy-->
```


例

```
add authentication authnProfile always_on -authnVsName
    always_on_auth_server
<!--NeedCopy-->
```

4. 認証 EPA アクションを作成します。

```
add authentication epaAction <name> -csecexpr <expression>
<!--NeedCopy-->
```

Example

‘‘‘

add authentication epaAction epa-act -csecexpr sys.client_expr("device-cert_0_0") -defaultgroup epa_pass

‘‘‘

5. 認証ポリシーを作成する

```
add authentication Policy <name> -rule <expression> -action <
    string>
```

例:

```
add authentication Policy always_on_epa_auth -rule is_aoservice -
    action epa_auth
```

> 重要:
>
> - これで、マシンレベルのトンネルの設定は完了です。Windows ログオン後にユーザーレベルトンネルを設定するには、「ユーザーレベルトンネル」のセクションを参照してください。
> - クライアントマシンでは、デバイス証明書は.pfx 形式です。Windows では.pfx 形式が認識されるため、.pfx 証明書は Windows マシンにインストールされます。このファイルには、証明書ファイルとキーファイルが含まれています。この証明書は、仮想サーバにバインドされているドメインと同じである必要があります。.pfx とサーバーの証明書とキーは、クライアント証明書ウィザードを使用して生成できます。これらの証明書を認証局で使用して、サーバー証明書とドメインを含むそれぞれの.pfx を生成できます。証明書.pfx は、コンピューターアカウントの個人用フォルダーにインストールされます。`show aaa session`コマンドは、NetScaler ADC アプライアンス上のデバイストンネルを表示します。

ユーザーレベルトンネル

GUI を使用して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

注: 式`is_aoservice.not`は、NetScaler Gateway バージョン 13.0.41.20 以降から適用できます。

1. ユーザー認証のポリシーを構成します。

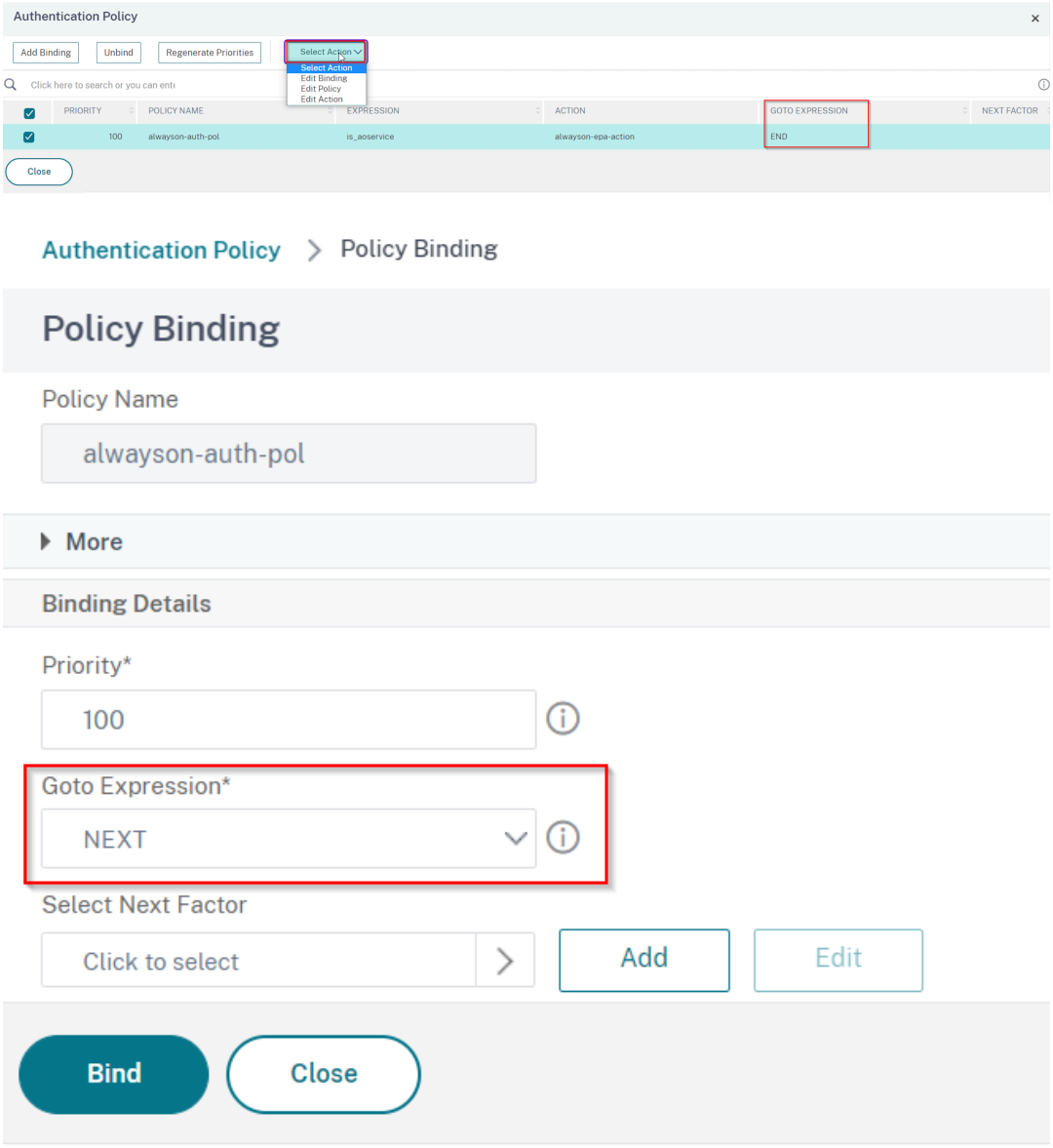
   a) [**NetScaler Gateway] > [**仮想サーバー] に移動し、仮想サーバーを選択します。

   b) [詳細設定] で、[認証プロファイル] をクリックします。

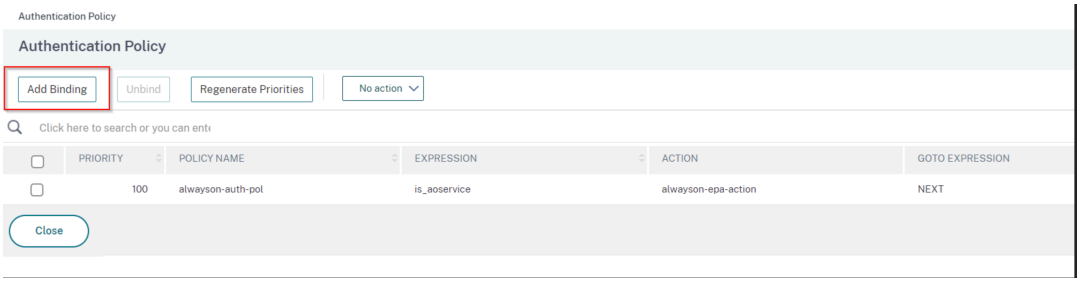
   c) 認証プロファイルを設定します。

   d) [構成] **> [**セキュリティ**] > [AAA** アプリケーショントラフィック**] > [**認証仮想サーバー] ページで、認証ポリシーを選択します。

   e) **[**アクションの選択] で [バインドの編集**]** をクリックし、ポリシーバインドの [**GoTo** 式] を [**END**] ではなく [**NEXT** 。



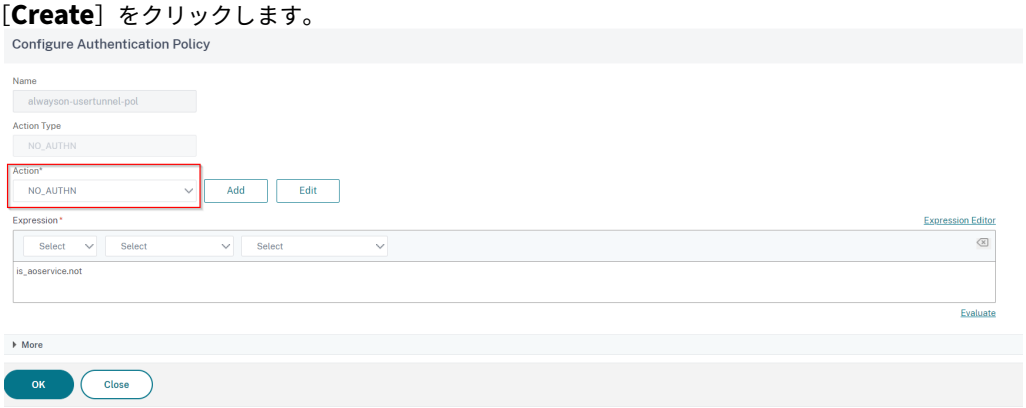
f) 「バインド」をクリックし、「認証ポリシー」ページで認証ポリシーを選択し、「バインドの追加」をクリックします。



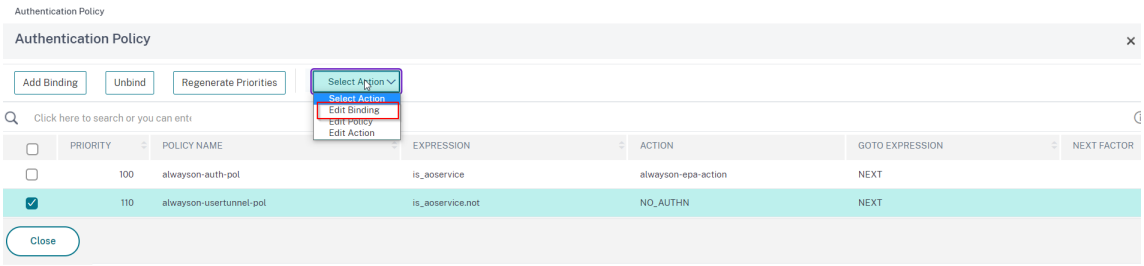
g) [ポリシーのバインド] ページで、[ポリシーの選択] の横にある [追加] をクリックします。

「認証ポリシーの作成」ページで。

i. 作成する「認証なし」ポリシーの名前を入力します。
ii. アクションタイプを **No_Authn** として選択します。
iii. [式] フィールドに **is_aoservice.NOT** と入力します。
iv. [**Create**] をクリックします。



2. 「アクションを選択」で、「バインドの編集」をクリックします。

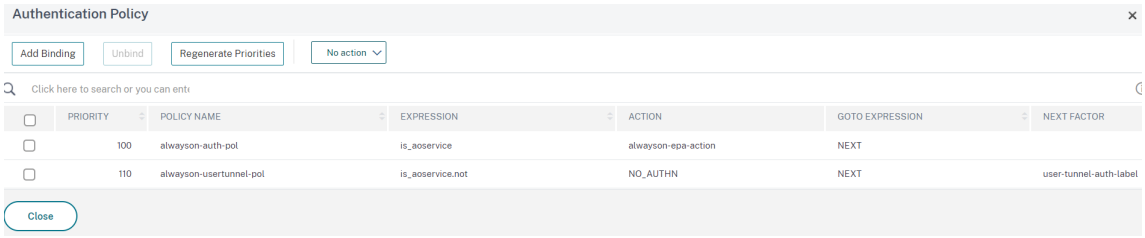


3. [ポリシーのバインド] ページで、[優先度] に **110** と入力します。[次の係数の選択**]** の横にある **[**追加] をクリックします。

a) [認証ポリシーラベル] ページで、ポリシーラベルのわかりやすい名前を入力し、ログインスキーマを選択して、[続行] をクリックします。
b) **[**ポリシーの選択] で、[追加] をクリックし、LDAP 認証ポリシーを作成します。
c) [作成**]** をクリックし、[バインド**]** をクリックします。

d) [完了] をクリックし、 [バインド] をクリックします。

[認証ポリシー] ページの [次の要素] 列に、構成済みの次の要素ポリシーが表示されます。



4. LDAP ポリシーを認証ポリシーの次の要素として設定できます。

   a) [認証ポリシーの作成] ページで、LDAP ポリシーの名前を入力します。
   b) [アクションタイプ] として [**LDAP**] を選択します
   c) 設定済みの LDAP アクションとして Action を入力します。

> 注:
>
> - ログインスキーマ XML ファイルの作成については、「ログインスキーマ XML ファイル」を参照してください。
> - ポリシーラベルの作成については、ポリシーラベルの認証を参照してください。
> - LDAP 認証ポリシーの作成については、「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。

CLI を使用してマシンレベルトンネルをユーザーレベルトンネルに置き換える

1. ポリシーを認証仮想サーバにバインドする

```
bind authentication vserver <name> -policy <name> -priority  <
    positive_integer> -gotoPriorityExpression <expression>
```

例

```
bind authentication vserver alwayson-auth-vserver -policy alwayson
    -auth-pol -priority 100 -gotoPriorityExpression NEXT
```

2. アクションをNO_AUTHと式is_aoservice.not,として持つ認証ポリシーを追加し、ポリシーにバインドします。

```
add authentication Policy <name> -rule <expression> -action <
    string>

bind authentication vserver <name> -policy <name> -priority <
    positive_integer> -gotoPriorityExpression <expression>
```

例


```
add authentication Policy alwayson-usertunnel-pol -rule
    is_aoservice.not -action NO_AUTHN

bind authentication vserver alwayson-auth-vserver -policy alwayson
    -usertunnel-pol -priority 110
```

3. 次の要素を追加し、ポリシーラベルを次の要素にバインドします。

```
add authentication policylabel <labelName> -loginSchema <string>

bind authentication  policylabel <string>  -policyName <string>  -
    priority <positive_integer> -gotoPriorityExpression <expression
    > -nextFactor <string>
```

例

```
add authentication policylabel user-tunnel-auth-label -loginSchema
     singleauth_alwayson

bind authentication policylabel user -policyName alwayson-
    usertunnel-pol -priority 100
```

4. LDAP ポリシーを設定し、ユーザトンネルポリシーラベルにバインドします。

```
add authentication policy <name>  -rule <expression>  -action <
    string>

bind authentication vserver <vserver_name> -policy <string>  -
    priorit < positive integer>  gotoPriorityExpression <string>
```

例

```
add authentication Policy LDAP_new -rule true -action LDAP_new

bind authentication policylabel user-tunnel-auth-label -policyName
     LDAP_new -priority 100 -gotoPriorityExpression NEXT
```

クライアント側の設定

`AlwaysOn`, `locationDetection`, and `suffixList registries` はオプションで、位置検出機能が必要な場合にのみ必要です。

レジストリキーエントリにアクセスするには、**Computer>HKEY_LOCAL_MACHINE>SOFTWARE>Citrix>Secure Access Client** のパスに移動します。

レジストリキー	レジストリタイプ	値と説明
AlwaysOnService	REG_DWORD	1 => マシンレベルのトンネルを確立するが、ユーザーレベルのトンネルは確立しない。2 => マシンレベルのトンネルとユーザーレベルのトンネルを確立する
AlwaysOnURL	REG SZ	ユーザーが接続する NetScaler Gateway 仮想サーバーの URL。例**:** `https://xyz.companyDomain.com` 重要**:** 1 つの URL だけがマシンレベルのトンネルとユーザーレベルのトンネルを担当します。alwaysOnUrl レジストリは、サービスレベルコンポーネントとユーザーレベルのコンポーネントの両方が動作し、設計に基づいて別のトンネル、つまりマシンレベルのトンネルとユーザーレベルのトンネルを接続するのに役立ちます
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
AlwaysOnAllowlist	REG_SZ	マシンが厳密モードで実行されている間にホワイトリストに登録する必要がある IP アドレスまたは FQDN のセミコロン区切りのリスト。例**:** `8.8.8.8;linkedin.com`
UserCertCAList	REG_SZ	カンマまたはセミコロンで区切られたルート CA 名のリスト。証明書の発行者名です。Always On サービスのコンテキストで使用され、カスタマーはクライアント証明書の選択元となる CA のリストを指定できます。例: `cgwsanity.net;xyz.gov.in`
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

レジストリキー	レジストリタイプ	値と説明
suffixList	REG SZ	セミコロンで区切られたドメインのリストで、位置検出が有効になっているときにいつでもマシンがイントラネット上にあるかどうかを確認する役割を果たします。**Example:** `citrite.net,cgwsanity.net`

これらのレジストリエントリの詳細については、「Always On」を参照してください。

> 注:
>
> 常時接続サービスが構成されている場合、NetScaler Gateway 仮想サーバーまたは NetScaler 上で構成された常時接続プロファイルはクライアント側では無視されます。そのため、Always On サービスを設定するときは、必ず`locationDetection` VPN レジストリと`AlwaysOn`VPN レジストリも有効にしてください。
> “‘

アドバンスポリシーを使用した **VPN** ポリシーの作成

February 1, 2024

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、NetScaler ADC が現在サポートしている 2 つの異なるポリシー構成および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、強力な表現言語で構成されています。式言語は、ポリシーでのルールの定義、アクションのさまざまな部分、およびサポートされている他のエンティティの定義に使用できます。式言語は、リクエストまたはレスポンスの任意の部分を解析でき、ヘッダーとペイロードを深く調べることもできます。同じ式言語が拡張され、NetScaler ADC がサポートするすべての論理モジュールで動作します。

> 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。

クラシックポリシーからアドバンス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はるかに高い柔軟性を提供します。NetScaler ADC はさまざまなクライアントに拡張および対応するため、高度なポリシーを大きく超える式をサポートすることが不可欠です。詳細については、「ポリシーと式」を参照してください。

アドバンスポリシーに追加された機能は次のとおりです。

- メッセージの本文にアクセスする機能。
- 他の多くのプロトコルをサポートします。
- システムの他の多くの機能にアクセスします。
- 基本関数、演算子、データ型の数が増えています。
- HTML、JSON、および XML ファイルの解析に対応します。
- 高速並列マルチストリングマッチング (`patsets`など) を容易にします。

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るようになりました。

- セッションポリシー
- 認可ポリシー
- 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 として設定できます。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 [ゲートウェイログオン（Gateway Logon）] ページが表示される前に、ゲートウェイ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許可されます。以前は、EPA はセッションポリシーの一部として構成されていました。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」トピックを参照してください。nFactor の詳細については、nFactor 認証のトピック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提供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 スキャンを使用する nFactor 認証用に NetScaler Gateway を構成する方法については、CTX224268 トピックを参照してください。

高度な **EPA** を使用したポスト認証 **EPA**

認証後 EPA スキャンは、ユーザーの資格情報が検証された後に実行されます。クラシックポリシーインフラストラクチャでは、認証後 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 スキャンは nFactor 認証の EPA 要素として構成されます。認証要素の 1 つとして認証後の EPA スキャンを使用する nFactor 認証用に NetScaler Gateway を構成する方法については、CTX224303 の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 **EPA**

EPA は認証の前に実行でき、認証後に実行できます。事前認証および認証後の EPA スキャンを使用した nFactor 認証用に NetScaler Gateway を構成する方法については、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

従来の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ていました。高度なポリシーインフラストラクチャでは、nFactor 認証の EPA 要素の一部として設定できます。

定期的な EPA スキャンを nFactor 認証の要素として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には、次の点に留意する必要があります。

- 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。
- プライオリティは、すべての PI ポリシーで必須です。
- 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。
- 設定されている認可ポリシーのいずれも選択されない場合は、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、認可ルールが失敗しても、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に相当する式**:**

クラシックポリシー式	高度なポリシー式
ns_true	true
ns_false	false
REQ.HTTP	HTTP.REQ
RES.HTTP	HTTP.RES
HEADER “foo”	HEADER(“foo”)
CONTAINS ” bar”	.CONTAINS(“bar”) [Note use of “..”]
REQ.IP	CLIENT.IP
RES.IP	SERVER.IP
SOURCEIP	SRC

クラシックポリシー式	高度なポリシー式
DESTIP	DST
REQ.TCP	CLIENT.TCP
RES.TCP	SERVER.TCP
SOURCEPORT	SRCPORT
DESTPORT	DSTPORT
STATUSCODE	STATUS
REQ.SSL.CLIENT.CERT	CLIENT.SSL.CLIENT_CERT

SSL VPN 仮想サーバを使用した DTLS VPN 仮想サーバの構成

April 1, 2024

NetScaler Gateway 用の DTLS VPN 仮想サーバーは、構成済みの SSL VPN 仮想サーバーと同じ IP アドレスとポート番号を使用して構成できます。DTLS VPN 仮想サーバを設定すると、高度な DTLS 暗号と証明書を DTLS トラフィックにバインドして、セキュリティを強化できます。

> 重要:
>
> - デフォルトでは、既存の SSL VPN 仮想サーバの DTLS 機能は ON に設定されています。DTLS VPN 仮想サーバーを作成する前に、サーバーの機能を無効にします。
> - DTLS ゲートウェイ仮想サーバー用の SNI は、NetScaler Gateway リリース 13.0 ビルド 64.x 以降でサポートされています。
> - NetScaler ADC リリース 13.0 ビルド 79.x 以降、この`helloverifyrequest`パラメータはデフォルトで有効になっています。DTLS プロファイルで`helloverifyrequest`パラメータを有効にすると、攻撃者またはボットがネットワークスループットを圧倒し、アウトバウンド帯域幅の枯渇につながるリスクを軽減できます。つまり、DTLS DDoS 増幅攻撃を軽減するのに役立ちます。`helloverifyrequest` パラメータの詳細については、DTLS プロファイルを参照してください。
> - UDP トラフィックを処理する場合、バックエンドサーバーが大量のトラフィックをプッシュすると、NetScaler ADC アプライアンスのメモリ消費量が増加します。その結果、クライアント側の TCP MUX 接続のため、NetScaler ADC アプライアンスはこのトラフィックをクライアントにプッシュできません。このような場合は、DTLS プロトコルを使用することをお勧めします。

注意事項

- NetScaler Gateway アプライアンス上の DTLS VPN 仮想サーバーは、リリース 13.0 ビルド 58.x から構成できます。
- NetScaler Gateway アプライアンスで DTLS VPN 仮想サーバーを構成する前に、アプライアンスに SSL VPN 仮想サーバーを構成しておく必要があります。
- DTLS VPN 仮想サーバは、設定された SSL VPN 仮想サーバの IP アドレスとポート番号を使用します。
- DTLS ハンドシェイクが失敗すると、接続は TLS にフォールバックします。
- DTLS だけを使用するには、DTLS トラフィックに DTLS 暗号だけをバインドすることで、TLS を無効にできます。
- TCP トラフィックが VPN 上でトンネリングされる場合、DTLS 多重化はサポートされません。

GUI を使用して **DTLS VPN** 仮想サーバーを構成する

1. ［構成］タブで、［**NetScaler Gateway**］**>** ［仮想サーバー］に移動します。
2. **NetScaler Gateway** 仮想サーバーページで、既存の **SSL VPN** 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、「DTLS」チェックボックスをオフにし、「**OK**」をクリックします。
4. **[**NetScaler Gateway] > [**仮想サーバー] に戻り、[追加] をクリックします ******。
5. 「基本設定」で、次のフィールドに値を入力し、「**OK**」をクリックします。
   - 名前-DTLS VPN 仮想サーバーの名前
   - プロトコル- DTLS を選択
   - IP アドレス—SSL VPN 仮想サーバーの IP アドレスを入力します
   - ポート—SSL VPN 仮想サーバーのポート番号を入力します
6. **NetScaler Gateway** 仮想サーバーページで、以前に追加した仮想サーバーを選択し、「編集」をクリックします。
7. [証明書] で、矢印アイコンをクリックして必要な証明書キーを選択します。
8. 「サーバー証明書のバインド」**>** 「サーバー証明書の選択」で、既存の SSL 証明書キーを選択するか、作成します。
9. **[**サーバー証明書のバインド**]** ページで **[**バインド**]** をクリックします。

> 注:
>
> - DTLS 1.2 を使用するには、「SSL パラメータ」の下の編集アイコンをクリックし、「**DTLS** 1.2」チェッ

> クボックスを選択します。
> - サーバ名表示（SNI）は、DTLS タイプの VPN 仮想サーバでサポートされます。

CLI を使用して DTLS VPN 仮想サーバーを設定します

コマンドプロンプトで、次の一連のコマンドを入力します：

```
set vpn vserver <ssl vpnvserver name> -dtls off
add vpn vserver <dtls vpnvserver name> dtls <ssl vpn vserver IP> <ssl vpn vserver port>
bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl cert key or newly created cert key>
<!--NeedCopy-->
```

DTLS 1.0 は通常どおりに動作します。DTLS 1.2 を使用するには、次のコマンドを入力します：

```
set ssl vserver < dtls vpnvserver name > -dtls12 ENABLED
<!--NeedCopy-->
```

例

```
set vpn vserver vpnvserver  -dtls off
add vpn vserver vpnvserver_dtls dtls 10.108.45.220 443
bind ssl vservser vpnvserver_dtls -certkeyName sslcertkey
set ssl vserver vpnvserver_dtls -dtls12 ENABLED
<!--NeedCopy-->
```

DTLS タイプ **VPN** 仮想サーバーの **SNI** を有効にするには、次のコマンドを入力します。

```
set ssl vserver <vServerName>@ [-SNIEnable ( ENABLED | DISABLED )
bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl cert key or newly created cert key> <-SNICert>
<!--NeedCopy-->
```

例

```
set ssl vserver _XD_10.106.40.225_443_DTLS -sniEnable eNABLED
bind ssl vserver _XD_10.106.40.225_443_DTLS -certkeyName "Insight/*.insight.net.cer_CERT_" -snICert

