StoreFront 3.12

Aug 14, 2017

StoreFrontについて

Aug 14, 2017

StoreFrontでは、データセンター内のXenApp、XenDesktop、XenMobileサーバーからユーザーデバイスへのデスクトップやアプリケーションの配信を管理できます。ユーザーがアクセス可能なデスクトップやアプリケーションは、StoreFrontストア上に列挙、集約されます。ユーザーはCitrix Receiverを使ったり、WebブラウザーでCitrix Receiver for Webサイトやデスクトップアプライアンスサイトを表示したりすることでStoreFrontストアにアクセスできます。シンクライアントやそのほか対応デバイスのユーザーは、XenApp Servicesサイト経由でStoreFrontストアにアクセスできます。

StoreFrontでは各ユーザーのアプリケーションのレコードが保持され、デバイスが自動で更新されます。ユーザーには、スマートフォン、タブレット、ラップトップ、デスクトップコンピューターを切り替えても一貫したエクスペリエンスが提供されます。StoreFrontはXenApp 7.xとXenDesktop 7.xの統合コンポーネントですが、ほかのバージョンのXenAppやXenDesktopでも使用できます。

StoreFrontの新機能

StoreFront 3.12について、複数の解決された問題と既知の問題があります。

Citrix Onlineアプリケーションをストアに統合する。Citrixは、XenAppおよびXenDesktop 7.14（StoreFront 3.11）のこの機能の廃止を発表しました。3.12では、StoreFront管理コンソールでこの機能を構成することはできません。StoreFront 3.12へのアップグレードでは、引き続きこの機能を使用できます。構成を変更するには、PowerShellコマンドレットのUpdate-DSGenericApplicationsを使用します。詳しくは、「Citrix Onlineアプリケーションをストアに統合する」を参照してください。

解決された問題

Aug 14, 2017

次の問題は、バージョン3.11以降で解決されています。

- 管理者がグループポリシー設定のMaxPasswordAgeの値を変更すると、StoreFrontのデフォルトのドメインサービスは新しい値を再読み込みしません。このため、ユーザーに誤った「パスワードの有効期限までの日数」が表示されます。

  注：この問題は解決されましたが、新しい値を読み込むには最大1時間を要することがあります。

  [#DNA-41380]

- マルチサイト集約環境で切断されたセッションに再接続しようとすると、失敗することがあります。これによって、同じリソースの2つ目のインスタンスを受信することがあります。

  [#LC7453]

- 集約されたアプリケーションのソースのいずれかが無効になっている場合は、アプリケーションが予期せずエンドユーザーから非表示になることがあります。

  [#LC7675]

- StoreFrontで［アカウントセルフサービス］オプションを無効にしようとすると、無効と表示されていても無効にならないことがあります。

  [#LC7744]

- StoreFrontでストアから共有認証を削除しようとすると、変更の保存中、次のメッセージが表示されることがあります。「変更の保存時にエラーが発生しました。」

  [#LC7781]

既知の問題

Aug 14, 2017

このリリースの既知の問題は次のとおりです。

- ワークスペースコントロールが、ワークスペースのすべてのアプリケーションではなく、1つのアプリケーションセッションにのみ再接続します。この問題は、ChromeでReceiver for Webサイトにアクセスした場合に報告されています。この問題を回避するには、切断されたアプリケーションごとに［接続］をクリックします。

  [# DNA-25140]

- カスタム認証フォームにID=confirmBtnの要素が含まれている場合、ユーザーがCitrix Receiver for Webにログオンできません。この問題を回避するには、カスタムフォーム内で拡張認証機能が別のIDの値を使用する必要があります。

  [# 603196, DNA-22593]

- Chromeブラウザーでアプリケーションに再接続すると失敗することがあります。公開アプリケーションに再接続する時に複数のセッションが使用中の場合、**［接続］**をクリックすると最初のセッションにのみ再接続する場合があります。この問題を回避するには、**［接続］**をもう一度クリックし、各セッションに再接続します。

  [# 575364, DNA-22561]

サードパーティ製品についての通知

Aug 14, 2017

StoreFrontには、次のドキュメントで定義された条件の元でライセンスが有効になったサードパーティのソフトウェアが含まれている可能性があります。

PDF StoreFrontのサードパーティ製品についての通知

システム要件

Aug 14, 2017

インストールを計画する時に、サーバーにインストールされているその他の製品の要件に加えて、StoreFront用に少なくとも2GBのRAMを使用できるかどうかを確認してください。サブスクリプションストアサービスでは、5MB以上の空きディスク領域が必要です。さらに、アプリケーションのサブスクリプション1000個について約8MBが必要になります。他のすべてのハードウェア仕様は、インストールされているオペレーティングシステムの要件を満たしている必要があります。

Citrix社では、以下のプラットフォームへのStoreFrontのインストールがテストされており、サポートが提供されます。

- Windows Server 2016のDatacenter、およびStandardエディション
- Windows Server 2012 R2のDatacenter、およびStandardエディション
- Windows Server 2012のDatacenter、およびStandardエディション
- Windows Server 2008 R2 Service Pack 1のEnterprise、およびStandardエディション

StoreFrontが動作するサーバー上のオペレーティングシステムをアップグレードすることはサポートされていません。新しくインストールしたオペレーティングシステムにStoreFrontをインストールすることをお勧めします。複数サーバーの展開環境の各サーバーでは同じバージョンのオペレーティングシステムが動作しており、ロケール設定が同一である必要があります。StoreFrontサーバーグループ内でオペレーティングシステムのバージョンやロケール設定が異なるサーバーを混在させることはサポートされていません。サーバーグループには最大で6つのサーバーを追加できますが、シミュレーションでは4つ以上のサーバーをグループに追加しても顕著なキャパシティ向上は確認されていません。サーバーグループ内のすべてのサーバーは同じ場所に配置されている必要があります。

サーバーにはMicrosoftインターネットインフォメーションサービス（IIS）とMicrosoft .NET Frameworkが必要です。これらの必須コンポーネントがインストール済みでも無効である場合は、StoreFrontのインストーラーにより、製品のインストール前に有効化されます。StoreFrontをインストールする前に、WebサーバーにWindows PowerShellおよびMicrosoft管理コンソールをインストールしておく必要があります。これらはWindows Serverのデフォルトのコンポーネントです。StoreFrontのIISでの相対パスが、グループ内のすべてのサーバーで同じである必要があります。

StoreFrontインストーラーにより、必要なIIS機能が追加されます。これらの機能を事前インストールする場合は、以下が必要です。

すべてのプラットフォーム：

- Web-Static-Content
- Web-Default-Doc
- Web-Http-Errors
- Web-Http-Redirect
- Web-Http-Logging
- Web-Mgmt-Console
- Web-Scripting-Tools
- Web-Windows-Auth
- Web-Basic-Auth
- Web-AppInit

Windows Server 2008 R2の場合：

- Web-Asp-Net
- As-Tcp-PortSharing

Windows Server 2012サーバーの場合：

- Web-Asp-Net45
- Net-Wcf-Tcp-PortSharing45

Windows Server 2016の場合：
- Web-Asp-Net45
- Net-Wcf-Tcp-PortSharing45

StoreFrontでは、以下の通信ポートが使用されます。ファイアウォールやほかのネットワークデバイスで、これらのポートへのアクセスが許可されることを確認してください。

- TCPポート80および443は、それぞれHTTPおよびHTTPS通信で使用されます。これらのポートは、社内ネットワーク内部および外部からアクセスできる必要があります。
- TCPポート808は、StoreFrontサーバー間の通信で使用されます。このポートは、社内ネットワーク内部からアクセスできる必要があります。
- サーバーグループ内のStoreFrontサーバー間の通信では、すべての未割り当てTCPポートからランダムに選択されるポートが使用されます。StoreFrontのインストール時に構成されるWindowsファイアウォール規則により、StoreFrontの実行可能ファイルへのアクセスが有効になります。ただし、その時に使用されるポートはランダムに選択されるため、内部ネットワーク上のファイアウォールやほかのネットワークデバイスで、すべての未割り当てTCPポートへのトラフィックがブロックされないことを確認する必要があります。
- Citrix Receiver for HTML5が有効な場合、内部ネットワーク上のローカルユーザーからデスクトップやアプリケーションを提供するサーバーへの通信でTCPポート8008が使用されます。

StoreFrontでは、ピュアIPv6ネットワークおよびデュアルスタックIPv4/IPv6環境の両方がサポートされます。

インフラストラクチャの要件

Citrixでは、以下のCitrixインフラストラクチャ製品でのStoreFrontの使用がテストされており、サポートが提供されます。

Citrixサーバー製品の要件

StoreFrontストアでは、以下の製品で提供されるデスクトップやアプリケーションを集約できます。

- XenAppおよびXenDesktop 7.15
- XenAppおよびXenDesktop 7.14
- XenAppおよびXenDesktop 7.13
- XenAppおよびXenDesktop 7.12
- XenAppおよびXenDesktop 7.11
- XenAppおよびXenDesktop 7.9
- XenAppおよびXenDesktop 7.8
- XenAppおよびXenDesktop 7.7
- XenAppおよびXenDesktop 7.6
- XenAppおよびXenDesktop 7.5
- XenDesktop 7.1
- XenDesktop 7
- XenApp 6.5
- XenMobile 9.0またはApp Controller 9.0

NetScaler Gatewayの要件

公共のネットワーク上のユーザーがStoreFrontにアクセスできるようにする場合、以下のバージョンのNetScaler Gatewayを使用できます。

- NetScaler Gateway 11.*x*
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10 Build 69.4（バージョン番号は構成ユーティリティの上部に表示されます）

Citrix Receiver for HTML5の要件

Citrix Receiver for Webサイト上で動作するCitrix Receiver for HTML5によるデスクトップやアプリケーションへのアクセスをユーザーに提供する場合、以下の追加要件があります。

内部ネットワーク接続では、Citrix Receiver for HTML5を使用して、以下の製品で提供されているデスクトップやアプリケーションにアクセスできます。

- XenAppおよびXenDesktop 7.15
- XenAppおよびXenDesktop 7.14
- XenAppおよびXenDesktop 7.13
- XenAppおよびXenDesktop 7.12
- XenAppおよびXenDesktop 7.11
- XenAppおよびXenDesktop 7.9
- XenAppおよびXenDesktop 7.8
- XenAppおよびXenDesktop 7.7
- XenAppおよびXenDesktop 7.6
- XenAppおよびXenDesktop 7.5
- XenDesktop 7.1
- XenDesktop 7
- XenApp 6.5 Feature Pack 2について
- XenApp 6.5 Feature Pack 1 for Windows Server 2008 R2（Hotfix XA650R01W2K8R2X64051必須。http://support.citrix.com/article/CTX136294から入手可能）

社内ネットワーク外のリモートユーザーがCitrix Receiver for HTML5を使用する場合、以下のバージョンのNetScaler Gatewayを介してデスクトップおよびアプリケーションにアクセスできます。

- NetScaler Gateway 11.*x*
- NetScaler Gateway 10.1
- Access Gateway 10 Build 71.6014（バージョン番号は構成ユーティリティの上部に表示されます）

NetScaler Gatewayを介した接続では、Citrix Receiver for HTML5を使用して、以下の製品で提供されているデスクトップやアプリケーションにアクセスできます。

- XenAppおよびXenDesktop 7.15
- XenAppおよびXenDesktop 7.14
- XenAppおよびXenDesktop 7.13
- XenAppおよびXenDesktop 7.12
- XenAppおよびXenDesktop 7.11
- XenAppおよびXenDesktop 7.9
- XenAppおよびXenDesktop 7.8
- XenAppおよびXenDesktop 7.7

- XenAppおよびXenDesktop 7.6
- XenAppおよびXenDesktop 7.5
- XenDesktop 7.1
- XenDesktop 7
- XenApp 6.5

ユーザーデバイスの要件

StoreFrontには、ユーザーがデスクトップおよびアプリケーションにアクセスするためのさまざまなオプションが用意されています。Citrix Receiverのユーザーは、Citrix Receiverを使用してストアにアクセスしたり、WebブラウザーからストアのCitrix Receiver for Webサイトにログオンしたりできます。Citrix Receiverをインストールできず、HTML5互換のWebブラウザーがあるユーザーの場合、Citrix Receiver for WebサイトでCitrix Receiver for HTML5を有効にして、Webブラウザー内でのデスクトップおよびアプリケーションへの直接アクセスを有効にできます。

ドメインに属していないデスクトップアプライアンスのユーザーは、Webブラウザーでデスクトップアプライアンスサイトにアクセスして自分のデスクトップにアクセスします。ドメインに属しているデスクトップアプライアンスのユーザー、Citrix Desktop Lockを実行している再目的化されたPCのユーザー、およびアップグレードできない古いバージョンのCitrixクライアントのユーザーは、ストアのXenApp Servicesサイト経由で接続する必要があります。

オフラインアプリケーションをユーザーに配信する場合は、Citrix Receiver for Windowsに加えてOffline Plug-inが必要です。Microsoft Application Virtualization（App-V）シーケンスをユーザーに配信する場合は、適切なバージョンのMicrosoft Application Virtualization Desktop Clientも必要です。詳しくは「ストリーム配信されるアプリケーションの管理」を参照してください。Citrix Receiver for Webサイトからオフラインアプリケーションや App-Vシーケンスにアクセスすることはできません。

ユーザーデバイスのハードウェア要件は、インストールされているオペレーティングシステムのものに準じます。

Citrix Receiver有効ストアの要件

内部ネットワーク接続、または外部ネットワークからNetScaler Gateway経由でStoreFrontストアにアクセスする場合、次のバージョンのCitrix Receiverを使用できます。NetScaler Gateway経由の接続は、NetScaler Gateway Plug-inを使用しても使用しなくても（クライアントレスアクセス）実行できます。Citrix Receiver for Windows 4.3は、Citrix Receiverエクスペリエンスが統合された完全なStoreFrontを受け取るために必要な最低のバージョンです。「統合されたCitrix Receiverエクスペリエンスのサポート」を参照してください。

- Citrix Receiver for Chrome 2.x
- Citrix Receiver for HTML5 2.x
- Citrix Receiver for Mac 12.x
- Citrix Receiver for Windows 4.x
- Citrix Receiver for Linux 13.x

Citrix Receiver for Webサイトからストアにアクセスするための要件

内部ネットワーク接続、または外部ネットワークからNetScaler Gateway経由でCitrix Receiver for Webサイトにアクセスする場合、次のCitrix Receiver、オペレーティングシステム、およびWebブラウザーの組み合わせが推奨されます。NetScaler Gateway経由の接続は、NetScaler Gateway Plug-inを使用しても使用しなくても（クライアントレスアクセス）実行できます。

- • Citrix Receiver for Windows 4.2.xからCitrix Receiver for Windows 4.9まで
  - Windows 10（32ビット版および64ビット版）

        - Microsoft Edge
        - Internet Explorer 11
        - Google Chrome
        - Mozilla Firefox
    - Windows 8.1（32ビット版および64ビット版）
        - Internet Explorer 11（32ビットモード）
        - Google Chrome
        - Mozilla Firefox
    - Windows 8（32ビット版および64ビット版）
        - Internet Explorer 10（32ビットモード）
        - Google Chrome
        - Mozilla Firefox
    - Windows 7 Service Pack 1（32ビット版および64ビット版）
        - Internet Explorer 9、10、または11
        - Google Chrome
        - Mozilla Firefox
    - Windows Embedded Standard 7 Service Pack 1またはWindows Thin PC
        - Internet Explorer 9、10、または11

- Citrix Receiver for Windows 4.0またはCitrix Receiver for Windows 3.4
    - Windows 8（32ビット版および64ビット版）
        - Internet Explorer 10（32ビットモード）
        - Google Chrome
        - Mozilla Firefox
    - Windows 7 Service Pack 1（32ビット版および64ビット版）
        - Internet Explorer 9、10、または11
        - Google Chrome
        - Mozilla Firefox
    - Windows Embedded Standard 7 Service Pack 1およびWindows Thin PC
        - Internet Explorer 9、10、または11
- Citrix Receiver for Mac 12.4
    - Mac OS X El Capitan（10.11）
        - Safari 9
        - Google Chrome
        - Mozilla Firefox
    - Mac OS X Yosemite（10.10）
        - Safari 8
        - Google Chrome
        - Mozilla Firefox
    - Mac OS X Mavericks（10.9）
        - Safari 7
        - Google Chrome
        - Mozilla Firefox
- Citrix Receiver for Linux 12.1およびCitrix Receiver for Linux 13.x
    - Ubuntu 12.04（32ビット）および14.04 LTS（32ビット）
        - Google Chrome
        - Mozilla Firefox

Receiver for HTML5を使用してデスクトップやアプリケーションにアクセスするための要件

Receiver for Webサイトで実行されるReceiver for HTML5を使用してデスクトップおよびアプリケーションにアクセスする場合、次のオペレーティングシステムとWebブラウザーが推奨されます。内部ネットワーク接続、および外部ネットワークからNetScaler Gateway経由での接続の両方がサポートされています。ただし、内部ネットワークからの接続の場合、Receiver for HTML5では特定の製品で提供されるリソースにのみアクセスできます。さらに、社内ネットワークの外から接続できるようにするには、特定のバージョンのNetScaler Gatewayが必要です。詳しくは、「インフラストラクチャの要件」を参照してください。

- Webブラウザー
  - Microsoft Edge
  - Internet Explorer 11および10（HTTP接続のみ）
  - Safari 7
  - Safari：5～6
  - Google Chrome
  - Mozilla Firefox
- オペレーティングシステム
  - Windows RT
  - Windows 10（32ビット版および64ビット版）
  - Windows 8.1（32ビット版および64ビット版）
  - Windows 8（32ビット版および64ビット版）
  - Windows 7 Service Pack 1（32ビット版および64ビット版）
  - Windows Vista Service Pack 2（32ビット版および64ビット版）
  - Windows Embedded XP
  - Mac OS X Yosemite（10.10）
  - Mac OS X Mavericks（10.9）
  - Mac OS® X 10.8（Mountain Lion®）
  - Mac OS® X 10.7（Lion®）
  - Mac OS® X 10.6（Snow Leopard®）
  - Google Chrome OS 48
  - Google Chrome OS 47
  - Ubuntu 12.04（32ビット）

デスクトップアプライアンスサイトからストアにアクセスするための要件

内部ネットワークからデスクトップアプライアンスサイトにアクセスする場合、次のCitrix Receiver、オペレーティングシステム、およびWebブラウザーの組み合わせが推奨されます。NetScaler Gateway経由での接続はサポートされません。

- Citrix Receiver for Windows 4.5、Citrix Receiver for Windows 4.4、Citrix Receiver for Windows 4.3、Citrix Receiver for Windows 4.2.x、Citrix Receiver for Windows 4.1
  - Windows 8.1（32ビット版および64ビット版）
    - Internet Explorer 11（32ビットモード）
  - Windows 8（32ビット版および64ビット版）
    - Internet Explorer 10（32ビットモード）
  - Windows 7 Service Pack 1（32ビット版および64ビット版）、Windows Embedded Standard 7 Service Pack 1、またはWindows Thin PC
    - Internet Explorer 9（32ビットモード）

        - Internet Explorer 8（32ビットモード）
    - Windows Embedded XP
        - Internet Explorer 8（32ビットモード）
- Citrix Receiver for Windows 4.0またはCitrix Receiver for Windows 3.4
    - Windows 8（32ビット版および64ビット版）
        - Internet Explorer 10（32ビットモード）
    - Windows 7 Service Pack 1（32ビット版および64ビット版）、Windows Embedded Standard 7 Service Pack 1、または Windows Thin PC
        - Internet Explorer 9（32ビットモード）
        - Internet Explorer 8（32ビットモード）
    - Windows Embedded XP
        - Internet Explorer 8（32ビットモード）
- Citrix Receiver for Windows（Enterprise） 3.4
    - Windows 7 Service Pack 1（32ビット版および64ビット版）、Windows Embedded Standard 7 Service Pack 1、または Windows Thin PC
        - Internet Explorer 9（32ビットモード）
        - Internet Explorer 8（32ビットモード）
    - Windows Embedded XP
        - Internet Explorer 8（32ビットモード）
- Citrix Receiver for Linux 12.1
    - Ubuntu 12.04（32ビット）
        - Mozilla Firefox

XenApp ServicesサイトのURLからストアにアクセスするための要件

前述したすべてのバージョンのCitrix Receiverを使用して、XenApp ServicesサイトのURL経由でStoreFrontストアにアクセスできます（この場合、一部の機能が制限されます）。また、Citrix Receiver for Linux 12.0（内部ネットワーク接続のみ）などのほかのアクセス方法をサポートしない古いクライアントを使用して、XenApp Servicesサイト経由でストアにアクセスできます。NetScaler Gateway経由の接続（サポートされる場合）は、NetScaler Gateway Plug-inを使用しても使用しなくても（クライアントレスアクセス）実行できます。

スマートカードの要件

Citrix Receiver for Windows 4.xでスマートカードを使用するための要件

Citrixは、National Institute of Standards and Technology Personal Identity Verification（NIST PIV）カード、および一部のUSBスマートカードトークンを対象として、互換性をテストします。USB Chip/Smart Card Interface Devices（CCID）仕様に準拠し、German Zentraler Kreditausschuss（ZKA）によりClass 1スマートカードリーダーとして分類される接触型カードリーダーを使用できます。ZKA Class 1接触型カードリーダーを使用するには、ユーザーがリーダーにスマートカードを挿入する必要があります。Class 2リーダー（PINを入力するためのテンキー付属）を含むそのほかの種類のスマートカードリーダー、非接触型リーダー、およびTrusted Platform Module（TPM）チップに基づく仮想スマートカードはサポートされません。

Receiver for Windowsのスマートカードのサポートは、MicrosoftのPC/SC（Personal Computer/Smart Card）標準仕様に基づいています。最小要件として、スマートカードおよびスマートカードリーダーがオペレーティングシステムでサポートされており、「Windowsハードウェア認定」を取得している必要があります。

Citrix互換のスマートカードとミドルウェアについて詳しくは、http://www.citrix.com/ready/jaを参照してください。

デスクトップアプライアンスサイトでスマートカードを使用するための要件

Citrix Desktop Lockを実行している再目的化されたPCやデスクトップアプライアンスのユーザーがスマートカードを使用して認証できるようにするには、Citrix Receiver for Windows Enterprise 3.4を使用する必要があります。その他のWindowsデバイスのユーザーは、Citrix Receiver for Windows 4.1を使用できます。

NetScaler Gatewayを介した認証の要件

公共のネットワーク上のユーザーがスマートカードでStoreFrontにアクセスできるようにする場合、以下のバージョンのNetScaler Gatewayを使用できます。

- NetScaler Gateway 11.x
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10 Build 69.4（バージョン番号は構成ユーティリティの上部に表示されます）

StoreFrontの展開計画

Aug 14, 2017

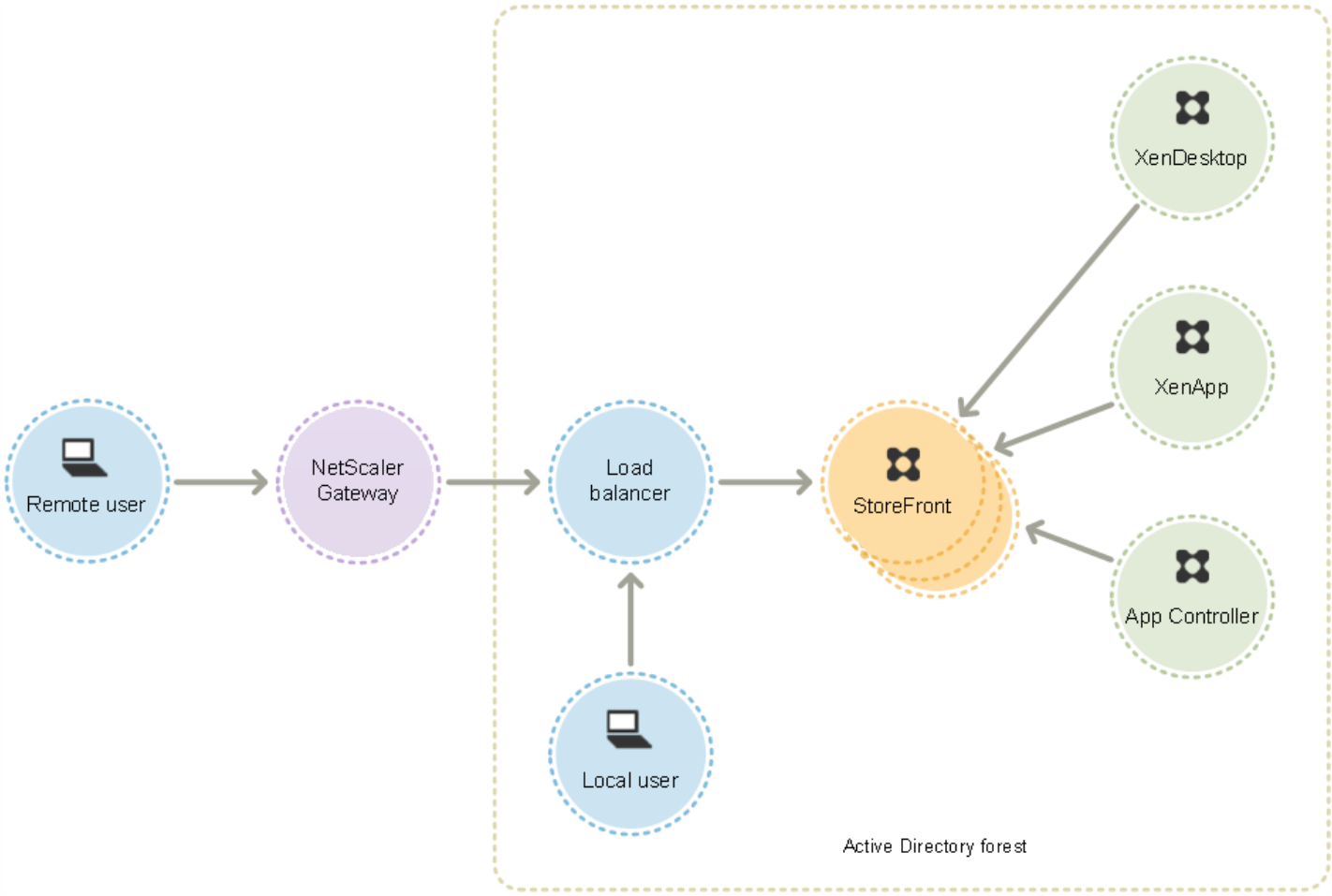
StoreFrontでは、Microsoftインターネットインフォメーションサービス（IIS）上で動作するMicrosoft .NETテクノロジーを使用して、リソースを集約してユーザーに配信するエンタープライズアプリケーションストアを提供します。XenDesktop、XenApp、およびApp Controller展開環境にStoreFrontを統合して、ユーザーにデスクトップおよびアプリケーションに対する単一のセルフサービスアクセスポイントを提供できます。

StoreFrontは、次のコアコンポーネントにより構成されています。

- 認証サービスにより、ユーザーがMicrosoft Active Directoryで認証され、ユーザーが再ログオンすることなくデスクトップやアプリケーションにアクセスできるようになります。詳しくは、「ユーザー認証」を参照してください。
- ストアには、XenDesktop、XenApp、およびApp Controllerで配信されるデスクトップやアプリケーションが列挙および集約されます。ユーザーは、Citrix Receiver、Citrix Receiver for Webサイト、デスクトップアプライアンスサイト、XenApp ServicesサイトのURL経由でストアにアクセスします。詳しくは、「ユーザーアクセスオプション」を参照してください。
- サブスクリプションストアサービスにより、ユーザーのアプリケーションサブスクリプションの詳細が記録され、ユーザーが複数のデバイスを使用しても一貫性のあるユーザーエクスペリエンスが提供されます。ユーザーのエクスペリエンスの向上について詳しくは、「ユーザーエクスペリエンスの最適化」を参照してください。

StoreFrontでは、単一サーバーの展開環境または複数サーバーの展開環境を構成できます。複数サーバーの環境では、処理能力だけでなく可用性も向上します。StoreFrontのモジュラーアーキテクチャにより、構成情報やユーザーのアプリケーションサブスクリプションの詳細がサーバーグループ内のすべてのサーバー上に格納され、複製されます。このため、何らかの理由でいずれかのStoreFrontサーバーが停止しても、ユーザーはほかのサーバーを使用してストアにアクセスできます。停止したサーバーが動作を再開してサーバーグループに再接続すると、構成およびサブスクリプションのデータが自動的に更新されます。サブスクリプションデータは、サーバーがオンラインに復帰したときに更新されますが、オフライン中の更新が反映されていない場合は、管理者が構成の変更を反映させる必要があります。ハードウェア障害などによりサーバーの交換が必要な場合でも、新しいサーバーにStoreFrontをインストールして既存のサーバーグループに追加するだけです。これにより、新しいサーバーが自動的に構成され、最新のアプリケーションサブスクリプションデータが同期されます。

次の図は、一般的なStoreFront展開環境を示しています。



負荷分散

複数サーバーの展開環境の場合は、NetScalerまたはWindowsのネットワーク負荷分散などによる外部の負荷分散機能が必要です。負荷分散環境を構成してサーバー間のフェールオーバーを有効にして、耐障害性を向上できます。NetScalerを使用した負荷分散について詳しくは、「負荷分散」を参照してください。Windowsのネットワーク負荷分散について詳しくは、http://technet.microsoft.com/ja-jp/library/hh831698.aspxを参照してください。

何千ものユーザーが使用したり、特定の時間帯に多くのユーザーのログオンが集中するなど、高負荷状態が発生したりする展開環境では、StoreFrontからXenDesktopサイトやXenAppファームへの要求を負荷分散することをお勧めします。この場合、NetScalerなど、XMLの監視機能やセッションパーシステンス機能を持つロードバランサーを使用してください。

SSL終了ロードバランサーを展開するか、またはトラブルシューティングの必要がある場合は、PowerShellコマンドレットの**Set-STFWebReceiverCommunication**を使用できます。

構文：

Set-STFWebReceiverCommunication [-WebReceiverService] [[-Loopback]] [[-LoopbackPortUsingHttp]]

有効な値は以下のとおりです。

- **On** – 新しいCitrix Receiver for Webサイトのデフォルト値です。Citrix Receiver for WebはスキーマHTTPSまたはHTTPおよびベースURLのポート番号を使用しますが、ホストをループバックIPアドレスと置き換えてStoreFront Servicesと通信します。これは単一サーバー展開および非SSL終了ロードバランサーがある展開で機能します。
- **OnUsingHttp** - Citrix Receiver for WebはHTTPおよびループバックIPアドレスを使用してStoreFront Servicesと通信しま

す。SSL終了ロードバランサーを使用している場合はこの値を選択します。また、デフォルトのポート80でない場合は、HTTPポートも指定する必要があります。
- **Off** - これはループバックをオフにし、Citrix Receiver for WebはStoreFrontベースURLを使ってStoreFront Servicesと通信します。インプレースアップグレードを実行する場合は、既存の展開に対する混乱を避けるため、これがデフォルトの値となります。

たとえば、SSL終了ロードバランサーを使用していて、HTTPに対してポート81を使用するようにIISが構成され、Citrix Receiver for Webサイトのパスが/Citrix/StoreWebの場合, 次のコマンドを使ってCitrix Receiver for Webサイトを構成できます。

```
$wr = Get-STFWebReceiverService -VirtualPath /Citrix/StoreWeb
Set-STFWebReceiverCommunication -WebReceiverService $wr -Loopback OnUsingHttp -LoopbackPortUsingHttp 81
```

Citrix Receiver for WebおよびStoreFront Services間のネットワークトラフィックをキャプチャするには、ループバックをオフにして、Fiddlerのような任意のWebプロキシツールを使用する必要があります。

Active Directoryに関する注意事項

単一サーバーの展開では、ドメインに参加していないサーバーにStoreFrontをインストールできます（ただし利用できない機能があります）。それ以外の場合、各StoreFrontサーバーは、XenAppまたはXenDesktopサイト/ファームに対する認証の委任を有効にしない限り、ユーザーアカウントが属しているActive Directoryドメイン、またはそのドメインと信頼関係があるドメインに属している必要があります。同一デリバリーグループで使用するすべてのStoreFrontサーバーが同じドメインに属している必要があります。

ユーザー接続

実務環境では、StoreFrontとユーザーデバイスの間の通信を保護するためにHTTPSを使用することをお勧めします。HTTPSを使用するには、認証サービスおよびストアをホストするIISインスタンスで、HTTPSを有効にする必要があります。IISでHTTPSが構成されていない場合、StoreFrontの通信にHTTPが使用されます。IISでHTTPSが適切に構成されている場合は、必要に応じていつでもHTTPをHTTPSに変更できます。

社内ネットワーク外からのStoreFrontへのアクセスを有効にする場合、安全な接続をリモートユーザーに提供するにはNetScaler Gatewayが必要です。NetScaler Gatewayを社内ネットワークの外にNetScaler Gatewayを配置して、ファイアウォールで公共のネットワークと内部ネットワークの両方からそのNetScaler Gatewayを分離します。NetScaler Gatewayが、StoreFrontサーバーを含んでいるActive Directoryフォレストにアクセスできることを確認してください。

複数のインターネットインフォメーションサービス（IIS）Webサイト

StoreFrontでは、Windowsサーバーごとに異なるIIS Webサイトで異なるストアを展開できます。これによって、ストアごとにそれぞれホスト名と証明書のバインドを持つことができます。

デフォルトのWebサイトに加えて、2つのWebサイト作成から始めます。IISで複数のWebサイトを作成してから、PowerShell SDKを使用して、IIS WebサイトにそれぞれStoreFront展開環境を作成します。IISでのWebサイトの作成方法について詳しくは、How to set up your first IIS Websiteを参照してください。

注：StoreFront管理コンソールとPowerShellコンソールを同時に開くことはできません。StoreFront管理コンソールを閉じてからPowerShellコンソールを開いてください。同様に、PowerShellのすべてのインスタンスを閉じてからStoreFront管理コンソールを開いてください。

例：2つのIIS Webサイト環境（1つはアプリケーション、1つはデスクトップ）を作成します。

1. Add-STFDeployment -SiteID 1 -HostBaseURL "https://www.storefront.app.com"
2. Add-STFDeployment -SiteID 2 -HostBaseURL "https://www.storefront.desktop.com"

StoreFrontは、複数のサイトを検出すると管理コンソールを無効にし、メッセージを表示します。

詳しくは、「インストールおよび構成する前に」を参照してください。

スケーラビリティ

単一のStoreFrontサーバーグループでサポートされるCitrix Receiverユーザーの数は、使用するハードウェアとユーザーアクティビティにより異なります。ユーザーがログオンして1つのリソースを開始するシミュレーションにおいては、100個の公開アプリケーションが列挙され、基になるデュアルIntel Xeon L5520 2.27Ghzプロセッササーバーで実行中の2つの仮想CPUの最小推奨仕様である単一のStoreFrontサーバーが、1時間あたり最大30,000のユーザー接続を有効にするとされます。

グループ内に同様の2つの構成サーバーがあるサーバーグループでは、1時間あたり最大で60,000のユーザー接続を有効にするとされます。3つのノードでは1時間あたり最大で90,000の接続、4つのノードでは1時間当たり最大で120,000の接続、5つのノードでは1時間あたり最大で150,000の接続、6つのノードでは1時間当たり最大で175,000の接続となります。

また、1時間当たり最大で55,000のユーザー接続を有効にする4つの仮想CPUと1時間当たり80,000の接続を有効にする8つの仮想CPUを使って、システムにより多くの仮想CPUを割り当てて単一のStoreFrontサーバーのスループットを増やすこともできます。

各サーバーの最小推奨メモリ割り当ては3GBです。Citrix Receiver for Webを使用する場合、基本のメモリ割り当てに加えてリソースごと、ユーザーごとに700バイトを追加で割り当てます。Citrix Receiver for Webを使用する場合、リソースごとおよびユーザーごとに、このバージョンのStoreFrontで基本の4GBメモリ要件に加えて、追加の700バイトを使用できるよう環境を設計します。

実際のユーザーアクティビティは上記シミュレーションとは異なるため、サーバーでサポートされるユーザー接続数は異なります。

重要：サーバーグループ内のすべてのサーバーは同じ場所に配置されている必要があります。StoreFrontサーバーグループ内でオペレーティングシステムのバージョンやロケール設定が異なるサーバーを混在させることはサポートされていません。

タイムアウトに関する注意事項

場合によっては、StoreFrontストアと接続先のサーバーの間でネットワークなどの問題が発生し、ユーザーにとっては遅延や障害が発生する可能性があります。これを回避するために、管理者はストアのタイムアウト設定を変更できます。タイムアウトの設定を短く指定すると、StoreFrontはサーバーとの接続試行をいつまでも繰り返さずに別のサーバーに接続しようとします。この設定は、フェールオーバーを目的として複数のサーバーを構成している場合などに便利です。

タイムアウトを長く設定すると、StoreFrontは1つのサーバーからの応答をその期間だけ待機します。この設定は、ネットワークやサーバーの信頼性が保証されず、遅延がよく発生する環境でメリットがあります。

Citrix Receiver for Webにもタイムアウトの設定があり、Citrix Receiver for Webサイトがストアからの応答を待つ時間を制御します。このタイムアウト値を変更するときは、ストアのタイムアウト以上の時間を設定します。タイムアウトの時間を長くすると耐障害性が向上しますが、ユーザーは長い遅延を経験する可能性があります。タイムアウトの時間を短くすると、ユーザーにとっての遅延は減りますが、接続の失敗が増える可能性があります。

タイムアウトの設定について詳しくは、「通信のタイムアウト期間およびサーバー再試行回数の構成」および「通信のタイムアウト期間および再試行回数の構成」を参照してください。

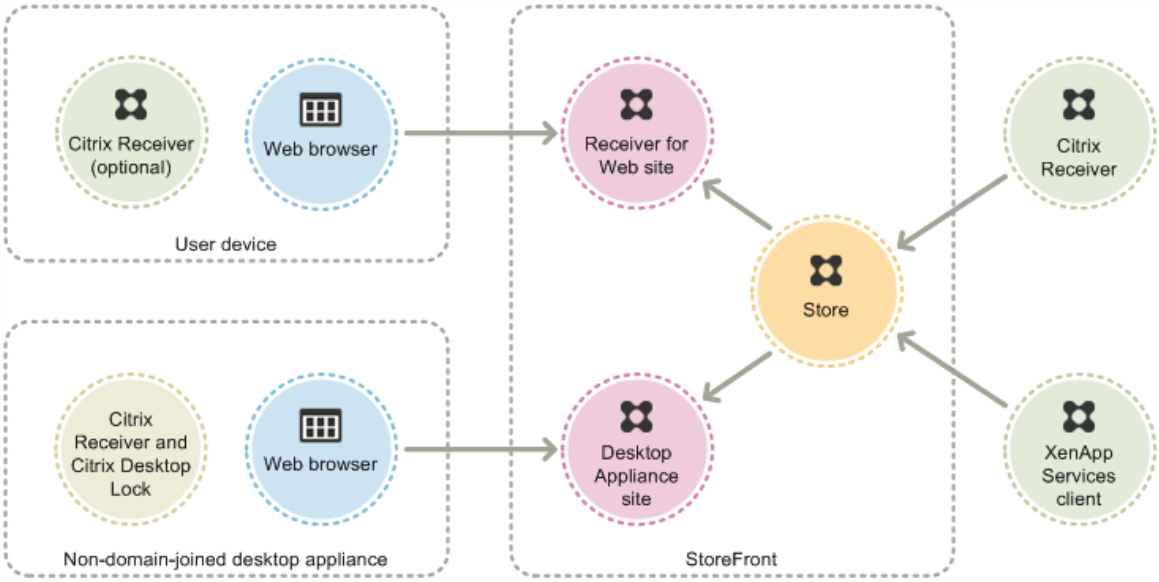
ユーザーアクセスのオプション

Aug 14, 2017

ユーザーは、以下の4つの方法でStoreFrontストアにアクセスできます。

- Citrix Receiver - 適切なバージョンのCitrix Receiverのユーザーは、Citrix Receiverのユーザーインターフェイスから StoreFrontストアにアクセスできます。Citrix Receiverからストアに透過的にアクセスできるため、最も簡単であり、より多くの機能が提供されます。
- Citrix Receiver for Webサイト - 適切なバージョンのWebブラウザーのユーザーは、Citrix Receiver for WebサイトからStoreFrontストアにアクセスすることができます。デフォルトでは、デスクトップとアプリケーションにアクセスするために、適切なバージョンのCitrix Receiverも必要です。ただし、管理者は、Citrix ReceiverをインストールできないユーザーがHTML5互換のWebブラウザーからデスクトップやアプリケーションに直接アクセスできるように、Citrix Receiver for Webサイトを構成できます。デフォルトでは、管理者が新しいストアを作成するときにそのストアのCitrix Receiver for Webサイトが作成されます。
- Desktop Applianceサイト - ドメインに参加していないデスクトップアプライアンスのユーザーは、全画面モードのWebブラウザーでデスクトップアプライアンスサイトにアクセスして自分のデスクトップにアクセスします。管理者がCitrix StudioでXenDesktop環境の新しいストアを作成すると、デフォルトでそのストアのデスクトップアプライアンスサイトが作成されます。
- XenApp Services URL - ドメインに参加しているデスクトップアプライアンスのユーザー、Citrix Desktop Lockを実行している再目的化されたPCのユーザー、およびアップグレードできない古いバージョンのCitrixクライアントのユーザーは、XenApp Servicesサイトからストアに接続できます。デフォルトでは、新しいストアを作成するときに、XenApp ServicesサイトのURLが有効になります。

この図は、ユーザーがStoreFrontストアにアクセスするためのオプションを示しています。



Citrix Receiver

Citrix Receiverのユーザーインターフェイスでストアにアクセスすると、最良のユーザーエクスペリエンスと多くの機能が提供されます。この方法でストアにアクセスできるCitrix Receiverのバージョンについては、「システム要件」を参照してください。

Citrix Receiverでは、ビーコンポイントとして内部URLおよび外部URLを使用します。これらのビーコンポイントにCitrix Receiverでアクセスできるかどうかにより、ユーザーがローカルに接続されているのかパブリックネットワークに接続されているのかが識別されます。ユーザーがデスクトップやアプリケーションにアクセスすると、そのリソースを提供するサーバー

がそのユーザーの位置情報に基づいて適切な接続詳細をCitrix Receiverに返します。これにより、ユーザーがCitrix Receiverでデスクトップやアプリケーションにアクセスするときに再ログオンする必要がなくなります。詳しくは、「ビーコンポインの構成」を参照してください。

Citrix Receiverをインストールしたら、デスクトップやアプリケーションのストアに接続するための構成を行う必要があります。管理者は、次のいずれかの方法を使用してユーザーによる構成操作を簡略化できます。

重要：デフォルトでは、Citrix ReceiverはストアへのHTTPSを必要とします。StoreFrontがHTTPS用に構成されていない場合、Citrix ReceiverでHTTP接続が使用されるようにユーザーが構成を変更する必要があります。実稼働環境では、StoreFrontへのすべてのユーザー接続が保護されるようにしてください。詳しくは、「*コマンドラインパラメーターを使用したCitrix Receiver for Windows*の構成とインストール」を参照してください。

プロビジョニングファイル

管理者は、ストアへの接続情報が定義されたプロビジョニングファイルをユーザーに提供します。Citrix Receiverをインストールした後で、提供されたCRファイルをユーザーが開くと、ストアのアカウントが自動的に構成されます。Citrix Receiver for Webサイトのデフォルトでは、そのサイトの単一ストア用のプロビジョニングファイルがユーザーに提供されます。管理者は、使用する各ストアのReceiver for Webサイトからプロビジョニングファイルをダウンロードするようユーザーに指示します。また、ユーザーの設定をより詳細に管理するには、Citrix StoreFront管理コンソールで特定のストアの接続情報を定義したプロビジョニングファイルを生成できます。その後で、それらのファイルを適切なユーザーに配布します。詳しくは、「ユーザーに対するストアプロビジョニングファイルのエクスポート」を参照してください。

セットアップURLの自動生成

Mac OSのユーザーには、Citrix Receiver for Mac Setup URL Generatorを使ってストアの接続情報を含んでいるセットアップURLを生成し、それをユーザーに提供できます。ユーザーがCitrix Receiverをインストールした後で、管理者から提供されたURLをクリックするとストアのアカウントが自動的に構成されます。管理者は、Citrix Receiver for Mac Setup URL Generatorで展開環境の詳細を入力してURLを生成し、そのURLをユーザーに配布します。

ユーザーによる構成

ユーザーがCitrix Receiverの構成に慣れている場合は、自分でストアのURLを入力して新しいアカウントを作成できます。NetScaler Gateway 10.1またはAccess Gateway 10経由でStoreFrontにアクセスするリモートユーザーは、そのゲートウェイアプライアンスのURLを入力します。Citrix Receiverでの初回接続時に、アカウントの構成に必要な情報が取得されます。Access Gateway 9.3経由で接続するユーザーは、自分でアカウントをセットアップすることはできません。上記のいずれかの方法を使用する必要があります。詳しくは、Citrix Receiverのドキュメントを参照してください。

メールアドレスによるアカウント検出

Citrix Receiverをデバイスに初めてインストールするユーザーは、Citrix社のWebサイトまたは内部ネットワーク上のダウンロードページからCitrix Receiverをダウンロードして、自分のメールアドレスを入力してアカウントをセットアップできます。管理者は、Microsoft Active Directory DNS（Domain Name System：ドメイン名システム）サーバー上でNetScaler GatewayまたはStoreFrontに対するサービスロケーション（SRV）ロケーターリソースレコードを構成します。ユーザーはストアへのアクセス情報を知っている必要はありません。代わりに、Citrix Receiverの初回構成時に自分のメールアドレスを入力します。Citrix Receiverはメールアドレスで指定されたドメインのDNSサーバーにアクセスして、SRVリソースレコードに追加されている詳細を取得します。これにより、アクセスできるストアの一覧がCitrix Receiverに表示されます。

メールアドレスによるアカウント検出を構成する

メールアドレスによるアカウント検出を有効にすると、デバイスにCitrix Receiverを新規インストールしたユーザーが、自分のメールアドレスを入力することでアカウントを自動的にセットアップできます。ユーザーがCitrix ReceiverをCitrix社のWebサ

イトまたは内部ネットワーク上のダウンロードページからダウンロードする場合は、ユーザーがストアへのアクセス方法を知っていなくてもCitrix Receiverをインストールして構成できます。Citrix ReceiverをReceiver for Webサイトなどのほかの場所からダウンロードする場合は、メールアドレスによるアカウント検出を使用できます。Citrix Receiver for Webからダウンロードしたreceiverweb.exeまたはReceiverWeb.dmgでは、ストアの構成は求められません。この場合も、ユーザーは［アカウントの追加］を使用してメールアドレスを入力できます。

Citrix Receiverの初回構成時に、ユーザーのメールアドレスまたはストアのURLを入力するためのダイアログボックスが開きます。ユーザーがメールアドレスを入力すると、Citrix Receiverはメールアドレスで指定されたドメインのMicrosoft Active Directory DNS（Domain Name System：ドメイン名システム）サーバーにアクセスして、ユーザーが選択可能なストアの一覧を取得します。

Citrix Receiverでユーザーのメールアドレスからストアを検索できるようにするには、DNSサーバー上でNetScaler GatewayまたはStoreFrontに対するサービスロケーション（SRV）ロケーターリソースレコードを構成します。また、フォールバックとして「discoverReceiver. domain」という名前のサーバーにStoreFrontを展開することもできます（ここではユーザーのメールアカウントのドメインです）。指定されたドメインにSRVレコードが見つからない場合、Citrix Receiverは「discoverReceiver」という名前のマシンを検索してStoreFrontサーバーを検出します。

メールアドレスによるアカウント検出を有効にするには、NetScaler GatewayアプライアンスまたはStoreFrontサーバー上に有効なサーバー証明書をインストールする必要があります。ルート証明書へのチェーンのすべてが有効である必要もあります。ユーザーエクスペリエンスを向上させるには、サブジェクトまたはサブジェクトの別名（SAN：Subject Alternative Name）エントリがdiscoverReceiver.domainである証明書をインストールします（ここで<domain>はユーザーのメールアカウントのドメインです）。このドメインのワイルドカード証明書を使用することもできますが、そのような証明書の使用が社内のセキュリティポリシーで許可されていることを確認してください。ユーザーのメールアカウントを含んでいるドメイン用のほかの証明書を使用することもできますが、ユーザーがCitrix ReceiverでStoreFrontサーバーに最初に接続したときに、証明書に関する警告が表示されます。上記以外の証明書を使用してメールアドレスによるアカウント検出機能を使用することはできません。

社内ネットワークの外から接続するユーザーに対してメールアドレスによるアカウント検出を有効にするには、NetScaler GatewayでStoreFront接続の詳細を構成する必要があります。詳しくは、「Connecting to StoreFront by Using Email-Based Discovery」を参照してください。

SRVレコードのDNSサーバーへの追加

1. Windowsの［**スタート**］画面で［**管理ツール**］をクリックして、［**管理ツール**］フォルダーの［**DNS**］をクリックします。
2. **DNSマネージャー**の左側のペインで、前方参照ゾーンまたは逆引き参照ゾーンのドメインを選択します。ドメインを右クリックして［**その他の新しいレコード**］を選択します。
3. ［**リソースレコードの種類**］ダイアログボックスで、［**サービスロケーション（SRV）**］を選択して［**レコードの作成**］をクリックします。
4. ［**新しいリソースレコード**］ダイアログボックスで、［**サービス**］ボックスにホスト値の**_citrixreceiver**を入力します。
5. ［**プロトコル**］ボックスに、値**_tcp**を入力します。
6. ［**このサービスを提供しているホスト**］ボックスに、NetScaler Gatewayアプライアンス（ローカルおよびリモートのユーザーをサポートする場合）またはStoreFrontサーバー（ローカルユーザーのみをサポートする場合）の完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）とポートを*servername.domain:port*形式で入力します。
   環境内に内部DNSサーバーと外部DNSサーバーの両方がある場合は、内部DNSサーバー上にStoreFrontサーバーFQDNのSRVレコードを追加し、外部DNSサーバー上にNetScaler Gateway FQDNの別のSRVレコードを追加できます。この構成により、リモートユーザーにはNetScaler Gatewayの接続情報が提供され、ローカルユーザーにはStoreFrontの接続情報が提供されます。
7. NetScaler GatewayアプライアンスにSRVレコードを構成した場合、セッションプロファイルまたはグローバル設定で

StoreFront接続の詳細をNetScaler Gatewayに追加します。

Citrix Receiver for Webサイト

適切なバージョンのWebブラウザーのユーザーは、Citrix Receiver for WebサイトからStoreFrontストアにアクセスすることができます。管理者が新しいストアを作成すると、そのストアのCitrix Receiver for Webサイトが自動的に作成されます。Citrix Receiver for Webサイトのデフォルト構成では、デスクトップとアプリケーションにアクセスするために、ユーザーが適切なバージョンのCitrix Receiverをインストールする必要があります。Citrix Receiver for WebサイトでサポートされるCitrix ReceiverとWebブラウザーのバージョンについて詳しくは、「ユーザーデバイスの要件」を参照してください。

デフォルトでは、ユーザーがWindowsまたはMac OS Xが動作するコンピューターからCitrix Receiver for Webサイトにアクセスすると、Citrix Receiverがユーザーデバイスにインストール済みであるかどうかが判別されます。Citrix Receiverが検出されない場合は、プラットフォームに適したCitrix Receiverをダウンロードしてインストールするためのページが開きます。デフォルトのダウンロード元はCitrix社のWebサイトですが、StoreFrontサーバーにインストールファイルをコピーして、ユーザーにこれらのローカルファイルを提供することもできます。Citrix Receiverのインストールファイルをローカルに保存すると、古いバージョンのクライアントを使用しているユーザーに対して、StoreFrontサーバー上のCitrix Receiverにアップグレードするためのオプションを提供することもできます。Citrix Receiver for WindowsおよびCitrix Receiver for Macの展開を構成する方法について詳しくは、「Citrix Receiver for Webサイトの構成」を参照してください。

Citrix Receiver for HTML5

Citrix Receiver for HTML5はStoreFrontのコンポーネントであり、デフォルトでCitrix Receiver for Webサイトに統合されています。Citrix Receiver for WebサイトのCitrix Receiver for HTML5を有効にすると、Citrix Receiverをインストールできないユーザーもリソースにアクセスできるようになります。Citrix Receiver for HTML5を使用すると、デスクトップやアプリケーションにHTML5互換のWebブラウザーからアクセスできます。デバイスにCitrix Receiverをインストールする必要はありません。サイトのCitrix Receiver for HTML5は、デフォルトで無効になります。Citrix Receiver for HTML5の有効化について詳しくは、citrix-receiver-download-page-template.htmlを参照してください。

Citrix Receiver for HTML5でデスクトップやアプリケーションにアクセスするには、HTML5互換のWebブラウザーでCitrix Receiver for Webサイトを開きます。Citrix Receiver for HTML5でサポートされるオペレーティングシステムとWebブラウザーについて詳しくは、「ユーザーデバイスの要件」を参照してください。

Citrix Receiver for HTML5は、内部ネットワーク上のユーザーとNetScaler Gateway経由で接続するリモートユーザーの両方が使用できます。内部ネットワークからの接続の場合、Citrix Receiver for HTML5では、Citrix Receiver for Webサイトでサポートされる一部の製品で配信されるデスクトップおよびアプリケーションへのアクセスのみがサポートされます。管理者がStoreFrontを構成するときにCitrix Receiver for HTML5をオプションとして選択すると、NetScaler Gateway経由で接続するユーザーがより多くの製品で提供されたリソースにアクセスできるようになります。Citrix Receiver for HTML5を使用する場合は、特定のバージョンのNetScaler Gatewayが必要です。詳しくは、「インフラストラクチャの要件」を参照してください。

デフォルトでは、内部ネットワーク上のローカルユーザーがXenDesktopやXenAppで提供されるリソースにCitrix Receiver for HTML5でアクセスすることはできません。Citrix Receiver for HTML5でデスクトップやアプリケーションへのローカルアクセスを有効にするには、XenDesktopおよびXenAppのサーバー側でポリシーの［ICA WebSockets接続］を有効にする必要があります。ファイアウォールとそのほかのネットワークデバイスで、ポリシーで指定されたCitrix Receiver for HTML5ポートへのアクセスが許可されていることを確認してください。詳しくは、「WebSocketのポリシー設定」を参照してください。

デフォルトでは、Citrix Receiver for HTML5は新しいブラウザータブでデスクトップやアプリケーションを起動します。ただし、ユーザーがCitrix Receiver for HTML5を使用してショートカットからリソースを起動した場合、既存のブラウザータブのCitrix Receiver for Webサイトが置き換わり、そこでデスクトップまたはアプリケーションが起動します。Receiver for Webサイトと同じタブでリソースが常に起動するようにCitrix Receiver for HTML5を構成することもできます。詳しくは、「Citrix

Receiver for HTML5のブラウザータブ使用の構成」を参照してください。

リソースのショートカット

Citrix Receiver for Webサイトからアクセスできるデスクトップやアプリケーションのリンクを生成できます。生成したリンクを内部ネットワーク上でホストされているWebサイトに埋め込んで、ユーザーがすばやくリソースにアクセスできるようにします。ユーザーがリンクをクリックすると、Receiver for Webサイトにリダイレクトされます。ここで、ユーザーがReceiver for Webサイトにログオンしていない場合はログオンします。Citrix Receiver for Webサイトでは、リソースが自動的に起動します。ユーザーがサブスクライブしていないアプリケーションの場合は、自動的にサブスクライブされます。リソースのショートカットの生成について詳しくは、「Citrix Receiver for Webサイトの構成」を参照してください。

Citrix Receiver for Webサイトからアクセスするデスクトップやアプリケーションと同様に、ショートカットを使用する場合もユーザーがCitrix ReceiverまたはCitrix Receiver for HTML5を使用する必要があります。Citrix Receiver for Webサイトで使用される方法（Citrix ReceiverまたはReceiver for HTML5）は、サイトの構成、Citrix Receiverをユーザーのデバイスで検出できるかどうか、およびHTML5互換のWebブラウザーを使用しているかどうかによって異なります。セキュリティ上の理由により、Internet Explorerユーザーには、ショートカット経由でアクセスしたリソースの起動を確認するメッセージが表示される場合があります。このメッセージが表示されなくなるようにするには、Internet Explorerの［ローカルイントラネット］または［信頼済みサイト］のゾーンにReceiver for Webサイトを追加するようユーザーに指示します。ショートカット経由でCitrix Receiver for Webサイトにアクセスする場合、ワークスペースコントロールとデスクトップの自動起動機能はどちらもデフォルトで無効になります。

アプリケーションのショートカットを生成するときは、Citrix Receiver for Webサイトで配信されているアプリケーションの名前が重複していないことを確認してください。ショートカットでは、同じ名前を持つアプリケーションの複数のインスタンスを区別できません。同様に、単一のデスクトップグループの複数のデスクトップインスタンスをCitrix Receiver for Webサイトで配信する場合、インスタンスごとに異なるショートカットを作成することはできません。ショートカットでは、コマンドラインパラメーターをアプリケーションに渡すことはできません。

アプリケーションのショートカットを生成するには、そのショートカットをホストする内部WebサイトのURLをStoreFrontで一覧に追加します。ユーザーがWebサイト上のショートカットをクリックすると、この一覧が照会され、要求が信頼されるWebサイトからのものであるかどうか確認されます。ただし、NetScaler Gateway経由で接続するユーザーの場合、URLがStoreFrontに渡されないため、ショートカットをホストしているWebサイトは検証されません。信頼される内部Webサイト上のショートカットにのみリモートユーザーがアクセスできるようにするには、これらのサイトへのアクセスのみが許可されるようにNetScaler Gatewayを構成します。詳しくは、http://support.citrix.com/article/CTX123610を参照してください。

サイトのカスタマイズ

Citrix Receiver for Webサイトでは、ユーザーインターフェイスをカスタマイズできます。表示される文字列、カスケーディングスタイルシート、およびJavaScriptファイルを編集できます。また、ログオン前やログオフ後にカスタムの画面を表示したり、言語パックを追加したりすることもできます。

重要な注意事項

ユーザーがCitrix Receiver for Webサイトからストアにアクセスする場合、アプリケーションの同期機能など、Citrix Receiver内でのストアへのアクセスでサポートされる多くの機能を使用できます。以下の制限事項を考慮して、Citrix Receiver for Webサイトでユーザーにストアへのアクセスを提供するかどうかを決定してください。

- 1つのCitrix Receiver for Webサイトから複数のストアにアクセスすることはできません。
- Citrix Receiver for Webサイトでは、SSL（Secure Sockets Layer）仮想プライベートネットワーク（VPN）接続を開始できません。VPN接続なしでNetScaler Gatewayを介してログオンしているユーザーは、App ControllerによりVPN接続を要求

されるWebアプリケーションにアクセスできません。
- Citrix Receiver for Webサイトからストアにアクセスする場合、サブスクライブしたアプリケーションはWindowsの[スタート]画面に追加されません。
- Citrix Receiver for Webサイトを経由してアクセスするホストアプリケーションでファイルタイプの関連付けを使用して、ローカルドキュメントを開くことはできません。
- オフラインアプリケーションには、Citrix Receiver for Webサイトからアクセスできません。
- Citrix Receiver for Webサイトでは、ストアに統合したCitrix Online製品はサポートされません。Citrix Receiver for WebサイトからCitrix Online製品にアクセスできるようにするには、App Controllerで配信するか、ホストされるアプリケーションとして公開する必要があります。
- VDAがXenApp 7.6またはXenDesktop 7.6でSSLが有効になっている、またはユーザーがNetScaler Gatewayを使って接続している場合、HTTPS接続でCitrix Receiver for HTML5を使用できます。
- Mozilla FirefoxでHTTPS接続のCitrix Receiver for HTML5を使用するには、Firefoxのアドレスバーに「about:config」と入力し、[network.websocket.allowInsecureFromHTTPS]をtrueに設定します。

デスクトップアプライアンスサイト

ドメイン不参加のデスクトップアプライアンスを使用するユーザーは、デスクトップアプライアンスサイト経由でデスクトップにアクセスできます。ドメイン不参加のデバイスとは、StoreFrontサーバーを含んでいるMicrosoft Active Directoryフォレスト内のドメインに属していないデバイスを意味します。

管理者がCitrix StudioでXenDesktop環境の新しいストアを作成すると、デフォルトでそのストアのデスクトップアプライアンスサイトが作成されます。デスクトップアプライアンスサイトは、StoreFrontがXenDesktopの一部としてインストールおよび構成されている場合にのみデフォルトで作成されます。管理者は、Windows PowerShellコマンドを使用してデスクトップアプライアンスサイトを作成することもできます。詳しくは、「デスクトップアプライアンスサイトの構成」を参照してください。

デスクトップアプライアンスサイトでは、ローカルデスクトップにログオンするときと同じようなユーザーエクスペリエンスが提供されます。デスクトップアプライアンス上のWebブラウザーは、全画面モードで起動して、デスクトップアプライアンスサイトのログオン画面を表示するように構成されます。デフォルトでは、ユーザーがデスクトップアプライアンスサイトにログオンすると、そのユーザーに提供されているデスクトップのうち（アルファベット順で）最初のデスクトップが自動的に起動します。ストアで複数のデスクトップをユーザーに提供する場合は、デスクトップアプライアンスサイトに複数のデスクトップを表示して、ユーザーが選択できるように構成できます。詳しくは、「デスクトップアプライアンスサイトの構成」を参照してください。

デスクトップが起動すると全画面モードで表示され、Webブラウザーは非表示になります。ユーザーは、デスクトップアプライアンスサイトから自動的にログアウトされます。ユーザーがデスクトップからログオフすると、Webブラウザーが再度表示され、デスクトップアプライアンスサイトのログオン画面が開きます。デスクトップが起動すると、デスクトップにアクセスできない場合にデスクトップを再起動するためのリンクを含んでいるメッセージが表示されます。この機能を有効にするには、管理者がデリバリーグループを構成するときにユーザーによるデスクトップの再起動を許可する必要があります。詳しくは、「デリバリーグループ」を参照してください。

デスクトップへのアクセスを提供するには、デスクトップアプライアンス上に適切なバージョンのCitrix Receiverが必要です。通常、XenDesktop互換のアプライアンスベンダーは、Citrix Receiverを自社の製品に統合しています。Windowsアプライアンスの場合は、Citrix Desktop Lockもインストールして、デスクトップアプライアンスサイトのURLを指定する必要があります。Internet Explorerを使用する場合は、[ローカルイントラネット]または[信頼済みサイト]のゾーンにデスクトップアプライアンスサイトを追加する必要があります。Citrix Desktop Lockについて詳しくは、「ユーザーがローカルデスクトップにアクセスできないようにする」を参照してください。

重要な注意事項

デスクトップアプライアンスサイトは、ドメイン不参加のデスクトップアプライアンスからデスクトップにアクセスする内
ネットワーク上のローカルユーザーを対象としています。以下の制限事項を考慮して、デスクトップアプライアンスサイトで
ユーザーにストアへのアクセスを提供するかどうかを決定してください。

- ドメインに参加しているデスクトップアプライアンスや再目的化されたPCを展開する場合は、それらのアプライアンスや
  PCでは、ストアにデスクトップアプライアンスサイト経由でアクセスするように構成しないでください。ストアのXenAp
  ServicesサイトのURLを使用してCitrix Receiverを構成できますが、ドメイン参加および不参加の使用例の両方に、新しい
  Desktop Lockをお勧めします。詳しくは、「Citrix Receiver Desktop Lock」を参照してください。
- デスクトップアプライアンスサイトでは、社内ネットワーク外のリモートユーザーからの接続はサポートされません。
  NetScaler Gatewayにログオンするユーザーは、デスクトップアプライアンスサイトにアクセスできません。

XenApp ServicesサイトのURL

アップグレードできない古いバージョンのCitrixクライアントのユーザーは、クライアントを構成するときにストアのXenApp
ServicesサイトのURLを指定することにより、ストアにアクセスできるようになります。また、管理者は、ドメインに参加し
いるデスクトップアプライアンスのユーザー、およびCitrix Desktop Lockを実行している再目的化されたPCのユーザーが
XenApp Servicesサイト経由でストアにアクセスできるように構成することもできます。ドメインに参加しているデバイスと
は、StoreFrontサーバーを含んでいるActive Directoryフォレスト内のドメインに属しているデバイスを意味します。

StoreFrontでは、Citrix ReceiverからXenApp Servicesサイトへの近接カードを使ったパススルー認証がサポートされます。
Citrix Fast Connect APIを使用するCitrix Readyパートナー製品では、Citrix Receiver for WindowsからXenApp Servicesサイトを
介して効率的にストアにログオンできます。ユーザーは、近接カードを使ってワークステーションにログオンし、
XenDesktopおよびXenAppから提供されるデスクトップやアプリケーションに迅速に接続できます。詳しくは、最新のCitrix
Receiver for Windowsのドキュメントを参照してください。

デフォルトでは、管理者が新しいストアを作成するときに、そのストアのXenApp Services URLが有効になります。ストアの
XenApp Services URLは、http[s]://serveraddress/Citrix/storename/PNAgent/config.xmlという形式になります。ここで、
serveraddressはStoreFront展開環境のサーバーまたは負荷分散環境の完全修飾ドメイン名であり、storenameはストアの作成
時に指定した名前です。これにより、PNAgentプロトコルのみを使用できるCitrix ReceiverがStoreFrontに接続できます。
XenApp Services URLを経由してストアにアクセスできるクライアントについては、「ユーザーデバイスの要件」を参照して
ください。

重要な注意事項

XenApp ServicesサイトのURLは、Citrix Receiverにアップグレードできず、代替のアクセス方法を使用できないユーザーをサ
ポートするために使用されます。以下の制限事項を考慮して、XenApp Servicesサイトでユーザーにストアへのアクセスを提供
するかどうかを決定してください。

- ストアのXenApp Services URLは変更できません。
- 構成ファイルconfig.xmlを編集してXenApp Services URL設定を変更することはできません。
- XenApp Servicesサイトでは、指定ユーザー認証、ドメインパススルー認証、スマートカード認証、スマートカードパス
  ルー認証がサポートされます。デフォルトでは、指定ユーザー認証が有効になります。各XenApp Servicesサイトに構成で
  きる認証方法と各ストアで使用できるXenApp Servicesサイトは、それぞれ1つだけです。複数の認証方法を有効にするに
  は、個別のストアを作成して、それらのXenApp Servicesサイトで異なる認証方法を有効にします。この場合、どのストア
  にアクセスすべきかをユーザーに通知してください。詳しくは、「XML-based authentication」を参照してください。
- XenApp ServicesサイトではワークスペースコントロールがXenApp有効になり、この構成を変更したり無効にしたりすることはで
  きません。
- ユーザーのパスワード変更要求は、StoreFrontの認証サービスを介さず、ストアにデスクトップとアプリケーションを提
  供するXenDesktopおよびXenAppサーバーからドメインコントローラーに直接送信されます。

ユーザー認証

Aug 14, 2017

StoreFrontではユーザーがストアにアクセスするときにさまざまな認証方法がサポートされますが、ユーザーのアクセス方法とネットワークの場所によっては一部の認証方法を使用できない場合があります。セキュリティ上の理由により、最初のストアの作成時には一部の認証方法がデフォルトで無効になります。ユーザーの認証方法の有効化および無効化について詳しくは、「認証サービスの作成および構成」を参照してください。

ユーザー名とパスワード

ユーザーは、ストアにアクセスするときに、資格情報を入力すると認証されます。デフォルトでは、指定ユーザー認証が有効になります。指定ユーザー認証は、すべてのアクセス方法でサポートされます。

ユーザーがNetScaler Gatewayを使用してCitrix Receiver for Webにアクセスする場合、NetScaler Gatewayによりログオンおよび期限切れパスワードの変更処理が行われます。ユーザーが自分でパスワードを変更する場合は、Citrix Receiver for Webのユーザーインターフェイスを使用します。ユーザーがパスワードを変更するとNetScaler Gatewayセッションが終了します。ユーザーは再ログオンする必要があります。Citrix Receiver for Linuxユーザーは、有効期限切れのパスワードのみを変更できます。

SAML 認証

ユーザーはAccess Gatewayにログオンすることによって認証を受け、ストアにアクセスするときは自動的にログオンします。StoreFrontでは、NetScalerを経由することなく社内ネットワーク内でSAML認証を直接サポートすることができます。

SAML（Security Assertion Markup Language：セキュリティアサーションマークアップランゲージ）は、Microsoft AD FS（Active Directoryフェデレーションサービス）などのIDおよび認証製品で採用されている公開標準規格です。StoreFrontとSAML認証を統合することで、管理者はたとえば、ユーザーが一度社内ネットワークへログオンすれば、以降は公開アプリケーションにシングルサインオンできるようにすることができます。

要件：

- 手順5：Citrix Federated Authentication Serviceを再起動します。
- SAML 2.0準拠のIDプロバイダー（IdPs）：
  - SAMLバインドのみを使用するMicrosoft AD FS v4.0（Windows Server 2016）（WSフェデレーションバインドは不可）。詳しくは、Microsoftの「AD FS 2016 Deployment」および「AD FS 2016 Operations」を参照してください。
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2008 R2
  - NetScaler Gateway構成：
- StoreFrontの管理コンソールを使用して、SAML認証を新しい展開環境（「新しい展開環境の作成」を参照）または既存の展開環境（「認証サービスの構成」を参照）で構成します。また、PowerShellコマンドレットを使用してSAML認証を構成することもできます。「StoreFront SDK」を参照してください。
- Citrix Receiver for Windows（4.6以降）またはCitrix Receiver for Web

現在、NetScalerでのSAML認証の使用は、Citrix Receiver for Webサイトでサポートされています。

ドメインパススルー

ユーザーはドメインに参加しているWindowsコンピューターにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。StoreFrontをインストールする際、ドメインパススルー認証はデフォルトで無効になっています。ドメインパススルー認証は、Citrix ReceiverおよびXenApp Servicesサイトからストアに接続するユーザーに対して有効

にすることができます。Citrix Receiver for Webサイトは、Internet Explorerを使用する場合のみドメインパススルー認証をサポートします。管理コンソールのCitrix Receiver for Webサイトのノードでドメインパススルー認証を有効にし、Citrix Receiver for Windows上でSSONを構成する必要があります。Citrix Receiver for HTML5では、ドメイン資格情報のパススルー認証はサポートされません。ドメインパススルー認証を使用するには、ユーザーがCitrix Receiver for WindowsまたはOnline Plug-in for Windowsを使用する必要があります。また、Citrix Receiver for WindowsまたはOnline Plug-in for Windowsをユーザーのデバイスにインストールするときにパススルー認証を有効にする必要があります。

NetScaler Gatewayからのパススルー

ユーザーはNetScaler Gatewayにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。NetScaler Gatewayからのパススルー認証は、ストアへのリモートアクセスを最初に構成するときにデフォルトで有効になります。ユーザーは、Citrix ReceiverまたはCitrix Receiver for Webサイトを使用してNetScaler Gateway経由でストアに接続できます。デスクトップアプライアンスサイトでは、NetScaler Gatewayを経由する接続はサポートされません。NetScaler Gatewayを使用するためのStoreFrontの構成について詳しくは、「NetScaler Gateway接続の追加」を参照してください。

StoreFrontは、次のNetScaler Gateway認証方法でのパススルーをサポートします。

- **セキュリティトークン：**ユーザーは、セキュリティトークンから生成されるトークンコードから得られるパスコードを使用してNetScaler Gatewayにログオンします。トークンコードと暗証番号を組み合わせてパスコードにする場合もあります。セキュリティトークンのみによるパススルー認証を有効にする場合は、ユーザーに提供するリソースでほかの認証方法（Microsoft Active Directoryドメインの資格情報など）が使用されないようにしてください。
- **ドメインおよびセキュリティトークン：**NetScaler Gatewayにログオンするユーザーは、ドメイン資格情報とセキュリティトークンパスコードの両方を入力する必要があります。
- **クライアント証明書：**ユーザーは、NetScaler Gateway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を受け、NetScaler Gatewayにログオンします。ユーザーがスマートカードを使用してNetScaler Gatewayにログオンできるようにするには、クライアント証明書認証を構成します。クライアント証明書による認証は、ほかの種類の認証と共に2要素認証でも使用できます。

StoreFrontでは、リモートユーザーがストアにアクセスするときに資格情報を再入力しなくて済むように、NetScaler Gatewayの認証サービスを使用してリモートユーザーをパススルー認証します。ただし、デフォルトでは、パスワードを使用してNetScaler Gatewayにログオンするユーザーに対してのみパススルー認証が有効になります。スマートカードユーザーに対してNetScaler GatewayからStoreFrontへのパススルー認証を構成するには、資格情報の検証をNetScaler Gatewayに委任します。詳しくは、「認証サービスの作成と構成」を参照してください。

NetScaler Gateway Plug-inを使用すると、SSL（Secure Sockets Layer）仮想プライベートネットワーク（VPN）トンネルを介したパススルー認証でCitrix Receiver内からストアに直接接続できます。NetScaler Gateway Plug-inをインストールできないリモートユーザーも、パススルー認証によりCitrix Receiver内からストアに接続できます（クライアントレスアクセス）。クライアントレスアクセスを使ってストアに接続するには、クライアントレスアクセスをサポートするバージョンのCitrix Receiverが必要です。

また、Citrix Receiver for Webサイトに対するパススルー認証によるクライアントレスアクセスを有効にできます。これを行うには、セキュアリモートプロキシとして動作するようにNetScaler Gatewayを構成する必要があります。ユーザーはNetScaler Gatewayに直接ログオンして、Citrix Receiver for Webサイトを使用して再認証なしでアプリケーションにアクセスします。

クライアントレスアクセスによりApp Controllerリソースに接続するユーザーは、外部のSaaS（Software-as-a-Service）アプリケーションにのみアクセスできます。リモートユーザーが内部のWebアプリケーションにアクセスするには、NetScaler Gateway Plug-inを使用する必要があります。

Citrix Receiver内でストアにアクセスするリモートユーザーに対してNetScaler Gatewayでの2要素認証を有効にする場合は、

NetScaler Gatewayで2つの認証ポリシーを作成する必要があります。プライマリの認証方法としてRADIUS（Remote Authentication Dial-In User Service）を構成し、セカンダリの認証方法としてLDAP（Lightweight Directory Access Protocol）を構成します。セッションプロファイルでセカンダリの認証方法が使用されるように資格情報インデックスを変更して、LDAP資格情報がStoreFrontに渡されるようにします。NetScaler Gatewayアプライアンスを StoreFront構成に追加する場合は、［ログオンの種類］を［ドメインおよびセキュリティトークン］に設定します。詳しくは、http://support.citrix.com/article/CTX125364を参照してください。

NetScaler GatewayからStoreFrontへの複数ドメイン認証を有効にするには、各ドメインのNetScaler Gateway LDAP認証ポリシーで［SSO Name Attribute］をuserPrincipalNameに設定します。使用されるLDAPポリシーが特定されるように、NetScaler Gatewayのログオンページでユーザーにドメインを指定させることができます。StoreFrontに接続できるようにNetScaler Gatewayセッションプロファイルを構成する場合は、シングルサインオンドメインを指定しないでください。管理者は、各ドメイン間の信頼関係を構成する必要があります。明示的に信頼されるドメインのみにアクセスを制限せず、ユーザーがどのドメインからもStoreFrontへログオンできるようにします。

NetScaler Gateway展開環境でサポートされる場合は、SmartAccess機能を使用して、XenDesktopおよびXenAppリソースへのユーザーアクセスをNetScaler Gatewayセッションポリシーに基づいて制御できます。SmartAccessについて詳しくは、「How SmartAccess works for XenApp and XenDesktop」を参照してください。

スマートカード

ユーザーはスマートカードとPINを使ってストアにアクセスします。StoreFrontをインストールする際、スマートカード認証はデフォルトで無効になっています。スマートカード認証は、Citrix Receiver、Citrix Receiver for Web、デスクトップアプライアンスサイト、およびXenApp Servicesサイトからストアに接続するユーザーに対して有効にすることができます。

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

スマートカードは、XenDesktopおよびXenApp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にスマートカードでログオンするユーザーは、App Controllerで提供され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App Controller Webアプリケーションにアクセスするには、再度認証を受ける必要があります。

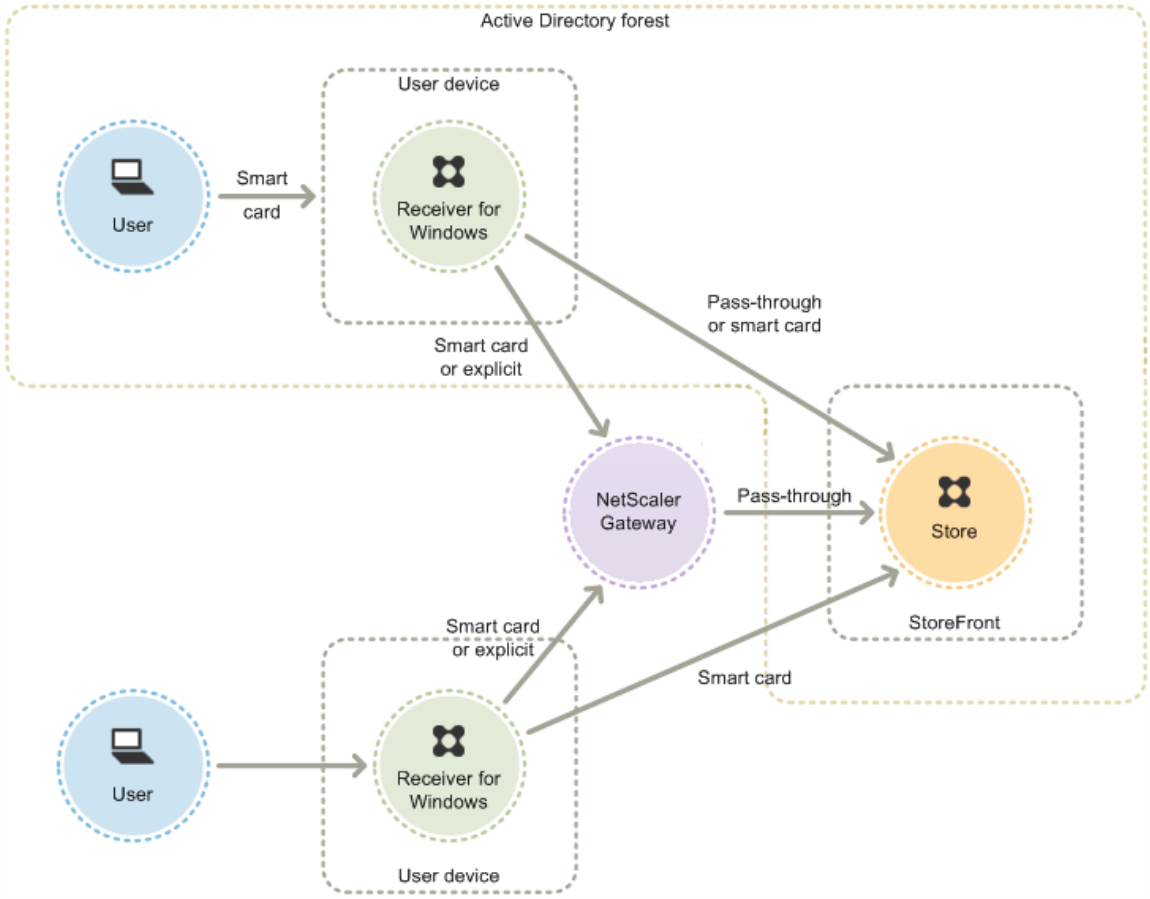
スマートカード認証を有効にする場合、StoreFrontサーバーが属しているMicrosoft Active Directoryドメインか、そのドメインと直接の双方向の信頼関係が設定されているドメインのいずれかにユーザーのアカウントが属している必要があります。双方向の信頼関係を含んでいるマルチフォレスト展開環境がサポートされます。

StoreFrontのスマートカード認証の構成は、ユーザーデバイス、インストールされているクライアント、およびデバイスがドメインに参加しているかどうかによって異なります。ドメインに参加しているデバイスとは、StoreFrontサーバーを含んでいるActive Directoryフォレスト内のドメインに属しているデバイスを意味します。

Citrix Receiver for Windowsでのスマートカードの使用

Citrix Receiver for Windowsを実行しているデバイスのユーザーは、スマートカードを使って直接またはNetScaler Gateway経由で認証を受けることができます。ドメイン参加デバイスとドメイン不参加デバイスの両方でスマートカード認証を使用できますが、ユーザーエクスペリエンスがわずかに異なります。

この図は、Citrix Receiver for Windowsを介したスマートカード認証を示しています。



ドメインに参加しているデバイスのローカルユーザーには、資格情報を再入力しなくて済むように、スマートカード認証を有効にします。ユーザーがスマートカードとPINを使ってデバイスにログオンしたら、それ以降PINを再入力する必要はありません。StoreFrontおよびデスクトップやアプリケーションにアクセスするときの認証は透過的に行われます。管理者は、Citrix Receiver for Windowsのパススルー認証を構成して、StoreFrontのドメインパススルー認証を有効にします。

ユーザーは、PINを使ってデバイスにログオンし、Citrix Receiver for Windowsの認証を受けます。アプリケーションおよびデスクトップを開始するときに、追加でPINの入力を求められることはありません。

ドメイン不参加デバイスのユーザーはCitrix Receiver for Windowsに直接ログオンするため、管理者は指定ユーザー認証へのフォールバックを有効にすることができます。管理者がスマートカード認証と指定ユーザー認証の両方を構成した場合、ユーザーは最初にスマートカードとPINを使ったログオンを要求されますが、スマートカードでログオンできない場合は指定ユーザー認証を選択することができます。