<!--NeedCopy-->
```

サポートされている DTLS VPN 仮想サーバーパラメーター

DTLS タイプの VPN 仮想サーバーでは、次のパラメーターのみがサポートされます。

- Ipaddress
- ポート

- 状態
- ダブルホップ
- downstateflush
- コメント
- Appflowlog
- Icmpvsrresponse

サポートされていない **DTLS VPN** 仮想サーバーパラメーター

次のパラメータは、DTLS タイプの VPN 仮想サーバーではサポートされていません。

- LinuxEPAPluginUpgrade
- WindowsEPAPluginUpgrade
- maxAAAUsers
- icaProxySessionMigration
- loginOnce
- cginfraHomePageRedirect
- logoutOnSmartcardRemoval
- L2Conn
- MacEPAPluginUpgradeRHIstate
- icaOnly
- maxLoginAttempts
- failedLoginTimeout
- vserverFqdn
- deviceCert
- rdpServerProfileName
- pcoipVserverProfileName
- tcpProfileName
- netProfile
- authnProfile
- Listenpriority
- Listenpolicy
- ipset
- certkeyNames

XenApp および **XenDesktop** ウィザードを使用して **DTLS** 仮想サーバーを構成します

1. 「**Citrix** 製品との統合」の「**XenApp** と **XenDesktop**」をクリックします。

2. **XenApp** および **XenDesktop** のセットアップウィザードで、［StoreFront］を選択し、［続行］をクリックします。
3. **NetScaler Gateway** 設定ページで、「**** この **VPN vServer** の **DTLS** リスナーを構成する」チェックボックスを有効にして、「続行」をクリックします **。

   DTLS リスナーの設定が完了しました。
4. 「サーバー証明書」で、「ファイルを選択」をクリックしてサーバー証明書を選択し、「続行」をクリックします。
5. 証明書ファイルとキーファイル名を指定し、[続行] をクリックします。
6. **StoreFront** セクションで、次のように必須パラメータの値を指定し、「続行」をクリックします。
7. 「認証」セクションで、次のように必須パラメータの値を指定し、「接続をテスト」をクリックします。

   サーバーが到達可能であることを確認し、[タイムアウト] の値と [サーバーログオン名属性] を指定して、**[**続行**]** をクリックします。
8. [完了] をクリックして設定を完了します。

制限事項

- DTLS 1.2 は、Windows クライアントでのみサポートされています。
- DTLS を使用した VPN 仮想サーバは IPv6 アドレスをサポートしていません。
- SSL ポリシーと SSL プロファイルは、DTLS VPN 仮想サーバではサポートされていません。また、VPN 仮想サーバポリシーのバインドはサポートされていません。
- NetScaler Gateway DTLS VPN 仮想サーバーは、次の機能をサポートしていません。ただし、NetScaler Gateway SSL VPN 仮想サーバーは次の機能をサポートしています。
  - コンテンツスイッチング仮想サーバを備えた Unified Gateway
  - UDP MUX
  - UDP ビデオ
  - UDP オーディオ
  - PCOIP
- DTLS VPN 仮想サーバーの統計に関連する`stat vpn vserver`コマンドはサポートされていません。
- HSM キーは DTLS 仮想サーバーではサポートされていません。
- クラスタ構成はサポートされていません。

NetScaler 製品との統合

February 1, 2024

NetScaler 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 をサポート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 Endpoint Management に直接接続できます。ユーザーが接続すると、Web、SaaS、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任意のデバイスからサポートすることもできます。

NetScaler 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 NetScaler Gateway の設定を構成します。ユーザーが接続すると、公開アプリケーションと仮想デスクトップにアクセスできます。

NetScaler Gateway と Endpoint Management、StoreFront、および Web Interface を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。

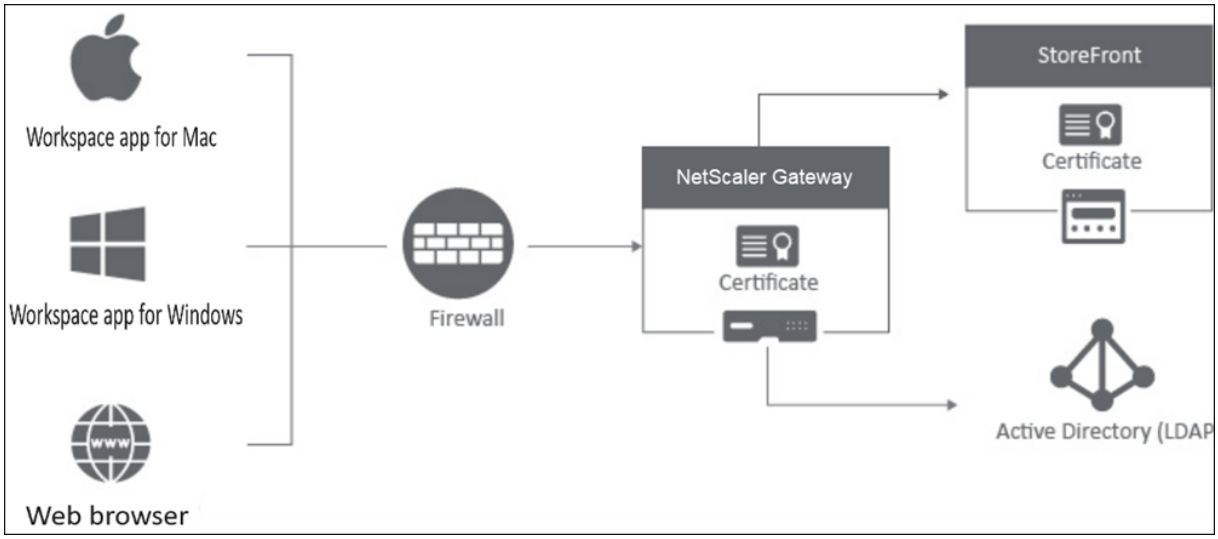
- NetScaler Gateway は DMZ に存在し、既存のネットワークに接続されています。
- NetScaler Gateway はスタンドアロンアプライアンスとして展開され、リモートユーザーは NetScaler Gateway に直接接続します。
- StoreFront、Endpoint Management、Citrix Virtual Apps、Citrix Virtual Desktops および Web Interface は、セキュリティで保護されたネットワーク内にあります。
- ShareFile は Endpoint Management で設定されています。ShareFile の詳細については、「ShareFile」トピックおよび「[ユーザーアクセス用の ShareFile の構成](http://docs.citrix.com/ja-jp/sharefile.html)」トピックを参照してください。

StoreFront と Endpoint Management の展開方法は、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。ユーザーが MDX Toolkit でラップされた MDX アプリにアクセスできる場合、Endpoint Management はセキュアネットワーク内の StoreFront の前に配置されます。MDX アプリへのアクセスを提供していない場合、StoreFront はセキュリティで保護されたネットワーク内の Endpoint Management の前に配置されます。

NetScaler Gateway と StoreFront の統合

April 1, 2024

この記事では、Citrix Workspace アプリまたは Web ブラウザーを使用しているユーザー向けに、StoreFront にリモートアクセスするための NetScaler Gateway 仮想サーバーを作成する方法について説明します。



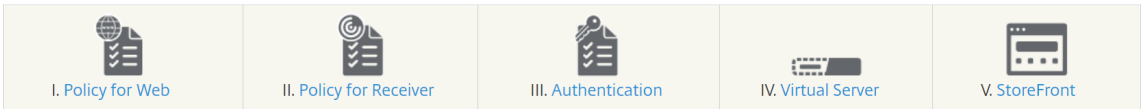
ユーザーは、ウェブブラウザーまたは Citrix Workspace アプリを介して NetScaler Gateway に接続します。NetScaler Gateway は、構成されたポリシーに基づいてユーザーを認証します。認証が成功すると、NetScaler Gateway はユーザーがストアにシングルサインオンできるようにし、StoreFront ストアをユーザーにプロキシします。

> 重要:
>
> NetScaler Gateway と StoreFront の統合に Citrix Virtual Apps and Desktops ウィザードを使用しないことをお勧めします。従来の認証ポリシー（非推奨）を使用して無効な構成が作成されるためです。

StoreFront で使用するように **NetScaler Gateway** を構成する

NetScaler Gateway を StoreFront と統合するには、次の手順を実行します:

1. Web ブラウザーベースのアクセス用のセッションポリシーを作成する
2. Citrix Workspace アプリベースのアクセス用のセッションポリシーを作成する
3. 認証プロファイルを作成する
4. NetScaler Gateway 仮想サーバーの作成
5. NetScaler Gateway インスタンスを StoreFront に追加します



1. Web ブラウザーベースのアクセス用のセッションポリシーを作成する

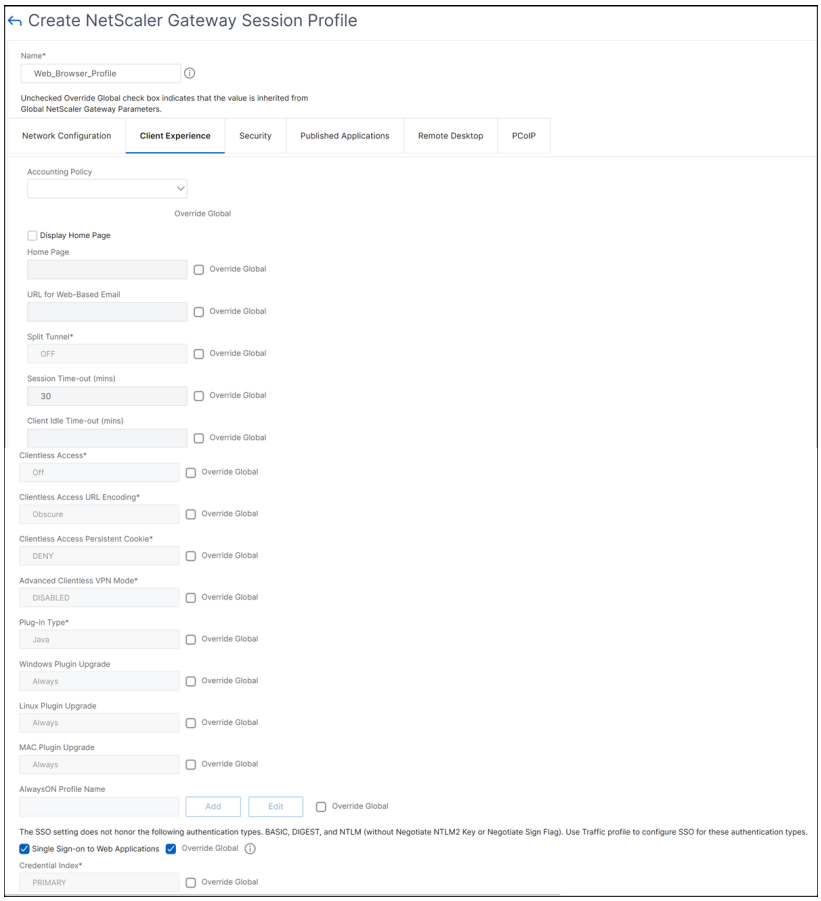
1. ［構成］ **>** ［**NetScaler Gateway**］ **>** ［ポリシー］［セッション］に移動します。

2.「セッションプロファイル」タブで、「追加」をクリックします。

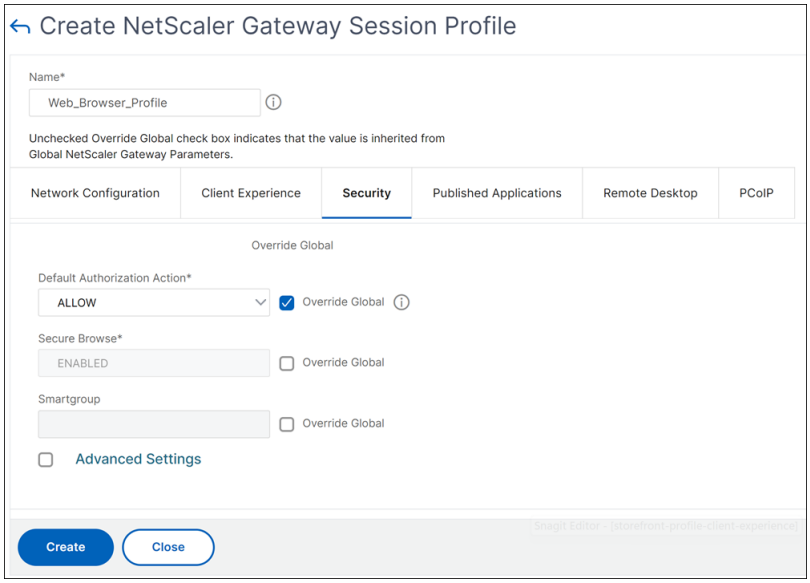
3. セッションプロファイルに名前を割り当てます。

4.［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：

- プラグインタイプ**:** プラグインタイプは、デフォルトで **Java** に設定されています。この設定はオプションですが、ユーザーがフル VPN を無効にする場合は推奨されます。
- **Web** アプリケーションへのシングルサインオン：このオプションを選択すると、ユーザーが NetScaler Gateway にログオンしたときに、資格情報が StoreFront Web サイトに転送されます。この設定により、ユーザーは資格情報を 2 回入力する必要がなくなります。ただし、StoreFront で NetScalerGateway からのパススルー認証方法も有効にする必要があります。ユーザーが NetScaler Gateway と StoreFront ストアに異なる資格情報でログオンする必要がある場合、このオプションを無効にしてください。

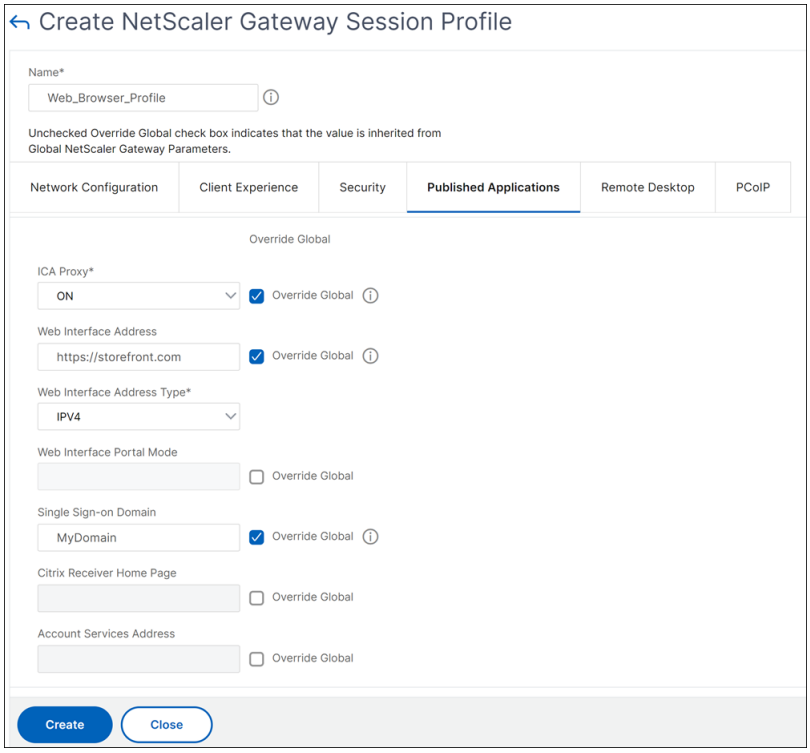


5.「セキュリティ」タブで、「デフォルト認証アクション」を有効にして「許可」に設定します。



6. [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:[オン] に設定します。
   - **Web Interface** アドレス: StoreFStoreFront サーバーの FQDN の後にストア Web サイトへのパスが続きます。
   - シングル・サインオン・ドメイン:1 つのドメインのみを使用する場合は、オプションでドメインの NetBIOS 名を入力します。

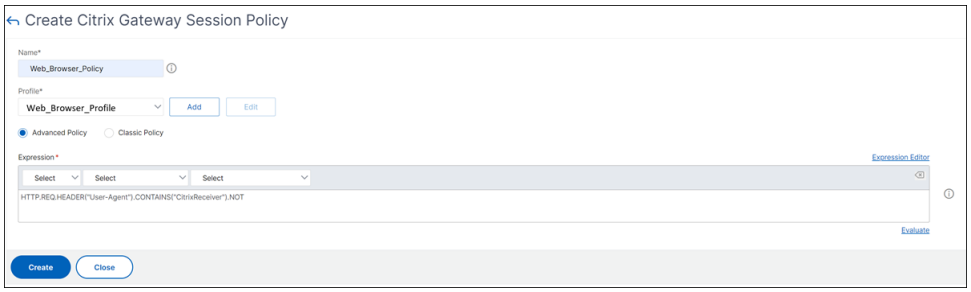


7. [**Create**] をクリックします。

8. ［セッションポリシー］タブで ［追加］をクリックします。NetScaler が Web ブラウザーベースの接続と Citrix Workspace アプリベースの接続を区別するには、セッションポリシーが必要です。このポリシーは、Web ブラウザーベースの接続に適用されます。
9. 「名前」で、セッションポリシーに名前を割り当てます。
10. 「プロファイル」で、作成したセッションプロファイルを選択します。
11. 「詳細ポリシー」オプションをクリックし、「式」に次の構文を入力します:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

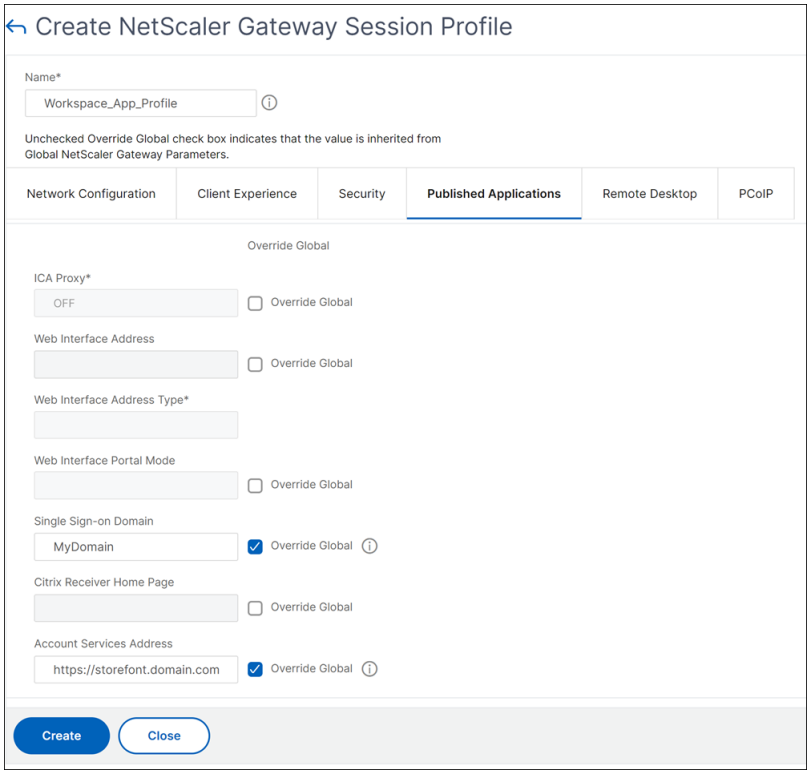
12. ［**Create**］をクリックします。



NetScaler Gateway セッションポリシーについて詳しくは、「セッションポリシー」を参照してください。

2. Citrix Workspace アプリベースのアクセス用のセッションポリシーを作成する

上記の手順を繰り返して、Citrix Workspace アプリベースのアクセス用のセッションポリシーとセッションプロファイルを作成します。ただし、「公開アプリケーション」タブでは、Web インターフェイスアドレスを構成する代わりに、アカウントサービスアドレス設定を構成する必要があります。このステップでは、StoreFStoreFront サーバーの完全修飾ドメイン名を指定する必要があります。Citrix Workspace アプリは、このアドレスを使用して、サーバー上で利用可能なストアを検出します。



3. 認証プロファイルを作成する

構成する必要のある認証方法の種類に基づいて、NetScaler で認証プロファイルを作成します。

この手順はオプションですが、StoreFStoreFront へのアクセスを許可する前に、NetScaler Gateway を使用してユーザーの身元を認証することをお勧めします。

詳細については、「認証と承認 」を参照してください。

4. NetScaler Gateway 仮想サーバーの作成

1. 「**NetScaler Gateway**」**>**「仮想サーバー」に移動します。
2. NetScaler Gateway 仮想サーバーを追加するには、［追加］をクリックします。
3. 仮想サーバーに名前とアドレスを割り当てます。

   > 注:
   >
   > NetScaler Gateway を使用してユーザーを認証しない場合は、[詳細] をクリックし、[認証を有効にする] チェックボックスをオフにします。

4. 「証明書」で、「サーバー証明書」をクリックします。
5. サーバー証明書をアップロードし、「バインド」をクリックします。

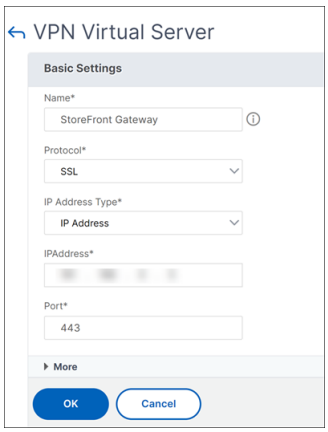
6. セッションポリシーを追加します：

   a)「ポリシー」で、「**+**」をクリックします。
   b)「ポリシーの選択」ドロップダウンリストから、「セッション」を選択します。「タイプ」ドロップダウンリストから「リクエスト」を選択し、「続行」をクリックします。
   c)「ポリシーバインド」で、「ポリシーの選択」をクリックし、以前に作成した Web ブラウザベースのセッションポリシーと Citrix Workspace アプリベースのセッションポリシーを選択し、「バインド」をクリックしてセッションポリシーを仮想サーバーにバインドします。

7.「公開アプリケーション」で、「**STA Server**」をクリックします。セキュリティチケット機関 (STA) URL を少なくとも 1 つ指定してください。Citrix Virtual Apps and Desktops を使用している場合は、Desktop Delivery Controller の URL を入力します。Citrix DaaS を使用している場合は、Citrix Cloud Connector の URL を入力します。

8.「認証プロファイル」で、作成した認証プロファイルを選択します。クラシックポリシーはサポートされなくなったため、この手順は必須です。

9.［完了］をクリックします。



5. NetScaler Gateway インスタンスを **StoreFront** に追加する

StoreFront に NetScaler Gateway インスタンスを追加する方法については、「NetScaler Gateway の構成」を参照してください。

参照ドキュメント

StoreFront と NetScaler Gateway の統合について詳しくは、以下のトピックを参照してください：

- NetScaler Gateway の追加
- StoreFront と NetScaler Gateway 統合の設計

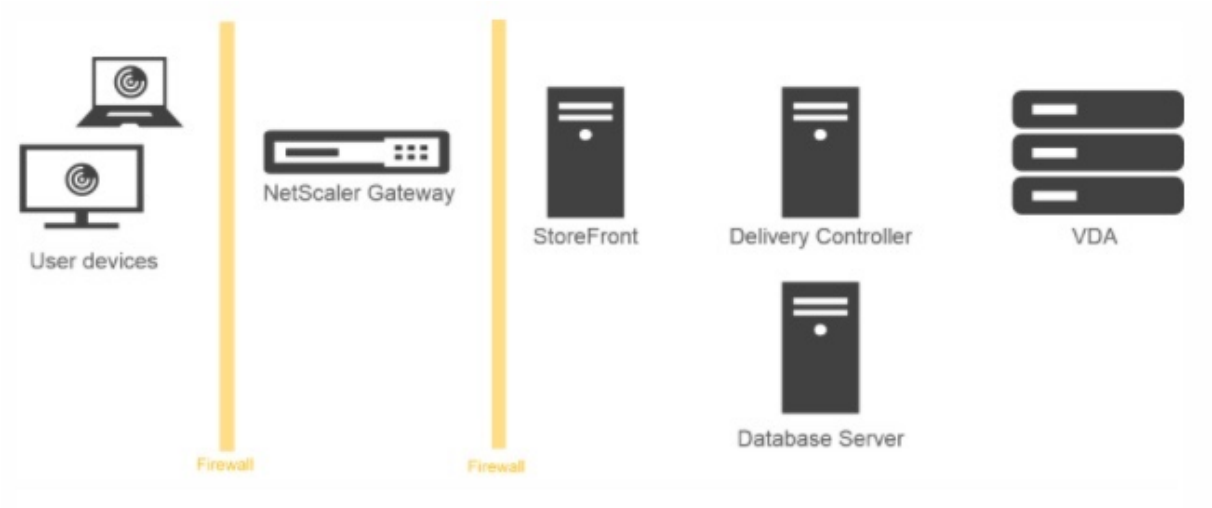
NetScaler Gateway を Citrix Virtual Apps and Desktops 統合する

February 1, 2024

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、NetScaler 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 NetScaler Gateway と統合する方法の詳細な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、NetScaler Gateway を含む Citrix の簡略化された Citrix itrix 展開の例を示しています。NetScaler 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、NetScaler Gateway を使用してログオンおよび認証を行います。NetScaler 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 Endpoint Management、Citrix Virtual Apps and Desktops を使用した展開

February 1, 2024

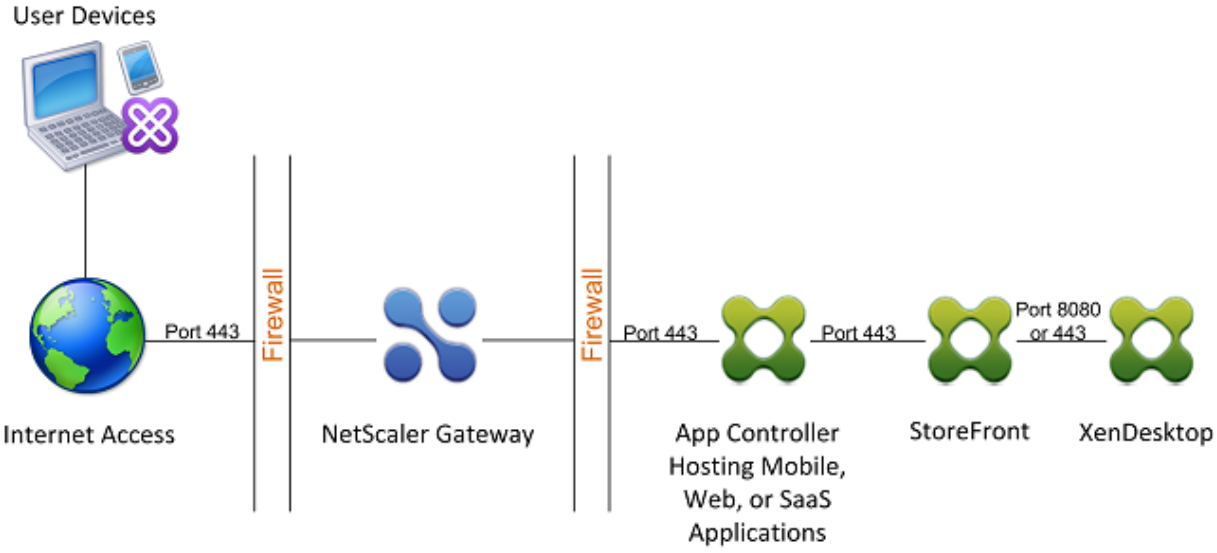
ユーザーは、ネットワークでホストされている Windows、Web、SaaS、モバイルアプリケーション、および仮想デスクトップに接続できます。NetScaler Gateway、Citrix Endpoint Management、および Citrix Virtual Apps and Desktops を使用して、リモートユーザーおよび内部ユーザーにアプリケーションおよびデスクトップへのアクセスを提供できます。NetScaler Gateway はユーザーを認証し、Citrix Workspace アプリまたは Secure Hub を使用してユーザーがアプリケーションにアクセスできるようにします。

ユーザーは、Citrix Workspace アプリおよび StoreFront を使用して、Citrix Virtual Apps で公開されている Windows ベースのアプリおよび 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 を使用すると、シングルサインオン（SSO）用のウェブ、SaaS、および MDX アプリケーションを、ShareFile ドキュメントとともに管理できます。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、NetScaler Gateway を介して Endpoint Management に接続し、アプリケーションと ShareFile データにアクセスします。リモートユーザーは、Citrix Secure Access クライアント、Citrix Workspace アプリ、または Secure Hub のいずれかに接続して、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 NetScaler Gateway を示しています。

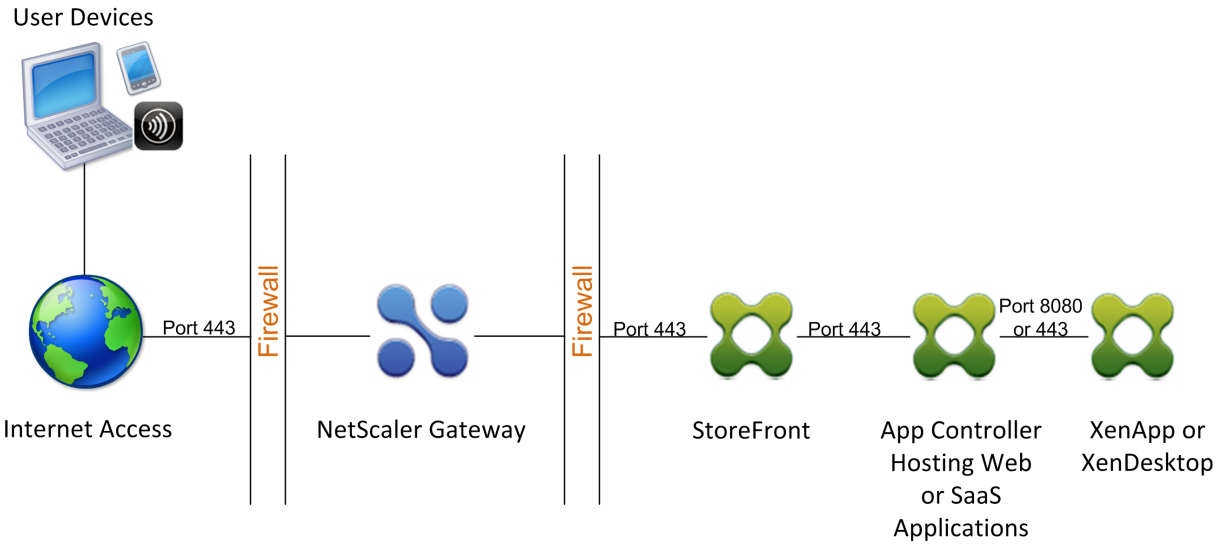
展開環境で、Endpoint Management から MDX アプリケーションにアクセスし、StoreFront から Windows ベースのアプリケーションにアクセスできる場合は、次の図に示すように、StoreFront Endpoint Management を展開します:

図 1: StoreFront の前に Endpoint Management 機能を備えた NetScaler Gateway を展開する



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ない場合、次の図に示すように、StoreFront は Endpoint Management の前に配置されます。

図 2: Endpoint Management StoreFront を使用した NetScaler Gateway の展開



展開ごとに、StoreFront および Endpoint Management は内部ネットワークに存在し、NetScaler Gateway は 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 のインストール」トピックを参照してください。
StoreFront の展開について詳しくは、「StoreFront のトピック」を参照してください。

Citrix Endpoint Management 環境の設定を構成する

April 1, 2024

Citrix Endpoint Management 用 NetScaler ADC ウィザードの指示に従って、Citrix Endpoint Management 展開環境用の NetScaler ADC 機能を構成できます。このウィザードを使用すると、次のことができます。

- マイクロ **VPN** をセットアップします。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ケーションとデスクトップにアクセスできます。
  - Citrix Endpoint Management の MAM 専用モードでは、認証に NetScaler 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 NetScaler Gateway をお勧めします。
  - ENT 展開の場合、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、NetScaler Gateway FQDN を使用して登録します。
- 証明書ベースの認証を構成します。Citrix Endpoint Management のデフォルトの構成は、ユーザー名とパスワードの認証です。Citrix Endpoint Management 環境への登録とアクセスのためのセキュリティレイヤーを追加するには、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。NetScaler ADC 負荷分散は、複数の Citrix Endpoint Management サーバーを使用している場合、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 NetScaler ADC、Citrix Endpoint Management へのトラフィックフロー）、すべての Citrix Endpoint Management デバイスモードで必要です。このシナリオでは、NetScaler アプライアンスはユーザーデバイスと Citrix Endpoint Management サーバーの間の DMZ に配置され、モバイルデバイスから Citrix Endpoint ManEndpoint Management サーバーに送信される暗号化されたデータの負荷を分散します。

- 電子メールフィルタリングを使用して **Microsoft Exchange** サーバーの負荷を分散します。このシナリオでは、NetScaler ADC アプライアンスは、ユーザーデバイスと Citrix Endpoint Management NetScaler ADC コネクタ（XNC）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すべての要求は NetScaler 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、NetScaler 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ドロップします。
- 要求されたコンテンツのタイプに基づいて、**ShareFile StorageZones** コネクタの負荷を分散します。このシナリオでは、ストレージゾーン 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 Controller 間でトラフィックを負荷分散します。
  - StorageZones コネクタのユーザー認証を提供します。
  - ShareFile のアップロードおよびダウンロードの URI 署名を検証します。
  - NetScaler ADC アプライアンスで SSL 接続を終了します。

ShareFile の構成の詳細については、「ストレージゾーン Controller 用の NetScaler 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、次の Citrix Endpoint Management の展開に関する記事を参照して、設計および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
>
> NetScaler Gateway および NetScaler 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 NetScaler ADC ウィザードは一度だけ使用できます。テスト環境、開発環境、本番環境など、複数の Citrix Endpoint Management インスタンスを使用する場合は、追加の環境用に NetScaler ADC を手動で構成する必要があります。次のサポート記事には、ウィザードによって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 NetScaler ADC インスタンスを作成する方法が記載されています。
>
> NetScaler ADC 上の Citrix Endpoint Management ウィザードによって生成されるコマンド-SSL ブリッジ

> NetScaler ADC 上の Citrix Endpoint Management ウィザードによって生成されるコマンド-SSL オフロード

NetScaler 機能のライセンス要件

次の NetScaler 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 の MDM 負荷分散には、NetScaler ADC 標準ライセンスが必要です。
- StorageZones を使用した ShareFile 負荷分散には、NetScaler ADC 標準ライセンスが必要です。
- Exchange 負荷分散には、NetScaler 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アドバンスドライセンスが必要です。

NetScaler for Citrix Endpoint Management ウィザード

このセクションでは、NetScaler for Citrix Endpoint Management ウィザードを使用して次の例を説明します:

- 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の詳細については、「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. NetScaler GUI で、[構成] タブをクリックし、[**Citrix** 製品との統合] セクションの [**XenMobile**] をクリックします。
2. Citrix Endpoint Management のバージョンを選択し、[始める] をクリックします。
3. 構成する機能を選択します。このウィザードは 1 回しか使用できないため、後続の設定は手動で実行する必要があります。この手順では、**NetScaler Gateway** 経由のアクセス（**ENT** または **MAM** モードで実行されている Citrix Endpoint Management 用）および Citrix EnEndpoint Management サーバーの負荷分散の設定を選択することを前提としています。
4. **NetScaler Gateway** 構成ページで、外部側 の NetScaler Gateway の IP アドレス、ポート、 および仮想サーバー名の値を入力します。
5. [**NetScaler Gateway** のサーバー証明書] ページの [証明書ファイル] で、[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。
   - ローカル: コンピュータ上の証明書を選択します
   - アプライアンス: NetScaler Gateway（アプライアンス）上の証明書を選択します。

6. [認証] ページの [プライマリ認証方法] で、[クライアント証明書] を選択し、証明書プロファイルの名前を入力します。

   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。

   証明書ポリシーを作成する必要がある場合は、[証明書ポリシーの作成] をクリックします。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属性には、必要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。

7. 2 要素認証を有効にするには、「2 段階認証」をクリックします。クライアント証明書認証に続いて、2 次認証タイプとして LDAP または RADIUS を指定します。

8. [二次認証方法] で、二次認証方法を選択します。

   - クライアント証明書をプライマリ認証タイプとして使用すると、LDPA（または RADIUS）をセカンダリ認証タイプとして構成するオプションがあります。

     クライアント証明書認証のみを使用する場合は、[**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。

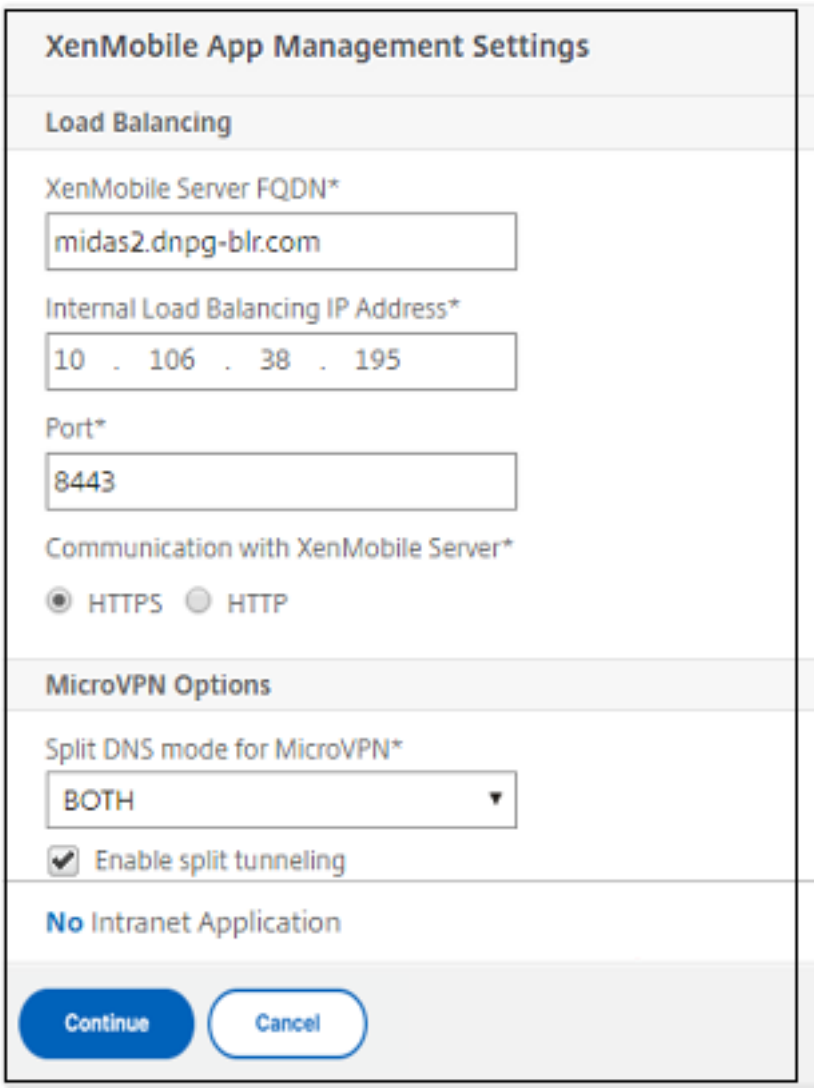
     クライアント証明書 + ドメイン (LDAP) 認証を使用するには、[セカンダリ認証方法] を **LDAP** に変更し、認証サーバーの設定を行います。

9. **Citrix Endpoint Management** の［アプリケーション管理］設定を構成します。

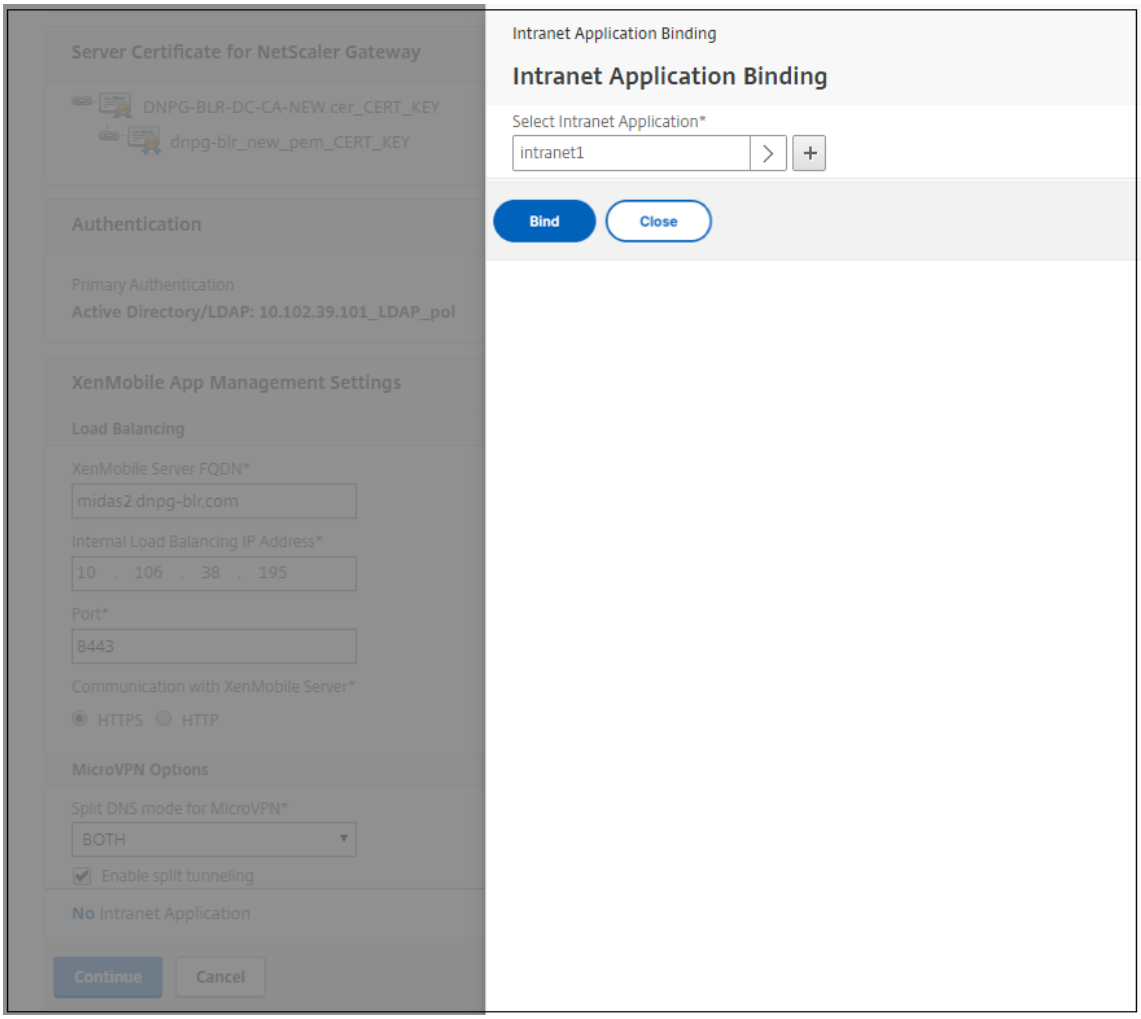
   - **Citrix Endpoint Management FQDN** を入力します。これは MAM の負荷分散 FQDN です。
   - Citrix Endpoint **Management** サーバーの負荷分散を行う仮想サーバーの **MAM** 専用内部負荷分散 **IP** アドレスを入力します。NetScaler Gateway は、この MAM 負荷分散仮想 IP を介して Citrix Endpoint Management と通信します。
   - これは SSL オフロード展開であるため、［**Citrix Endpoint Management** サーバーとの通信］で［**HTTP**］を選択します。
   - [**MicroVPN** のスプリット **DNS** モード] フィールドは自動的に [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。分割トンネリングを有効にする場合は、次に、イントラネットアプリケーションバインディングを構成します。

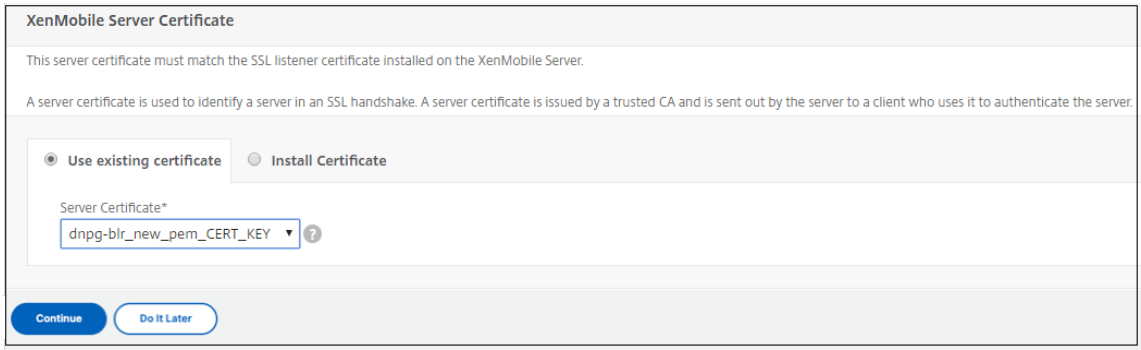
   デフォルトでは、Secure Web アクセスは内部ネットワークにトンネリングされます。つまり、Secure Web はすべてのネットワークアクセスに対してアプリケーションごとの VPN トンネルを使用して内部ネットワークに戻り、NetScaler ADC アプライアンスは分割トンネル設定を使用します。



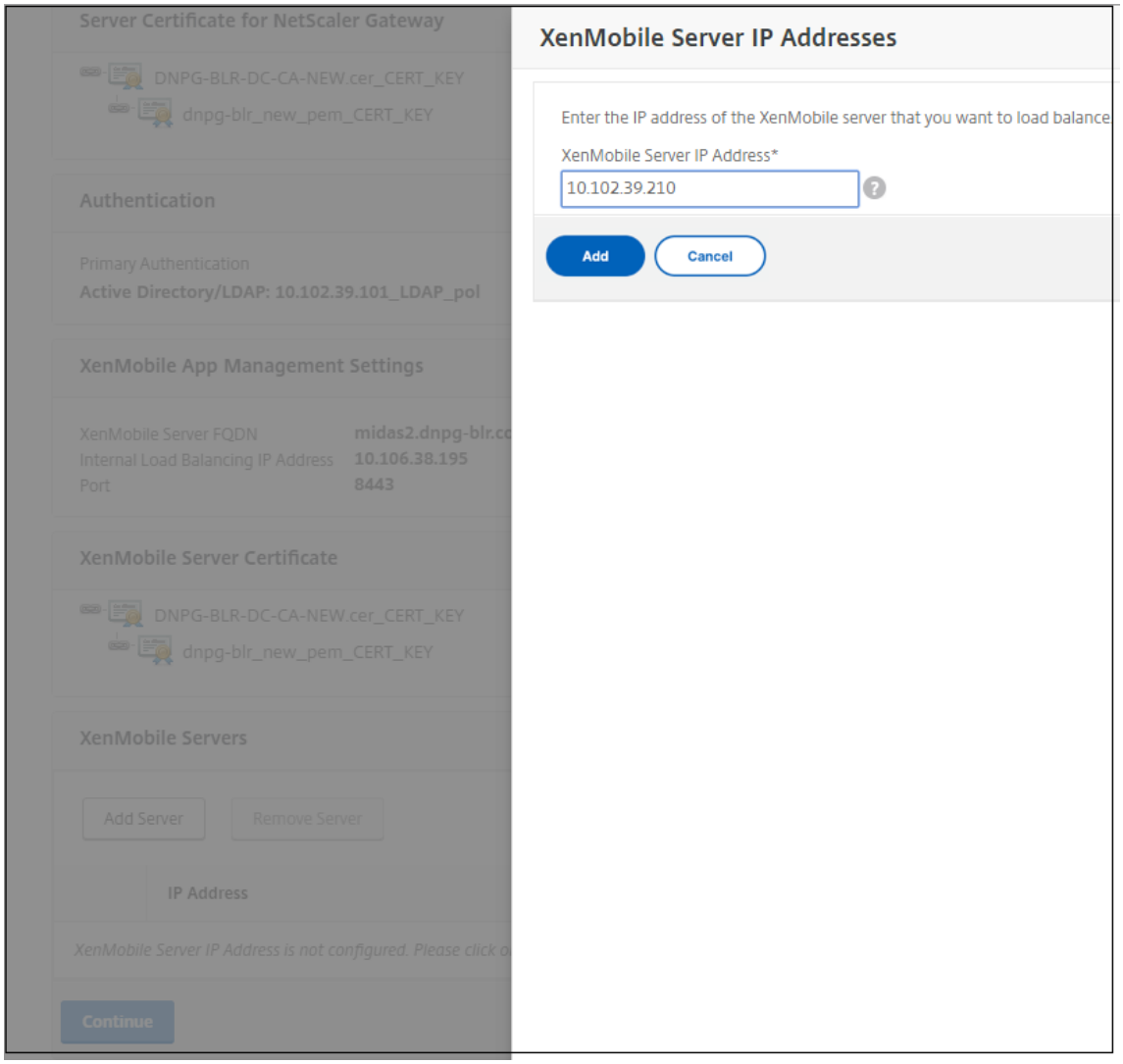
10. NetScaler Gateway でユーザー接続の傍受ルールを構成するには、イントラネットアプリケーションバインドを構成する必要があります。[**+**] をクリックして、バインドを追加します。



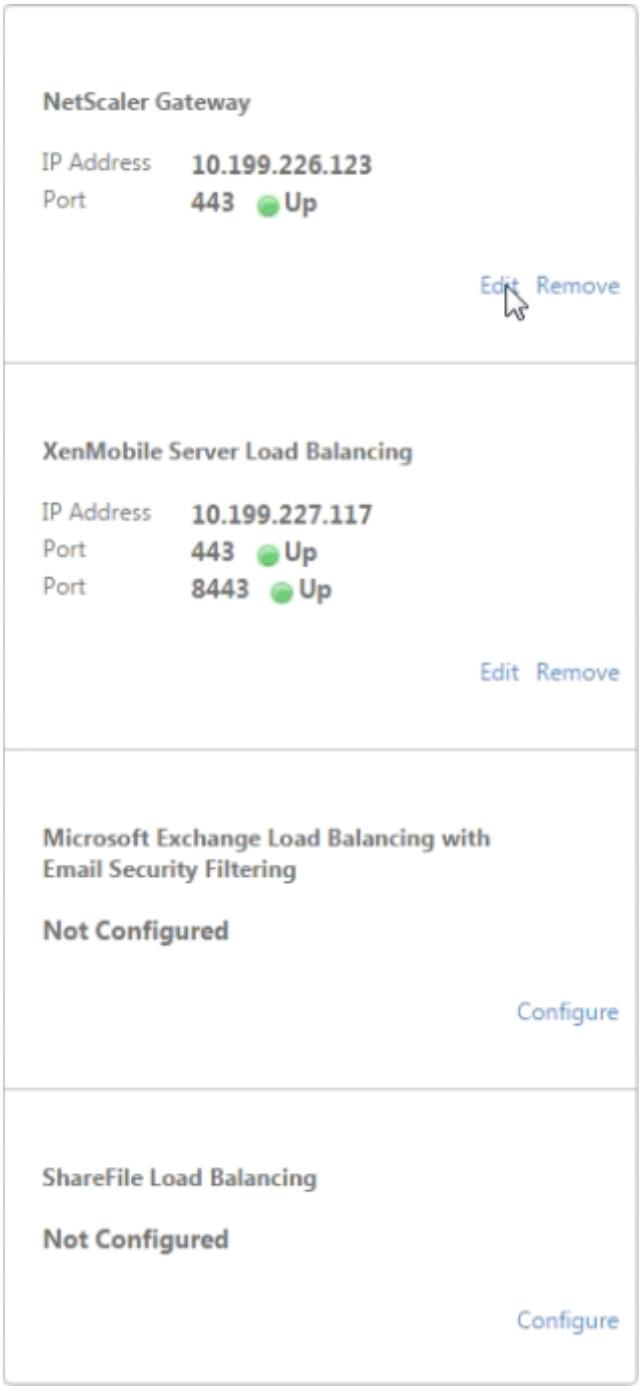
11. ネットワークアクセスを許可するためのパラメータを入力し、[**Create**] をクリックします。
12. Citrix Endpoint Management 証明書を追加します。これは MAM 負荷分散仮想サーバーに使用されます。



13. [**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** の **IP** アドレスを追加します。



NetScaler ダッシュボードで、NetScaler Gateway と Citrix Endpoint Management 負荷分散が構成されていることを確認します。



ユーザー証明書でユーザープリンシパル名（UPN）の代わりに SamAccount 属性を使用する場合は、「クライアント証明書認証用のNetScaler Gateway の手動構成」の説明に従って証明書プロファイルを構成します。

Citrix Endpoint Management または CitrixXenMobile Server の負荷分散サーバーを構成する

April 1, 2024

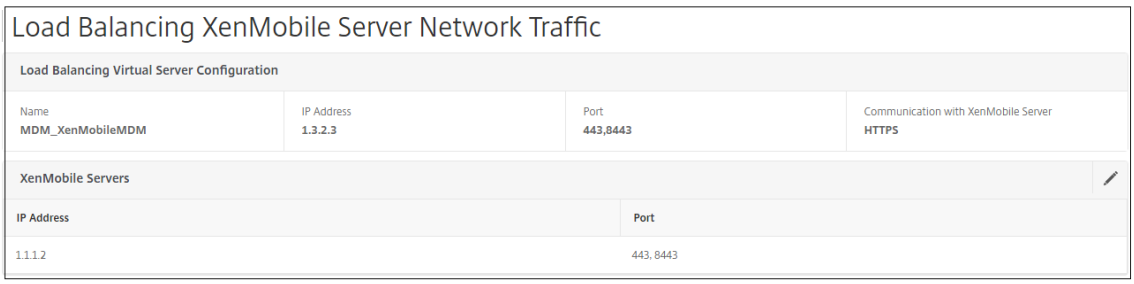
Citrix Endpoint Management 用 **NetScaler ADC** ウィザードを初期セットアップに使用した後、このセクションの説明に従って、NetScaler Gateway 構成ユーティリティを使用して負荷分散を構成します。Citrix Endpoint Management の場合は、SSL オフロードを使用します。Citrix Endpoint Management サーバーについては、Citrix Gateway および NetScaler ADC との統合の「展開の概要」の下にある負荷分散モードの推奨事項を必ず参照してください。

NetScaler VIP で SSL ブリッジモードを使用するには

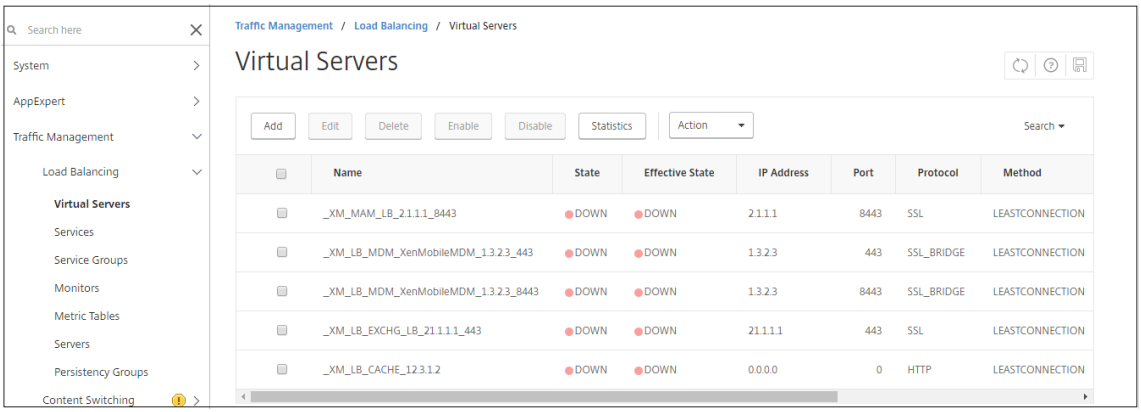
Citrix Endpoint Management が DMZ にある場合は、SSL ブリッジモードを使用します。SSL ブリッジモードで Citrix Endpoint Management と NetScaler ADC VIP の負荷分散を行うと、インターネットトラフィックは Citrix Endpoint Management サーバーに直接流れ、そこで接続が終了します。SSL ブリッジモードはセットアップとトラブルシューティングが最も簡単なモードです。

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の設定] 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 Server 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. 負荷分散の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。

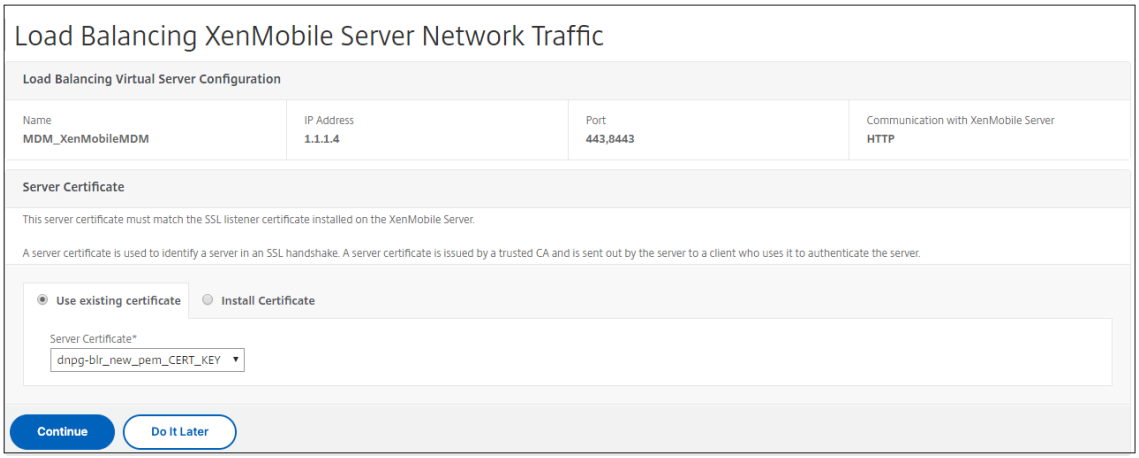


NetScaler VIP で **SSL** オフロードモードを使用するには

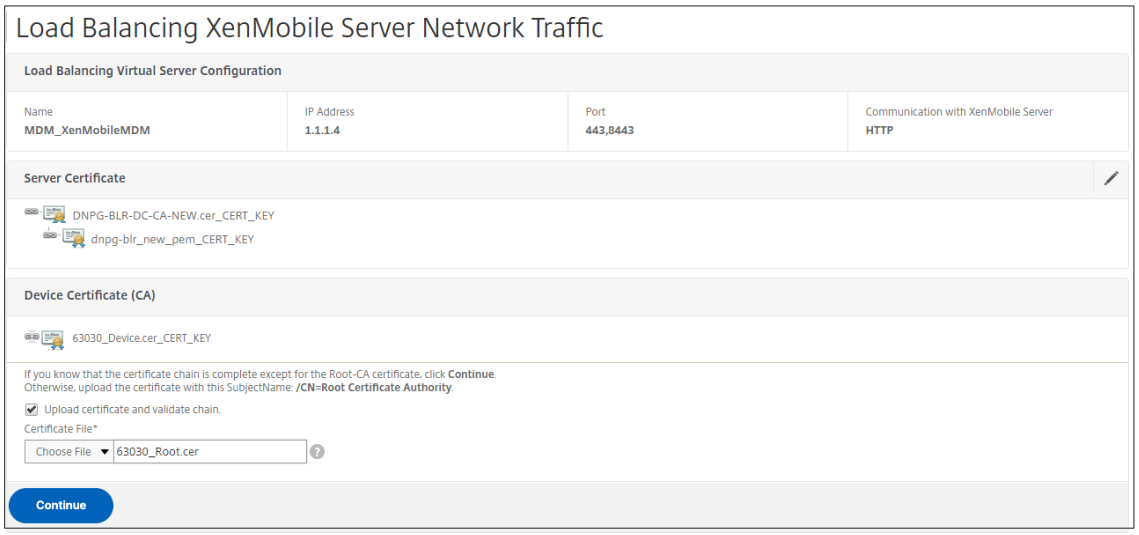
Citrix Endpoint Management に SSL オフロードを使用します。また、オンプレミスの Citrix Endpoint Management が内部ネットワークにある場合は、セキュリティ標準を満たすために必要に応じて SSL オフロードを使用します。SSL オフロードモードで Citrix Endpoint Management と NetScaler ADC VIP の負荷分散を行うと、インターネットトラフィックは NetScaler ADC アプライアンスに直接流れ、そこで接続が終了します。その後、NetScaler Gateway は、アプライアンスから Citrix Endpoint Management への新しいセッションを確立します。SSL オフロードモードは、セットアップとトラブルシューティングの際に、より複雑になります。

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の設定] 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。

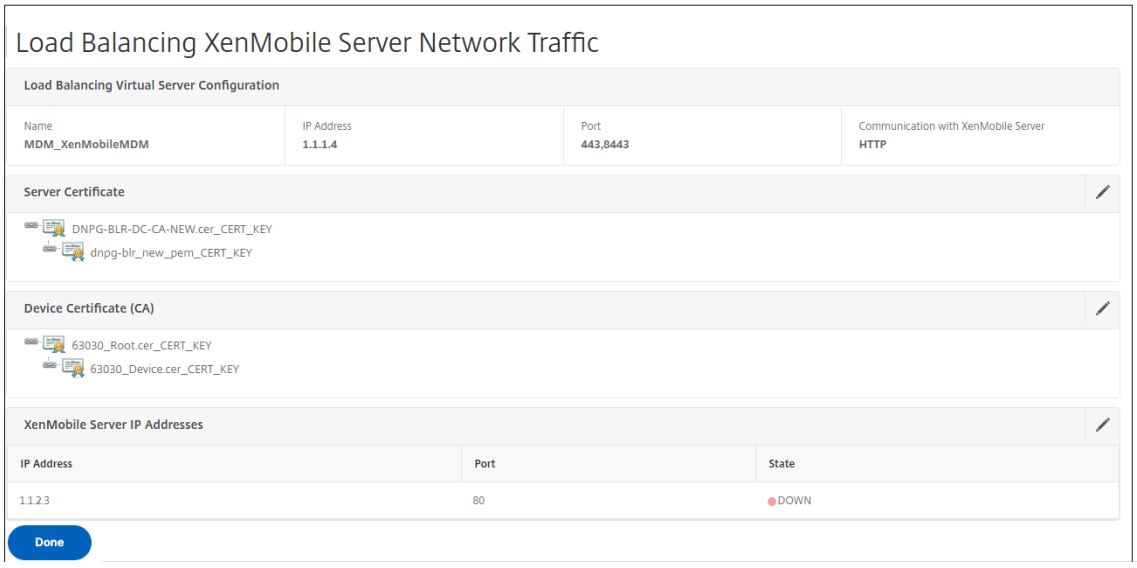
2. 構成ユーティリティにログオンします。[ホーム] タブの [**MDM** サーバー **LB**] で、[構成] をクリックします。
3. [デバイス管理用 **LB** 仮想サーバー] の [名前] に、サーバーの名前を入力します。
4. [**IP** アドレス] に、仮想サーバーの IP アドレスを入力し、[続行] をクリックします。
5. [**Citrix Endpoint Management MDM** サーバーの負荷分散] ページで、手順 3 と 4 を繰り返し、[作成] をクリックします。
6. 設定を確認し、[完了] をクリックします。
7. サーバー証明書の追加を求めるメッセージが表示されたら、サーバー証明書を選択し、[**Continue**] をクリックします。



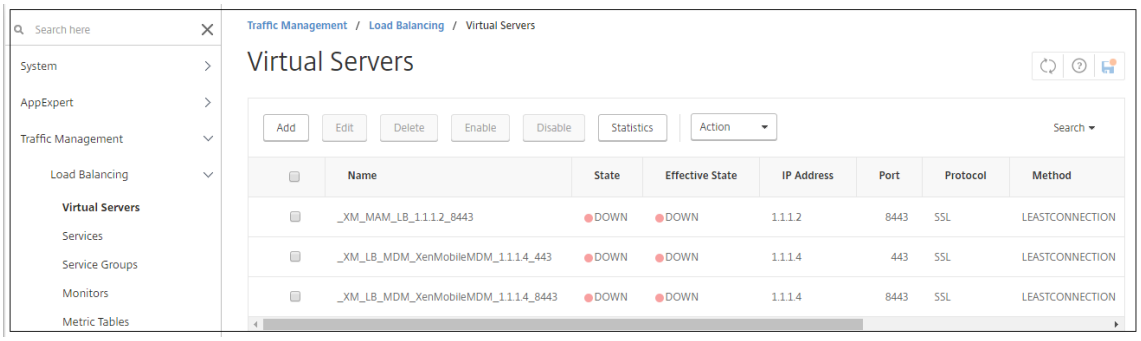
8. CA 証明書を指定し、[続行] をクリックします。



9. 同じ Citrix Endpoint Management IP アドレスを保持します。［完了］をクリックします。



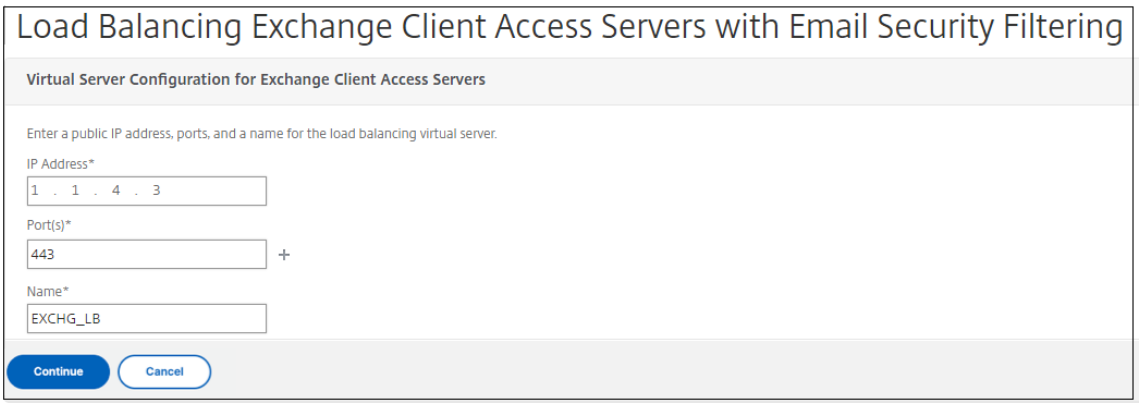
10. 負荷分散の設定を確認するには、[トラフィック管理] **>** [仮想サーバー] に移動します。



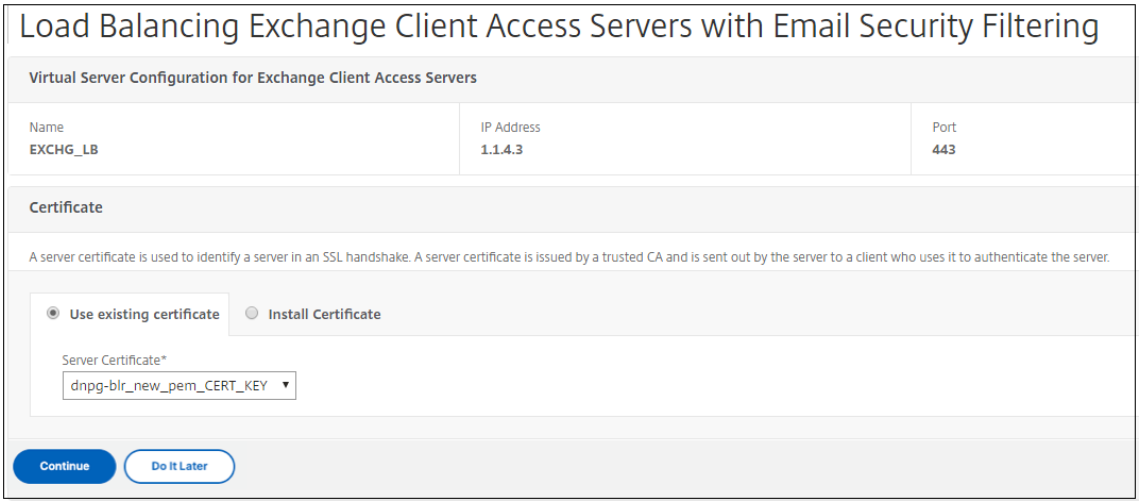
電子メールセキュリティフィルタを使用した **Microsoft Exchange** の負荷分散サーバーを構成する

February 1, 2024

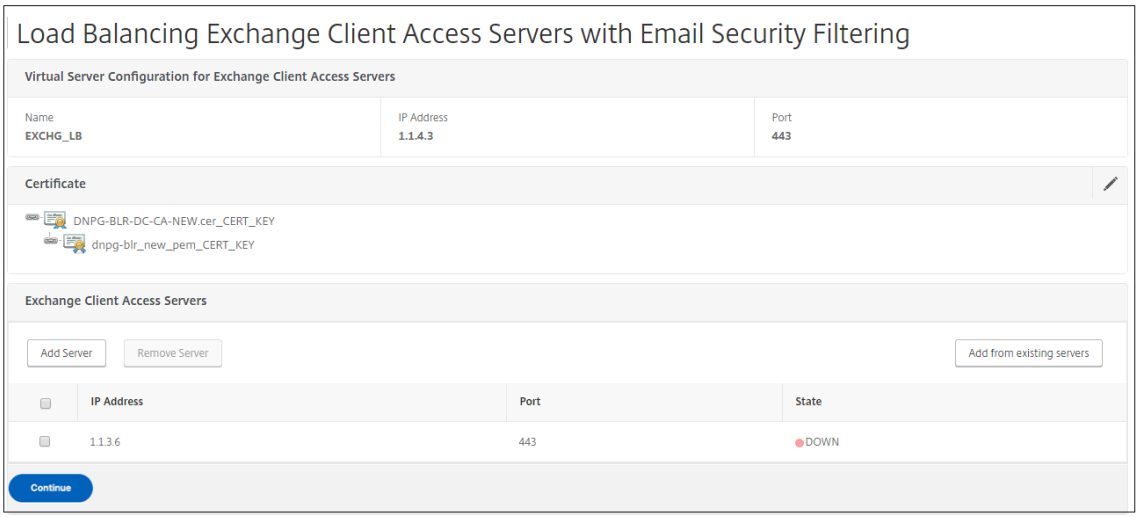
1. [ホーム] タブの [**MDM** サーバー **LB**] で、[構成] をクリックします。
2. [**Exchange CAS** 用 **LB** 仮想サーバー] の [名前] に、サーバーの名前を入力します。
3. [**IP** アドレス] に、仮想サーバーの IP アドレスを入力します。
4. [**Port**] ボックスにポート番号を入力します。さらにポートを追加するには、プラス記号 (**+**) をクリックし、ポート番号を入力します。
5. [続行] をクリックします。



6. [証明書] で、既存の証明書を選択するか、コンピューター（ローカル）または NetScaler ADC アプライアンス（アプライアンス）にある証明書をインストールします。
7. [続行] をクリックします。



8. 「**Exchange Citrix Analytics** 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、および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 NetScaler 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。

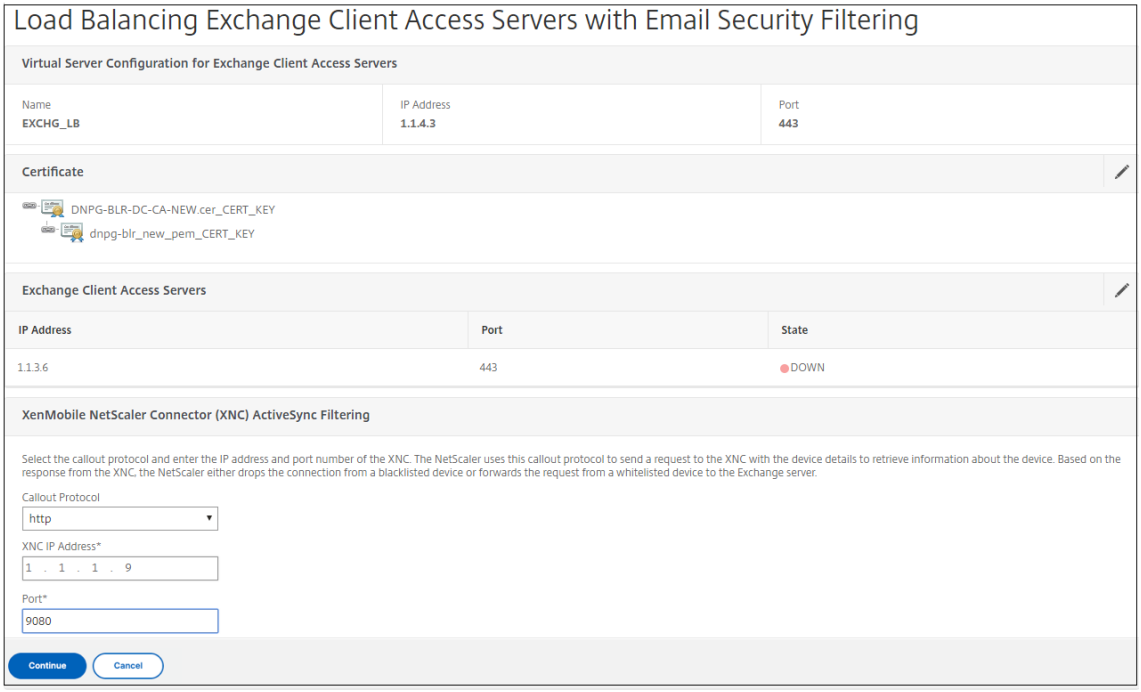
Citrix Endpoint Management を構成する **NetScaler ADC** コネクタ（**XNC**）**ActiveSync** フィルタリング

February 1, 2024

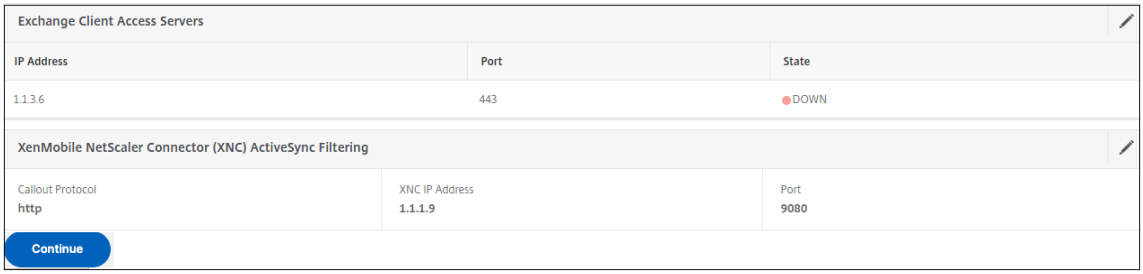
Citrix Endpoint Management NetScaler ADC コネクタ（XNC）は、ActiveSync クライアントのデバイスレベルの承認サービスを提供します。NetScaler ADC は、Exchange ActiveSync プロトコルのリバースプロキシとし

て機能します。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り、承認が制御されます。

1. [**Citrix Endpoint Management NetScaler 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 NetScaler ADC コネクタの IP アドレスを入力します。
3. [ポート] に、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 業務用モバイルアプリでモバイルデバイスからのアクセスを許可する

April 1, 2024

NetScaler for XenMobile ウィザードでは、サポートされているデバイスから NetScaler Gateway を介して内部ネットワークのモバイルアプリおよびリソースにユーザーが接続できるようにするために必要な設定を構成します。ユーザーは、マイクロ VPN トンネルを確立するセキュアハブ（以前の Citrix Secure Hub）を使用して接続します。ユーザーが接続すると、VPN トンネルが NetScaler Gateway に開かれ、内部ネットワークの XenMobile に渡されます。ユーザーは、XenMobile Mobile 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。

複数のデバイスで同時に NetScaler Gateway 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。詳細については、仮想サーバーでの接続タイプの構成を参照してください。

XenMobile 用 NetScaler ADC 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ガイダンス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いることを確認してください。詳しくは、XenMobile の展開に関する記事を参照してください 。

NetScaler Gateway で **Secure Browse** を構成する

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ときは、[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、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、[**NetScaler 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、[グローバル設定の変更] をクリックします。
3. ［グローバル **NetScaler Gateway** 設定］ダイアログボックスの［セキュリティ］タブで、[**SecureBrowse**] 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の［構成］タブのナビゲーションペインで、［NetScaler 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、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、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、次のいずれかを実行します:
   - 「リクエストプロファイル」の横にある「新規」をクリックします。

- 「リクエストプロファイル」の横にある「変更」をクリックします。

4. [セキュリティ**]** タブで、**[**セキュリティ **SecureBrowse**] の横にある [グローバルを上書き] をクリックし、[セキュリティ **Secure Browse**] 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、[作成] 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、[作成]、[閉じる] の順にクリックします。
   - 既存のプロファイルを変更する場合は、選択後に「**OK**」を 2 回クリックします。

Secure Browse モードで Secure Web のトラフィックポリシーを構成するには、次の手順を実行します。

次の手順に従って、Secure Web トラフィックを Secure Browse モードでプロキシサーバ経由でルーティングするようにトラフィックポリシーを構成します。

1. 構成ユーティリティの［構成］タブで、［**NetScaler 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. 右側のペインで、[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。
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. [**Create**］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。クライアントレス VPN 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は、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. [**Create**］をクリックします。
9. [トラフィックポリシー] 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、[要求プロファイル（**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.HTTP.HEADER HOST contains ActiveSyncServer || REQ.HTTP.HEADER
    User-Agent CONTAINS WorxMail || REQ.HTTP.HEADER User-Agent
    CONTAINS com.zenprise || REQ.HTTP.HEADER User-Agent CONTAINS
    Citrix Secure Hub || REQ.HTTP.URL CONTAINS AGServices || REQ.
    HTTP.URL CONTAINS StoreWeb
<!--NeedCopy-->
```

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 Active Sync サーバ名で置き換えます。

11. [トラフィックポリシー] 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、[要求プロファイル（**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.HEADER User-Agent CONTAINS Mozilla	REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser

12. [トラフィックポリシー] 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、[要求プロファイル（**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.HEADER User-Agent CONTAINS Mozilla	REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser

13. ［**NetScaler 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て、［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] で、**[**ポリシーの選択**]** の横にある [**] をクリックします。
18. ステップ 10 で作成したポリシーを選択し、**OK** をクリックします。
19. ［**Bind**］ 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** 仮想サーバトラフィックポリシーのバインド**]** で、**[**** バインドの追加 ****]** をクリックします。
22. [ポリシーバインド] 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リストを表示します。
23. ステップ 11 で作成したポリシーを選択し、［**OK**］ をクリックします。
24. ［**Bind**］ 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** 仮想サーバトラフィックポリシーのバインド**]** で、**[**** バインドの追加 ****]** をクリックします。
27. [ポリシーバインド] 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リストを表示します。
28. ステップ 12 で作成したポリシーを選択し、［**OK**］ をクリックします。

29. [**Bind**] 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。

必ず XenMobile コンソールで Secure Web（WorxWeb）アプリを構成してください。[構成] **>** [アプリ] の順に選択し、Secure Web アプリを選択して [編集] をクリックし、次の変更を行います。

- [アプリ情報] 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。

アプリケーションと **MDX** トークンのタイムアウトを構成する

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。

トークンをアクティブにす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ると、ユーザーはアプリケーションやウェブページなどの要求されたリソースにアクセスできなくなります。

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、NetScaler 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、[**NetScaler 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、[グローバル設定の変更] をクリックします。
3. [グローバル **NetScaler 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を無効にする

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を作成する必要があります。事前認証ポリシーまたは認証後ポリシーをモバイルデバイス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構成する場合は、Android または iOS を除外する User-Agent 文字列を追加します。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、次のポリシー式を作成して、User-Agent に Android が含まれているかどうか、アプリケーション virus.exe が存在しないかどうかを確認し、事前認証プロファイルを使用してプロセス keylogger.exe が実行されている場合はプロセスを終了します。ポリシー式は次のようになります。