ユーザーがNetScaler Gateway経由でデスクトップやアプリケーションにアクセスする場合は、スマートカードとPINを使って最低でも2回ログオン操作を行う必要があります。これはドメイン参加デバイスとドメイン不参加デバイスの両方に適用されます。ユーザーは、スマートカードとPINを使ってデバイスにログオンし、デスクトップやアプリケーションにアクセスするときにもう一度PINを入力します。管理者は、NetScaler Gateway認証のStoreFrontへのパススルーを有効にして、資格情報の検証をNetScaler Gatewayに委任します。さらにNetScaler Gateway仮想サーバーを追加して、デスクトップやアプリケーションへのユーザー接続がそのNetScaler Gateway経由で行われるように構成します。ドメインに参加しているデバイスに対しては、Citrix Receiver for Windowsのパススルー認証も構成する必要があります。

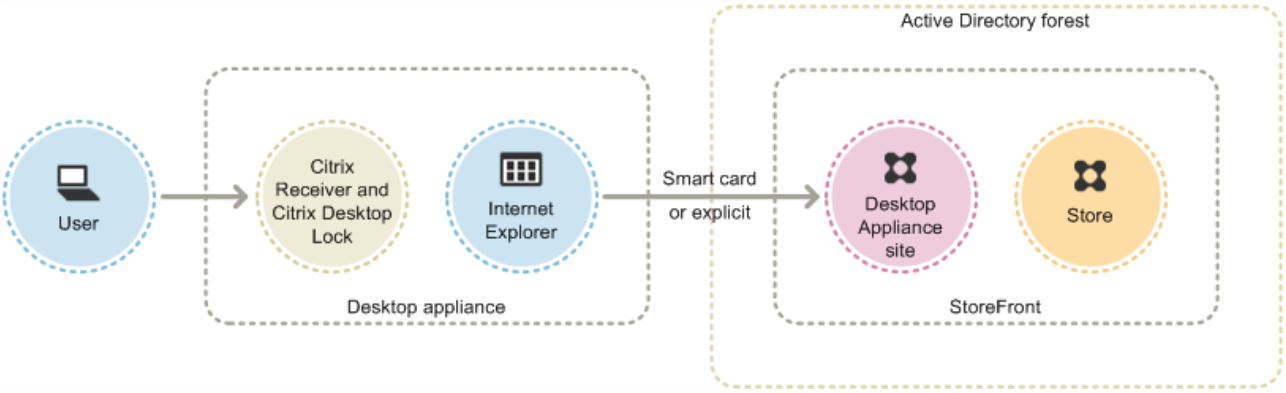
注:Citrix Receiver for Windows 4.2（最新バージョン）をお使いの場合、2つめのvServerをセットアップし、最適なゲートウェイルーティング機能を使用して、アプリケーションおよびデスクトップの開始時にPINの入力が不要となるようにすることができます。

ユーザーは、スマートカードとPINを使って、または指定ユーザーの資格情報を使ってNetScaler Gatewayにログオンできます。これにより、管理者はユーザーがNetScaler Gatewayにログオンするときに指定ユーザー認証へのフォールバックを有効にすることができます。ユーザーがStoreFrontに透過的に認証されるように、NetScaler GatewayからStoreFrontへのパススルー認証を構成し、スマートカードユーザーの資格情報の検証をNetScaler Gatewayに委任します。

デスクトップアプライアンスサイトでのスマートカードの使用

ドメイン不参加のWindowsデスクトップアプライアンスでは、ユーザーがスマートカードを使用してデスクトップにログオンできるように構成できます。アプライアンスにはCitrix Desktop Lockが必要で、デスクトップアプライアンスサイトへのアクセスにはInternet Explorerを使用する必要があります。

この図は、ドメイン不参加のデスクトップアプライアンスからのスマートカード認証を示しています。



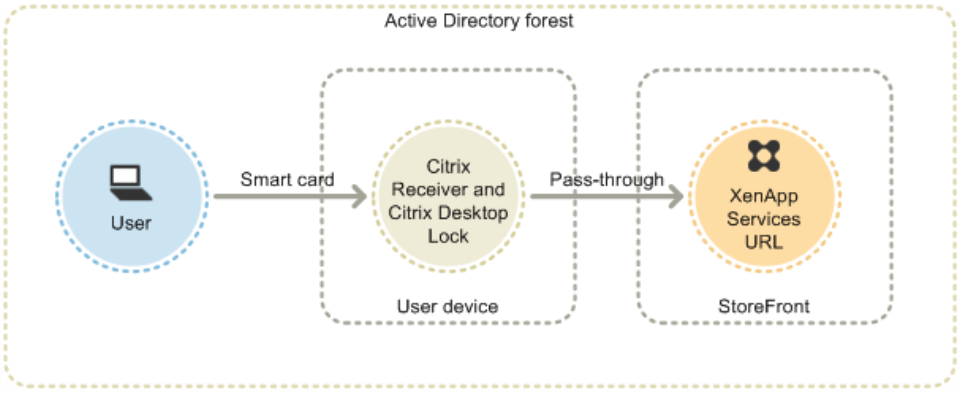
ユーザーがデスクトップアプライアンスにアクセスすると、Internet Explorerが全画面モードで起動し、デスクトップアプライアンスサイトのログオン画面が表示されます。ユーザーは、スマートカードとPINを使ってサイトの認証を受けます。デスクトップアプライアンスサイトでパススルー認証が構成されている場合、ユーザーはデスクトップやアプリケーションにアクセスするときに自動的に認証されます。PINの再入力は要求されません。パススルー認証が構成されていない場合は、デスクトップまたはアプリケーションにアクセスするときにPINをもう一度入力する必要があります。

管理者は、スマートカードでの認証に問題が生じた場合に指定ユーザー認証を使用できるように設定できます。これを行うには、デスクトップアプライアンスサイトにスマートカード認証と指定ユーザー認証の両方を構成します。この構成では、スマートカード認証がプライマリのアクセス方法とみなされます。そのため、ユーザーはまずPINの入力を要求されます。たとし、指定ユーザーの資格情報でログオンするためのリンクも表示されます。

XenApp Servicesサイトでのスマートカードの使用

ドメイン参加のデスクトップアプライアンスとCitrix Desktop Lockを実行している再目的化されたPCのユーザーは、スマートカードを使って認証を受けることができます。ほかのアクセス方法とは異なり、スマートカードのパススルー認証は、XenApp Servicesサイトでスマートカード資格情報が構成されている場合には自動的に有効になります。

この図は、Citrix Desktop Lockを実行しているドメイン参加のデバイスからのスマートカード認証を示しています。



ユーザーは、スマートカードとPINを使ってデバイスにログオンします。その後、Citrix Desktop Lockにより、ユーザーはXenApp Servicesサイトを介してサイレントにStoreFrontに認証されます。デスクトップやアプリケーションにアクセスするときは自動的に認証され、PINの再入力が要求されることはありません。

Citrix Receiver for Webでのスマートカードの使用

StoreFrontの管理コンソールを使用して、Citrix Receiver for Webでのスマートカード認証を有効にすることができます。

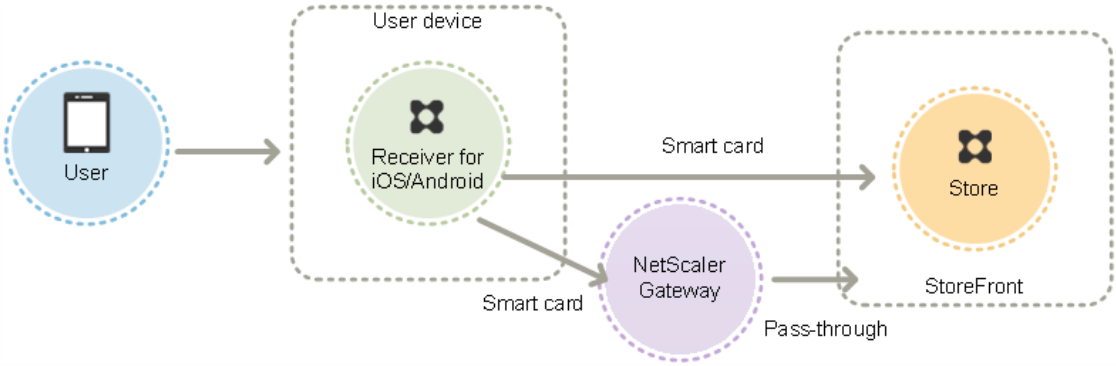
1. 左ペインで［Citrix Receiver for Web］ノードを選択します。
2. スマートカード認証を使用するサイトを選択します。
3. 右ペインで［認証方法の選択］を選択します。
4. ポップアップダイアログボックスでスマートカードのチェックボックスをオンにして、［OK］をクリックします。

ドメイン参加デバイスを使用するCitrix Receiver for WindowsユーザーがNetScaler Gatewayを使用せずにストアにアクセスする場合、XenDesktopおよびXenAppへのスマートカードでのパススルー認証を有効にすると、その設定がストアのすべてのユーザーに適用されます。デスクトップおよびアプリケーションに対するドメインパススルー認証とスマートカードパススルー認証の両方を有効にするには、これらの認証方法について個別のストアを作成する必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。

ドメイン参加デバイスを使用するCitrix Receiver for WindowsユーザーがNetScaler Gatewayを使用してストアにアクセスする場合、XenDesktopおよびXenAppへのスマートカードでのパススルー認証を有効にすると、その設定がストアのすべてのユーザーに適用されます。一部のユーザーに対してのみパススルー認証を有効にする場合は、それらのユーザー用に個別のストアを作成する必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。

Citrix Receiver for iOSおよびAndroidでのスマートカードの使用

Citrix Receiver for iOSおよびCitrix Receiver for Androidを実行しているデバイスのユーザーは、スマートカードを使って直接またはNetScaler Gateway経由で認証を受けることができます。また、ドメインに参加していないデバイスを使用することもできます。



ローカルネットワーク上のデバイスの場合、ユーザーは最低でも2回ログオン操作を行う必要があります。ユーザーがStoreFrontで認証する場合、または初めてストアを作成する場合は、スマートカードPINの入力が求められます。さらに、ユーザーがデスクトップやアプリケーションにアクセスするときに、もう一度PINを入力します。この認証方法を構成するには、StoreFrontでスマートカード認証を有効にして、VDAにスマートカードドライバーをインストールします。

これらのCitrix Receiverに対しては、スマートカード認証またはドメイン資格情報による認証のいずれかを指定する必要があります。スマートカード認証を有効にしてストアを作成した後でドメイン資格情報による接続を許可するには、スマートカード認証が無効な別のストアを追加する必要があります。

ユーザーがNetScaler Gateway経由でデスクトップやアプリケーションにアクセスする場合は、スマートカードとPINを使って最低でも2回ログオン操作を行う必要があります。ユーザーは、スマートカードとPINを使ってデバイスにログオンし、デスクトップやアプリケーションにアクセスするときにもう一度PINを入力します。管理者は、NetScaler Gateway認証のStoreFrontへのパススルーを有効にして、資格情報の検証をNetScaler Gatewayに委任します。さらにNetScaler Gateway仮想サーバーを追加して、デスクトップやアプリケーションへのユーザー接続がそのNetScaler Gateway経由で行われるように構成します。

ユーザーは、管理者が接続の認証をどう指定しているかに応じて、スマートカードとPIN、または指定ユーザー認証の資格情報を使用してNetScaler Gatewayにログオンできます。ユーザーがStoreFrontに透過的に認証されるように、NetScaler GatewayからStoreFrontへのパススルー認証を構成し、スマートカードユーザーの資格情報の検証をNetScaler Gatewayに委任します。認証方法を変更する場合は、接続を削除し、再作成する必要があります。

Citrix Receiver for Linuxでのスマートカードの使用

Citrix Receiver for Linuxを実行するデバイスを使用するユーザーは、ドメイン不参加のWindowsデバイスのユーザーと同様の方法で、スマートカードを使用して認証できます。ユーザーがスマートカードを使用してLinuxデバイスで認証されている場合にも、Citrix Receiver for Linuxには入力済みのPINを取得または再利用するメカニズムがありません。

Citrix Receiver for Windows用に構成したときと同じ方法で、サーバー側のコンポーネントのスマートカード認証を構成します。詳しくは、「How To Configure StoreFront 2.x and Smart Card Authentication for Internal Users using Stores」を参照してください。また、スマートカードの使用方法について詳しくは、docs.citrix.comの「Citrix Receiver for Linux」を参照してください。

ユーザーは最低でも1回のログオン操作を行う必要があります。ユーザーは、スマートカードとPINを使ってデバイスにログオンし、Citrix Receiver for Linuxの認証を受けます。ユーザーがデスクトップやアプリケーションにアクセスするときにPINを再入力する必要はありません。管理者は、StoreFrontのスマートカード認証を有効にします。

ユーザーはCitrix Receiver for Linuxに直接ログオンするので、管理者は指定ユーザー認証へのフォールバックを有効にすることができます。管理者がスマートカード認証と指定ユーザー認証の両方を構成した場合、ユーザーは最初にスマートカードとPINを使ったログオンを要求されますが、スマートカードでログオンできない場合は指定ユーザー認証を選択することができます。

ユーザーがNetScaler Gateway経由でデスクトップやアプリケーションにアクセスする場合は、スマートカードとPINを使って最低でも1回のログオン操作を行う必要があります。ユーザーは、スマートカードとPINを使ってデバイスにログオンします。デスクトップやアプリケーションにアクセスするときに、PINを再入力する必要はありません。管理者は、NetScaler Gateway認証のStoreFrontへのパススルーを有効にして、資格情報の検証をNetScaler Gatewayに委任します。さらにNetScaler Gateway仮想サーバーを追加して、デスクトップやアプリケーションへのユーザー接続がそのNetScaler Gateway経由で行われるように構成します。

ユーザーは、スマートカードとPINを使って、または指定ユーザーの資格情報を使ってNetScaler Gatewayにログオンできます。これにより、管理者はユーザーがNetScaler Gatewayにログオンするときに指定ユーザー認証へのフォールバックを有効にすることができます。ユーザーがStoreFrontに透過的に認証されるように、NetScaler GatewayからStoreFrontへのパススルー認証を構成し、スマートカードユーザーの資格情報の検証をNetScaler Gatewayに委任します。

Citrix Receiver for LinuxでXenApp Servicesサポートサイトにアクセスする場合、スマートカードはサポートされません。

サーバーとCitrix Receiverの両方でスマートカードのサポートを有効にすると、スマートカード証明書のアプリケーションポリシーで許可されていれば、以下の目的でスマートカードを使用できます。

- スマートカードによるログオン認証。スマートカードを使って、Citrix XenAppサーバーやXenDesktopサーバーにログオンするユーザーを認証します。
- スマートカード対応アプリケーションのサポート。スマートカード対応の公開アプリケーションを使って、ローカルのスマートカードリーダーにアクセスできます。

XenApp Servicesサポートサイトでのスマートカードの使用

XenApp Servicesサポートサイトにログオンしてアプリケーションやデスクトップを開始するユーザーは、スマートカードを使って認証を受けることができます。特定のハードウェア、オペレーティングシステム、およびCitrix Receiverを使用する必要はありません。ユーザーがXenApp Servicesサポートサイトにアクセスしてスマートカードと PINを使ってログオンすると、PNAがユーザーIDを決定してStoreFrontでの認証を行い、使用できるリソースを返します。

パススルーおよびスマートカード認証が正しく動作するためには、[Citrix XML Serviceへの要求を信頼する] をオンにする必要があります。

Delivery Controller上でローカルの管理者アカウントを使用してWindows PowerShellを起動して、コマンドプロンプトで次のコマンドを実行します。これにより、StoreFrontから送信されたXML要求をDelivery Controllerが信頼するようになります。次の手順は、XenApp 7.5～7.8、およびXenDesktop 7.0～7.8に適用されます。

1. 「asnp Citrix*.」と入力してCitrixコマンドレットを読み込みます
2. **Add-PSSnapin citrix.broker.admin.v2**を実行します。
3. **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True**を実行します。
4. PowerShellを閉じます。

XenApp Servicesサポートのスマートカード認証方法の構成について詳しくは、「XenApp Services URLの認証の構成」を参照してください。

重要な注意事項

StoreFrontでのユーザー認証にスマートカードを使用する場合は、次の要件と制限があります。

- スマートカード認証で仮想プライベートネットワーク（VPN）トンネルを使用するには、ユーザーがNetScaler Gateway Plug-inをインストールしてWebページ経由でログオンする必要があります。この場合、各手順でスマートカードとPINによる認証が必要になります。スマートカードユーザーは、NetScaler Gateway Plug-inを使用したStoreFrontへのパススルー

認証を使用できません。

- 同一ユーザーデバイス上で複数のスマートカードやスマートカードリーダーを使用することのできますが、スマートカードでのパススルー認証を有効にする場合は、ユーザーがデスクトップやアプリケーションにアクセスするときにスマートカードが1枚のみ挿入されていることを確認する必要があります。
- アプリケーション内でスマートカードを使用する場合（デジタル署名または暗号化機能など）、スマートカードの挿入またはPINの入力を求めるメッセージが表示されることがあります。これは、同時に複数のスマートカードが挿入されている場合に発生します。また、構成設定（通常グループポリシーを使用して構成されるPINキャッシュなどのミドルウェア設定）が原因で発生することもあります。スマートカードをリーダーに挿入しているにもかかわらずスマートカードの挿入を求めるメッセージが表示された場合は、［キャンセル］をクリックする必要があります。ただし、PINの入力が求められた場合は、PINを再入力する必要があります。
- ドメイン参加デバイスを使用するCitrix Receiver for WindowsユーザーがNetScaler Gatewayを使用せずにストアにアクセスする場合、XenDesktopおよびXenAppへのスマートカードでのパススルー認証を有効にすると、その設定がストアのすべてのユーザーに適用されます。デスクトップおよびアプリケーションに対するドメインパススルー認証とスマートカードパススルー認証の両方を有効にするには、これらの認証方法について個別のストアを作成する必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。
- ドメイン参加デバイスを使用するCitrix Receiver for WindowsユーザーがNetScaler Gatewayを使用してストアにアクセスする場合、XenDesktopおよびXenAppへのスマートカードでのパススルー認証を有効にすると、その設定がストアのすべてのユーザーに適用されます。一部のユーザーに対してのみパススルー認証を有効にする場合は、それらのユーザー用に個別のストアを作成する必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。
- 各XenApp Servicesサイトに構成できる認証方法と各ストアで使用できるXenApp Servicesサイトは、それぞれ1つだけです。スマートカード認証に加えてほかの認証方法を有効にする必要がある場合は、認証方法ごとに個別のストアを作成し、それぞれのストアにXenApp Servicesサイトを1つずつ割り当てる必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。
- StoreFrontインストール時のMicrosoftインターネットインフォメーションサービス（IIS）のデフォルト構成では、StoreFront認証サービスの証明書認証URLへのHTTPS接続でのみクライアント証明書が要求されます。それ以外のStoreFront URLにはクライアント証明書は必要ありません。この構成により、管理者は、スマートカードでの認証に問題が生じた場合に指定ユーザー認証を使用できるように設定できます。適用されるWindowsポリシー設定によっては、ユーザーが再認証なしにスマートカードを取り出すこともできます。

  すべてのStoreFront URLへのHTTPS接続でクライアント証明書が必要になるようにIISを構成する場合は、認証サービスとストアを同じサーバー上に配置する必要があります。この場合、すべてのストアに有効なクライアント証明書を使用する必要があります。このIISサイト構成では、スマートカードユーザーがNetScaler Gateway経由で接続できなくなり、指定ユーザー認証にもフォールバックされません。また、スマートカードをデバイスから取り出す場合は再度ログオンする必要があります。

ユーザーエクスペリエンスの最適化

Aug 14, 2017

StoreFrontには、ユーザーエクスペリエンスを向上させる機能があります。これらの機能は、新しいストアや、それに関連するCitrix Receiver for Webサイト、デスクトップアプライアンスサイト、およびXenApp Servicesサイトの作成時にデフォルトで構成されます。

ワークスペースコントロール

ワークスペースコントロール機能を有効にすると、ユーザーがセッションの途中でデバイスを切り替えても、新しいデバイス上でそのアプリケーションでの作業を継続できます。ユーザーは、新しいデバイスにログオンするたびにすべてのアプリケーションを再起動する必要がなく、複数のデバイスを切り替えながら同じアプリケーションインスタンスを使用できます。これにより、たとえば病院で臨床医がワークステーションを切り替えて患者データにアクセスするときの時間を節約できます。

Citrix Receiver for Webサイト、およびXenApp Servicesサイト経由でストアに接続すると、ワークスペースコントロールがデフォルトで有効になります。ユーザーがログオンすると、実行したままのアプリケーションに自動的に再接続されます。たとえば、あるユーザーがCitrix Receiver for WebサイトまたはXenApp Servicesサイト経由でストアにログオンして、いくつかのアプリケーションを起動します。その後、ユーザーが別のデバイスで同じアクセス方法を使用して同じストアにログオンすると、実行中のアプリケーションが自動的に新しいデバイスで使用可能になります。ユーザーがストアで起動したすべてのアプリケーションは、そのストアからログオフすると自動的に切断されます。ただし、シャットダウンはされません。Citrix Receiver for Webサイトの場合は、同じWebブラウザーを使用してログオン、アプリケーションの起動、およびログオフを行う必要があります。

XenApp Servicesサイトでは、ワークスペースコントロールの構成を変更したり無効にしたりすることはできません。Citrix Receiver for Webサイトのワークスペースコントロールの構成について詳しくは、「ワークスペースコントロールの構成」を参照してください。

Citrix Receiver for Webサイトでワークスペースコントロールを使用する場合は、次の要件と制限があります。

- ホストされているデスクトップやアプリケーションからCitrix Receiver for Web サイトにアクセスする場合は、ワークスペースコントロールを使用できません。
- WindowsデバイスからCitrix Receiver for Webサイトにアクセスするユーザーについては、ユーザーデバイスにCitrix Receiverがインストールされていることをサイトで検出できる場合、およびCitrix Receiver for HTML5が使用される場合にのみ、ワークスペースコントロールが有効になります。
- 切断したアプリケーションに再接続するには、Internet ExplorerでCitrix Receiver for Webサイトにアクセスするユーザーは［ローカルイントラネット］または［信頼済みサイト］のゾーンにサイトを追加する必要があります。
- ただし、ワークスペースコントロールの設定にかかわらず、Citrix Receiver for Webサイトで使用可能なデスクトップが1つのみの場合、ユーザーのログオン時にそのデスクトップが自動的に起動するように構成すると、アプリケーションは再接続されません。
- アプリケーションを切断するときに、起動に使用したWebブラウザーを使用する必要があります。別のWebブラウザーで起動したリソースや、デスクトップや［スタート］メニューからCitrix Receiverで起動したリソースは、Receiver for Webサイトで切断したりシャットダウンしたりできません。

コンテンツリダイレクト

ユーザーが適切なアプリケーションをサブスクライブしてある場合、コンテンツリダイレクトにより、ユーザーデバイス上のローカルファイルがサブスクライブされたアプリケーションで開きます。このリダイレクトを有効にするには、XenDesktopまたはXenAppでアプリケーションを必要なファイルタイプと関連付けます。コンテンツリダイレクトは、新しいストアでデフォルトで有効になります。詳しくは、「ファイルタイプの関連付けを無効にするには」を参照してください。

ユーザーによるパスワードの変更

管理者は、Microsoft Active Directoryドメインの資格情報でCitrix Receiver for Webサイトにログオンするユーザーがパスワードをいつでも変更できるように構成できます。または、パスワードの有効期限が切れたユーザーにのみパスワードの変更を許可することもできます。これにより、ユーザーがパスワードの失効によりデスクトップやアプリケーションにアクセスできなくなることを防ぐことができます。

Citrix Receiver for Webサイトのユーザーがいつでもパスワードを変更できるように設定してある場合は、パスワードの有効期限切れが近いローカルユーザーがログオンしたときに警告が表示されます。デフォルトでは、ユーザーに対する通知期間は、適用されるWindowsポリシーの設定によって決まります。パスワードの有効期限切れの警告は、内部ネットワークから接続しているユーザーにのみ表示されます。ユーザーによるパスワードの変更を有効にする方法について詳しくは、「認証サービスの構成」を参照してください。

デスクトップアプライアンスサイトにログオンするユーザーは、パスワードをいつでも変更できるようになっている場合でも、有効期限の切れたパスワードしか変更できません。デスクトップアプライアンスサイトにログオンした後では、パスワードを変更するためのオプションが提供されません。

認証サービスを作成したときのデフォルトの構成では、パスワードが失効しても、Citrix Receiver for Webサイトのユーザーはパスワードを変更できません。この機能を有効にする場合は、サーバーが属しているドメインのポリシーでユーザーによるパスワード変更が禁止されていないことを確認してください。ユーザーのパスワードを変更するには、StoreFrontはドメインコントローラーと通信する必要があります。

ユーザーによるパスワードの変更を有効にすると、この認証サービスを使用するストアにアクセスできるすべてのユーザーに、慎重に扱うべきセキュリティ機能が公開されることになります。組織のセキュリティポリシーにより、ユーザーパスワード変更機能が内部使用のみに制限される環境では、社内ネットワークの外側からそれらのストアにアクセスできないことを確認してください。

Citrix Receiver for Webサイトのデスクトップビューとアプリケーションビュー

Citrix Receiver for Webサイトからデスクトップとアプリケーションの両方にアクセスできる場合、デフォルトでデスクトップとアプリケーションが別々のビューで表示されます。サイトにログオンすると、最初にデスクトップビューが表示されます。Citrix Receiver for Webサイトでユーザーがアクセスできるデスクトップが1つのみの場合、アクセス可能なアプリケーションがあるかどうかにかかわらず、ユーザーのログオン時にそのデスクトップが自動的に起動します。管理者は、Citrix Receiver for Webサイトに表示するビューを指定したり、デスクトップが自動的に起動するのを無効にしたりできます。詳しくは、「Configure how resources are displayed for users」を参照してください。

Citrix Receiver for Webサイトのビューの動作は、配信されるリソースの種類により異なります。たとえば、アプリケーションビューにアプリケーションが表示されるようにするには、ユーザーがそのアプリケーションをサブスクライブする必要があります。一方、ユーザーが使用できるすべてのデスクトップは自動でデスクトップビューに表示されます。このため、ユーザーはデスクトップビューからデスクトップを削除できず、デスクトップのアイコンをドラッグアンドドロップで並び替えることはできません。XenDesktop管理者がユーザーによるデスクトップの再起動を許可している場合は、デスクトップビューにデスクトップを再起動するためのコントロールが表示されます。単一のデスクトップグループの複数のデスクトップインスタンスがユーザーに提供される場合、Citrix Receiver for Webサイトではデスクトップ名に数字が追加されます。

Citrix ReceiverやXenApp Servicesサイトでストアに接続するユーザーの場合、デスクトップおよびアプリケーションの表示と動作は使用するCitrixクライアントにより異なります。

そのほかの推奨事項

XenDesktopやXenAppでアプリケーションをユーザーに配信するときは、ストアのアプリケーションにアクセスするユーザーのエクスペリエンスを向上させるために、次のオプションについて検討します。アプリケーションの配信について詳しくは、

「デリバリーグループアプリケーションの作成」を参照してください。

- 使用できるリソースから必要なアプリケーションを簡単に見つけられるように、アプリケーションをフォルダー別に整理してユーザーに提供します。XenDesktopおよびXenAppでアプリケーションをフォルダーで管理すると、そのフォルダーがユーザーのCitrix Receiverでのアプリケーション一覧に反映されます。フォルダーを使用すると、アプリケーションの種類またはユーザーの役割に応じてアプリケーションをグループ化できます。
- アプリケーションを簡単に識別できるように、アプリケーションを配信するときにわかりやすい説明を入力します。この説明は、ユーザーのCitrix Receiverに表示されます。
- アプリケーションの説明として文字列KEYWORDS:Mandatoryを追加すると、そのアプリケーションはすべてのユーザーのCitrix Receiverのホーム画面に追加され、ユーザーがこれを削除できなくなります。ただし、ユーザーはホーム画面にほかのアプリケーションを追加したり、このキーワードが指定されていないアプリケーションをホーム画面から削除したりできます。
- アプリケーションを配信するときに説明としてKEYWORDS:Autoという文字列を追加すると、そのアプリケーションはストアのすべてのユーザーに自動的にサブスクライブされるようになります。この場合、ユーザーがストアにログオンすると、そのアプリケーションを手動でサブスクライブしなくても自動的にプロビジョニングされます。
- AppControllerで管理されるWebアプリケーションやSoftware-as-a-Service（SaaS）アプリケーションがストアのすべてのユーザーに自動的にサブスクライブされるようにするには、アプリケーション設定を構成するときに［App is available in Receiver to all users automatically］チェックボックスをオンにします。
- ユーザーが特定のXenDesktopアプリケーションに簡単にアクセスできるようにするために、そのアプリケーションをユーザーのCitrix Receiverの［おすすめ］一覧に表示できます。これを行うには、アプリケーションの説明として文字列KEYWORDS:Featuredを追加します。
  注：複数のキーワードを追加する場合は、KEYWORDS:Auto Featuredのようにスペースで区切ります。
- Citrix Receiver for Webサイトのデフォルトでは、XenDesktopおよびXenAppでホストされる共有デスクトップがほかの仮想デスクトップと同じように表示されます。この動作を変更するには、デスクトップの説明としてKEYWORDS:TreatAsAppという文字列を追加します。これにより、そのデスクトップはCitrix Receiver for Webサイトのデスクトップビューではなくアプリケーションビューに表示され、ユーザーはそのデスクトップをサブスクライブする必要があります。また、そのデスクトップはCitrix Receiver for Webサイトへのログオン時に自動起動せず、Desktop Viewerでアクセスできません。
- Windowsユーザーに対しては、ローカルにインストールされたアプリケーションのバージョンと、それに相当する配信されたインスタンスの両方が使用可能な場合に、ローカルにインストールされたアプリケーションが優先的に使用されるように指定できます。これを行うには、アプリケーションの説明として「**KEYWORDS:prefer="application"**」という文字列を追加します。ここでapplicationは、ショートカットファイル名として指定されたローカルアプリケーションの名前に含まれる単語、またはStart Menuフォルダーからローカルアプリケーションへの実行可能ファイル名を含む絶対パスです。このキーワードを持つアプリケーションをユーザーがサブスクライブすると、指定された名前またはパスがユーザーのデバイス上で検索され、アプリケーションがローカルにインストールされているかどうかが判断されます。アプリケーションが見つかった場合、ユーザーがアプリケーションをサブスクライブしてもショートカットは作成されません。この場合、サブスクライブしたアプリケーションをCitrix Receiverで起動すると、ローカルにインストールされたインスタンスが代わりに実行されます。詳しくは、「アプリケーション配信の構成」を参照してください。

StoreFrontの高可用性とマルチサイト構成

Aug 14, 2017

StoreFrontには、ストアにリソースを提供している展開環境間の負荷分散とフェールオーバーを有効にするための機能が多数用意されています。また、障害回復専用の展開環境を指定して回復性を高めることもできます。これらの機能を使用すると、StoreFrontの分散展開環境を構成してストアの高可用性を有効にできます。詳しくは、「可用性の高いマルチサイトストア構成のセットアップ」を参照してください。

リソースの集約

StoreFrontのデフォルトでは、ストアにデスクトップとアプリケーションを配信するすべての展開環境が列挙され、そのすべてのリソースが個別に扱われます。このため、複数の展開環境から同じリソースが同じ名前で配信されていても、リソースごとにアイコンが表示されます。ストアの高可用性やマルチサイト構成を有効にすると、同じデスクトップまたはアプリケーションを配信するXenDesktopおよびXenAppの展開環境をグループ化して、それらのリソースを集約してユーザーに提供できます。グループ化された展開環境は同一である必要はありませんが、集約対象のリソースは、各サーバー上で名前とパスが同じである必要があります。

この機能により、すべてのXenDesktopおよびXenAppの展開環境で配信されているリソースがストアで集約され、ユーザーには1つのアイコンだけが表示されます。App Controllerアプリケーションは集約されません。ユーザーが集約リソースを起動すると、サーバーの可用性、そのユーザーがアクティブなセッションを確立済みかどうか、および管理者が指定した順番に基づいて、対象リソースから最適なインスタンスが選択されます。

StoreFrontでは、過負荷状態、または一時的に使用できない状態などで要求に応答できないサーバーが動的に監視されます。そのサーバーとの通信が再確立されるまで、別のサーバー上のリソースインスタンスがユーザーに提供されます。リソースの提供サーバーでサポートされている場合は、ユーザーが追加リソースを起動したときに、既存のユーザーセッションの再利用が試行されます。このため、ユーザーが選択した追加リソースが、そのユーザーの既存のセッションを実行している展開環境で提供されている場合、そのセッション内で追加リソースが起動します。これにより、各ユーザーのセッション数が最小限に抑えられるため、追加のデスクトップやアプリケーションの起動にかかる時間が短縮され、製品ライセンスをより効率的に使用できます。

サーバーの可用性と既存のユーザーセッションを確認した後、StoreFrontは指定された順番に基づいて、ユーザーが接続する展開環境を決定します。ユーザーが使用できる同等の展開環境が複数ある場合は、管理者の構成に基づいて、一覧の最初の展開環境または任意の展開環境が選択されます。一覧で最初に使用可能な展開環境が選択されるように構成すると、現在のユーザー数に対して使用中の展開環境の数を最小限に抑えることができます。一覧から展開環境がランダムに選択されるように構成すると、使用可能な展開環境間でユーザー接続を均一に分散させることができます。

XenDesktopおよびXenAppで配信されるリソースでは、一覧での展開環境の順序を無視して、ユーザーが特定の展開環境のデスクトップやアプリケーションに接続されるように設定できます。これにより、特定のデスクトップやアプリケーションでは専用の展開環境に優先的にユーザーが接続されるようにして、ほかのリソースでは別の展開環境に接続されるように構成できます。このように構成するには、優先する展開環境のデスクトップやアプリケーションの説明に「KEYWORDS:Primary」という文字列を追加し、別の展開環境のリソースに「KEYWORDS:Secondary」という文字列を追加します。この場合、管理者が指定した展開環境の順序にかかわらず、ユーザーは優先される展開環境（プライマリ）に接続されます。優先される展開環境が使用できない場合、セカンダリリソースを提供する展開環境に接続されます。

リソースに対するユーザーのマッピング

デフォルトでは、ストアにアクセスしているユーザーには、そのストア用に構成されているすべての展開環境から使用可能なすべてのリソースが集約されて表示されます。ユーザーごとに異なるリソースを提供するには、ストアやStoreFront展開環境を個別に構成できます。マルチサイト構成による高可用性をセットアップすると、Microsoft Active Directoryグループのユー

ザーメンバーシップに基づいて、特定の展開環境へのアクセスを提供することができます。これにより、単一のストアで、ユーザーグループごとに異なるエクスペリエンスを構成できます。

たとえば、すべてのユーザーに共通するリソースを1つの展開環境でグループ化し、別の展開環境では経理（Accounts）部門用に財務アプリケーションをグループ化します。このような構成では、Accountsユーザーグループに属していないユーザーは、このストアにアクセスしても共通リソースしか表示されません。Accountsユーザーグループのメンバーには、共通リソースと財務アプリケーションの両方が表示されます。

別の例として、より高速で強力なハードウェアを使用するパワーユーザー用の展開環境を作成して、ほかの展開環境と同じリソースを提供します。これにより、エグゼクティブチームなど、ビジネスクリティカルなユーザーのエクスペリエンスを向上させることができます。このストアにアクセスすると、すべてのユーザーに同じデスクトップやアプリケーションが表示されますが、Executivesユーザーグループのメンバーは、パワーユーザー用の展開環境のリソースに優先的に接続されます。

サブスクリプションの同期

異なるStoreFront展開環境内の類似のストアから同じアプリケーションにユーザーがアクセスできるようにした場合、ユーザーのアプリケーションサブスクリプションをサーバーグループ間で同期する必要があります。サブスクリプションを同期しない場合、あるStoreFront展開環境のストアでアプリケーションをサブスクライブしたユーザーが別のストアにログオンしたときに、それらのアプリケーションをサブスクライブし直す必要があります。異なるStoreFront展開環境間を移動するユーザーにシームレスなエクスペリエンスを提供するため、異なるサーバーグループのストア間でユーザーのアプリケーションサブスクリプションが定期的に同期されるように構成できます。特定の間隔で同期したり、1日の特定の時刻に同期したりできます。詳しくは、「サブスクリプション同期の構成」を参照してください。

専用の障害回復リソース

管理者は、障害回復専用の展開環境を構成できます。この展開環境は、ほかのすべての展開環境が使用できない場合にのみ使用されます。通常、障害回復用の展開環境はメインの展開環境とは異なる場所に配置し、メインの展開環境のリソースのサブセットだけを提供します。また、障害回復用の展開環境では必要以上に高いユーザーエクスペリエンスを提供しません。展開環境を障害回復用に使用することを指定した場合、その展開環境を負荷分散やフェールオーバーの対象から除外します。ほかのすべての展開環境が使用できなくならない限り、ユーザーは障害回復用の展開環境で提供されるデスクトップやアプリケーションにアクセスできません。

メインの展開環境での障害が解決した後では、ユーザーが障害回復用の展開環境のリソースを既に実行している場合でも、追加のリソースはメインの展開環境で起動します。この場合、障害回復用の展開環境で実行しているリソースから切断されることはありません。ただし、ユーザーがそのリソースを終了した後では、そのリソースを再度起動することはできなくなります。同様に、メインの展開環境での障害が解決した後では、障害回復用の展開環境の既存のセッションが再利用されることはありません。

最適なNetScaler Gatewayルーティング

同一ストアの複数の展開環境で個別のNetScaler Gatewayアプライアンスを構成している場合は、ユーザーが各展開環境にアクセスするための最適なアプライアンスを定義できます。たとえば、それぞれがNetScaler Gatewayアプライアンスを持つ、地理的に異なる2つの場所からリソースを集約するストアを作成する場合、一方の場所のNetScaler Gatewayを経由して接続しているユーザーは、もう一方の場所のデスクトップやアプリケーションを起動できます。ただし、デフォルトでは、ユーザーが最初に接続したアプライアンス経由でリソースが配信されるため、コーポレートWANを通過する必要があります。

ユーザーエクスペリエンスを向上させ、WANを経由するトラフィックを削減するため、展開環境ごとに「最適なNetScaler Gatewayアプライアンス」を指定できます。これにより、ユーザーがストアにアクセスするときに経由したアプライアンスにかかわらず、リソースを提供する展開環境のローカルのアプライアンスにユーザー接続が自動的にルーティングされます。

内部ネットワーク上のローカルユーザーをNetScaler Gatewayにログオンさせてエンドポイント解析を行う場合でも、最適な

NetScaler Gatewayアプライアンス機能を使用できます。この構成では、ユーザーはNetScaler Gatewayアプライアンスを経由してストアに接続しますが、ユーザーが内部ネットワーク上にいるため、リソースへの接続はNetScaler Gateway経由である必要はありません。この場合、最適なNetScaler Gatewayアプライアンスは有効にしますが、展開環境用のアプライアンスは指定しません。このため、デスクトップとアプリケーションへのユーザー接続はNetScaler Gateway経由ではなく、直接ルーティングされます。また、NetScaler Gatewayアプライアンスに特定の内部仮想サーバーIPアドレスを構成する必要がある点に注意してください。さらに、ローカルユーザーがアクセスできない内部ビーコンポイントを指定して、Citrix Receiverがネットワーク上の場所にかかわらずNetScaler Gateway経由でストアにアクセスするようにします。

NetScaler Gatewayの広域サーバー負荷分散

StoreFrontでは、単一のFQDN（Fully Qualified Domain Name：完全修飾ドメイン名）を持つ複数のアプライアンスで構成される、広域サーバー負荷分散用のNetScaler Gateway展開環境がサポートされます。StoreFrontでユーザーを認証して適切なアプライアンスにユーザー接続をルーティングするためには、負荷分散構成の各アプライアンスを識別できる必要があります。アプライアンスのFQDNは広域サーバー負荷分散構成で一意の識別子として使用できないため、アプライアンスごとに一意のIPアドレスを使ってStoreFrontを構成する必要があります。通常、これはNetScaler Gateway仮想サーバーのIPアドレスになります。

負荷分散について詳しくは、「NetScalerによる負荷分散」を参照してください。

重要な注意事項

可用性の高いマルチサイトストアを構成するかどうかを決定する場合は、以下の要件と制限について考慮してください。

- デスクトップとアプリケーションは、集約対象の各サーバー上で名前とパスが同じである必要があります。さらに、それらのリソースのプロパティ（名前やアイコンなど）も同じであることが必要です。プロパティが異なる場合、Citrix Receiverが使用可能なリソースを列挙するときに、リソースプロパティの変更が発生することがあります。
- 割り当て済みのデスクトップ（事前割り当ておよび初回使用時割り当てのデスクトップ）は集約しないでください。このようなデスクトップのデリバリーグループに、集約対象のものと同じ名前およびパスが設定されていないことを確認してください。
- App Controllerアプリケーションは集約されません。
- 異なるStoreFront展開環境のストア間で、ユーザーのアプリケーションサブスクリプションを同期する場合は、各サーバーグループのストアに同じ名前を付ける必要があります。さらに、両方のサーバーグループは、ユーザーアカウントが属しているActive Directoryドメイン、またはそのドメインと信頼関係があるドメインのいずれかに属している必要があります。
- 同等展開環境グループ内のすべてのプライマリサイトが使用できない場合のみ、障害回復用のバックアップ展開環境へのアクセスが提供されます。複数の同等展開環境グループ間でバックアップ展開環境を共有する場合、各グループのすべてのプライマリサイトが使用できなくなったときにのみ障害回復リソースにアクセスできるようになります。