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS Android &&
CLIENT.APPLICATION.PROCESS(keylogger.exe) contains
```

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。

Android デバイスの **DNS** サフィックスを使用して **DNS** クエリをサポートする

ユーザーが Android デバイスからマイクロ VPN 接続を確立すると、NetScaler 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。NetScaler Gateway は、構成するスプリット DNS 設定に基づくスプリット DNS クエリをサポートします。NetScaler Gateway は、アプライアンスに構成した DNS サフィックスに基づくスプリット 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、NetScaler 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 リクエストをローカル DNS サーバに送信します。
- スプリット **DNS** をリモートに設定すると、すべての DNS 要求は、解決のために NetScaler 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ます。
- スプリット DNS を [両方] に設定すると、Android デバイスは DNS リクエストタイプをチェックします。
  - DNS 要求タイプが「A」でない場合、DNS 要求パケットはローカルおよびリモート DNS サーバの両方に送信されます。
  - 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 NetScaler ADC アプライアンスに構成された 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 要求はリモート 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リストに基づいて動作するスプリット DNS をまとめたものです。

スプリット DNS 設定	タイプ A のレコードですか	接尾辞リストに載ってるの?	DNS リクエストの送信先
ローカル	はいまたはいいえの両方	はいまたはいいえの両方	ローカル
リモート	はいまたはいいえの両方	はいまたはいいえの両方	リモート
両方	いいえ	-	両方
両方	はい	はい	リモート
両方	はい	いいえ	ローカル

DNS サフィックスを設定するには、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、[NetScaler 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 [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.「リクエストプロファイル」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」の横にある「グローバルを上書き」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。

NetScaler Gateway でスプリット DNS 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、[**NetScaler 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、[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

NetScaler 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の［構成］タブのナビゲーションペインで、[NetScaler 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 [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.「リクエストプロファイル」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、［スプリット **DNS**］の横にある［グローバルを上書き］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**］
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 のドメインおよびセキュリティトークン認証を構成する

April 1, 2024

RADIUS プロトコルを使用して、LDAP 資格情報と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 要素認証の種類に必要な NetScaler Gateway 構成について説明します。

前提条件

Citrix Endpoint Management 用 NetScaler ADC ウィザードをまだ実行していない場合は、「Citrix Endpoint Management 環境の設定を構成する」の「*NetScaler for Citrix Endpoint Management* ウィザード」セクションを参照してください。NetScaler ADC 構成に次のもの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 **userPrincipalName** （要件に応じて）

ドメインとセキュリティトークンの認証を構成するには

1. [**NetScaler Gateway**] **>** [仮想サーバー] に移動します。仮想サーバーを選択し、[編集] 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**」をクリックし、「バインド」をクリックして、「完了」をクリックします。
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、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] タブをクリックします。
6. 「認証情報インデックス」で「セカンダリ」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 Virtual Apps and Desktops に別々の NetScaler Gateway VIP を使用するには、次の式を使用してください。

   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」ドロップダウンメニューから、作成した RADIUS サーバ名を選択します。
14. 「式」に「REQ.HTTP.HEADER ユーザーエージェントには **CitrixReceiver** が含まれています」と入力し、「作成」をクリックします。
15. 仮想サーバーを選択し、[編集] 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**]** の **[**ポリシーの選択] から [**RADIUS**] を選択します。
20. [**Bind**] 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、[挿入] 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. [**Bind**] 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プライオリティが最も高いことを確認します。これにより、モバイルユーザー以外のユーザーに対してさらに多くのポリシーが追加された場合でも、そのユーザーの優先度が最高になります。詳細については、認証ポリシーの優先度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とドメイン認証を構成する

April 1, 2024

NetScaler for Citrix Endpoint Management ウィザードを使用して、NetScaler 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 NetScaler ADC ウィザードは一度だけ実行できます。ウィザードの使用について詳しくは、「Citrix Endpoint Management 環境の設定を構成する」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、この記事の手順を使用して、クライアント証明書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の構成を行います。

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「NetScaler ADC 証明書失効リスト（CRL）」を参照してください。

GUI を使用してクライアント証明書認証用に NetScaler Gateway を構成する

1. **Traffic Management > Load Balancing > Virtual Servers** に移動します。
2. **SSL** タイプの仮想サーバーを選択し、**[SSL** パラメータ] セクションで [セッションの再利用を有効にする] を [無効] に設定します。
3. 「**NetScaler Gateway**」**>**「仮想サーバー」に移動します。
4. **SSL** タイプの仮想サーバを選択し、[編集（Edit）] をクリックします。
5. [**SSL** パラメータ] セクションで、[編集] アイコンをクリックします。
6. [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。
7. 認証証明書ポリシーを作成して、Citrix Endpoint Management が Secure Hub から NetScaler Gateway ****** に提供された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 ****** 。
8. ［**NetScaler Gateway**］**>**［ポリシー］**>**［認証］**>**［証明書］に移動します。
9. [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. 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 要素: **OFF** (証明書のみの認証)

    ユーザー名フィールド: 件名: **CN**

    Group Name Field：**SubjectAltName:PrincipalName**
11. 証明書認証ポリシーのみを NetScaler Gateway 仮想サーバーのプライマリ認証としてバインドします。
12. ルート CA 証明書をバインドして、NetScaler 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。

GUI を使用してクライアント証明書とドメイン認証用に NetScaler Gateway を構成する

1. **Traffic Management > Load Balancing > Virtual Servers** に移動します。
2. **SSL** タイプの仮想サーバーを選択し、**[SSL** パラメータ] セクションで [セッションの再利用を有効にする] を [無効] に設定します。

3. **NetScaler Gateway >** ポリシー **>** 認証 **>** 証明書に移動します。
4. [プロファイル] タブをクリックし、[追加] をクリックします。
5. プロファイルの名前を入力し、[**2** 要素] を [オン] に設定し、[ユーザー名フィールド] から [**subjectAltNamePrincipalName**] を選択します。
6. [ポリシー] タブをクリックし、[追加] をクリックします。
7. 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] を設定して **[**作成] をクリックします。
8. [仮想サーバー] に移動し、タイプ **SSL** の仮想サーバーを選択して、[編集] をクリックします。
9. [認証] の横にある [**+**] をクリックして、証明書認証を追加します。
10. 認証方法を選択するには、「ポリシーの選択」で「証明書」を選択し、「タイプの選択」で「プライマリ」を選択します。これにより、証明書認証が LDAP 認証タイプと同じ優先順位のプライマリ認証としてバインドされます。
11. [ポリシーのバインド] で、**[**クリックして選択] をクリックし、以前に作成した証明書ポリシーを選択します。
12. 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。
13. [優先度] を **100** に設定し、[バインド] をクリックします。以降の手順で 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。
14. [**LDAP** ポリシー] の行で、[**] をクリックします。
15. ポリシーを選択し、[編集] ドロップダウンメニューから [バインドの編集] をクリックします。
16. 証明書ポリシーに指定したのと同じ [**Priority**] 値を入力します。［**Bind**］をクリックします。
17. ［閉じる］をクリックします。
18. **SSL** パラメータセクションの編集アイコンをクリックします。
19. 「クライアント認証」チェックボックスを選択し、「クライアント証明書」で「必須」を選択し、「**OK**」をクリックします。
20. ［完了］をクリックします。

NetScaler ADC 証明書失効一覧（**CRL**）

Citrix Endpoint Management は、サードパーティの認証局の証明書失効リスト（CRL）のみをサポートしています。Microsoft CA が構成されている場合、Citrix Endpoint Management は NetScaler 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、NetScaler ADC 証明書失効一覧（CRL）設定 ［**Enable CRL Auto Refresh**］を構成する必要があるかどうか検討します。この手順を使用すると、MAM のみ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 は、新しい証明書を再発行します。これは、失効したユーザー証明書がユーザー証明書を生成するこ

とを制限しないためです。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。

Microsoft Intune グレーション

February 1, 2024

Microsoft Intune と NetScaler Gateway の統合により、NetScaler Gateway および Intune が提供するクラス最高のアプリケーションアクセスおよびデータ保護ソリューションが提供されます。

電子メール、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、さまざまなプラットフォーム間で一元管理できる、安全な生産性向上アプリケーションの最も完全なスイートを入手できます。Intune と NetScaler 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、Citrix Secure Access クライアントサイドテクノロジーにより、これらの Intune 対応アプリケーションは NetScaler Gateway を介して企業データやアプリケーションに安全にアクセスできます。

この統合により、NetScaler Gateway は Intune からコンプライアンスデータをプルし、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、NetScaler Gateway は、デバイスの機能などに基づいてアクセスを制御するためのより細かい制御を提供します。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。

NetScaler Gateway 仮想サーバーが構成されると、NetScaler Gateway は Azure 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 Network-Only 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、アプリが AAD から直接フェッチできる ADAL トークンを使用して NetScaler Gateway にアクセスします。

Citrix マイクロ VPN と Microsoft Endpoint Manager との統合

NetScaler Gateway のお客様は、Microsoft Endpoint Manager（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るため、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。これは、モバイルバッテリーの寿命を向上させるのにも役立ちます。NetScaler のマイクロ VPN テクノロジーは、モバイルユーザーに最高のユーザーエクスペリエンスを提供しながら、社内のビジネスリソースへの安全なアクセスを提供します。

Micro VPN は、次のユースケースでのみサポートされています。

- 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:
>
> SSL VPN 機能を利用するには、マイクロ VPN には NetScaler Gateway Advanced または Premium エディション（VPX 3000 以上）と Citrix Endpoint Management の使用権限が必要です。Citrix Endpoint Management の資格を取得すると、Microsoft Edge モバイルブラウザ（iOS および Android）上のマイクロ VPN SDK が引き続きサポートされます。詳細については、営業、アカウント、またはパートナーの担当者にお問い合わせください。

Microsoft エンドポイントマネージャーとの Citrix マイクロ VPN 統合の設定について詳しくは、「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 NetScaler 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場合

February 1, 2024

次のシナリオは、統合された Intune MDM ソリューションの使用方法を示しています。

- 新しい顧客が、オンプレミスの NetScaler Gateway 展開で Intune をオンボーディングすることにしました
- 既存の NetScaler Gateway ユーザーが Intune でモバイルデバイス管理を追加したいと考えています
- 既存の Intune ユーザーは、モバイルデバイスまたはアプリケーションが、企業 DMZ 内の NetScaler Gateway 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、企業ネットワーク内にあるデータにアクセスすることを許可したいと考えています。

> 注
>
> iOS および Android クライアントのみがサポートされています。

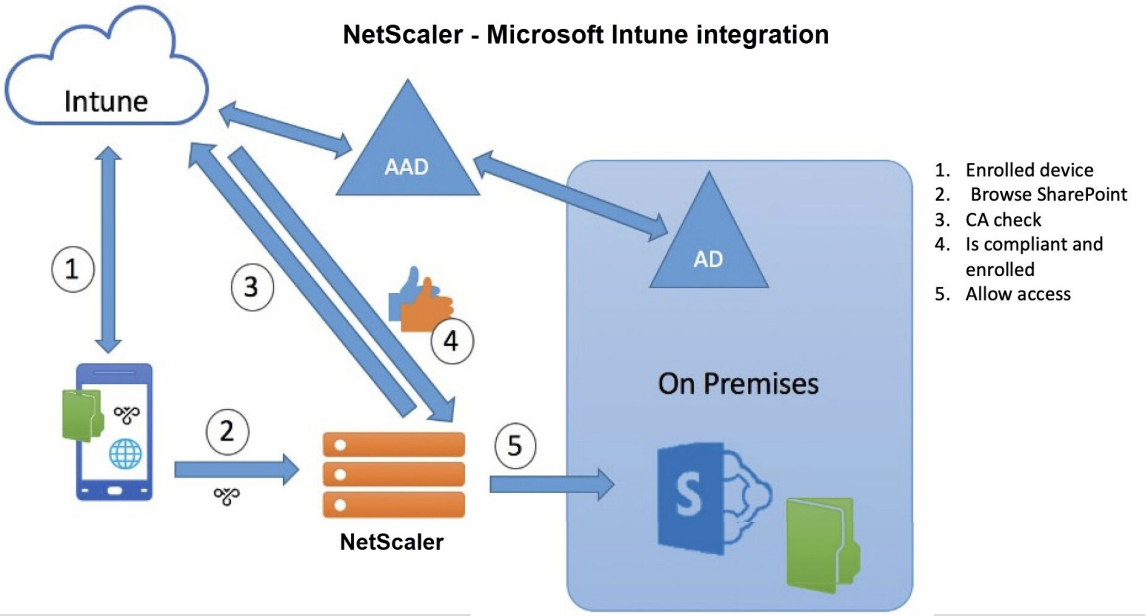
NetScaler Gateway MDM と **Intune** の統合を理解する

February 1, 2024

以下は、Intune との典型的な NetScaler Gateway MDM 統合におけるイベントのフローの例です。

1. Intune でモバイルデバイスを登録します。
2. 企業が承認し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. ブラウザ要求は NetScaler Gateway に送信されます。

5. NetScaler Gateway アプライアンスは、デバイスの登録ステータスを Intune で確認します。
6. 準拠している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。



デバイスが条件付きアクセスポリシーを満たしていない場合、NetScaler Gateway VPN クライアントはエラーメッセージを表示します。このメッセージは、デバイスから Intune がホストするページへのリンクを提供し、デバイスのコンプライアンス状態を登録または修復するオプションをユーザーに提供します。

> 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 にプッシュするときに次のこと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サマリーは区別する必要があります。

Intune NAC v2 API サポート

Intune NAC v2 API サポートの一環として、NetScaler アプライアンスがモバイルデバイスから有効な証明書を取得できるように、認証局ファイル（CA 証明書）をバインドする必要があります。Intune NAC v2 では、モバイルデバイスは CA 証明書の一部としてデバイス ID を送信します。ここでバインドされる CA 証明書は、エンドユーザーの iOS および Android デバイスにクライアント証明書を発行するために使用される証明書である必要があります。中間証明書がある場合は、その証明書もここでバインドする必要があります。

詳細については、「Intune NAC v2 API サポート」を参照してください。

単一要素ログイン用の **NetScaler 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を構成する

April 1, 2024

このトピックでは、Microsoft Intune e が提供するネットワークアクセスコンプライアンス（NAC）セキュリティを使用して、モバイルデバイス（iOS および Android）から内部ネットワークに接続するように NetScaler Gateway を構成する方法について説明します。ユーザーが iOS または Android VPN クライアントから NetScaler Gateway に接続しようとすると、ゲートウェイはまずデバイスが管理対象デバイスであり、準拠しているデバイスであるかどうかを Intune サービスで確認します。

- 管理対象: デバイスは Intune 企業ポータルクライアントを使用して登録されます。
- 準拠:Intune MDM サーバーからプッシュされた必須ポリシーが適用されます。

デバイスが管理対象で準拠している場合にのみ、VPN セッションが確立され、ユーザに内部リソースへのアクセスが提供されます。

> 注:
>
> - このセットアップでは、バックエンドの NetScaler Gateway が Intune サービスと通信します。SSL プロファイルは、NetScaler Gateway への着信接続を処理します。NetScaler Gateway バックエンド通信は、バックエンドクラウドサービス（Intune）の SNI 要件をすべて処理します。
> - DTLS ゲートウェイ仮想サーバー用の SNI は、NetScaler Gateway リリース 13.0 ビルド 64.x 以降でサポートされています。
> - Intune NAC チェックは、アプリごとの VPN またはデバイス全体の VPN でも、VPN プロファイルが Intune 管理ポータル（現在は Microsoft エンドポイントマネージャと呼ばれる）によってプロビジョニングされている場合にのみサポートされます。これらの機能は、エンドユーザが追加した VPN プロファイルではサポートされません。NAC チェックを使用するには、エンドユーザーデバイスの Intune 管理者によって Microsoft Endpoint Manager からデバイスに VPN プロファイルが展開されている必要があります。

ライセンス

この機能を使用するには、Citrix エンタープライズエディションのライセンスが必要です。

システム要件

- NetScaler Gateway リリース 11.1 ビルド 51.21 以降
- iOS VPN —10.6 以降
- Android VPN —2.0.13 以降

- Microsoft
  - Azure AD アクセス (テナント権限と管理者権限を持つ)
  - Intune が有効なテナント
- ファイアウォール
  サブネット IP アドレスから`https://login.microsoftonline.com`および`https://graph.windows.net` (ポート 53 およびポート 443) へのすべての DNS および SSL トラフィックに対するファイアウォールルールを有効にします。

前提条件

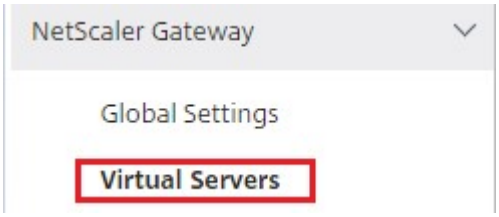
- 既存の認証ポリシーはすべて、クラシックポリシーから高度なポリシーに変換する必要があります。クラシックポリシーから高度なポリシーに変換する方法については、https://support.citrix.com/article/CTX131024を参照してください。
- Azure Portal で NetScaler Gateway アプリケーションを作成します。詳しくは、「Azure Portal での NetScaler Gateway アプリケーションの構成」を参照してください。
- 次のアプリケーション固有の情報を使用して、作成した NetScaler Gateway アプリケーションで OAuth ポリシーを構成します。
  - クライアント ID/アプリケーション ID
  - クライアントシークレット/アプリケーションキー
  - Azure テナント ID

参照ドキュメント

- このドキュメントでは、NetScaler Gateway のセットアップ構成について説明します。Citrix SSO クライアント (iOS/Android) の構成のほとんどは Intune 側で行われる。NAC 用の Intune VPN 設定の詳細については、https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrateを参照してください。
- iOS アプリの VPN プロファイルを設定するには、「https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-ios」を参照してください。
- Azure Portal で NetScaler Gateway アプリケーションをセットアップするには、「Azure Portal での NetScaler Gateway アプリケーションの構成」を参照してください。

ゲートウェイ展開用に **nFactor** を搭載した **NetScaler Gateway** 仮想サーバーを追加するには

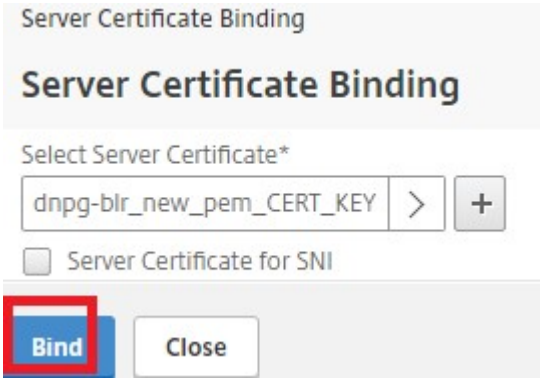
1. 「**NetScaler Gateway**」**>**「仮想サーバー」に移動します。



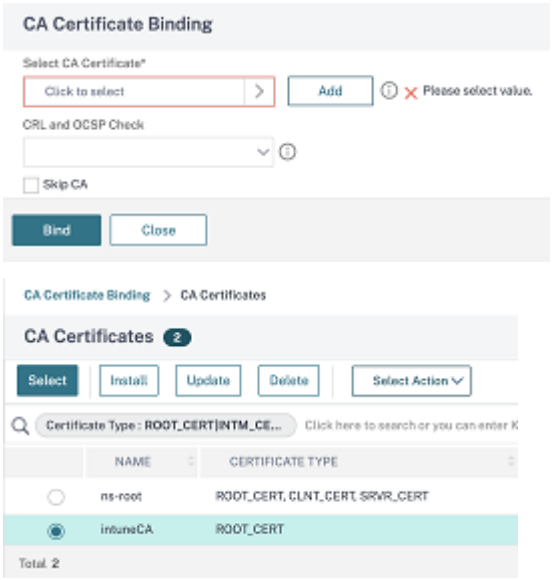
2. ［追加］をクリックします。
3. 「基本設定」領域に必要な情報を入力し、「**OK**」をクリックします。

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。

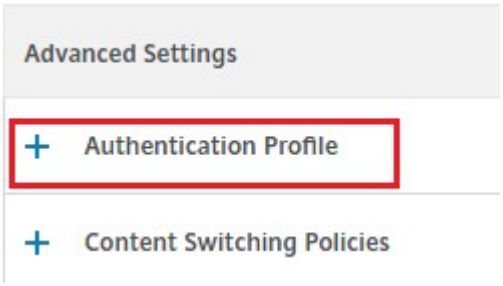


6. Intune NAC v2 API サポートの一環として、NetScaler アプライアンスがモバイルデバイスから有効な証明書を取得できるように、認証局ファイル（CA 証明書）をバインドする必要があります。Intune NAC v2 では、モバイルデバイスはクライアント証明書の一部としてデバイス ID を送信します。ここでバインドされる CA 証明書は、エンドユーザーの iOS および Android デバイスにクライアント証明書を発行するために使用される証明書である必要があります。中間証明書がある場合は、その証明書もここでバインドする必要があります。Intune の構成について詳しくは、「Azure Portal での NetScaler Gateway アプリケーションの構成」を参照してください。Intune NAC v2 API サポートの場合は、必要な CA 証明書を選択し、[バインド] をクリックします。

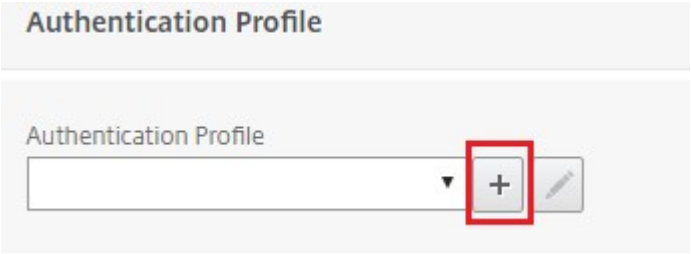


7. [続行] をクリックします。
8. [続行] をクリックします。
9. [続行] をクリックします。
10. **[**ポリシー**]** の横にあるプラスアイコン [+] をクリックし、**[**** ポリシーの選択] リストから [セッション] を選択し、[タイプの選択] リストから [要求] を選択して [続行] をクリックします。******
11. [ポリシーの選択] の横にあるプラスアイコン **[+]** をクリックします。
12. [**NetScaler Gateway** セッションポリシーの作成] ページで、セッションポリシーの名前を入力します。

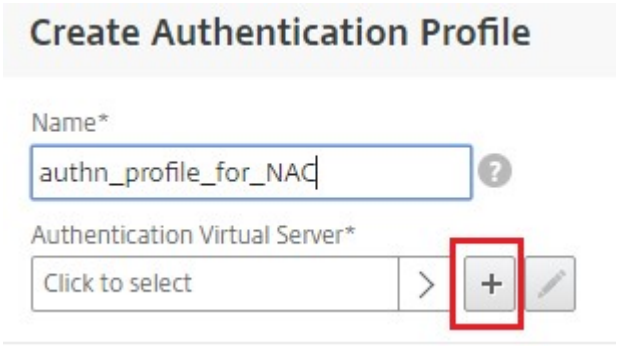
13. ［プロファイル］の横にあるプラスアイコン [+] をクリックし、［**NetScaler Gateway** セッションプロファイルの作成］ページでセッションプロファイルの名前を入力します。
14. [クライアントエクスペリエンス] タブで、[クライアントレスアクセス] の横にあるチェックボックスをクリックし、リストから [オフ] を選択します。
15. [プラグインタイプ] の横にあるチェックボックスをクリックし、リストから [Windows/Mac OS X] を選択します。
16. [詳細設定] をクリックし、[クライアントの選択] の横にあるチェックボックスをオンにし、その値を [オン] に設定します。
17. [セキュリティ] タブで、[既定の承認アクション] の横にあるチェックボックスをクリックし、リストから [許可] を選択します。
18. [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、一覧から [オフ] を選択します。
19.「作成」をクリックします。
20. ［**NetScaler Gateway** セッションポリシーの作成］ページの［式］領域で、修飾式を構成します。
21. ［**Create**］をクリックします。
22. ［**Bind**］をクリックします。
23. [詳細設定] で [認証プロファイル] を選択します。



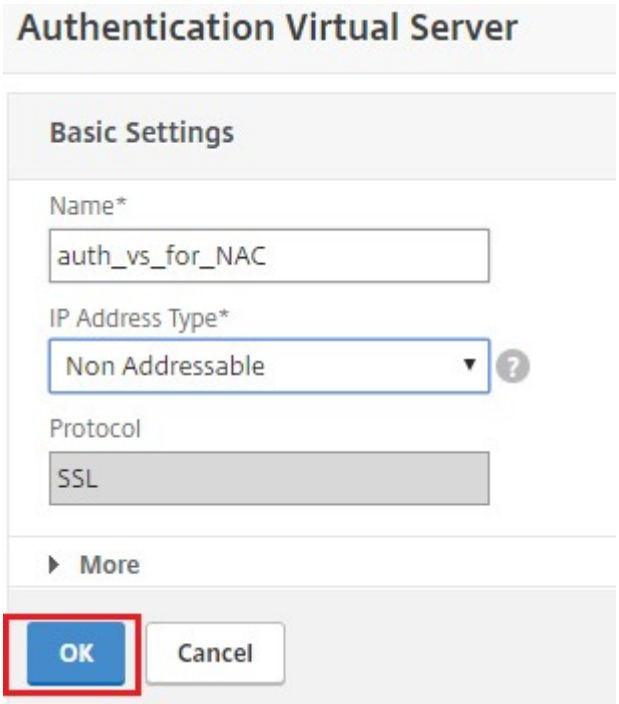
24. プラスアイコン **[+]** をクリックし、認証プロファイルの名前を入力します。



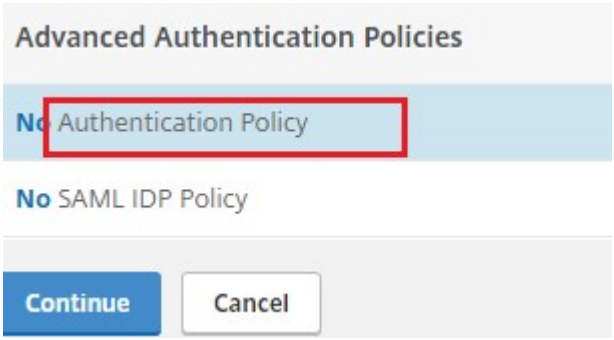
25. プラスアイコン **[+]** をクリックして、認証仮想サーバを作成します。



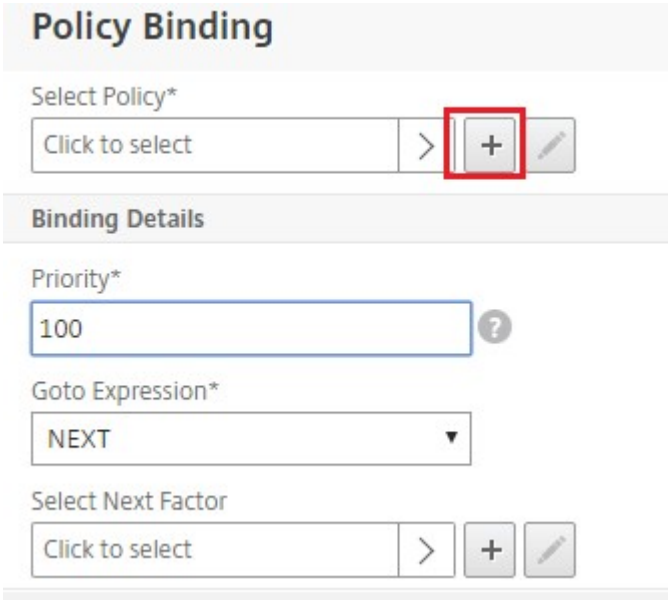
26. ［基本設定］領域で認証仮想サーバーの名前と IP アドレスの種類を指定し、［**OK**］をクリックします。IP アドレスタイプは、アドレス指定不可にもできます。



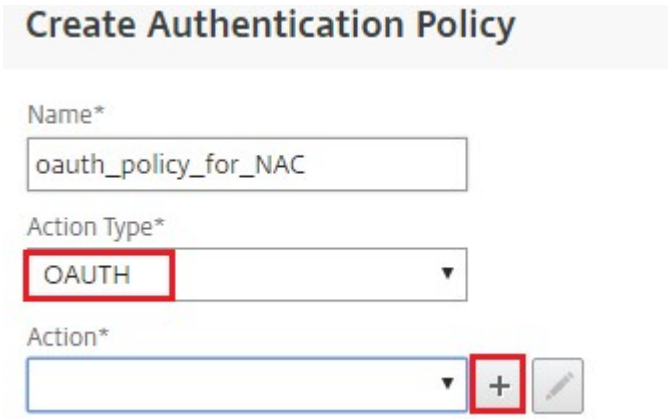
27. [認証ポリシー] をクリックします。



28. [Policy Binding] ビューで、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。



29. [アクションタイプ] として [**OAUTH**] を選択し、プラスアイコン **[+]** をクリックして NAC の OAuth アクションを作成します。



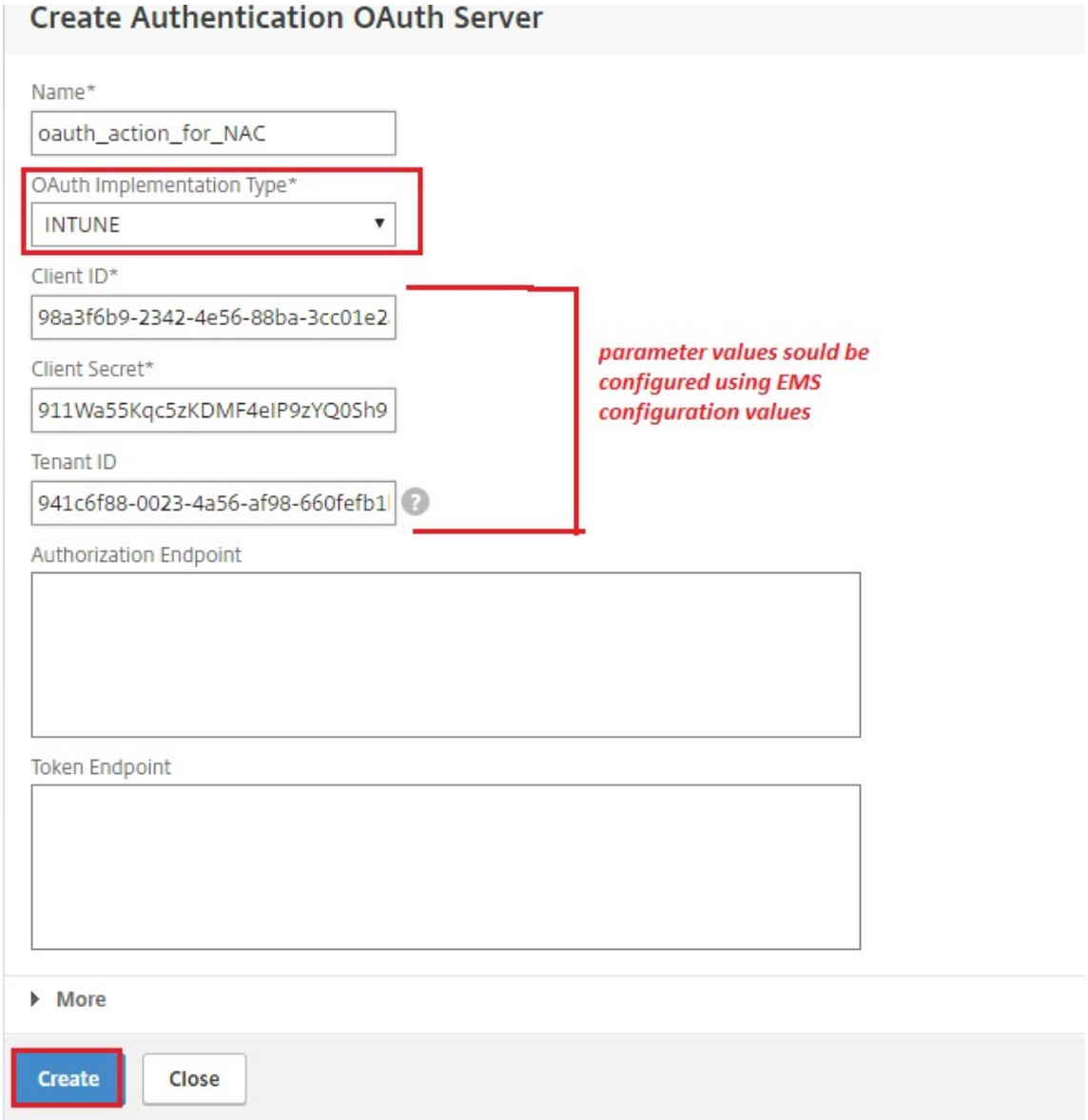
30. クライアント **ID**、クライアントシークレット、およびテナント **ID** を使用して OAuth アクションを作成します。

> 注:
>
> - クライアント **ID**、クライアントシークレット、およびテナント **ID** は、Azure Portal で NetScaler Gateway アプリケーションを構成した後に生成されます。
> - クライアント ID/アプリケーション ID、クライアントシークレット/アプリケーションシークレット、および Azure テナント ID の情報は、後で NetScaler Gateway で OAuth アクションを作成する際に必要になるため、書き留めておきます。

アプライアンスに適切な DNS ネームサーバが設定されていて、解決して到達できることを確認します。

```
-https://login.microsoftonline.com/,
-https://graph.windows.net/,
```

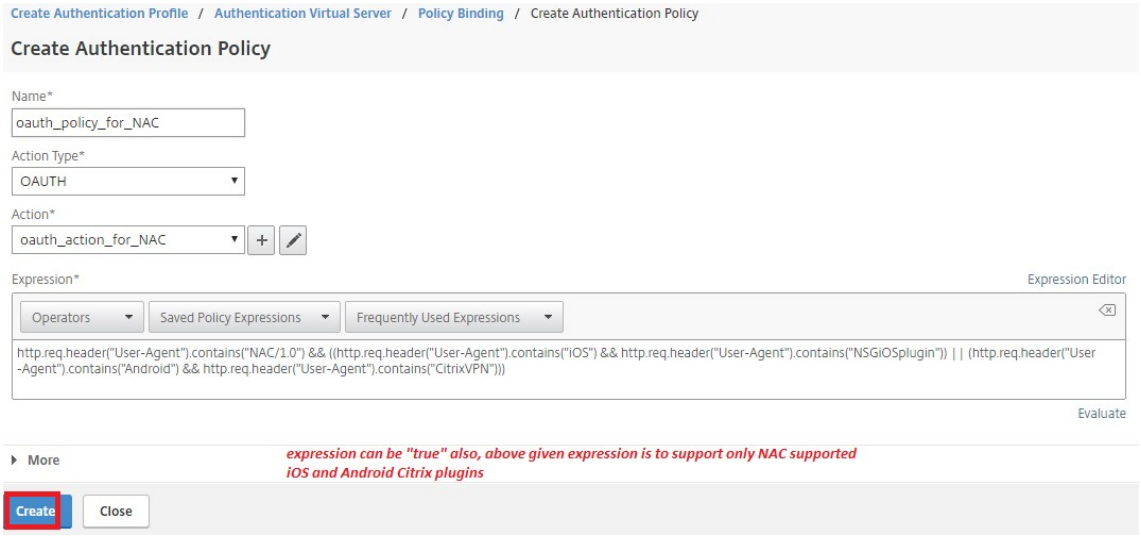

- *.manage.microsoft.com。



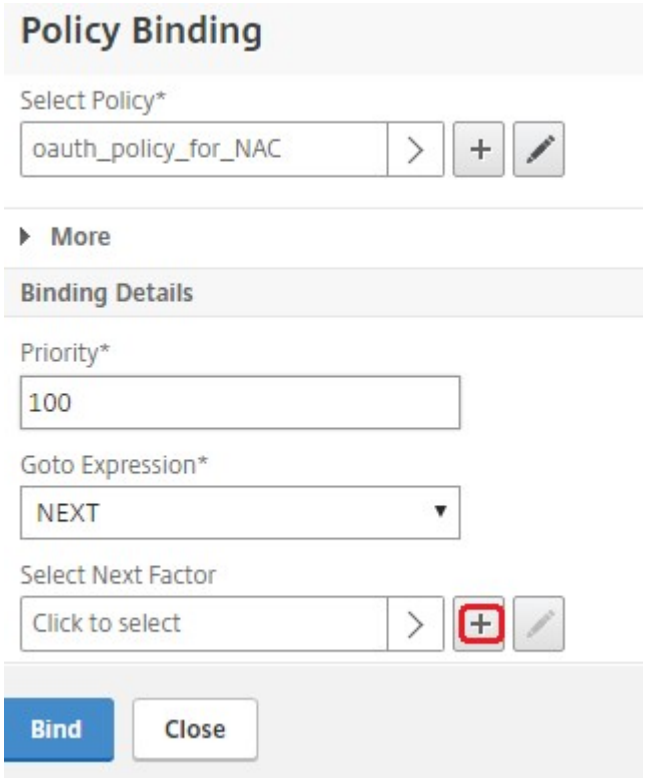
31. **OAuth** アクションの認証ポリシーを作成します。

規則:

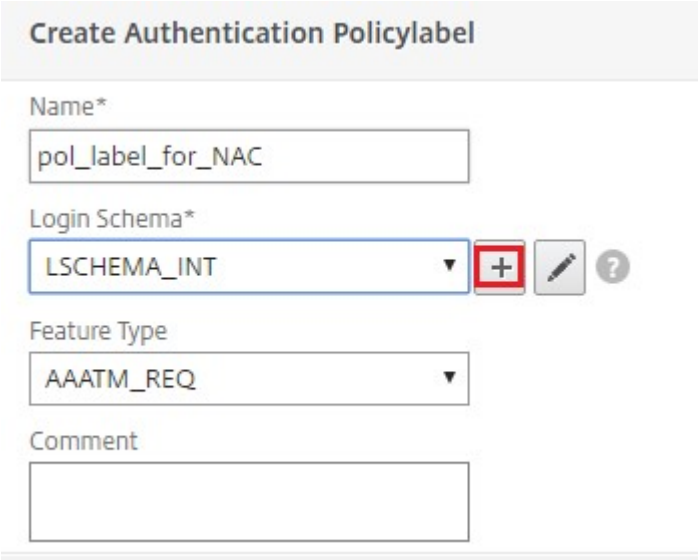
```
1 http.req.header("User-Agent").contains("NAC/1.0")&& ((http.req.
    header("User-Agent").contains("iOS") && http.req.header("User-
    Agent").contains("NSGiOSplugin")) || (http.req.header("User-
    Agent").contains("Android") && http.req.header("User-Agent").
    contains("CitrixVPN")))
2 <!--NeedCopy-->
```

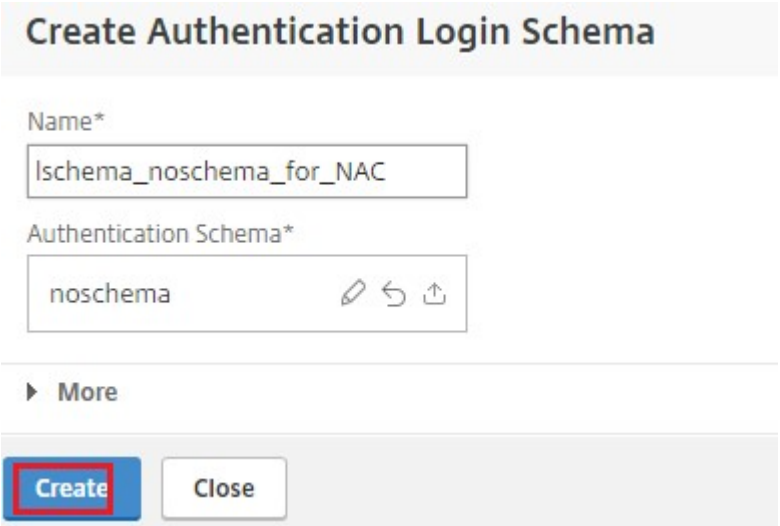
32. プラスアイコン **[+]** をクリックして NextFactor ポリシーラベルを作成します。



33. プラスアイコン **[+]** をクリックして、ログインスキーマを作成します。



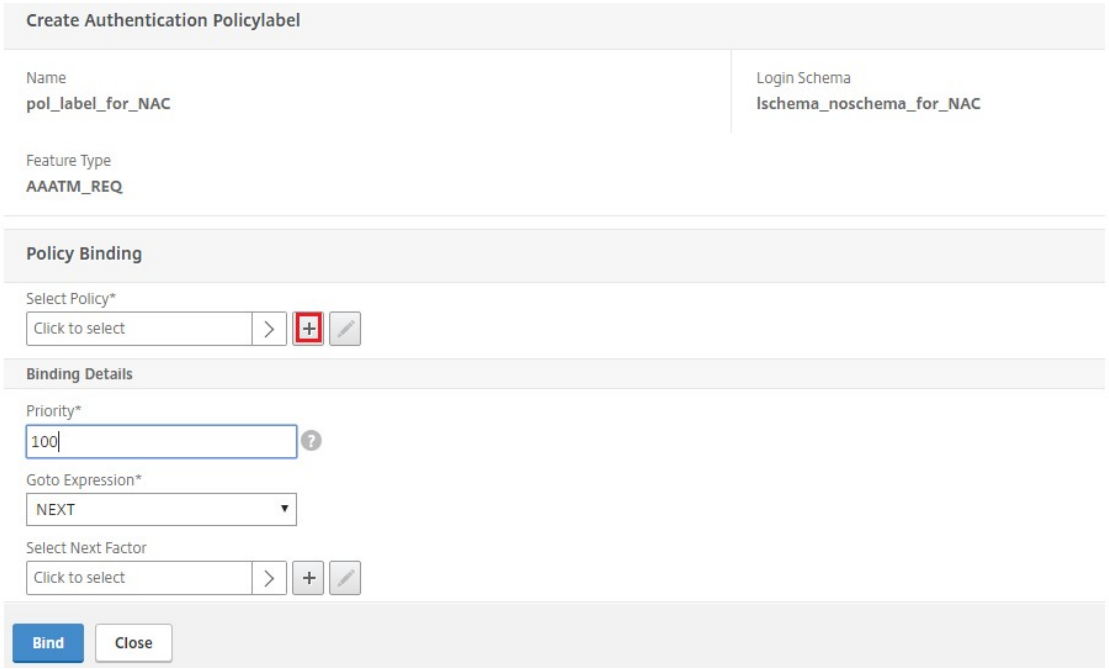
34. 認証スキーマとして**noschema**を選択し、[作成] をクリックします。



35. 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。

    ![続ける] をクリックします](/ja-jp/netscaler-gateway/media/intune_18.jpg)

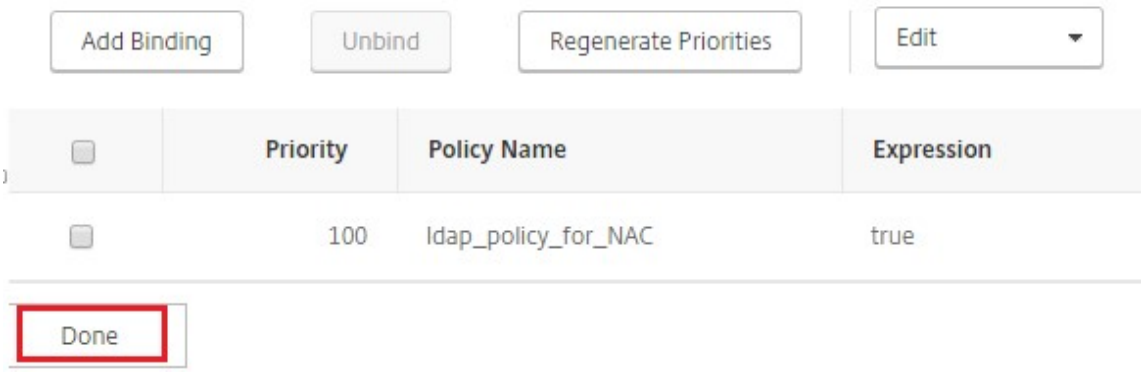
36. **[**ポリシーの選択（Select Policy）] で、ユーザログイン用の既存の認証ポリシーを選択するか、プラスアイコン [**+**] をクリックして認証ポリシーを作成します。
    認証ポリシーの作成について詳しくは、[高度な認証ポリシーの構成および LDAP 認証の設定を参照してください](/ja-jp/netscaler-gateway/13-1/authentication-authorization/configure-ldap.html)。



37. [**Bind**] をクリックします。

    ![バインド] をクリックします](/ja-jp/netscaler-gateway/media/intune_21.jpg)

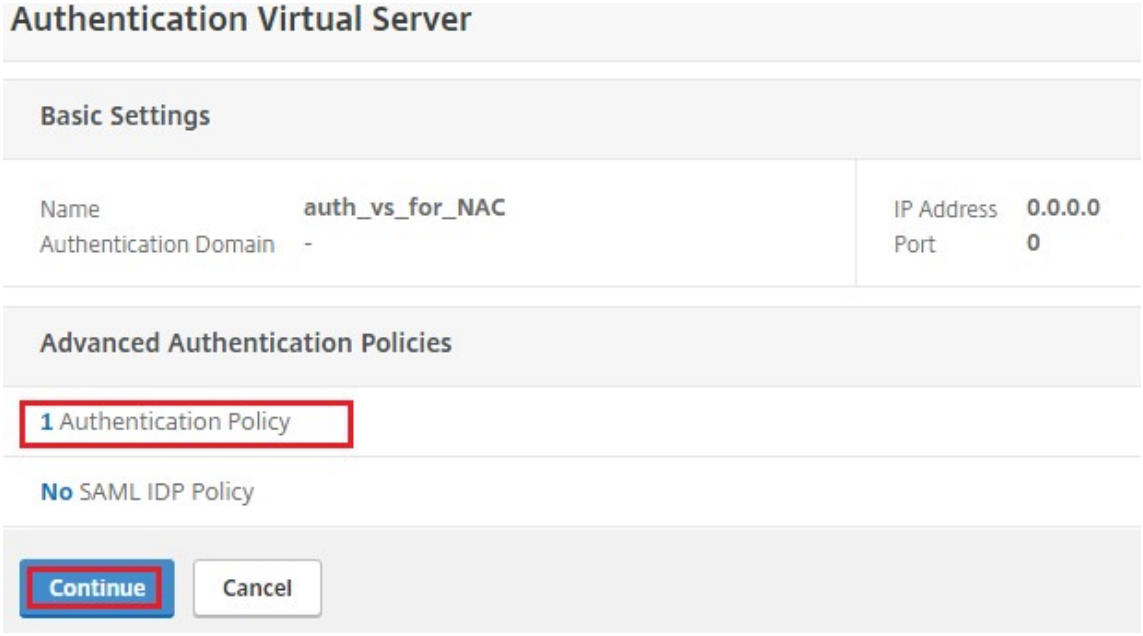
38. [完了] をクリックします。



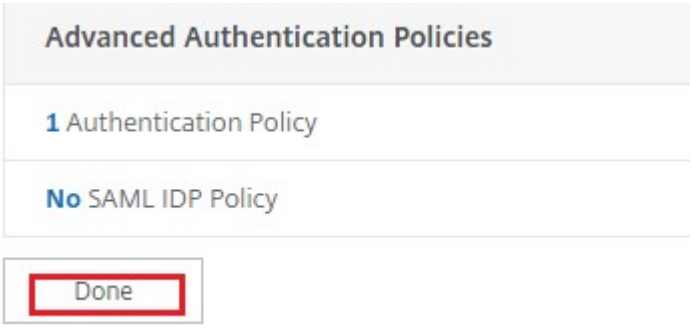
39. [**Bind**] をクリックします。

    ![バインド] をクリックします](/ja-jp/netscaler-gateway/media/intune_23.jpg)

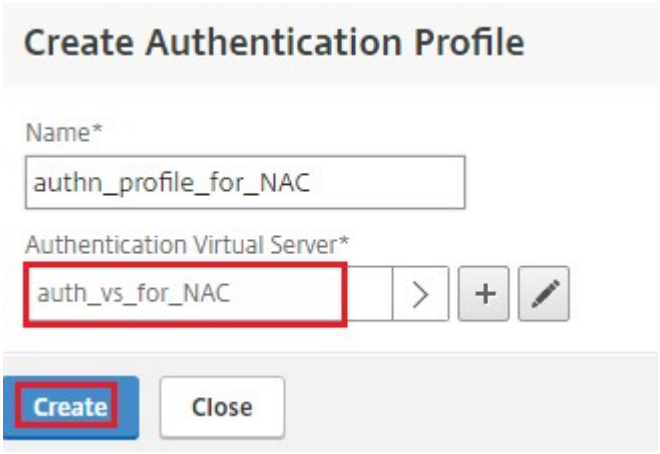
40. [続行] をクリックします。



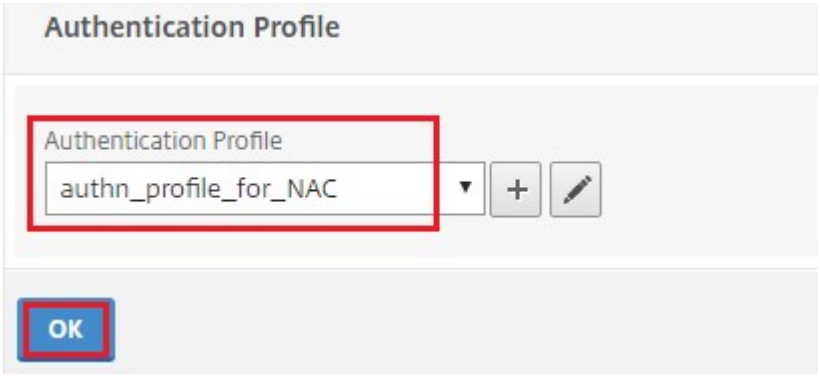
41. ［完了］をクリックします。



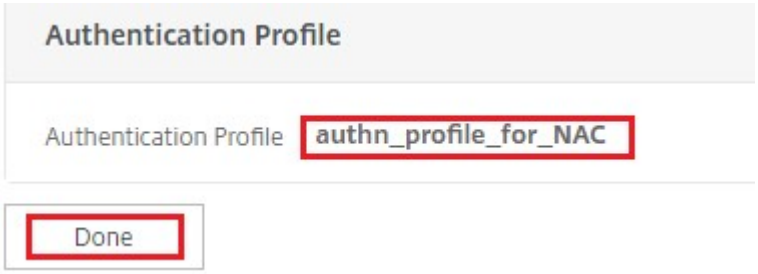
42. ［**Create**］をクリックします。



43. ［**OK**］をクリックします。



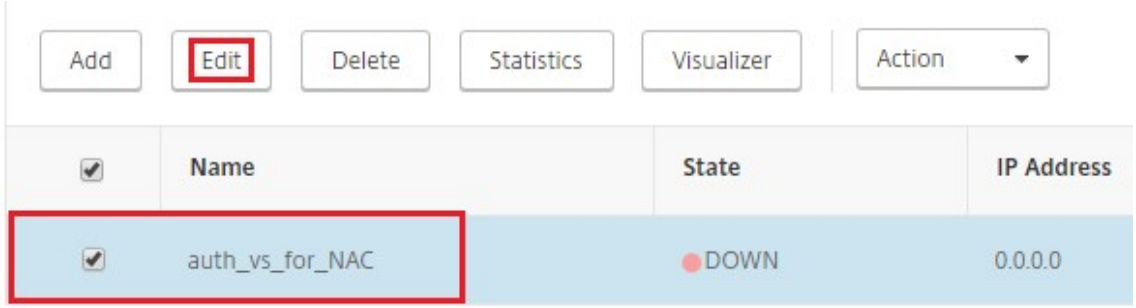
44. ［完了］をクリックします。



認証ログインスキーマを認証仮想サーバーにバインドして、**VPN** プラグインが **/cgi/login** 要求の一部としてデバイス **ID** を送信するように指示するには

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。

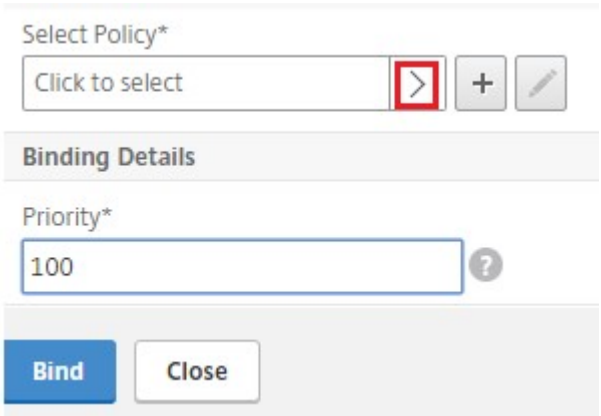
2. 以前に選択した仮想サーバを選択し、[編集（Edit）] をクリックします。



3. [詳細設定] の [ログインスキーマ] をクリックします。

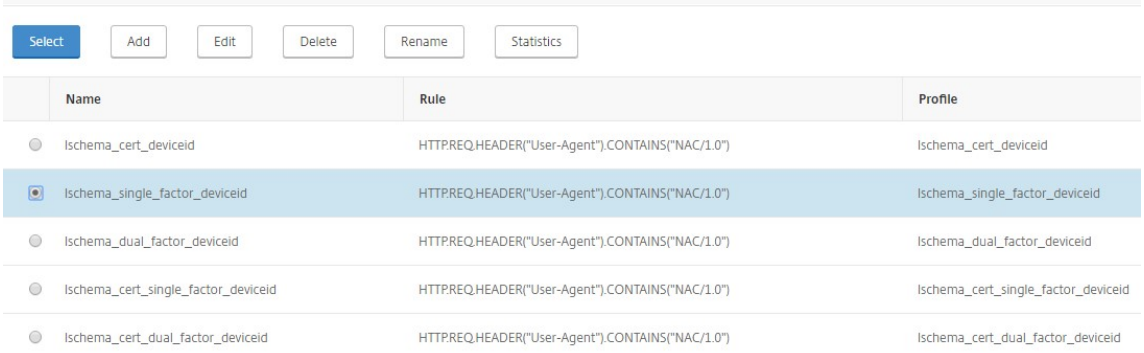
4. [ログインスキーマ] をクリックしてバインドします。

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てバインドします。



6. 認証展開に適した必要なログインスキーマポリシーを選択し、[選択（**Select**）] をクリックします。

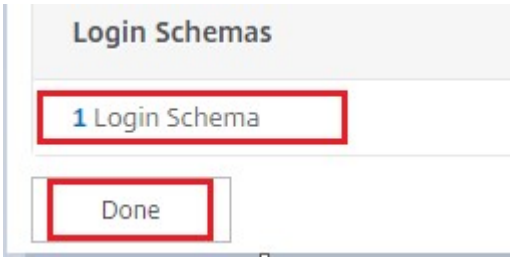
   前述の展開では、単要素認証（LDAP）と NAC OAuth Action ポリシーが使用されます。したがって、**lschema_single_factor_deviceid** が選択されます。



7. [**Bind**] をクリックします。

   ![バインド] をクリックします](/ja-jp/netscaler-gateway/media/a_intune_7.jpg)

8. [完了] をクリックします。



Intune NAC v2 API サポート

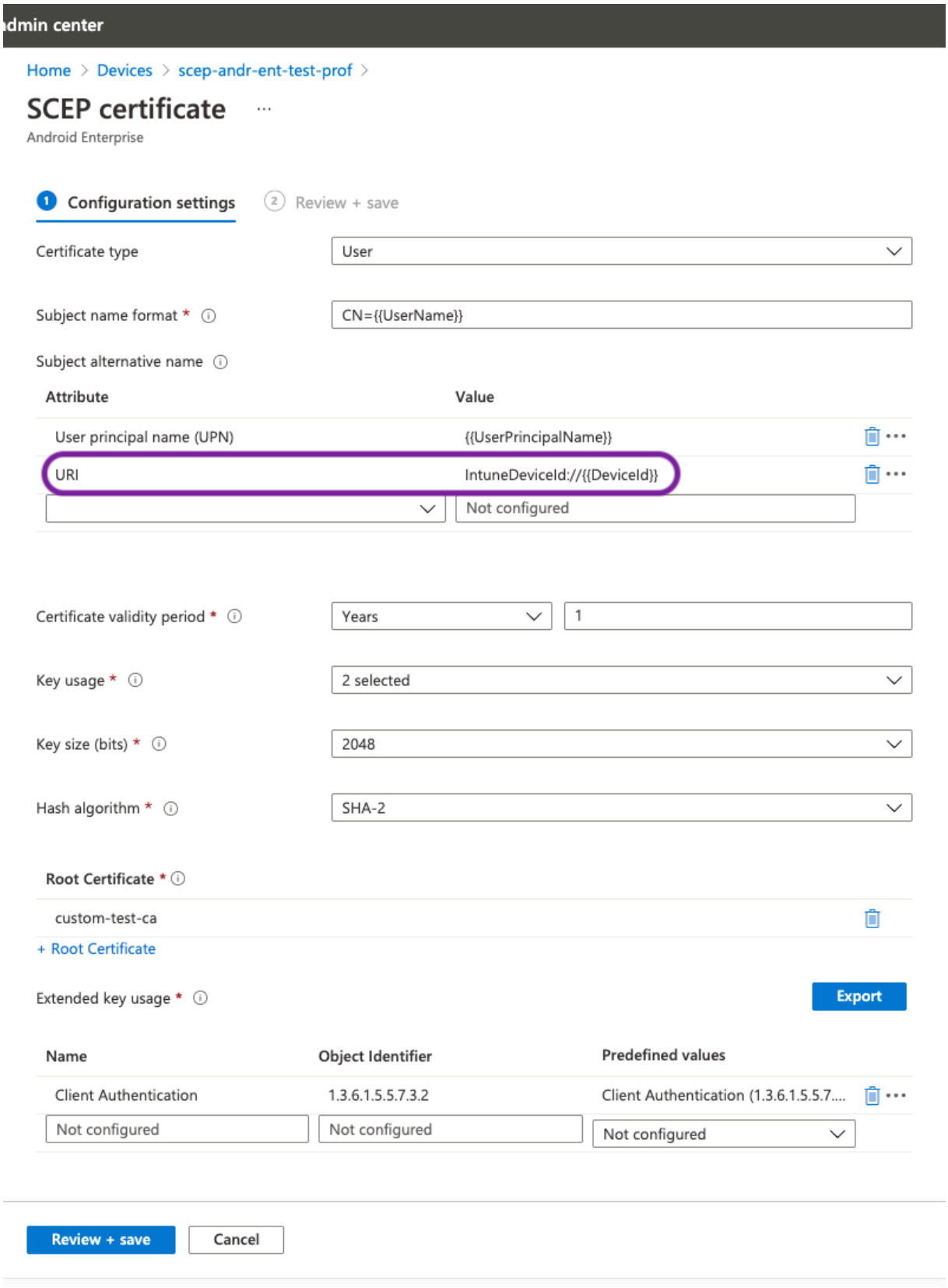
Intune NAC v2 API サポートの一環として、NetScaler アプライアンスがモバイルデバイスから有効な証明書を取得できるように、認証局ファイル（CA 証明書）をバインドする必要があります。Intune NAC v2 では、モバイルデバイスは CA 証明書の一部としてデバイス ID を送信します。ここでバインドされる CA 証明書は、エンドユーザーの iOS および Android デバイスにクライアント証明書を発行するために使用される証明書である必要があります。中間証明書がある場合は、その証明書もここでバインドする必要があります。

以下のサンプルコマンドを使用して CA 証明書をバインドできます。

```
bind ssl vserver intune_nac_check_443 -certkeyName clientca -CA -
    ocspCheck Optional
<!--NeedCopy-->
```

> 重要:
>
> - Intune NAC v2 API サポートは、NetScaler Gateway バージョン 13.1 ビルド 12.50 以降、および 13.0 ビルド 84.11 以降で利用できます。
> - VPN および認証仮想サーバーで`clientAuth`を [ENABLED] および`clientCert`を [OPTIONAL] に設定して、クライアント証明書ベースの認証を有効にする必要があります。Intune NAC チェックを必要としない他のエンドポイントが、クライアント証明書を提供しなくても同じ仮想サーバを介して認証できるように、`clientCert` パラメータは OPTIONAL に設定されます。Android デバイスと iOS デバイスはクライアント証明書を提供する必要があります。そうしないと、Intune NAC チェックは失敗します。
> - モバイルデバイスの Intune 経由でプロビジョニングされるクライアント証明書の、「ネットワークアクセスコントロール用の新しい Microsoft Intune サービス」ドキュメントで示されている URI タイプの SAN フィールドに Intune デバイス ID が含まれていることを確認する必要があります。詳しくは、https://techcommunity.microsoft.com/t5/intune-customer-success/new-microsoft-intune-service-for-network-access-control/ba-p/2544696を参照してください。
>   URI 値フィールドの形式は、次の図に示すものと同じである必要があります。また、Citrix SSO アプリ

はゲートウェイでの認証に同じ証明書を使用する必要があります。



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る	アプリごとに許可されるポリシーは 1 つだけです。
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、正しいテナント ID が使用されていることなどを確認する

NetScaler Gateway の問題

問題	解像度
Azure 上のゲートウェイアプリに対して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。manage.windowsazure.com ポータルを使用して、権限を追加できるかどうかを確認してください。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。
NetScaler Gateway は`login.microsoftonline.comandgraph.windows.net`に到達できません。	NS Shell 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-k https://login.microsoftonline.com。次に、NetScaler Gateway で DNS が構成されているかどうかを確認します。また、ファイアウォールの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 のゲートウェイ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 ステータスが完了と表示されない。	DNS 設定と Azure のゲートウェイ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。

NetScaler Gateway OAuth の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はダウンまたは到達不能です
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、シェルプロンプトに移動し、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「完了」と表示されます。

Intune 構成チェック

[**Citrix SSO** の基本 **iOS VPN** 構成] **>** [ネットワークアクセス制御（**NAC**）を有効にする] で、[同意する] チェックボックスをオンにします。そうでない場合、NAC チェックは機能しません。

Azure Portal での **NetScaler Gateway** アプリケーションの構成

April 1, 2024

次のセクションでは、Azure Portal で NetScaler Gateway アプリケーションを構成する手順を示します。

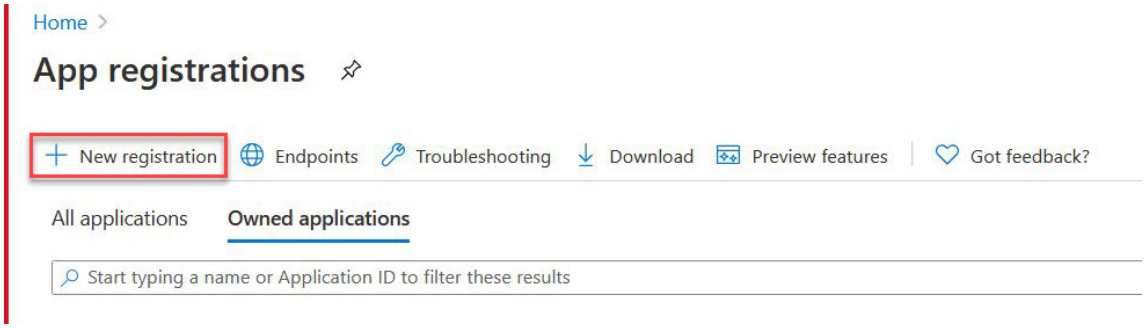
前提条件

- Azure グローバル管理者の認証情報
- Intune ライセンスが有効になっている
- Intune 統合の場合は、Azure Portal で NetScaler Gateway アプリケーションを作成する必要があります。
- NetScaler Gateway アプリケーションが作成されたら、次のアプリケーション固有の情報を使用して、NetScaler Gateway で OAuth ポリシーを構成します。
  - クライアント ID/アプリケーション ID
  - クライアントシークレット/アプリケーションキー
  - Azure テナント ID

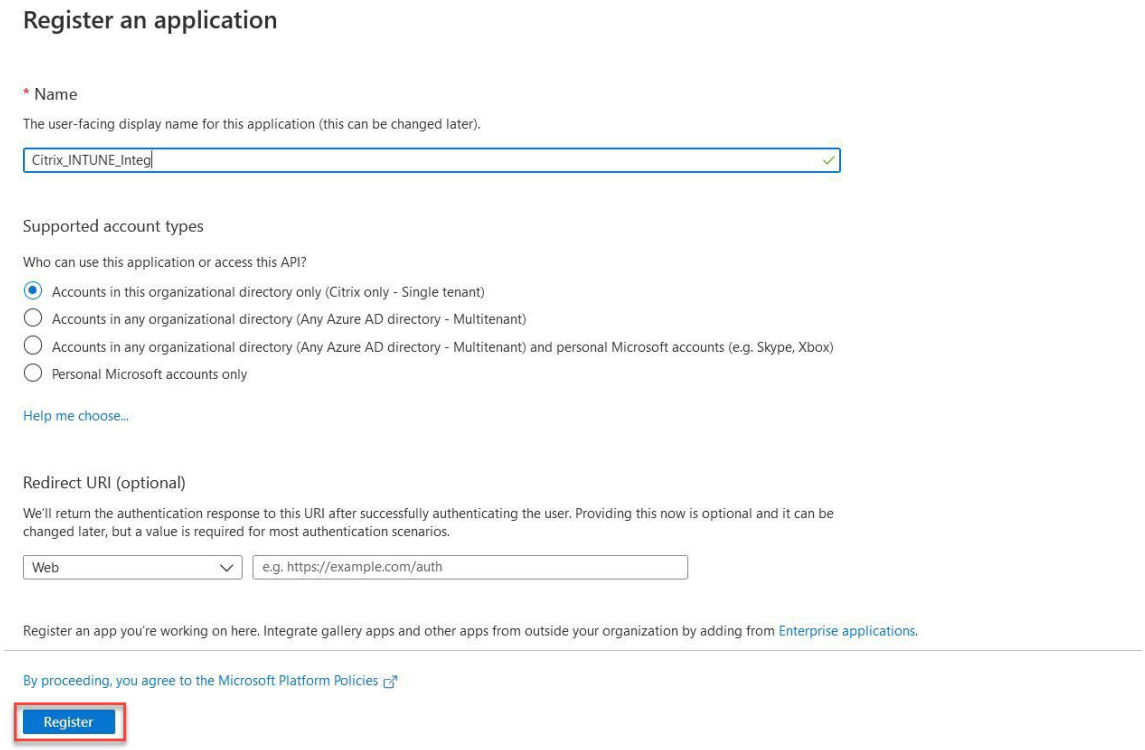
- NetScaler Gateway は、アプリクライアント ID とクライアントシークレットを使用して Azure と通信し、NAC コンプライアンスをチェックします。

Azure で NetScaler Gateway アプリを作成するには

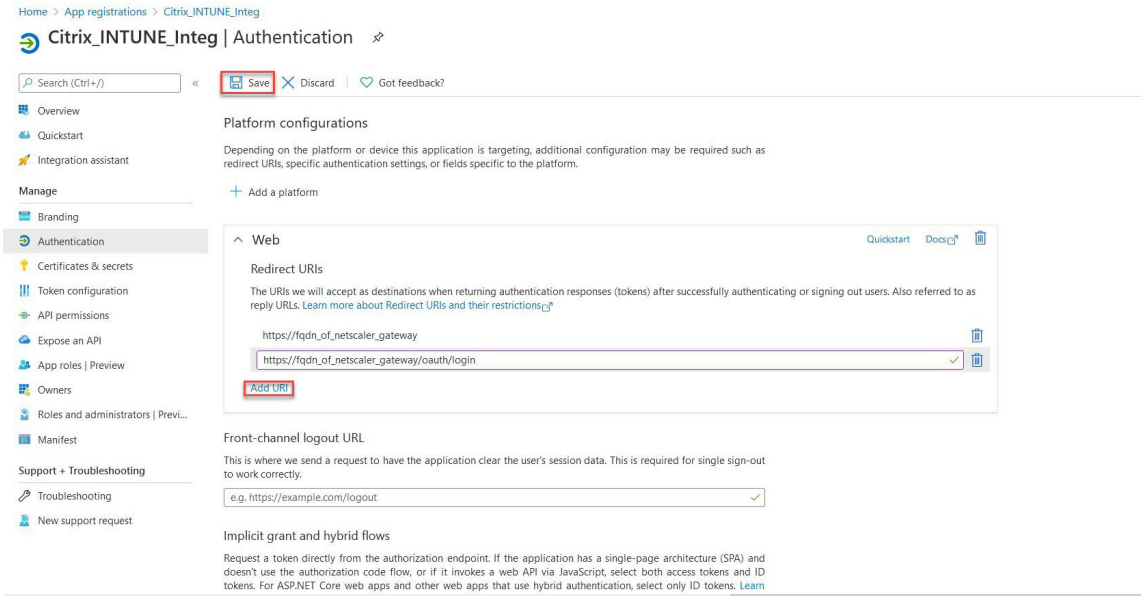
1. portal.azure.com にログインします
2. [**Azure Active Directory**] をクリックします。
3. [アプリの登録] をクリックし、[新規登録] をクリックします。



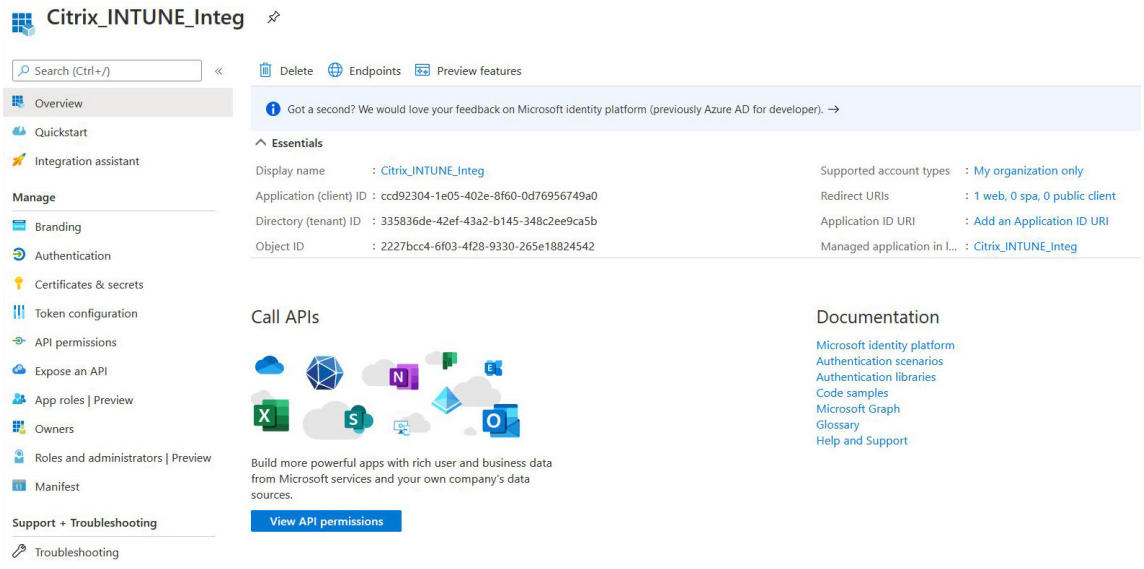
4. [アプリケーションの登録] ページで、アプリケーション名を入力し、[登録] をクリックします。



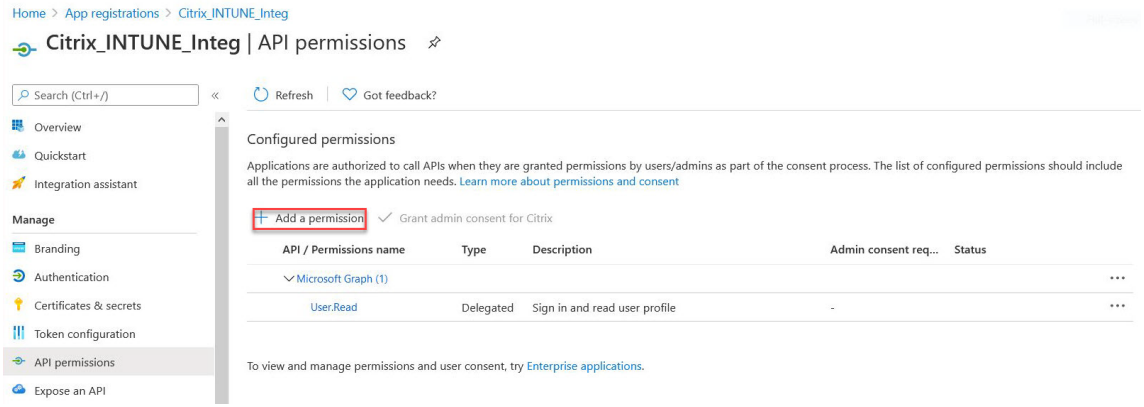
5. ［認証］に移動し、［**URI** の追加］をクリックし、NetScaler Gateway の FDQN を入力して、［保存］をクリックします。



6. [概要] ページに移動して、クライアント ID、テナント ID、およびオブジェクト ID を取得します。

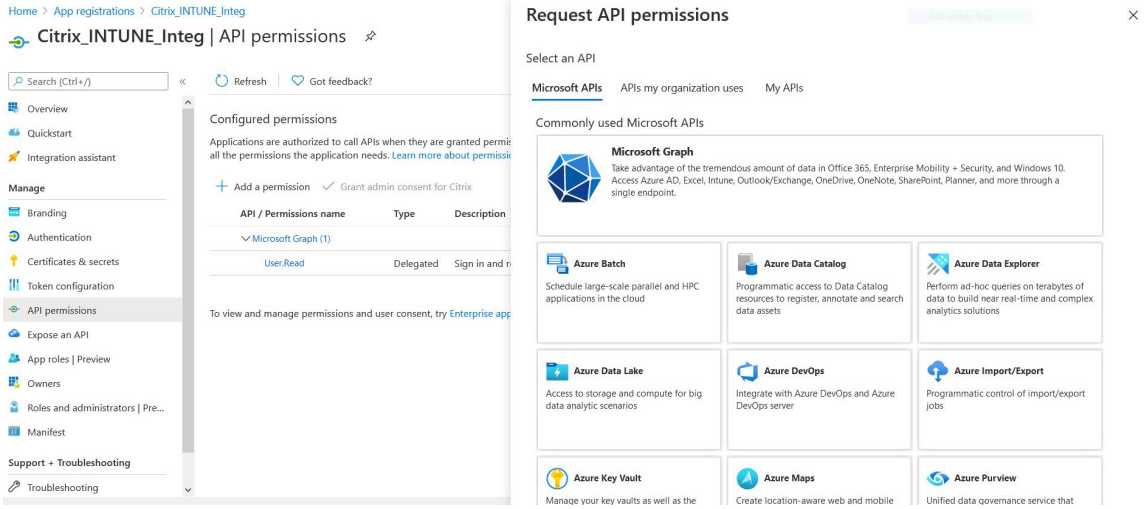


7. [**API** 権限] に移動し、[権限の追加] をクリックします。

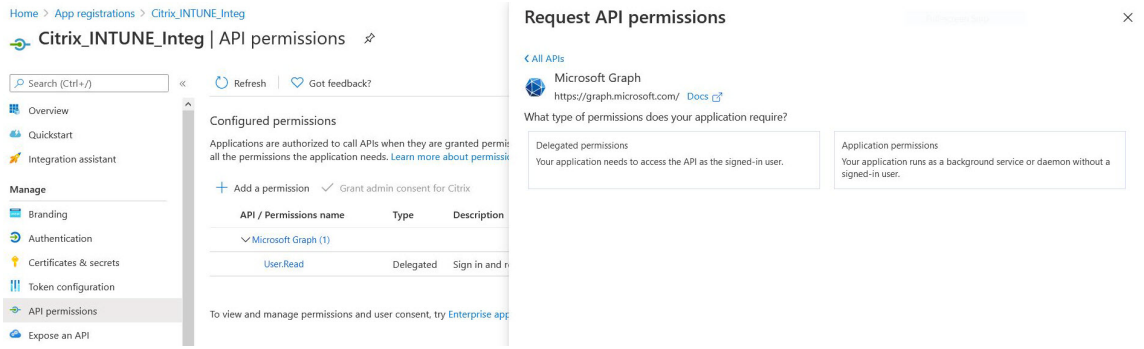


> 注:
>
> https://login.microsoftonline.com、https://graph.microsoft.com、またはhttps://graph.windows.netサービスエンドポイントを呼び出すすべての Azure AD アプリケーションでは、ゲートウェイが NAC API を呼び出すには、API 権限を割り当てる必要があります。利用可能な API 権限は次のとおりです。
>
> - Application.Read.All
> - Application.ReadWrite.All
> - application.ownedBy
> - Directory.Read.All
>
> 優先されるパーミッションは **Application.Read.All** です。
>
> 詳細については、以下を参照してください。https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040

8. [**Microsoft Graph**] タイルをクリックして、Microsoft Graph の API 権限を設定します。

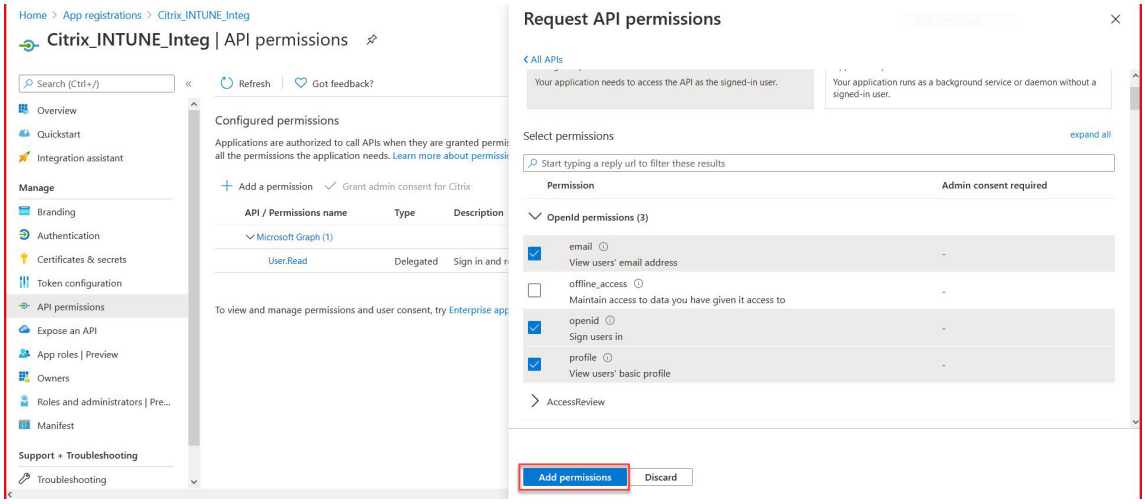


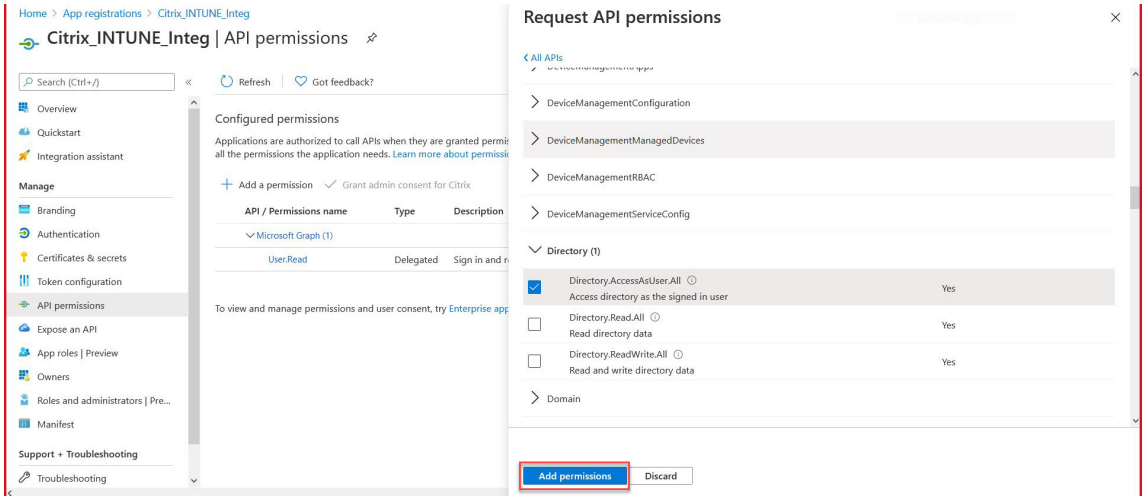
9. [委任されたアクセス許可] タイルをクリックします。

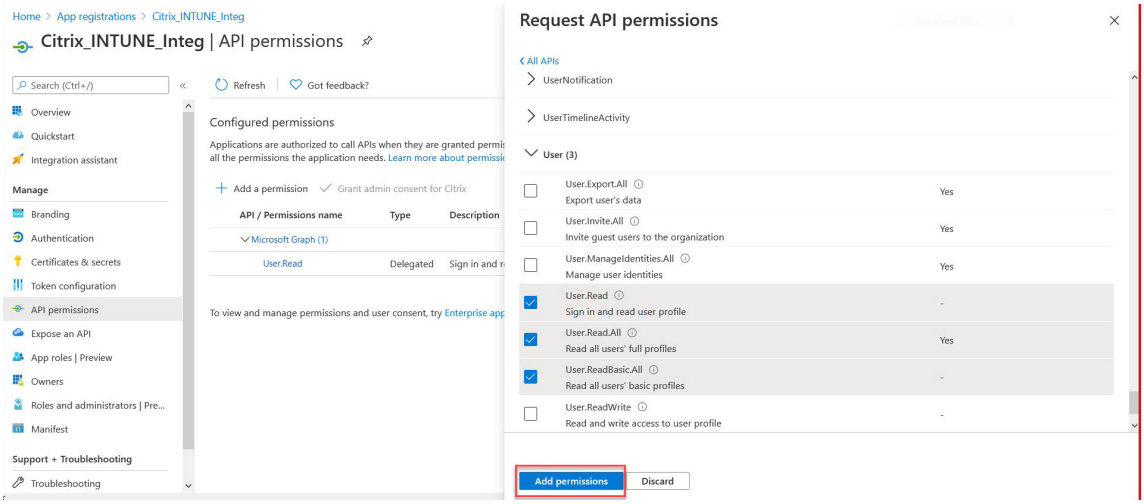


10. 次の権限を選択し、[権限の追加] をクリックします。

- メール
- openid
- Profile
- Directory.AccessAsUser.All
- User.Read
- User.Read.All
- User.ReadBasic.All







Intune NAC チェックのアクセス許可**:**

`https://login.microsoftonline.com`、`https://graph.microsoft.com`、`https://graph.windows.net` またはサービスエンドポイントを呼び出すすべての Azure AD アプリケーションでは、ゲートウェイが NAC API を呼び出せるように API 権限を割り当てる必要があります。利用可能な API 権限は次のとおりです。

- Application.Read.All
- Application.ReadWrite.All
- application.ownedBy
- Directory.Read.All

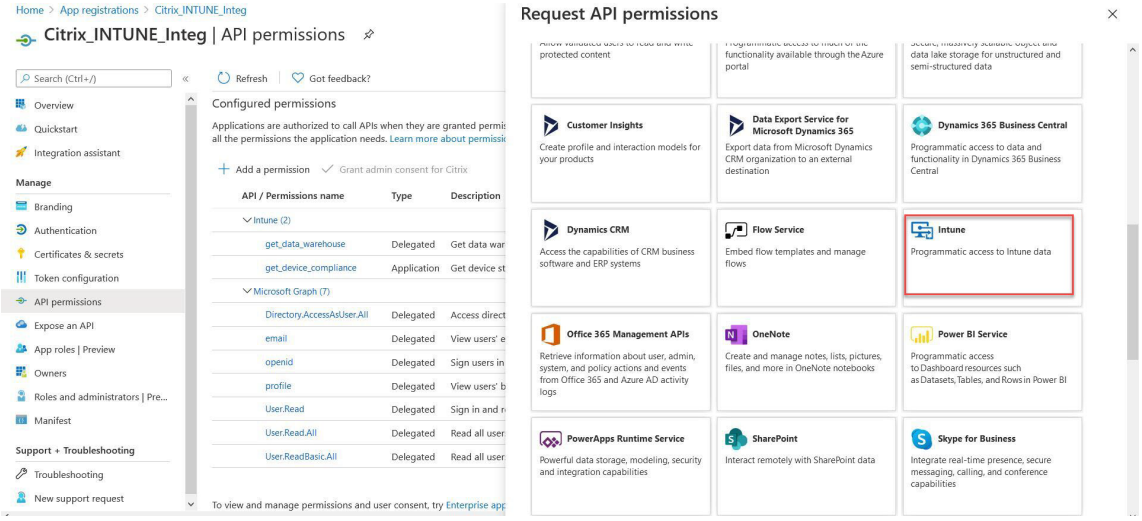
優先されるパーミッションは **Application.Read.All** です。

詳細については、https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040

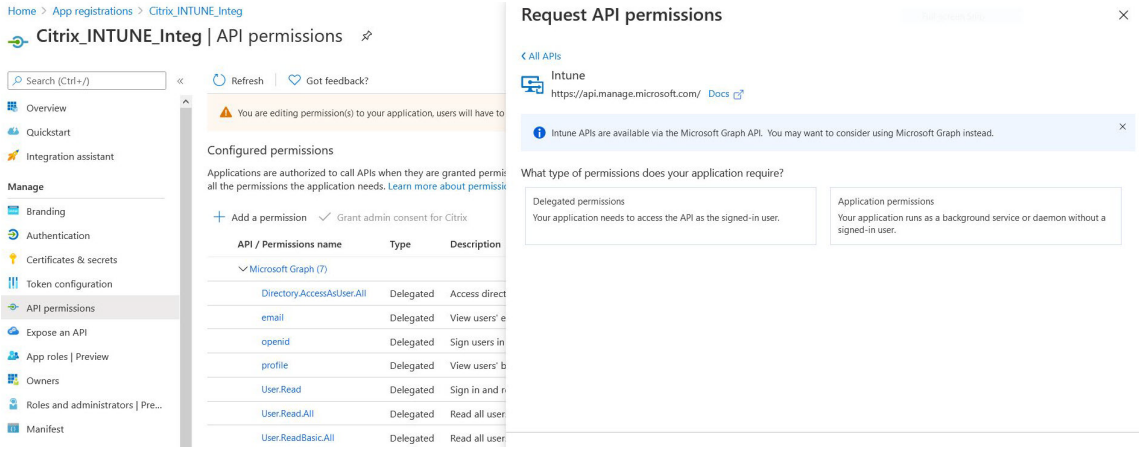
注**:**

お客様が NAC チェックに Intune アクションのみを使用している場合、必要な権限は Microsoft Graph の **Application.Read.All** だけです。

11. **Intune** タイルをクリックして、Intune の API パーミッションを設定します。



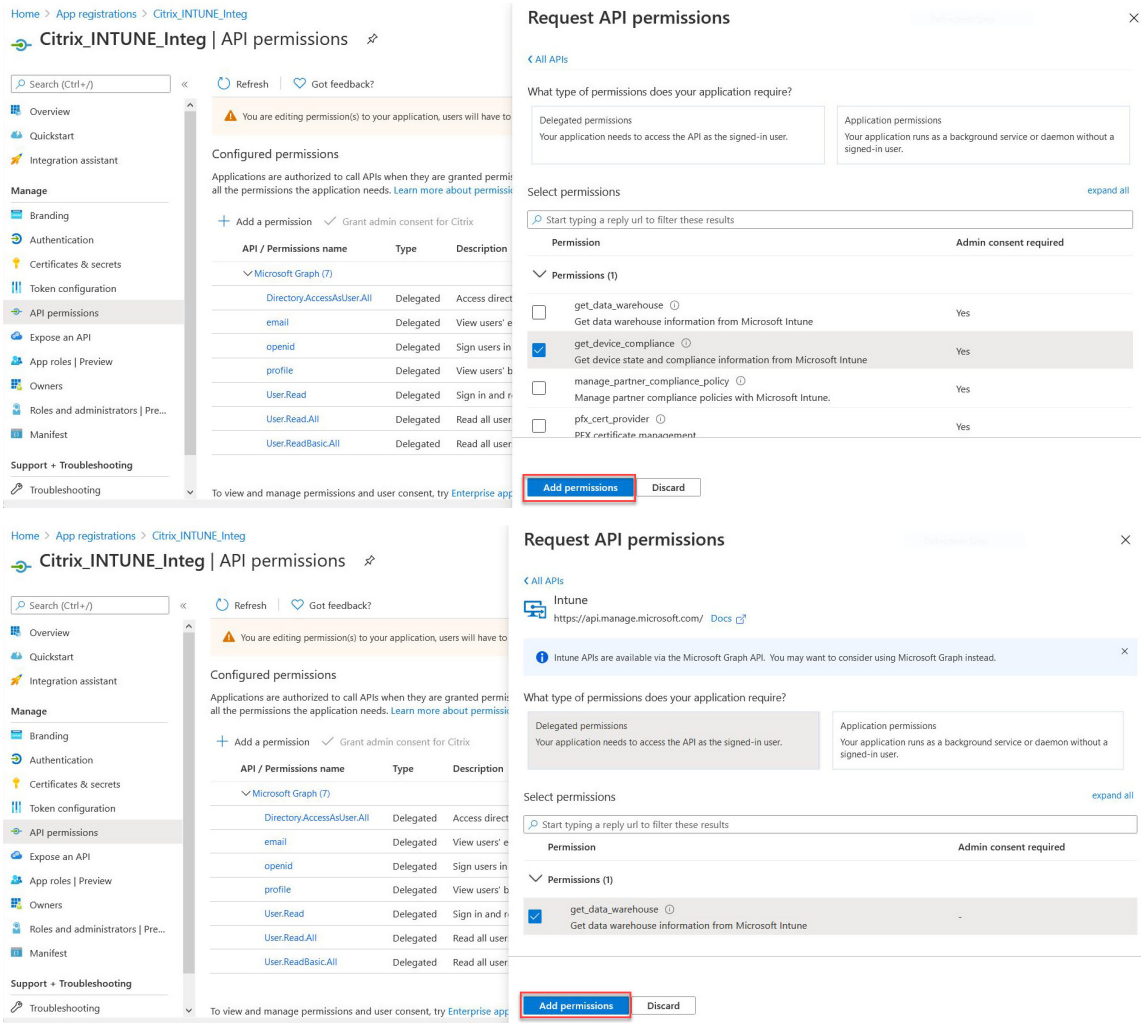
12. [アプリケーションのアクセス許可] タイルと [委任されたアクセス許可] タイルをクリックして、それぞれ Get_Device_Compliance と Get_Data_Warehouse のアクセス許可を追加します。



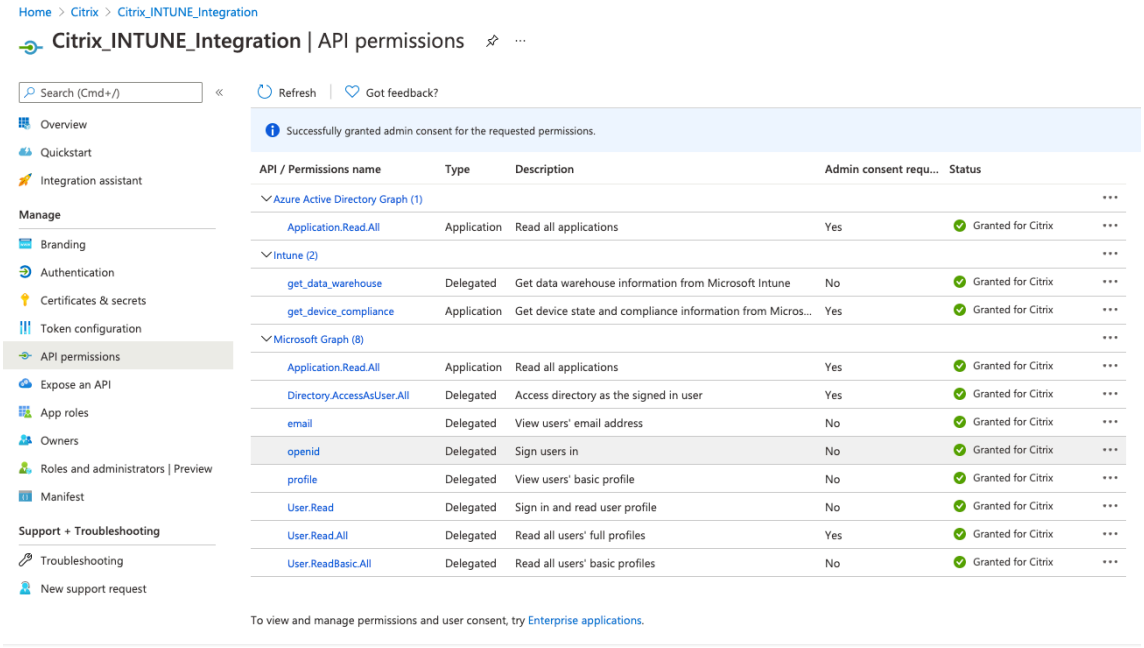
13. 次の権限を選択し、[権限の追加] をクリックします。

    - get_device_Compliance-アプリケーションのアクセス許可
    - Get_Data_Warehouse-委任されたアクセス許可

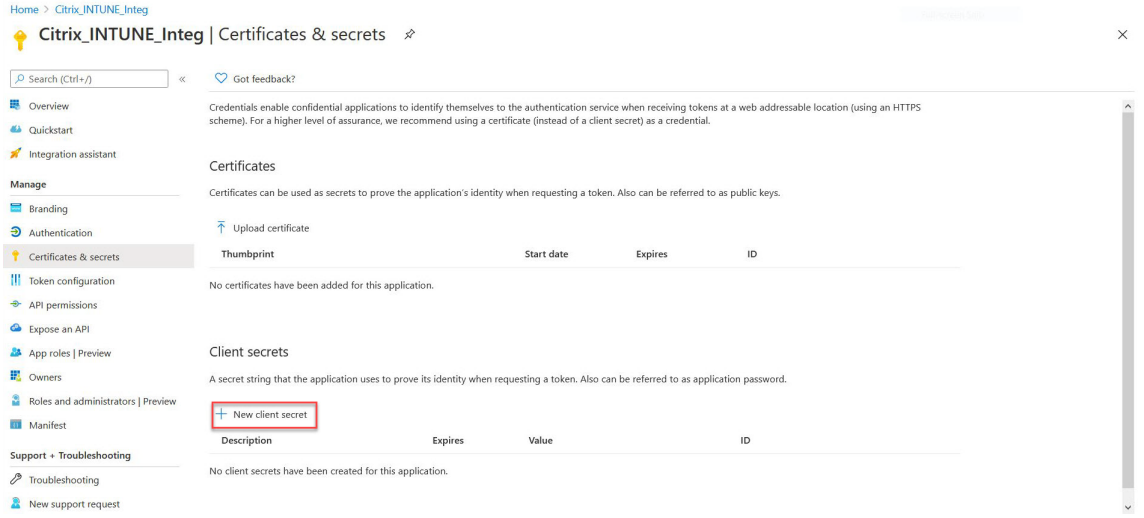
> 注:
>
> Intune NAC チェックでは、必要な権限は **get_device_Compliance** だけです。



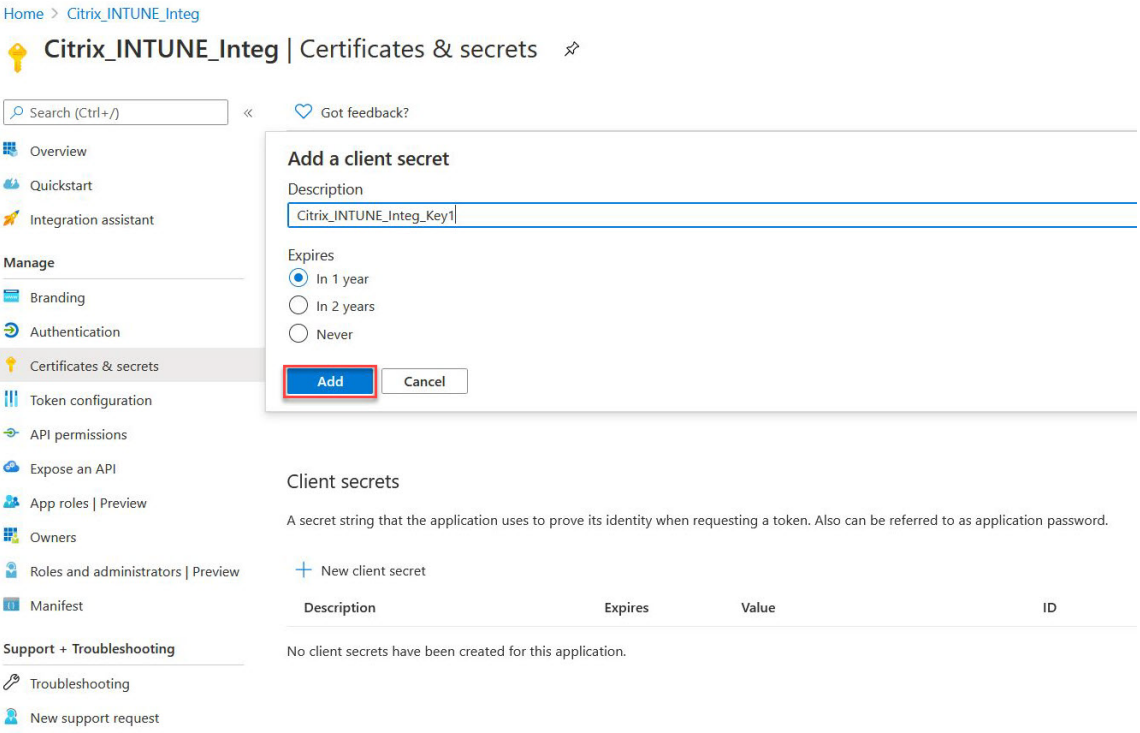
14. 次のページには、設定された API 権限が一覧表示されます。



15. [証明書とシークレット] に移動し、[新しいクライアントシークレット] をクリックします。

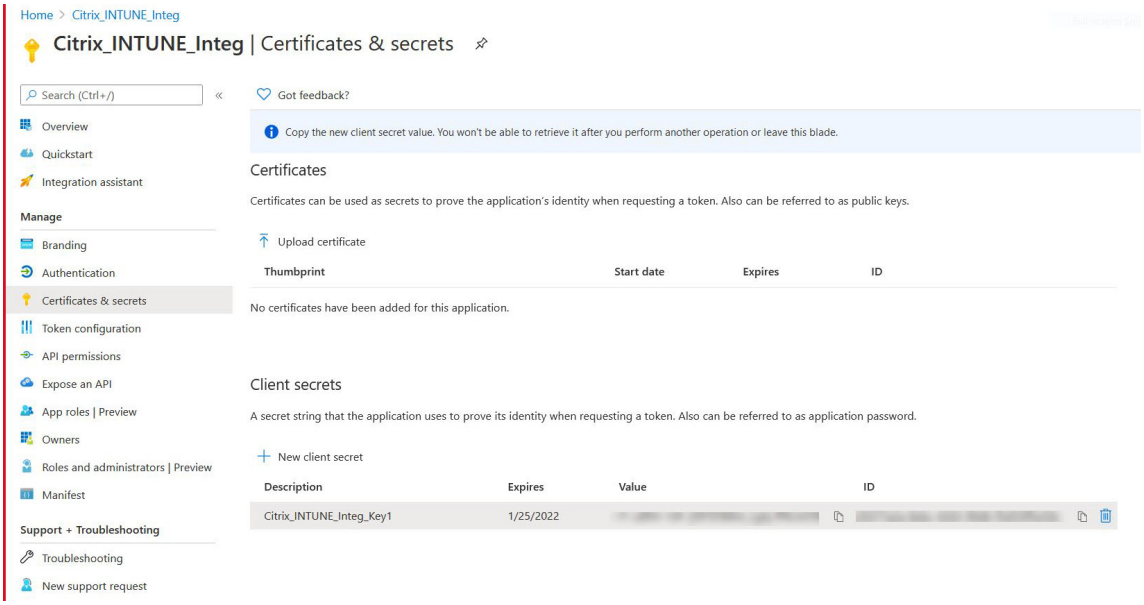


16. [クライアントシークレットの追加] ページで、説明を入力し、[有効期限] を選択して、[追加] をクリックします。



17. 次の画面は、設定されたクライアントシークレットを示しています。

> (注
>
>) クライアントシークレットは、生成時に一度だけ表示されます。表示されたクライアントシークレットをローカルにコピーします。Intune 用の NetScaler Gateway アプライアンスで OAuth アクションを構成するときに、新しく登録されたアプリに関連付けられたクライアント ID と同じクライアントシークレットを使用します。



Azure Portal のアプリケーション構成はこれで完了です。

Azure ADAL トークン認証について

February 1, 2024

以下は、一般的な NetScaler Gateway-Microsoft ADAL トークン認証のイベントのフローです。

1. iOS または Android でアプリを起動すると、アプリは Azure に接続します。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 NetScaler Gateway に提示されます。

3. NetScaler 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. 検証が成功すると、NetScaler 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 NetScaler Gateway 仮想サーバーの構成

April 1, 2024

Microsoft ADAL トークン認証を監視するように NetScaler 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 ウェブキー (JWK) を含むエンドポイントの URL。
- 対象者: アプリが ADAL トークンを送信する NetScaler ADC 仮想サーバーの FQDN。
- 発行者:AAD 発行者の名前。既定で値が設定されます。
- **tenantiID**: Azure ADAL 登録のテナント ID。
- クライアント **ID**: ADAL 登録の一部としてゲートウェイアプリに付与される一意の ID。
- クライアントシークレット:ADAL 登録の一部としてゲートウェイアプリに与えられるシークレットキー。
- **resourceURI**: リソース URI をキャプチャするためのオプションのパラメータです。構成されていない場合、NetScaler ADC は Azure 商用リソース URI を使用します。

コマンドラインインターフェイスを使用して、次の手順を実行します。

1. OAuth アクションを作成します。

```
add authentication OAuthAction <oauth-action-name> -OAuthType <
    INTUNE>  - clientid <clientID> -clientsecret <client-secret> -
    audience <audience name> -tenantid <tenantID> -issuer <issuer-
    name> -userNameField <upn> -certEndpoint <certEndpoint-name> -
    resourceURI <name of resource URI>
```



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

2. 新しく作成した OAuth アクション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>
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

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

5. AuthVs をログインスキーマでバインドします。

```
bind authentication vserver <auth-vs> -policy <oauth-pol> -
    priority 2 -gotoPriorityExpression END
<!--NeedCopy-->
```

6. 認証プロファイルを追加し、VPN 仮想サーバに割り当てます。

```
add authnprofile <nfactor-profile-name> -authnvsName <authvserver>
set vpn vserver <vserver-name> -authnprofile <nfactor-profile-name
    >
<!--NeedCopy-->
```

設定例

```
add authentication OAuthAction tmp-action -OAuthType INTUNE -clientid
    id 1204 -clientsecret a -audience "[http://hello](http://hello/)" -
    tenantid xxxx -issuer "[https://hello](https://hello/)" -
    userNameField upn -certEndpoint https://login.microsoftonline.com/
    common/discovery/v2.0/keys --resourceURI htpps://api.manage.
    microsoft.com

add authentication Policy oauth-intune-pol -rule true -action tmp-
    action
bind authentication vserver auth-vs-for-gw1-intune -policy oauth-pol -
    priority 2 -gotoPriorityExpression END

add authentication loginSchema oauth-loginschema -authenticationSchema
    "/nsconfig/loginschema/LoginSchema/OnlyOAuthToken.xml"

```



```
add authentication loginSchemaPolicy oauth-loginschema-pol -rule true -
    action oauth-loginschema `

bind authentication vserver auth-vs-for-gw1-intune -policy oauth-
    loginschema-pol -priority 2 -gotoPriorityExpression END

add authnprofile nfactor-prof-intune -authnvsName auth-vs-for-gw1-
    intune

set vpn vserver gw1-intune-authnprofile nfactor-prof-intune
<!--NeedCopy-->
```

Microsoft Endpoint Manager でマイクロ VPN を使用するように NetScaler Gateway をセットアップする

April 1, 2024

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、Citrix マイクロ VPN と Microsoft Endpoint Manager の統合を参照してください。

システム要件

- NetScaler Gateway バージョン
  - 13.1
  - 13.0
  - 12.1.50.x またはそれ以降
  - 12.0.59.x またはそれ以降

  NetScaler Gateway の最新バージョンは、NetScaler 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
- ファイアウォール規則
  - NetScaler Gateway サブネット IP から`*.manage.microsoft.com`、`https://login.microsoftonline.com`および`https://graph.windows.net`（ポート 443）への SSL トラフィックに対するファイアウォールルールを有効にする
  - NetScaler Gateway は、前述の URL を外部で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 のドキュメントを参照してください。
- エッジブラウザーアプリ**:** マイクロ VPN SDK は、iOS および Android 用の Microsoft Edge アプリと 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。
- **Citrix Endpoint Management** 資格: Microsoft Edge モバイルブラウザ（iOS および Android）でマイクロ VPN SDK を引き続きサポートするには、アクティブな Citrix Endpoint Management 資格が必要です。詳細については、営業、アカウント、またはパートナーの担当者にお問い合わせください。

Azure Active Directory (AAD) アプリケーションのアクセス許可を付与する

1. NetScaler Gateway が AAD ドメインで認証することを許可することを、Citrix マルチテナント AAD アプリケーションに同意します。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。

2. Citrix マルチテナント AAD アプリケーションに同意して、モバイルアプリケーションが NetScaler Gateway Micro 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 [ユーザーはアプリケーションを登録できます] 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 Portal の [**Azure 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 (
   テナント ID を追加) する必要があります。https://login.microsoftonline.com/%5Btenant_id%5D/adminconsent?client_id=9215b80e-186b-43a1-8aed-9902264a5af7

NetScaler Gateway をマイクロ **VPN** 用に構成する

Intune でマイクロ VPN を使用するには、NetScaler 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 NetScaler 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 NetScaler Gateway との間の認証を適切に行うために必要です。

スクリプトのダウンロード**:**.zip ファイルには、スクリプトの実装手順を含む 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、NetScaler 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 NetScaler のダウンロードページからダウンロードできます。

> 重要: NetScaler Gateway の構成が完了し、OAuth ステータスが COMPLETE 以外に表示される場合は、「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。

Microsoft Edge Browser の設定

1. https://endpoint.microsoft.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 Edge アプリを公開し、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）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）	Value	説明
–	–	–
MvpnGatewayAddress	`https://external.companyname.com`	NetScaler Gateway の外部 URL
MvpnNetworkAccess	mvpnNetworkAccessTunneledWebSSOor Unrestricted	mvpnNetworkAccessTunneledWebS
が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カンマ区切りリスト	オプションです。既定値は [空白] です
TunnelExcludeDomains	このクライアントプロパティを使用して、除外されるドメインのデフォルトリストを上書きします。デフォルト =`app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream.launchdarkly.com,crashlytics.com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com,hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com`

> 注**:** Web SSO は設定で Secure Browse の名前です。動作は同じです。

- **mvpnNetworkAccess** -mvpnNetworkAccessTunneledWebSSO を使用すると、NetScaler Gateway（トンネルウェブ SSO とも呼ばれる）を介した HTTP/HTTPS リダイレクトが可能になります。ゲートウェイは 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。ウェブ SSO を使用するには、このポリシーを **mvpnNetworkAccessTunneledWebSSO** に設定します。フルトンネルリダイレクト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のままにするには、[制限なし] を使用します。
- **mvpnExcludeDomains** -NetScaler 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名またはドメイン名のカンマ区切りのリスト。NetScaler Gateway 構成のスプリット DNS 設定で

ドメインまたはホストが選択される場合がありますが、ホストまたはドメイン名は除外されます。

> 注:
>
> - このポリシーは、**MVPN** ネットワークアクセスのトンネリング **WebSSO** 接続にのみ適用されます。MvpnNetworkAccessが **Unrestricted** の場合、このポリシーは無視されます。
> - このポリシーは、NetScaler Gateway がリバース分割トンネリング用に設定されているトンネル Web SSO モードにのみ適用されます。

- トンネル除外ドメイン -デフォルトでは、MDX は一部のサービスエンドポイントをマイクロ VPN トンネリングから除外します。モバイルアプリの SDK とアプリは、これらのサービスエンドポイントをさまざまな機能に使用します。たとえば、サービスエンドポイントには、Google Analytics、Citrix Cloud サービス、Active Directory サービスなど、エンタープライズネットワーク経由のルーティングを必要としないサービスが含まれます。このクライアントプロパティを使用して、除外ドメインのデフォルトリストを上書きします。

  このグローバルクライアントポリシーを構成するには、Microsoft Endpoint Management コンソールで [設定] **>** [クライアントプロパティ] に移動し、カスタムキー **TUNNEL_EXCLUDE_DOMAINS** を追加して値を設定します。

  値: デフォルトのリストをトンネリングから除外するドメインに置き換えるには、ドメインサフィックスのリストをカンマで区切って入力します。すべてのドメインをトンネルに含めるには、「none」と入力します。デフォルトは次のとおりです:

  ```
  app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis
  -test.citrix.com,clientstream.launchdarkly.com,crashlytics.com
  ,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com,
  hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf
  .citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.
  google-analytics.com,stream.launchdarkly.com
  ```

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る	アプリごとに許可されるポリシーは 1 つだけです。
アプリをラップすると、「アプリのパッケージ化に失敗しました」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、次の表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

問題	解像度
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 が正しいことなどを確認します。

アプリのパッケージ化に失敗しました。エラーメッセージ**:**

アプリのパッケージ化に失敗しました*。com.microsoft.intune.mam.appPackager.utils.appPackageException:* このアプリにはすでに *MAM SDK* が統合されています。
com.microsoft.intune.mam.appPackager.appPackager.appPackagerApp (appPackager.java: 113)
com.microsoft.intune.mam.appPackager.Packager.PackagerMain.mainInternal (packagerMain.java: 198)
com.microsoft.intune.mam.appPackager.Packager.PackagerMAIN.main (packagerMain.MAIN .java:56)
アプリケーションはラッピングできません。

NetScaler Gateway の問題

問題	解像度
Azure 上のゲートウェイアプリに対して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。manage.windowsazure.com ポータルを使用して、権限を追加できるかどうかを確認してください。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。
NetScaler Gateway は`login.microsoftonline.com and graph.windows.net`に到達できません。	NS Shell 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-k https://login.microsoftonline.com。次に、NetScaler Gateway で DNS が構成されているかどうかを確認します。また、ファイアウォールの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 のゲートウェイ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 のゲートウェイ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。

NetScaler Gateway OAuth の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はダウンまたは到達不能です
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。この設定を検証するには、shell に移動して 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「完了」と表示されます。

Azure AD グラフの拡張サポート

April 1, 2024

Azure AD Graph は廃止されたため、新しいアプリケーションをトリガーする顧客は、Azure AD Graph で使用可能だった以前の権限を使用できません。ただし、既存のアプリケーションを使用していて、Azure AD Graph の古い権限をしばらく使用したいお客様は、ゲートウェイアプライアンスでいくつかの構成変更を行うことで引き続き使用できます。この構成は、NetScaler Gateway リリース 13.1-27.xx 以降でサポートされています。

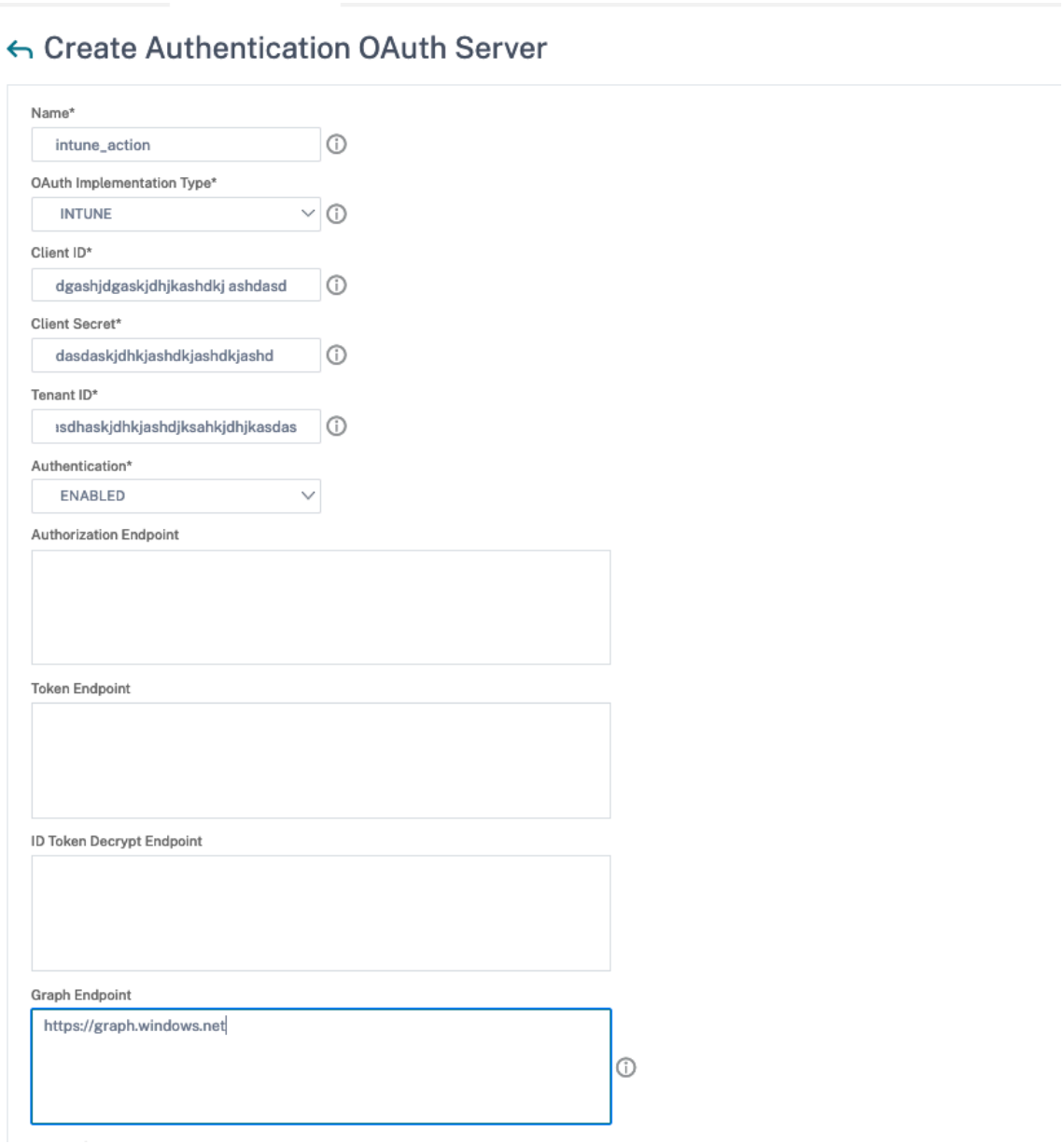
NetScaler Gateway アプライアンスで次の構成変更を行います。

1. コマンドプロンプトで、次のコマンドを実行します。