インストール、セットアップ、アップグレードおよびアンインストール

Aug 14, 2017

インストールおよび構成する前に

StoreFrontをインストールして構成するには、次の手順に従います。

1. StoreFrontでXenDesktopおよびXenAppのリソースをユーザーに配信する場合は、ユーザーアカウントが属しているMicrosoft Active Directoryドメイン、またはそのドメインと信頼関係があるドメインのいずれかにStoreFrontサーバーが属していることを確認してください。

   重要：
   - 単一サーバー展開では、ドメインに参加していないサーバーにStoreFrontをインストールできます。
   - StoreFrontをドメインコントローラー上にインストールすることはできません。

2. StoreFrontを使用するにはMicrosoft .NET 4.5 Frameworkが必要です。このフレームワークは、Microsoft社のWebサイトからダウンロードできます。Microsoft .NET 4.5がインストールされていることを確認してから、StoreFrontをインストールしてください。
3. 複数サーバーのStoreFront展開環境を構成する計画の場合は、必要に応じてStoreFrontサーバーの負荷分散環境をセットアップします。

   NetScalerを使用して負荷分散を行うには、StoreFrontサーバーのプロキシとなる仮想サーバーを定義します。NetScalerを使用した負荷分散の構成について詳しくは、「NetScalerによる負荷分散」を参照してください。

   1. NetScalerアプライアンスで負荷分散機能が有効になっていることを確認します。
   2. 必要に応じて、各StoreFrontサーバーについて個別のHTTPまたはTLS負荷分散サービス（StoreFrontモニター）を作成します。
   3. StoreFrontに転送されるHTTP要求のX-Forwarded-Forヘッダーに、クライアントのIPアドレスが挿入されるようにサービスを構成して、グローバルポリシーの設定を上書きします。

      StoreFrontでは、ユーザーのリソースへの接続を確立する時に、そのユーザーのIPアドレスが必要です。

   4. 仮想サーバーを作成し、これらのサービスを仮想サーバーにバインドします。
   5. すべてのプラットフォームに最新のCitrix Receiverがインストールされていて、Androidをサポートする必要がない場合は、仮想サーバーでクッキー挿入メソッドを使用してパーシステンスを構成します。そうでない場合は、ソースIPアドレスに基づいてパーシステンスを構成します。ユーザーが必要な時間だけログオンし続けていられるように、Time To Live（TTL）を十分に設定します。

      パーシステンス設定により、最初のユーザー接続だけが負荷分散の対象になり、同じユーザーのそれ以降の要求は同じStoreFrontサーバーに割り当てられるようになります。

4. 必要に応じて、以下の機能を有効にします。

   - ［.NET Framework 4.5の機能］>［.NET Framework 4.5］、［ASP.NET 4.5］

   必要に応じて、StoreFrontサーバーで以下の役割と依存関係を有効にします。

   - ［Webサーバー（IIS）］>［Webサーバー］>［HTTP共通機能］>［既定のドキュメント］、［HTTPエラー］、［静的コンテンツ］、［HTTPリダイレクト］
   - ［Webサーバー（IIS）］>［Webサーバー］>［健全性と診断］>［HTTPログ］
   - ［Webサーバー（IIS）］>［Webサーバー］>［セキュリティ］>［要求のフィルタリング］、［Windows認証］
   - Windows Server 2012サーバーの場合：

     ［Webサーバー（IIS）］>［Webサーバー］>［アプリケーション開発］>［.NET拡張機能4.5］、［アプリケーションの初期化］、［ASP.NET 4.5］、［ISAPI拡張機能］、［ISAPIフィルター］

     Windows Server 2008 R2サーバーの場合：

     ［Webサーバー（IIS）］>［Webサーバー］>［アプリケーション開発］>［.NET拡張機能］、［アプリケーションの初期化］、［ASP.NET］、［ISAPI拡張機能］、［ISAPIフィルター］

   - ［Webサーバー（IIS）］>［管理ツール］>［IIS管理コンソール］、［IIS管理スクリプトおよびツール］

   StoreFrontのインストール時に、これらの機能や役割が有効になっているかどうかが検証されます。

5. StoreFrontをインストールします。

   サーバーをサーバーグループに含める場合は、StoreFrontのインストール場所設定とIIS Webサイト設定の両方で、物理パスおよびサイトIDを一致させる必要があります。

6. StoreFrontとユーザーデバイス間の通信をHTTPSで保護する場合は、Microsoft IIS（インターネットインフォメーションサービス）でHTTPSを構成します。

   スマートカード認証を使用する場合はHTTPSが必要です。デフォルトでは、Citrix Receiverはストアへの接続にHTTPSを必要とします。IISでHTTPSが適切に構成されている場合は、StoreFrontのインストール後に必要に応じていつでもHTTPをHTTPSに変更できます。

   IISでHTTPSを構成するには、StoreFrontサーバー上でインターネットインフォメーションサービス（IIS）マネージャーコンソールを使用して、ドメイン証明機関により署名されたサーバー証明書を作成します。次に、HTTPSバインドをデフォルトのWebサイトに追加します。IISでのサーバー証明書の作成について詳しくは、http://technet.microsoft.com/ja-jp/library/hh831637.aspx#CreateCertificateを参照してください。IISサイトへのHTTPSバインドの追加について詳しくは、http://technet.microsoft.com/ja-jp/library/hh831632.aspx#SSLBindingを参照してください。

7. ファイアウォールやほかのネットワークデバイスで、社内ネットワーク内外からのTCPポート80または443へのアクセスが許可されることを確認します。また、内部ネットワーク上のファイアウォールやほかのネットワークデバイスで、すべての未割り当てTCPポートへのトラフィックがブロックされないことを確認します。

   StoreFrontのインストール時にWindowsファイアウォールで構成される規則により、すべての未割り当てTCPポートからランダムに選択されるポートを介したStoreFrontの実行可能ファイルへのアクセスが有効になります。このポートは、サーバーグループ内のStoreFrontサーバー間の通信で使用されます。

8. 複数のインターネットインフォメーションサービス（IIS）Webサイトを使用する場合、PowerShell SDKを使用して各IIS WebサイトにStoreFront展開環境を作成します。詳しくは、「複数のインターネットインフォメーションサービス（IIS）Webサイト」を参照してください。
   注：StoreFrontは、複数のサイトを検出すると管理コンソールを無効にし、メッセージを表示します。

9. Citrix StoreFront管理コンソールを使用して、サーバーを構成します。

StoreFrontのインストール

> **Important**
>
> StoreFrontインストール時にエラーやデータの損失が発生するのを回避するために、すべてのアプリケーションが閉じられていて、ターゲットシステム上で他のタスクや操作が実行されていないことを確認します。

1. ダウンロードページからインストーラーをダウンロードします。
2. ローカルの管理者権限を持つアカウントでStoreFrontサーバーにログオンします。
3. 必要なMicrosoft .NET 4.5 Frameworkがサーバー上にインストールされていることを確認します。
4. ダウンロードパッケージを参照して、CitrixStoreFront-x64.exeを管理者として実行します。
   注：Windows Server 2008 R2サーバーでは、.NET機能が有効になることを.NET機能が有効になることを知らせるメッセージが表示される場合があります。このメッセージが表示された場合は、［はい］をクリックします。
5. ライセンス契約書を読み、同意することを選択して、［次へ］をクリックします。
6. ［必須条件の確認］ページが開いた場合は、［次へ］をクリックします。
7. ［インストールの開始］ページで、インストール対象の必須ツールおよびStoreFrontコンポーネントを確認して、［インストール］をクリックします。
   コンポーネントがインストールされる前に、サーバー上の以下の役割が必要に応じて自動的に有効になります。

   - ［Webサーバー（IIS）］>［Webサーバー］>［HTTP共通機能］>［既定のドキュメント］、［HTTPエラー］、［静的コンテンツ］、［HTTPリダイレクト］
   - ［Webサーバー（IIS）］>［Webサーバー］>［健全性と診断］>［HTTPログ］
   - ［Webサーバー（IIS）］>［Webサーバー］>［セキュリティ］>［要求のフィルタリング］、［Windows認証］
   - Windows Server 2012サーバーの場合：

     ［Webサーバー（IIS）］>［Webサーバー］>［アプリケーション開発］>［.NET拡張機能4.5］、［アプリケーションの初期化］、［ASP.NET 4.5］、［ISAPI拡張機能］、［ISAPIフィルター］

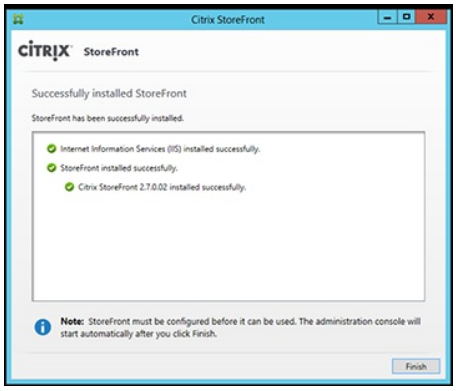
     Windows Server 2008 R2サーバーの場合：

     ［Webサーバー（IIS）］>［Webサーバー］>［アプリケーション開発］>［.NET拡張機能］、［アプリケーションの初期化］、［ASP.NET］、［ISAPI拡張機能］、［ISAPIフィルター］

   - ［Webサーバー（IIS）］>［管理ツール］>［IIS管理コンソール］、［IIS管理スクリプトおよびツール］

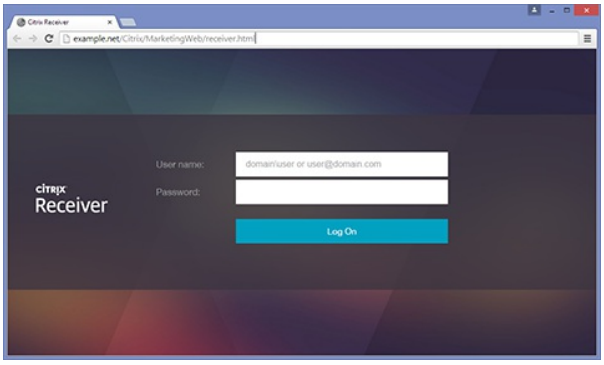
   以下の機能が必要に応じて自動的に有効になります。

   - ［.NET Framework 4.5の機能］>［.NET Framework 4.5］、［ASP.NET 4.5］
8. インストールが完了したら、［完了］をクリックします。Citrix StoreFront管理コンソールが自動的に起動します。また、［起動］画面からStoreFrontを開くこともできます。



9. Citrix StoreFront管理コンソールで、［新しい展開環境の作成］をクリックします。
    1. **［ベースURL］**ボックスにStoreFrontサーバーのURLを指定します。
    2. **［ストア名］**ページで、ストアの名前を指定して、［次へ］をクリックします。
10. **［Delivery Controller］**ページに、ストアで使用できるようにするリソースを提供するインフラストラクチャ（XenAppまたはXenDesktopサービスの詳細）が一覧表示されます。ここには「ダミー」のサーバーを入力できます。ストアにはアプリケーションが表示されません。
11. **［トランスポートの種類］**および**［ポート］を設定します。**HTTPおよびポート443を指定でき、 **［OK］**をクリックします。または、既存のWeb InterfaceまたはStoreFront展開環境から設定をコピーします。
12. **［リモートアクセス］**ページで［なし］を選択します。NetScaler Gatewayを使用している場合は、［VPNトンネルなし］を選択し、ゲートウェイ詳細を入力します。
13. **［リモートアクセス］**ページで［作成］を選択します。ストアが作成されたら、［完了］をクリックします。

ユーザーはCitrix Receiver for Webサイトを介してストアにアクセスできるようになりました。これによりユーザーは、Webページからデスクトップやアプリケーションにアクセスできます。
新しいストアのCitrix Receiver for WebサイトのURLが表示されます。たとえば、 example.net/Citrix/MarketingWeb/などです。ログオンして、Citrix Receiverの新しいユーザーインターフェイスにアクセスします。



CEIP

Citrixのカスタマーエクスペリエンス向上プログラム（CEIP）に参加すると、匿名の統計および使用状況情報が、Citrix製品の品質およびパフォーマンスを向上させる目的で送信されます。

StoreFrontをインストールするとCEIPに自動的に登録されるようになりました。VDAのインストールからおよそ7日後に、初回データアップロードが行われます。このデフォルトはレジストリ設定で変更できます。VDAインストールの前にレジストリ設定を変更すると、その値が使用されます。VDAインストールの前にレジストリ設定を変更すると、その値が使用されます。

> **警告**
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

インストール/アップグレード分析の自動アップロードを制御するレジストリ設定（デフォルト = 1）：

場所：HKLM:\Software\Citrix\Telemetry\CEIP

値の名前：Enabled

種類：REG_DWORD

値：0 = 無効、1 = 有効

デフォルトで、「Enabled」プロパティはレジストリに表示されません。未指定のままの場合、自動アップロード機能は有効です。

PowerShellを使用する場合、次のコマンドレットはCEIPへの登録を無効にします。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled -PropertyType DWORD -Value 0
```

注： このレジストリ設定では、同一サーバー上にあるすべてのコンポーネントの匿名の統計情報と使用状況情報の自動アップロードを制御します。たとえば、Delivery Controllerと同じサーバー上にStoreFrontをインストールし、レジストリ設定でCEIPへの参加を無効にした場合、両方のコンポーネントでCEIPへの参加が無効になります。

StoreFrontで収集されるCEIPデータ

次の表に、収集される匿名情報の種類の例を示します。データでは、お客様を特定するすべての詳細は含まれません。

データ	説明
StoreFrontのバージョン	インストールされているStoreFrontのバージョンを示す文字列。例：3.8.0.0。
ストア数	展開環境に含まれるストア数を表すカウンター。
サーバーグループ内のサーバー数	サーバーグループに含まれるサーバー数を表すカウンター。
ストアごとのDelivery Controller数	展開環境内の各ストアで利用可能なDelivery Controllerの数を表す数値の一覧。
HTTPS有効	展開でHTTPSが有効化されているかどうかを示す文字列。TrueまたはFalseです。
Citrix Receiverのクラシックエクスペリエンスの有効化	各Web Receiverで「クラシックエクスペリエンス」が有効にされているかどうかを示すブール値の一覧。値はWeb ReceiverごとにTRUEまたはFALSEとなります。
Citrix ReceiverのHTML5設定	各Web ReceiverのHTML5の設定を示す文字列の一覧。Web Receiverごとに「常に有効」、「フォールバック」、または「オフ」となります。
Citrix Receiverのワークスペースコントロールの有効化	各Web Receiverで「ワークスペースコントロール」が有効にされているかどうかを示すブール値の一覧。値はWeb ReceiverごとにTRUEまたはFALSEとなります。
ストアのリモートアクセスの有効化	展開内の各ストアで「リモートアクセス」が有効になっているかどうかを示す文字列の一覧。スコアごとに「有効」または「無効」となります。
ゲートウェイ数	展開環境で構成されているゲートウェイの数を表すカウンター。

コマンドプロンプトからStoreFrontをインストールするには

1. ローカルの管理者権限を持つアカウントでStoreFrontサーバーにログオンします。
2. StoreFrontをインストールする前に、すべてのインストール要件を満たしていることを確認してください。詳しくは、「インストールおよび構成する前に」を参照してください。
3. インストールメディアの内容を参照するかパッケージをダウンロードして、CitrixStoreFront-x64.exeをサーバー上の任意のフォルダーに一時的にコピーします。
4. コマンドプロンプトでインストールファイルを含んでいるフォルダーに移動して、次のコマンドを入力します。
   CitrixStoreFront-x64.exe [-silent] [-INSTALLDIR installationlocation] [-WINDOWS_CLIENT filelocation\filename.exe] [-MAC_CLIENT filelocation\filename.dmg]
   StoreFrontおよびすべての必須コンポーネントをサイレントインストールするには、-silent引数を使用します。StoreFrontは、デフォルトでC:\Program Files\Citrix\Receiver StoreFront\にインストールされます。ただし、-INSTALLDIR引数を使用して別のインストール場所を指定することもできます。installationlocationにはStoreFrontのインストール先のフォルダーを指定します。サーバーをサーバーグループに含める場合は、StoreFrontのインストール場所設定とIIS Webサイト設定の両方で、物理パスおよびサイトIDを一致させる必要があることに注意してください。

デフォルトでは、ユーザーがWindowsまたはMac OS Xが動作するコンピューターからCitrix Receiver for Webサイトにアクセスすると、Citrix Receiverがユーザーデバイスにインストール済みであるかどうかが判別され、インストールされていない場合はプラットフォームに適したCitrix ReceiverをCitrix社のWebサイトからダウンロードしてインストールするためのメッセージが表示されます。この動作を変更して、Citrix Receiverのインストールファイルを StoreFrontサーバーからダウンロードできるように構成することもできます。詳しくは、「Citrix Receiverインストールファイルをサーバーから入手できるようにする」を参照してください。

Citrix ReceiverのインストールファイルをStoreFrontサーバーからダウンロードできるように構成する場合は、-WINDOWS_CLIENTと-MAC_CLIENT引数を指定して、Citrix Receiver for WindowsとCitrix Receiver for Macのインストールファイルを StoreFront展開環境の適切な場所にコピーしておきます。ここで filelocationはコピー対象のインストールファイルが格納されているフォルダーを示し、filenameはCitrix Receiverのインストールファイルの名前を示します。Citrix Receiver for WindowsとCitrix Receiver for Macのインストールファイルは、StoreFrontのインストールメディアまたはダウンロードパッケージに収録されています。

StoreFrontのアップグレード

既存のStoreFront 2.0～3.0.x展開環境をこのバージョンのStoreFrontにアップグレードするには、このバージョンのStoreFrontインストールファイルを実行します。StoreFront 2.0よりも古いバージョンを直接アップグレードすることはできません。この場合は、最初にStoreFront 1.2をStoreFront 2.0にアップグレードしてください。同様に、Storefront 1.1をこのバージョンのStoreFrontに直接アップグレードすることはできません。StoreFront1.1をStoreFront 1.2にアップグレードしてからStoreFront 2.0にアップグレードし、最後にこのバージョンにアップグレードしてください。

アップグレード処理を開始した後では、元に戻すことはできません。アップグレードが中断されたり、完了できなかったりする場合、StoreFrontはアップグレードされず既存の構成も削除されます。アップグレードを行う前に、ユーザーをStoreFront展開環境から切断し、ユーザーがアップグレード中にサーバーにアクセスできないようにしてください。これにより、アップグレード時にインストーラーがすべてのStoreFrontファイルに確実にアクセスできるようになります。インストーラーからアクセスできないファイルがあると、それらのファイルを置き換えることができないため、アップグレードに失敗して既存のStoreFront構成が削除されます。StoreFrontでは、複数の製品バージョンが混在する複数サーバー展開環境がサポートされないため、グループ内のすべてのサーバーを同じバージョンにアップグレードしてから、展開環境へのアクセスをユーザーに提供してください。複数サーバー展開環境では、同時アップグレードはサポートされません。各サーバーを順番にアップグレードする必要があります。アップグレードを実行する前に、データをバックアップしておくことをお勧めします。

StoreFrontをアンインストールすると、認証サービス、ストア、ユーザーのアプリケーションサブスクリプション、Citrix Receiver for Webサイト、デスクトッププアプライアンスサイト、およびXenApp ServicesのURLが削除されます。つまり、StoreFrontをアンインストールした後でStoreFrontを再インストールする場合、サービス、ストア、およびサイトを手動で再作成する必要があります。アップグレードする場合はStoreFront構成が保存されてユーザーのアプリケーションサブスクリプションデータはそのまま保持されるため、すべてのアプリケーションのサブスクリプションを再度実行する必要はありません。

StoreFrontが動作するサーバー上のオペレーティングシステムをアップグレードすることはサポートされていません。新しくインストールしたオペレーティングシステムにStoreFrontをインストールすることをお勧めします。

Important

アップグレードを開始する前に、以下の操作を行います。

- StoreFrontサーバー上のすべてのアプリケーションを終了します。
- すべてのコマンドラインおよびPowerShell画面を終了します。

既存のStoreFront 2.0～3.0.xをこのバージョンのStoreFrontにアップグレードするには

1. 負荷分散環境で展開へのアクセスを無効にします。負荷分散URLを無効にすると、ユーザーがアップグレードプロセス中に展開環境に接続できなくなります。
2. サーバーグループ内のすべてのサーバーをバックアップします。
3. 既存のサーバーグループから1つのサーバーを削除します。
4. 削除したサーバーを再起動します。
   並行ロードバランサーを使用して、新しいサーバーグループを作成しながら確認できます。可用性を最大化し、さらにリスクを最小化するには、元のサーバーグループから1つのサーバーのみを削除し、アップグレードします。これによって、元のサーバーグループのマシンを使用するのではなく、新しいマシンから新しいグループを作成できます。
5. 他のStoreFrontが実行中ではなく、最低限の他のアプリケーションがある管理者アカウントを使用して、削除したサーバーをアップグレードします。
6. 削除したサーバーがアップグレードされたことを確認します。
7. 既存のサーバーグループで別のサーバー1つをロードバランサーから削除します。
8. 手順1と同様の理由で、削除したサーバーを再起動します。
9. 現在インストールされているStoreFrontをアンインストールし、新しいバージョンをインストールします。
10. すべてのアップグレードされたサーバーと新たにインストールされたサーバーで構成された、新しいサーバーグループに、新しくインストールしたサーバーを追加し、正しく機能することを確認します。
11. 新しいサーバーグループが古いサーバーグループに置き換わるのに十分な容量になるまで手順3～10を繰り返し、新しいサーバーグループでロードバラン

サーを選択し、正しく機能することを確認します。

12. 残りのサーバーについても、手順3～10を繰り返し、アップグレードが完了するたびに、サーバーをロードバランサーに追加します。

注意

- 新しいサーバーグループが使用可能になるまで、アップグレードプロセスの間、元のサーバーグループへのアクセスを維持して、可用性を最大化できます。このためには、次の操作を行います。
  1. 手順1をスキップします。
  2. 手順11で、ロードバランサーを使用して元のサーバーグループへのアクセスを無効にする手順を加えます。サブスクリプションデータを元のサーバーグループからエクスポートして、新しいサーバーグループにインポートします。ロードバランサーを使用した新しいサーバーグループへのアクセスを有効にします。

     これによって、手順4～手順10の間、サブスクリプションの変更を新しいサーバーグループで使用できるようになります。

- 元のサーバーグループから1つのサーバーのみを削除してアップグレードし、新しいサーバーグループの作成に、元のサーバーグループから削除されたサーバーではなく、新しいサーバーを使用することで、可用性を最大化できます。新しいサーバーグループが稼働中の場合は、古いサーバーを破棄できます。
- StoreFront 2.xから3.xにアップグレード後、サーバーグループへの反映によって、認証構成ファイルにpnaAuthenticationStartupModuleのエントリが追加されることがあります。エントリはPNA認証サービスおよびPNAパスワード変更で有効になった認証サービスにのみ追加されることがあるため、指定されたスタートアップモジュールがなく、認証サービスが起動しないことがあります。この問題を回避するには、認証構成ファイルからエントリを削除してください。デフォルトでは、構成ファイルはC:\inetpub\wwwroot\Citrix\\web.configにあります。

StoreFrontの構成

Citrix StoreFront管理コンソールの初回起動時に、2つのオプションが表示されます。

- 新しい展開環境の作成。新しいStoreFront展開環境の最初のサーバーを構成します。StoreFrontを評価したり、小規模な展開環境を作成したりするには、単一サーバー環境が理想的です。最初のStoreFrontサーバーを構成した後では、いつでもサーバーをグループに追加して展開環境の許容能力を拡張できます。
- 既存のサーバーグループへの参加。既存のStoreFront展開環境に別のサーバーを追加します。StoreFront展開環境の許容能力をすばやく拡張するには、このオプションを選択します。複数サーバーの展開環境には、外部の負荷分散機能が必要です。新しいサーバーを追加する管理者には、展開環境内の既存のサーバーに対するアクセス権が必要です。

StoreFrontのアンインストール

StoreFrontをアンインストールすると、StoreFront自体のほか、認証サービス、ストア、Citrix Receiver for Webサイト、デスクトップアプライアンスサイト、XenApp ServicesサイトのURL、および関連する構成が削除されます。ユーザーのアプリケーションサブスクリプションデータを含んでいるサブスクリプションストアサービスも削除されます。単一サーバー環境では、これによりユーザーのサブスクリプションデータが削除されてしまいます。複数サーバーの展開環境の場合は、これらのデータは展開環境内のほかのサーバー上で保持されます。.NET Frameworkの機能やWebサーバー（IIS）の役割サービスなど、StoreFrontインストーラーにより有効になった必須機能は、StoreFrontをアンインストールしても無効になりません。

1. ローカルの管理者権限を持つアカウントでStoreFrontサーバーにログオンします。
2. Windowsの **[スタート]** 画面または［アプリ］画面で、 **[Citrix StoreFront]** タイルを探します。タイルを右クリックして、 **[アンインストール]** を選択します。
3. **[プログラムと機能]** ダイアログボックスで、 **[Citrix StoreFront]** を選択して **[アンインストール]** をクリックします。これにより、サーバーからすべてのStoreFrontコンポーネントが削除されます。
4. **[Citrix StoreFrontのアンインストール]** ダイアログボックスで **[はい]** をクリックします。アンインストールが完了したら、 **[OK]** をクリックします。

新しい展開環境の作成

Aug 14, 2017

1. 新しいサーバー上でCitrix StoreFront管理コンソールを開きます。これを行うには、Windowsの[スタート]画面または［アプリ］画面で［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの結果ペインで、［新しい展開環境の作成］をクリックします。
3. ［ベースURL］ボックスで、StoreFrontサーバーまたは負荷分散環境（複数サーバーの展開環境の場合）のURLを指定します。
   負荷分散環境をセットアップしていない場合は、サーバーのURLを入力します。展開環境のベースURLはいつでも変更できます。

   Microsoftインターネットインフォメーションサービス（IIS）でHTTPSが正しく構成されている場合は、StoreFront管理コンソールの［ベースURLの変更］タスクでHTTPをHTTPSに変更することもできます。

4. ［次へ］を選択して、認証サービスをセットアップします。このサービスは、ユーザーをMicrosoft Active Directoryで認証します。
   StoreFrontとユーザーデバイス間の通信をHTTPSで保護するには、Microsoftインターネットインフォメーションサービス（IIS）でHTTPSを構成する必要があります。IISでHTTPSが構成されていない場合、StoreFrontの通信にHTTPが使用されます。

   デフォルトでは、Citrix Receiverはストアへの接続にHTTPSを必要とします。StoreFrontがHTTPS用に構成されていない場合、Citrix ReceiverでHTTP接続が使用されるようにユーザーが構成を変更する必要があります。スマートカード認証を使用する場合はHTTPSが必要です。IISでHTTPSが適切に構成されている場合は、StoreFrontの構成後に必要に応じていつでもHTTPをHTTPSに変更できます。詳しくは、「サーバーグループの構成」を参照してください。

   Microsoftインターネットインフォメーションサービス（IIS）でHTTPSが正しく構成されている場合は、StoreFront管理コンソールの**［ベースURLの変更］**タスクでHTTPをHTTPSに変更することもできます。

5. ［ストア名］ページで、ストアの名前を指定して、非認証（匿名）ユーザーのみにストアへのアクセスを許可するかしないかを指定し、［次へ］をクリックします。
   StoreFrontストアでは、ユーザーに提供するデスクトップとアプリケーションが集約されます。ストアの名前はCitrix Receiverでユーザーアカウントの下に表示されるため、ユーザーにとってわかりやすい名前を指定してください。

6. ［Controller］ページでは、リソースを提供するインフラストラクチャを一覧に追加します。ストアにデスクトップとアプリケーションを追加するには、以下の適切な手順に従います。XenDesktop、XenApp、およびXenMobile（App Controller）の展開環境を自由に組み合わせてストアを作成できます。必要に応じて手順を繰り返し、ストアにリソースを提供するすべての展開環境を追加します。
   - XenDesktopおよびXenAppのリソースのストアへの追加
   - App Controllerアプリケーションのストアへの追加
7. 必要なリソースをすべてストアに追加したら、［Controller］ページの［次へ］をクリックします。
8. ［リモートアクセス］ページでは、公共のネットワーク上のユーザーに内部リソースへのアクセス（リモートアクセス）を提供するかどうか、およびその方法を指定します。
   - 公共のネットワーク上でストアをユーザーが使用できるようにするには、**［リモートアクセスの有効化］**チェックボックスをオンにします。このチェックボックスをオフにすると、内部ネットワークのローカルユーザーのみがストアにアクセスできるようになります。
   - NetScaler Gateway経由でアクセスするユーザーにストアのリソースのみを提供するには、**［StoreFrontを介して配信されたリソースへのアクセスのみをユーザーに許可する（VPNトンネルなし）］**を選択します。
   - SSL（Secure Sockets Layer）仮想プライベートネットワーク（Virtual Private Network：VPN）トンネルを介して内部

ネットワーク上のストアおよびそのほかのすべてのリソースへのアクセスを提供するには、**[内部ネットワーク上のすべてのリソースへのアクセスをユーザーに許可する（完全VPNトンネル）]**を選択します。この場合、ユーザーはVPNトンネルを確立するためのNetScaler Gateway Plug-inを使用する必要があることがあります。

NetScaler Gatewayを経由するストアへのリモートアクセスを有効にすると、認証方法としてNetScaler Gatewayからのパススルーが自動的に有効になります。ユーザーはNetScaler Gatewayにログオンする時に認証されるため、ストアにアクセスする時は自動的にログオンできます。

9. リモートアクセスを有効にした場合は、ユーザーがストアにアクセスする時に使用するNetScaler Gateway展開環境を一覧に追加します。NetScaler Gateway展開環境を追加するには、以下の適切な手順に従います。必要に応じて手順を繰り返し、新しい展開環境を追加します。
   - NetScaler Gatewayアプライアンスを介したストアへのリモートアクセスを有効にする
   - Access Gateway 5.0クラスターを介したストアへのリモートアクセスを有効にする
10. NetScaler Gatewayの展開環境をすべて追加したら、［NetScaler Gatewayアプライアンス］の一覧で、ユーザーがストアへのアクセスに使用する展開環境を選択します。複数のゲートウェイ環境を介したアクセスを有効にする場合は、デフォルトで使用されるアプライアンスを指定します。［次へ］をクリックします。
11. **[認証方法]**ページで、ユーザーがストアへの認証に使用する方法を選択し、**[次へ]**をクリックします。次の方法から選択できます。

- **ユーザー名とパスワード**：ユーザーは、ストアにアクセスする時に、資格情報を入力すると認証されます。
- **SAML認証**：ユーザーはNetScaler Gatewayにログオンする時に認証されるため、ストアにアクセスする時は自動的にログオンできます。
- **ドメインパススルー**：ユーザーはドメインに参加しているWindowsコンピューターにログオンする時に認証されるため、ストアにアクセスする時は自動的にログオンできます。
- **スマートカード**：ユーザーはスマートカードとPINを使ってストアにアクセスします。
- **HTTP基本認証**：ユーザー認証は、StoreFrontサーバーのIIS Webサーバーで実行されます。
- **NetScaler Gatewayを介したパススルー**：ストアにアクセスする場合、NetScaler Gatewayへの認証を実行して自動的にログオンされます。リモートアクセスが有効になるとこれは自動的にチェックされます。

12. **[XenApp Services URL]**ページで、Program Neighborhood Agentを使ってアプリケーションおよびデスクトップにアクセスするユーザーのXenApp Service URLを構成します。

13. ストアを作成した後は、Citrix StoreFront管理コンソールでさらに多くのオプションを使用できるようになります。詳しくは、さまざまな管理アーティクルを参照してください。

ストアが作成されました。ただし、Citrix Receiver側でもストアに接続するための詳細を構成する必要があります。ユーザーによるReceiverの構成プロセスを簡単にするために、いくつかの方法が用意されています。詳しくは、「ユーザーアクセスオプション」を参照してください。

また、Citrix Receiver for Webサイトを使用すると、ユーザーがWebページからデスクトップやアプリケーションにアクセスできるようになります。新しいストアにアクセスするためのCitrix Receiver for WebサイトのURLは、ストアを作成する時に表示されます。

デフォルトでは、新しいストアを作成する時に、XenApp ServicesサイトのURLが有効になります。ドメインに参加しているデスクトップアプライアンスのユーザー、Citrix Desktop Lockを実行している再目的化されたPCのユーザー、およびアップグレードできない古いバージョンのCitrixクライアントのユーザーは、XenApp Servicesサイトから直接そのストアに接続できます。XenApp Services URLの形式は、http[s]://serveraddress/Citrix/storename/PNAgent/config.xmlの形式です。ここで、serveraddressはStoreFront展開環境のサーバーまたは負荷分散環境の完全修飾ドメイン名で、storenameは上記手順5で指定した名前です。

StoreFrontの追加のインスタンスをインストールする時に既存のサーバーグループにサーバーを追加するオプションを選択す

ることで、展開環境に複数のサーバーをすばやく追加できます。

XenDesktopおよびXenAppのリソースのストアへの追加

XenAppおよびXenDesktopで提供されるデスクトップやアプリケーションを、StoreFrontサーバーの初回構成時に作成されるストアで使用できるようにするには、次の手順に従います。このトピック冒頭の「新しい展開環境の作成」の手順1～6を完了しておいてください。

1. StoreFrontコンソールの［Controller］ページで、［追加］をクリックします。
2. ［Controllerの追加］ダイアログボックスで、この展開環境に対するわかりやすい名前を指定し、リソースを提供するインフラストラクチャの種類（［XenDesktop］、［XenApp］、または［XenMobile］）を選択します。
3. サーバーの名前またはIPアドレスを［サーバー］の一覧に追加します。この一覧に複数のサーバーを追加すると、その順番に基づいてフェールオーバーされます。XenDesktopサイトの場合は、Controllerの詳細を指定します。XenAppファームの場合は、Citrix XML Serviceを実行しているサーバーを一覧に追加します。
4. ［トランスポートの種類］ボックスの一覧から、StoreFrontでサーバーとの通信に使用する接続の種類を選択します。
   - 暗号化されていない接続でデータを送信するには［HTTP］を選択します。このオプションを選択する場合は、StoreFrontとサーバー間の接続を何らかの方法で保護することを検討してください。
   - SSL（Secure Sockets Layer）またはTLS（Transport Layer Security）を使用する保護されたHTTP接続でデータを送信するには、［HTTPS］を選択します。XenDesktopまたはXenAppサーバーに対してこのオプションを選択する場合は、Citrix XML ServiceがポートをIIS（Microsoftインターネットインフォメーションサービス）と共有する設定になっていることと、IISがHTTPSをサポートするように構成されていることを確認してください。
   - XenAppサーバーとの通信でSSL Relayによるホスト認証とデータの暗号化を実行するには、［SSL Relay］を選択します。

   注：StoreFrontとサーバーの間の通信でHTTPSまたはSSL Relayを使用する場合は、［サーバー］ボックスの一覧に指定したサーバー名がそのサーバーの証明書のサーバー名と一致することを確認してください（大文字/小文字は区別されます）。
5. StoreFrontがサーバーに接続する時に使用するポートを指定します。デフォルトでは、HTTP接続およびSSL Relay接続では80、HTTPS接続では443が使用されます。XenDesktopおよびXenAppサーバーの場合、Citrix XML Serviceで使用されるポート番号を指定する必要があります。
6. StoreFrontとXenAppサーバーの間の接続をSSL Relayで保護する場合は、SSL RelayのTCPポートを［SSL Relayポート］ボックスで指定します。デフォルトのTCPポートは443です。SSL Relayを実行するすべてのサーバーで同じポートが構成されていることを確認してください。

XenDesktop、XenApp、およびXenMobileの展開環境を自由に組み合わせてストアを作成できます。XenDesktopサイトまたはXenAppファームをさらに追加する場合は、上記手順を繰り返します。App Controllerで管理されるアプリケーションをストアで使用できるようにするには、「App Controllerアプリケーションのストアへの追加」の手順に従います。必要なリソースをすべてストアに追加したら、このトピック冒頭の「新しい展開環境の作成」の手順7以降に従います。

App Controllerアプリケーションのストアへの追加

App Controllerで管理されるアプリケーションを、StoreFrontサーバーの初回構成時に作成されるストアで使用できるようにするには、次の手順に従います。このトピック冒頭の「新しい展開環境の作成」の手順1～6を完了しておいてください。

1. ［ストアの作成］ウィザードの［Delivery Controller］ページで、［追加］をクリックします。
2. ［Delivery Controllerの追加］ダイアログボックスで、追加するApp Controller仮想アプライアンスに対するわかりやすい名前を指定します。名前にスペースが含まれないようにしてください。［AppController］を選択します。
3. App Controller仮想アプライアンスの名前またはIPアドレスを［サーバー］ボックスに入力し、App Controllerへの接続に使用するStoreFrontのポートを指定します。デフォルトのTCPポートは443です。

XenDesktop、XenApp、およびApp Controllerの展開環境を自由に組み合わせてストアを作成できます。ほかのApp Controlle

仮想アプライアンスで管理されるアプリケーションをストアに追加するには、上記の手順を繰り返します。XenDesktopおよびXenAppで提供されるデスクトップやアプリケーションをストアで使用できるようにするには、「XenDesktopおよびXenAppのリソースのストアへの追加」の手順に従います。必要なリソースをすべてストアに追加したら、このトピック冒頭の「新しい展開環境の作成」の手順7以降に従います。

制限：AppControllerで公開されているアプリケーションが起動しないことがあります。この問題を回避するには、StoreFront PowerShellコマンドを使用して、**http://*sfserver*/Citrix/Authenticationにある認証サービスでストアを手動作成します。**

NetScaler Gatewayアプライアンスを介したストアへのリモートアクセスを有効にする

StoreFrontサーバーの初回構成時に作成されるストアへの、NetScaler Gatewayアプライアンスを介したリモートアクセスを構成するには、次の手順に従います。このトピック冒頭の「新しい展開環境の作成」の手順1～9を完了しておいてください。

1. StoreFrontコンソールの［リモートアクセス］ページで、［追加］をクリックします。
2. ［NetScaler Gatewayアプライアンスの追加］ダイアログボックスで、NetScaler Gatewayアプライアンスにわかりやすい名前を指定します。
   ここで指定する表示名がユーザーのCitrix Receiverに表示されます。そのため、ユーザーが使用するNetScaler Gatewayを判断しやすいように、名前に関連情報を含める必要があります。たとえば、ユーザーが自分のいる場所に最も便利なNetScaler Gatewayを簡単に特定できるように、表示名に地理情報を含めることができます。
3. アプライアンスの仮想サーバーまたはユーザーログオンポイント（Access Gateway 5.0の場合）のURLを入力します。展開環境で使用する製品のバージョンを指定します。
   ストアに内部および外部アクセスするための単一の完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）の作成について詳しくは、「ストアに内部および外部アクセスするための単一のFQDNの作成」を参照してください。
4. スタンドアロンAccess Gateway 5.0アプライアンスを追加する場合は、［展開モード］の一覧で［アプライアンス］を選択します。それ以外の場合は、必要に応じてNetScaler Gatewayアプライアンスのサブネット IPアドレスを指定します。サブネットIPアドレスは、Access Gateway 9.3アプライアンスの場合は必須ですが、それより後の製品バージョンではオプションです。
   このサブネットアドレスは、NetScaler Gatewayで内部ネットワークのサーバーと通信する時に、ユーザーデバイスを表すために使用するIPアドレスです。このアドレスは、NetScaler Gatewayアプライアンスのマップされた IPアドレスである場合もあります。StoreFrontは、サブネットIPアドレスを使用して、受信要求が信頼されているデバイスから発信されているかどうかを検証します。
5. NetScaler Gateway 10.1、Access Gateway 10、またはAccess Gateway 9.3のアプライアンスを追加する場合は、［ログオンの種類］の一覧から、Citrix Receiverユーザー用にアプライアンスで構成した認証方法を選択します。
   NetScaler Gatewayアプライアンスに関する構成情報は、ストアのプロビジョニングファイルに追加されます。これにより、Citrix Receiverは、アプライアンスへの初回接続時に適切な接続要求を送信できるようになります。

   - ユーザーのMicrosoft Active Directoryドメインの資格情報を入力させる場合は、［ドメイン］を選択します。
   - セキュリティトークンから取得するトークンコードを入力させる場合は、［セキュリティトークン］を選択します。
   - ユーザーのドメイン資格情報とセキュリティトークンから取得するトークンコードの両方を入力させる場合は、［ドメインおよびセキュリティトークン］を選択します。
   - テキストメッセージで送信されるワンタイムパスワードを入力させる場合は、［SMS認証］を選択します。
   - スマートカードを挿入してPINを入力させる場合は、［スマートカード］を選択します。

   スマートカードでの認証に問題が生じた場合に代替の認証方法を使用できるようにするには、［スマートカードフォールバック］の一覧から代替の認証方法を選択します。
6. ［コールバックURL］ボックスに、NetScaler Gateway認証サービスのURLを入力します。URLの標準的な部分は自動的に

補完されます。［Next］をクリックします。
アプライアンスの内部URLを入力します。StoreFrontはNetScaler Gateway認証サービスに接続して、NetScaler Gatewayからの要求の送信元がそのアプライアンスであることを確認します。

7. XenDesktopまたはXenAppが提供するリソースをストアで使用できるようにするには、［Secure Ticket Authority（STA）］ページで、STAを実行しているサーバーのURLを一覧に追加します。一覧に複数のSTAのURLを追加すると、その順番に基づいてフェールオーバーされます。
STAは、XenDesktopおよびXenAppサーバーでホストされ、接続要求に応答してセッションチケットを発行します。セッションチケットは、XenDesktopおよびXenAppリソースへのアクセスを認証および承認するための基本機能です。

8. Citrix Receiverが自動的に再接続を実行する間に、切断したセッションをXenDesktopおよびXenAppで開いたままにするには、［セッション画面の保持を有効にする］チェックボックスをオンにします。複数のSTAを構成した環境でセッション画面の保持機能を常に使用できるようにするには、［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにします。
［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにすると、セッションの途中で1つのSTAが使用できなくなってもユーザーセッションが中断されないように、StoreFrontにより2つの異なるSTAからセッションチケットが取得されます。StoreFrontがどちらのSTAにもアクセスできない場合は、単一のSTAを使用するようにフォールバックされます。

9. ［作成］をクリックします。これにより、［リモートアクセス］ページの一覧にNetScaler Gatewayの展開環境が追加されます。

展開環境をさらに追加する場合は、上記手順を繰り返します。Access Gateway 5.0クラスターを介したリモートアクセスを構成するには、「Access Gateway 5.0クラスターを介したストアへのリモートアクセスを有効にする」の手順に従います。
NetScaler Gatewayの展開環境をすべてストアに追加したら、このトピック冒頭の「新しい展開環境の作成」の手順10.以降に従います。

Access Gateway 5.0クラスターを介したストアへのリモートアクセスを有効にする

StoreFrontサーバーの初回構成時に作成されるストアへの、Access Gateway 5.0クラスターを介したリモートアクセスを構成するには、次の手順に従います。このトピック冒頭の「新しい展開環境の作成」の手順1～9を完了しておいてください。

1. StoreFrontコンソールの［リモートアクセス］ページで、［追加］をクリックします。
2. ［NetScaler Gatewayアプライアンスの追加］ダイアログボックスで、クラスターにわかりやすい名前を指定します。
ここで指定する表示名がユーザーのCitrix Receiverに表示されます。そのため、ユーザーが使用するNetScaler Gatewayを判断しやすいように、名前に関連情報を含める必要があります。たとえば、ユーザーが自分のいる場所に最も便利なNetScaler Gatewayを簡単に特定できるように、表示名に地理情報を含めることができます。

3. クラスターのユーザーログオンポイントのURLを入力して、［バージョン］の一覧で［5.x］を選択します。
4. ［展開モード］の一覧で［Access Controller］を選択して、［次へ］をクリックします。
5. ［アプライアンス］ページで、クラスター内のアプライアンスのIPアドレスまたはFQDN（Fully Qualified Domain Names：完全修飾ドメイン名）を一覧に追加して、［次へ］をクリックします。
6. ［サイレント認証を有効にする］ページで、Access Controllerサーバーで実行されている認証サービスのURLを一覧に追加します。一覧に複数のサーバーのURLを追加すると、その順番に基づいてフェールオーバーされます。［Next］をクリックします。
StoreFrontでは認証サービスを使用してリモートユーザーが認証されるため、リモートユーザーがストアにアクセスする時に資格情報を再入力する必要はありません。

7. XenDesktopおよびXenAppが提供するリソースをストアで使用できるようにするには、［Secure Ticket Authority（STA）］ページで、STAを実行しているサーバーのURLを一覧に追加します。一覧に複数のSTAのURLを追加す

ると、その順番に基づいてフェールオーバーされます。
STAは、XenDesktopおよびXenAppサーバーでホストされ、接続要求に応答してセッションチケットを発行します。セッションチケットは、XenDesktopおよびXenAppリソースへのアクセスを認証および承認するための基本機能です。

8. Citrix Receiverが自動的に再接続を実行する間に、切断したセッションをXenDesktopおよびXenAppで開いたままにするには、［セッション画面の保持を有効にする］チェックボックスをオンにします。複数のSTAを構成した環境でセッション画面の保持機能を常に使用できるようにするには、［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにします。
［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにすると、セッションの途中で1つのSTAが使用できなくなってもユーザーセッションが中断されないように、StoreFrontにより2つの異なるSTAからセッションチケットが取得されます。StoreFrontがどちらのSTAにもアクセスできない場合は、単一のSTAを使用するようにフォールバックされます。

9. ［作成］をクリックします。これにより、［リモートアクセス］ページの一覧にNetScaler Gatewayの展開環境が追加されます。

クラスターをさらに追加する場合は、上記手順を繰り返します。NetScaler Gateway 10.1、Access Gateway 10、Access Gateway 9.3、またはスタンドアロンAccess Gateway 5.0アプライアンスを介したリモートアクセスを構成するには、「NetScaler Gatewayアプライアンスを介したストアへのリモートアクセスを有効にする」の手順に従います。NetScaler Gatewayの展開環境をすべてストアに追加したら、このトピック冒頭の「新しい展開環境の作成」の手順10.以降に従います。

既存のサーバーグループへの参加

Aug 14, 2017

StoreFrontをインストールする前に、グループに追加するサーバーのオペレーティングシステムのバージョンおよびロケール設定が、グループ内のほかのサーバーと同じであることを確認してください。StoreFrontサーバーグループ内でオペレーティングシステムのバージョンやロケール設定が異なるサーバーを混在させることはサポートされていません。サーバーグループには最大で5つのサーバーを追加できますが、シミュレーションでは4つ以上のサーバーをグループに追加しても顕著なキャパシティ向上は確認されていません。また、追加するサーバーのStoreFrontのIISでの相対パスが、グループ内のほかのサーバーと同じであることも確認してください。

> ## Important
>
> サーバーグループに新しいサーバーを追加すると、そのサーバーのローカル管理者グループにいくつかのStoreFrontサービスアカウントが追加されます。これは、サーバーグループに参加したり情報を同期したりするために、これらのサービスでローカル管理者権限が必要になるためです。グループポリシーでローカル管理者グループへのアカウントの追加が禁止されている場合、またはサーバーのローカル管理者グループの権限が制限されている場合、StoreFrontでサーバーをサーバーグループに追加できません。

1. 新しいサーバー上でCitrix StoreFront管理コンソールを開きます。これを行うには、Windowsの［スタート］画面または［アプリ］画面で［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの結果ペインで、［既存のサーバーグループへの参加］をクリックします。
3. 参加先のStoreFront展開環境のサーバーにログオンして、Citrix StoreFront管理コンソールを開きます。コンソールの左ペインで［サーバーグループ］ノードを選択して、［操作］ペインで［サーバーの追加］をクリックします。表示される承認コードをメモしておきます。
4. 新しいサーバーに戻り、［サーバーグループへの参加］ダイアログボックスの［承認サーバー］ボックスに、既存のサーバーの名前を指定します。そのサーバーから取得した承認コードを入力して［参加］をクリックします。
   サーバーを既存のグループに追加すると、そのサーバーの構成がグループの既存のサーバーの構成と一致するように更新されます。また、グループ内のほかのすべてのサーバーは、新しいサーバーの詳細情報で更新されます。

複数サーバー展開環境を管理する場合、同時に複数のサーバー上でサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。また、展開環境内で一貫した構成を保つため、構成の変更内容をグループ内のほかのサーバーに反映させる必要があります。

既存のサーバーグループからのサーバーの削除

StoreFrontサーバーがサーバーグループのメンバーで、削除されてしまった場合は、Clear-DSConfiguration PowerShellコマンドレットを実行してStoreFrontサーバーを工場出荷時の状態にリセットする必要があります。切断されたサーバーでClear-DSConfigurationコマンドレットを実行した後、サーバーを元のサーバーグループに戻したり、別の新しく作成したサーバーグループに追加したりできます。

1. サーバーグループ全体の管理に使用するプライマリStoreFrontサーバーでStoreFront管理コンソールを開きます。
2. 左側のペインでサーバーグループノードを選択し、削除するほかのサーバーを選択します。
3. 選択したサーバーをサーバーグループから削除します。
4. 操作ペインで、サーバーグループメンバーの1つを切断するために使用したサーバーからの変更を反映させます.残りのいずれのサーバーグループのメンバーにも、グループからサーバーが削除されことが認識されます。切断されたサーバーを工場出荷時設定にリセットしない限り、それがグループのメンバーではなくなったことが認識されません。
5. 切断されたサーバーで管理コンソールを閉じます。

6. 切断されたサーバーグループから削除された後でそのサーバー上でPowerShellセッションを開き、次のものを使用するStoreFront PowerShellモジュールをインポートします。 & "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\ImportModules.ps1"
7. Clear-DSConfigurationコマンドを実行します。これにより、サーバーがデフォルト設定にリセットされます。
8. StoreFront管理コンソールを開き、切断されたサーバーがリセットされ、ほかのサーバーグループに追加される準備が整ったことを確認します。

Web Interface機能のStoreFrontへの移行

Aug 14, 2017

Web Interfaceのほとんどのカスタマイズは、JavaScriptを微調整したり、Citrixが公開しているAPIを使用したり、またはStoreFront管理コンソールを使用したりすることで、StoreFront内で同等の設定ができます。

カスタマイズの概要とそれに対応する方法に関する基本的な情報を次の表に示します。

フォルダーの場所

- スクリプトのカスタマイズの場合、次の場所にあるscript.jsファイルに例を追加します：

  \Inetpub\wwwroot\Citrix\StoreNameWeb

- スタイルのカスタマイズの場合、次の場所にあるstyle.cssファイルに例を追加します：

  \Inetpub\wwwroot\Citrix\StoreNameWeb

- 動的コンテンツの場合、次の場所にあるテキストファイルに動的コンテキストを追加します：

  \Inetpub\wwwroot\Citrix\StoreNameWeb

- マルチサーバー展開環境の場合は、 StoreFront管理コンソールやPowerShellを使って変更をほかのサーバーにも繰り返して適応させることができます。

注：Web Interfaceでは、個々のユーザーがさまざまな設定をカスタマイズできます。現在、StoreFrontにはこの機能はありません。これをサポートするためにより詳細なカスタマイズを追加することは可能ですが、このアーティクルではそれに焦はあてません。

Web Interfaceの機能	**StoreFrontの同等のもの**
管理コンソールによるカスタマイズ	
• 低レイアウトのグラフィック • フルレイアウトのグラフィック • ユーザーによる選択の許可	該当なしStoreFrontではUIは自動的に検出され、デバイス画面に合わせて調整されます。
• 検索の有効化 • 検索の無効化	• 検索は、デフォルトで有効になっています。 • Disable：デスクトップまたはWeb UIで検索ボックスを非表示にするには、style.cssに次のスタイルを追加します。 **.search-container {** **display: none;** **}** スマートフォンUIで検索ボックスを非表示にするには、次のスタイルを

	追加します。 **#searchBtnPhone {** **display: none;** **}**
更新の有効化	デフォルトで有効になっています（ブラウザー更新）。
前のフォルダーに戻る	デフォルトでは有効になっていません。 前のフォルダーに戻る - 現在のフォルダーを記憶して、読み込み時にそこに戻るには、次のものをscript.jsに追加します。 **CTXS.Extensions.afterDisplayHomeScreen = function ()** **{** **// check if view was saved last time** **CTXS.ExtensionAPI.localStorageGetItem("view",** **function (view) {** **if (view) {** **// if view was saved, change to it** **CTXS.ExtensionAPI.changeView(view);** **}** **if (view == "store") {** **// if view is store, see if folder was saved** **CTXS.ExtensionAPI.localStorageGetItem("folder",** **function(folder) {** **if (folder != "") {** **// if folder was saved, change to it** **CTXS.ExtensionAPI.navigateToFolder(folder);** **}** **}** **);** **}**

	// set up monitoring of folder
	CTXS.Extensions.onFolderChange = function(folder) {
	CTXS.ExtensionAPI.localStorageSetItem("folder",
	folder);
	};
	// set up monitoring of view
	CTXS.Extensions.onViewChange = function(newview) {
	// don't retain search or appinfo views
	// instead, remember parent view.
	if ((newview != "appinfo") &&
	(newview != "search")) {
	CTXS.ExtensionAPI.localStorageSetItem(
	"view", newview);
	}
	};
	});
	};

ヒントの有効化	Citrix Receiverはタッチデバイスと非タッチデバイスを対象としているため、ツールチップの使用は非常に限定化されたものになります。カスタムスクリプトを使うとツールチップを追加できます。
• アイコンビュー • ツリービュー • 詳細ビュー • リストビュー • グループビュー • デフォルトビューの設定 • （低グラフィックの）アイコンビュー • （低グラフィックの）リストビュー （低グラフィックの）デフォルトビュー	Citrix Receiverには異なるUIがあるため、これらについては適用されません。StoreFront管理コンソールを使ってビューを構成できます。詳しくは、「アプリケーションとデスクトップへの異なるビューの指定」を参照してください。
• 単一のタブUI • タブ付けUI • アプリケーションタブ	Citrix Receiver UIはデフォルトでタブ付けされています。アプリケーションとコンテンツは1つのタブに、デスクトップは別のタブにあります。また、オプションとして**お気に入り**タブがあります。

• デスクトップタブ • コンテンツタブ • （タブ順）	
• ヘッダーロゴ • 文字の色 • ヘッダー背景色 • ヘッダー背景画像	StoreFront管理コンソールを使った同等の色とロゴ。StoreFront管理コンソールで［Webサイト外観のカスタマイズ］をクリックし、 表示される画面でカスタマイズを実行します。 スタイルをカスタマイズして、ヘッダーに背景画を設定できます。例 **.theme-header-bgcolor {** **background-image: url('spirals.png');** **}**

• 事前ログオンウェルカムメッセージ（事前ロケール）
  • タイトル
  • テキスト
  • ハイパーリンク
  • ボタンラベル
	デフォルトでは、別個のログオン前画面はありません。
	
	この例のスクリプトは、クリックスルーメッセージボックスを追加します。
	
	var doneClickThrough = false;
	
	//Webログインの前
	
	CTXS.Extensions.beforeLogon = function (callback) {
	
	doneClickThrough = true;
	
	CTXS.ExtensionAPI.showMessage({
	
	messageTitle: "Welcome!",
	
	messageText: "Only for WWCo Employees",
	
	okButtonText: "Accept",
	
	okAction: callback
	
	});
	
	};
	
	// Before main screen (for native clients)
	
	CTXS.Extensions.beforeDisplayHomeScreen
	
	= function (callback) {
	
	if (!doneClickThrough) {
	
	CTXS.ExtensionAPI.showMessage({
	
	messageTitle: "Welcome!",

	messageText: "Only for WWCo Employees", **okButtonText: "Accept",** **okAction: callback** **});** **} else {** **callback();** **}** **};**
• ログオン画面タイトル • ログオン画面メッセージ • ログオン画面システムメッセージ	ログオン画面にはカスタマイズできる4つの領域があります。画面の上部と下部（ヘッダーとフッター）およびログオンボックス自体の上部と下部。 **.customAuthHeader** **.customAuthFooter** **.customAuthTop** **.customAuthBottom {** **text-align: center;** **color: white;** **font-size: 16px;** **}** スクリプト例（静的コンテンツ） **$('.customAuthHeader').html("Welcome to ACME");** スクリプト例（動的コンテンツ） **function setDynamicContent(txtFile, element) {** **CTXS.ExtensionAPI.proxyRequest({** **url: "customweb/"+txtFile,** **success: function(txt) {$(element).html(txt);}});** **}** **setDynamicContent("Message.txt", ".customAuthTop");** 注：ここでの変更によりすべてのクライアントでUIが強制的に再読み込みされるため、動的コンテンツをスクリプトに明示的に含めたり、**custom**ディレクトリに置いたりしないでください。動的コンテンツは**customweb** ディレ

	クトリにおいてください。
• アプリケーション画面のウェルカムメッセージ • アプリケーション画面のシステムメッセージ	前述した**CustomAuth**ウェルカム画面の例を参照してください。 前述の動的コンテンツの例を参照してください。ホーム画面にコンテンツを置くには、**'.customAuthTop'**ではなく、**'#customTop'**を使います。
フッター文字列（すべての画面）	スクリプト例： **#customBottom {** **中央揃え** **color: white;** **font-size: 16px;** **}** スクリプトを使った静的コンテンツ例： **$('#customBottom').html("Welcome to ACME");**
直接的に同等なものがない機能	
• ヘッダーなしのログオン画面 • ヘッダーありのログオン画面（メッセージを含む）	StoreFrontには直接同等するものがありません。ただし、カスタムヘッダーを作成することはできます。前述の「ログオン画面のタイトル」を参照してください。
ユーザー設定	デフォルトでは、ユーザー設定はありません。JavaScriptからメニューやボタンを追加できます。
ワークスペースコントロール	管理者設定の同等の機能。拡張APIにより、柔軟性が著しく向上します。 http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/receiver-customization-api.htmlを参照してください。
詳細なカスタマイズ（コード）	
ICAファイル生成フックおよびそのほかのコールルーティングのカスタマイズ。	同等またはそれ以上のAPI。 http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-customization-sdk.html

認証カスタマイズ	同等またはそれ以上のAPI。 http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-authentication-sdks.html
JSP/ASPソースアクセス	UIが同じ方法によってレンダリングされないため、StoreFrontには同等のAPIがありません。UIのカスタマイズを有効にするための、多くのJavaScript APIがあります。

サーバーグループの構成

Aug 14, 2017

以下のタスクでは、複数サーバーのStoreFront展開環境の設定を変更します。複数サーバー展開環境を管理する場合、同時に複数のサーバー上でサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。また、展開環境内で一貫した構成を保つため、構成の変更内容をグループ内のほかのサーバーに反映させる必要があります。

StoreFrontサーバーグループに含まれるサーバーは、StoreFrontのインストール場所の設定とIIS Webサイトの設定（物理パスやサイトIDなど）の両方が同じになるように構成する必要があります。

サーバーグループへのサーバーの追加

［サーバーの追加］タスクを使用して、新しくインストールしたStoreFrontサーバーを既存の展開環境に追加するための承認コードを取得します。新しいサーバーを既存のStoreFront展開環境に追加する方法について詳しくは、「既存のサーバーグループへの参加」を参照してください。グループ内のいくつのサーバーにアクセスする必要があるかについては、「StoreFrontの展開計画」の「*スケーラビリティ*」の説明を参照してください。

サーバーグループからのサーバーの削除

複数サーバーのStoreFront展開環境からサーバーを削除するには、［サーバーの削除］タスクを使用します。このタスクでは、StoreFront管理コンソールを実行しているサーバー以外の任意のサーバーをグループから削除できます。ただし、複数サーバーの展開環境からサーバーを削除する前に、そのサーバーを負荷分散環境から削除しておく必要があります。

サーバーグループへのローカルの変更の反映

現在のサーバー上で行った変更内容を、複数サーバーのStoreFront展開環境内のほかのすべてのサーバーに反映させるには、［変更の伝達］タスクを使用します。これにより、グループ内のほかのサーバー上で行ったすべての変更が破棄されます。このタスクの実行中は、グループ内のすべてのサーバーが更新されるまで、追加の変更を加えることはできません。

重要：サーバーの構成を変更してからグループ内のほかのサーバーにその変更を反映させないと、後で展開環境内の別のサーバーでの変更が反映された場合に元の変更内容が失われる可能性があります。

展開環境のベースURLの変更

StoreFront展開環境でホストされるストアやほかのStoreFrontサービスのルートURLを変更するには、[ベースURLの変更］タスクを使用します。複数サーバーの展開環境の場合は、負荷分散URLを指定します。Microsoftインターネットインフォメーションサービス（IIS）でHTTPSが正しく構成されている場合は、［ベースURLの変更］タスクでHTTPをHTTPSに変更することもできます。

IISでHTTPSを構成するには、StoreFrontサーバー上でインターネットインフォメーションサービス（IIS）マネージャーコンソールを使用して、Microsoft Active Directoryドメイン証明機関により署名されたサーバー証明書を作成します。次に、HTTPSバインドをデフォルトのWebサイトに追加します。IISでのサーバー証明書の作成について詳しくは、http://technet.microsoft.com/ja-jp/library/hh831637.aspx#CreateCertificateを参照してください。IISサイトへのHTTPSバインドの追加について詳しくは、http://technet.microsoft.com/ja-jp/library/hh831632.aspx#SSLBindingを参照してください。

サーバーバイパス動作の構成

リソースを提供するサーバーの一部が使用できなくなったときのパフォーマンスを向上させるために、応答しないサーバーがStoreFrontにより一時的にバイパスされます。バイパスされたサーバーはStoreFrontにより無視され、リソースのアクセスに使用されません。このバイパスの期間は、次のパラメーターで指定します。

- **[すべての失敗のバイパス時間]** では、特定のDelivery Controllerのすべてのサーバーがバイパスされている場合に、**[バイパス時間]** の代わりに適用される短い期間を分単位で指定します。デフォルトは10分です。
- **[バイパス時間]** では、特定のサーバーへの接続に失敗した後で、StoreFrontがそのサーバーをバイパスする期間を分単位で指定します。デフォルトのバイパス時間は60分間です。

[すべての失敗のバイパス時間] 指定時の考慮事項

[すべての失敗のバイパス時間] を長く設定すると、特定のDelivery Controllerを使用できないことによる影響を小さくすることができますが、一時的なネットワーク障害やサーバー障害の後で、ユーザーがこのDelivery Controllerのリソースをその期間使用できなくなるという悪影響もあります。多くのDelivery Controllerを単一のストア用に構成している場合、特に、業務に重要ではないDelivery Controllerの場合は、 **[すべての失敗のバイパス時間]** の値を大きめにすることを検討してください。

[すべての失敗のバイパス時間] を短くするとそのDelivery Controllerで提供されるリソースの可用性は高まりますが、単一のストアを構成する多くのDelivery Controllerのうちの複数台が使用できない場合に、クライアント側でタイムアウトが発生しやすくなります。少数のファームを構成していて、業務に重要なDelivery Controllerの場合は、デフォルト値の0分を使用することをお勧めします。

ストアのバイパスパラメーターを変更するには

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、 **[操作]** ペインの **[Delivery Controllerの管理]** をクリックします。
3. Controllerを選択し、 **[編集]** をクリックして、 **[Delivery Controllerの編集]** 画面の **[設定]** をクリックします。
4. **[すべての失敗のバイパス時間]** の行で2列目をクリックし、サーバーがすべて応答できなくなってからDelivery Controllerがオフラインとみなされるまでの時間を分単位で入力します。
5. **[バイパス時間]** の行で2列目をクリックし、単一のサーバーが応答しなくってからオフラインとみなされるまでの時間を分単位で入力します。

認証と委任の構成

Aug 14, 2017

自分の要件によって、複数の認証と委任法方式があります。

認証サービスの構成	認証サービスにより、ユーザーがMicrosoft Active Directoryで認証され、ユーザーが再ログオンすることなくデスクトップやアプリケーションにアクセスできるようになります。
XMLサービスベースの認証	StoreFrontがXenAppまたはXenDesktopと同じドメイン内にない場合、またActive Directoryの信頼を適切に配置できない場合には、XenAppおよびXenDesktop XML Serviceを使ってユーザー名とパスワード資格情報を認証するようにStoreFrontを構成できます。
XenApp 6.5のKerberos制約付き委任。	StoreFrontでDelivery Controllerの認証に単一ドメインKerberos制約付き委任を使用するかどうかを指定するには、［Kerberos委任の構成］タスクを使用します。
スマートカード認証	一般的なStoreFront展開のすべてのコンポーネントに対するスマートカード認証をセットアップします。
パスワードの有効期限切れ通知期間	Citrix Receiver for Webサイトのユーザーがいつでもパスワードを変更できるように設定してある場合は、パスワードの有効期限切れが近いローカルユーザーがログオンしたときに警告が表示されます。

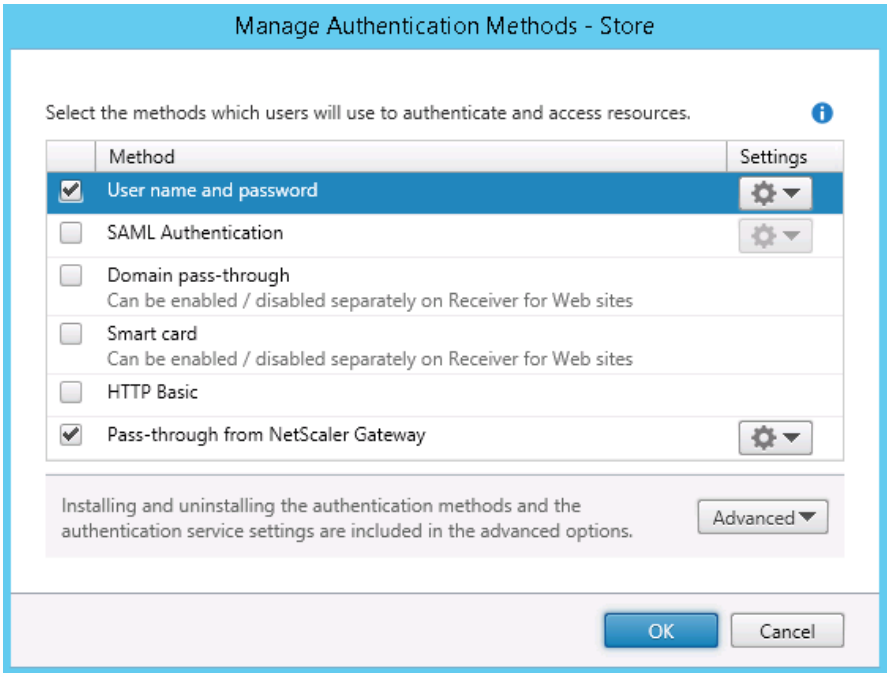
認証サービスの構成

Aug 14, 2017

認証方法の管理

ユーザーの認証方法を有効にしたり無効にしたりするには、Citrix StoreFront管理コンソールの結果ペインで認証方法を選択して、［操作］ペインの［認証方法の管理］をクリックします。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix**StoreFront**］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、**[操作]** ペインの **[認証方法の管理]** をクリックします。
3. ユーザーに許可するアクセス方法を指定します。



- 指定ユーザー認証を有効にするには **[ユーザー名とパスワード]** チェックボックスをオンにします。この場合、ユーザーは資格情報を入力してストアにアクセスします。
- SAML IDプロバイダーとの統合を有効にするには、**[SAML認証]** チェックボックスをオンにします。ユーザーはAccess Gatewayにログオンすることによって認証を受け、ストアにアクセスするときは自動的にログオンします。［設定］ボックスの一覧で次を選択します。
  - **IDプロバイダー**：IDプロバイダーの信頼性を構成する場合。
  - **サービスプロバイダー**：サービスプロバイダーの信頼性を構成する場合。この情報は、IDプロバイダーから要求されます。
- ユーザーデバイスからActive Directoryドメイン資格情報がパススルーされるようにするには、[ドメインパススルー] チェックボックスをオンにします。

この場合、ユーザーはドメインに参加しているWindowsコンピューターにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。このオプションを使用する場合は、Citrix Receiver for Windowsをユーザーデバイスにインストールするときにパススルー認証を有効にする必要があります。

- スマートカード認証を有効にするには、［スマートカード］チェックボックスをオンにします。ユーザーはスマートカードとPINを使ってストアにアクセスします。
- HTTP基本認証を有効にするには、［HTTP基本］チェックボックスをオンにします。ユーザー認証は、StoreFrontサーバーのIIS Webサーバーで実行されます。
- NetScaler Gatewayからのパススルー認証を有効にするには、［NetScaler Gatewayからのパススルー］チェックボックスをオンにします。ユーザーはNetScaler Gatewayにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。

NetScaler Gatewayを経由してストアにアクセスするスマートカードユーザーのパススルー認証を有効にするには、［認証の委任構成］タスクを使用します。

信頼されるユーザードメインの構成

ドメインの資格情報を明示的に入力して（直接またはNetScaler Gatewayを介したパススルー認証で）ログオンするユーザーのストアへのアクセスを制限するには、［信頼されるドメイン］タスクを使用します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、結果ペインで認証方法を選択します。［操作］ペインで **［認証方法の管理］** をクリックします。
3. **［ユーザー名とパスワード（明示的）］ > ［設定］** ドロップダウンメニューから、**［信頼されるドメイン**の構成］を選択します。
4. **［信頼済みドメインのみ］** をクリックして［追加］をクリックし、信頼されるドメインの名前を入力します。この認証サービスを使用するすべてのストアでは、ここで追加したドメインのアカウントでログオンできるようになります。ドメインを変更するには、［信頼されるドメイン］の一覧でエントリを選択して［編集］をクリックします。特定ドメインのユーザーアカウントでのアクセスを禁止するには、一覧でそのドメインを選択して［削除］をクリックします。
   管理者がドメイン名を指定する方法により、ユーザーが資格情報の入力時に使用すべき形式が決まります。ユーザーにドメインユーザー名形式で資格情報を入力させるには、一覧にNetBIOS名を追加します。ユーザーにユーザープリンシパル名形式で資格情報を入力させるには、一覧に完全修飾ドメイン名を追加します。ユーザーがドメインユーザー名形式でもユーザープリンシパル名形式でも資格情報を入力できるようにするには、一覧にNetBIOS名と完全修飾ドメイン名の両方を追加する必要があります。
5. 信頼されるドメインを複数構成する場合は、ユーザーがログオンするときにデフォルトで選択されるドメインを[デフォルトドメイン］ボックスの一覧から選択します。
6. ログオンページに信頼されるドメインを一覧表示するには、［ログオンページにドメイン一覧を表示する］チェックボックスをオンにします。

ユーザーがパスワードを変更できるようにする

ドメインの資格情報を使ってデスクトップのReceiverとReceiver for Webサイトにログオンするユーザーがパスワードを変更できるようにするには、**［パスワードオプションの管理］** タスクを使用します。認証サービスを作成したときのデフォルトの構成では、パスワードが失効しても、Citrix ReceiverとCitrix Receiver for Webサイトのユーザーはパスワードを変更できません。この機能を有効にする場合は、サーバーが属しているドメインのポリシーでユーザーによるパスワード変更が禁止されていないことを確認してください。ユーザーによるパスワードの変更を有効にすると、この認証サービスを使用するストアにアクセスできるすべてのユーザーに、慎重に扱うべきセキュリティ機能が公開されることになります。組織のセキュリティポリシーにより、ユーザーパスワード変更機能が内部使用のみに制限される環境では、社内ネットワークの外側からそれらのストアにアクセスできないことを確認してください。

1. Citrix Receiver for Webは、選択的なパスワードの変更に加えて、有効期限が切れた時のパスワードの変更をサポートします。すべてのデスクトップCitrix Receiverは、有効期限が切れた時にのみNetScaler Gatewayを介したパスワードの変更を

ポートします。Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。

2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、［操作］ペインの［認証方法の管理］をクリックします。
3. **［ユーザー名とパスワード］ > ［設定］** ドロップダウンメニューから、**[パスワードオプションの管理]** を選択し、ドメインの資格情報を使ってCitrix Receiver for Webサイトにログオンするユーザーに、パスワードの変更を許可する条件を指定します。