```
shell nsapimgr_wr.sh -ys call=” ns_intune_enable_old_endpoints”
<!--NeedCopy-->
```

2. 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 **>** 詳細ポリシー **>** アクション **>** **OAUTH** アクションに移動します。

   a) 既存の OAuth サーバーを選択します。
   b) ［詳細］クリックします。
   c) グラフエンドポイントで、URL が図に表示されているものと同じであることを確認します。



HDX Enlightened Data Transport サポート

February 1, 2024

NetScaler Gateway の Enlightened Data Transport（EDT）サポートにより、Citrix WorkCitrix Workspace アプリを実行しているユーザーに、仮想デスクトップの高精細なセッション内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。詳細については、DTLS プロトコルのサポートを参照してください。

EDT 対応の NetScaler Gateway は、LAN と WAN の両方の状態で優れたユーザーエクスペリエンスを提供します。EDT を使用すると、一方から他方へのローミング時に管理設定やユーザー設定は必要ありません。この利点は、パケット損失が中程度の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通常、代替案と遅れます。

Enlightened Data Transport サポートを使用する場合

April 1, 2024

次のシナリオは、EDT が有効な NetScaler Gateway の使用を示しています。

- 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望んでいます。
- 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低下する Wi-Fi およびセルラーネットワーク上で、リッチな仮想アプリケーションおよびデスクトップユーザーエクスペリエンスを望んでいます。

EDT を使用する際は、以下の点に留意すべきである。

- 仮想サーバレベルの 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 IPv6 はサポートされていません。
- アプライアンスは、Receiver と VDA 間の EDT トラフィックのダブルホップ機能用に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。Intel 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 がサポートされています。

EDT および HDX Insight をサポートするように NetScaler Gateway を構成

April 1, 2024

ゲートウェイを通過する 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。リアルタイムと履歴の両方の可視性データの可用性により、NetScaler ADM は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
NetScaler Gateway	はい

シナリオ	EDT サポート
高可用性（HA）を備えた NetScaler Gateway	はい
高可用性（HA）最適化機能を備えた NetScaler Gateway	はい
Unified Gateway を搭載した NetScaler ADC	はい
GSLB を搭載した NetScaler Gateway	はい
NetScaler Gateway とクラスター	はい
Citrix Workspace アプリから NetScaler Gateway への DTLS 暗号化	はい
NetScaler Gateway のデュアル Secure Ticket Authority（STA）	はい
NetScaler Gateway ICA セッションタイムアウト	はい
NetScaler Gateway マルチストリーム ICA	いいえ
NetScaler Gateway セッション画面の保持性（ポート 2598）	はい
NetScaler Gateway ダブルホップ	はい
NetScaler ADC から VDA への DTLS 暗号化	はい
HDX Insight	はい
IPv6 モードの NetScaler Gateway	いいえ
NetScaler Gateway SOCKS (ポート 1494)	いいえ
NetScaler ピュア LAN プロキシ（注記を参照）	いいえ

> 注:
>
> NetScaler LAN プロキシが LAN ユーザーモードまたはトランスペアレントモードで構成されている場合、EDT はサポートされません。ただし、TCP はサポートされています。詳しくは、次のトピックを参照してください:
>
> - アウトバウンド ICA プロキシの構成
> - SOCKS を使用した NetScaler による LAN ユーザー向けの HDX Insight 分析の収集

Enlightened Data Transport をサポートするように **NetScaler Gateway** を構成する

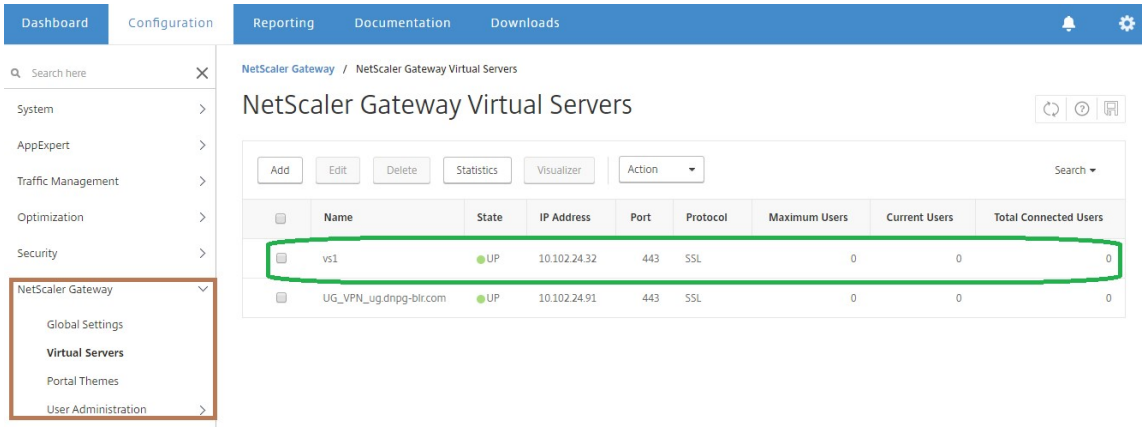
Enlightened Data Transport (EDT) を使用する場合、EDT によって使用される UDP 接続を暗号化するには、データグラムトランスポート層セキュリティ (DTLS) を有効にする必要があります。DTLS パラメータは、ゲートウェ

イ VPN 仮想サーバレベルで有効にする必要があります。また、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を暗号化するには、Citrix Virtual Apps and Desktops コンポーネントを正しくアップグレードして構成する必要があります。

> 注：仮想サーバーが DTLS 接続を受信するには、NetScaler 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 NetScaler Gateway と互換性を持つための前提条件です。

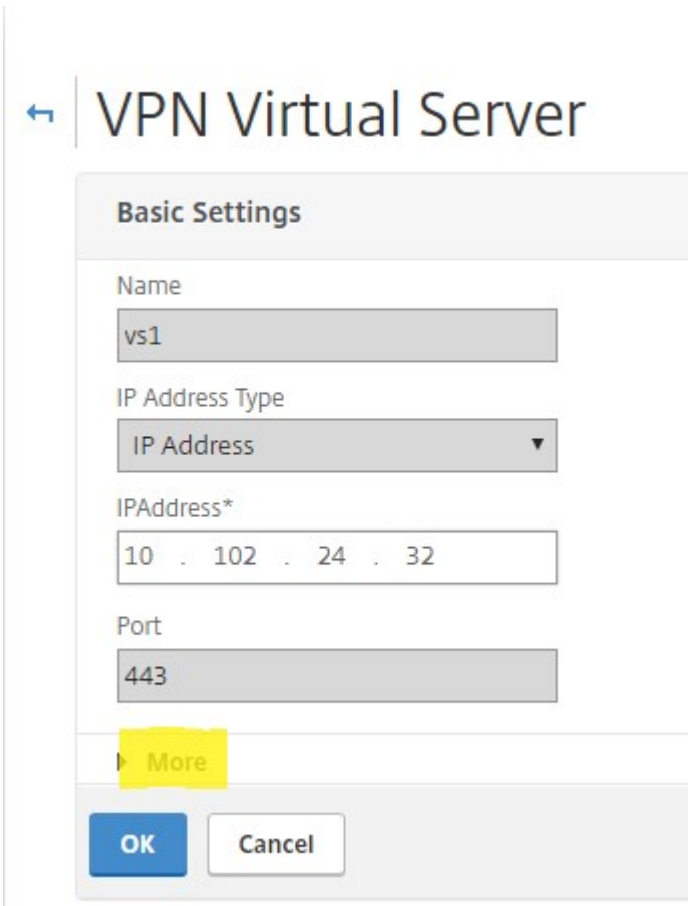
GUI を使用して **EDT** をサポートするように **NetScaler Gateway** を構成するには

1. NetScaler 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. NetScaler GUI の［構成］タブで、［**NetScaler Gateway**］を展開し、［仮想サーバー］を選択します。

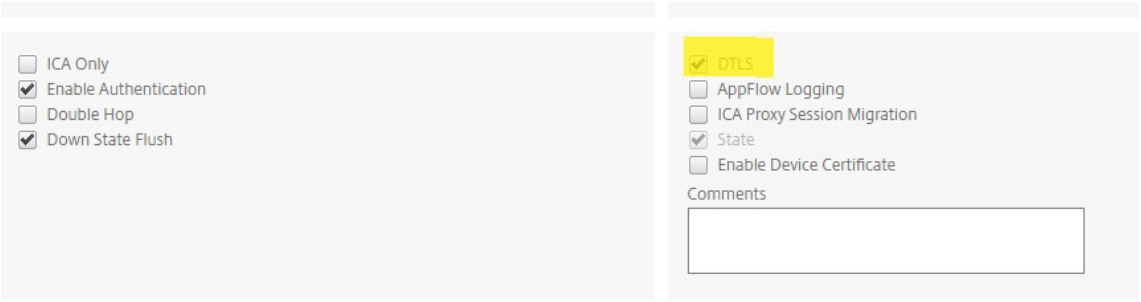


3. [編集] をクリックして VPN 仮想サーバーの基本設定を表示し、DTLS 設定の状態を確認します。

4. その他の設定オプションを表示するには、[詳細] 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、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 **NetScaler Gateway** を構成するには

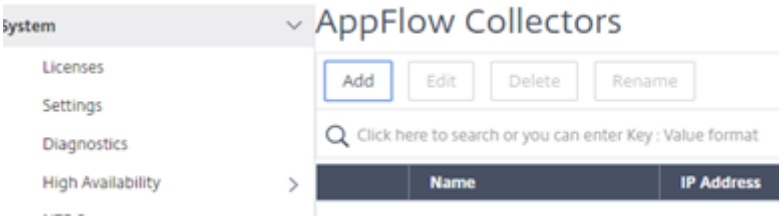
```
set vpn vserver vs1 -DTLS ON
```

HDX Insight をサポートするように **NetScaler Gateway** を構成する

HDX Insight は、NetScaler 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 トラフィックのエンドツーエンドの可視性を提供します。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、パフォーマンスの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 **NetScaler Gateway** を構成するには

1. [構成] タブで、[システム**] > [AppFlow] > [**コレクタ] に移動し、[追加] をクリックします。



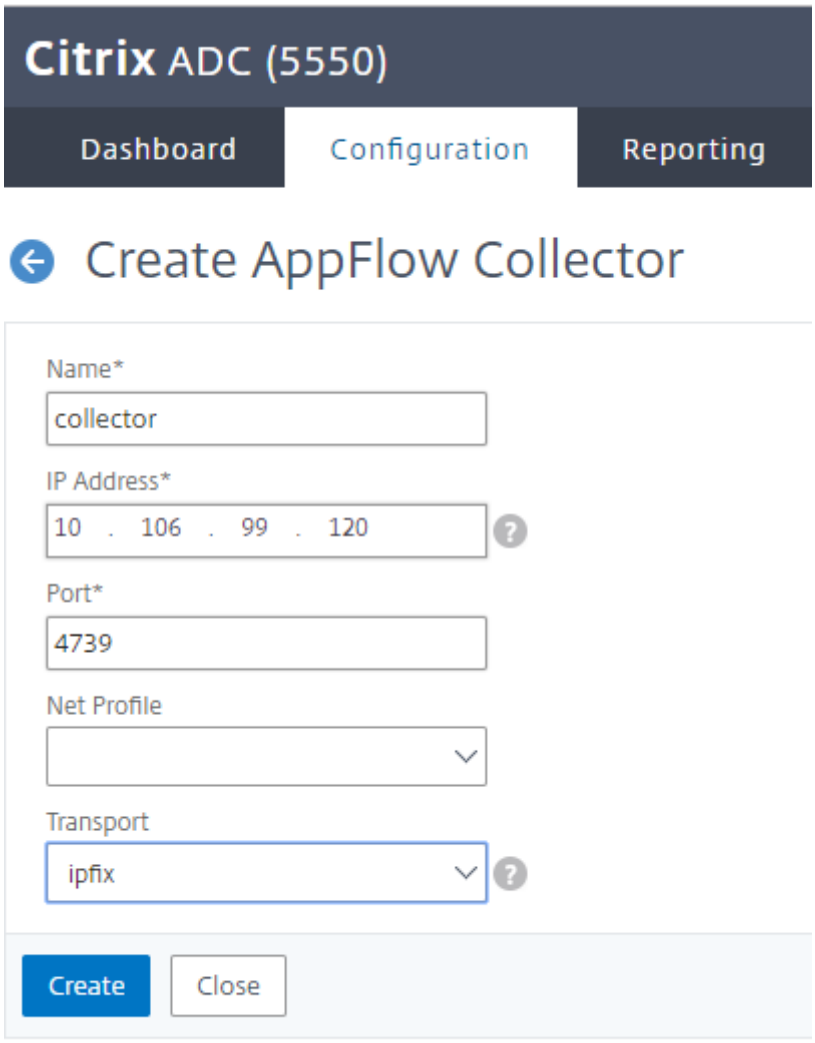
2. [**AppFlow** コレクタの作成] ページで、次のフィールドに入力し、[作成] をクリックします。
   Name —コレクタの名前

   IP アドレス：コレクタの IPv4 アドレス

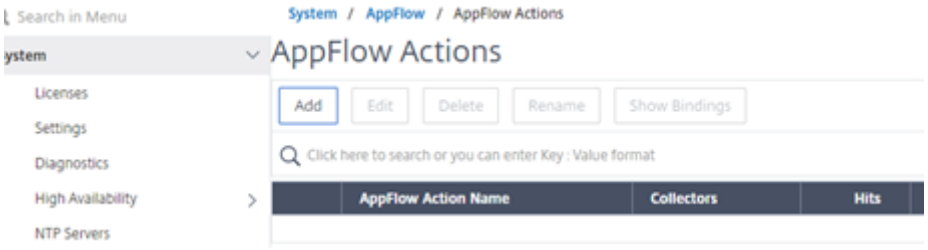
   Port：コレクタがリッスンするポート

   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。このパラメーターを設定しない場合、NetScaler IP（NSIP）アドレスがソース 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。

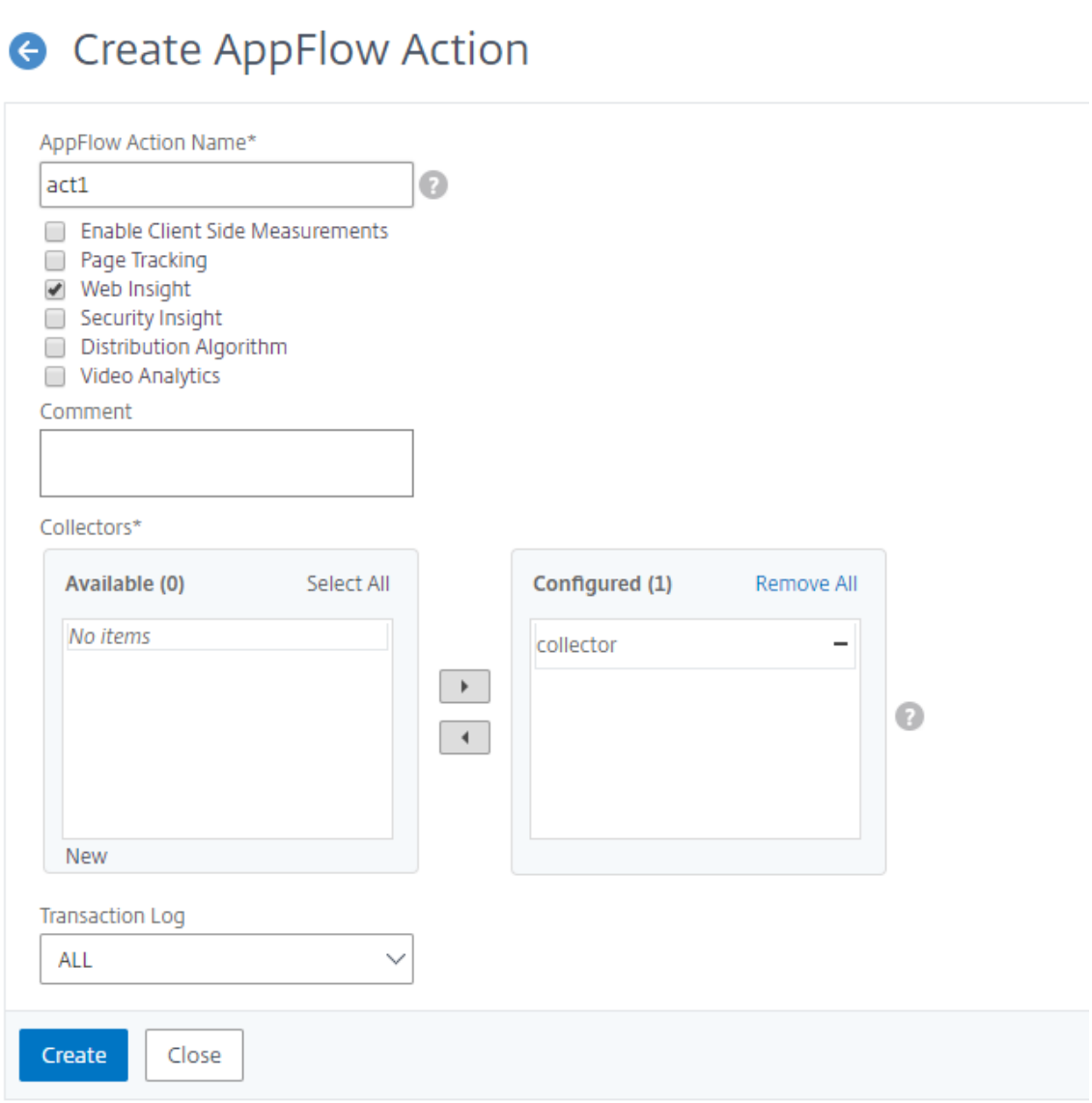


4. [**AppFlow** アクションの作成] ページで、次のフィールドに入力し、[作成] をクリックします。
   AppFlow アクション名—アクションの名前

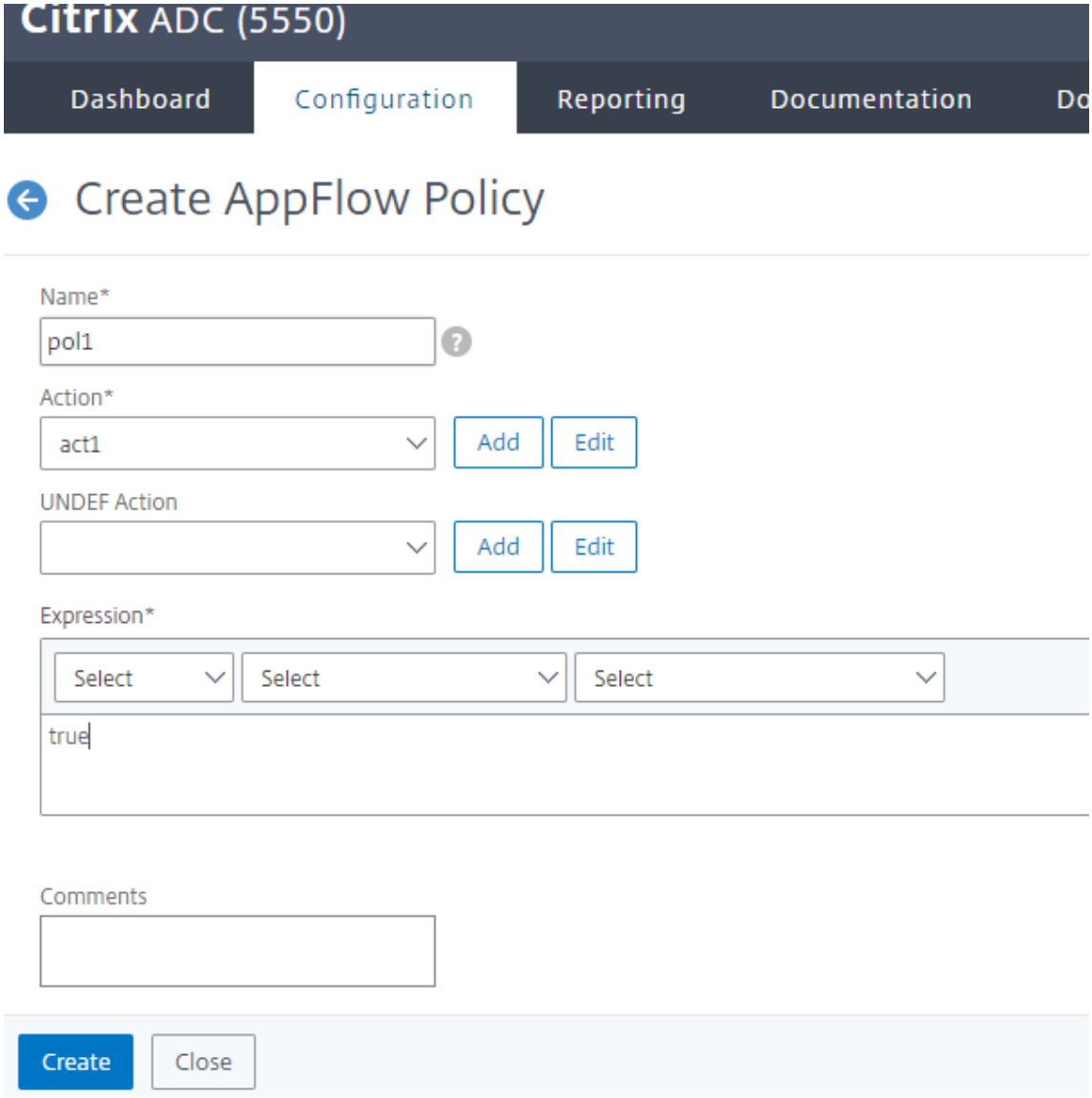
   コメント—アクションに関するコメント

   「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] —ログに記録す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。

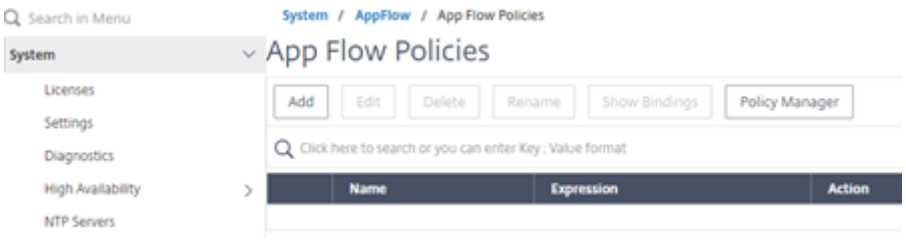
   [Name]：ポリシーの名前。

   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られる 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。ブール式でなければなりません。

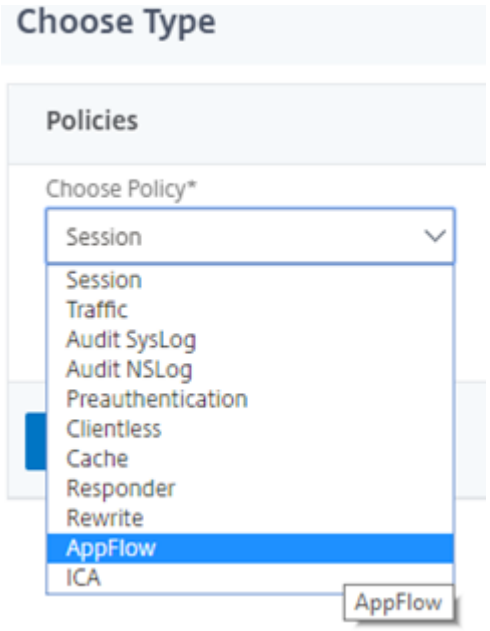
   コメント—このポリシーに関するコメント。



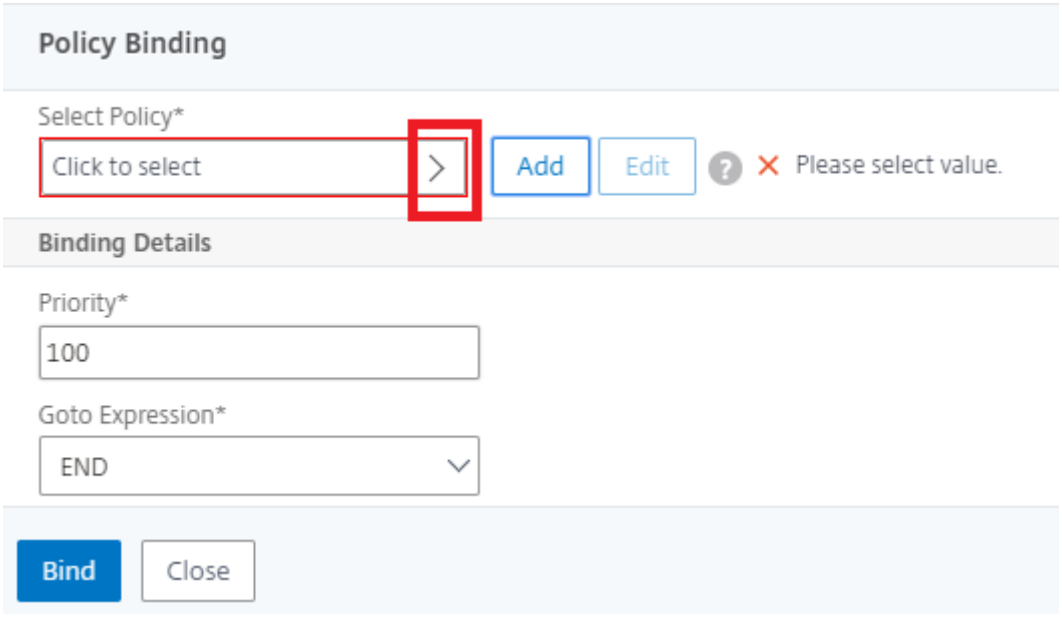
7. [**NetScaler Gateway**] **>** [仮想サーバー] に移動し、仮想サーバーを選択して [編集] をクリックします。

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。

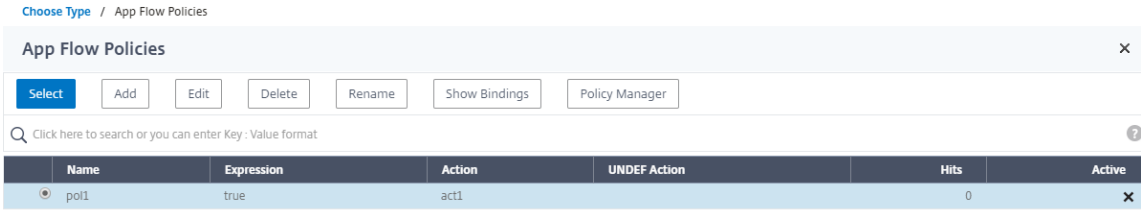
9. **[**タイプの選択**]** 画面の [ポリシーの選択] ドロップダウンメニューで、[**AppFlow**] を選択します。[タイプの選択] ドロップダウンメニューで、[要求] または [**ICA** 要求] を選択し、[続行] をクリックします。



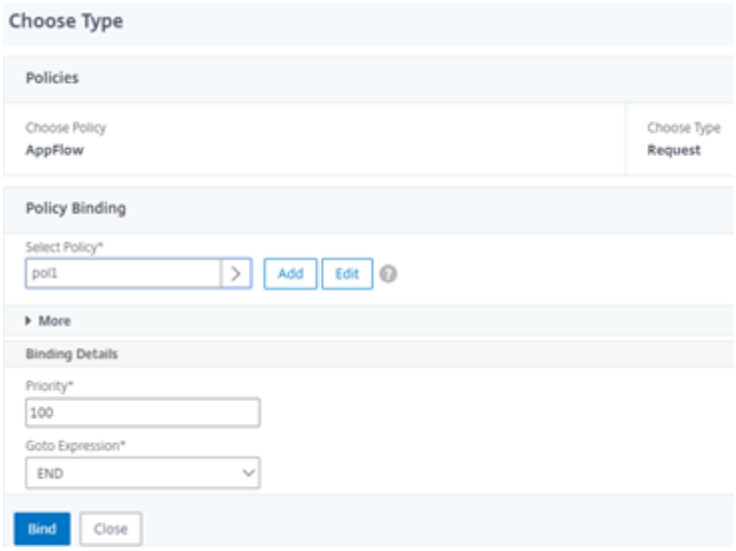
10. [ポリシーの選択] で強調表示された矢印をクリックします。



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 **HDX Insight** サポート用に **NetScaler Gateway** 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>
```



```
add appflow action act1 <action_name>
add appflow policy <policy_name> true <action_name>
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

NetScaler ADC アプライアンスでは、NSAP HDX 以外のセッションに対して 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入力します:

```
set ica parameter HDXInsightNonNSAP (YES | NO )
<!--NeedCopy-->
```

デフォルトでは、非 NSAP セッションの HDX Insight は有効になっています。

NetScaler Gateway を介した EDT の PMTUD 検出と DF ビット伝播

April 1, 2024

リリース 13.1 ビルド 17.x 以降、NetScaler Gateway アプライアンスは、EDT パスの最大伝送ユニット検出 (PMTUD) に対する DF ビット強制をサポートします。パス MTU 検出は、セッションの確立時に最大伝送単位 (MTU) を動的に決定するのに役立ちます。DF ビット強制により、パフォーマンスの低下やセッションの確立の失敗につながる可能性がある EDT フラグメンテーションが防止されます。

以前のリリースでは、NetScaler Gateway は EDT パス MTUD をサポートしていましたが、DF ビットの強制はサポートしていませんでした。

詳細については、「EDT MTU 検出」を参照してください。

CLI を使用して PMTUD サポートを有効にする

コマンドプロンプトで次を入力します:

```
set ica parameter [-EnableSRonHAFailover ( YES | NO )] [-
    HDXInsightNonNSAP ( YES | NO )] [-EDTPmtudDF ( ENABLED | DISABLED )]
     [-EDTPmtudDFTimeout <positive_integer>] [-L7LatencyFrequency <
    positive_integer>]
<!--NeedCopy-->
```

例:

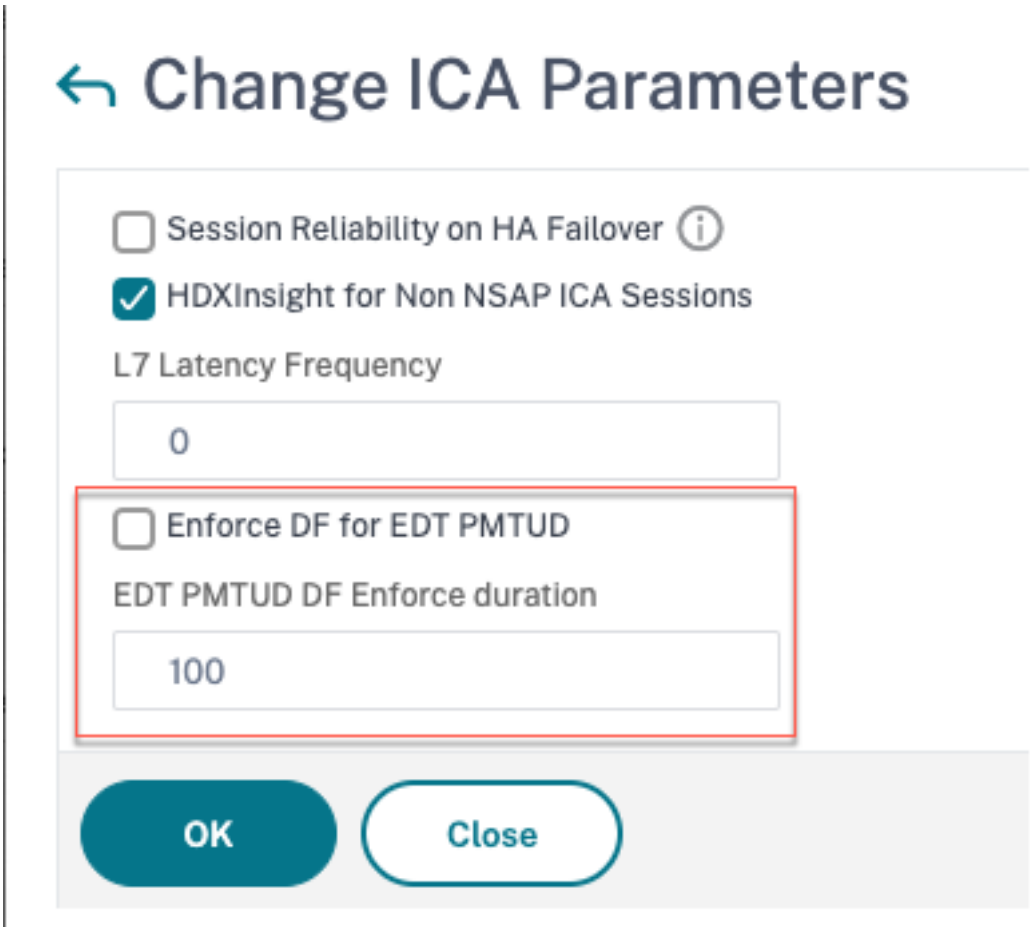

```
set ica parameter -EnableSRonHAFailover YES -EDTPmtudDF ENABLED -
    EDTPmtudDFTimeout 100
<!--NeedCopy-->
```

> 注:
>
> リリース 13.1 ビルド 42.x 以降では、EdTPmTuddf パラメータはデフォルトで有効になっています。以前は、このオプションはデフォルトで無効になっていました。

GUI を使用して PMTUD サポートを有効にする

1. [システム] > [設定] > [ICA パラメータの変更] に移動します。
2. [**EDT PMTUD DF** 強制期間] に、PMTUD DF 強制のタイムアウトを秒単位で入力します。

> 注:
>
> リリース 13.1 ビルド 42.x 以降では、**EDT PMTUD** に **DF** を強制するオプションがデフォルトで有効になっています。以前は、このオプションはデフォルトで無効になっていました。



L7 遅延しきい値処理

April 1, 2024

HDX Insight の L7 遅延しきい値処理機能は、アプリケーションレベルでエンドツーエンドのネットワーク遅延の問題を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 レイテンシーしきい値処理機能は、ライブレイテンシーモニタリング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を超えた場合に通知を HDX Insight に送信します。

以前は、クライアント側とサーバー側の平均 L7 遅延値は、60 秒ごとに HDX Insight に送信されていました。この間隔内に見られるスパイクはすべて平均化されているため、検出されませんでした。また、これらのスパイクを検出するためのライブレイテンシーモニタリングはありませんでした。

L7 レイテンシは L4 レイテンシとどう違うのですか

ネットワークの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は TCP レイヤーから計算され、ICA トラフィックの解析を必要としません。したがって、これらは比較的入手しやすく、CPU 負荷も少なくなります。ただし、L4 レイテンシの主な欠点は、エンドツーエンドのレイテンシ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 NetScaler ADC から TCP プロキシへのレイテンシーのみ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 レイテンシは ICA トラフィックの解析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、中間プロキシによってレイテンシ値が不完全になることはありません。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。

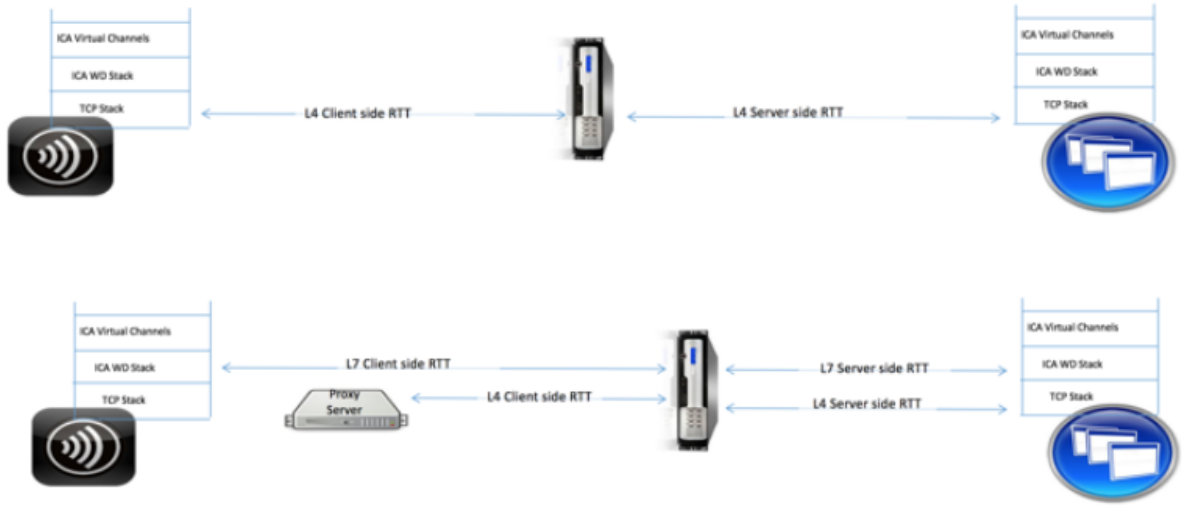


Fig 2. Deployment with TCP Proxies

ICA RTT と L7 のレイテンシー計算の違い

ICA RTT は、Citrix Workspace アプリから Virtual Delivery Agent（VDA）への合計ラウンドトリップ時間を表します。L7 レイテンシは、クライアント側とサーバー側のレイテンシに関する詳細な詳細を提供します。L7 クライアントの待ち時間は、Citrix Workspace アプリと NetScaler Gateway の間の遅延です。L7 サーバーの遅延は、NetScaler Gateway と VDA の間の遅延です。

> 注：サーバーのサーバー側の L7 遅延計算は、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。このパラメーターを有効にすると、設定した条件が満たされたときに通知が HDX Insight に送信されます。

  デフォルト値: 無効

- **latencyThresholdFactor**：しきい値を超えたため、HDX Insight に通知を送信する必要があると判断するために、アクティブなレイテンシーが最小観測レイテンシよりも大きくなければならない係数。

  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た後、HDX Insight に通知を送信するためにアプライアンスが待機する時間（秒）。

  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、アプライアンスが後続の通知を HDX Insight に送信する時間間隔（秒）。

  デフォルト値:20

  最小値:1

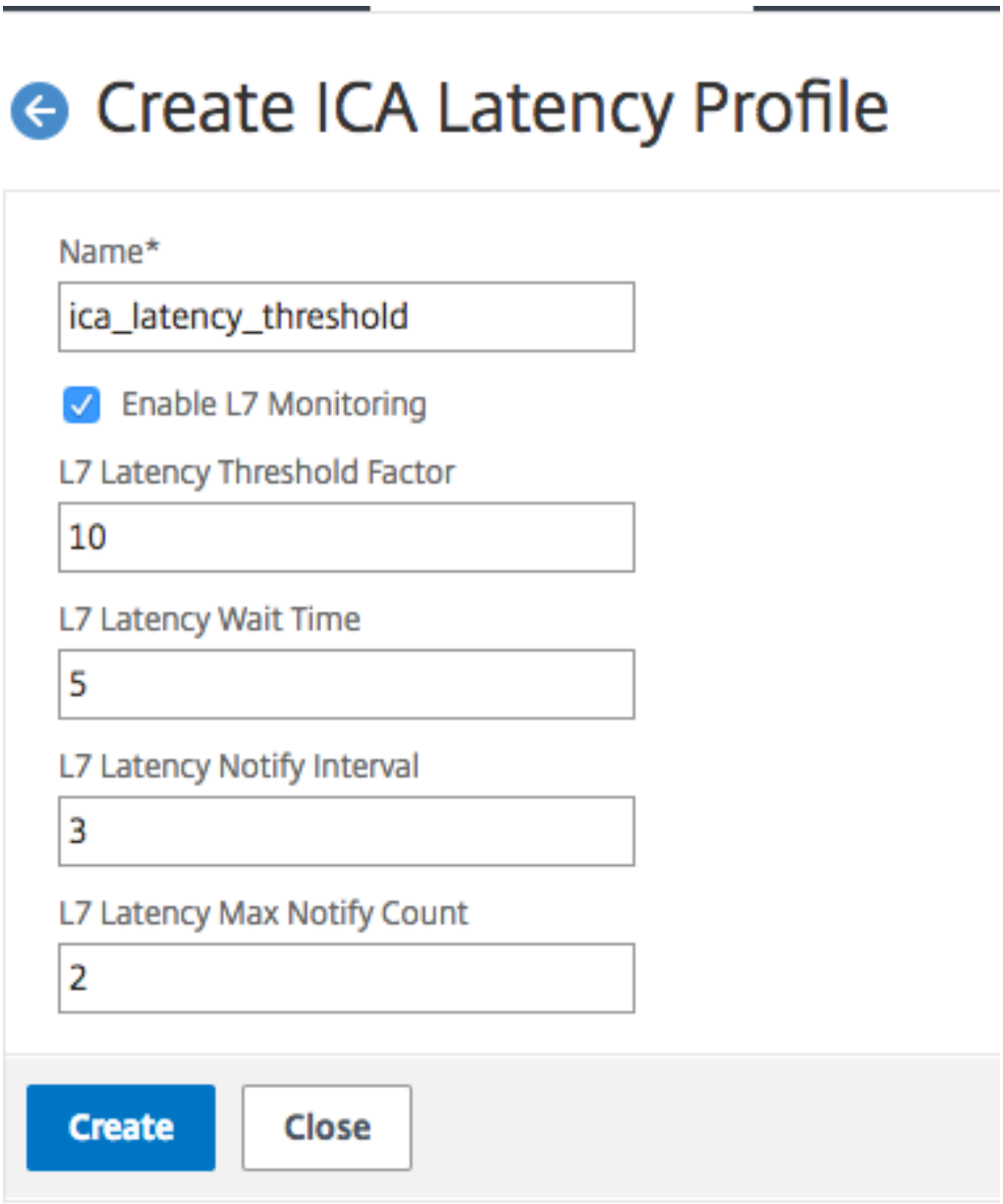
  最大値:65535

- **latencyMaxNotifyCount**：レイテンシーがしきい値を上回る間隔内に HDX Insight 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** 遅延プロファイル] タブを選択し、[追加] をクリックします。
3. **[ICA** 遅延プロファイルの作成] ページで、次の手順を実行します。



- [**L7** 遅延モニタリング] 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、HDX Insight に通知を送信するために、アクティブなレイテンシーが観測された最小レイテンシを超える必要がある値を入力します。
- [**L7 Latency Wait**Time］に、しきい値を超えた後に HDX Insight 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後続の通知を HDX Insight に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 HDX Insight に送信できる通知の最大数を入力します。
  注**:** L7 遅延の最大通知カウントは、しきい値を超えると適用され、アクティブな遅延がしきい値を下回

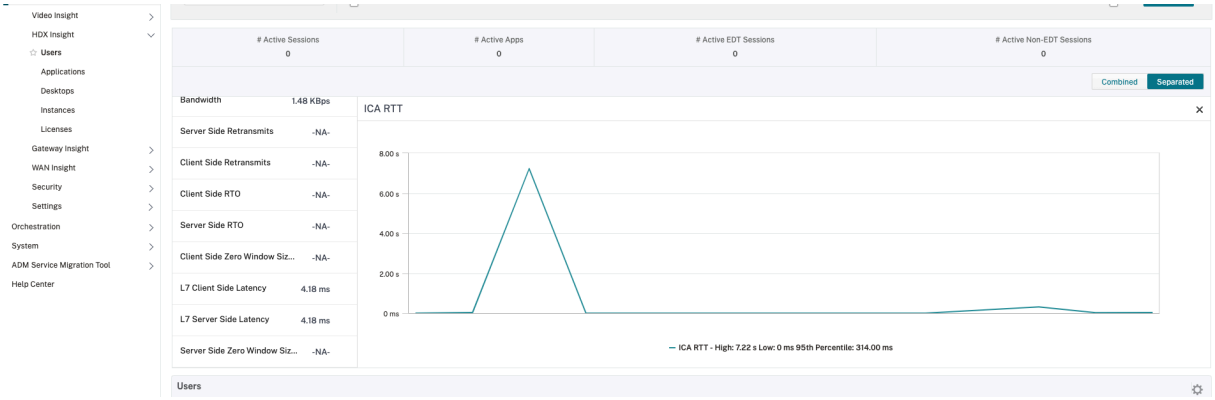
るとリセットされます。これらの通知の周期性は、通知間隔によって制御されます。

4. [**Create**] をクリックします。

> 重要:
>
> L7 遅延しきい値パラメーターを構成したら、HDX Insight を構成する必要があります。詳しくは、「HDX Insight をサポートするように NetScaler Gateway を構成する」を参照してください。

NetScaler ADM で **L7** レイテンシーパラメーターを表示する

NetScaler ADM で L7 レイテンシーパラメーターを表示するには、[分析] **> [HDX Insight] > [**アプリケーション] または [分析] **> [HDX Insight] > [**ユーザー] に移動します。

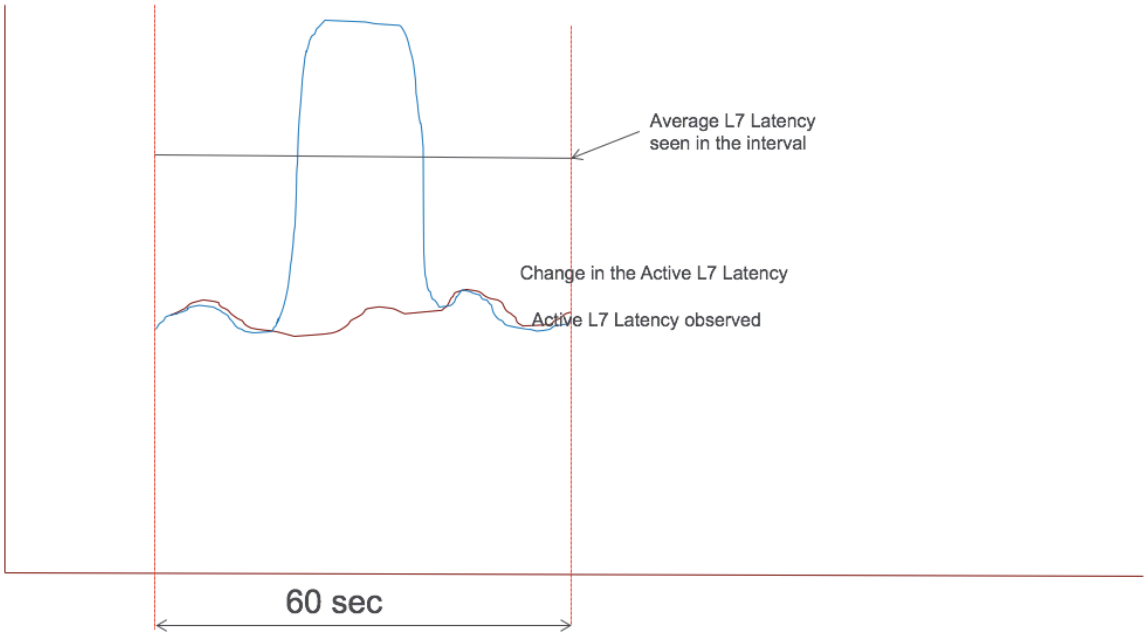


L7 レイテンシ測定モデルと **L7** レイテンシしきい値レポートモデル

L7 レイテンシー測定モデル

L7 レイテンシ測定モジュールでは、クライアント側とサーバー側の平均 L7 レイテンシー値が 60 秒ごとに HDX Insight に送信されます。その結果、この間隔内に見られるスパイクは平均化されるため、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モニタリング機能はありません。

次の図は、L7 レイテンシー測定モデルのサンプルを示しています。

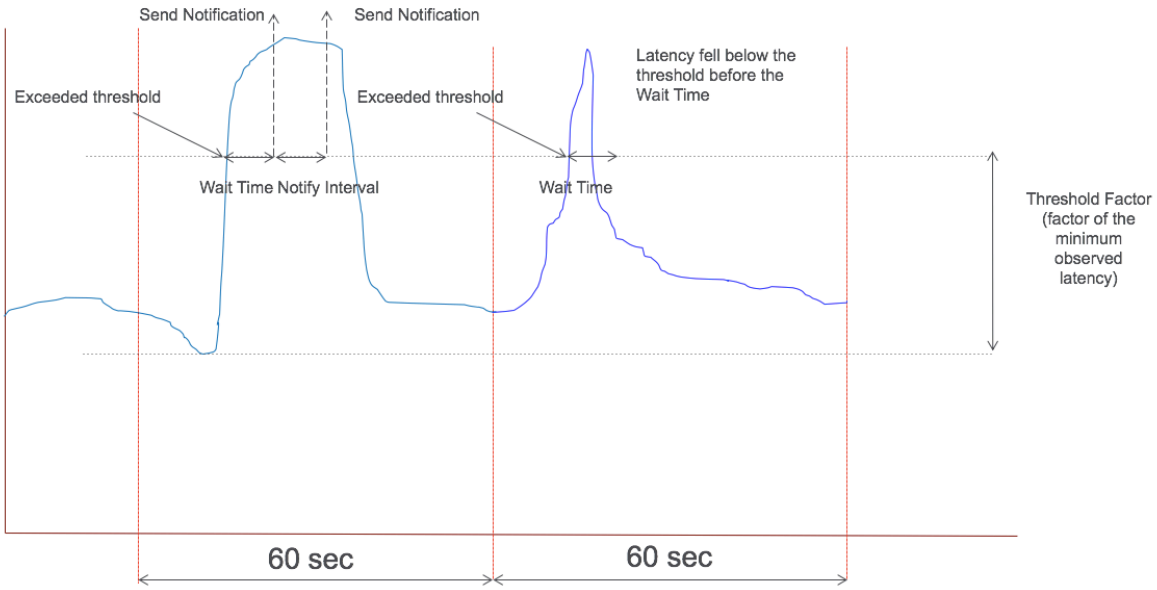


L7 遅延しきい値レポートモデル

L7 レイテンシー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、通知が HDX Insight に送信されます。

しきい値を超えると、遅延の増加が検出されます。設定したしきい値の待機時間が経過すると、HDX Insight に通知が送信されます。後続の通知は、待機時間が経過してもしきい値係数を超過した後も HDX Insight に送信されます。待機時間が経過する前にレイテンシ値がしきい値係数を下回った場合、HDX Insight に通知は送信されません。

次の図は、L7 遅延しきい値レポートモデルの例を示しています。



次のパラメータは、実行時に構成できます。

- しきい値監視 (ON/OFF)
- しきい値係数
- しきい値の待機時間
- 通知間隔
- 最大通知数

RDP プロキシ

April 1, 2024

RDP プロキシ機能は、NetScaler 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。NetScaler 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。

1. NetScaler Gateway パブリック IP アドレスに接続する
2. SSL VPN 接続を確立します。
3. 認証する
4. NetScaler 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します。

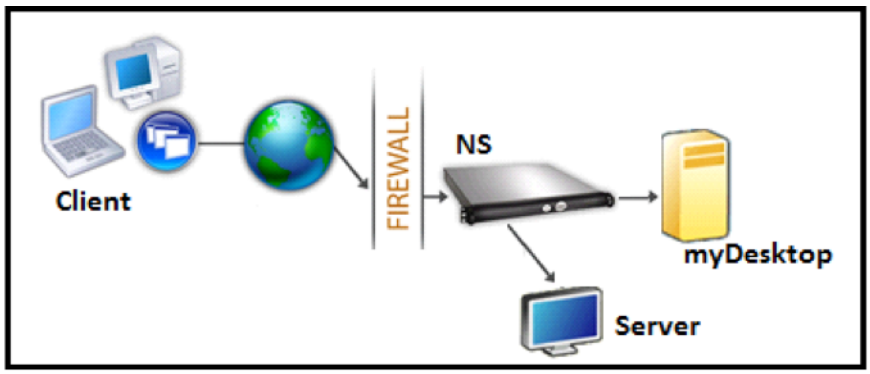
RDP プロキシ機能は、クライアントレス VPN および ICA プロキシモードでサポートされます。

> 注:
>
> NetScaler 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、RDS マルチユーザー、RDP セッション、または RDP アプリをサポートしていません。

次の RDP プロキシ機能は、NetScaler Gateway を介してリモートデスクトップファームへのアクセスを提供します。

- クライアントレス VPN 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。
- NetScaler Gateway を介した RDP サーバーへの SSO（シングルサインオン）。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。
- 強制（SmartAccess）機能。NetScaler ADC 管理者は、NetScaler 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）ゲートウェイソリューション（VPN/ICA/RDP/Citrix Endpoint Management）。
- RDP 用のネイティブ Windows MSTSC クライアントとの互換性は、カスタムクライアントを必要としません。
- Microsoft が提供している既存の RDP クライアントを MACOSX、iOS、Android で使用する。

次の図は、展開の概要を示しています。



クライアントレス **VPN** を介した導入

このモードでは、RDP リンクは Gateway ホームページまたはポータルで、ブックマークとして、`add vpn url`構成または外部ポータルを介して公開されます。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 プロキシを介した展開

このモードでは、`wihome`パラメータを使用して、Gateway VIP でカスタムホームページを設定します。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、NetScaler ADC でホストすることも、外部の場合は既存の Gateway ポータルページの iFrame にすることもできます。

どちらのモードでも、ユーザーが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、対応するリソースの HTTPS リクエストが NetScaler Gateway に到着します。Gateway は、要求された接続の RDP ファイル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、ゲートウェイ上の RDP リスナーに接続します。ゲートウェイは、強制 (SmartAccess) をサポートすることによって RDP サーバーへの SSO を実行します。ゲートウェイは、NetScaler ADC 構成に基づいて特定の 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

NetScaler ADC 管理者は、NetScaler Gateway 構成を通じて特定の RDP 機能を構成できます。NetScaler Gateway は、重要な RDP パラメータに対して「RDP 強制」機能を提供します。NetScaler 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の場合、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、適用されません。

> 重要：強制機能は、SSO が有効な場合にのみ適用できます。

強制用にサポートされている **RDP** パラメータ

次のリダイレクトパラメータの強制がサポートされています。これらのパラメータは、RDP クライアントプロファイルの一部として設定できます。

- 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。

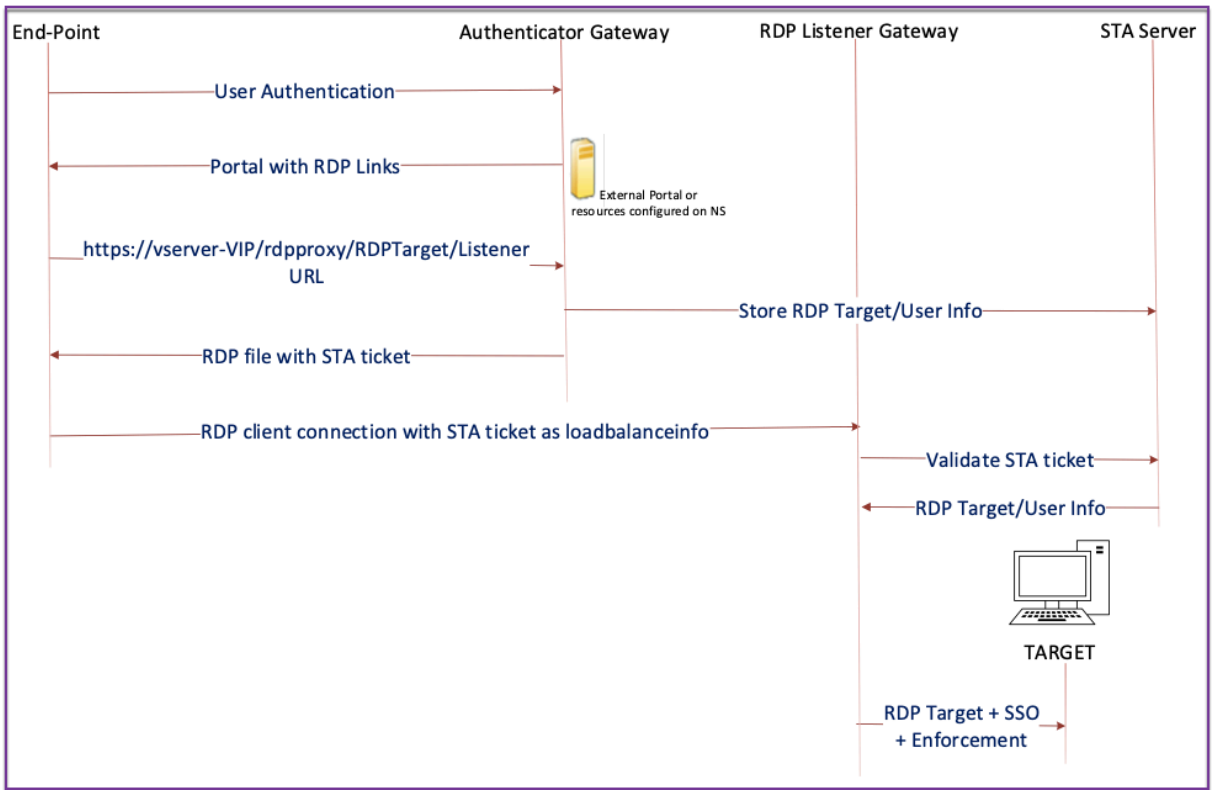
- RDP リソースの列挙と RDP ファイルのダウンロード。
- RDP 接続の起動。

前述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）ゲートウェイソリューション-RDP リソースの列挙と RDP ファイルのダウンロードは Authenticator Gateway を介して行われますが、RDP 接続の起動は RDP リスナーゲートウェイを介して行われます。
- 単一ゲートウェイソリューション-RDP リソースの列挙、RDP ファイルのダウンロード、および RDP 接続の起動は、同じゲートウェイを介して行われます。

ステートレス (デュアル) ゲートウェイの互換性

次の図は、展開を示しています。



- ユーザは Authenticator Gateway VIP に接続し、クレデンシャルを提供します。
- ゲートウェイ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、Authenticator Gateway VIP は、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`で要求を受信します。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。
- Authenticator Gateway は /rdpproxy/ 要求を処理します。ユーザ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 Cookie が付属しています。

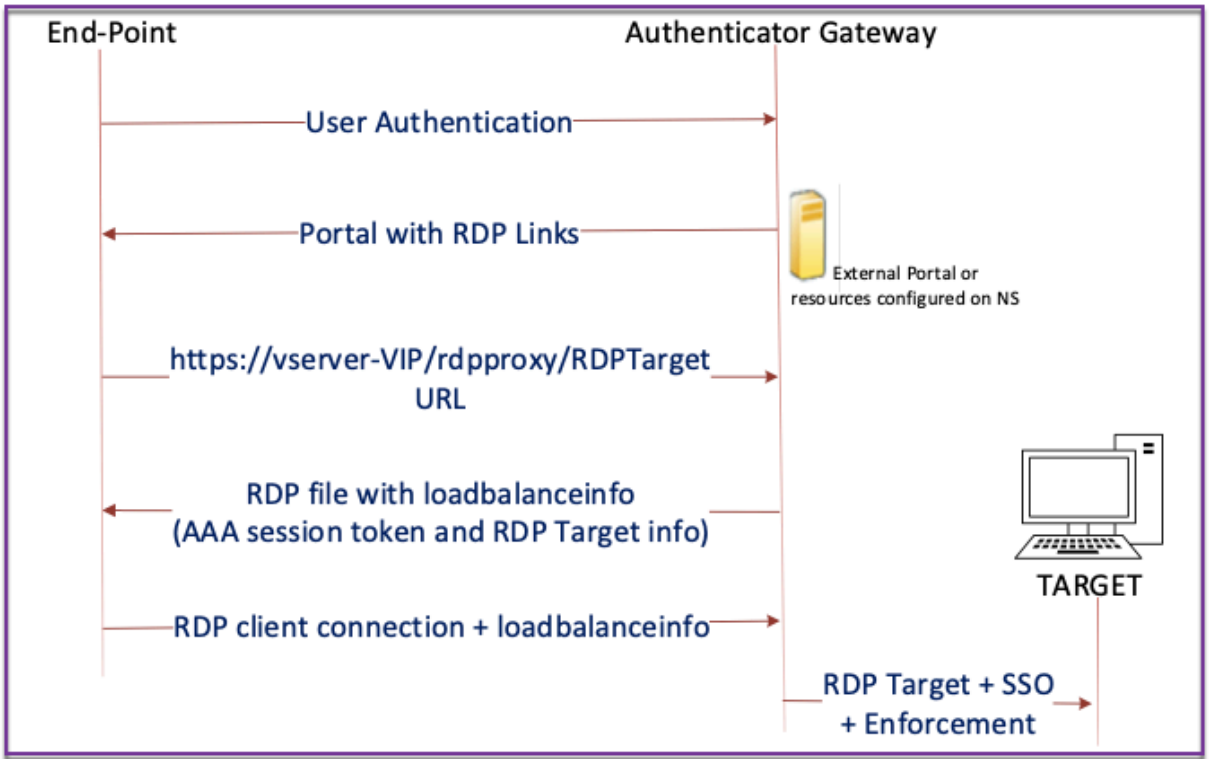
- RDPTargetおよびRDPUser情報は STA サーバに保存され、STA チケットが生成されます。STA サーバに保存された情報は、設定済みの事前共有キーを使用して暗号化されます。Authenticator Gateway は、ゲートウェイ仮想サーバ上に設定されている STA サーバの 1 つを使用します。
- /rdpproxy/ 要求で取得された「リスナー」情報は、.rdp fileに「fulladdress」としてに追加され、STA チケット（STA AuthId が前に付く）は.rdp fileに「loadbalanceinfo」として追加されます。
- .rdp fileがクライアントエンドポイントに返送されます。
- 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 チケットを最初のパケットで送信します。

  RDPListenerゲートウェイは STA チケットを検証し、RDPTargetおよびRDPUser情報を取得します。使用する STA サーバは、loadbalanceinfoに存在する「AuthID」を使用して取得されます。
- ゲートウェイセッションは、承認/監査ポリシーを格納するために作成されます。ユーザーのセッションが存在する場合、そのセッションは再利用されます。
- RDPListenerゲートウェイは、RDPTargetに接続し、CREDSSP を使用してシングルサインオンします。

> 重要:
>
> - ステートレス RDP プロキシの場合、STA サーバは RDP クライアントによって送信された STA チケットを検証してRDPTarget/RDPUser情報を取得します。VPN 仮想サーバーに加えて STA サーバーをバインドする必要があります。

シングルゲートウェイの互換性

次の図は、展開を示しています。



> 重要:
>
> 単一ゲートウェイ展開の場合、STA サーバーは必要ありません。オーセンティケータゲートウェイは、RDPTargetおよび NetScaler の認証、承認、および監査セッション Cookie を安全にエンコードし、.rdp fileのloadbalanceinfoとして送信します。RDP クライアントがこのトークンを最初のパケットで送信すると、Authenticator Gateway はRDPTarget情報をデコードし、セッションを検索し、RDPTargetに接続します。

シングル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応する単一リスナー。
- RDP ファイルのダウンロードと RDP トラフィックは、NetScaler ADC アプライアンスの同じ 2 つのタプル（IP とポート）を介して処理できます。

RDP プロキシのライセンス要件

プレミアムエディション、アドバンスドエディション

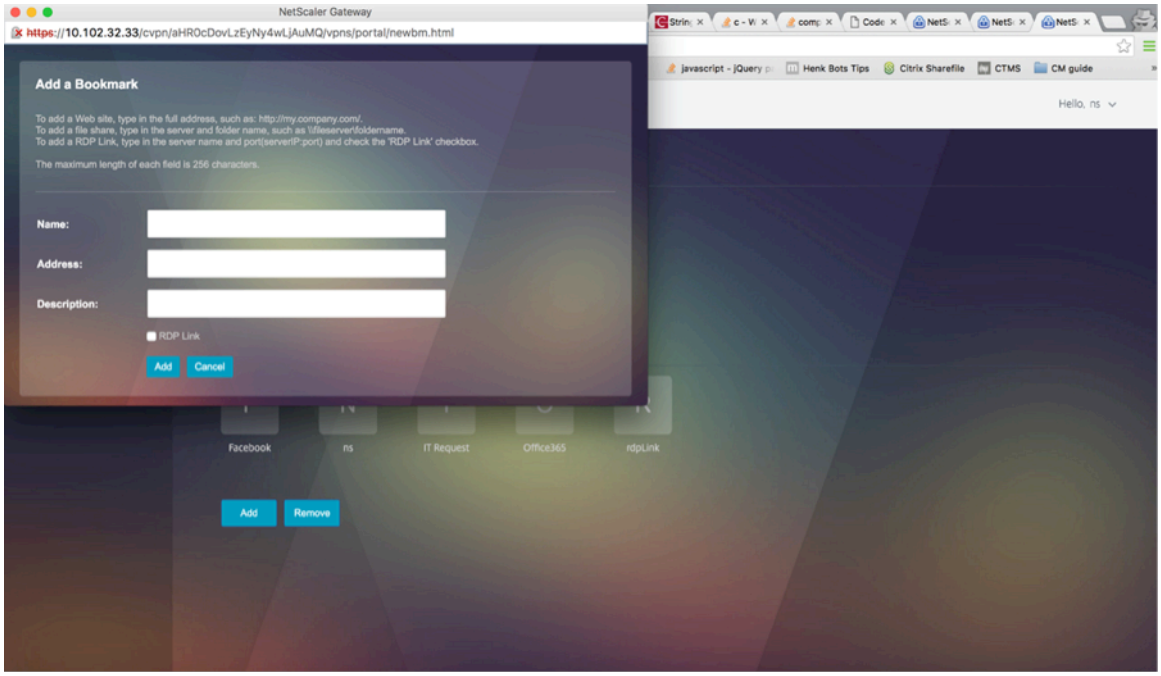
> 注:
>
> RDP プロキシ機能は、Gateway プラットフォームライセンスのみ、または Standard エディションのみをお持ちのお客様にはご利用いただけません。

RDP プロキシを有効にするには、次のコマンドを使用します。