   - ユーザーがいつでもパスワードを変更できるようにするには、［常時］を選択します。パスワードの期限切れが近いローカルユーザーには、ログオン時に警告が表示されます。パスワードの有効期限切れの警告は、内部ネットワークから接続しているユーザーにのみ表示されます。デフォルトでは、ユーザーに対する通知期間は、適用されるWindowsポリシーの設定によって決まります。この通知期間の設定について詳しくは、「パスワードの有効期限切れ通知期間の構成」を参照してください。Citrix Receiver for Webでのみサポートされます。
   - 有効期限切れのパスワードだけをユーザーが変更できるようにするには、［失効したとき］を選択します。パスワードが失効してログオンできなくなったユーザーには、［パスワードの変更］ダイアログボックスが開きます。デスクトップのCitrix ReceiverとCitrix Receiver for Webでサポートされます。
   - ユーザーによるパスワードの変更を禁止するには、**[ユーザーにパスワードの変更を許可する]** の選択を解除します。このオプションを選択しない場合は、パスワードが失効してデスクトップやアプリケーションにアクセスできないユーザーをどのようにサポートするかを検討しておく必要があります。

   Citrix Receiver for Webサイトのユーザーがいつでもパスワードを変更できるように構成する場合は、StoreFrontサーバー上にすべてのユーザーのプロファイルを保存するための空き領域があることを確認してください。StoreFrontではユーザーのパスワードの失効が近いかどうかを確認するため、サーバー上に各ユーザーのローカルプロファイルが作成されます。ユーザーのパスワードを変更するには、StoreFrontはドメインコントローラーと通信する必要があります。

Citrix Receiver	StoreFrontで有効になっている場合、ユーザーが有効期限切れのパスワードできる	パスワードの有効期限が切れたら、ユーザーに通知される	StoreFrontで有効になっている場合は、パスワードの有効期限が切れる前に、ユーザーがそれを変更できる
Windows：	はい		
Mac：	はい		
Android			
iOS			
Linux：	はい		
Web	はい	はい	はい

セルフサービスパスワードリセットのセキュリティの質問

セルフサービスパスワードリセットにより、エンドユーザーは自身のユーザーアカウントをより詳細に制御できるようになります。セルフサービスパスワードリセットが構成されると、エンドユーザーは、システムへのログオンで問題がある場合にいくつかのセキュリティの質問に答えることによって、アカウントのロックを解除するか、パスワードをリセットして新しいパスワードを設定できます。

セルフサービスパスワードリセットのセットアップ時に、管理コンソールを使用してパスワードのリセットとアカウントのロック解除を許可するユーザーを指定します。StoreFrontでこれらの機能を有効にしても、セルフサービスパスワードリセットの設定で許可されていないユーザーは、これらの操作を行うことができません。

セルフサービスパスワードリセットは、ユーザーがHTTPS接続を使ってStoreFrontにアクセスする場合にのみ使用できます。ユーザーは、HTTP接続とセルフサービスパスワードリセットを使用しても、StoreFrontにアクセスすることはできません。セルフサービスパスワードリセットは、ユーザー名とパスワードでStoreFrontに直接認証する場合にのみ利用できます。

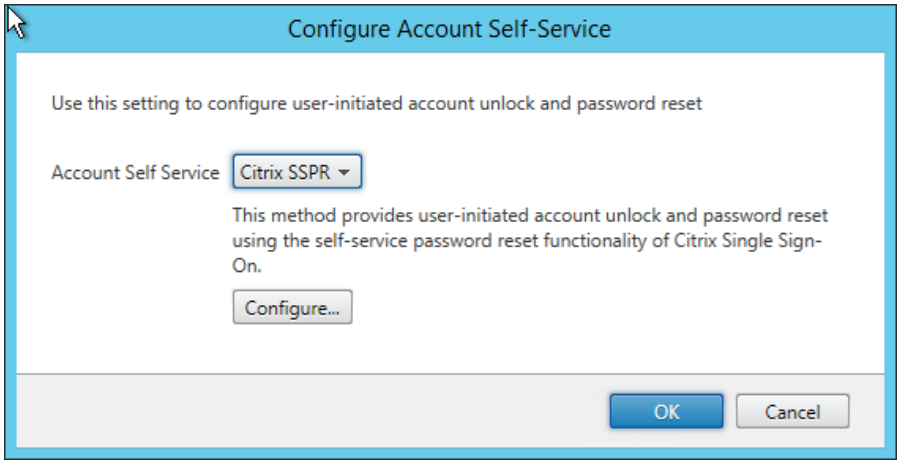
セルフサービスパスワードリセットでは、username@domain.comなどのUPNログオンはサポートされません。

ストアのセルフサービスパスワードリセットを設定する前に、次のことを確認する必要があります。

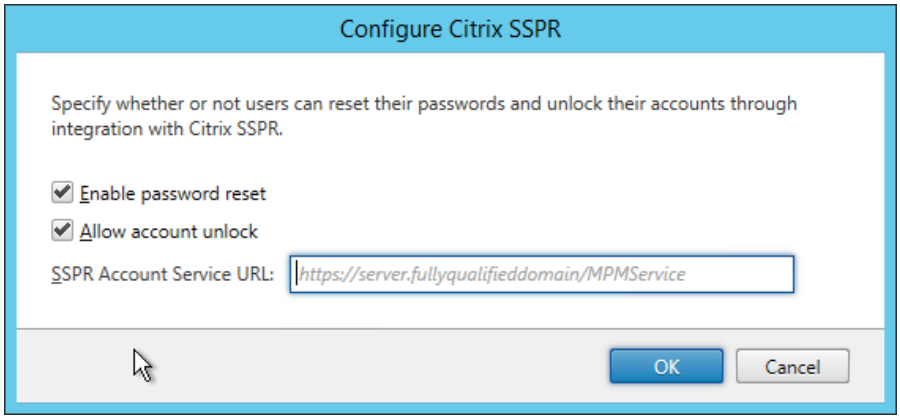
- ストアが、ユーザー名とパスワードによる認証を使用するように構成されている。
- ストアが、1つのセルフサービスパスワードリセットのみを使用するように構成されている。StoreFrontが、複数の同じドメインまたは信頼されているドメイン内にある複数のサーバーファームを使用するように構成されている場合は、これらすべてのドメインの資格情報を受け入れるようにセルフサービスパスワードリセットを構成する必要があります。
- ストアが、ユーザーがパスワードを常時変更できるように構成されている（パスワードのリセット機能を有効にする場合）。
- StoreFrontストアをReceiver for Webサイトに割り当てる必要があり、そのサイトが統合エクスペリエンスを使用するように構成する必要がある。

セルフサービスパスワードリセットを使用できるようにするには、インストールして構成する必要があります。XenApp 7.11およびXenDesktop 7.11のメディアで可能です。詳しくは、「セルフサービスパスワードリセット」を参照してください。

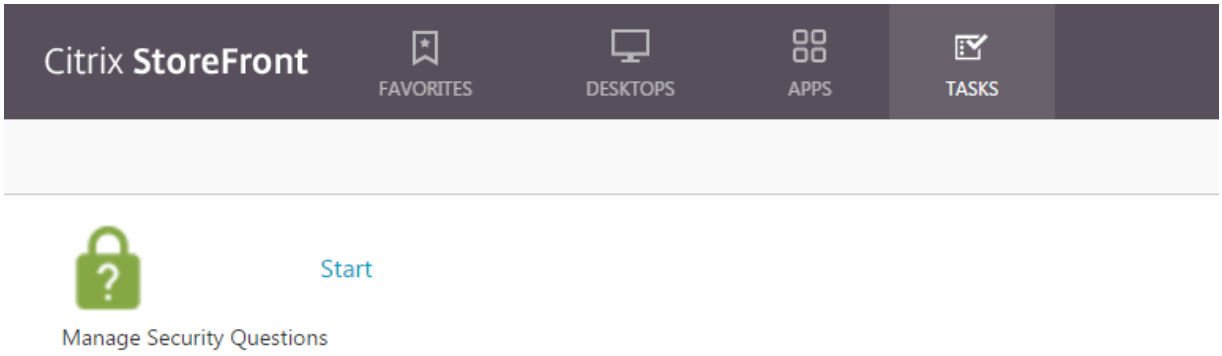
1. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、 **[操作]** ペインの **[認証方法の管理] > [ユーザー名とパスワード]** をクリックし、ドロップダウンメニューから **[パスワードオプションの管理]** を選択します。
2. パスワードの変更を許可するユーザーを選択し、 **[OK]** をクリックします。
3. **[ユーザー名とパスワード]** ボックスの一覧で **[アカウントセルフサービスの設定]** を選択し、ドロップダウンメニューで **[Citrix SSPR]** を選択して **[OK] をクリックします。**
4. ユーザーに対して、セルフサービスパスワードリセットを使用したパスワードのリセットおよびアカウントのロック解除を許可するかどうかを指定して、パスワードリセットサービスのアカウントURLを追加し **[OK]** 、そして **[OK] をクリックします。**



このオプションは、StoreFrontベースのURLがHTTPS（HTTPではない）の場合にのみ利用可能であり、**[パスワードリセットを有効にする]** オプションは、 **[パスワードオプションの管理]** を使用してユーザーがいつでもパスワードを変更できるようにした後でのみ利用可能です。



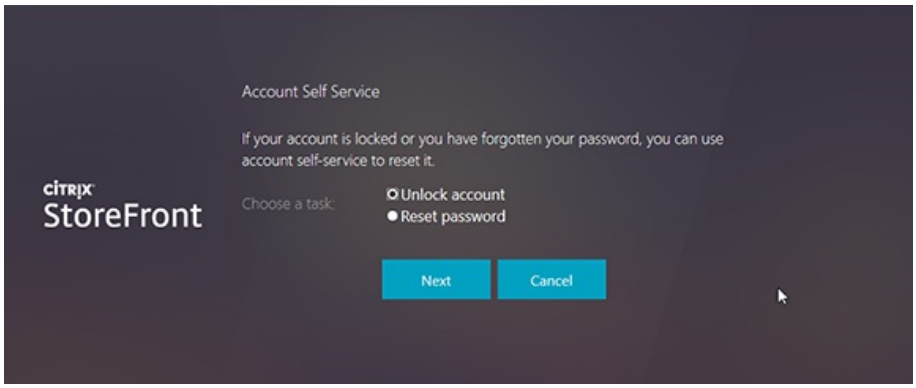
CitrixReceiverまたはCitrix Receiver for Webへの次回ユーザーログオン時に、セキュリティ用の質問に対する回答を登録できるようになります。 **[開始]** をクリックすると、ユーザーが回答を登録する必要のある質問が表示されます。



StoreFrontでの設定後、Citrix Receiver for Webのログオン画面に **[アカウントセルフサービス]** リンクが表示されるようになります（ほかのCitrix Receiverではボタンとして表示されます）。

このリンクをクリックすると、 **[アカウントのアンロック]** と **[パスワードのリセット]** （両方とも利用可能な場合）の間で、最初に選択する一連のフォームが表示されます。

ラジオボタンを選択して **[次へ]** をクリックすると、次の画面ではドメインとユーザー名（*ドメイン\ユーザー*）の入力を求められます（この情報がログオンフォームで入力されていない場合）。アカウントセルフサービスでは、username@domain.comなどのUPNログオンはサポートされないことに注意してください。



ユーザーは、セキュリティの質問に回答するように求められます。すべての回答が、ユーザーが入力した回答と一致すると、要求した操作（ロック解除またはリセット）が実行され、操作に成功したことを示すメッセージが表示されます。

共有認証サービス設定

共有認証サービス設定タスクを使ってストアを指定し、ストア間でシングルサインオンを有効にする認証サービスを共有します。

1. Windowsの［**スタート**］画面または［**アプリ**］画面で、［**Citrix StoreFront**］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［**ストア**］ノードを選択して、結果ペインでストアを選択します。［**操作**］ペインで［**認証方法の管理**］をクリックします。
3. ［**詳細**］ドロップダウンメニューから、［**共有認証サービス設定**］を選択します。
4. ［**共有認証サービスを使用する**］チェックボックスをオンにして、［**ストア**］名ドロップダウンメニューからストアを選択します。

注：共有認証サービスと専用認証サービス間には機能的な差異はありません。2つ以上のストアによって共有される認証サービスは、共有認証サービスとして扱われ、構成の変更はいずれも共有認証サービスを使用するすべてのストアに対して適用されます。

資格情報の検証をNetScaler Gatewayに委任する

NetScaler Gatewayを経由してストアにアクセスするスマートカードユーザーのパススルー認証を有効にするには、［認証の委任構成］タスクを使用します。このタスクは、［NetScaler Gatewayからのパススルー］が有効で、その認証方法が結果ペインで選択されている場合のみ使用できます。

資格情報の検証をNetScaler Gatewayに委任した場合、ユーザーはスマートカードを使ってNetScaler Gatewayにログオンし、ストアにアクセスするときは自動的に認証されます。スマートカードユーザーのパススルー認証は、管理者がNetScaler Gatewayからのパススルー認証を有効にするとデフォルトで無効になるため、ユーザーがパスワードを使ってNetScaler Gatewayにログオンした場合にのみパススルー認証が発生します。

XMLサービスベースの認証

Aug 14, 2017

StoreFrontがXenAppまたはXenDesktopと同じドメイン内にない場合、またActive Directoryの信頼を適切に配置できない場合には、XenAppおよびXenDesktop XML Serviceを使ってユーザー名とパスワード資格情報を認証するようにStoreFrontを構成できます。

XMLサービスベースの認証の有効化

1. Windowsの **[スタート]** 画面または［アプリ］画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、［操作］ペインの **[認証方法の管理]** をクリックします。
3. **[認証方法の管理]** ページで、 **[ユーザー名とパスワード] > [設定]** ドロップダウンメニューから、 **[パスワード確認の構成]** を選択します。
4. **[パスワード検証方法]** ドロップダウンメニューから **[Delivery Controller]** を選択し、 **[構成]** をクリックします。
5. **[Delivery Controllerの構成]** 画面に従って、1つまたは複数の**Delivery Controller**を追加して、ユーザー資格情報を確認し、 **[OK]** をクリックします。

XMLサービスベースの認証を無効にします

1. Windowsの **[スタート]** 画面または［アプリ］画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、［操作］ペインの **[認証方法の管理]** をクリックします。
3. **[認証方法の管理]** ページで、 **[ユーザー名とパスワード] > [設定]** ドロップダウンメニューから、 **[パスワード確認の構成]** を選択します。
4. **[パスワード検証方法]** ドロップダウンメニューから **[Active Directory]** を選択し、 **[OK]** をクリックします。

XenApp 6.5でのKerberos制約付き委任の構成

Aug 14, 2017

［ストア設定の構成］>［Kerberos委任］タスクを使って、StoreFrontでDelivery Controllerの認証に単一ドメインKerberos制約付き委任を使用するかどうかを指定します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、結果ペインでストアを選択します。［操作］ペインで、**［ストア設定の構成］**をクリックし、［Kerberos委任］をクリックします。
3. ［Delivery Controllerでの認証にKerberos委任］を有効または無効にして、Kerberos制約付き委任を有効または無効にします。

委任用のStoreFrontサーバーの構成

StoreFrontがXenAppと同じマシンにインストールされていない場合は、次の手順に従います。

1. ドメインコントローラーで、MMCの［Active Directoryユーザーとコンピューター］スナップインを開きます。
2. ［表示］メニューで［詳細］を選択します。
3. コンソールツリーで、ドメイン名の下の［Computers］から、StoreFrontサーバーを選択します。
4. ［操作］ペインの［プロパティ］を選択します。
5. ［委任］タブで、［指定されたサービスへの委任でのみこのユーザーを信頼する］、［任意の認証プロトコルを使う］の順にクリックし、［追加］をクリックします。
6. ［サービスの追加］ダイアログボックスで、［ユーザーまたはコンピューター］をクリックします。
7. ［ユーザーまたはコンピューターの選択］ダイアログボックスの［選択するオブジェクト名を入力してください］ボックスに、Citrix XML Service（XenApp）サーバーの名前を入力し、［OK］をクリックします。
8. 一覧からHTTPサービスタイプを選択し、［OK］をクリックします。
9. 変更を適用し、ダイアログボックスを閉じます。

委任用のXenAppサーバーの構成

各XenAppサーバーでのActive Directoryの信頼済み委任を構成します。

1. ドメインコントローラーで、**MMCの［Active Directoryユーザーとコンピューター］**スナップインを開きます。
2. コンソールツリーで、ドメイン名の下の**［Computers］**から、StoreFrontが接続するCitrix XML Service（XenApp）のサーバーを選択します。
3. **［操作］**ペインの**［プロパティ］**を選択します。
4. **［委任］**タブで、**［指定されたサービスへの委任でのみこのユーザーを信頼する］**、**［任意の認証プロトコルを使う］**の順にクリックし、**［追加］**をクリックします。
5. **［サービスの追加］**ダイアログボックスで、**［ユーザーまたはコンピューター］**をクリックします。
6. **［ユーザーまたはコンピューターの選択］**ダイアログボックスの**［選択するオブジェクト名を入力してください］**ボックスに、Citrix XML Service（XenApp）サーバーの名前を入力し、**［OK］**をクリックします。
7. 一覧からHOSTサービスタイプを選択して、**［OK］**、**［追加］**の順にクリックします。
8. **［ユーザーまたはコンピューターの選択］**ダイアログボックスの**［選択するオブジェクト名を入力してください］**ボックスにDomain Controllerの名前を入力し、**［OK］**をクリックします。
9. 一覧から**cifs**および**ldap**サービスタイプを選択し、**［OK］**をクリックします。注：ldapサービスが2つある場合は、使用するドメインコントローラーの完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）に一致する方を選択してくださ

い。

10. 変更を適用し、ダイアログボックスを閉じます。

重要な注意事項

Kerberos制約付き委任を使用するかどうかを判断するときは、以下の点に注意してください。

- 主な注意事項：
  - Kerberos制約付き委任を使用しない状態でパススルー認証（スマートカードPINのパススルー認証）を行わない限り、ssonsvr.exeは必要ありません。
- StoreFrontとCitrix Receiver for Webのドメインパススルー：
  - クライアントでは、ssonsvr.exeは必要ありません。
  - Citrix icaclient.admテンプレートの［Local username and password］は、ssonsvr.exe機能を制御する任意のものに対して設定できます。
  - icaclient.admテンプレートの［Kerberos］設定が必要です。
  - Internet Explorerの［信頼済みサイト］一覧にStoreFrontのFQDNを追加します。Internet Explorerの信頼済みゾーンのセキュリティ設定の［Use local username］チェックボックスをオンにします。
  - クライアントはドメイン内に配置する必要があります。
  - StoreFrontサーバーで［ドメインパススルー］認証方法を有効にし、Citrix Receiver for Webでも有効にします。
- StoreFront、Citrix Receiver for Web、およびPINプロンプトによるスマートカード認証：
  - クライアントでは、ssonsvr.exeは必要ありません。
  - スマートカード認証は構成済みです。
  - Citrix icaclient.admテンプレートの［Local username and password］は、ssonsvr.exe機能を制御する任意のものに対して設定できます。
  - icaclient.admテンプレートの［Kerberos］設定が必要です。
  - StoreFrontサーバーで［スマートカード］認証方法を有効にし、Citrix Receiver for Webでも有効にします。
  - スマートカード認証が選択されるようにするには、Internet ExplorerのStoreFrontサイトゾーンのセキュリティ設定で[Use local username］チェックボックスをオフにします。
  - クライアントはドメイン内に配置する必要があります。
- NetScaler Gateway、StoreFront、Citrix Receiver for Web、およびPINプロンプトによるスマートカード認証：
  - クライアントでは、ssonsvr.exeは必要ありません。
  - スマートカード認証は構成済みです。
  - Citrix icaclient.admテンプレートの［Local username and password］は、ssonsvr.exe機能を制御する任意のものに対して設定できます。
  - icaclient.admテンプレートの［Kerberos］設定が必要です。
  - StoreFrontサーバーで［NetScaler Gatewayからのパススルー］認証方法を有効にし、Citrix Receiver for Webでも有効にします。
  - スマートカード認証が選択されるようにするには、Internet ExplorerのStoreFrontサイトゾーンのセキュリティ設定で[Use local username］チェックボックスをオフにします。
  - クライアントはドメイン内に配置する必要があります。
  - NetScaler Gatewayのスマートカード認証を構成し、追加の仮想サーバーを構成します。この認証不要なNetScaler Gateway仮想サーバー経由でICAトラフィックがStoreFront HDXでルーティングされるように構成します。
- Citrix Receiver for Windows（AuthManager）、PINプロンプトによるスマートカード認証、およびStoreFront：
  - クライアントでは、ssonsvr.exeは必要ありません。
  - Citrix icaclient.admテンプレートの［Local username and password］は、ssonsvr.exe機能を制御する任意のものに対して設定できます。
  - icaclient.admテンプレートの［Kerberos］設定が必要です。
  - クライアントはドメイン内に配置する必要があります。
  - StoreFrontサーバーで［スマートカード］認証方法を有効にします。
- Citrix Receiver for Windows（AuthManager）、KerberosおよびStoreFront：
  - クライアントでは、ssonsvr.exeは必要ありません。
  - Citrix icaclient.admテンプレートの［Local username and password］は、ssonsvr.exe機能を制御する任意のものに対して設定できます。
  - icaclient.admテンプレートの［Kerberos］設定が必要です。
  - Internet Explorerの信頼済みゾーンのセキュリティ設定の［Use local username］チェックボックスをオンにします。
  - クライアントはドメイン内に配置する必要があります。
  - StoreFrontサーバーで［ドメインパススルー］認証方法を有効にします。
  - 次のレジストリキーが設定されていることを確認します。

    注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

    32ビットマシンの場合：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManagerProtocols\integratedwindows
    名前：SSONCheckEnabled

種類：REG_SZ
値：trueまたはfalse

64ビットマシンの場合：
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\AuthManagerProtocols\integratedwindows

名前： SSONCheckEnabled
種類： REG_SZ
値：trueまたはfalse

スマートカード認証の構成

Aug 14, 2017

このトピックでは、一般的なStoreFront展開環境のすべてのコンポーネントでスマートカード認証を設定するための概要について説明します。詳細と構成手順については、各製品のドキュメントを参照してください。

Citrix環境のスマートカード構成

This overview for configuring a Citrix deployment for smart cards uses a specific smart card type. Note that similar steps apply to smart cards from other vendors.

- StoreFrontサーバーを展開するMicrosoft Active Directoryドメインか、そのドメインと直接の双方向の信頼関係が設定されているドメインのいずれかにすべてのユーザーアカウントが属していることを確認します。
- スマートカードパススルー認証を有効にする場合は、スマートカードリーダーの種類、ミドルウェアの種類と構成、およびミドルウェアのPINのキャッシュポリシーでパススルー認証が許可されることを確認します。
- ユーザーのデスクトップやアプリケーションを提供する、Virtual Delivery Agentが動作する仮想マシンや物理マシンに、スマートカードのベンダーが提供するミドルウェアをインストールします。XenDesktop環境でスマートカードを使用する方法については、「スマートカードによる認証セキュリティ」を参照してください。
- 事前に公開キーインフラストラクチャが正しく構成されていることを確認します。アカウントマッピングのための証明書がActive Directory環境に対して正しく構成されており、ユーザー証明書の検証を正しく実行できることを確認します。

- NetScaler Gatewayアプライアンスに、証明機関からの署名入りサーバー証明書をインストールします。詳しくは、「Installing and Managing Certificates」を参照してください。
- アプライアンスに、スマートカードユーザーの証明書を発行した証明機関のルート証明書をインストールします。詳しくは、「To install a root certificate on NetScaler Gateway」を参照してください。
- クライアント証明書認証用の仮想サーバーを作成して構成します。証明書認証ポリシーを作成し、証明書のユーザー名抽出オプションとして「SubjectAltName:PrincipalName」を指定します。さらに、このポリシーを仮想サーバーにバインドして、クライアント証明書を要求するように構成します。詳しくは、「Configuring and Binding a Client Certificate Authentication Policy」を参照してください。
- 証明機関のルート証明書を仮想サーバーにバインドします。詳しくは、「To add a root certificate to a virtual server」を参照してください。
- 資格情報を再入力せずにリソースに接続されるようにするには、仮想サーバーをもう1つ作成し、SSL（Secure Sockets Layer）パラメーターでクライアント認証を無効にします。詳しくは、「スマートカード認証の構成」を参照してください。
  管理者は、作成した仮想サーバー経由でユーザー接続がルーティングされるようにStoreFrontを構成する必要もあります。ユーザーは最初の仮想サーバーにログオンします。作成した（2つ目の）仮想サーバーはリソースへの接続に使用されます。接続時にNetScaler Gatewayにログオンする必要はありませんが、デスクトップやアプリケーションへのログオン時にPINを入力する必要があります。スマートカードでの認証の失敗時に指定ユーザー認証を使用できるように設定する場合を除き、2つ目の仮想サーバーをリソースへのユーザー接続用に構成することは省略可能です。

- NetScaler Gateway経由でStoreFrontに接続するためのセッションポリシーおよびセッションプロファイルを作成して、それらを適切な仮想サーバーにバインドします。詳しくは、「Access to StoreFront Through NetScaler Gateway」を参照してください。
- StoreFrontへの接続用の仮想サーバーを構成するときに、すべての通信がクライアント証明書で認証されるように指定した場合は、StoreFrontのコールバックURLを提供する仮想サーバーをさらに作成する必要があります。この仮想サーバーは、

StoreFrontでNetScaler Gatewayアプライアンスからの要求を検証するためだけに使用されるため、公開ネットワークからアクセス可能である必要はありません。クライアント証明書による認証が必要な場合は、隔離された仮想サーバーが必要です。これは、認証用の証明書をStoreFrontで提示できないためです。詳しくは、「仮想サーバーの作成」を参照してください。

- スマートカード認証を有効にするには、StoreFrontとユーザーデバイス間の通信でHTTPSが使用されるように構成する必要があります。Microsoftインターネットインフォメーションサービス（IIS）でHTTPSを構成します。これを行うには、IISでSSL証明書を入手して、HTTPSバインドをデフォルトのWebサイトに追加します。IISでのサーバー証明書の作成について詳しくは、http://technet.microsoft.com/ja-jp/library/hh831637.aspx#CreateCertificateを参照してください。IISサイトへのHTTPSバインドの追加について詳しくは、http://technet.microsoft.com/ja-jp/library/hh831632.aspx#SSLBindingを参照してください。
- すべてのStoreFront URLへのHTTPS接続でクライアント証明書が要求されるようにするには、StoreFrontサーバー上でIISを構成します。
  StoreFrontインストール時のIISのデフォルト構成では、StoreFront認証サービスの証明書認証URLへのHTTPS接続でのみクライアント証明書が要求されます。この構成は、ユーザーがスマートカードでログオンできない場合に指定ユーザー認証でログオンできるようにしたり、再認証なしにスマートカードを取り出せるようにするために必要です。

  すべてのStoreFront URLへのHTTPS接続でクライアント証明書が要求されるようにIISを構成すると、スマートカードユーザーがNetScaler Gateway経由で接続できなくなり、指定ユーザー認証にもフォールバックされません。また、スマートカードをデバイスから取り出す場合は再度ログオンする必要があります。このIISサイト構成を有効にするには、認証サービスとストアを同じサーバー上に配置して、すべてのストアに対して有効なクライアント証明書を使用する必要があります。また、すべてのStoreFront URLへのHTTPS接続でクライアント証明書が要求されるようにIISを構成すると、Citrix Receiver for Webクライアントでの認証に問題が生じます。このため、Citrix Receiver for Webクライアントを使用しない場合のみ、この構成を使用してください。

  StoreFrontをWindows Server 2012上にインストールして、IISでSSLとクライアント証明書による認証を有効にする場合、サーバー上の「信頼されたルート証明機関」の証明書ストアにインストールされた非自己署名証明書が拒否されることに注意してください。詳しくは、http://support.microsoft.com/kb/2802568を参照してください。

- StoreFrontをインストールして構成します。必要に応じて、認証サービスを作成し、ストアを追加します。NetScaler Gatewayを介したリモートアクセスを有効にする場合は、仮想プライベートネットワーク（VPN）統合を有効にしないでください。詳しくは、「StoreFrontのインストールとセットアップ」を参照してください。
- 内部ネットワーク上のローカルユーザーに対して、StoreFrontへのスマートカード認証を有効にします。スマートカードユーザーがNetScaler Gateway経由でストアにアクセスする場合は、認証方法としてNetScaler Gatewayからのパススルーを有効にして、資格情報の検証をNetScaler Gatewayに委任します。ドメインに参加しているユーザーデバイスにCitrix Receiver for Windowsをインストールするときにパススルー認証を有効にする場合は、ドメインパススルー認証を有効にしておきます。詳しくは、「認証サービスの構成」を参照してください。
  Citrix Receiver for Webクライアントでスマートカードによる認証を許可するには、各Citrix Receiver for Webサイトでこの認証方法を有効にする必要があります。方法については、「Citrix Receiver for Webサイトの構成」を参照してください。

  スマートカード認証で指定ユーザー認証へのフォールバックを有効にする場合は、ユーザー名とパスワードを使用する認証方法を無効にしないでください。

- ドメインに参加しているユーザーデバイスにCitrix Receiver for Windowsをインストールするときにパススルー認証を有効にする場合は、デスクトップやアプリケーションにアクセスするときにスマートカードの資格情報がパススルーされるようにストアのdefault.icaファイルを編集します。詳しくは、「Citrix Receiver for Windowsのスマートカードパススルー認証を有効にする」を参照してください。
- デスクトップやアプリケーションへのユーザー接続のみに使用されるNetScaler Gateway仮想サーバーを追加した場合は、

その仮想サーバーを経由する「最適なNetScaler Gatewayルーティング」を構成します。詳しくは、「ストアの最適なHDX
ルーティングの構成」を参照してください。

- ドメインに不参加のWindowsデスクトップアプライアンスのユーザーがスマートカードを使用してデスクトップにログオンできるようにするには、デスクトップアプライアンスサイトへのスマートカード認証を有効にします。詳しくは、「デスクトップアプライアンスサイトの構成」を参照してください。

  デスクトップアプライアンスサイトでスマートカード認証および指定ユーザー認証の両方を有効にして、スマートカードでログオンできない場合は資格情報を入力してログオン（指定ユーザー認証）できるようにします。

- ドメインに参加しているデスクトップアプライアンスのユーザー、およびCitrix Desktop Lockを実行している再目的化されたPCのユーザーがスマートカードを使用して認証できるようにするには、XenApp Servicesサイトへのスマートカードパススルー認証を有効にします。詳しくは、「XenApp Services URLの認証の構成」を参照してください。

- すべてのユーザーデバイスに、スマートカードのベンダーが提供するミドルウェアをインストールします。
- ユーザーが、ドメインに不参加のWindowsデスクトップアプライアンスを使用する場合は、管理者権限を持つアカウントでReceiver for Windows Enterpriseをインストールします。デバイスの電源を入れたときにInternet Explorerが全画面モードで起動して、デスクトップアプライアンスサイトが表示されるように構成します。デスクトップアプライアンスサイトのURLでは大文字と小文字が区別されることに注意してください。デスクトップアプライアンスサイトをInternet Explorerのローカルイントラネットまたは信頼済みサイトのゾーンに追加します。スマートカードを使用してデスクトップアプライアンスサイトにログオンして、ストアからリソースにアクセスできることを確認した後で、Citrix Desktop Lockをインストールします。詳しくは、「Desktop Lockをインストールするには」を参照してください。
- ユーザーが、ドメインに参加しているデスクトップアプライアンスや再目的化されたPCを使用する場合は、管理者権限を持つアカウントでReceiver for Windows Enterpriseをインストールします。Receiver for Windowsを構成するときに、適切なストアのXenApp ServicesサイトのURLを指定します。スマートカードを使用してデバイスにログオンして、ストアからリソースにアクセスできることを確認した後で、Citrix Desktop Lockをインストールします。詳しくは、「Desktop Lockをインストールするには」を参照してください。
- そのほかの場合は、適切なバージョンのCitrix Receiverをユーザーデバイスにインストールします。ドメインに参加しているデバイスのユーザーがXenDesktopやXenAppに接続するときのスマートカードパススルー認証を有効にするには、管理者アカウントを使ってReceiver for Windowsをコマンドラインでインストールします。このときに、/includeSSONオプションを指定します。詳しくは、「コマンドラインパラメーターを使用したReceiver for Windowsの構成とインストール」を参照してください。
  ドメインポリシーまたはローカルコンピューターポリシーで、スマートカード認証が使用されるようにReceiver for Windowsが構成されていることを確認します。ドメインポリシーは、グループポリシー管理コンソールを使用してReceiver for Windowsのグループポリシーオブジェクトのテンプレートファイルicaclient.admを、ユーザーアカウントが属しているドメインのドメインコントローラーにインポートします。デバイスごとに構成する場合は、そのデバイス上のグループポリシーオブジェクトエディターを使用してこのテンプレートを構成します。詳しくは、「グループポリシーオブジェクトテンプレートによるReceiverの構成」を参照してください。

  [Smart card authentication] ポリシーを有効にします。スマートカードの資格情報が自動的に使用（パススルー）されるようにするには、 [Use pass-through authentication for PIN] チェックボックスをオンにします。さらに、XenDesktopおよびXenAppにスマートカードの資格情報がパススルーされるようにするには、 [Local user name and password] ポリシーを有効にして、 [Allow pass-through authentication for all ICA connections] チェックボックスをオンにします。詳しくは、「ICA Settings Reference」を参照してください。

  ドメインに参加しているデバイスのユーザーがXenDesktopやXenAppに接続するときのスマートカードパススルー認証を有効にした場合は、ストアのURLをInternet Explorerのローカルイントラネットまたは信頼済みサイトのゾーンに追加します。この場合、そのゾーンのセキュリティ設定で [現在のユーザー名とパスワードで自動的にログオンする] が選択されて

いることを確認してください。

- 必要な場合は、ストア（内部ネットワーク上のユーザーの場合）やNetScaler Gatewayアプライアンス（リモートユーザーの場合）に接続するための詳細を適切な方法でユーザーに提供します。構成情報のユーザーへの提供について詳しくは、「Citrix Receiver」を参照してください。

ドメインに参加しているユーザーデバイスにReceiver for Windowsをインストールするときに、パススルー認証（シングルサインオン）を有効にできます。XenDesktopおよびXenAppによってホストされているデスクトップおよびアプリケーションにアクセスするときにスマートカードの資格情報が自動的に使用（パススルー）されるようにするには、ストアのdefault.ストア用のデフォルトの.icaファイルを編集します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. テキストエディターを使ってストアのdefault テキストエディターを使ってストアのicaファイルを開きます。このファイルは通常、C:\inetpub\wwwroot\Citrix\storename\App_Data\フォルダーにあります。ここで、storenameはストアの作成時に指定した名前です。
2. NetScaler Gatewayを使用しないでストアにアクセスするユーザーのスマートカード資格情報のパススルーを有効にするには、次の設定を[Application]セクションに追加します。
   DisableCtrlAltDel=Off
   この設定はストアのすべてのユーザーに適用されます。デスクトップおよびアプリケーションに対するドメインパススルー認証とスマートカードパススルー認証の両方を有効にするには、これらの認証方法について個別のストアを作成する必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。
3. NetScaler Gatewayを使用してストアにアクセスするユーザーのスマートカード資格情報のパススルーを有効にするには、次の設定を[Application]セクションに追加します。
   UseLocalUserAndPassword=On
   この設定はストアのすべてのユーザーに適用されます。一部のユーザーに対してのみパススルー認証を有効にする場合は、それらのユーザー用に個別のストアを作成する必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。

パスワードの有効期限切れ通知期間の構成

Aug 14, 2017

Citrix Receiver for Webサイトのユーザーがいつでもパスワードを変更できるように設定してある場合は、パスワードの有効期限切れが近いローカルユーザーがログオンしたときに警告が表示されます。デフォルトでは、ユーザーに対する通知期間は、適用されるWindowsポリシーの設定によって決まります。すべてのユーザーに対するカスタムの通知期間を設定するには、認証サービスの構成ファイルを編集します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの **[スタート]** 画面または［アプリ］画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、［操作］ペインの **[認証方法の管理]** をクリックします。
3. **[認証方法の管理]** ページで、 **[ユーザー名とパスワード]** > **[設定]** ドロップダウンメニューから **[パスワードオプションの管理]** を選択し、 **[ユーザーにパスワードの変更を許可する]** チェックボックスをオンにします。
4. **[常に許可...]** を選択し、 **[パスワードの期限が切れる前にユーザーにリマインドする]** の下で項目を選択します。

注：StoreFrontでは、Active Directoryの細かい設定が可能なパスワードポリシーはサポートされません。

ストアの構成と管理

Aug 14, 2017

Citrix StoreFrontでは、XenAppおよびXenDesktopからアプリケーションやデスクトップをまとめるストアを作成して管理し、ユーザーにリソースに対するセルフサービスアクセスをオンデマンドで提供できます。

ストアの作成または削除	必要とするできるだけ多くの追加ストアを構成します。
認証が不要なストアの作成	追加の未認証のストアを構成し、認証不要（匿名）ユーザーのアクセスをサポートする。
ユーザー用のストアプロビジョニングファイルのエクスポート	ストアに対して構成されたNetScaler Gateway展開やビーコンなど、ストアに対する接続の詳細を含んでいるファイルを生成します。
ストアの非表示とアドバタイズ	ユーザーがメールアドレスによるアカウント検出機能または完全修飾ドメイン名（FQDN）を使ってCitrix Receiverを構成する場合、ユーザーに表示されているストアがユーザーのアカウントに追加されないようにします。
ストアに表示するリソースの管理	ストアからのリソースの追加と削除
NetScaler Gatewayを介したストアへのリモートアクセスの管理	公共のネットワークから接続するユーザーに対してNetScaler Gatewayを介したストアへのアクセスを構成します。
Citrix Onlineアプリケーションのストアへの統合	ストアに追加するCitrix Onlineアプリケーションを選択して、ユーザーがCitrix OnlineアプリケーションをサブスクライブしたときのCitrix Receiverの動作を指定します。
共通のサブスクリプションデータストアを共有する2つのStoreFrontストアの構成	共通のサブスクリプションデータベースを共有する2つのストアの構成
上級ストア設定	上級ストア設定を構成します。

ストアの作成または削除

Aug 14, 2017

追加のストアを構成するには、［ストアの作成］タスクを使用します。ストアは必要なだけ作成できます。たとえば、特定のユーザーグループ用にストアを作成したり、特定のリソースセットを集約するストアを作成したりできます。また、認証が不要な匿名ユーザー用のストアを作成することもできます。この種類のサイトの作成方法については、「認証が不要なストアの作成」を参照してください。

ストアを作成するには、そのストアのユーザーにリソースを提供するサーバーを指定して、その通信構成を行います。次に、リモートアクセスを有効にする場合は、使用するNetScaler Gatewayアプライアンスを指定します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、［操作］ペインの［ストアの作成］をクリックします。
3. ［ストア名］ページで、ストアの名前を指定して、［次へ］をクリックします。
   ストアの名前はCitrix Receiverでユーザーアカウントの下に表示されるため、ユーザーにとってわかりやすい名前を指定してください。
4. ［Delivery Controller］ページでは、リソースを提供するインフラストラクチャを一覧に追加します。［Add］をクリックします。
5. ［Delivery Controllerの追加］ダイアログボックスで、この展開環境に対するわかりやすい名前を指定し、リソースを提供するインフラストラクチャの種類（［XenDesktop］、［XenApp］、または［AppController］）を選択します。App Controllerを選択する場合は、表示名として入力した文字列にスペースが含まれていないことを確認してください。
6. インフラストラクチャの種類としてXenDesktopまたはXenAppサーバーを選択した場合は、手順7.に進みます。App Controllerにより管理されるアプリケーションをストアで使用できるようにするには、App Controller仮想アプライアンスの名前またはIPアドレスを［サーバー］ボックスに入力し、App Controllerへの接続に使用するStoreFrontのポートを指定します。デフォルトのTCPポートは443です。手順10.に進みます。
7. リソースを提供するインフラストラクチャの種類としてXenDesktop、またはXenAppを選択した場合は、サーバーの名前またはIPアドレスを［サーバー］一覧に追加します。この一覧に複数のサーバーを追加すると、その順番に基づいてフェールオーバーされます。XenDesktopサイトの場合は、Delivery Controllerの詳細を指定します。XenAppファームの場合は、Citrix XML Serviceを実行しているサーバーを一覧に追加します。
8. ［トランスポートの種類］ボックスの一覧から、StoreFrontでサーバーとの通信に使用する接続の種類を選択します。
   - 暗号化されていない接続でデータを送信するには［HTTP］を選択します。このオプションを選択する場合は、StoreFrontとサーバー間の接続を何らかの方法で保護することを検討してください。
   - SSL（Secure Sockets Layer）またはTLS（Transport Layer Security）を使用する保護されたHTTP接続でデータを送信するには、［HTTPS］を選択します。XenDesktopまたはXenAppサーバーに対してこのオプションを選択する場合は、Citrix XML ServiceがポートをIIS（Microsoftインターネットインフォメーションサービス）と共有する設定になっていることと、IISがHTTPSをサポートするように構成されていることを確認してください。
   - XenAppサーバーとの通信でSSL Relayによるホスト認証とデータの暗号化を実行するには、［SSL Relay］を選択します。

   注：StoreFrontとサーバーの間の通信でHTTPSまたはSSL Relayを使用する場合は、［サーバー］ボックスの一覧に指定したサーバー名がそのサーバーの証明書のサーバー名と一致することを確認してください（大文字/小文字は区別されます）。

9. StoreFrontがサーバーに接続するときに使用するポートを指定します。デフォルトでは、HTTP接続およびSSL Relay接続では80、HTTPS接続では443が使用されます。XenDesktopおよびXenAppサーバーの場合、Citrix XML Serviceで使用されるポート番号を指定する必要があります。
10. StoreFrontとXenAppサーバーの間の接続をSSL Relayで保護する場合は、SSL RelayのTCPポートを［SSL Relayポート］ボックスで指定します。デフォルトのTCPポートは443です。SSL Relayを実行するすべてのサーバーで同じポートが構成されていることを確認してください。
11. ［OK］をクリックします。XenDesktop、XenApp、およびApp Controllerの展開環境を自由に組み合わせてストアを作成できます。必要に応じて手順4.～12.を繰り返し、ストアにリソースを提供する展開環境を一覧に追加します。必要なリソースをすべてストアに追加したら、［次へ］をクリックします。
12. ［リモートアクセス］ページでは、公共のネットワーク上のユーザーにNetScaler Gatewayを介したアクセス（リモートアクセス）を提供するかどうか、およびその方法を指定します。
    - 公共のネットワーク上でストアをユーザーが使用できないようにするには、**［リモートアクセスの有効化］**チェックボックスをオフにします。これにより、内部ネットワークのローカルユーザーのみがストアにアクセスできるようになります。
    - リモートアクセスを有効にするには、**［リモートアクセスの有効化］**をオンにします。
      - NetScaler Gateway経由でアクセスするユーザーにストアのリソースのみを提供するには、［VPNトンネルなし］を選択します。この場合、ユーザーはNetScaler Gatewayに直接ログオンするため、NetScaler Gateway Plug-inを使用する必要はありません。
      - SSL仮想プライベートネットワーク（VPN）トンネルを介して内部ネットワーク上のストアおよびそのほかのすべてのリソースへのアクセスを提供するには、［完全VPNトンネル］を選択します。この場合、ユーザーはVPNトンネルを確立するためのNetScaler Gateway Plug-inを使用する必要があります。

    ストアへのリモートアクセスを有効にすると、認証方法としてNetScaler Gatewayからのパススルーが自動的に有効になります。ユーザーはNetScaler Gatewayにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。
13. リモートアクセスを有効にした場合は、次の手順に進んでNetScaler Gatewayの展開環境を指定します。ユーザーはこの展開環境を介してストアにアクセスできます。リモートアクセスを有効にしない場合は、［リモートアクセス］ページで［作成］をクリックします。ストアが作成されたら、［完了］をクリックします。

前の手順で作成したストアにNetScaler Gatewayを介したリモートアクセスを構成するには、次の手順に従います。上記の手順が完了していることを前提としています。

1. **［ストアの作成］**ウィザードの**［リモートアクセス］**ページで、ユーザーがストアにアクセスする時に使用するゲートウェイ環境を、**［NetScaler Gatewayアプライアンス］**一覧で選択します。この一覧には、ほかのストアの作成時に追加したゲートウェイ環境が表示されます。一覧にゲートウェイ環境を追加する場合は、［追加］をクリックします。追加しない場合は、手順26.に進みます。
2. **［NetScaler Gatewayアプライアンスの追加］の［全般設定］**ページで、NetScaler Gateway展開環境にわかりやすい名前を指定します。
   ここで指定する表示名がユーザーのCitrix Receiverに表示されます。そのため、ユーザーが使用するNetScaler Gatewayを判断しやすいように、名前に関連情報を含める必要があります。たとえば、ユーザーが自分のいる場所に最も便利なNetScaler Gatewayを簡単に特定できるように、表示名に地理情報を含めることができます。
3. 展開環境の仮想サーバーまたはユーザーログオンポイントのURLを入力します。展開環境で使用する製品のバージョンを指定します。
   StoreFront展開環境のFQDN（Fully Qualified Domain Name：完全修飾ドメイン名）は一意で、NetScaler Gateway仮想サーバーのFQDNと異なるものである必要があります。StoreFrontとNetScaler Gateway仮想サーバーに同じFQDNを使用することはサポートされていません。

4. 使用可能なオプションから、NetScaler Gatewayの使用法を選択します。
   +認証およびHDXルーティング：NetScaler Gatewayが認証とHDXセッションのルーティングの両方に使用されます。
   +認証のみ：NetScaler Gatewayが認証に使用されますが、HDXセッションのルーティングには使用されません。
   +HDXルーティングのみ：NetScaler GatewayがHDXセッションのルーティングに使用されますが、認証には使用されません。
5. ［Secure Ticket Authority（STA）］ページで、XenDesktopまたはXenAppが提供するリソースをストアで使用できるようにするには、STAを実行しているサーバーの［Secure Ticket Authority］ページのURLをすべて一覧に追加します。一覧に複数のSTAのURLを追加すると、その順番に基づいてフェールオーバーされます。

   STAは、XenDesktopおよびXenAppサーバーでホストされ、接続要求に応答してセッションチケットを発行します。セッションチケットは、XenDesktopおよびXenAppリソースへのアクセスを認証および承認するための基本機能です。
6. 負荷分散するSecure Ticket Authorityを選択して設定します。応答しないSTAをバイパスするまでの間隔を指定することもできます。
7. Citrix Receiverが自動的に再接続を実行する間に、切断したセッションをXenDesktopおよびXenAppで開いたままにするには、**［セッション画面の保持を有効にする］**チェックボックスをオンにします。複数のSTAを構成した環境でセッション画面の保持機能を常に使用できるようにするには、**［可能な場合は2つのSTAにチケットを要求する］**チェックボックスをオンにします。セッションの途中で1つのSTAが使用できなくなってもユーザーセッションが中断されないように、StoreFrontにより2つの異なるSTAからセッションチケットが取得されます。StoreFrontがどちらのSTAにもアクセスできない場合は、単一のSTAを使用するようにフォールバックされます。
8. ［認証設定］ページで、構成するNetScaler Gatewayのバージョンを選択します。
9. 必要に応じてNetScaler Gatewayアプライアンスの仮想サーバーのIPアドレスを指定します。仮想サーバーのIPアドレスは、Access Gateway 9.xアプライアンスの場合は必須ですが、それより後の製品バージョンではオプションです。この仮想サーバーのIPアドレスは、NetScaler Gatewayで内部ネットワークのサーバーと通信するときに、ユーザーデバイスを表すために使用するIPアドレスです。このアドレスは、NetScaler GatewayアプライアンスのマップされたIPアドレスである場合もあります。StoreFrontは、仮想サーバーのIPアドレスを使用して、受信要求が信頼されているデバイスから発信されているかどうかを検証します。
10. ［ログオンの種類］の一覧から、Citrix Receiverユーザー向けにアプライアンス上で構成した認証方法を選択します。NetScaler Gatewayアプライアンスに関する構成情報は、ストアのプロビジョニングファイルに追加されます。これにより、Citrix Receiverは、アプライアンスへの初回接続時に適切な接続要求を送信できるようになります。

    - ユーザーのMicrosoft Active Directoryドメインの資格情報を入力させる場合は、［ドメイン］を選択します。
    - セキュリティトークンから取得するトークンコードを入力させる場合は、［セキュリティトークン］を選択します。
    - ユーザーのドメイン資格情報とセキュリティトークンから取得するトークンコードの両方を入力させる場合は、［ドメインおよびセキュリティトークン］を選択します。
    - テキストメッセージで送信されるワンタイムパスワードを入力させる場合は、［SMS認証］を選択します。
    - スマートカードを挿入してPINを入力させる場合は、［スマートカード］を選択します。

    スマートカードでの認証に問題が生じた場合に代替の認証方法を使用できるようにするには、［スマートカードフォールバック］の一覧から代替の認証方法を選択します。

11. ［コールバックURL］ボックスに、NetScaler Gateway認証サービスのURLを入力します。これはオプションのフィールドです。URLの標準的な部分は自動的に補完されます。アプライアンスの内部URLを入力します。StoreFrontはNetScaler Gateway認証サービスに接続して、NetScaler Gatewayからの要求の送信元がそのアプライアンスであることを確認します。
12. ［作成］をクリックします。これにより、［リモートアクセス］ページの一覧にNetScaler Gatewayの展開環境が追加されます。必要に応じて手順1.～11.を繰り返し、［NetScaler Gatewayアプライアンス］の一覧にNetScaler Gatewayの展開環境を追加します。一覧で複数のエントリを選択して複数のゲートウェイ環境を介したアクセスを有効にする場合は、デフォルトで使用されるアプライアンスを選択します。
13. ［リモートアクセス］ページで［作成］をクリックします。ストアが作成されたら、［完了］をクリックします。

ストアが作成されました。ただし、Citrix Receiver側でもストアに接続するための詳細を構成する必要があります。ユーザーによるReceiverの構成プロセスを簡単にするために、いくつかの方法が用意されています。詳しくは、「ユーザーアクセスオプション」を参照してください。

また、Receiver for Webサイトを使用すると、ユーザーがWebページからデスクトップやアプリケーションにアクセスできるようになります。新しいストアにアクセスするためのReceiver for WebサイトのURLは、ストアを作成するときに表示されます。

デフォルトでは、新しいストアを作成するときに、XenApp ServicesサイトのURLが有効になります。ドメインに参加しているデスクトップアプライアンスのユーザー、Citrix Desktop Lockを実行している再目的化されたPCのユーザー、およびアップグレードできない古いバージョンのCitrixクライアントのユーザーは、XenApp Servicesサイトから直接そのストアに接続できます。XenApp ServicesサイトのURLは、http[s]:///Citrix//PNAgent/config.xmlの形式です。ここで、はStoreFront展開環境のサーバーまたは負荷分散環境の完全修飾ドメイン名で、は上記手順3.で指定した名前です。

ドメイン不参加サーバー上の単一のサーバー展開環境へのストアの作成

1. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、 **[操作]** ペインの **[ストアの作成]** をクリックします。
3. **[ストア名]** ページで、ストアの名前を指定して、 **[次へ]** をクリックします。
   ストアの名前はCitrix Receiverでユーザーアカウントの下に表示されるため、ユーザーにとってわかりやすい名前を指定してください。

4. **[Delivery Controller]** ページでは、リソースを提供するインフラストラクチャを一覧に追加します。**[Add]** をクリックします。
5. **[Delivery Controllerの追加]** ダイアログボックスで、この展開環境に対するわかりやすい名前を指定し、リソースを提供するインフラストラクチャの種類（［XenDesktop］、［XenApp］、または［AppController］）を選択します。App Controllerを選択する場合は、表示名として入力した文字列にスペースが含まれていないことを確認してください。
6. インフラストラクチャの種類としてXenDesktopまたはXenAppサーバーを選択した場合は、手順7.に進みます。App Controllerにより管理されるアプリケーションをストアで使用できるようにするには、App Controller仮想アプライアンスの名前またはIPアドレスを［サーバー］ボックスに入力し、App Controllerへの接続に使用するStoreFrontのポートを指定します。デフォルトのTCPポートは443です。手順10.に進みます。
7. リソースを提供するインフラストラクチャの種類としてXenDesktopまたはXenAppを選択した場合は、サーバーの名前またはIPアドレスを **[サーバー]** ボックスに追加します。XenDesktopサイトの場合は、Delivery Controllerの詳細を指定します。XenAppファームの場合は、Citrix XML Serviceを実行しているサーバーを一覧に追加します。
8. **[トランスポートの種類]** ボックスの一覧から、StoreFrontでサーバーとの通信に使用する接続の種類を選択します。
   - 暗号化されていない接続でデータを送信するには［HTTP］を選択します。このオプションを選択する場合は、StoreFrontとサーバー間の接続を何らかの方法で保護することを検討してください。
   - SSL（Secure Sockets Layer）またはTLS（Transport Layer Security）を使用する保護されたHTTP接続でデータを送信するには、［HTTPS］を選択します。XenDesktopまたはXenAppサーバーに対してこのオプションを選択する場合は、Citrix XML ServiceがポートをIIS（Microsoftインターネットインフォメーションサービス）と共有する設定になっていることと、IISがHTTPSをサポートするように構成されていることを確認してください。
   - XenAppサーバーとの通信でSSL Relayによるホスト認証とデータの暗号化を実行するには、［SSL Relay］を選択します。

     注：StoreFrontとサーバーの間の通信でHTTPSまたはSSL Relayを使用する場合は、 **[サーバー]** ボックスに指定したサーバー名がそのサーバーの証明書のサーバー名と一致することを確認してください（大文字/小文字は区別されます）。

9. StoreFrontがサーバーに接続するときに使用するポートを指定します。デフォルトでは、HTTP接続およびSSL Relay接続では80、HTTPS接続では443が使用されます。XenDesktopおよびXenAppサーバーの場合、Citrix XML Serviceで使用されるポート番号を指定する必要があります。
10. StoreFrontとXenAppサーバーの間の接続をSSL Relayで保護する場合は、SSL RelayのTCPポートを［SSL Relayポート］ボックスで指定します。デフォルトのTCPポートは443です。SSL Relayを実行するすべてのサーバーで同じポートが構成されていることを確認してください。
11. **［OK］**をクリックします。XenDesktop、XenApp、およびApp Controllerの展開環境を自由に組み合わせてストアを作成できます。必要に応じて手順4.～12.を繰り返し、ストアにリソースを提供する展開環境を一覧に追加します。必要なリソースをすべてストアに追加したら、［次へ］をクリックします。
12. **［リモートアクセス］**ページでは、公共のネットワーク上のユーザーにNetScaler Gatewayを介したアクセス（リモートアクセス）を提供するかどうか、およびその方法を指定します。
    - 公共のネットワーク上のユーザーにストアへのアクセスを禁止するには、**［なし］**を選択します。これにより、内部ネットワークのローカルユーザーのみがストアにアクセスできるようになります。
    - NetScaler Gateway経由でアクセスするユーザーにストアのリソースのみを提供するには、**［VPNトンネルなし］**を選択します。この場合、ユーザーはNetScaler Gatewayに直接ログオンするため、NetScaler Gateway Plug-inを使用する必要はありません。
    - SSL仮想プライベートネットワーク（VPN）トンネルを介して内部ネットワーク上のストアおよびそのほかのすべてのリソースへのアクセスを提供するには、**［完全VPNトンネル］**を選択します。この場合、ユーザーはVPNトンネルを確立するためのNetScaler Gateway Plug-inを使用する必要があります。

      ストアへのリモートアクセスを有効にすると、認証方法としてNetScaler Gatewayからのパススルーが自動的に有効になります。ユーザーはNetScaler Gatewayにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。
13. リモートアクセスを有効にした場合は、「NetScaler Gatewayを介したストアへのリモートアクセスを有効にする」に進んでNetScaler Gatewayの展開環境を指定します。ユーザーはこの展開環境を介してストアにアクセスできます。リモートアクセスを有効にしない場合は、**［リモートアクセス］**ページで**［次へ］**をクリックします。
14. **［認証方法の構成］**ページで、ユーザーが認証とリソースへのアクセスに使用する方法を選択し、**［次へ］**をクリックします。
15. **［パスワード検証の構成］**ページで、パスワード検証を行うDelivery Controllerを選択して、**［次へ］**をクリックします。
16. **［XenApp Services URL］**ページで、PNAgentを使用してアプリケーションおよびデスクトップにアクセスするユーザーのURLを構成し、**［作成］**をクリックします。

左側の**［サーバーグループノード］**ペインと**［アクション］**ペインが、**［ベースURLの変更］**に置き換わります。ドメインに参加していないサーバーではサーバーグループを利用できないため、使用できる唯一のオプションは、ベースURLを変更することです。

ストアの削除

ストアを削除するには、［ストアの削除］タスクを使用します。ストアを削除すると、関連付けられているReceiver for Webサイト、デスクトップアプライアンスサイト、およびXenApp Servicesサイトもすべて削除されます。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

認証が不要なストアの作成

Aug 14, 2017

認証不要（匿名）ユーザーのアクセスをサポートする、認証が不要なストアを追加で構成するには、[ストアの作成] タスクを使用します。このストアは必要なだけ作成できます。たとえば、特定のユーザーグループ用にストアを作成したり、特定のリソースセットを集約するストアを作成したりできます。

認証不要なストアでは、NetScaler Gatewayを介したリモートアクセスは許可されません。

認証不要なストアを作成するには、そのストアのユーザーにリソースを提供するサーバーを指定して、その通信構成を行います。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、［操作］ペインの［ストアの作成］をクリックします。
3. ［ストア名］ページで、ストアの名前を指定して、**［このストアへのアクセスを非認証 (匿名) ユーザーにのみ許可する］**を選択し、［次へ］をクリックします。
   ストアの名前はCitrix Receiverでユーザーアカウントの下に表示されるため、ユーザーにとってわかりやすい名前を指定してください。
4. **［Delivery** Controller］ページでは、リソースを提供するインフラストラクチャを一覧に追加します。［Add］をクリックします。
5. ［Delivery Controllerの追加］ダイアログボックスで、この展開環境に対するわかりやすい名前を指定し、ストアで使用できるようにするリソースが［XenApp］または［AppController］で提供されるかどうかを指定します。XenMobile（App Controller）を選択する場合は、表示名として入力した文字列にスペースが含まれていないことを確認してください。Controllerを追加するときは、匿名アプリ機能をサポートしていることを確認してください。匿名アプリ機能をサポートしないControllerで認証不要なストアを構成すると、ストアから匿名アプリを使用できなくなります。
6. XenAppサーバーの詳細を追加している場合は、手順7.に進みます。App Controllerにより管理されるアプリケーションをストアで使用できるようにするには、XenMobile（App Controller）仮想アプライアンスの名前またはXenMobile（App Controller）アドレスを［サーバー］ボックスに入力し、XenMobile（App Controller）への接続に使用するIPのポートを指定します。デフォルトのTCPポートは443です。手順10.に進みます。
7. リソースを提供するインフラストラクチャの種類としてXenAppを選択した場合は、サーバーの名前またはIPアドレスを［サーバー］一覧に追加します。この一覧に複数のサーバーを追加すると、その順番に基づいてフェールオーバーされます。XenDesktopサイトの場合は、Controllerの詳細を指定します。XenAppファームの場合は、Citrix XML Serviceを実行しているサーバーを一覧に追加します。
8. ［トランスポートの種類］ボックスの一覧から、StoreFrontでサーバーとの通信に使用する接続の種類を選択します。
   - 暗号化されていない接続でデータを送信するには［HTTP］を選択します。このオプションを選択する場合は、StoreFrontとサーバー間の接続を何らかの方法で保護することを検討してください。
   - SSL（Secure Sockets Layer）またはTLS（Transport Layer Security）を使用する保護されたHTTP接続でデータを送信するには、［HTTPS］を選択します。XenDesktopまたはXenAppサーバーに対してこのオプションを選択する場合は、Citrix XML ServiceがポートをIIS（Microsoftインターネットインフォメーションサービス）と共有する設定になっていることと、IISがHTTPSをサポートするように構成されていることを確認してください。

   注：StoreFrontとサーバーの間の通信をHTTPSで保護する場合は、［サーバー］ボックスの一覧に指定したサーバー名が

そのサーバーの証明書のサーバー名と一致することを確認してください（大文字/小文字は区別されます）。

9. StoreFrontがサーバーに接続するときに使用するポートを指定します。デフォルトでは、HTTP接続では80、HTTPS接続では443が使用されます。XenDesktopおよびXenAppサーバーの場合、Citrix XML Serviceで使用されるポート番号を指定する必要があります。
10. ［OK］をクリックします。XenDesktop、XenApp、およびApp Controllerの展開環境を自由に組み合わせてストアを作成できます。必要に応じて手順4.～12.を繰り返し、ストアにリソースを提供する展開環境を一覧に追加します。必要なリソースをすべてストアに追加したら、［作成］をクリックします。

これで認証不要なストアが作成されました。このストアにユーザーがアクセスできるようにするには、Citrix Receiverでアクセス情報を構成する必要があります。ユーザーによるReceiverの構成プロセスを簡単にするために、いくつかの方法が用意されています。詳しくは、「ユーザーアクセスオプション」を参照してください。
また、Receiver for Webサイトを使用すると、ユーザーがWebページからデスクトップやアプリケーションにアクセスできるようになります。認証が不要なストアのデフォルトでは、Receiver for Webにアプリケーションがフォルダー階層で表示されるようになり、フォルダーパスの情報も表示されます。新しいストアにアクセスするためのReceiver for WebサイトのURLは、ストアを作成するときに表示されます。

デフォルトでは、新しいストアを作成するときに、XenApp ServicesサイトのURLが有効になります。ドメインに参加していないデスクトップアプライアンスのユーザー、Citrix Desktop Lockを実行している再目的化されたPCのユーザー、およびアップグレードできない古いバージョンのCitrixクライアントのユーザーは、XenApp Servicesサイトから直接そのストアに接続できます。XenApp Services URLの形式は、http[s]://serveraddress/Citrix/storename/PNAgent/config.xmlの形式です。ここで、serveraddressはStoreFront展開環境のサーバーまたは負荷分散環境の完全修飾ドメイン名で、storenameは上記手順3で指定した名前です。

注：web.configファイルでパラメーター LogoffAction=”terminate"を構成しても、認証不要なストアにアクセスするCitirx Receiver for Webセッションは終了しません。このweb.configファイルは、通常C:\inetpub\wwwroot\Citrix\storename\フォルダーにあります（storenameはストア作成時に指定したストア名）。これらのセッションが正しく終了するようにするには、ストアのXenAppサーバーで［XML要求を信頼する］オプションが有効になっている必要があります（XenAppおよびXenDesktopドキュメントの「*Citrix XML Serviceのポートと信頼を設定する*」を参照）。

ユーザー用のストアプロビジョニングファイルのエクスポート

Aug 14, 2017

ストアで使用されるNetScaler Gateway環境やビーコンポイントなどの詳細情報が定義されたプロビジョニングファイルを生成するには、［複数ストアのプロビジョニングファイルのエクスポート］および［プロビジョニングファイルのエクスポート］タスクを使用します。ユーザーにプロビジョニングを提供すると、ユーザーがCitrix Receiverを簡単に構成できるようになります。Citrix Receiverプロビジョニングファイルは、Receiver for Webサイトから入手できるようにすることもできます。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。Citrix StoreFront管理コンソールの左ペインで、［ストア］ノードを選択します。
2. 複数のストアの詳細情報が定義されたプロビジョニングファイルを生成するには、［操作］ペインの［複数ストアのプロビジョニングファイルのエクスポート］をクリックして、対象のサイトを選択します。
3. ［エクスポート］をクリックして、拡張子が.crのプロビジョニングファイルをネットワーク上の適切な場所に保存します。

ユーザーに対するストアの非表示および提供

Aug 14, 2017

ユーザーがメールアドレスによるアカウント検出機能または完全修飾ドメイン名（FQDN）を使ってCitrix Receiverを構成する場合、特定のストアがユーザーのアカウントに追加されないように、そのストアを非表示に設定できます。これを行うには、［ストアを表示しない］タスクを使用します。新規に作成するストアのデフォルトでは、ユーザーがCitrix ReceiverでStoreFrontストアを追加するときに、オプションとしてそのストアが表示されます。ストアを非表示にしても、ユーザーがストアにアクセスできなくなるわけではありません。ユーザーは、メールアドレスによるアカウント検出機能の代わりにCitrix Receiverでのストア接続を手作業で構成したり、セットアップURLやプロビジョニングファイルを使用したりする必要があります。ストアの非表示状態を解除するには、［ストアのアドバタイズ］タスクを使用します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、［操作］ペインで［ストア設定の構成］>［ストアのアドバタイズ］の順にクリックします。
3. ［ストアのアドバタイズ］ページで［ストアのアドバタイズ］または［ストアの非表示］を選択します。

ストアに表示するリソースの管理

Aug 14, 2017

XenDesktop、XenApp、およびApp Controllerによって提供されたストアリソースから追加または削除したり、これらのリソースを提供するサーバーの詳細を変更したりするには、［Controllerの管理］タスクを使用します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、結果ペインでストアを選択します。［操作］ペインの［Delivery Controllerの管理］をクリックします。
3. ストアにデスクトップやアプリケーションを提供するXenDesktop、XenApp、またはApp Controller展開環境を追加するには、［Delivery Controllerの管理］ダイアログボックスで［追加］をクリックします。展開環境の設定を変更するには、［Delivery Controller］ボックスの一覧でエントリを選択して［編集］をクリックします。展開環境により提供されるリソースをストアから削除するには、ボックスの一覧でエントリを選択して［削除］をクリックします。
4. ［Controllerの追加］または［Controllerの編集］ダイアログボックスで、この展開環境に対するわかりやすい名前を指定し、リソースを提供するインフラストラクチャの種類（［XenDesktop］、［XenApp］、または［AppController］）を選択します。App Controllerを選択する場合は、表示名として入力した文字列にスペースが含まれていないことを確認してください。
5. インフラストラクチャの種類としてXenDesktopまたはXenAppサーバーを選択した場合は、手順7.に進みます。App Controllerにより管理されるアプリケーションをストアで使用できるようにするには、App Controller仮想アプライアンスの名前またはIPアドレスを［サーバー］ボックスに入力し、App Controllerへの接続に使用するStoreFrontのポートを指定します。デフォルトのTCPポートは443です。手順10.に進みます。
6. XenDesktopまたはXenAppが提供するデスクトップやアプリケーションをストアに追加するには、［追加］をクリックしてサーバーの名前またはIPアドレスを入力します。複数のサーバーを指定すると、web.configファイルの構成に基づいて負荷分散またはフェールオーバーが有効になります。デフォルトでは、負荷分散が構成されています。フェールオーバーを構成すると、サーバーの一覧の順番に基づいてフェールオーバーされます。XenDesktopサイトの場合は、Delivery Controllerの詳細を指定します。XenAppファームの場合は、Citrix XML Serviceを実行しているサーバーを一覧に追加します。サーバーの名前またはIPアドレスを変更するには、［サーバー］ボックスの一覧でエントリを選択して［編集］をクリックします。一覧からエントリを削除するには、そのエントリを選択して［削除］をクリックします。これにより、そのサーバーからのリソースがストアに列挙されなくなります。
7. ［トランスポートの種類］ボックスの一覧から、StoreFrontでサーバーとの通信に使用する接続の種類を選択します。
   - 暗号化されていない接続でデータを送信するには［HTTP］を選択します。このオプションを選択する場合は、StoreFrontとサーバー間の接続を何らかの方法で保護することを検討してください。
   - SSL（Secure Sockets Layer）またはTLS（Transport Layer Security）を使用する保護されたHTTP接続でデータを送信するには、［HTTPS］を選択します。XenDesktopまたはXenAppサーバーに対してこのオプションを選択する場合は、Citrix XML ServiceがポートをIIS（Microsoftインターネットインフォメーションサービス）と共有する設定になっていることと、IISがHTTPSをサポートするように構成されていることを確認してください。
   - XenAppサーバーとの通信でSSL Relayによるホスト認証とデータの暗号化を実行するには、［SSL Relay］を選択します。

   注：StoreFrontとサーバーの間の通信でHTTPSまたはSSL Relayを使用する場合は、［サーバー］ボックスの一覧に指定したサーバー名がそのサーバーの証明書のサーバー名と一致することを確認してください（大文字/小文字は区別されます）。
8. StoreFrontがサーバーに接続するときに使用するポートを指定します。デフォルトでは、HTTP接続およびSSL Relay接続では80、HTTPS接続では443が使用されます。XenDesktopおよびXenAppサーバーの場合、Citrix XML Serviceで使用され

るポート番号を指定する必要があります。

9. StoreFrontとXenAppサーバーの間の接続をSSL Relayで保護する場合は、SSL RelayのTCPポートを［SSL Relayポート］ボックスで指定します。デフォルトのTCPポートは443です。SSL Relayを実行するすべてのサーバーで同じポートが構成されていることを確認してください。
10. ［OK］をクリックします。XenDesktop、XenApp、およびApp Controllerの展開環境を自由に組み合わせてストアを作成できます。必要に応じて手順3.～10.を繰り返し、［Delivery Controller］の一覧にほかの展開環境を追加したり既存のエントリを変更したりします。

NetScaler Gatewayを介したストアへのリモートアクセスの管理

Aug 14, 2017

公共のネットワークから接続するユーザーに対してNetScaler Gatewayを介したストアへのアクセスを構成するには、[リモートアクセス設定]タスクを使用します。認証不要なストアでは、NetScaler Gatewayを介したリモートアクセスは許可されません。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、結果ペインでストアを選択します。［操作］ペインで［リモートアクセス設定の**構成**］**をクリックします。**
3. ［リモートアクセス設定の**構成**］ダイアログボックスでは、公共のネットワーク上のユーザーにNetScaler Gatewayを介したアクセスを提供するかどうか、およびその方法を指定します。
   - 公共のネットワーク上でストアをユーザーが使用できないようにするには、**[リモートアクセスの有効化]** チェックボックスをオフにします。これにより、内部ネットワークのローカルユーザーのみがストアにアクセスできるようになります。
   - リモートアクセスを有効にするには、**[リモートアクセスの有効化]** をオンにします。
     - NetScaler Gateway経由でアクセスするユーザーにストアのリソースのみを提供するには、[VPNトンネルなし]を選択します。この場合、ユーザーはNetScaler Gatewayに直接ログオンするため、NetScaler Gateway Plug-inを使用する必要はありません。
     - SSL（Secure Sockets Layer）仮想プライベートネットワーク（VPN）トンネルを介して内部ネットワーク上のストアやほかのリソースへのアクセスを提供するには、［完全VPNトンネル］を選択します。この場合、ユーザーはVPNトンネルを確立するためのNetScaler Gateway Plug-inを使用する必要があります。

   ストアへのリモートアクセスを有効にすると、認証方法としてNetScaler Gatewayからのパススルーが自動的に有効になります。ユーザーはNetScaler Gatewayにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。

4. リモートアクセスを有効にした場合は、ユーザーがストアにアクセスするときに使用する展開環境を[NetScaler Gatewayアプライアンス]一覧から選択します。この一覧には、このストアやほかのストアの作成時に追加したゲートウェイ環境が表示されます。一覧にゲートウェイ環境を追加する場合は、［追加］をクリックします。追加しない場合は、手順26.に進みます。
5. ［全般設定］ページで、NetScaler Gateway展開環境にわかりやすい名前を指定します。
   ここで指定する表示名がユーザーのCitrix Receiverに表示されます。そのため、ユーザーが使用するNetScaler Gatewayを判断しやすいように、名前に関連情報を含める必要があります。たとえば、ユーザーが自分のいる場所に最も便利なNetScaler Gatewayを簡単に特定できるように、表示名に地理情報を含めることができます。
6. 展開環境の仮想サーバーまたはユーザーログオンポイント（Access Gateway 5.0の場合）のURLを入力します。展開環境で使用する製品のバージョンを指定します。
   StoreFront展開環境のFQDN（Fully Qualified Domain Name：完全修飾ドメイン名）は一意で、NetScaler Gateway仮想サーバーのFQDNと異なるものである必要があります。StoreFrontとNetScaler Gateway仮想サーバーに同じFQDNを使用することはサポートされていません。
7. 展開環境でAccess Gateway 5.0が実行されている場合は、手順9.に進みます。それ以外の場合は、必要に応じてNetScaler

GatewayアプライアンスのサブネットIPアドレスを指定します。サブネットIPアドレスは、Access Gateway 9.3アプライアンスの場合は必須ですが、それより後の製品バージョンではオプションです。
このサブネットアドレスは、NetScaler Gatewayで内部ネットワークのサーバーと通信するときに、ユーザーデバイスを表すために使用するIPアドレスです。このアドレスは、NetScaler GatewayアプライアンスのマップされたIPアドレスである場合もあります。StoreFrontは、サブネットIPアドレスを使用して、受信要求が信頼されているデバイスから発信されているかどうかを検証します。

8. NetScaler Gateway 11、NetScaler Gateway 10.1、Access Gateway 10、またはAccess Gateway 9.3のアプライアンスを追加する場合は、［ログオンの種類］の一覧から、Citrix Receiverユーザー用にアプライアンスで構成した認証方法を選択します。
   NetScaler Gatewayアプライアンスに関する構成情報は、ストアのプロビジョニングファイルに追加されます。これにより、Citrix Receiverは、アプライアンスへの初回接続時に適切な接続要求を送信できるようになります。

   - ユーザーのMicrosoft Active Directoryドメインの資格情報を入力させる場合は、［ドメイン］を選択します。
   - セキュリティトークンから取得するトークンコードを入力させる場合は、［セキュリティトークン］を選択します。
   - ユーザーのドメイン資格情報とセキュリティトークンから取得するトークンコードの両方を入力させる場合は、［ドメインおよびセキュリティトークン］を選択します。
   - テキストメッセージで送信されるワンタイムパスワードを入力させる場合は、［SMS認証］を選択します。
   - スマートカードを挿入してPINを入力させる場合は、［スマートカード］を選択します。

   スマートカードでの認証に問題が生じた場合に代替の認証方法を使用できるようにするには、［スマートカードフォールバック］の一覧から代替の認証方法を選択します。手順10.に進みます。

9. Access Gateway 5.0のアプライアンスを追加する場合は、ユーザーのログオンポイントのホスト（スタンドアロンのアプライアンスまたはクラスターの一部であるAccess Controllerサーバー）を指定します。クラスターを追加する場合は、［次へ］をクリックして手順11.に進みます。
10. NetScaler Gateway 11、NetScaler Gateway 10.1、Access Gateway 10、Access Gateway 9.3、またはスタンドアロンAccess Gateway 5.0アプライアンスを追加する場合は、［コールバックURL］ボックスにNetScaler Gateway認証サービスのURLを入力します。URLの標準的な部分は自動的に補完されます。［次へ］をクリックして手順13.に進みます。
    アプライアンスの内部URLを入力します。StoreFrontはNetScaler Gateway認証サービスに接続して、NetScaler Gatewayからの要求の送信元がそのアプライアンスであることを確認します。

11. StoreFrontにAccess Gateway 5.0クラスターを追加する場合は、［アプライアンス］ページでクラスター内のアプライアンスのIPアドレスまたはFQDNを一覧に追加して、［次へ］をクリックします。
12. ［サイレント認証を有効にする］ページで、Access Controllerサーバーで実行されている認証サービスのURLを一覧に追加します。一覧に複数のサーバーのURLを追加すると、その順番に基づいてフェールオーバーされます。［Next］をクリックします。
    StoreFrontでは認証サービスを使用してリモートユーザーが認証されるため、リモートユーザーがストアにアクセスするときに資格情報を再入力する必要はありません。

13. すべての展開環境で、XenDesktopまたはXenAppが提供するリソースをストアで使用できるようにするには、［Secure Ticket Authority（STA）］ページで、STAを実行しているサーバーのURLを一覧に追加します。一覧に複数のSTAのURLを追加すると、その順番に基づいてフェールオーバーされます。
    STAは、XenDesktopおよびXenAppサーバーでホストされ、接続要求に応答してセッションチケットを発行します。セッションチケットは、XenDesktopおよびXenAppリソースへのアクセスを認証および承認するための基本機能です。

14. Citrix Receiverが自動的に再接続を実行する間に、切断したセッションをXenDesktopおよびXenAppで開いたままにするには、［セッション画面の保持を有効にする］チェックボックスをオンにします。複数のSTAを構成した環境でセッション画面の保持機能を常に使用できるようにするには、［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにします。

［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにすると、セッションの途中で1つのSTAが使用できなくなってもユーザーセッションが中断されないように、StoreFrontにより2つの異なるSTAからセッションチケットが取得されます。StoreFrontがどちらのSTAにもアクセスできない場合は、単一のSTAを使用するようにフォールバックされます。

15. ［作成］をクリックします。これにより、［リモートアクセス設定］ダイアログボックスの一覧にNetScaler Gatewayの展開環境が追加されます。
16. 必要に応じて手順4.～15.を繰り返し、［NetScaler Gatewayアプライアンス］の一覧にNetScaler Gatewayの展開環境を追加します。一覧で複数のエントリを選択して複数のゲートウェイ環境を介したアクセスを有効にする場合は、デフォルトで使用されるアプライアンスを選択します。

Citrix Onlineアプリケーションをストアに統合する

Aug 14, 2017

> ## 注意
>
> 3.12からは、StoreFront管理コンソールでこの機能を構成することはできません。StoreFront 3.12へのアップグレードでは、引き続きこの機能を使用できます。構成を変更するには、PowerShellコマンドレットのUpdate-DSGenericApplicationsを使用します。
>
> 以前のバージョンのStoreFront管理コンソールでこの機能を構成する方法について詳しくは、StoreFront 3.11の記事の「Citrix Onlineの統合」を参照してください。

名前
Update-DSGenericApplications

概要
ストアサービスの一般的なアプリケーション設定を更新します。

構文

Update-DSGenericApplications [[-StoreServiceSiteId]] [[-StoreServiceVirtualPath]] [[-GoToMeetingEnabled]] [[-GoToMeetingDeliveryOption]] [[-GoToWebinarEnabled]] [[-GoToWebinarDeliveryOption]] [[-GoToTrainingEnabled]] [[-GoToTrainingDeliveryOption]] []

説明

ストアサービスの一般的な（Citrix Online）機能を更新するために使用されるコマンドレット。

共通のサブスクリプションデータストアを共有する2つのStoreFrontストアの構成

Aug 14, 2017

StoreFront Version 2.0以降では、サブスクリプションデータの管理にSQLデータベースを使用することはなくなりました。SQLデータベースはWindowsデータストアに置き替えられています。このデータストアは、StoreFrontを初めてインストールするときに追加の構成が必要ありません。このWindowsデータストアは、各StoreFrontサーバーにローカルにインストールされます。StoreFrontサーバーグループ環境では、各サーバーで、そのデータストアが使用するサブスクリプションデータのコピーも管理されます。このデータは、ほかのサーバーに反映され、グループ全体でユーザーのサブスクリプションが管理されます。デフォルトでは、StoreFrontは各ストアに対して1つのデータストアを作成します。各サブスクリプションデータストアは、ストアごとに独立して更新されます。

異なる構成設定が必要な場合、一般的には、管理者が2つの異なるストアでStoreFrontを構成します。ストアの1つはNetScaler Gatewayを使用してリソースに外部アクセスするため、もう1つは会社のLANを使用して内部アクセスするために設定します。ストア用web.configファイルに簡単な変更を加えることで、共通のサブスクリプションデータストアを共有するように、「外部」ストアと「内部」ストアの両方を構成できます。

2つのストアとそれらのサブスクリプションデータストアを使用するデフォルトのシナリオでは、ユーザーが同じリソースを2回サブスクライブする必要があります。共通のサブスクリプションデータベースを共有するように2つのストアを構成すると、ユーザーが同じリソースに会社のネットワーク内外から簡単にアクセスできるようになり、ローミングエクスペリエンスが向上します。共有サブスクリプションデータストアを使用すると、新しいリソースを最初にサブスクライブするときに、ユーザーが「外部」ストアを使用しているのか「内部」ストアを使用しているのかは問題になりません。

- 各ストアのweb.configファイルはC:\inetpub\wwwroot\citrix\<storename>にあります。
- 各ストアのweb.configには、Subscription Store Serviceのクライアントエンドポイントが含まれています。

StoreName>" authenticationMode="windows" transferMode="Streamed">
各ストアのサブスクリプションデータは次の場所にあります。

C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>
2つのストアでサブスクリプションデータストアを共有するには、一方のストアが、もう一方のストアのサブスクリプションサービスエンドポイントを参照するように設定します。サーバーグループ展開環境では、すべてのサーバーが、定義された同一の組み合わせのストアと、これらの両ストアが共有する共有データストアの同一のコピーを持ちます。

注：各ストアのXenApp、XenDesktop、およびApp Controllerの構成は一致している必要があります。構成が一致していない場合、各ストアでのリソースのサブスクリプションが一貫しなくなることがあります。データストアの共有は、2つのストアが同じStoreFrontサーバーまたはサーバーグループ展開環境に存在する場合にのみサポートされます。

StoreFrontサブスクリプションデータストアのエンドポイント

1. 単一StoreFront展開環境では、メモ帳を使用して外部ストアのweb.configファイルを開き、clientEndpointを検索します。
   例：
   External" authenticationMode="windows" transferMode="Streamed">
2. 外部ストアエンドポイントを内部ストアエンドポイントと一致するように変更します。
   Internal" authenticationMode="windows" transferMode="Streamed">
3. StoreFrontサーバーグループを使用している場合は、プライマリノードのweb.configファイルに対する変更をほかのすべてのノードに反映させます。

両ストアが内部ストアのサブスクリプションデータストアを共有するように設定されました。

上級ストア設定

Aug 14, 2017

［ストア設定の構成］の［詳細な設定］ページを使って、詳細ストアのプロパティを構成できます。

アドレス解決の種類

フォントスムージングを許可する

セッションの再接続を許可する

特殊なフォルダーのリダイレクトを許可する

バックグラウンドヘルスチェックポーリング期間

通信のタイムアウト期間

接続タイムアウト

拡張列挙機能を有効にする

ソケットプール機能の有効化

リソースを除外キーワードでフィルターする

リソースを包含キーワードでフィルターする

リソースを種類でフィルターする

同時列挙の最大数

同時列挙の最小ファーム数

ICAクライアント名を上書きする

トークンの整合性を要求する

サーバー通信試行回数

古いクライアントでDesktop Viewerを表示する

> **Important**
>
> 複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択し、真ん中のペインでストアを選択して、［操作］

ペインで **[ストア設定の構成]** を選択します。

3. **[ストア設定の構成]** ページで **[詳細な設定]** を選択して、構成する詳細オプションを選択し、必要な変更を加えて［**OK**］をクリックします。

[詳細な設定] タスクを使って、サーバーからの要求のアドレスの種類を指定します。デフォルトは［DnsPort］です。**[詳細な設定]** の **[アドレス解決の種類]** ドロップダウンメニューから、以下のいずれかを選択します。

- DNS
- DnsPort
- IPV4
- IPV4Port
- ドット
- DotPort
- Uri
- 0 = 変更なし

HDXセッションでフォントスムージングを行うかどうかを指定できます。デフォルトは［On］です。

[詳細な設定] タスクを使用して、 **[フォントスムージングを許可する]** チェックボックスをチェックし、 **[OK]** をクリックします。

HDXセッションが再接続されるようにするかどうかを指定できます。デフォルトは［On］です。

[詳細な設定] タスクを使用して、 **[セッションの再接続を許可する]** チェックボックスをチェックし、 **[OK]** をクリックしてセッションの再接続を有効にします。

[詳細な設定] タスクを使ってユーザーフォルダーのリダイレクトを有効または無効にします。ユーザーフォルダーのリダイレクト機能により、サーバー上のWindowsの特殊フォルダーがローカルコンピューター上のフォルダーにマップされます。ユーザーフォルダーという用語は、［ドキュメント］、［デスクトップ］など、ユーザー固有のWindowsフォルダー（特殊フォルダー）を指すもので、Windowsのバージョンが異なっていても同様のフォルダーが存在します。

[詳細な設定] タスクを使用して、 **[特殊なフォルダーのリダイレクトを許可する]** チェックボックスをオンまたはオフにして特殊なフォルダーのリダイレクトを有効または無効にし、 **[OK]** をクリックします。

StoreFrontは、各XenDesktopブローカーやXenAppサーバー上で定期的にヘルスチェックを実行し、断続的なサーバー可用性のインパクトを減少させます。デフォルトは1分毎（00:01:00）です。［詳細な設定］タスクを使用して、 **[バックグラウンドヘルスチェックポーリング期間]** の時間を指定し、 **[OK]** をクリックしてヘルスチェックの頻度を制御します。

デフォルトでは、ストアにリソースを提供するサーバーへのStoreFrontからの要求は、30秒でタイムアウトします。通信の試行が1回失敗すると、サーバーが使用できないとみなされます。 **[詳細な設定]** タスクを使用して、デフォルトの時間に変

更を行い、 **[OK]** をクリックしてこれらの設定を変更します。

Delivery Controllerで最初の接続を確立するときに待機する秒数を指定できます。デフォルトは6です。

[詳細な設定] タスクを使用して、最初の接続を確立するときに待機する秒数を指定して **[OK]** をクリックします。

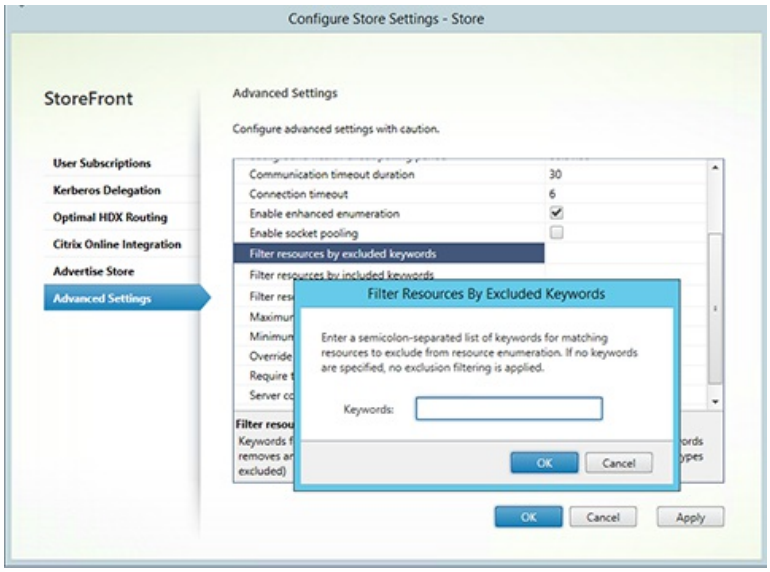
Delivery Controllerで、並列通信を有効（無効）にすることができます。デフォルトは［On］です。

[詳細な設定] タスクを使用して、 **[拡張列挙機能を有効にする]** チェックボックスをオン（オフ）にし、 **[OK]** をクリックします。

ストアのソケットプール機能はデフォルトでは無効になっています。ソケットプール機能を有効にすると、StoreFrontでソケットのプールが保持されます。これにより、必要になるたびにソケットを作成して接続が閉じたときにオペレーティングシステムに戻すという処理が不要になります。この機能を有効にすると、特にSSL（Secure Sockets Layer）接続でパフォーマンスが向上します。ソケットプール機能を有効にするには、ストアの構成ファイルを編集します。 **[詳細な設定]** タスクを使用し **[ソケットプール機能を有効にする]** チェックボックスをオンにして、 **[OK]** をクリックしてソケットプール機能を有効にします。

一致するリソースを、除外キーワードでフィルターできます。除外キーワードを指定すると、それまで構成されていた包含キーワードは削除されます。既定値：［フィルターなし］（どのリソースの種類も除外されません）。

[詳細な設定] タスクを使用して、 **[リソースを除外キーワードでフィルターする]** を選択し、その右側をクリックして、セミコロンで区切ったキーワードをキーワード入力用ボックスに入力してから **[OK]** をクリックします。



一致するリソースを、包含キーワードでフィルターできます。包含キーワードを指定すると、それまで構成されていた除外キーワードは削除されます。既定値：［フィルターなし］（どのリソースの種類も除外されません）。

[詳細な設定] タスクを使用して、 **[リソースを包含キーワードでフィルターする]** を選択し、その右側をクリックして、セミコロンで区切ったキーワードをキーワード入力用ボックスに入力してから **[OK]** をクリックします。

リソースの列挙に含めるリソースの種類を選択します。既定値：［フィルターなし］（すべてのリソースの種類が含まれます）。

[詳細な設定] タスクを使用して、 **[リソースを種類でフィルターする]** を選択し、その右側をクリックして、列挙に含めるリソースの種類を選択し、 **[OK]** をクリックします。

複数のDelivery Controllerに送信する同時要求の最大数を指定します。規定値は0（制限なし）です。

[詳細な設定] タスクを使用して、 **[同時列挙の最大数]** を選択し、 **[OK]** をクリックします。

並列で列挙を行うDelivery Controllerの最小数を指定します。デフォルトは、［3］です。

[詳細な設定] タスクを使用して、 **[同時列挙の最小ファーム数]** を選択し、数値を入力してから **[OK]** をクリックします。

.ica 起動ファイルのクライアント名設定を、Citrix Receiver for Webで生成されたIDで上書きします。無効にすると、Citrix Receiverによってクライアント名が指定されます。デフォルトは、［Off］です。

[詳細な設定] タスクを使用して、 **[ICAクライアント名を上書きする]** チェックボックスをオンにし、 **[OK]** をクリックします。

有効にすると、StoreFrontによって、認証に使用されるゲートウェイとストア全体のゲートウェイとの整合性が強制されます。これらの値に不整合がある場合、ユーザーは再認証を行う必要があります。Smart Accessではこのオプションを有効にする必要があります。デフォルトは［On］です。

[詳細な設定] タスクを使用して、 **[トークンの整合性を要求する]** チェックボックスをオンにし、 **[OK]** をクリックします。

Delivery Controllerが利用不可とマークされるまでの、Delivery Controllerとの通信を試行する回数を指定します。デフォルトは［1］です。

[詳細な設定] タスクを使用して、 **[サーバー通信試行回数]** を選択し、数値を入力して **[OK]** をクリックします。

ユーザーが古いクライアントからデスクトップにアクセスする際に、Citrix Desktop Viewerウィンドウおよびツールバーを表示するかどうかを指定します。デフォルトは、［Off］です。

[詳細な設定] タスクを使用して、 **[古いクライアントでDesktop Viewerを表示する]** チェックボックスをオンにし、 **[OK]** をクリックします。

Citrix Receiver for Webサイトの管理

Aug 14, 2017

Citrix Receiver for Webを使って、さまざまなデバイスからアプリケーション、データ、デスクトップに簡単かつ安全にアクセスできます。StoreFrontを使って、Citrix Receiver for Webに対するCitrix Receiver for Webアプリケーションを構成します。

StoreFront管理コンソールを使って、次のCitrix Receiver for Web関連タスクを実行します。

Citrix Receiver for Webサイトの作成	Citrix Receiver for Webサイトを作成し、Webページを経由してストアにアクセスできます。
Citrix Receiver for Webサイトの構成	Receiver for Webサイトの設定を変更します。
統合Receiverエクスペリエンスのサポートの構成	StoreFrontは、クラシックと統合の両方のユーザーエクスペリエンスをサポートします。新しい統合エクスペリエンスは、中央集中管理されたHTML5ユーザーエクスペリエンス。
おすすめのアプリケーションの作成および管理	特定のカテゴリに関連するまたはそれと適合するエンドユーザーに対するお勧めのアプリケーショングループを作成します。
ワークスペースコントロールの構成	ワークスペースコントロール機能を有効にすると、ユーザーがセッションの途中でデバイスを切り替えても、新しいデバイス上でそのアプリケーションでの作業を継続できます。
Citrix Receiver for HTML5のブラウザータブ使用の構成	ユーザーがCitrix Receiver for HTML5を使用してショートカットからリソースを起動した場合、新しいタブが表示されるのではなく、既存のブラウザータブのCitrix Receiver for Webサイトが置き換わり、そこでデスクトップまたはアプリケーションが起動するように指定します。
通信のタイムアウト期間および再試行回数の構成	デフォルトでは、Citrix Receiver for Webサイトからそのストアへの要求は、3分でタイムアウトします。通信の試行が1回失敗すると、ストアが使用できないとみなされます。デフォルトの設定を変更できます。

Citrix Receiver for Webサイトの作成

Aug 14, 2017

ユーザーがWebページからストアにアクセスできるようにするには、［Webサイトの作成］タスクを使用してReceiver for Webサイトを追加します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、Citrix Receiver for Webサイトを作成するストアを選択し、［操作］ペインの［Receiver for Webサイトの管理］をクリックします。
3. **［追加］**をクリックして、新しいCitrix Reciver for Webサイトを作成します。［Webサイトパス］ボックスに希望するURLを指定して、**［次へ］**をクリックします。
4. Citrix Receiverエクスペリエンスを選択して、**［次へ］**をクリックします。
5. 認証方法を選択して［作成］をクリックし、サイトが作成されたら［完了］をクリックします。
   ユーザーがこのCitrix Receiver for WebサイトにアクセスするためのURLが表示されます。Citrix Receiver for Webサイトの設定の変更について詳しくは、「Citrix Receiver for Webサイトの構成」を参照してください。

デフォルトでは、ユーザーがWindowsまたはMac OS Xが動作するコンピューターからReceiver for Webサイトにアクセスすると、Citrix Receiverがユーザーデバイスにインストール済みであるかどうかが判別されます。Citrix Receiverが検出されない場合は、プラットフォームに適したCitrix Receiverをダウンロードしてインストールするためのページが開きます。この動作を変更する方法については、「Citrix Receiverの検出と展開の無効化」を参照してください。

Receiver for Webサイトのデフォルト構成では、デスクトップとアプリケーションにアクセスするために、ユーザーが適切なバージョンのCitrix Receiverをインストールする必要があります。Citrix Receiver for WebサイトのReceiver for HTML5を有効にすると、Citrix Receiverをインストールできないユーザーもリソースにアクセスできるようになります。詳しくは、「Citrix Receiver for Webサイトの構成」を参照してください。

Citrix Receiver for Webサイトの構成

Aug 14, 2017

Citrix Receiver for Webサイトを構成すると、ユーザーがWebページからストアにアクセスできるようになります。以下のタスクでは、Citrix Receiver for Webサイトの設定を変更します。一部の詳細設定を変更するには、サイトの構成ファイルを編集する必要があります。詳しくは、「構成ファイルを使ったCitrix Receiver for Webサイトの構成」を参照してください。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

Citrix Receiver for Webサイトに接続するユーザーの認証方法を指定するには、［認証方法］タスクを使用します。これにより、各Receiver for Webサイトでは、認証方法のサブセットを指定できます。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、結果ペインでストアを選択します。
3. ［操作］ペインで **[Receiver for Webサイトの管理]** > **[構成]** の順にクリックし、 **[認証方法]** を選択して、ユーザーに提供するアクセス方法を選択します。
   - 指定ユーザー認証を有効にするには［ユーザー名とパスワード］チェックボックスをオンにします。この場合、ユーザーは資格情報を入力してストアにアクセスします。
   - SAML IDプロバイダーとの統合を有効にするには、 **[SAML認証]** チェックボックスをオンにします。ユーザーはAccess Gatewayにログオンすることによって認証を受け、ストアにアクセスするときは自動的にログオンします。［設定］ボックスの一覧で次を選択します。
     - **[IDプロバイダー]** ：IDプロバイダーの信頼性を構成する場合。
     - **サービスプロバイダー**：サービスプロバイダーの信頼性を構成する場合。この情報は、IDプロバイダーから要求されます。
   - ユーザーデバイスからActive Directoryドメイン資格情報がパススルーされるようにするには、［ドメインパススルー］チェックボックスをオンにします。この場合、ユーザーはドメインに参加しているWindowsコンピューターにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。このオプションを使用する場合は、Citrix Receiver for Windowsをユーザーデバイスにインストールするときにパススルー認証を有効にする必要があります。Citrix Receiver for Webでのドメインパススルー認証は、Windows上のChrome、Firefox、Internet Explorer、Edgeでのみサポートされることに注意してください。
   - スマートカード認証を有効にするには、［スマートカード］チェックボックスをオンにします。ユーザーはスマートカードとPINを使ってストアにアクセスします。
   - NetScaler Gatewayからのパススルー認証を有効にするには、［NetScaler Gatewayからのパススルー］チェックボックスをオンにします。ユーザーはNetScaler Gatewayにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。
4. 認証方法を選択したら、［OK］をクリックします。
   認証方法の設定の変更について詳しくは、「認証サービスの構成」を参照してください。

内部ネットワーク上でホストされているWebサイトからデスクトップやアプリケーションにすばやくアクセスできるようにするには、［Webサイトへのショートカットの追加］タスクを使用します。Citrix Receiver for Webサイトで配信するリソースのURLを生成して、これらのリンクをWebサイトに埋め込みます。ユーザーがリンクをクリックすると、Receiver for Webサイトにリダイレクトされます。ここで、ユーザーがReceiver for Webサイトにログオンしていない場合はログオンします。Receiver for Webサイトでは、リソースが自動的に起動します。ユーザーがサブスクライブしていないアプリケーションの場

合は、自動的にサブスクライブされます。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、結果ペインでサイトを選択します。
3. **［操作］** ペインで **[Receiver for Webサイトの管理]** > **[構成]** の順にクリックし、 **[Webサイトのショートカット]** を選択します。
4. **［追加］をクリックして、ショートカットをホストしようとするWebサイトのURLを入力します。**URLは、http[s]://hostname[:port],の形式で指定する必要があります。ここで、hostnameはWebサイトホストの完全修飾ドメイン名です。portはホストとの通信に使用するポートで、プロトコルのデフォルトポートを使用できない場合に指定します。Webサイトの特定のページへのパスを指定する必要はありません。URLを変更するには、［Webサイト］の一覧でエントリを選択して［編集］をクリックします。Citrix Receiver for Webサイトのホストのリソースへのショートカットを削除するには、一覧でWebサイトを選択して、［削除］をクリックします。
5. ［ショートカットを取得］をクリックし、変更内容の保存を確認するメッセージが表示されたら、［保存］をクリックします。
6. WebブラウザーにCitrix Receiver for Webサイトにログオンして、必要なURLをコピーします。

また、Citrix Receiver for Webサイト上のユーザーセッションは、デフォルトでアイドル状態が20分続くとタイムアウトします。ユーザーはセッションがタイムアウトしても既に実行中のデスクトップとアプリケーションを引き続き使用できますが、アプリケーションのサブスクライブなどのCitrix Receiver for Webサイトの機能にアクセスするには、再ログオンする必要があります。

［Receiver for Webサイトの管理］の **[セッションのタイムアウト]** タスクを使って、セッションのタイムアウト値を変更します。

1. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. 左ペインで **[ストア]** ノードを選択して、 **[操作]** ペインで **[Receiver for Webサイトの管理]** 、 **[構成]** の順にクリックし、 **[セッション設定]** を選択します。**セッションタイムアウト**の時間と分を指定できます。すべての時間間隔の最小値は1です。最大値は、各時間間隔で1年に相当する値です。

[Receiver for Webサイトの管理] の **[Receiver for Webでのアプリケーションおよびデスクトップ表示]** タスクを使って、セッションのタイムアウト値を変更します。

1. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. 左ペインで **[ストア]** ノードを選択して、 **[操作]** ペインで［Receiver for Webサイトの管理］、 **[構成]** の順にクリックし、 **[クライアントインターフェイス設定]** を選択します。
3. **［ビューの選択］** および **[デフォルトビュー]** ドロップダウンメニューから、表示するビューを選択します。

フォルダービューを有効にするには、次の手順を実行します。

1. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. 左ペインで **[ストア]** ノードを選択して、 **[操作]** ペインで **[Receiver for Webサイトの管理]** > **[構成]** の順にクリックします。
3. **［詳細な設定］** を選択し、 **[フォルダービューを有効にする]** をオンにします。

デフォルトでは、Citrix Receiver for Webサイトによりプロビジョニングファイルが提供されます。ユーザーは、このファイ

ルを使用してCitrix Receiverでストアを構成します。このプロビジョニングファイルには、そのReceiver for Webサイトのリソースを提供するストアに接続するための詳細（NetScaler Gateway展開環境やビーコンの詳細など）が定義されています。

[Receiver for Webサイトの管理] の **[Receiver構成を有効にする]** タスクを使って、セッションのタイムアウト値を変更します。

1. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. 左ペインで **[ストア]** ノードを選択して、 **[操作]** ペインで **[Receiver for Webサイトの管理]** > **[構成]** の順にクリックし、 **[クライアントインターフェイス設定]** を選択します。
3. **[Receiver構成を有効にする]** をオンにします。

Citrix ReceiverをインストールしていないWindowsまたはMac OS Xユーザーがアクセスしたときの**Citrix Receiver for Web**サイトの動作を構成するには、［Citrix Receiverの展開］タスクを使用します。デフォルトでは、WindowsまたはMac OS Xを実行しているコンピューターからアクセスすると、Citrix Receiverがインストールされているかどうかが自動的に判別されます。

Citrix Receiverが検出されない場合は、プラットフォームに適したCitrix Receiverをダウンロードしてインストールするためのページが開きます。デフォルトのダウンロード元はCitrix社のWebサイトですが、StoreFrontサーバーにインストールファイルをコピーして、ユーザーにこれらのローカルファイルを提供することもできます。

Citrix Receiverをインストールできないユーザーについては、Citrix Receiver for WebサイトでCitrix Receiver for HTML5を有効にできます。Citrix Receiver for HTML5を使用すると、デスクトップやアプリケーションにHTML5互換のWebブラウザーからアクセスできます。デバイスにCitrix Receiverをインストールする必要はありません。内部ネットワーク接続、および外部ネットワークからNetScaler Gateway経由での接続の両方がサポートされています。ただし、内部ネットワークからの接続の場合、Citrix Receiver for HTML5では特定の製品で提供されるリソースにのみアクセスできます。さらに、社内ネットワークの外から接続できるようにするには、特定のバージョンのNetScaler Gatewayが必要です。詳しくは、「インフラストラクチャの要件」を参照してください。

デフォルトでは、内部ネットワーク上のローカルユーザーがXenDesktopやXenAppで提供されるリソースにCitrix Receiver for HTML5でアクセスすることはできません。Citrix Receiver for HTML5でデスクトップやアプリケーションへのローカルアクセスを有効にするには、XenDesktopおよびXenAppのサーバー側でポリシーの［ICA WebSockets接続］を有効にする必要があります。XenDesktopおよびXenAppでは、Citrix Receiver for HTML5での接続にポート8008が使用されます。ファイアウォールやほかのネットワークデバイスで、このポートへのアクセスが許可されることを確認してください。詳しくは、「WebSocketのポリシー設定」を参照してください。

Citrix Receiver for HTML5は、Internet ExplorerではHTTP接続でのみ使用できます。Mozilla FirefoxでHTTPS接続のCitrix Receiver for HTML5を使用するには、Firefoxのアドレスバーに「**about:config**」と入力し、 **[network.websocket.allowInsecureFromHTTPS]** を**true**に設定します。

1. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、結果ペインでサイトを選択します。 **[操作]** ペインで **[Receiver for Webサイトの管理]** > **[構成]** の順にクリックします。
3. **[Citrix Receiverの展開]** を選択し、ユーザーのデバイスでCitrix Receiverが検出されない場合の、Citrix Receiver for Webサイトの動作を指定します。

- プラットフォームに適したCitrix Receiverをダウンロードしてインストールするためのページを表示するには、**[ローカルにインストール]** を選択します。この場合、ユーザーがReceiver for Webサイトからデスクトップやアプリケーションにアクセスするには、Citrix Receiverのインストールが必要になります。
  - **[ユーザーによる HDX エンジン（プラグイン）のダウンロードを許可する]**をオンにすると、Citrix Receiverを使用で

きない場合は、Citrix Receiver for WebによりユーザーはCitrix Receiverをエンドユーザークライアント上にダウンロードしてインストールできます。
  - **[ログオン時にプラグインをアップグレードする]**を選択すると、Citrix Receiver for Webではユーザーのログオン時にCitrix Receiverクライアントがアップグレードされます。この機能を有効にするには、StoreFrontサーバー上でCitrix Receiverファイル使用できるようにしてください。
  - ドロップダウンメニューからソースを選択します。
- Citrix Receiverをダウンロードしてインストールするためのメッセージが表示された時に、インストールができない場合はCitrix Receiver for HTML5が使用できるように、**[ローカルのReceiverが使用できない場合はReceiver for HTML5を使用する]**を選択します。この場合、Citrix Receiverをインストールしていないユーザーが Receiver for Webサイトにログオンするたびに、Citrix Receiverをダウンロードしてインストールすることを求めるメッセージが表示されます。
- Citrix Receiverをダウンロードしてインストールすることを求めるメッセージを表示せずに、Citrix Receiver for HTML5を使用してリソースにアクセスできるようにするには、**[常にReceiver for HTML5を使用する]**を選択します。この場合、ユーザーは常にCitrix Receiver for HTML5を使用してデスクトップやアプリケーションにアクセスします。ただし、HTML5互換のWebブラウザーが必要です。HTML5互換のWebブラウザーがない場合は、通常のCitrix Receiverをインストールする必要があります。

デフォルトでは、ユーザーがWindowsまたはMac OS Xが動作するコンピューターからCitrix Receiver for Webサイトにアクセスすると、Citrix Receiverがユーザーデバイスにインストール済みであるかどうかが判別されます。Citrix Receiverが検出されない場合は、プラットフォームに適したCitrix Receiverをダウンロードしてインストールするためのページが開きます。

1. Windowsの**[スタート]**画面または**[アプリ]**画面で、**[Citrix StoreFront]**タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで**[ストア]**ノードを選択して、結果ペインでサイトを選択します。**[操作]**ペインで**[Receiver for Webサイトの管理]** > **[構成]**の順にクリックします。
3. **[Citrix Receiverの展開]**および**[Receiversのソース]**を選択し、インストールファイルを指定します。

ユーザーのコンピューターにCitrix Receiverがまだインストールされていない場合（Internet Explorer、Firefox、およびSafariユーザー）、またはユーザーが初めてサイトにアクセスした場合（Chromeユーザー）、Citrix Receiver for Webにより、StoreFrontにログオンする前に最新のCitrix Receiverをインストールするよう求められます。構成により異なりますが、ユーザーのCitrix Receiverインストールがアップグレード可能かどうかも表示される場合があります。

StoreFrontへのログイン後にプロンプトを表示するように、Citrix Receiver for Webを構成できます。

1. Windowsの**[スタート]**画面または**[アプリ]**画面で、**[Citrix StoreFront]**タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで**[ストア]**ノードを選択して、結果ペインでサイトを選択します。
3. **[操作]**ペインで**[Receiver for Webサイトの管理]**、**[構成]**の順にクリックします。
4. **[詳細な設定]**を選択し、**[ログオン後に、Citrix Receiverのインストールメッセージが表示されます]**をオンにします。

[操作]ペインで**[Receiver for Webサイトの管理]**を使用してCitrix Receiver for Webサイトを削除します。サイトを削除すると、ユーザーはそのWebページを使用してストアにアクセスできなくなります。

統合Citrix Receiverエクスペリエンスのサポート

Aug 14, 2017

StoreFrontは、**クラシック**と**統合**の両方のユーザーエクスペリエンスをサポートします。クラシックエクスペリエンスでは、配信は各Citrix Receiverのプラットフォームのユーザーエクスペリエンスに依存します。新しい統合エクスペリエンスは、集中管理されたHTML5ユーザーエクスペリエンスをすべてのWebおよびネイティブCitrix Receiverに配信します。これはカスタマイズとお勧めのアプリケーショングループの管理をサポートしています。

このバージョンのStoreFrontを使って作成されたストアは、デフォルトで統合エクスペリエンスを使用しますが、アップグレードされたものについては、デフォルトでクラシックエクスペリエンスとなります。統合エクスペリエンスをサポートするには、StoreFrontストアをReceiver for Webサイトに割り当てる必要があり、そのサイトが統合エクスペリエンスを使用するように構成する必要があります。

重要：制限付きゾーンにReceiver for Webサイトを追加した場合、統合エクスペリエンスはサポートされません。制限付きゾーンにReceiver for Webサイトを追加する必要がある場合、クラシックエクスペリエンスを使用するようにストアを設定します。

StoreFront管理コンソールを使って、次のCitrix Receiver for Web関連タスクを実行します。

- Citrix Receiver for Webサイトの作成。
- Citrix Receiver for Webサイトエクスペリエンスの変更。
- ストアに割り当てる統合Citrix Receiver for Webサイトの選択。
- Receiverの外観をカスタマイズします。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

> ### 注意
>
> XenApp 6.xを使用している場合、統合エクスペリエンスが有効な**[クライアントにストリーム配信する]**または**[ストリーム配信できない場合はサーバー上で実行する]**に設定したアプリケーションはサポートされません。

ストアを作成すると、Citrix Receiver for Webサイトが自動的に作成されます。また、次のことを実行して追加のReceiver for Webサイトを作成することもできます。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、［操作］ペインで［Receiver for Webサイトの管理］>［追加］の順にクリックしてウィザードの指示に従います。

Citrix Receiver for Webの Webサイトが**クラシック**または**統合**エクスペリエンスを配信するかどうかを選択できます。クラシックエクスペリエンスを有効にすると、詳細なカスタマイズとお勧めのアプリケーショングループの管理ができなくなります。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。

2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択し、真ん中のペインで変更するストアを選択して、［操作］ペインで **[Receiver for Webサイトの管理]**、次に **[構成]** の順にクリックします。
3. **[Receiverエクスペリエンス]** を選択し、**[クラシックエクスペリエンスの無効化]** または **[クラシックエクスペリエンスの有効化]** を選択します。

ストアに割り当てる統合Citrix Receiver for Webサイトの選択

StoreFrontを使って新しいストアが作成されると、統合モードのCitrix Receiver for Webサイトが自動的に作成され、ストアに割り当てられます。ただし、以前のバージョンのStoreFrontからアップグレードした場合は、デフォルトでクラシックエクスペリエンスに設定されます。

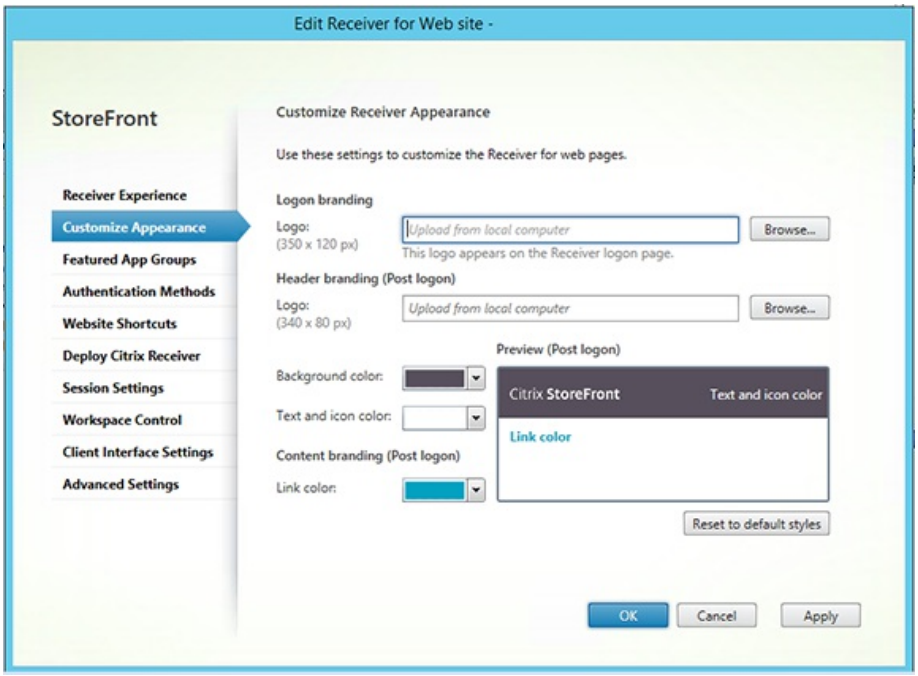
Citrix Receiver for Webサイトを選択してストアに統合エクスペリエンスを提供するには、クラシックエクスペリエンスを無効にして作成されたCitrix Receiver for Webサイトが1つ以上必要です。

1. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、**[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択し、真ん中のペインでストアを選択して、**[操作]** ペインで **[統合エクスペリエンスの構成]** をクリックします。ストアのデフォルトとしては、（クラシックエクスペリエンスを無効にして）統合エクスペリエンスをサポートするWebサイトだけを使用できます。作成されたCitrix Receiver for WebのWebサイトがない場合は、新しいReceiver for WebのWebサイトの作成へのリンクを含むメッセージが表示されます。また、既存のReceiver for WebサイトをReceiver for WebのWebサイトに変更することもできます。「Citrix Receiverエクスペリエンス」を参照してください。
3. Citrix Receiver for Webサイトを作成したら、このストアの **[統合エクスペリエンスの構成]** を選択し、特定のWebサイトを選択します。

> **Important**
>
> Receiver for Webサイト上で統合エクスペリエンスをクラシックエクスペリエンスに変更する場合、ネイティブのCitrix Receiverクライアントに影響が及ぶ可能性があります。このReceiver fot Webサイト上でエクスペリエンスを統合エクスペリエンスに戻しても、ネイティブのCitrix Receiverクライアントのエクスペリエンスが統合エクスペリエンスに更新されることはありません。管理コンソールで［ストア］ノードの統合エクスペリエンスをリセットする必要があります。

Citrix Receiverの外観をカスタマイズするには、お使いのCitrix Receiver for WebのWebサイトでクラシックCitrix Receiverエクスペリエンスを無効にする必要があります。

1. Windowsの **[スタート]** 画面または［アプリ］画面で、**[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、［操作］ペインで **[Receiver for Webサイトの管理]** > **[構成]** の順にクリックします。
3. **[Receiverエクスペリエンス]** > **[クラシックエクスペリエンスの無効化]** の順に選択します。
4. **[外観のカスタマイズ]** を選択し、項目を選択してログオン後のWebサイトの表示方法をカスタマイズします。



おすすめのアプリケーションの作成および管理

Aug 14, 2017

特定のカテゴリに関連するまたはそれと適合するエンドユーザーに対するお勧めのアプリケーショングループを作成できます。たとえば、営業部により使用されるアプリケーションを含む、営業部におすすめのアプリケーショングループを作成できます。アプリケーション名を使ったり、Studioコンソールで定義されたキーワードまたはあプリケーションカテゴリを使ったりして、StoreFront管理コンソールでおすすめのアプリケーションを定義できます。

［おすすめのアプリケーショングループ］タスクを使って、おすすめのアプリケーショングループを追加、編集、または削除します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

この機能は、クラシックエクスペリエンスを無効にした場合に限り使用できます。

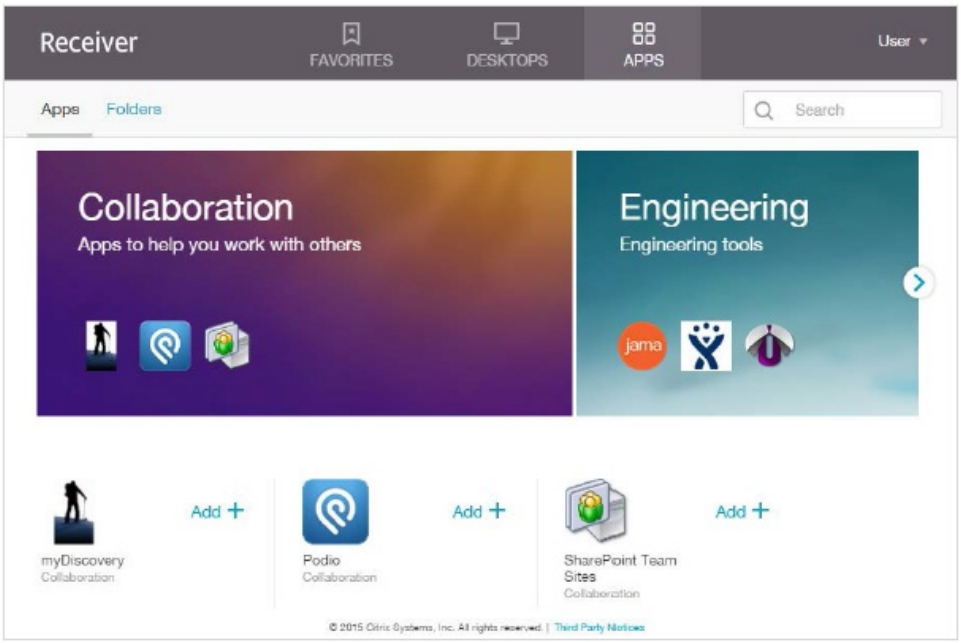
1. Windowsの **[スタート]** 画面または［アプリ］画面で、［Citrix**StoreFront**］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、［操作］ペインで**[Receiver for Webサイトの管理]** > **[構成]** の順にクリックします。
3. **[おすすめのアプリケーショングループ]** を選択します。
4. **[おすすめのアプリケーショングループ]** ダイアログボックスで、**[作成]** をクリックして新しいお勧めのアプリケーショングループを定義します。
5. **[お勧めのアプリケーショングループの作成]** ダイアログボックスで、おすすめのアプリケーショングループ名、説明（任意）、背景、およびおすすめのアプリケーショングループを定義する方法を指定します。キーワード、アプリケーション名、またはアプリケーションカテゴリを選択し、 **[OK]** をクリックします。

オプション	説明
キーワード	Studioでキーワードを定義します。
アプリケーションカテゴリ	Studioでアプリケーションカテゴリを定義します。
アプリケーション名	アプリケーション名を使っておすすめのアプリケーショングループを定義します。［お勧めのアプリケーショングループの作成］ダイアログボックスのここに含まれている名前と一致するすべてのアプリケーション名は、おすすめのアプリケーショングループに含まれます。 StoreFrontはアプリケーション名でワイルドカードをサポートしません。一致する内容では大文字と小文字は区別されませんが、全体が一致する必要があります。たとえば、「Excel」と入力すると、StoreFrontでは公開アプリケーション名のMicrosoft Excel 2013が一致となりますが、「Exc」と入力しても一致するものはありません。

たとえば、次のように指定します。

2つのおすすめアプリケーショングループを作成しました。

- コラボレーション - Studioの**Collaboration**カテゴリに含まれるアプリケーションとの一致を指定することによって作成しました。
- 開発 - アプリケーショングループに名前を付けて、アプリケーション名のコレクションを指定することによって作成しました。



ワークスペースコントロールの構成

Aug 14, 2017

ワークスペースコントロール機能を有効にすると、ユーザーがセッションの途中でデバイスを切り替えても、新しいデバイス上でそのアプリケーションでの作業を継続できます。これにより、たとえば病院で臨床医がほかのワークステーションに移動しても、移動先のデバイスでアプリケーションを起動し直す必要がなくなります。Citrix Receiver for Webサイトでは、ワークスペースコントロールがデフォルトで有効になります。ワークスペースコントロールを無効にしたり設定を変更したりするには、サイトの構成ファイルを編集します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、［Citrix StoreFront］タイルをクリックします。
2. 左ペインで **[ストア]** を選択し、［操作］ペインで **[Receiver for Webサイトの管理] >構成の順にクリックします。**
3. **[ワークスペースコントロール]** を選択します。
4. ワークスペースコントロールのデフォルト設定を構成します。以下の設定が含まれます。

    ワークスペースコントロールの有効化

    セッション再接続オプションの設定

    ログオフ操作の指定

Citrix Receiver for HTML5のブラウザータブ使用の構成

Aug 14, 2017

デフォルトでは、Citrix Receiver for HTML5は新しいブラウザータブでデスクトップやアプリケーションを起動します。ただし、ユーザーがCitrix Receiver for HTML5を使用してショートカットからリソースを起動した場合、既存のブラウザータブのCitrix Receiver for Webサイトが置き換わり、そこでデスクトップまたはアプリケーションが起動します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、［Citrix StoreFront］タイルをクリックします。
2. 左ペインで **[ストア]** を選択し、［操作］ペインで **[Receiver for Webサイトの管理]** >**構成**の順にクリックします。
3. **[Citrix Receiverの展開]** を選択します。
4. **[展開オプション]** ドロップダウンメニューから **[常にHTML 5 Receiverを使用する]** を選択し、アプリケーションを起動するタブに応じて、 **[Receiver for Webと同じタブでアプリケーションを起動]** をオンまたはオフにします。

通信のタイムアウト期間および再試行回数の構成

Aug 14, 2017

デフォルトでは、Citrix Receiver for Webサイトからそのストアへの要求は、3分でタイムアウトします。通信の試行が1回失敗すると、ストアが使用できないとみなされます。デフォルトの設定を変更するには、**[セッション設定]**タスクを使用します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの**[スタート]**画面または**[アプリ]**画面で、**[Citrix StoreFront]**タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで**[ストア]**ノードを選択し、真ん中のペインでストアを選択して、**[操作]**ペインで**[Receiver for Webサイトの管理]** > **[構成]の順にクリックします。**
3. **[セッション設定]**を選択し、変更を加えて**[OK/適用]**をクリックして、変更を保存します。

ユーザーアクセスの構成

Aug 14, 2017

このアーティクルは、次の情報で構成されています。

XenApp Servicesサイトを介した接続のサポート

すべてのCitrix Receiverに対するワークスペースコントロールの再接続を無効にする

ユーザーサブスクリプションの構成

サブスクリプションデータの管理

> ## Important
>
> 複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

XenApp ServicesサイトのURLからストアにアクセスできるようにするには、**[XenApp Servicesサポートの構成]**タスクを使用します。ドメインに参加しているデスクトップアプライアンスのユーザー、Citrix Desktop Lockを実行している再目的化されたPCのユーザー、およびアップグレードできない古いバージョンのCitrixクライアントのユーザーは、XenApp Servicesサイトから直接そのストアに接続できます。デフォルトでは、新しいストアを作成するときに、XenApp ServicesサイトのURLが有効になります。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの**[スタート]**画面または**[アプリ]**画面で、**[Citrix StoreFront]**タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで**[ストア]**ノードを選択して、結果ペインでストアを選択します。**[操作]**ペインの**[XenApp Servicesサポートの構成]**をクリックします。
3. **[XenApp Servicesサポートを有効にする]**チェックボックスをオンまたはオフにして、XenApp ServicesサイトのURLを介したストアへのユーザーアクセスを有効または無効にします。
   ストアのXenApp Services URLの形式は、http[s]*://serveraddress/Citrix/storename/PNAgent/config.xml*の形式です。ここで、*serveraddress*はStoreFront展開環境のサーバーまたは負荷分散環境の完全修飾ドメイン名で、*storename*はストアの作成時に指定した名前です。
4. XenApp Servicesサポートを有効にする場合は、必要に応じてCitrix Online Plug-inユーザーのデフォルトストアを指定します。
   デフォルトストアを指定すると、ユーザーが特定ストアのXenApp Services URLではなくStoreFrontサーバーのURLまたは負荷分散URLを使用してCitrix Online Plug-inを構成できるようになります。

ワークスペースコントロール機能を有効にすると、ユーザーがデバイスを移動してもそのアプリケーションでの作業を継続で

きます。これにより、たとえば病院で臨床医がほかのワークステーションに移動しても、移動先のデバイスでアプリケーションを起動し直す必要がなくなります。

StoreFrontには、すべてのCitrix Receiverのストアサービスでワークスペースコントロールの再接続を無効にする構成があります。この機能は、StoreFrontコンソールまたはPowerShellを使って管理します。

StoreFront管理コンソールの使用

1. Windowsの **[スタート]** 画面または［アプリ］画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、 **[操作]** ペインで **[ストア設定の構成]** をクリックします。
3. **[詳細な設定]** を選択し、 **[セッションの再接続を許可する]** チェックボックスをオンまたはオフにします。

PowerShellの使用

管理コンソールを閉じる必要があります。次のコードスニペットを実行して、StoreFront PowerShellモジュールをインポートします。