```
enable feature rdpProxy
<!--NeedCopy-->
```

ブックマーク

ポータルを介した **RDP** リンク生成。ユーザーの RDP リンクを構成したり、外部ポータルを使用して RDP リンクを公開したりする代わりに、`targerIP:Port`を提供して独自の URL を生成するオプションをユーザーに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、RDP リスナー情報を FQDN: ポート形式で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、デュアルゲートウェイモードのポータル経由の RDP リンク生成に使用されます。



ブックマークを作成する

1. RDP リソースにアクセスするための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 を追加 <urlName> <linkName> <actualURL>
   - URL は次の形式にする必要があります。`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ー、グループ、VPN 仮想サーバー、または VPN グローバルにバインドします。

RDP プロキシで有効にする機能とモード

```
1 -  enable ns feature ssl
2
3 -  enable ns feature sslvpn
4
5 -  enable ns feature rdpproxy
6
7 -  enable mode usnip
8 <!--NeedCopy-->
```

RDP プロキシの概要設定手順

ステートレス RDP プロキシ設定に関連する次の高レベルのステップ。

- RDP サーバープロファイルを作成する
- RDP クライアントプロファイルを作成する
- 仮想サーバーを作成してバインドする
- ブックマークを作成する
- 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する
- ブックマークをバインドする

クライアントプロファイルを構成する

Authenticator 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 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行うことができます。

例:

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>

add vpn sessionpolicy <polname> NS_TRUE <actname>

bind vpn vserver <vservername> -policy <polname> -priority <
    prioritynumber>
<!--NeedCopy-->
```

または

```
set vpn parameter  - rdpClientprofile <name>
<!--NeedCopy-->
```

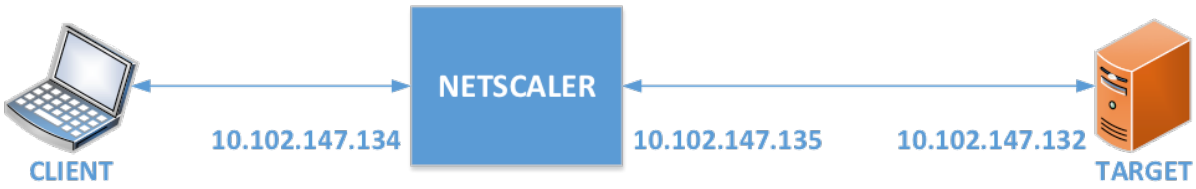
サーバープロファイルを構成する

リスナーゲートウェイでサーバプロファイルを設定します。

```
add rdp ServerProfile <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>`
<!--NeedCopy-->
```

`rdp ServerProfile`は VPN 仮想サーバ上で設定する必要があります。

```
add vpn vserver v1 SSL <publicIP> <portforterminatingvpnconnections> -
    rdpServerProfile <rdpServer Profile>`
<!--NeedCopy-->
```



CLI を使用した RDP プロキシの設定

CLI を使用した RDP プロキシ設定の例を次に示します。

- ターゲット情報を含むユーザの VPN URL を追加します。


```
add aaa user Administrator  -password freebsd123$%^

add vpn url rdp RdpLink rdp://rdpserverinfo

add dns addrec rdpserverinfo 10.102.147.132

bind aaa user Administrator   -urlName rdp
<!--NeedCopy-->
```

- VPN 接続用の RDP クライアントおよびサーバプロファイルを設定します。

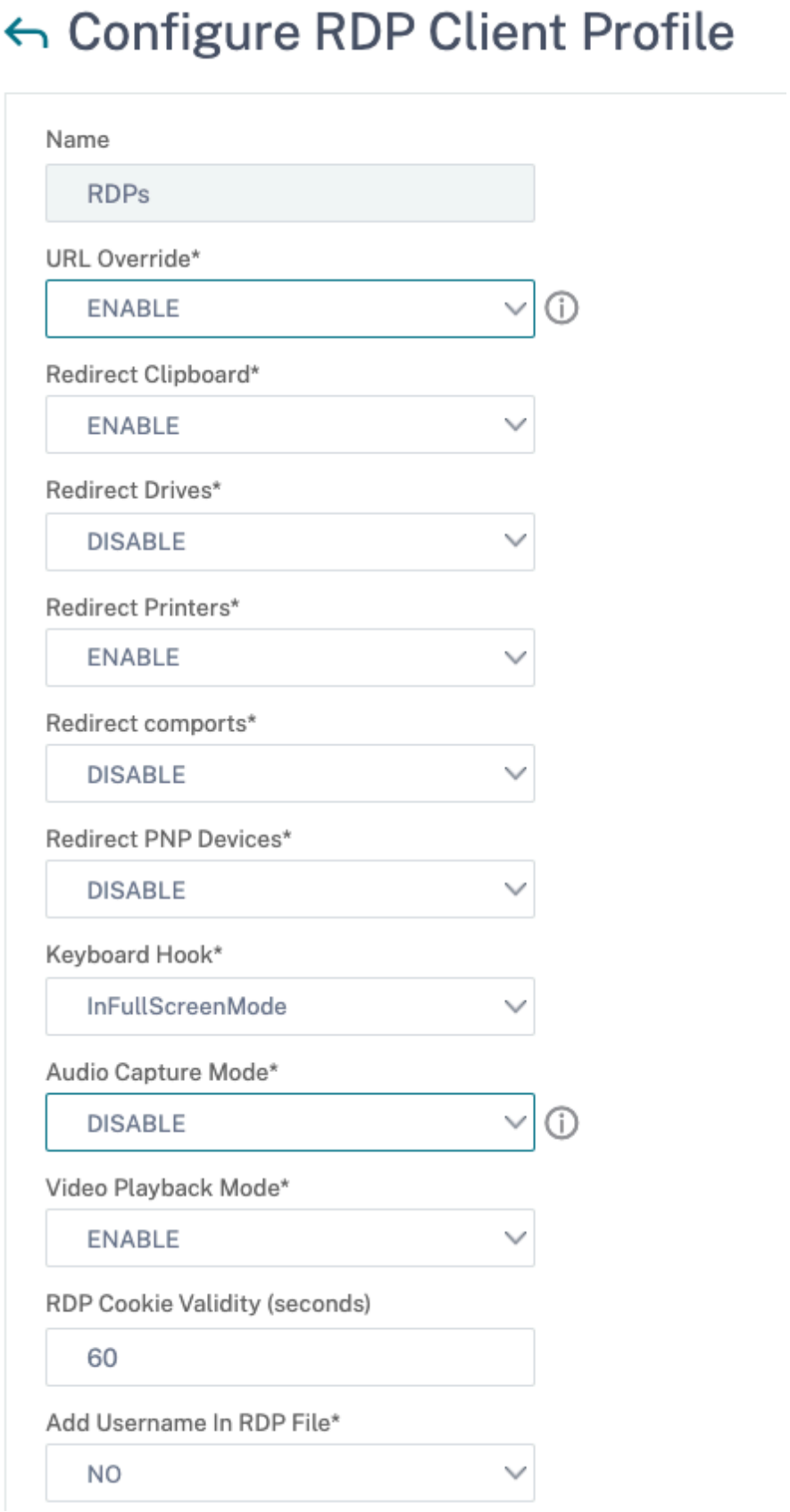
```
add rdp clientprofile p1  -psk citrix -redirectClipboard ENABLE

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-->
```

- NetScaler ADC からターゲットに接続するための SNIP を追加します。

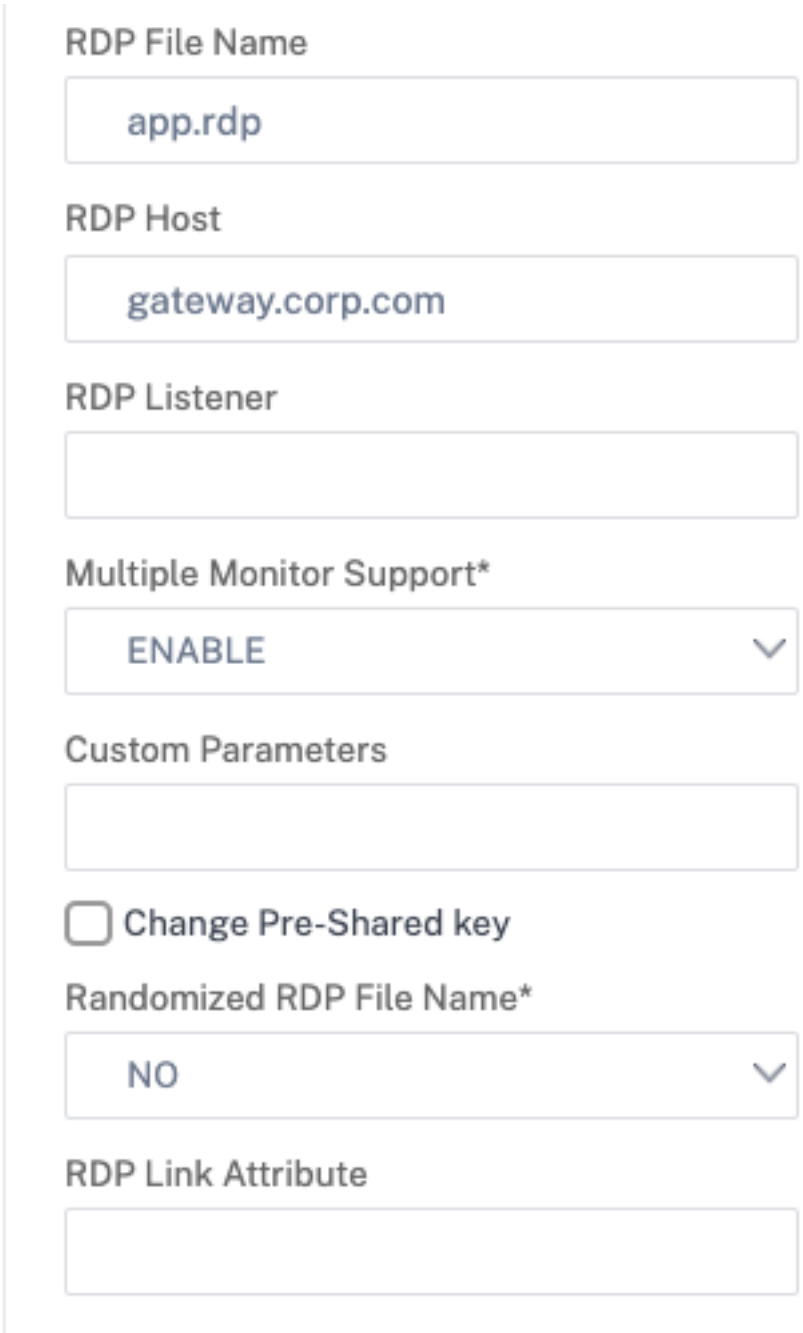
```
add ns ip 10.102.147.135  255.255.255.0  -type SNIP
<!--NeedCopy-->
```

GUI を使用した RDP プロキシの設定

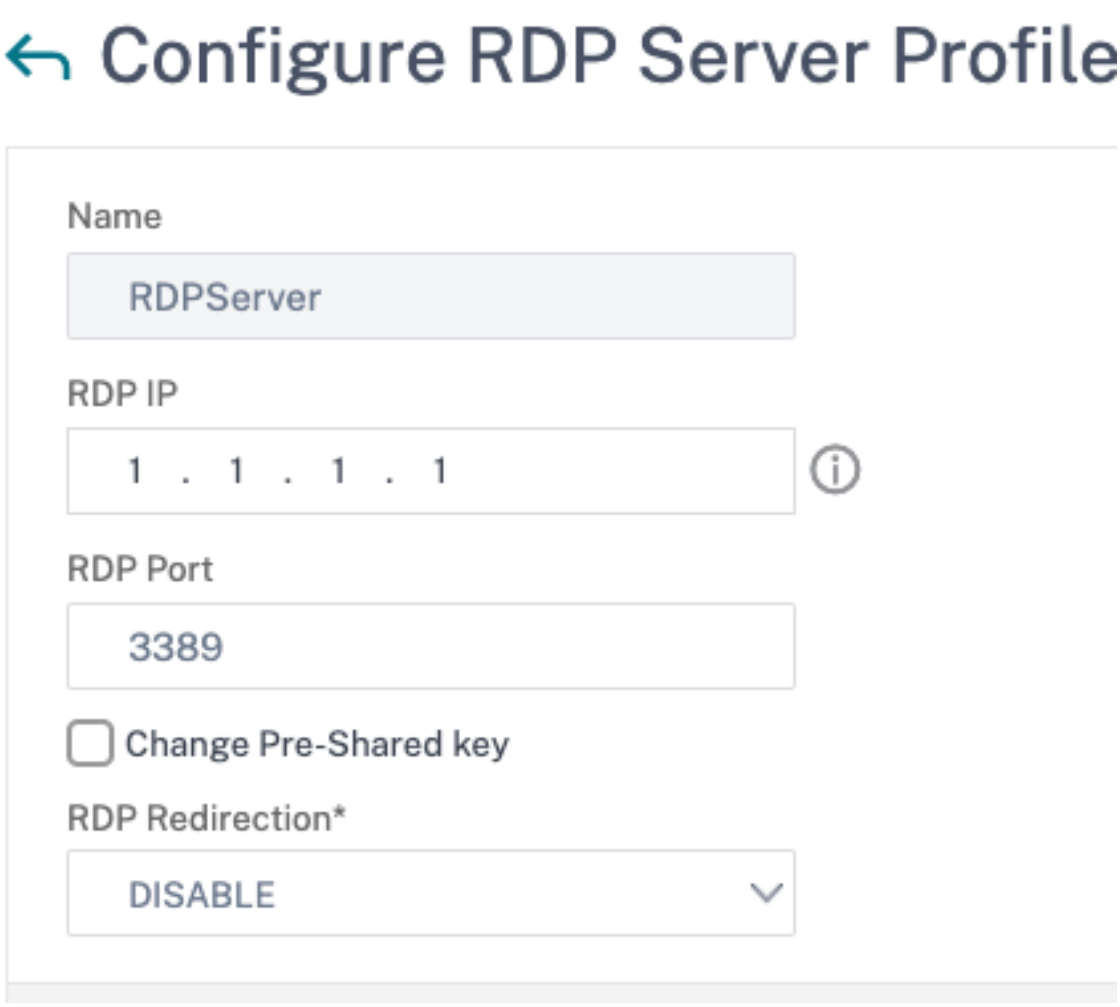
1. [**NetScaler Gateway**] **>** [ポリシー] に移動し、[**RDP**] を右クリックして [機能を有効にする] をクリックします。
2. ナビゲーションペインで [RDP] をクリックします。右側の [クライアントプロファイル] タブを選択し、[追加] をクリックします。
3. クライアントプロファイルの名前を入力し、設定します。



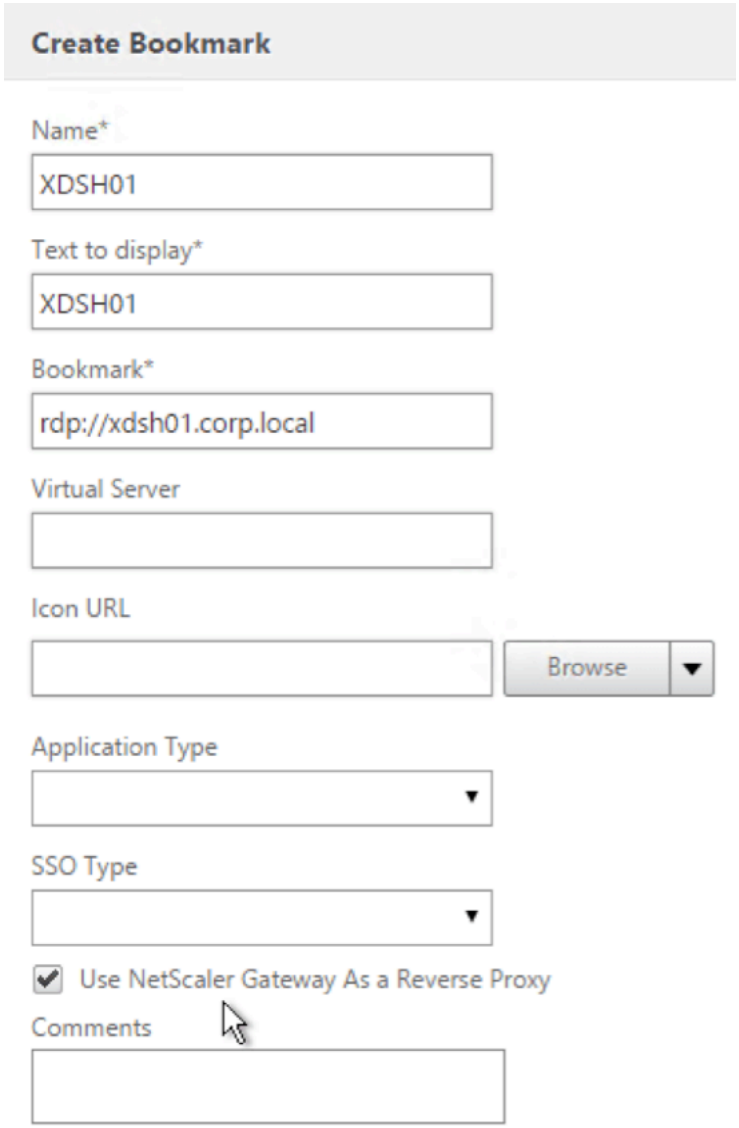
4. ［RDP ホスト］フィールドに、RDP プロキシリスナーに解決される FQDN を入力します。これは通常、NetScaler Gateway アプライアンスの FDQN と同じ FQDN です。
5. 「事前共有キー」にパスワードを入力し、「**OK**」をクリックします。



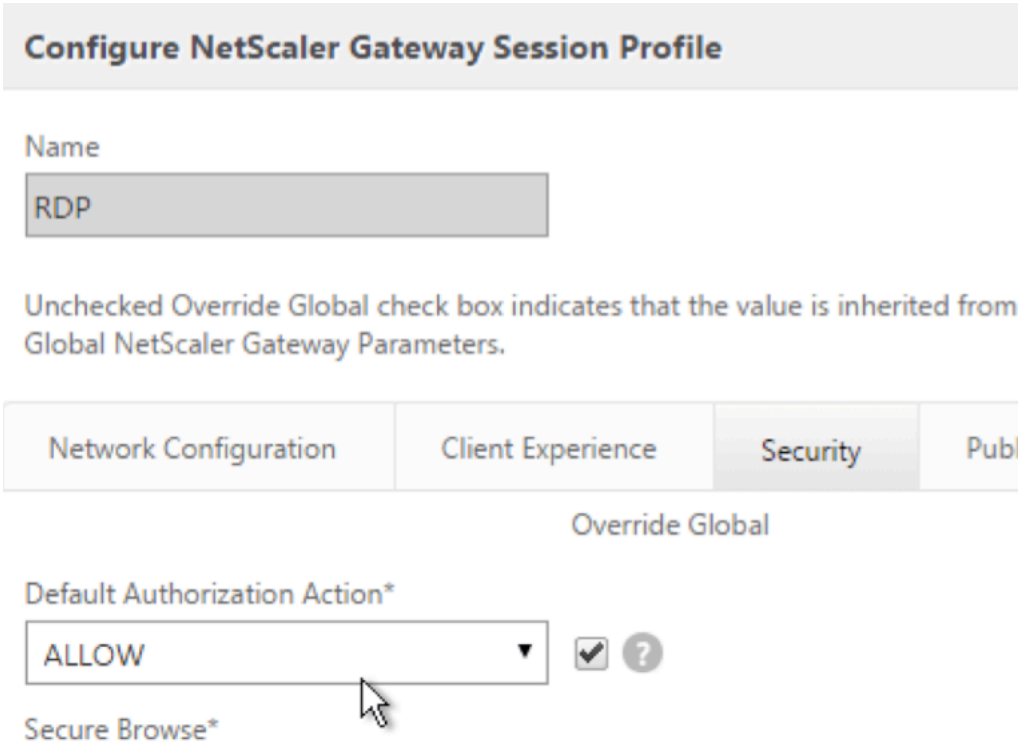
6. サーバプロファイルの名前を入力します。
7. このプロファイルをバインドするゲートウェイ仮想サーバーの IP アドレスを入力します。
8. RDP クライアントプロファイルに設定したのと同じ事前共有キーを入力します。［**Create**］をクリックします。



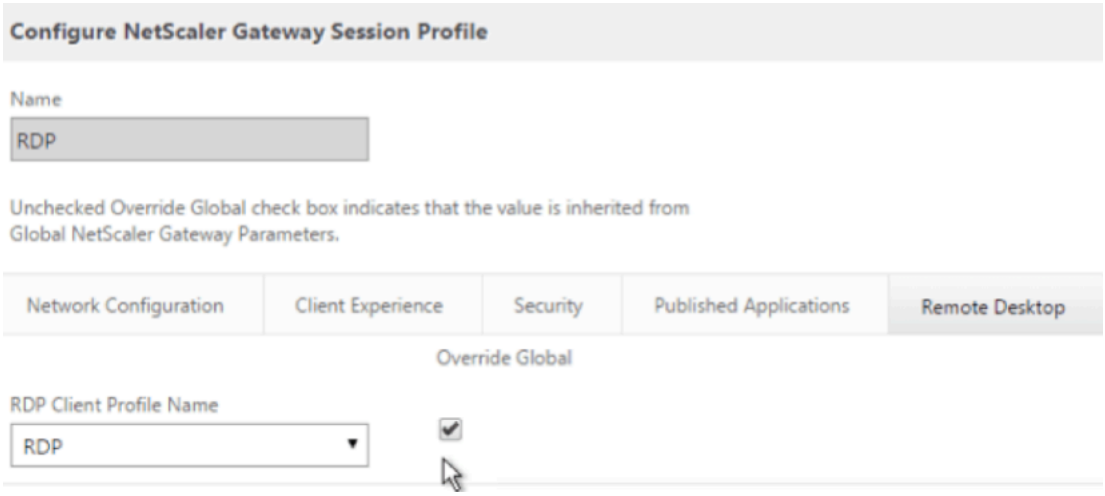
9. クライアントレスアクセスポータルページで RDP ブックマークを追加する場合は、左側で［**NetScaler Gateway**］、［リソース］、［ブックマーク］の順に展開します。
10. 右側の [追加] をクリックします。
11. ブックマークに名前を付けます。
12. URL には、**IP** または **DNS** を使用して **rdp: //myrdpServer** と入力します。
13. ［**NetScaler Gateway** をリバースプロキシとして使用］を選択し、［作成］をクリックします。
14. 要件に従ってブックマークを作成します。



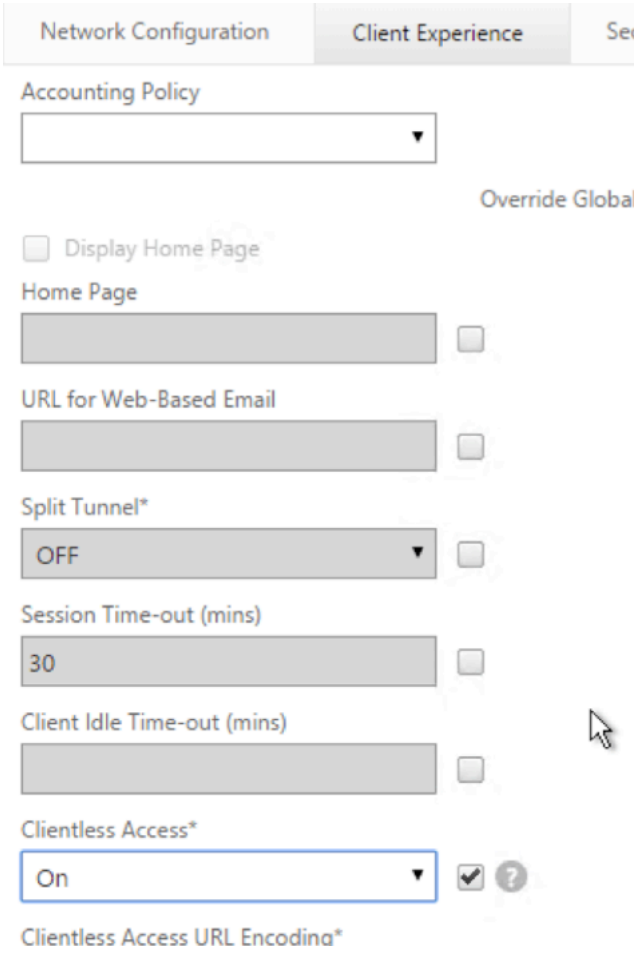
15. セッションプロファイルを作成または編集します。[**NetScaler Gateway**] **>** [ポリシー] **>** [セッション] に移動します。
16. [セキュリティ] タブで、[既定の承認アクション] を [許可] に設定します。または、認可ポリシーを使用してアクセスを制御することもできます。



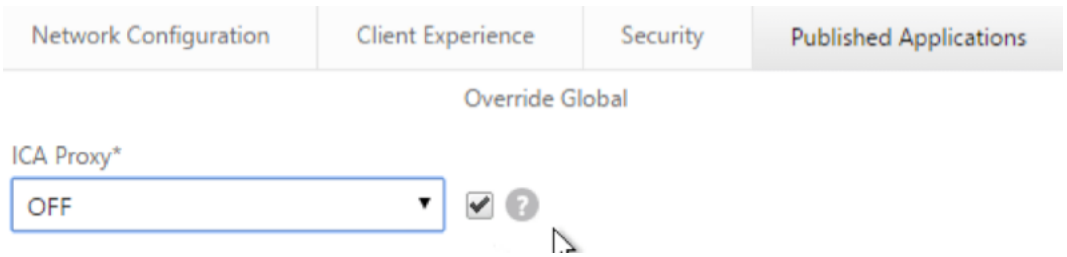
17. [リモートデスクトップ] タブで、前に作成した RDP クライアントプロファイルを選択します。



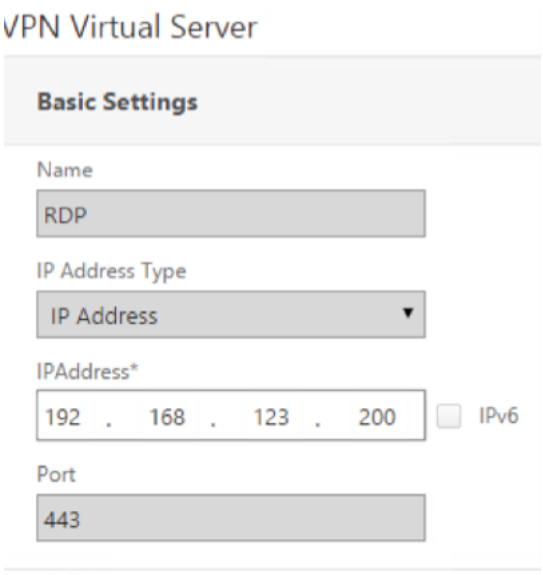
18. ブックマークを使用する場合は、[クライアントエクスペリエンス] タブで、**[**** クライアントレスアクセス ****]** を [オン] に設定します。



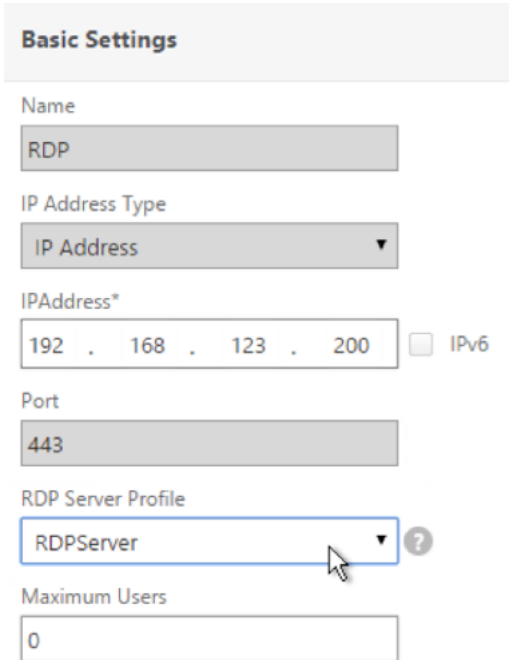
19. [公開アプリケーション] タブで、[ICA プロキシ] がオフになっていることを確認します。



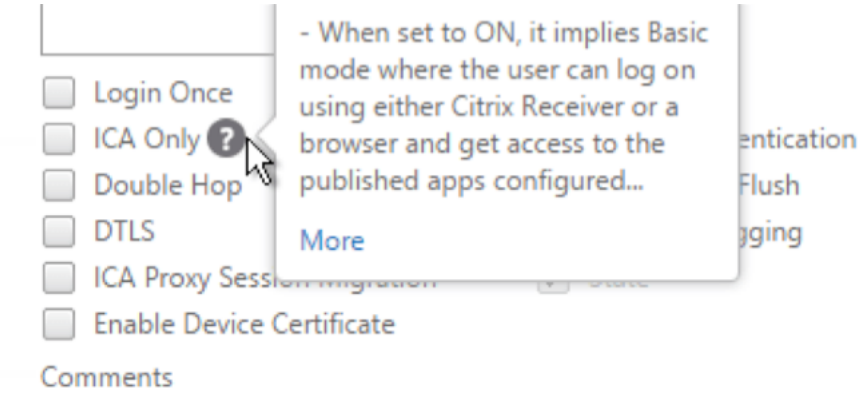
20. ゲートウェイ仮想サーバーを変更または作成します。
21. [基本設定] セクションで、[詳細] をクリックします。



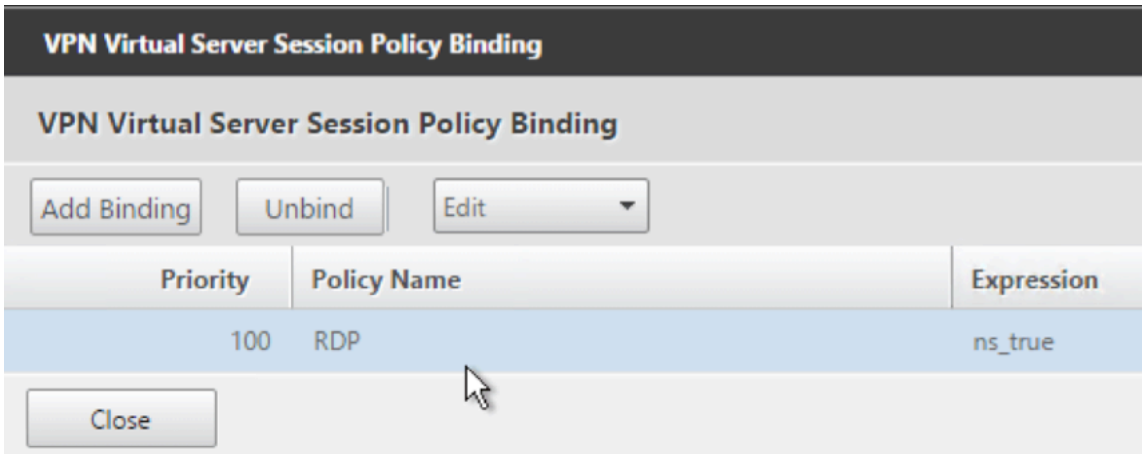
22. RDP サーバプロファイルリストを使用して、前に作成した RDP サーバプロファイルを選択します。



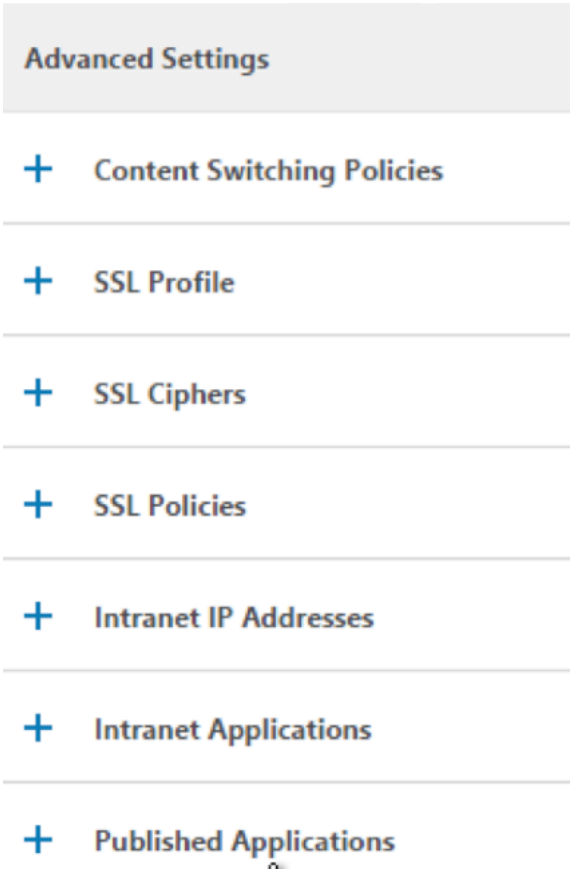
23. 下にスクロールします。[**ICA** のみ] がオフになっていることを確認します。



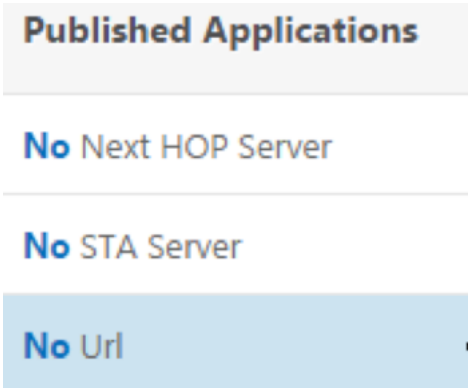
24. 証明書をバインドします。
25. 認証ポリシーをバインドします。
26. RDP クライアントプロファイルが設定されているセッションポリシー/プロファイルをバインドします。



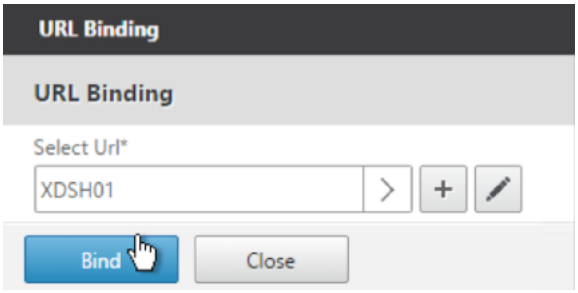
27. ブックマークは、NetScaler Gateway 仮想サーバー、または認証、承認、および監査グループにバインドできます。NetScaler Gateway 仮想サーバーにバインドするには、右側の［詳細設定］セクションで、［公開アプリケーション］をクリックします。



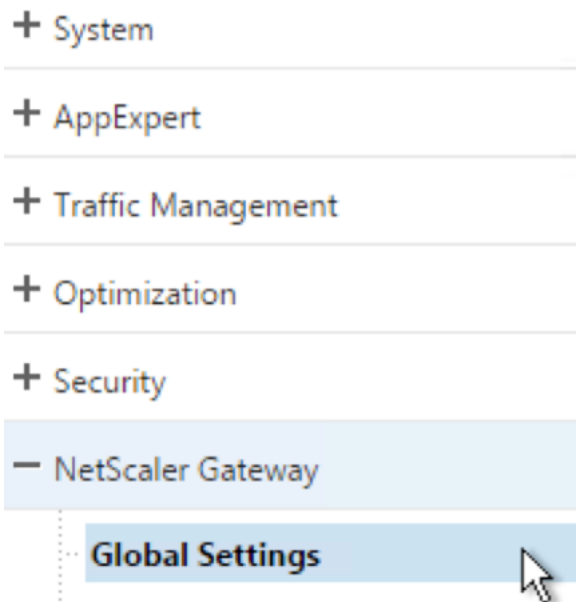
28. 左側の [公開アプリケーション] セクションで、[**URL** なし] をクリックします。



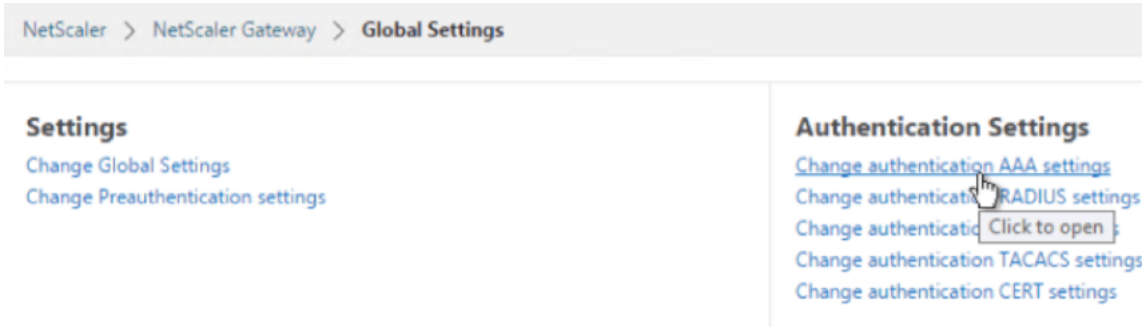
29. ブックマークをバインドします。



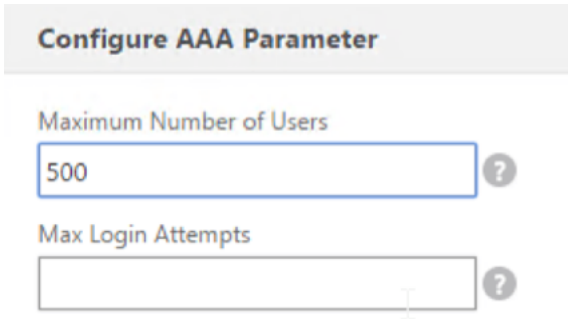
30. この NetScaler Gateway 仮想サーバーには［ICA のみ］が指定されていないため、NetScaler Gateway ユニバーサルライセンスが正しく構成されていることを確認してください。左側で、［**NetScaler Gateway**］を展開し、［グローバル設定］をクリックします。



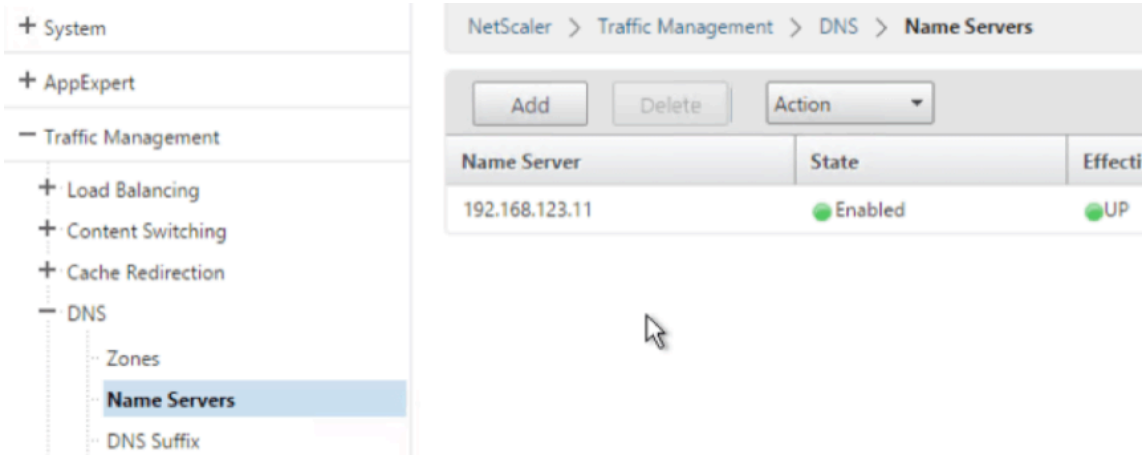
31. 右側の [認証 **AAA** 設定の変更] をクリックします。



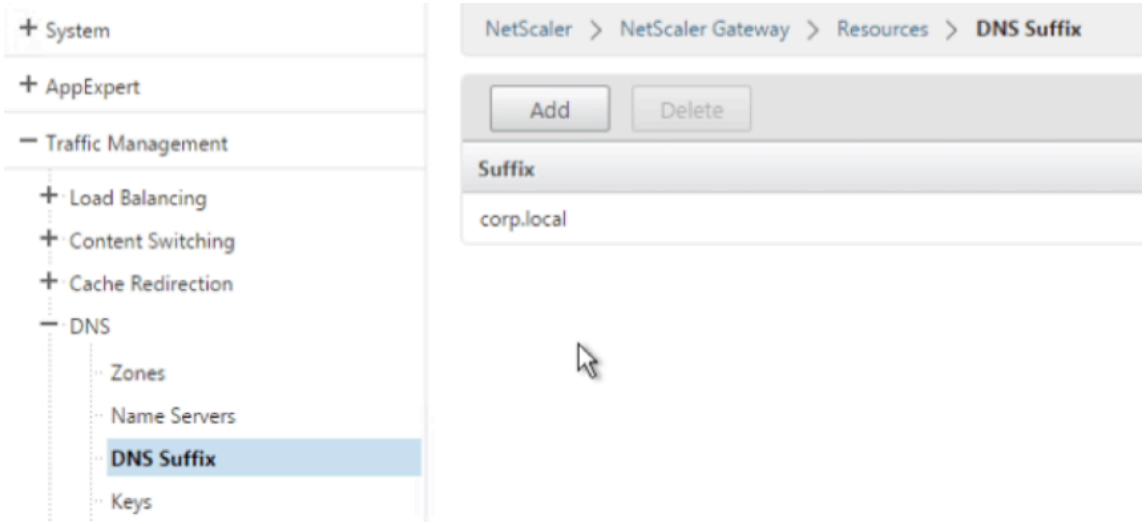
32. [最大ユーザー数**]** をライセンス制限に変更します。



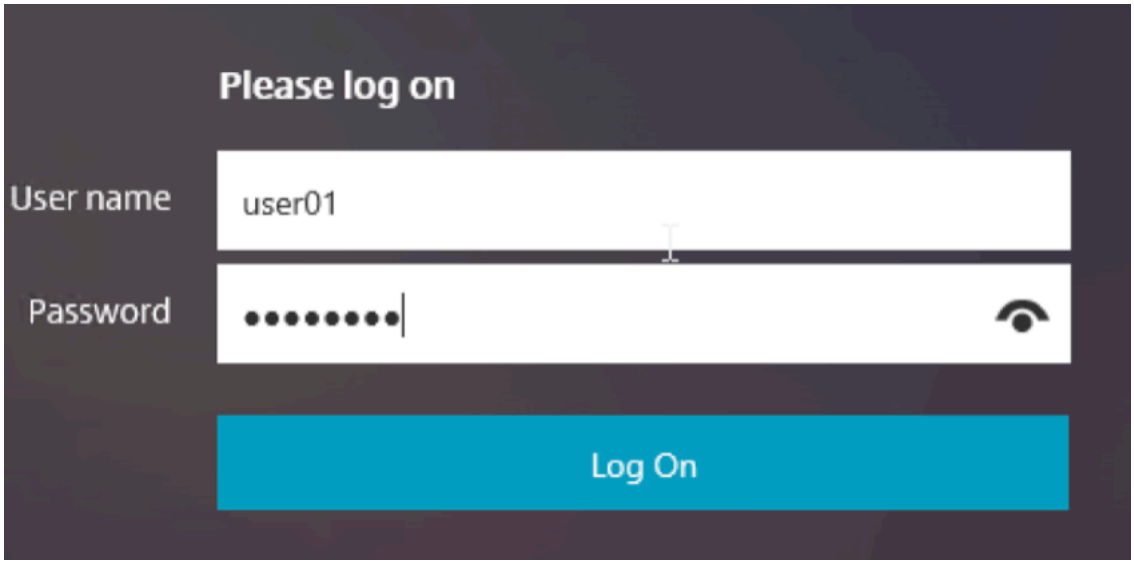
33. DNS を使用して RDP サーバーに接続する場合は、アプライアンスで DNS サーバーが設定されていることを確認します（[トラフィック管理**] > [DNS] > [**ネームサーバー**]**）。



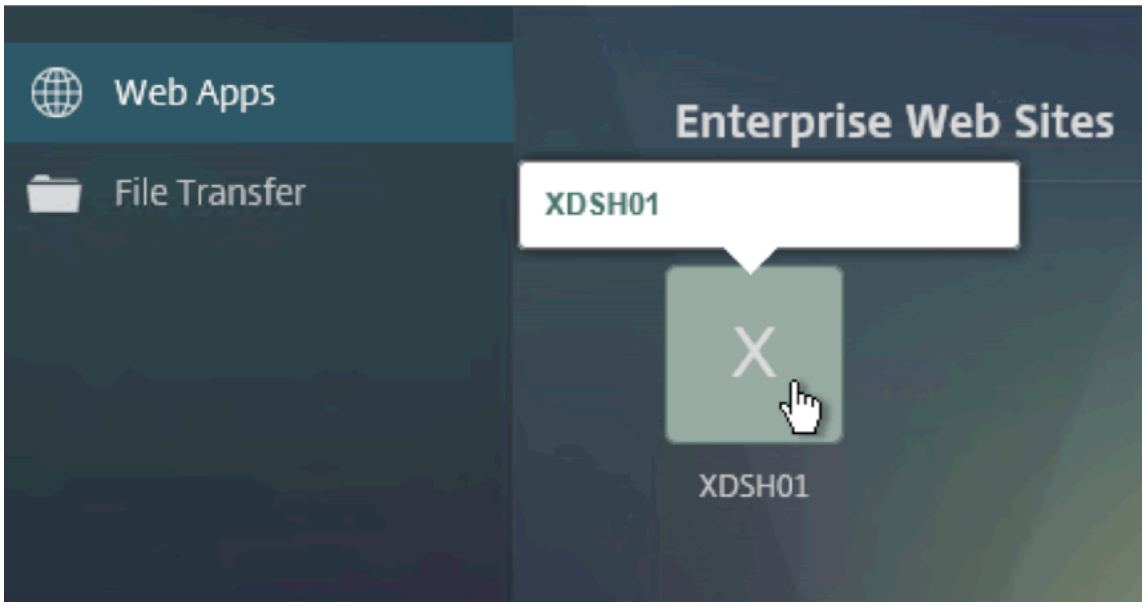
34. FQDN の代わりに短い名前を使用する場合は、DNS サフィックスを追加します **([**トラフィック管理**] > [DNS] > [DNS** サフィックス**])**。



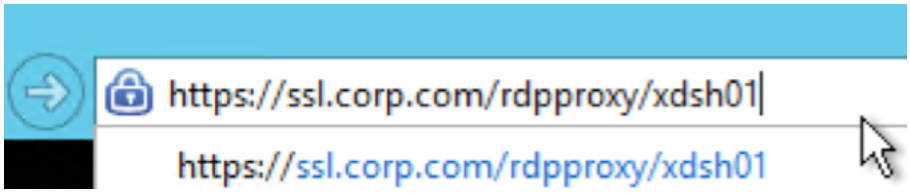
35. ゲートウェイに接続してログオンします。



36. [ブックマーク] を構成した場合は、[ブックマーク] をクリックします。

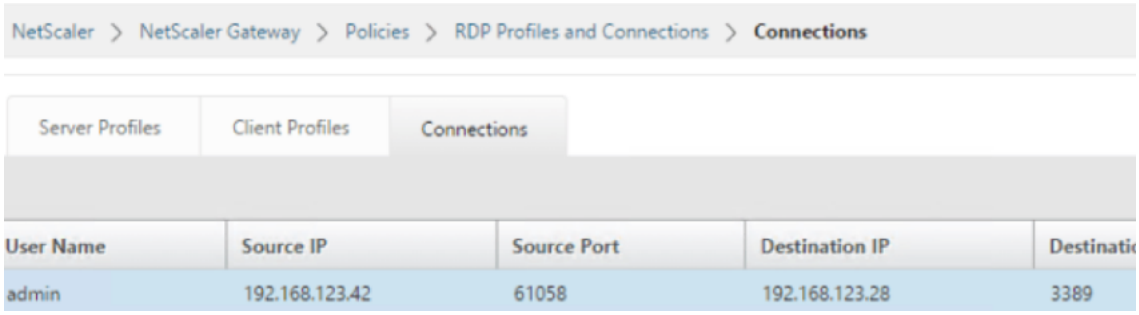


37. アドレスバーを **/rdpProxy/myrdpServer** に変更できます。IP アドレス (rdpproxy/192.168.1.50 など) または DNS 名 (/rdpproxy/myserver) を入力できます。



38. ダウンロードした`.rdp file`を開きます。

39. 現在接続しているユーザーを表示するには、[**NetScaler Gateway** ポリシー] **>** [**RDP**] の順に選択します。右側には [接続] タブがあります。



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、NetScaler 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 強制 (SmartAccess) は機能しません。

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に対して 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>  "HTTP.REQ.URL.CONTAINS
    ("rdpproxy") && CLIENT.IP.SRC.EQ(<IP>)" <TrafficActionName>
bind vpnvserver rdp -policy <TrafficPolicyName> -priority 10
<!--NeedCopy-->
```

ステートレス **RDP** プロキシ

April 1, 2024

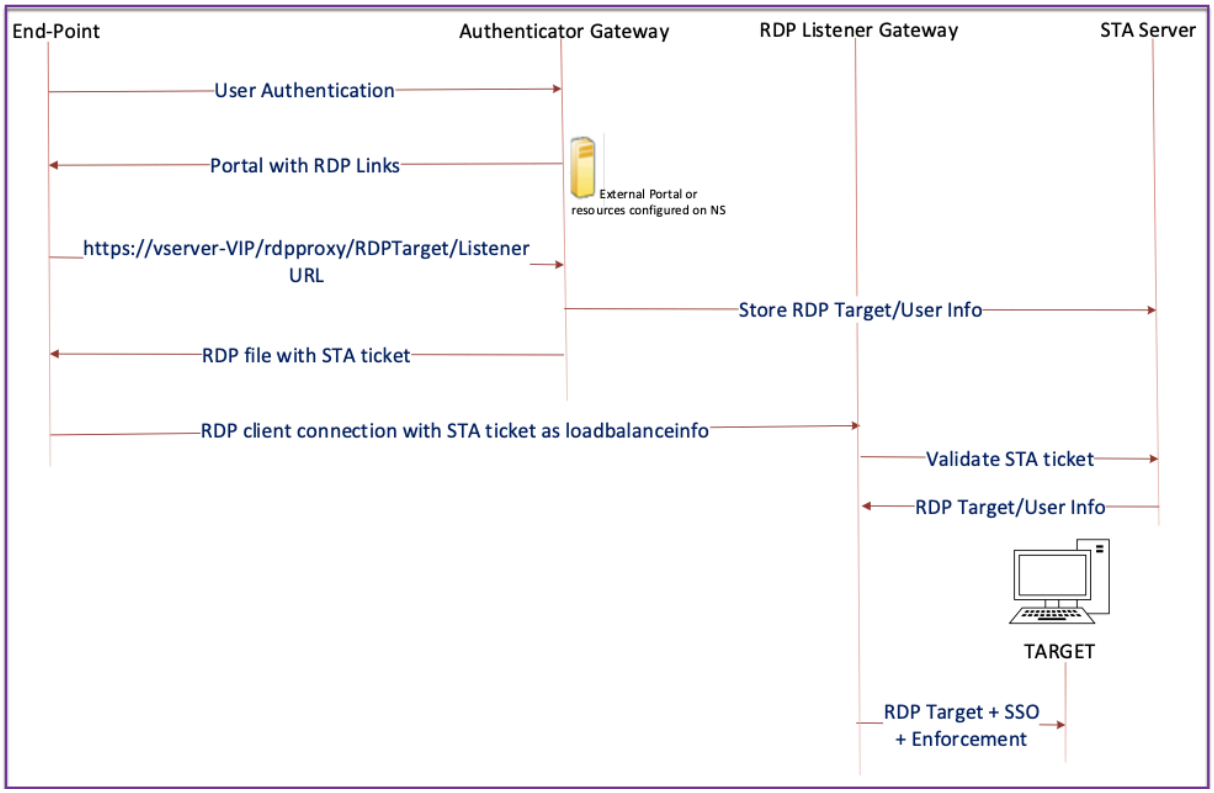
ステートレス RDP プロキシは RDP ホストにアクセスします。ユーザーが別の NetScaler Gateway Authenticator で認証すると、NetScaler Gateway 上の`RDPListener`を介してアクセスが許可されます。NetScaler Gateway

用にRDPListenerに必要な情報は、STA サーバーに安全に保存されます。STA サーバーは、NetScaler Gateway およびアプリケーション列挙サーバーが到達できる限り、どこにでも配置できます。詳細については、https://support.citrix.com/article/CTX101997を参照してください。

接続フロー

RDP プロキシフローには 2 つの接続が含まれます。最初の接続は、NetScaler Gateway VIP へのユーザーの SSL VPN 接続と、RDP リソースの列挙です。

2 番目の接続は、NetScaler Gateway 上の RDP リスナー（RDPIP および rdpPort を使用して構成）へのネイティブ RDP クライアント接続と、その後の RDP クライアントのサーバーパケットへの安全なプロキシです。



1. ユーザは Authenticator Gateway VIP に接続し、クレデンシャルを提供します。
2. ゲートウェイ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ます。このポータルには、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が列挙されます。
3. ユーザーが RDP リソースを選択すると、Authenticator Gateway VIP によって、ユーザーがクリックした公開リソースを示す形式https://AGVIP/rdpproxy/ip:port/rdptargetproxyで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. Authenticator Gateway は /rdpproxy/ 要求を処理します。ユーザはすでに認証されているため、この要求には有効なゲートウェイ Cookie が付属しています。

5. RDPTargetとRDPUserの情報は STA サーバに保存され、STA チケットが生成されます。情報は XML BLOB として格納され、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 でエンコードされて格納されます。Authenticator Gateway は、ゲートウェイ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 の形式は次のとおりです。

```
<Value name=" IPAddress" >ipaddr</Value>\n<Value name=" Port" >
    port</Value>n

<Value name=" `Username`" >username</Value>\n<Value name="
    Password" >pwd</Value>
<!--NeedCopy-->
```

7. /rdpproxy/ リクエストで取得されたrdptargetproxyは’ fulladdress’として配置され、STA チケット (STA AuthID の前に) がloadbalanceinfoとして.rdp ファイルに配置されます。
8. .rdpファイルはクライアントの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 チケットは最初の x.224 パケットで送信されます。
10. RDPListener Gatewayは STA チケットを検証し、RDPTargetおよびRDPUser情報を取得します。使用する STA サーバは、loadbalanceinfo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、承認/監査ポリシーを格納するために作成されます。ユーザーのセッションが存在する場合、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。

前提条件

- ユーザーは NetScaler Gateway Authenticator で認証されます。
- 最初の /rdpproxy URL と RDP クライアントは、別のRDPListener NetScaler Gatewayに接続されています。
- STA サーバを使用する Authenticator Gateway は、RDPListener Gateway 情報を安全に渡します。

CLI を使用したステートレス RDP プロキシの設定

- 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で設定されます。

  注:

- RDPSServer プロファイルが VPN 仮想サーバーで設定されると、変更できません。また、同じ ServerProfile を別の VPN 仮想サーバーで再利用することはできません。

```
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].
<!--NeedCopy-->
```

次のコマンドを使用して、VPN 仮想サーバーの RDP サーバープロファイルを設定します。

```
add vpn vserver v1 SSL [publicIP] [
   portforterminatingvpnconnections] -rdpServerProfile [rdpServer
    Profile]
<!--NeedCopy-->
```

例

```
add vpn vserver v1 SSL 1.1.1.1 443 -rdpServerProfile
   rdp_server_prof
<!--NeedCopy-->
```

> 重要:
>
> - 同じ STA サーバーを RDP 認証ゲートウェイとリスナーゲートウェイの両方にバインドする必要があります。
> - 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た STA チケットを検証して、RDP ターゲットサーバーと RDP ユーザーの情報を取得します。VPN 仮想サーバーに加えて STA サーバーをバインドする必要があります。次の例では、RDP ターゲットサーバーは 1.1.1.0 で、RDP リスナーゲートウェイ仮想サーバー 1.1.1.2 です。
>
> ```
>     add vpn url url4 RDP2 "rdp://1.1.1.0/1.1.1.2:443"
> <!--NeedCopy-->
> ```

次のコマンドを使用して、オーセンティケータ Gateway のクライアントプロファイルを設定します。

```
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 )]

      [-redirectPrinters ( ENABLE | DISABLE )] [-keyboardHook <
         keyboardHook>] [-audioCaptureMode ( ENABLE | DISABLE )] [-
         videoPlaybackMode ( ENABLE | DISABLE )]

      [-rdpCookieValidity <positive_integer>][-multiMonitorSupport (
         ENABLE | DISABLE )] [-rdpCustomParams <string>]
<!--NeedCopy-->
```


—rdpHost 設定は、単一のゲートウェイ展開で使用されます。pskのみ は必須の引数で、RDP リスナーゲートウェイの RDP サーバープロファイルに追加された PSK と同じ PSK でなければなりません。

- RDP プロファイルを VPN 仮想サーバに関連付けます。

RDP プロファイルを関連付けるには、SessionAction+SessionPolicy を設定するか、グローバル VPN パラメータを設定します。

例:

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>

add vpn sessionpolicy <polname> NS_TRUE <actname>

bind vpn vserver <vservername> -policy <polname> -priority <
    prioritynumber>
<!--NeedCopy-->
```

または

```
set vpn parameter  - rdpClientprofile <name>
<!--NeedCopy-->
```

GUI を使用してステートレス RDP プロキシを構成する

ステートレス RDP プロキシの設定には、次の高レベルの手順が含まれます。詳細な手順については、「RDP プロキシの設定」を参照してください。

- RDP サーバープロファイルを作成する
- RDP クライアントプロファイルを作成する
- 仮想サーバーの作成
- ブックマークを作成する
- 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する
- ブックマークをバインドする

> 重要:
>
> ステートレス RDP プロキシの場合は、VPN 仮想サーバーに加えて STA サーバーをバインドする必要があります。

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。これは、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 ADC シェルのnsconmsgコマンドの一部として表示できます。これらのカウンタを表示する CLI コマンドは、後で追加される予定です。

アップグレードノート

以前 VPN 仮想サーバー上で構成されていた rdpIP と rdpPort は、rdpServerProfile の一部です。`rdp Profile` の名前が`rdp ClientProfile`に変更され、パラメータ clientSSL が削除されます。したがって、以前の設定は機能しません。

RDP 接続リダイレクト

April 1, 2024

NetScaler 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の 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接続ごとに排他的な 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し、管理者のメンテナンスと構成のオーバーヘッドを削減します。

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、シングルゲートウェイモードとステートレスモードまたはデュアルゲートウェイモードの両方でサポートされます (SmartAccess)。
- RDP プロキシ機能は、IP Cookie 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の使用] 機能が無効になっている場合、Windows セッションブローカまたは接続ブローカによって返されます。
- [**IP** アドレスリダイレクトを使用する] 設定を無効にすると、次の場所でトークンベースのリダイレクトを有効にできます。
  `Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > RD Connection Broker`。
- 接続ブローカマシンではなく、RDSH マシンで [IP アドレスリダイレクトを使用する] 設定を無効にします。
- RDP プロキシ接続用の専用リダイレクタを設定できます。

前提条件

- RDP サーバープロファイルを作成して、NetScaler Gateway 仮想サーバーで 3389 リスナーを有効にします。
  RDP するマシンが RDS 接続ブローカインフラストラクチャのメンバーでない場合は、3389 リスナーは必要ありません。
- NetScaler Gateway アプライアンスで RDP 接続リダイレクトを有効にして、接続ブローカーの存在下で RDP プロキシをサポートします。

接続ブローカの存在下で **RDP** プロキシを展開する

接続ブローカの存在下の RDP プロキシは、次の 2 つの方法で展開できます。

- RD 接続ブローカーの負荷分散に参加している RD セッションホストサーバーを使用する。
- RDP 負荷分散機能がある場合。

RD 接続ブローカーの負荷分散に参加している **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、RDP サーバの 1 つを宛先サーバとして指すように設定できます。このサーバは、リダイレクタとして機能します。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使用することもできます (この場合、サーバーは RDP セッションを受け入れません)。

RDP 負荷分散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は、NetScaler ADC で RDP 負荷分散機能を利用して、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実行できます。この場合、RDP URL リンクは、RDP ロードバランサを宛先サーバ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 NetScaler Gateway アプライアンス上に置くことができます。詳細については、「RDP サーバーの負荷分散」を参照してください。

CLI を使用して、接続ブローカの存在下で **RDP** プロキシを構成する

コマンドプロンプトで次を入力します:

```
1 add rdpserverprofile <Name> -psk <string> -rdpRedirection ( ENABLE |
     DISABLE )
2
3 add rdpserverprofile serverProfileName -psk  “secretString”  -
     rdpRedirection ENABLE
4 <!--NeedCopy-->
```

NetScaler GUI を使用して **RDP** 接続リダイレクトを構成する

1. [**NetScaler 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

February 1, 2024

NetScaler Gateway アプライアンスは、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、アプライアンスはユーザーがアクセスできるサーバーの RDP URL を表示します。

CLI を使用して LDAP 属性に基づいて RDP URL を入力するには

コマンドプロンプトで入力します:

```
add rdpclientprofile <Name>  - rdpUrlLinkAttribute <string>

add rdpclientprofile clientProfileName  - rdpUrlLinkAttribute
    rdpServerAttribute

<!--NeedCopy-->
```

前の例では、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ています。

注: LDAP サーバから LDAP 属性の詳細を取得するには、LDAP アクションを次のようにpUrlLinkAttributeで設定したのと同じ文字列で設定する必要があります。

```
add authentication ldapAction dnpg_ldap -serverIP <IP address>-ldapBase
     <"domain name"> -ldapBindDn <username> -ldapLoginName
    sAMAccountName -ldapbindDnpassword <password>

add authentication ldapAction dnpg_ldap -serverIP 10.102.39.101 -
    ldapBase "dc=dnpg-blr,dc=com" -ldapBindDn sqladmin@dnpg-blr.com -
    ldapLoginName sAMAccountName -ldapbindDnpassword xxxx

add authentication ldapPolicy dnpg_ldap_pol ns_true dnpg_ldap

bind vpn vs vserver<name> -pol dnpg_ldap_pol

set ldapaction dnpg_ldap -attributes "rdpServerAttribute"

set rdpclientprofile ldap -rdpLinkAttribute rdpServerAttribute
<!--NeedCopy-->
```

LDAP サーバ設定

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]、[詳細] の順にクリックします。
3. ユーザ名を右クリックし、[属性エディタ] をクリックします。
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

1. [**NetScaler 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 リンク属性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] ページの [**RDP** リンク属性] に、LDAP 属性名を入力します。

   注**:** LDAP 属性値は、カンマ区切りのリストにすることができます。

RDP プロキシで RDP ファイル名をランダム化する

April 1, 2024

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、新しいファイルを既存のファイルに置き換えるポップアップが表示されます。これを回避するために、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、time () 関数の出力を <rdpFileName>_<outputof time()>.rdp の形式で追加することでランダム化されます。これにより、ファイルをダウンロードするたびに、アプライアンスは一意の RDP ファイル名を生成します。

RDP プロキシを使用した RDP ファイル名のランダム化のサポートを構成する

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** プロキシを使用した **RDP** ファイル名のランダム化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-->
```

NetScaler GUI を使用して、**RDP** プロキシを使用した **RDP** ファイル名のランダム化のサポートを構成するには:

1. **[**NetScaler 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構成] ページで、[ランダム化された **RDP** ファイル名] フィールドの横のメニューで [はい] を選択します。

RDP ファイルの名前を設定する

April 1, 2024

RDP ファイルをダウンロードすると、設定したファイル名でローカルに保存できます。

RDP ファイルの名前を設定する

CLI を使用して RDP ファイルの名前を設定するには、コマンドプロンプトで次のように入力します。**:

```
set rdpclientprofile <Name> -rdpfilename <filename>.rdp
<!--NeedCopy-->
```

GUI を使用して **RDP** ファイルの名前を設定するには:

1. **[**NetScaler 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。ランダム化 RDP ファイル名機能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 **RDP** プロファイルの名前を入力します。ファイルの名前は、次の形式で指定する必要があります。名前には最大 31 文字を使用できます。

送信 **ICA** プロキシのサポート

February 1, 2024

NetScaler Gateway のアウトバウンド ICA プロキシサポートにより、ネットワーク管理者は、Receiver と NetScaler Gateway が異なる組織に展開されている場合でも、SmartControl 機能を利用することができます。

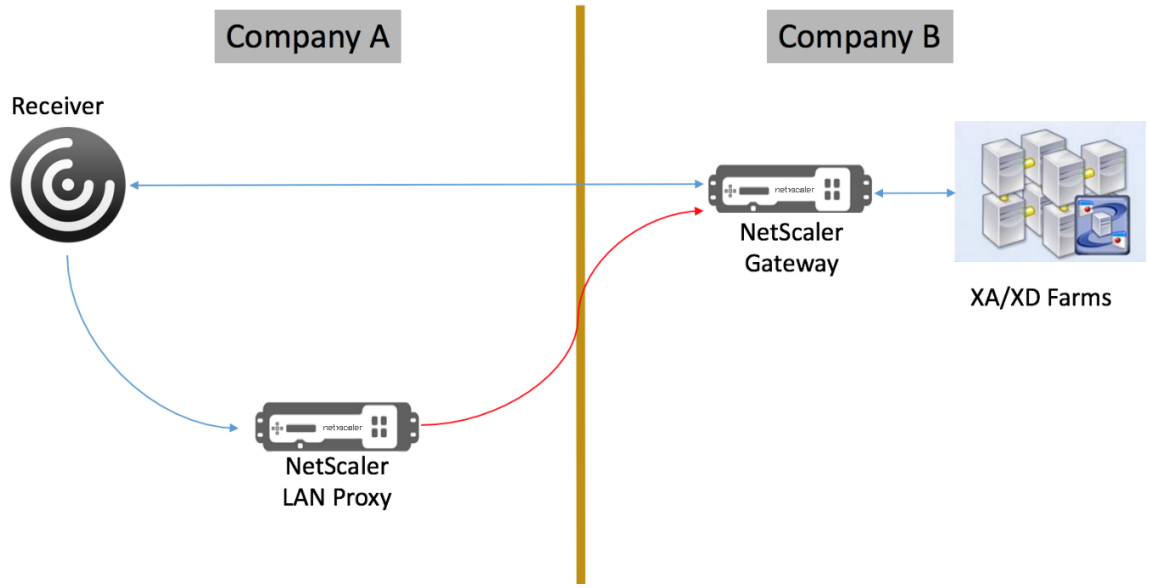
次のシナリオは、アウトバウンド ICA プロキシソリューションの使用方法を示しています。

Receiver と NetScaler Gateway が異なる組織に展開されている場合、ネットワーク管理者は、ICA セッションに関連する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

SmartControl 機能をレシーバを持つエンタープライズ組織である A 社に導入するには、LAN プロキシとして機能する NetScaler ADC アプライアンスを追加する必要があります。NetScaler LAN プロキシは SmartControl を強制し、トラフィックを B 社の NetScaler Gateway にプロキシします。この展開シナリオでは、レシーバはトラフィ

ックを NetScaler ADC LAN プロキシに転送します。これにより、A 社のネットワーク管理者は SmartControl を強制できます。次の図に、展開を示します。



このシナリオでは、LAN プロキシと NetScaler Gateway 間のトラフィックは SSL 経由です。

> 注: NetScaler Gateway でクライアント証明書ベースの認証を有効にしないでください。

NetScaler LAN プロキシでの SSL サポート

リリース 13.0 ビルド xx.xx から、Citrix Workspace アプリと NetScaler ADC LAN プロキシ間のトラフィックは、SSL 経由でもサポートされています。Citrix Workspace アプリは、SSL 経由で LAN プロキシに送信するトラフィックを暗号化します。LAN プロキシでの SSL サポートは、既存の展開と共存できます。

Citrix Workspace アプリと NetScaler ADC LAN プロキシ間の SSL を介したトラフィック暗号化を有効にするには、NetScaler LAN プロキシで以下を実行する必要があります。

- VPN 仮想サーバーで認証を無効にし、ダブルホップを有効にします。
- Windows クライアント上のホストを VPN 仮想サーバの IP アドレスに設定します。
- SNI と証明書の検証を有効にします。
- 適切な CA 証明書を追加し、グローバルに有効にします。

アウトバウンド ICA プロキシの構成

April 1, 2024

アウトバウンド ICA プロキシ構成には、NetScaler LAN プロキシと NetScaler Gateway の構成が含まれます。

ICA アウトバウンドプロキシ用の NetScaler ADC LAN プロキシを構成する

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、次の手順を実行します。

- VPN 仮想サーバーを追加します。

```
add vpn vserver <name> <serviceType> [<IPAddress> [-range <
    positive_integer>] [-ipset <string>]] [<port>] [-state (
    ENABLED | DISABLED )] [-authentication ( ON | OFF )] [-
    doubleHop ( ENABLED |DISABLED )]
<!--NeedCopy-->
```

- VPN パラメータを設定します。

```
set vpn parameter[-backendServerSni ( ENABLED | DISABLED )][-
    backendCertValidation ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

- SSL 証明書とキーのペアを追加します。

```
add ssl certKey ca_cert_verify -cert <certificate name>
<!--NeedCopy-->
```

- SSL 証明書とキーのペアをグローバルにバインドします。

```
bind vpn global -cacert ca_cert_verify
<!--NeedCopy-->
```

例:

```
-  add vpn vserver ssl_lan_proxy SSL 65.219.17.34 443 -authentication
    OFF - doubleHop ENABLED

-  set vpn parameter backendserverSni ENABLED backendcertValidation
    ENABLED

-  add ssl certKey dnpg_ca -cert dnpg_ca_cert.cer

-  bind vpn global -cacert dnpg_ca

<!--NeedCopy-->
```

> 注:
>
> NetScaler LAN プロキシで SSL をサポートする場合、NetScaler Gateway の構成を変更する必要はありません。

NetScaler Gateway 対応の PCoIP プロキシサポート（VMware Horizon View）

February 1, 2024

NetScaler Gateway 12.0 は、PC-over-IP（PCoIP）プロトコルをサポートしています。PCoIP 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 プロトコルに似ています。PCoIP は UDP ポート 4172 を使用します。

PCoIP が NetScaler Gateway を介してプロキシされると、NetScaler Gateway は、View セキュリティサーバーや 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。

次のシナリオは、**NetScaler Gateway** 対応の **VMware Horizon View** ソリューションの使用を示しています。

- VMware Horizon PCoIP ユーザーは、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、NetScaler 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ります。
- PCoIP ユーザーは、NetScaler 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
>
> NetScaler 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。

NetScaler Gateway が有効な PCoIP プロキシを VMware Horizon View 用に構成する

April 1, 2024

前提条件

バージョン -NetScaler 12.0 以上

ユニバーサルライセンス -PCoIP プロキシは、NetScaler 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 NetScaler Gateway 接続には、NetScaler Gateway ユニバーサルのライセンスが必要です。NetScaler 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 -Horizon View の内部インフラストラクチャの機能 NetScaler Gateway なしで内部で Horizon View エージェントに接続できることを確認します。NetScaler が接続をプロキシする View

接続サーバで、Horizon View **HTTP (S)** セキュアトンネルおよび **PCoIP** セキュアゲートウェイが有効になっていないことを確認します。
VMware Horizon ビューの次のバージョン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、Horizon View クライアントから NetScaler Gateway VIP に開かれている。
- UDP 4172 は、NetScaler SNIP からすべての内部の Horizon View エージェントに対して開い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 NetScaler 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 仮想サーバーの 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 はサポートしない
  - 443 ポートと 4172 ポートのみをサポート
  - スタティック NAT である必要がある

証明書 -NetScaler Gateway 仮想サーバーに対して有効な証明書です。

認証—高度な構文を使用した LDAP 認証ポリシー/サーバー。

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 ポータルテーマ—Web ブラウザで Horizon View にアクセスするには、NetScaler Gateway 仮想サーバを RfWebUI テーマで構成する必要があります。

Horizon View クライアント -NetScaler RfWebUI ポータルを使用して Horizon 公開アイコンにアクセスする場合でも、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 View の **PCoIP** プロキシをサポートするように **NetScaler Gateway** を構成するには:

1. ［構成］**>** ［**NetScaler Gateway** ポリシー］**>** ［**PCoIP**］に移動します。
2. [PCoIP プロファイルと接続**]** ページで、仮想サーバープロファイルと **PCoIP** プロファイルを作成します。
   a) 仮想サーバープロファイルを作成するには、[仮想サーバープロファイル] タブで、[追加] をクリックします。
   b) 仮想サーバプロファイルの名前を入力します。
   c) 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： NetScaler Gateway 仮想サーバーごとにサポートされる Active Directory y ドメインは 1 つだけです。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。

d) [ログイン] をクリックします。

e) 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。

   i. PCoIP プロファイルの名前を入力します。

   ii. 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。

f) ［構成］**>**［**NetScaler Gateway**］**>**［ポリシー］［セッション］に移動します。

g) 右側の [セッションプロファイル] タブを選択します。

h) ［**NetScaler Gateway** セッションポリシーとプロファイル］ページで、NetScaler Gateway セッションプロファイルを作成または編集します。

   i. NetScaler 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入力します。

   ii. NetScaler 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。

i) [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。

j) [セキュリティ] タブで、[既定の承認アクション] の値が [許可] に設定されていることを確認します。

k) [**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。

l)「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。

m) 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。

   i. ［構成］**>**［**NetScaler Gateway**］**>**［ポリシー］［セッション］に移動します。

   ii. [セッションポリシー] タブを選択し、[追加] をクリックします。

   iii. ［NetScaler Gateway セッションポリシーの作成］ページで、ポリシーの名前を入力します。

   iv. [プロファイル] で、既存のプロファイルを選択するか、[追加] をクリックしてプロファイルを作成します。

   v. 式を追加します。

      A. ［高度なポリシー］をクリックし、［式エディター］をクリックします。
      B. [式] で、要件に従って式を選択します。

   vi.「**OK**」をクリックします。

n) 作成した PCoIP 仮想サーバープロファイルとセッションポリシーを NetScaler Gateway 仮想サーバーにバインドします。

i. ［**NetScaler Gateway**］**>**［仮想サーバー］に移動します。

ii. 右側の［新しい Citrix **Gateway** 仮想サーバーを追加する］または［既存の Citrix **Gateway** 仮想サーバーを編集する］のいずれかです。

iii. 既存の NetScaler 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。

iv. 追加と編集の両方で、[基本設定] セクションの [詳細] をクリックします。

v. **PCoIP** 仮想サーバープロファイルメニューを使用して、必要な PCoIP 仮想サーバープロファイルを選択します。

vi. 下にスクロールして、[ICA Only] 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。

vii. NetScaler 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。

viii. [**Policies**] セクションまでスクロールダウンし、プラスアイコンをクリックします。

ix.「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。

x. [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。

xi. 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、[選択（**Select**）] をクリックします。

xii. [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。

xiii. Web ブラウザを使用して VMware Horizon View に接続する場合は、[詳細設定] で [ポータルテーマ] セクションを追加します。Horizon View Client のみを使用して NetScaler Gateway に接続している場合は、この手順を実行する必要はありません。

xiv. ポータル・テーマ・メニューを使用して「**RfWebUI** 」を選択し、「**OK**」をクリックします。

xv. Horizon View の公開済みアイコンが rfWebI ポータルに追加されます。

> 注： VMware は、RDP 以外のプロトコルを使用する場合、2 つ以上のプロトコルを使用します。これにより、2 つの異なるバックエンドサーバー間で要求の負荷が分散される可能性があります。この問題を解決するには、すべてのプロトコルで単一の永続性グループを設定して、すべての接続を同じ Citrix 仮想サーバー上に維持します。

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 デバイスは、仮想デスクトップおよび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**] > [**設定サーバの表示**]** に移動します。
3. [接続サーバ] タブを選択します。
4. 一覧表示された接続サーバを選択し、[編集] をクリックします。
5. [全般] タブで、[**HTTP (S) **** セキュアトンネル**]** の下にある **[**マシンへのセキュアな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 **NetScaler Gateway **** の外部 **URL** を入力します。

Unified Gateway のコンテンツスイッチング式の更新

NetScaler Gateway 仮想サーバーが Unified Gateway（コンテンツスイッチ仮想サーバー）の背後にある場合は、PCoIP URL パスを含めるようにコンテンツスイッチング式を更新する必要があります。

1. NetScaler GUI で、［構成］**>**［トラフィック管理］**>**［コンテンツスイッチング］**>**［ポリシー］に移動します。
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.path.eq (「/broker/xml」)	http.req.url.path.contains(「/broker/resources」)	http.req.url.path.eq (「/pcoip-client」)

PCoIP ゲートウェイを使用する

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 Client のユーザーインターフェイスを使用して NetScaler Gateway に接続するか、NetScaler Gateway の 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、**NetScaler Gateway >**［**PCoIP**］に移動します。
3. 右側で、[接続] タブに切り替えます。アクティブなセッションは、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、[****** 接続の終了**]** をクリックします。または、**[**** すべての接続を強制終了] 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

February 1, 2024

NetScaler 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. [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. 一覧表示された接続サーバを選択し、[編集] 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な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. リストされているすべての接続サーバで、4 ～6 の手順を実行します。

NetScaler Gateway の送信プロキシサポートのプロキシ自動構成

February 1, 2024

プロキシ自動構成（PAC）をサポートするように NetScaler 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、送信プロキシ用の PAC の一般的なユースケースをいくつか示します。

- 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の負荷分散を行うため。

CLI を使用して送信プロキシの **PAC** をサポートするように **NetScaler Gateway** グローバルパラメーターを構成する

コマンドプロンプトで入力します:

```
set vpn parameter -proxy BROWSER -autoProxyUrl <URL>
<!--NeedCopy-->
```

CLI を使用してセッションプロファイルで **PAC** をサポートするように **NetScaler Gateway** を構成する

コマンドプロンプトで入力します:

```
add vpn sessionAction <name> -proxy BROWSER -autoProxyUrl <URL>
<!--NeedCopy-->
```

どこ;

- **URL** —プロキシサーバーの URL
- **Name**： VPN セッションアクションの名前

GUI を使用して送信プロキシの **PAC** をサポートするように **NetScaler Gateway** グローバルパラメーターを構成する

1. 構成 **> NetScaler 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、[自動構成を使用する] を選択 します。
5. [自動プロキシ構成ファイルへの **URL**] フィールドに、必要な PAC ファイルの URL を入力します。
6. [**Create**] をクリックします。

GUI を使用してセッションプロファイルで **PAC** をサポートするように **NetScaler Gateway** を構成する

1. 構成 **> NetScaler Gateway >** ポリシー **>** セッションに移動します。
2. [NetScaler Gateway セッションポリシーとプロファイル] ページで、NetScaler Gateway セッションプロファイルを作成します。
3. [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。
4. [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。
5.「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。
6. [自動プロキシ構成ファイルへの **URL**] フィールドに、必要な PAC ファイルの URL を入力します。
7. [**Create**] をクリックします。
8. [**Create**] をクリックします。

SameSite Cookie 属性の構成サポート

April 1, 2024

`SameSite`属性は、Cookie をクロスサイトコンテキストに使用するか、同一サイトコンテキストにのみ使用できるかをブラウザに示します。アプリケーションがクロスサイトコンテキストでアクセスされる場合は、HTTPS 接続を介してのみアクセスできます。詳細については、RFC6265 を参照してください。

2020 年 2 月まで、`SameSite`属性は NetScaler ADC アプライアンスで明示的に設定されていませんでした。ブラウザはデフォルト値 (None) を使用しました。`SameSite`属性の設定なしは、NetScaler Gateway および NetScaler AAA 展開には影響しませんでした。

Google Chrome 80 などの特定のブラウザのアップグレードでは、Cookie のデフォルトのクロスドメイン動作に変更があります。`SameSite` この属性は、次のいずれかの値に設定できます。Google Chrome のデフォルト値は Lax に設定されています。他のブラウザーの特定のバージョンでは、`SameSite`属性のデフォルト値がまだ None に設定されている場合があります。

- なし: ブラウザーが安全な接続でのみクロスサイトコンテキストで Cookie を使用することを示します。
- **Lax**: ブラウザが同一サイトコンテキストのリクエストに Cookie を使用することを示します。クロスサイトコンテキストでは、GET リクエストなどの安全な HTTP メソッドのみが Cookie を使用できます。
- 厳格:Cookie は同じサイトコンテキストでのみ使用します。

クッキーにSameSite属性がない場合、Google Chrome は SameSite = Lax の機能性を前提としています。その結果、ブラウザーによって Cookie を挿入する必要があるクロスサイトコンテキストを持つ iframe 内の展開では、Google Chrome はクロスサイト Cookie を共有しません。その結果、Web サイト内の iframe が読み込まれないことがあります。

SameSite Cookie 属性を設定する

SameSite という名前の新しいクッキー属性が、VPN および NetScaler AAA 仮想サーバに追加されます。この属性は、グローバルレベルおよび仮想サーバレベルで設定できます。

SameSite属性を設定するには、次の手順を実行する必要があります。

1. 仮想サーバのSameSite属性を設定する
2. クッキーをpatsetにバインドする（ブラウザがクロスサイトクッキーをドロップした場合、ブラウザによってドロップされる）

CLI を使用した SameSite 属性の設定

仮想サーバレベルでSameSite属性を設定するには、次のコマンドを使用します。

```
set vpn vserver VP1 -SameSite  [ STRICT | LAX | None ]
set aaa vserver VP1 -SameSite  [ STRICT | LAX | None ]
<!--NeedCopy-->
```

グローバルレベルでSameSite属性を設定するには、次のコマンドを使用します。

```
set vpn param VP1 -SameSite  [ STRICT | LAX | None ]
set aaa param VP1 -SameSite  [ STRICT | LAX | None ]
<!--NeedCopy-->
```

注：仮想サーバーレベルの設定は、グローバルレベル設定よりも優先されます。SameSiteCookie 属性を仮想サーバーレベルで設定することをお勧めします。

CLI を使用したへの patset Cookie のバインド

ブラウザーがクロスサイト Cookie をドロップした場合､その Cookie 文字列を既存のns_cookies_SameSite patsetにバインドして、SameSite属性が Cookie に追加されるようにすることができます。

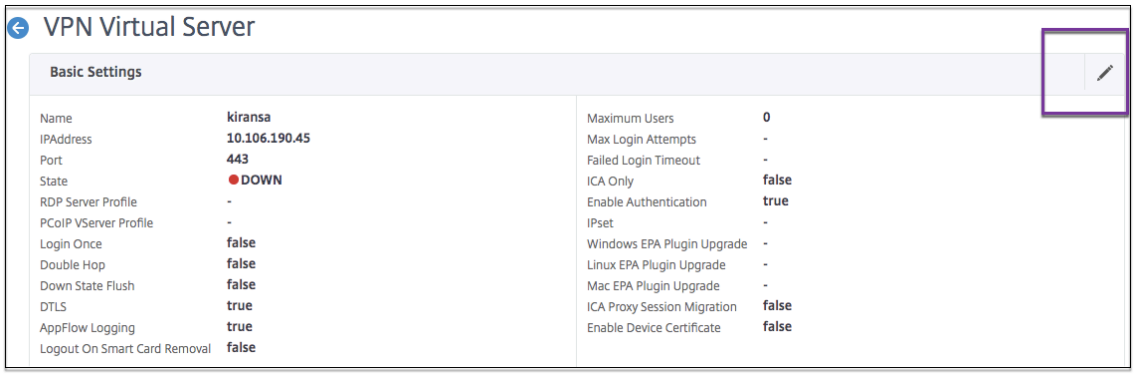
例:


```
bind patset ns_cookies_SameSite "NSC_TASS"
bind patset ns_cookies_SameSite "NSC_TMAS"
<!--NeedCopy-->
```

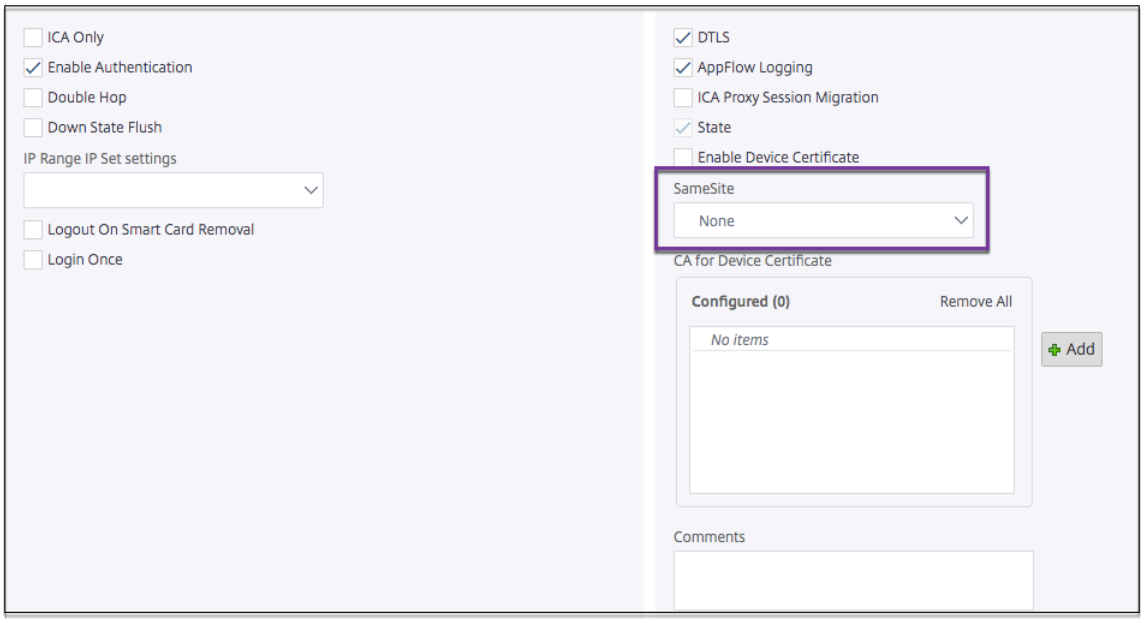
GUI を使用して **sameSite** 属性を設定する

仮想サーバレベルで**SameSite**属性を設定するには、次の手順を実行します。

1. 「**NetScaler Gateway**」**>**「仮想サーバー」に移動します。
2. 仮想サーバを選択し、[編集（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選択し、[詳細] をクリックします。



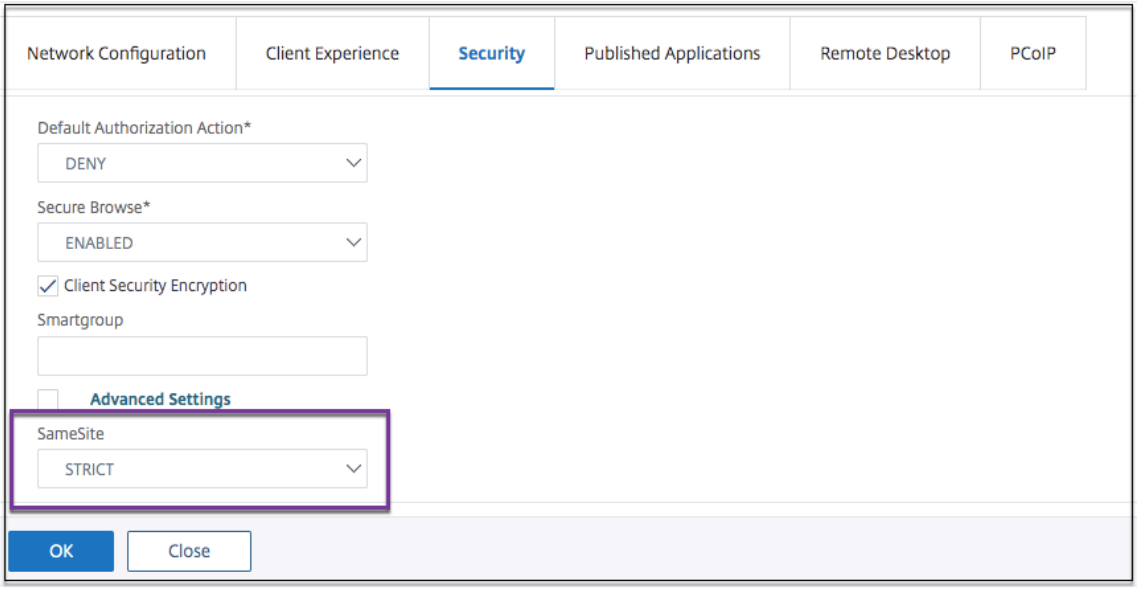
4. **SameSite** で、必要に応じてオプションを選択します。



グローバルレベルで**SameSite**属性を設定するには、次の手順を実行します。

1. [**NetScaler Gateway**] **>** [グローバル設定] **>** [グローバル設定の変更] に移動します。

2. ［セキュリティ］タブをクリックします。
3. **SameSite**で、必要に応じてオプションを選択します。



ゲートウェイ **UX** 構成での **RfWebUI** ペルソナ

April 1, 2024

RFWebI ペルソナは、NetScaler Gateway を介してログオンする NetScaler Gateway ユーザーに新しいログオンおよび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、これらの製品のいずれかに直接アクセスする場合と同じ GUI が表示されます。

RfWebUI ペルソナを使用する時は

NetScaler Gateway の RfWebUI ペルソナは、Web アプリケーションやサービスとしてのソフトウェア（SaaS）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、さまざまな NetScaler 製品によって提供されるすべてのアプリケーションを一元的に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 なしで製品にアクセスしたときに表示される GUI とは異なる GUI が見つかります。
  解決方法: ユーザーがゲートウェイを使用して 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。
- ユーザーが 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ていないため、目的

のアプリケーションを見つけるのに苦労します。
解決策： RfWebUI ペルソナは、Receiver、StoreFront、Citrix Endpoint Management などのさまざまな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により、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 ペルソナによって提供される機能

新しい RfWebUI は次の機能を提供します。

- GO
- アプリケーションの集約
- ユーザー構成リモートデスクトッププロトコル (RDP) プロキシリンク
- お気に入りのアプリケーション

GO

GO： Go 機能は、クライアントレス VPN 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**」をクリックするだけです。

現在、移動機能は Outlook Web アプリケーション (OWA) と SharePoint の URL のみをサポートしています。

> 注**:**
> [移動] タブは、`clientlessAccessVPNMode` セッションポリシーのパラメータが [有効] の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、異なる製品によって提供されるアプリケーションを説明的なバナーの下に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、NetScaler ADC 管理者によって構成されたすべての VPN URL は、**Web** 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、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。Citrix Virtual Apps and Desktops アプリケーションバンドルが StoreFront で構成されている場合、NetScaler 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 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は、[デスクトップ] タブの下に表示されます。

次の RDP モードがサポートされています。

- シングルゲートウェイ
- ステートレス (デュアル) ゲートウェイ

> 注**:** RDP プロキシリンクを追加できるのは、`RDPclientprofile`が設定されている場合だけです。RDP 構成の詳細については、RDP Proxy 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] および [個人用ブックマーク] の下に表示されている目的のアプリケーションを **[**お気に入り**]** タブに追加できます。一度追加されたアプリケーションは、[お気に入り] タブの下に表示されます。また、［お気に入り］タブ内のアプリケーションの横にある［削除］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もできます。

RfWebUI ペルソナを有効にする際の考慮事項

RfWebUI ペルソナは、以下を完全にはサポートしていません。

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、NetScaler Gateway ポータルの埋め込みビューとしては使用できません。RfWebUI の APPS タブにある **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. NetScaler ADC インターフェイスで、［構成］**>**［**NetScaler 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オンにします。
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。

RfWebUI 設定パラメーター

April 1, 2024

NetScaler Gateway ポータルの全体的な動作は、ローカル NetScaler Gateway 構成ファイルと StoreFront ファイルの 2 つの構成ファイルの影響を受けます。

展開環境に応じて、”plugins.xml”ファイルのプロパティを変更して、NetScaler Gateway ポータルの動作を変更できます。このファイルは、/var/netscaler/logon/themes/<custom_theme>/plugins.xmlのリクエストであるブラウザの設定ファイルとして表示されます。

ログオン中は、NetScaler Gateway 構成ファイルが使用されます。ただし、StoreFront に接続すると、StoreFront は新しい構成を送信し、以前の構成は上書きされます。この動作は、クライアントレス VPN と ICA では異なります。

ICA の場合、StoreFront 構成が常に優先されますが、NetScaler Gateway 構成の影響を受けるクライアントレス VPN の一部の動作は、新しい構成が StoreFront から更新された後でも保持されます。

次の表に、クライアントレス VPN および ICA よりも優先される設定を記述するパラメータを示します。

コンフィグタイプ	サブコンフィグタイプ	パラメーター	クライアントレス VPN	ICA	説明
クライアントレス VPN のセッション/認証マネージャ for ICA	-	loginFormTimeout	NetScaler Gateway	-	ログオンページのタイムアウト時間を分単位で定義します
プラグインアシスタント	-	enabled	StoreFront	StoreFront	プラグインアシスタントを有効または無効にする
プラグインアシスタント	-	upgradeAtLogin	StoreFront	StoreFront	ログイン時にプラグインのアップグレードを促す
プラグインアシスタント	-	showAfterLogin	NetScaler Gateway	StoreFront	ログイン後にプラグインプロンプトを表示します
プラグインアシスタント	-	showOnlyIfRequiredByApps	NetScaler Gateway	StoreFront	アプリで必要な場合、ログイン後にプラグインプロンプトを表示します
プラグインアシスタント	macOS/win32	path	NetScaler Gateway	StoreFront	プラグインのダウンロードパスを定義します

コンフィグタイプ	サブコンフィグタイプ	パラメーター	クライアントレス VPN	ICA	説明
プラグインアシスタント	protocolHandler	enabled	NetScaler Gateway	StoreFront	プラグインを起動する前にプロトコルハンドラページを切り替える
プラグインアシスタント	protocolHandler	platforms	NetScaler Gateway	StoreFront	プラグインでサポートされるプラットフォームを識別します
プラグインアシスタント	-	skipDoubleHopCheck	WhenDisabled • NetScaler Gateway	StoreFront	ICA パススルーのダブルホップ NetScaler Gateway 構成チェックを切り替えます
ユーザーインターフェイス	-	frameOptions	-	-	-
ユーザーインターフェイス		autoLaunchDesktop	StoreFront	StoreFront	デスクトップ起動を有効または無効にする
ユーザーインターフェイス	workspaceControl	enabled	StoreFront	StoreFront	ワークスペースコントロールを有効または無効にする
ユーザーインターフェイス	workspaceControl	autoReconnectAtLogon	StoreFront	StoreFront	可能であれば、前のセッションを自動再接続するように切り替えます
ユーザーインターフェイス	workspaceControl	logoffAction	StoreFront	StoreFront	Citrix Workspace のログオフ動作を定義します
ユーザーインターフェイス	workspaceControl	showReconnectButton	StoreFront	StoreFront	再接続ボタンを表示または非表示にする

コンフィグタイプ	サブコンフィグタイプ	パラメーター	クライアントレス VPN	ICA	説明
ユーザーインターフェイス	workspaceControl	showDisconnectButton	StoreFront	StoreFront	切断ボタンを表示または非表示にする
ユーザーインターフェイス	workspaceControl	showDesktopsView	StoreFront	StoreFront	[デスクトップ] ビューを表示または非表示にする
ユーザーインターフェイス	workspaceControl	showappsView	StoreFront	StoreFront	アプリビューを表示または非表示にする
ユーザーインターフェイス	workspaceControl	defaultView	StoreFront	StoreFront	デスクトップビューまたはアプリビューのいずれかを選択します
ユーザーインターフェイス	receiverConfiguration	enabled	StoreFront	StoreFront	受信機の構成を切り替える
ユーザーインターフェイス	receiverConfiguration	showOnlyIfRequiredByApps	NetScaler Gateway	NetScaler Gateway	アプリが必要とする場合は受信機プロンプトを表示する
ユーザーインターフェイス	receiverConfiguration	downloadURL	StoreFront	StoreFront	受信者の URL をダウンロードする
ユーザーインターフェイス	appShortcuts	enabled	StoreFront	StoreFront	アプリのショートカットタブを有効または無効にする
ユーザーインターフェイス	appShortcuts	allowSessionReconnect	StoreFront	StoreFront	セッションの再接続を許可する

カスタムプラグインを使用したゲートウェイポータルのカスタマイズ

April 1, 2024

NetScaler Gateway RFWebI フレームワークは、カスタムプラグインを追加してゲートウェイポータルをカスタマイズする機能を提供します。これらのカスタムプラグインは、ゲートウェイフローに新しいページ全体を追加する場合など、ゲートウェイに大規模な機能を追加するために使用できます。その他のユースケースでは、ゲートウェイテーマ用のカスタムスクリプトファイルに、/var/netscaler/logon/themes/<custom_theme>/script.jsという場所にあるコードを追加できます。

1. カスタムプラグインを追加するには、その場所/var/netscaler/logon/LogonPoint/plugins/ns-gateway/に JavaScript ファイルを作成します。たとえば、/var/netscaler/logon/LogonPoint/plugins/ns-gateway/には次のプラグインがあります。

   - ns-nfactor.js
   - nsg-epa.js
   - nsg-setclient.js

   プラグイン名は、<plugin_name>.js の形式で入力することをお勧めします。

   これらのプラグインファイルはすべて、機能に必要な RfWebUI フレームワークによって取得されます。

2. プラグインファイルを作成したら、次のコードを例として使用して、プラグインを RfWebUI フレームワークに登録します。

```
1          (function ($) {
2
3                       CTXS.ExtensionAPI.addPlugin( {
4
5                                   Name :  “plugin name” ,
6                                   initialize: function() {
7    }
8
9                        }
10  );
11              }
12  )(jQuery);
13 <!--NeedCopy-->
```

   各項目の意味は次のとおりです。

   name は、プラグインに付けられた名前です。これは、プラグインの識別子として使用されます。

   initialize は、プラグインの初期化に使用されるパラメータとして関数を取ります。

3. プラグインを登録するCTXS.ExtensionAPI.addPlugin()関数に、プラグイン名と初期化関数を入力します。
   追加したプラグインの名前と場所は、その場所/var/netscaler/logon/themes/<custom_theme>/plugins.xmlの plugins.xml ファイルに登録する必要があります。

4. プラグインコードを記述したら、新しく追加したプラグインの名前と場所を、その場所/var/netscaler/logon/themes/<custom_theme>/plugins.xmlのplugins.xmlファイルに登録する必要があります。プラグインは、plug-in タグで登録する必要があります。


```
<plugins>
<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js"/>
<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient.js"/>
<plugin name="ns-nfactorn" src="plugins/ns-gateway/ns-nfactor.js" />
</plugins>
<!--NeedCopy-->
```

5. RfWebUI がプラグインを識別して取得できるように、プラグインの名前と src を入力します。

設定例

次の構成例を使用して、カスタムプラグインを追加して、NetScaler Gateway ログオンページにフッターを追加できます。

1. 次の場所に JavaScript プラグインファイルを作成します。/var/netscaler/logon/LogonPoint/plugins/ns-gateway/.
2. プラグインに ns-footer.js /var/netscaler/logon/LogonPoint/plugins/ns-gateway/ns-footer.jsという名前を付けます。
3. 登録されたプラグインに次のコードを RfWebUI に追加し、初期化関数でゲートウェイにフッターを追加します。

```
(function ($) {

CTXS.ExtensionAPI.addPlugin({

    name: "ns-footer", // Name of plugin - must match name sent in configuration
    initialize: function () {

        CTXS.Extensions.beforeLogon = function (callback) {

            $("#customExplicitAuthBottom").append("<div style='text-align:center;color:white;font-size:15px;'><br>Disclaimer<BR><BR>"+
                " Access to this website is restricted to employees of Login Consultants<BR></div>");
            callback();
         }
;
     }

}
);
}
```

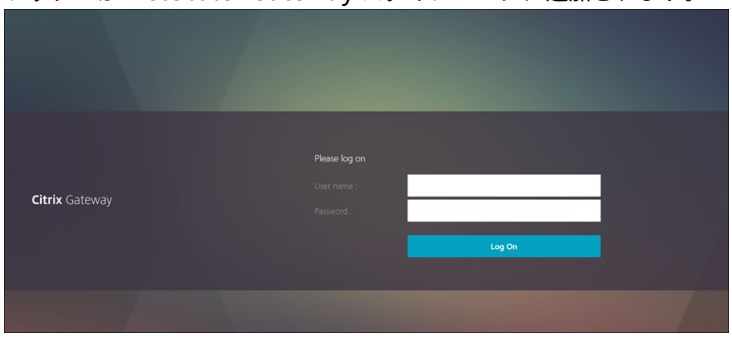


```
20   )(jQuery);
21  <!--NeedCopy-->
```

4. ファイルを保存します。
5. その場所var/netscaler/logon/themes/<custom_theme>/plugins.xmlの plug-ins.xml に name と src を追加します。

```
1  <plugins>
2  <plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js" />
3  <plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient
       .js" />
4  <plugin name="ns-nfactor" src="plugins/ns-gateway/ns-nfactor.js"
       />
5  <plugin name="ns-footer" src="plugins/ns-gateway/ns-footer.js" />
6  </plugins>
7  <!--NeedCopy-->
```

6. プラグインを追加するカスタムテーマを設定します。
7. flush cache contentgroup loginstaticobjectsコマンドを使用してキャッシュをフラッシュします。
8. ポータル画面をリロードします。
   フッターが NetScaler Gateway ログインページに追加されます。



ログインスキーマの作成とカスタマイズ

February 1, 2024

ログインスキーマは、フォームベース認証の構造を提供する XML ファイルです。
ユーザーは、基本的な HTML フォームに似た一連のユーザーインターフェイス構造を使用して、幅広い認証フォームを使用できます。

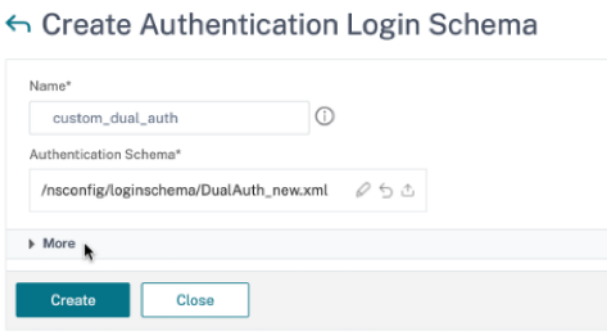
nFactor 認証では、認証要素は連鎖されます。各ファクタは、異なるログインスキーマページまたはファイルを持つことができます。一部の認証シナリオでは、ユーザーに複数のログオン画面を表示することができます。また、1 つ

のログインスキーマで複数のファクタに渡すことができる情報を収集して、後者のファクタが別のログインスキーマを表示する必要がないようにすることもできます。

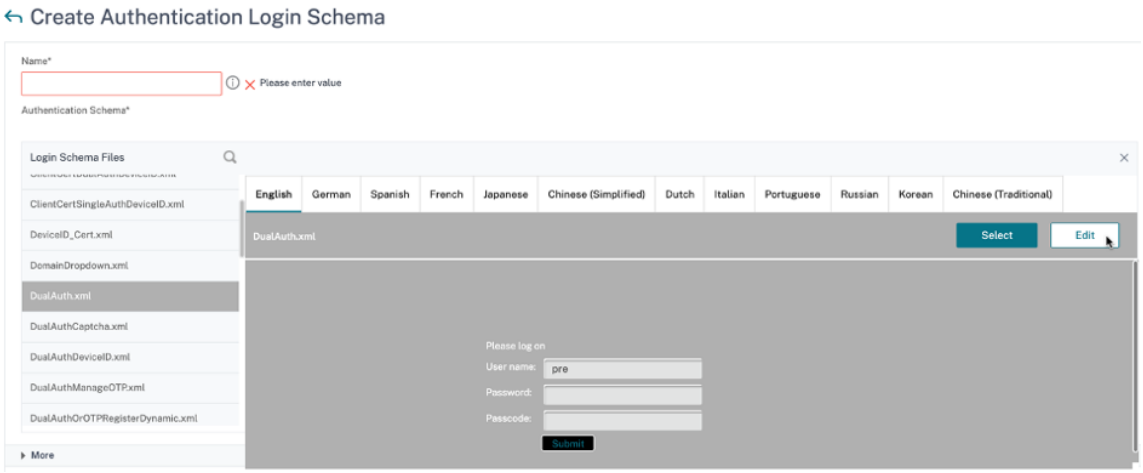
ログインスキーマの XML ファイルは、/nsconfig/loginschema/LoginSchemaの NetScaler ADC アプライアンスに含まれています。

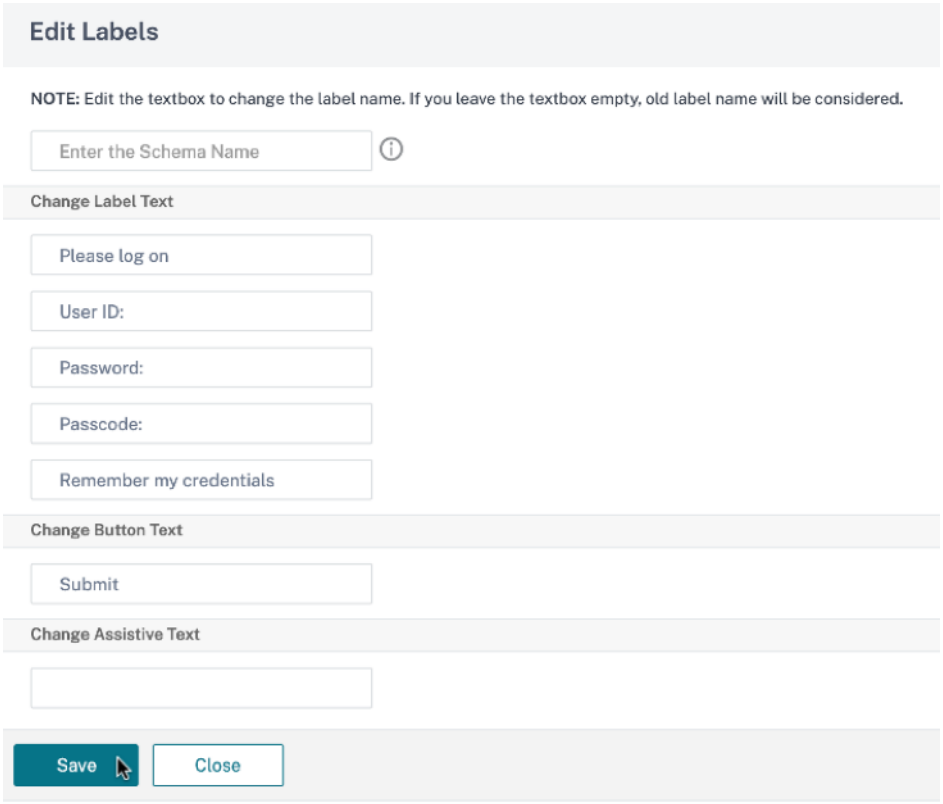
ログインスキーマプロファイルの作成

1. セキュリティ **> AAA >** ログインスキーマに移動します。
2. [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. [認証スキーマ] で、鉛筆アイコンをクリックします。



4. **LoginSchema** フォルダをクリックして、フォルダ内のファイルを表示します。
5. ファイルの 1 つを選択し、必要に応じて変更を実行します。
   - 右上の [編集] ボタンをクリックして、ラベルを変更します。
   - 言語を選択してスキームを編集します。

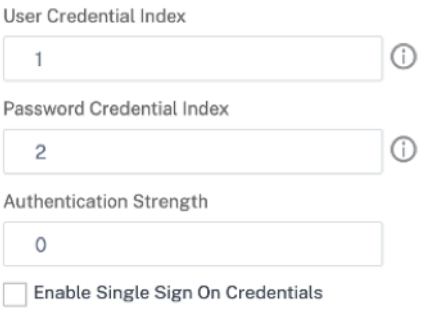


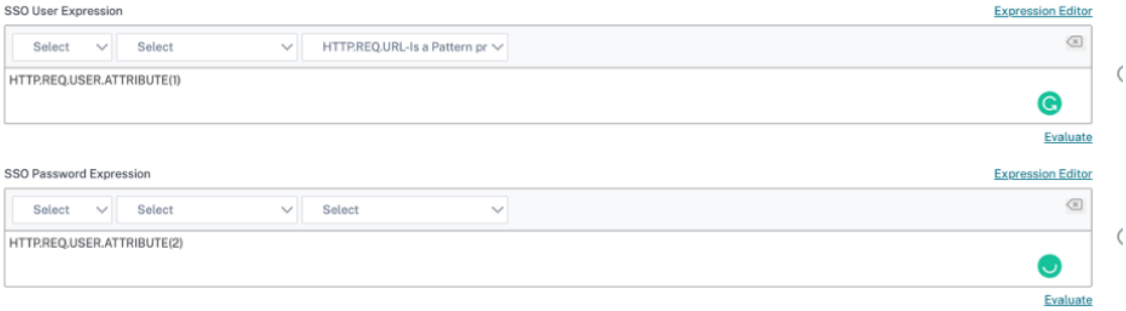


注**:** 変更後に変更を保存すると、変更内容を含む新しいスキーマ XML ファイルが作成されます。

6. 右上の [選択] をクリックして、変更したスキーマ XML を選択します。
7. ログインスキーマ名を入力し、[**More**] をクリックします。

   注**:** 既に入力された認証情報は他の場所で使用できます。たとえば、StoreFront へのシングルサインオンには、ユーザー名とパスワードのいずれかを使用できます。[詳細] をクリックして、インデックスに一意の値を入力できます。これらの値は 1 ～16 の範囲です。REQ.USER.ATTRIBUTE (#) という式を使用して、トラフィックポリシーまたはプロファイルでこれらのインデックス値を参照できます。





8. [**Create**] をクリックして、ログインスキーマプロファイルを作成します。

ログインスキーマプロファイルを認証、承認、および監査仮想サーバーにバインドする

ログインスキーマプロファイルを認証、承認、および監査仮想サーバーにバインドするには、最初にログインスキーマポリシーを作成する必要があります。ログインスキーマポリシーは、ログインスキーマプロファイルを認証ポリシーラベルにバインドするときには必要ありません。

ログインスキーマポリシーを作成してバインドするには、次の手順に従います。

1. セキュリティ **> AAA >** ログインスキーマに移動します。
2. [ポリシー] 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」で、以前に作成したログインスキーマプロファイルを選択します。
4.「ルール」に、デフォルトの構文式を入力し、「作成」をクリックします。

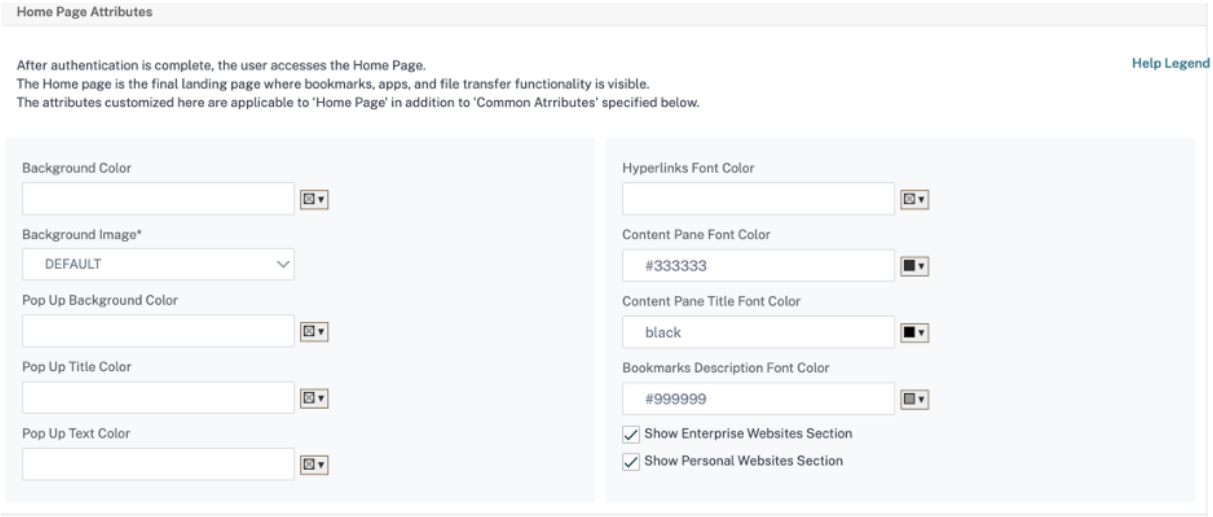
管理 **UI** からのポータルのカスタマイズ

April 1, 2024

管理者は、カスタムテーマを作成してポータルテーマをカスタマイズし、ユーザーポータルのルックアンドフィールをパーソナライズできます。カスタムテーマは、RfWebUI、Default、X1、および GreenBubble テーマに基づいて作成できます。

カスタムテーマを作成するには**:**

1.［構成］タブで、［**NetScaler Gateway**］**>**［ポータルテーマ］に移動し、［追加］をクリックします。
2. カスタムテーマの名前を入力します。
3. [テンプレートテーマ] で、必要に応じてベーステーマを選択します。**RfWebUI** はデフォルトで選択されています。
4.［**OK**］をクリックします。
5.「**Look &** Feel」セクションで、ホームページの要件に従って属性を変更し、「**OK**」をクリックします。

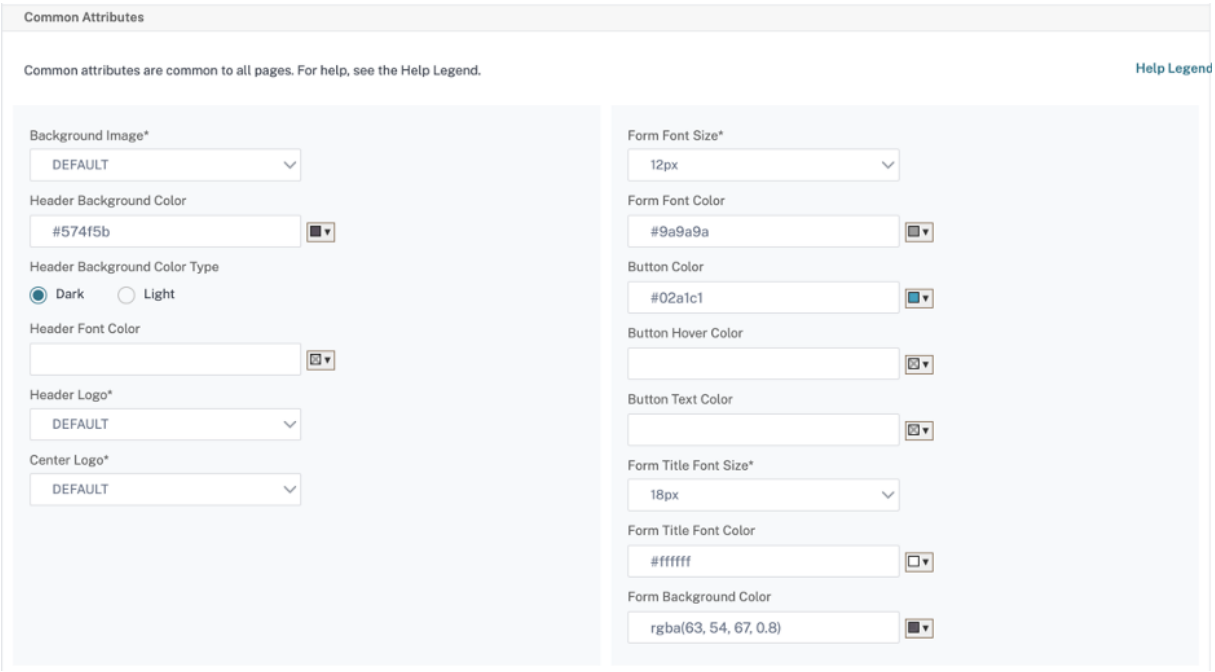


次の図に、RfWebUI ベースのカスタムテーマを示します。

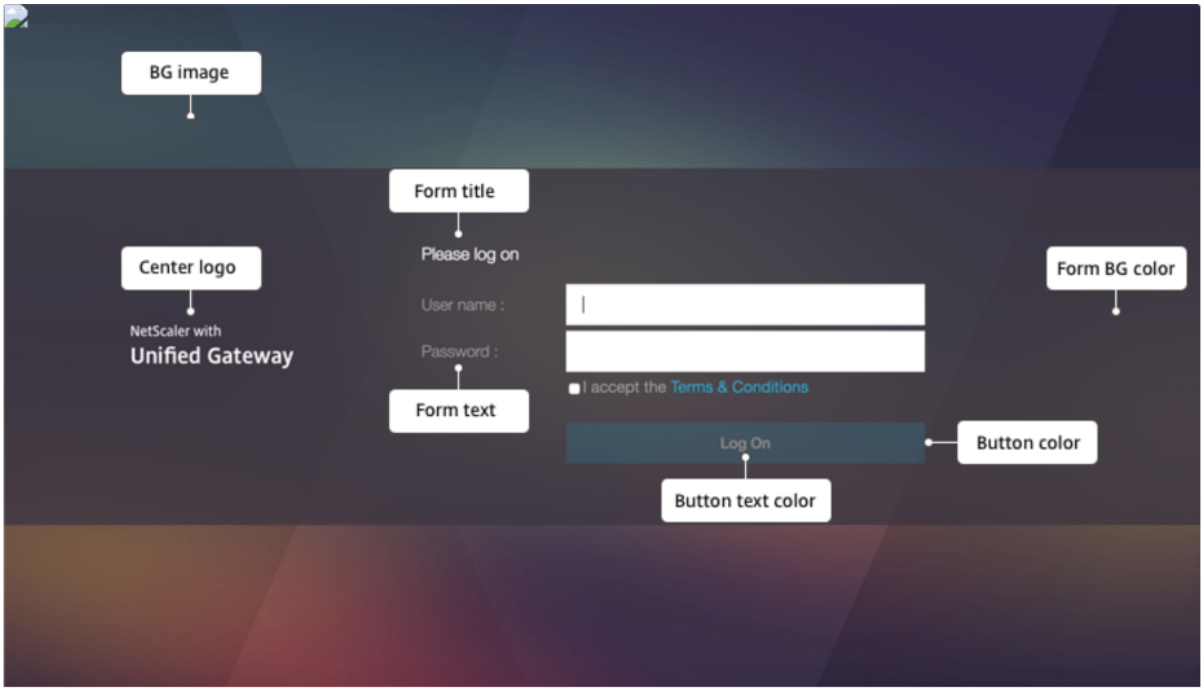
[**Help Legend**] リンクをクリックすると、編集する内容を選択しやすくするために、セクション名を含むグラフィカルなページが表示されます。

共通属性

[共通属性] セクションには、すべての NetScaler Gateway ログオンページに共通する構成可能な設定が表示されます。

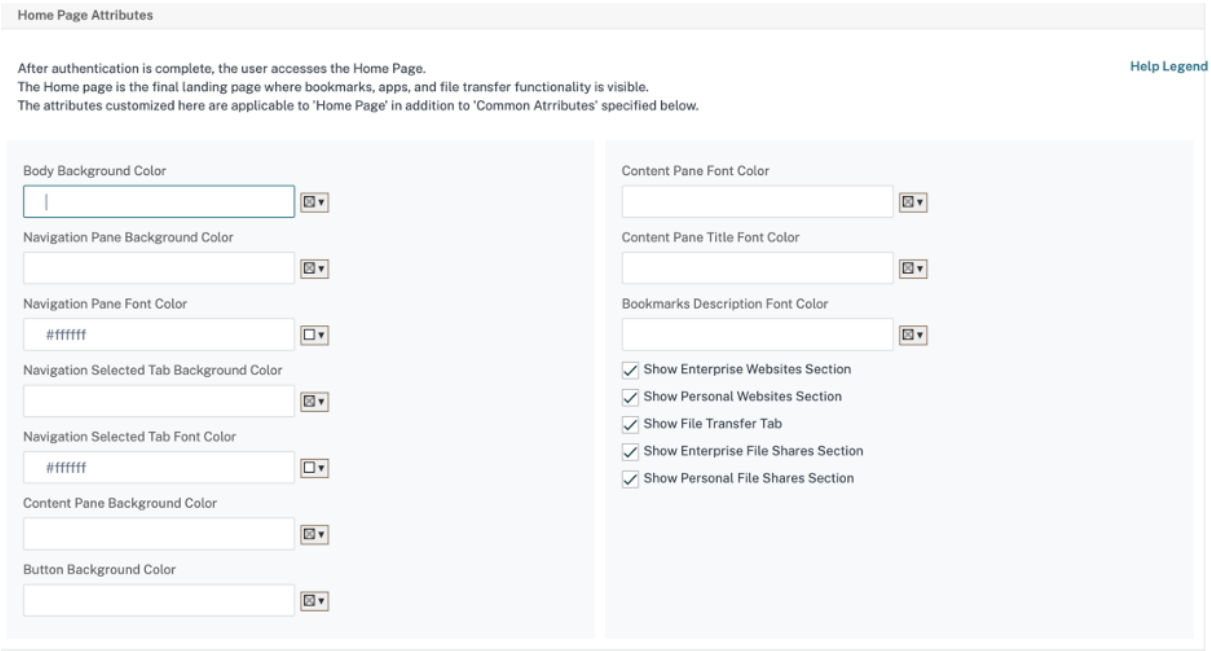


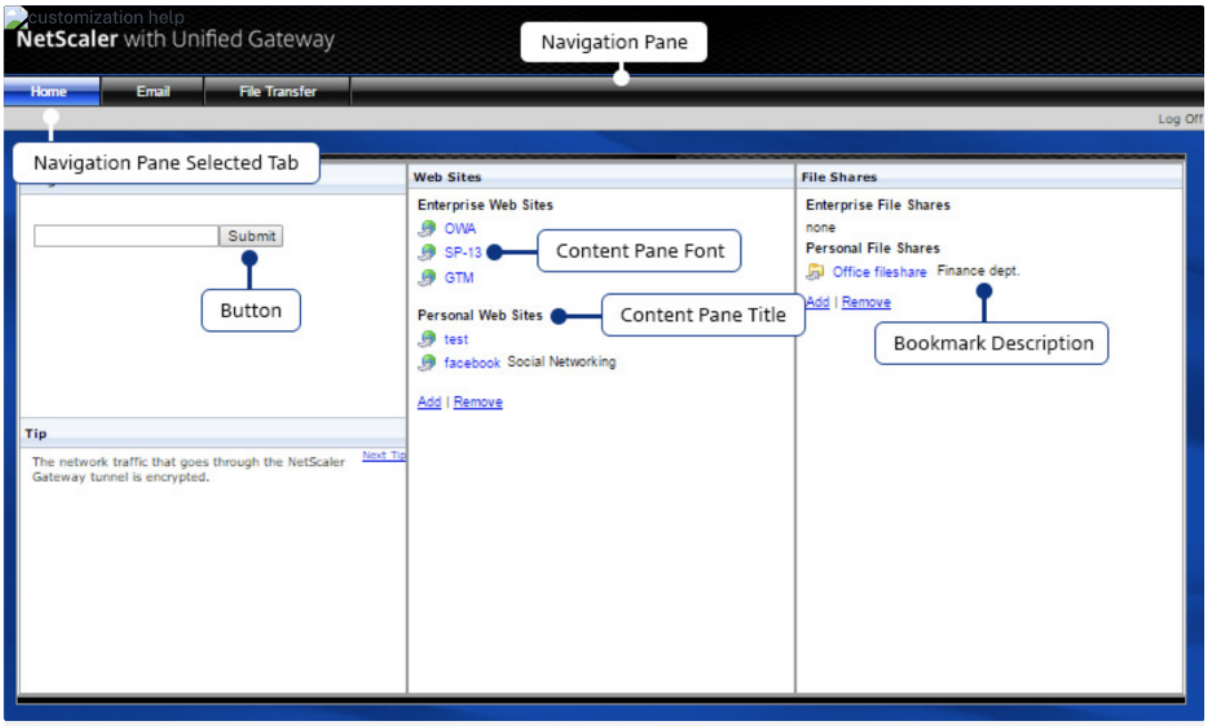
[**Help Legend**] リンクをクリックすると、共通の設定可能な各パラメータが表示されます。

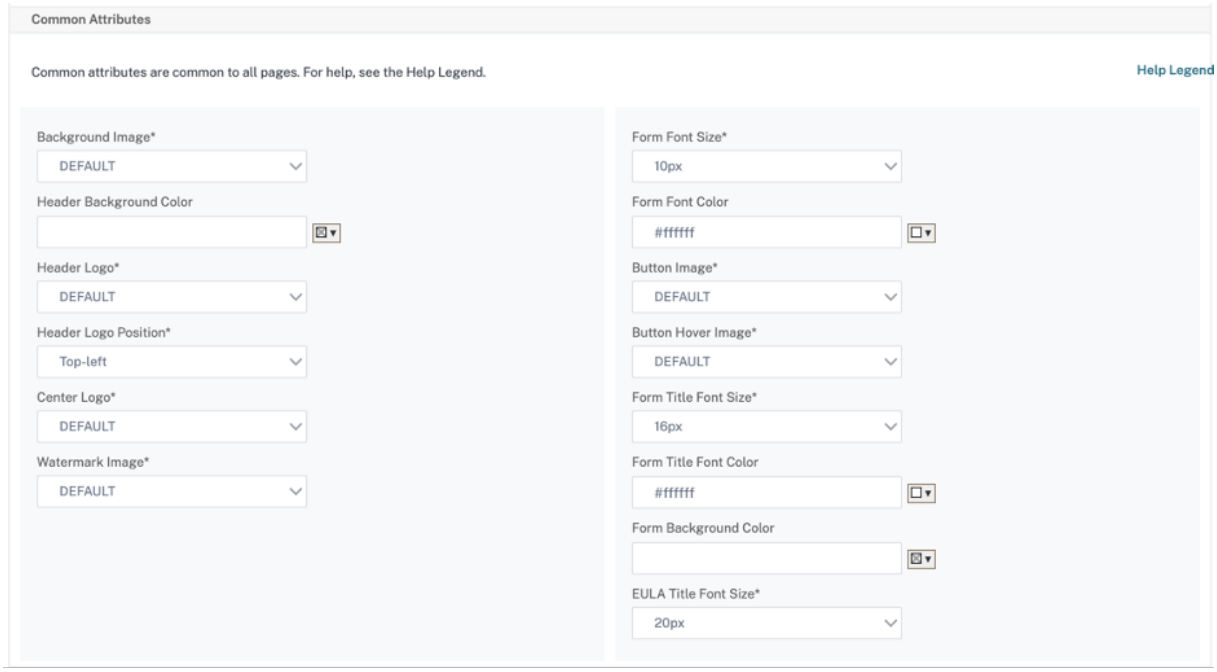


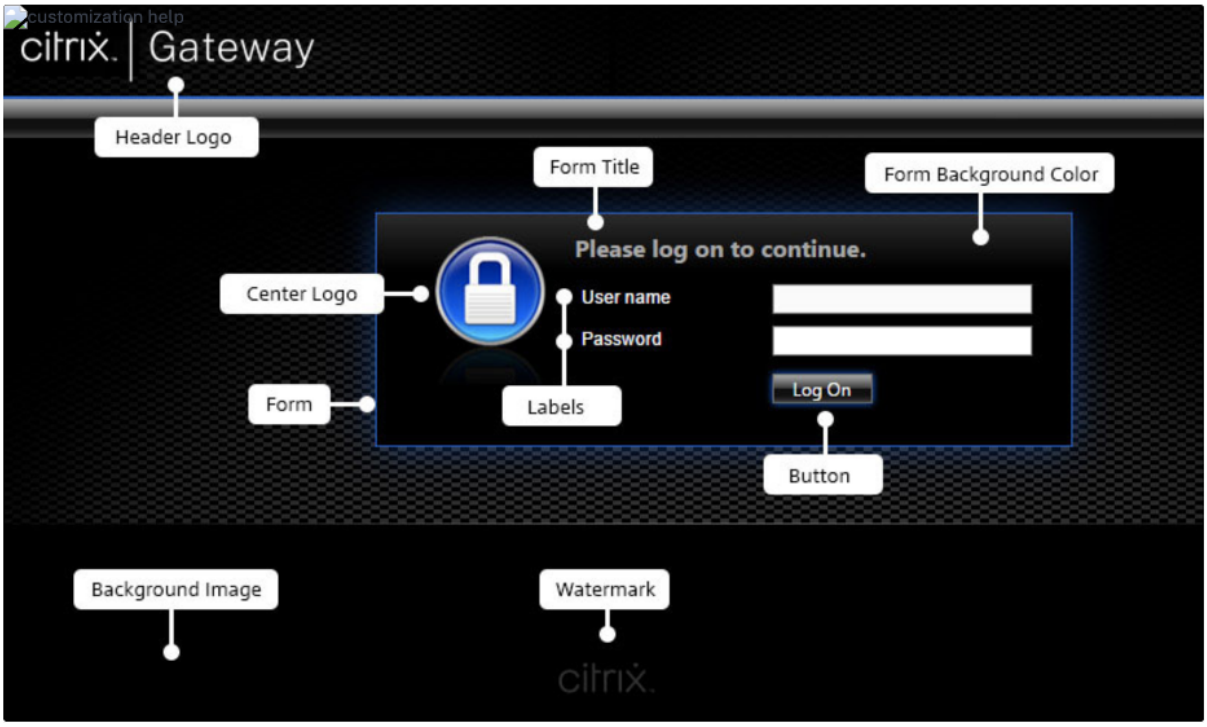
同様に、**Default** に基づくカスタムテーマの場合、次の図はホームページで使用可能な設定を示しています。

注**:** この構成は x1 と GreenBubble では異なります。







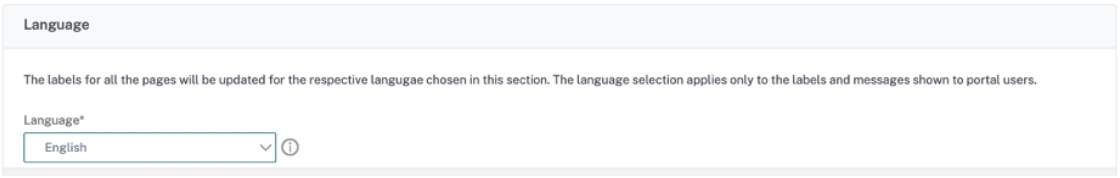


文字列のカスタマイズ

管理 UI では、ゲートウェイポータルのホームページの外観と外観に加えて、すべてのページで文字列のカスタマイズも可能です。

文字列をカスタマイズするには、次の手順を実行します。

1. 文字列を編集する言語を選択します。選択した言語で文字列が表示されます。既定では、[英語] が選択されています。



   注**:** 選択した言語では、ポータル・テーマ言語は定義されません。これは、文字列がカスタマイズされる言語です。

2. 右側の **[**詳細設定**]** に、文字列のカスタマイズに使用できるページが一覧表示されます。

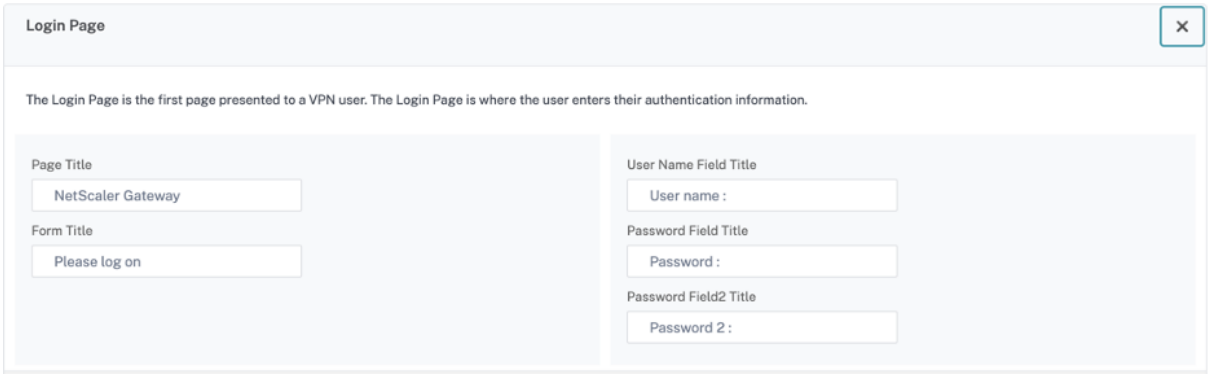
   - ログインページ
   - EPA ページ
   - EPA エラーページ
   - 環境保護庁後のページ
   - [VPN 接続] ページ
   - ホームページ

3. 文字列をカスタマイズするページを選択し、「編集」アイコンをクリックします。文字列のカスタマイズがあらかじめ入力されたフォームが表示されます。
4. フィールドを選択し、必要に応じて文字列を追加または編集します。
5. [**Done**] をクリックして、カスタムポータルテーマの作成を完了します。テーマは、**NetScaler Gateway > [**ポータルテーマ] から後で編集できます。

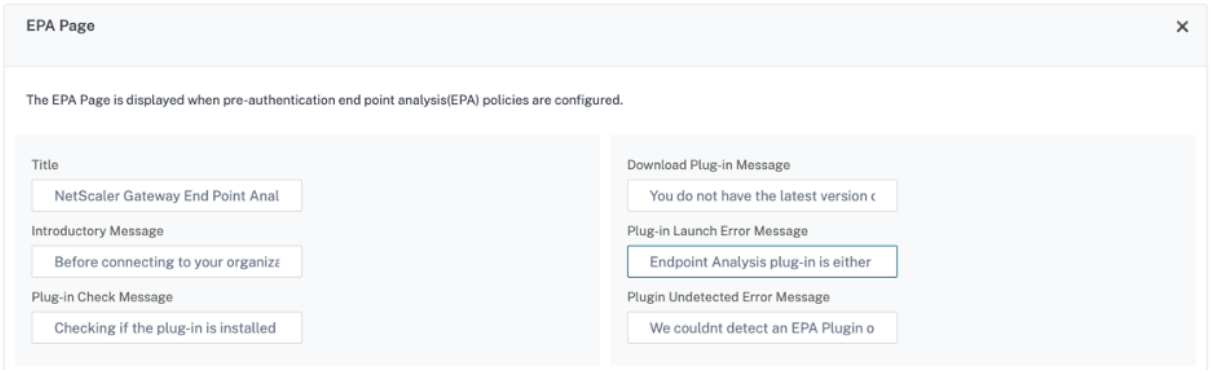
注**:** セクションに以前に選択した言語の文字列が引き続き表示される場合は、言語が変更されたときにセクションが既に開かれていた可能性があります。この場合は、セクションを閉じて言語を選択し、[詳細設定] からページを再度開きます。

次のスクリーンショットは、各ページで使用できるカスタマイズ可能な文字列のセットを示しています。

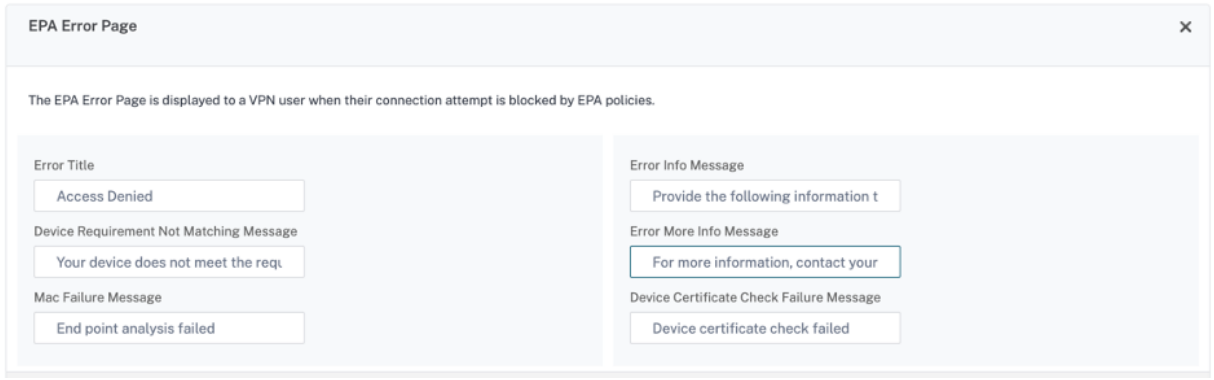
ログインページ**:**



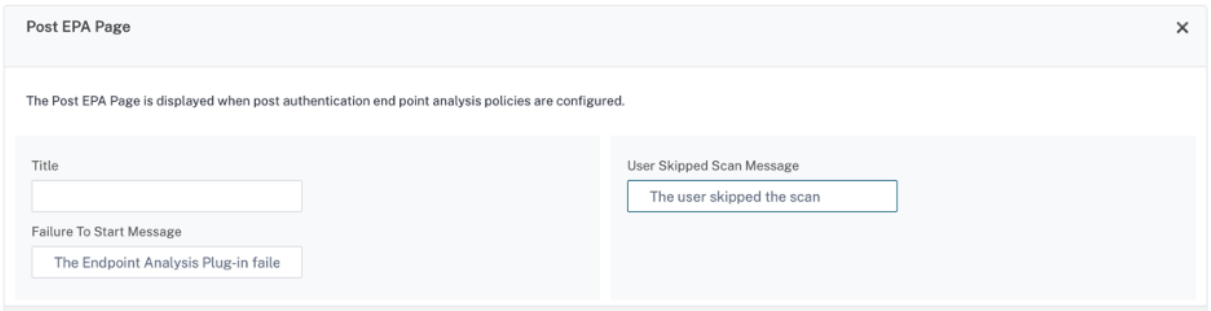
環境保護庁ページ**:**



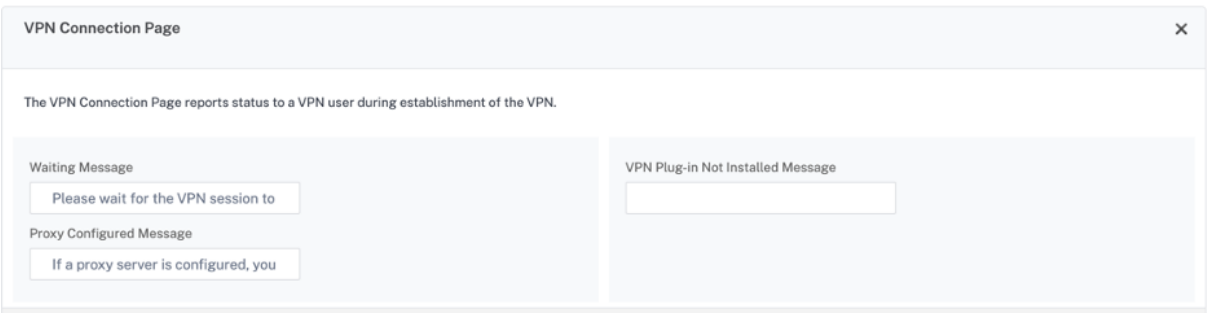
EPA エラーページ**:**



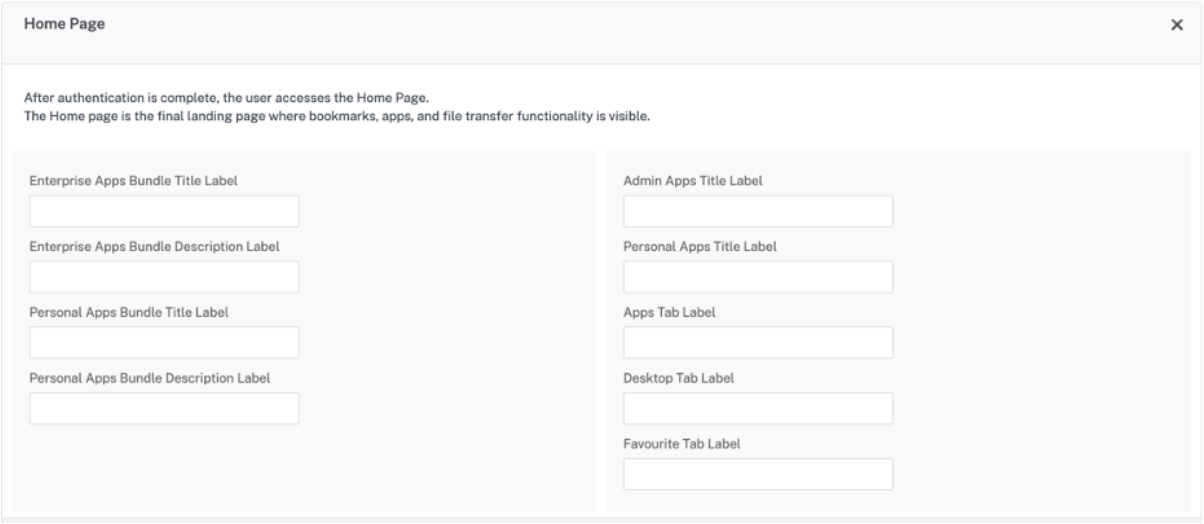
環境保護庁後のページ**:**



[VPN 接続**]** ページ**:**



ホームページ**:**



NetScaler Gateway VPN 分割トンネルの Office365 用に最適化

April 1, 2024

組織はリモートワークオプションに以前よりも迅速に適応しているため、トラフィック負荷の増加時にシームレスな接続を可能にするために、リモートアクセスインフラストラクチャを最適化する必要があります。

> 重要:
>
> Microsoft では、公開されている IPv4 および IPv6 のアドレス範囲を使用して分割トンネリングを構成することにより、主要な Office 365 サービスを宛先とするトラフィックを VPN 接続の範囲から除外することを推奨しています。パフォーマンスを最大限に高め、VPN 容量を最も効率的に使用するには、次のアプリケーションに関連する専用 IP アドレス範囲へのトラフィックを VPN トンネルの外部に直接ルーティングする必要があります。
>
> - Office 365 Exchange Online
> - SharePoint Online
> - Microsoft Teams (Microsoft のドキュメントでは「最適化」カテゴリと呼ばれています)
>
> この推奨事項の詳細については、Microsoft のガイダンスを参照してください 。

NetScaler Gateway での Microsoft の推奨は、分割トンネルのリバース構成を使用して、Microsoft が提供する IP アドレスのリストを O365 トラフィック用にインターネットに直接ルーティングすることで実現されます。

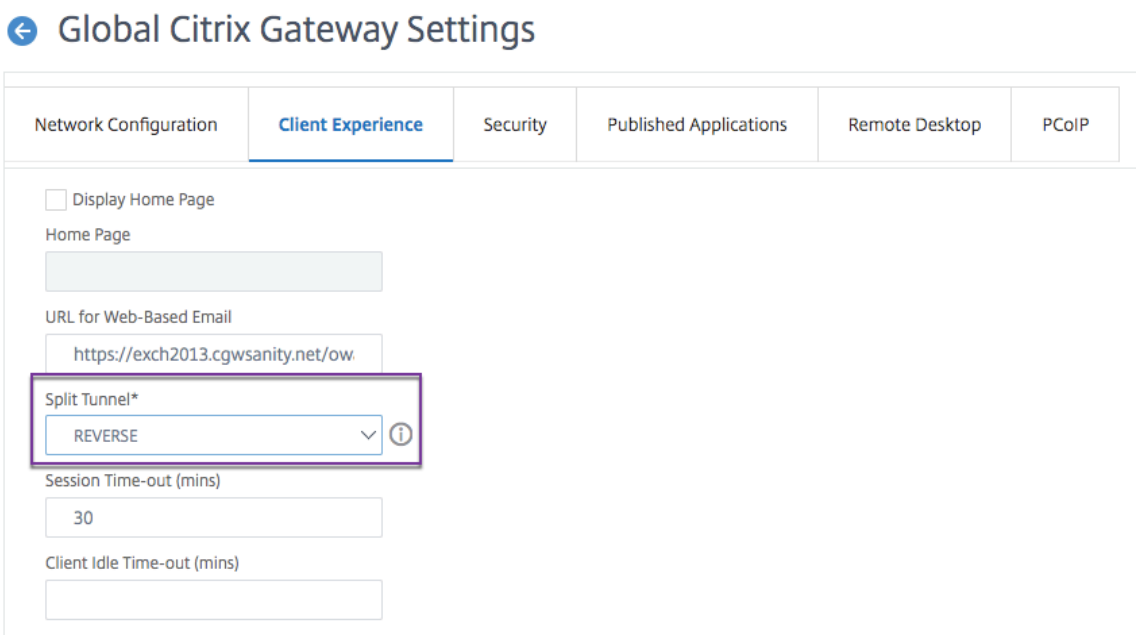
設定には以下が含まれます。これらの設定は、GUI または CLI を使用して手動で実行できます:

- 分割トンネルをリバース構成に設定します。詳細については、「分割トンネリングオプション」を参照してください。
- リソースへのユーザーアクセス用にイントラネットアプリケーションを構成します。

GUI を使用した設定

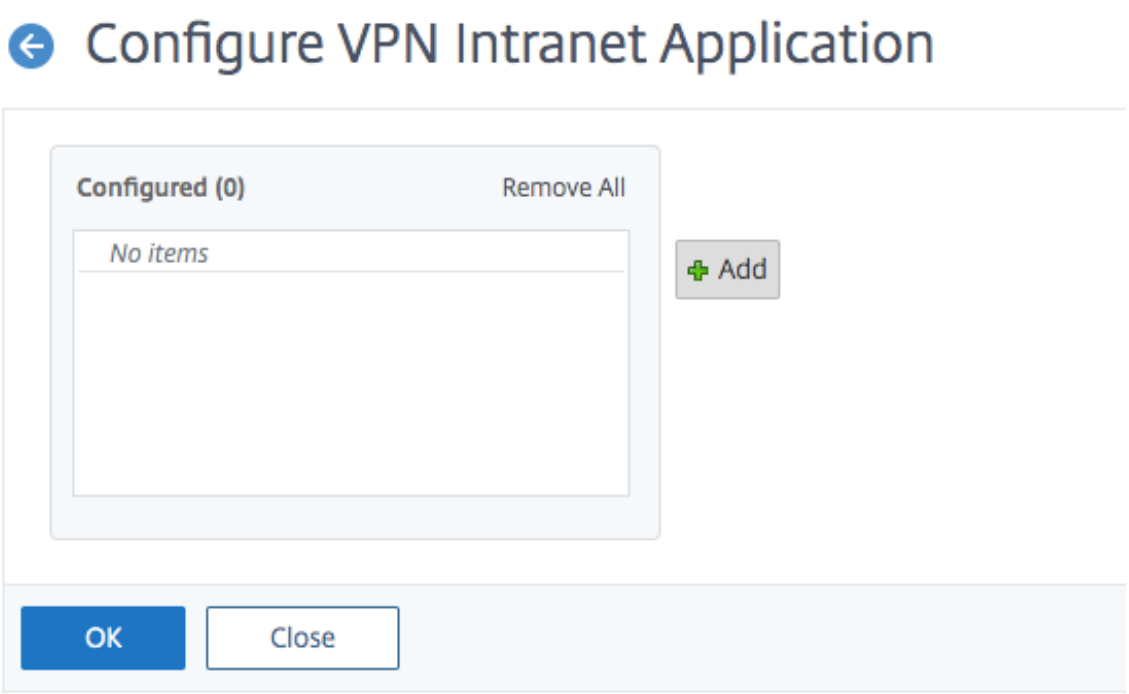
GUI を使用して分割トンネリングを設定するには

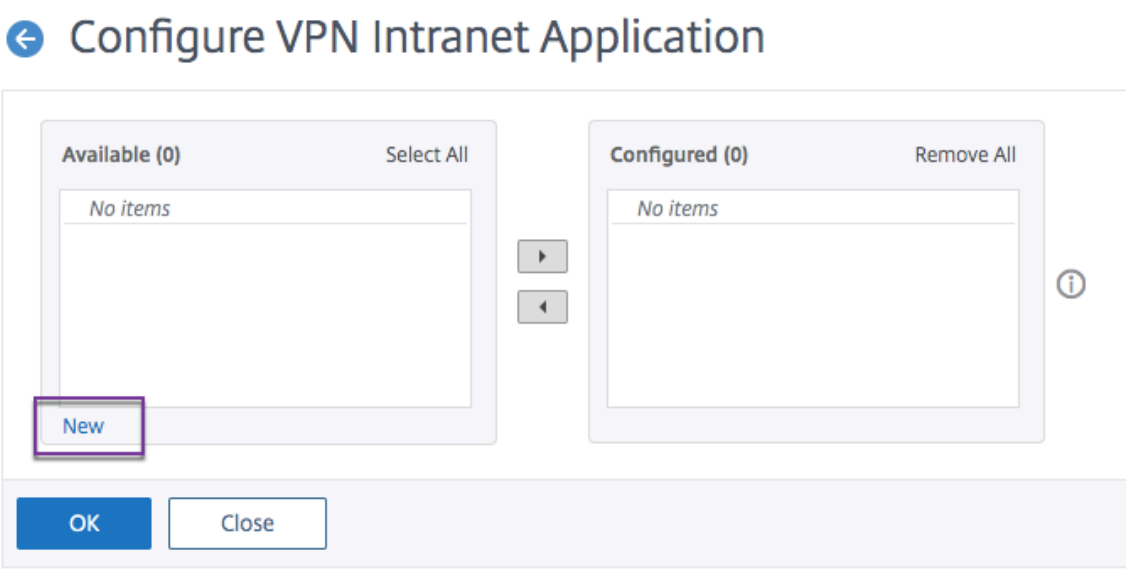
1. ［構成］タブで、［**NetScaler Gateway**］**>** ［グローバル設定］に移動します。
2. 詳細ウィンドウの [設定] で、[グローバル設定の変更] をクリックします。
3. [クライアントエクスペリエンス] タブの [分割トンネル] で、[リバース] を選択します。
4. ［**OK**］をクリックします。



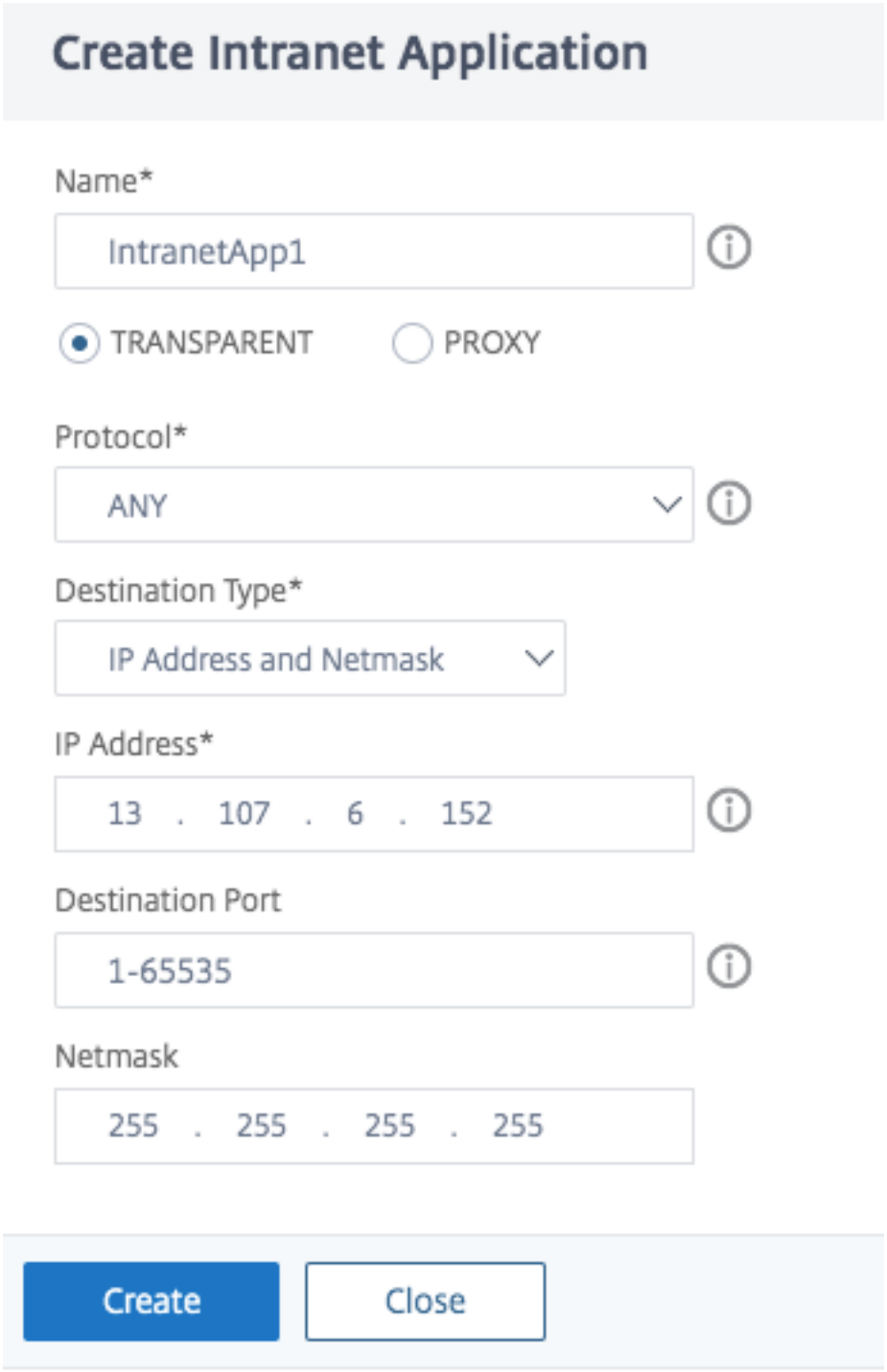
GUI を使用して **VPN** イントラネットアプリケーションを作成するには

1. ［構成］タブで、［**NetScaler Gateway**］**>** ［グローバル設定］に移動します。
2. 詳細ウィンドウの [イントラネットアプリケーション] で、リンクをクリックします。
3. [**VPN** イントラネットアプリケーションの構成] ページで、[追加]、[新規] の順にクリックします。





4. **[**名前] に、プロファイルの名前を入力します。
5. 「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。
6. [宛先タイプ] で、[**IP** アドレス**]** と **[**ネットマスク] を選択します。
7. [**IP Address**] に、O365 トラフィック用にインターネットに直接ルーティングする必要がある IP アドレスを入力します。IP アドレスの一覧については、IP アドレスの一覧を参照してください。
8. [ネットマスク] に、ネットマスク IP アドレスを入力します。



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

注**:** すべての IP アドレスに対してこの手順を繰り返します。

CLI を使用した設定

- 分割トンネルをリバースに設定するには、コマンドプロンプトで; と入力します。

```
set vpn parameter -splitTunnel REVERSE
<!--NeedCopy-->
```

- VPN イントラネットアプリケーションを追加するには、コマンドプロンプトで; と入力します。

```
add vpn intranetApplication intranetapp1 ANY 13.107.6.152 -netmask
    255.255.255.254 -destPort 1-65535 -interception TRANSPARENT
<!--NeedCopy-->
```

注: すべての IP アドレスに対してこの手順を繰り返します。

- イントラネットアプリケーションをバインドするには、コマンドプロンプトで次のように入力します。

```
bind vpn global -intranetApplication intranetapp1
<!--NeedCopy-->
```

Office 365 サービス (EXO、SPO、および Microsoft Teams) の IP アドレスのリスト

参考: https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges

> **Microsoft** からのメモ:
>
> 新型コロナウイルス感染症の状況に対する Microsoft の対応の一環として、Microsoft は予定されている一部の URL と IP アドレスの変更を一時的に停止することを宣言しました。このモラトリアムは、顧客の IT チームが、自宅勤務の Office 365 シナリオで推奨されるネットワーク最適化を実装する際に、自信を持ってシンプルに実装できるようにすることを目的としています。2020 年 3 月 24 日から 2020 年 6 月 30 日まで、このモラトリアムでは、主要な Office 365 サービス (Exchange Online、SharePoint Online、および Microsoft Teams) の IP 範囲と [最適化] カテゴリに含まれる URL への変更が停止されます。

IPv4 アドレス範囲

104.146.128.0/17
13.107.128.0/22
13.107.136.0/22
13.107.18.10/31
13.107.6.152/31
13.107.64.0/18
131.253.33.215/32
132.245.0.0/16

150.171.32.0/22
150.171.40.0/22
191.234.140.0/22
204.79.197.215/32
23.103.160.0/20
40.104.0.0/15
40.108.128.0/17
40.96.0.0/13
52.104.0.0/14
52.112.0.0/14
52.96.0.0/14
52.120.0.0/14

IPv6 アドレス範囲

2603:1006::/40
2603:1016::/36
2603:1026::/36
2603:1036::/36
2603:1046::/36
2603:1056::/36
2603:1096::/38
2603:1096:400::/40
2603:1096:600::/40
2603:1096:a00::/39
2603:1096:c00::/40
2603:10a6:200::/40
2603:10a6:400::/40
2603:10a6:600::/40
2603:10a6:800::/40
2603:10d6:200::/40
2620:1ec:4::152/128
2620:1ec:4::153/128
2620:1ec:c::10/128
2620:1ec:c::11/128
2620:1ec:d::10/128
2620:1ec:d::11/128
2620:1ec:8f0::/46
2620:1ec:900::/46

2620:1ec:a92::152/128
2620:1ec:a92::153/128
2a01:111:f400::/48
2620:1ec:8f8::/46
2620:1ec:908::/46
2a01:111:f402::/48

UDP トラフィックのサービスタイプサポート

February 1, 2024

UDP のタイプ（ToS）のサポートにより、送信者によって UDP パケットの ToS 値が構成されると、NetScaler Gateway はパケットが宛先に到達するまでその値を保持します。設定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 パケットを優先された発信キューに配置します。

> （注
> ）ToS 情報を使用して、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。

サーバー名表示拡張機能の設定

February 1, 2024

NetScaler 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「クライアントこんにちは」パケットにサーバー名表示（SNI）拡張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ーが SSL ハンドシェイク中に要求される 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は、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 **NetScaler Gateway** を構成するには:

1. NetScaler GUI で、[構成] > [NetScaler] **> [**グローバル設定] に移動します。
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ー **SNI**] メニューから [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 **NetScaler 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。


```
set vpn parameter backendServerSni <ENABLED><DISABLED>
<!--NeedCopy-->
```

SSL ハンドシェイク中のサーバ証明書の検証

February 1, 2024

NetScaler 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から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 NetScaler Gateway グローバルパラメーターを構成するには

CA 証明書をバインドする

1. [構成] > [**NetScaler Gateway**] > [**NetScaler Gateway** ポリシーマネージャー] > [証明書のバインド] に移動します。**
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。

証明書の検証を有効にします。

1. [**NetScaler 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ー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 NetScaler 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:

```
    bind vpn global cacert DNPGCA1

    set vpn parameter backendcertValidation ENABLED
<!--NeedCopy-->
```

テンプレートを使用した簡略化された SaaS アプリ設定

February 1, 2024

NetScaler Gateway でのシングルサインオンによる SaaS アプリの構成は、一般的な SaaS アプリのテンプレートドロップダウンメニューをプロビジョニングすることで簡素化されます。構成する SaaS アプリは、メニューから選択できます。テンプレートには、アプリケーションの構成に必要な情報の大部分があらかじめ入力されています。ただし、顧客固有の情報は引き続き提供する必要があります。

> 注:
>
> SaaS アプリを構成して公開するには、NetScaler Gateway で構成して公開し、次にアプリケーションサーバーで構成して公開します。
>
> 次のセクションの手順は、テンプレートを使用して NetScaler Gateway でアプリを構成して公開するのに役立ちます。次に、アプリケーションサーバー上で構成して公開する方法を説明するセクションに進みます。

テンプレートを使用したアプリの構成と公開-NetScaler Gateway 固有の構成

次の設定では、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方法の例として AWS Console アプリケーションを使用しています。

開始する前に、次のものが必要です:

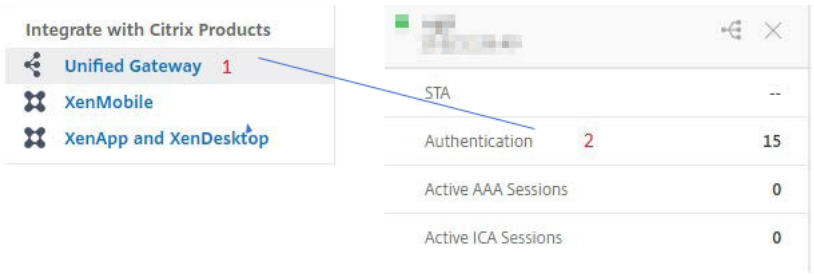
- AWS コンソールの管理者アカウント
- NetScaler Gateway の管理者アカウント

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. AWS コンソール IdP メタデータを NetScaler ADC からエクスポートします。
3. IdP を AWS コンソールに設定します。

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

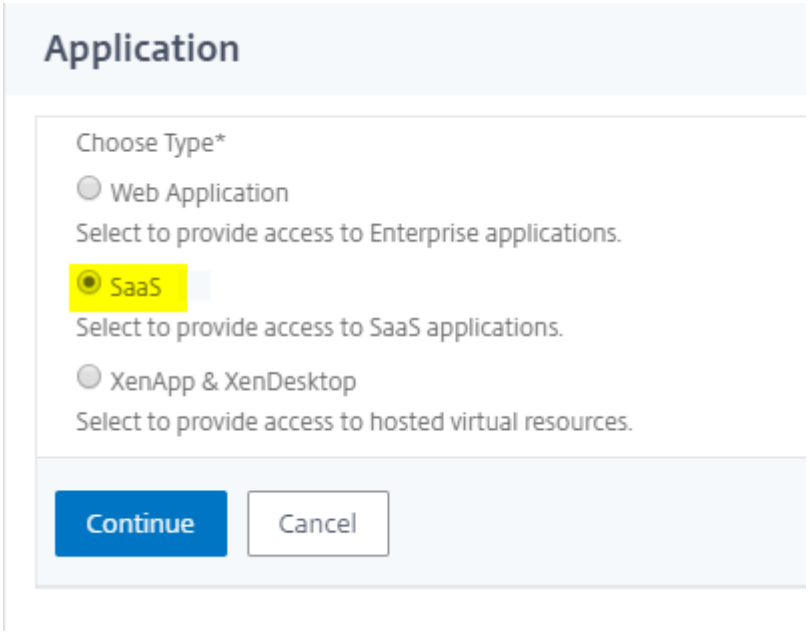
1. **Unified Gateway >** 認証をクリックします。



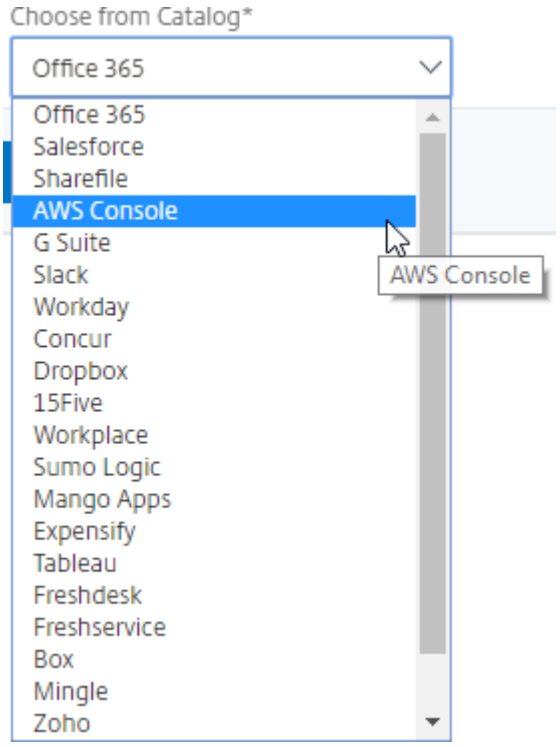
   [Unified Gateway の設定] 画面が表示されます。

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。次に、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. [アプリケーションの種類] から [**SaaS**] を選択します。



4. ドロップダウンリストから [**AWS Console**] 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ー **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—発行者名は選択に従って入力できます

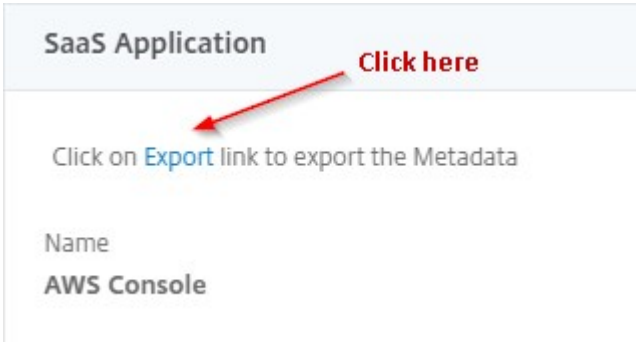
   属性 **1** —`https://aws.amazon.com/SAML/Attributes/Role`

   属性 **1** 式 - `Role ARN, IdP ARN`（ステップ 3 を参照）

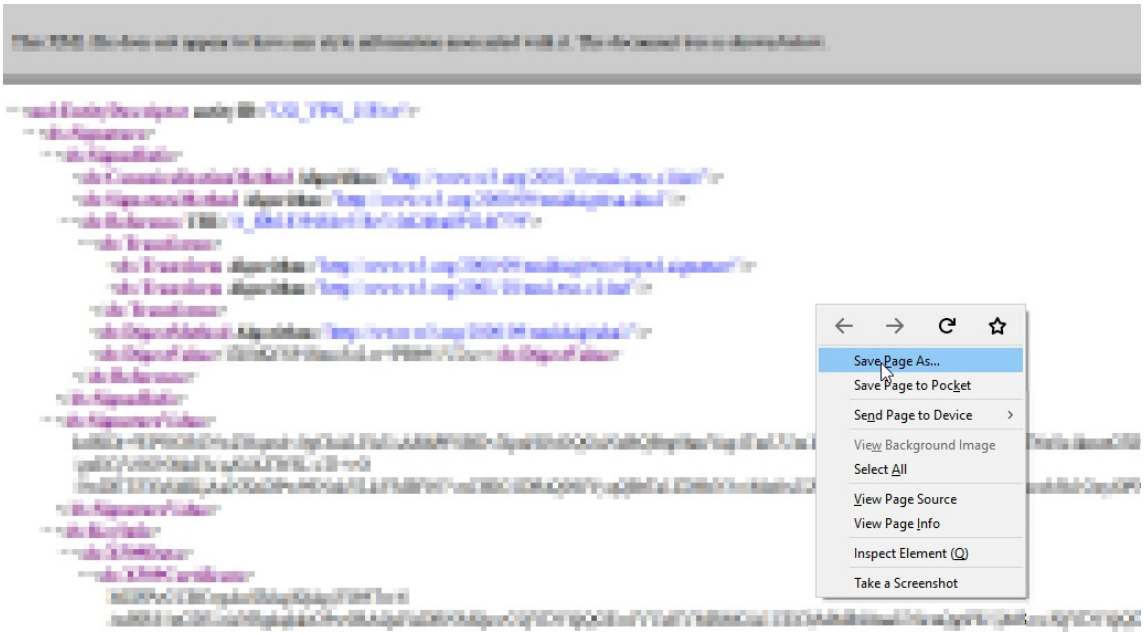
7. [完了] をクリックします。

ステップ **2:** AWS コンソール IdP メタデータを NetScaler Gateway から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。[リンクをエクスポート] をクリックします。



3. メタデータは別のウィンドウで開きます。**IdP** メタデータファイルを保存する



ステップ **3:** IdP を AWS コンソールに設定します。

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

次のリンクは、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具体的なガイダンスを提供する PDF ドキュメントを開きます。

- 15Five
- Absorb
- Accompa
- Adobe Captivate Prime
- Adobe Creative Cloud
- Aha

- AlertOps
- Allocadia
- Ariba
- Assembla
- AWS Console
- BambooHR
- Base CRM
- BitaBIZ
- BlueJeans
- Blissbook
- Bonusly
- Box
- Bugsnag
- Buildkite
- CakeHR
- Cardboard
- Cedexis
- Celoxis
- Cisco Meraki
- ClearSlide
- CloudCheckr
- ConceptShare
- Concur
- Confluence
- Contactzilla
- Convo
- Circonus
- 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
- Sumo Logic
- 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