```
$dsInstallProp = Get-ItemProperty `
-Path HKLM:\SOFTWARE\Citrix\DeliveryServicesManagement -Name InstallDir
$dsInstallDir = $dsInstallProp.InstallDir
& $dsInstallDir\..\Scripts\ImportModules.ps1
```

次にPowerShellコマンドの**Set-DSAllowSessionReconnect**でワークスペースコントロールの再接続をオンまたはオフに設定します。

構文

```
Set-DSAllowSessionReconnect [[-SiteId] ] [[-VirtualPath] ] `
[[-IsAllowed] ]
```

たとえば、/Citrix/Storeのストアでワークスペースコントロールの再接続をオフにするには、次のコマンドでストアを構成します。

```
Set-DSAllowSessionReconnect -SiteId 1 -VirtualPath /Citrix/Store ` -IsAllowed $false
```

ユーザーサブスクリプションタスクを使用して、以下のオプションのどちらかを選択します。

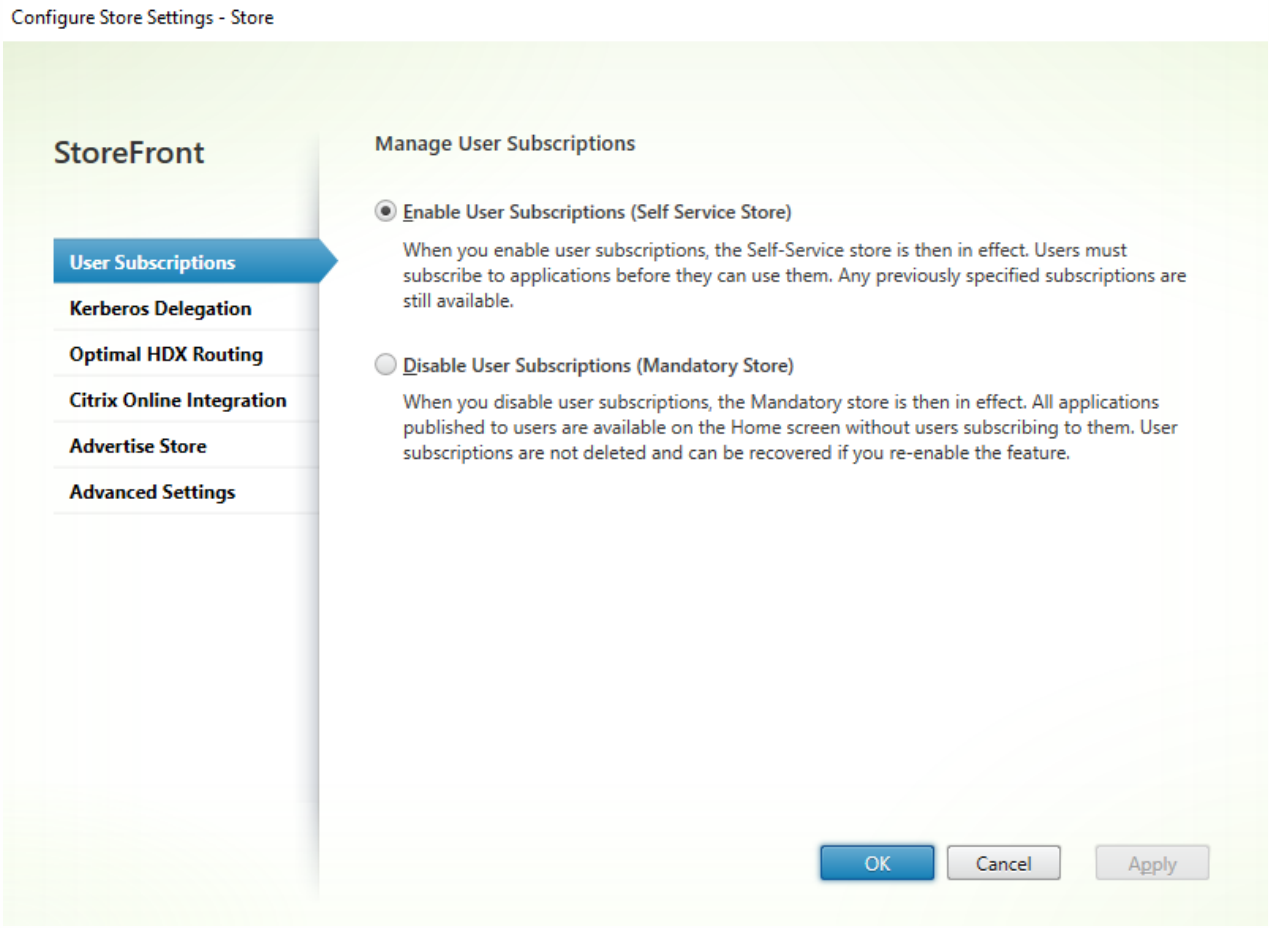
- アプリケーションを使用する前に、ユーザーがサブスクライブする必要がある（セルフサービスストア）。
- ストアに接続すると、ユーザーはすべてのアプリケーションを受信できる（必須ストア）。

StoreFrontでストアのユーザーサブスクリプションを無効にすると、Citrix Receiverでユーザーに［お気に入り］タブが表示されなくなります。サブスクリプションを無効にしても、ストアのサブスクリプションデータは削除されません。ストアのサブスクリプションを再度有効にすると、ユーザーが次回ログオンしたときにサブスクライブされたアプリが［お気に入り］に表示されます。

1. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、結果ペインでストアを選択します。 **[操作]** ペインで **[ストア設定の構成]** > **[ユーザーのサブスクリプション]** の順にクリックして、ユーザーサブスクリプション機能の有効/無効を切り替えます。
3. **[ユーザーのサブスクリプションの有効化（セルフサービスストア）]** を選択すると、アプリケーションを使用するため

にユーザーにサブスクライブさせます。以前指定したサブスクリプションはいずれも有効なままです。

4. **［ユーザーのサブスクリプションの無効化（必須ストア）］**を選択すると、サブスクライブすることなくユーザーに公開されているすべてのアプリケーションを［ホーム］画面で利用できるようにします。サブスクリプションは削除されず、再度有効にしようとするときには有効にすることができます。



StoreFront 3.5以降では、次のPowerShellスクリプトを使用して、ストアのユーザーサブスクリプションを構成できます。

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/"

Set-STFStoreService -StoreService $StoreObject -LockedDown $True -Confirm:$False
```

Get-STFStoreServiceについて詳しくは、https://citrix.github.io/storefront-sdk/Citrix.StoreFront.Stores/Get-STFStoreService/を参照してください。

PowerShellコマンドレットを使用してストアのサブスクリプションデータを管理します。

> ## 注意
>
> StoreFront管理コンソールまたはPowerShellのどちらかを使用して、StoreFrontを管理します。両方を同時に使用しないでください。StoreFront構成を変更する場合、StoreFront管理コンソールを閉じてからPowerShellを使用してください。既存のサブスクリプションデータを変更するときは、変更前の状態にロールバックできるようにバックアップを作成しておくことをお勧めします。

サブスクリプションデータの完全消去

サブスクリプションデータを格納するフォルダーおよびデータストアは、既存の環境の各ストアに存在します。

1. StoreFrontサーバー上で、Citrix Subscriptions Storeサービスを停止します。Citrix Subscriptions Storeサービスの実行中は、ストアのサブスクリプションデータを削除できません。
2. StoreFrontサーバー上で、サブスクリプションストアフォルダーを開きます。C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<ストア名>
3. サブスクリプションストアフォルダー内のすべてのファイルを削除します。フォルダー自体は削除しないでください。
4. StoreFrontサーバー上で、Citrix Subscriptions Storeサービスを再起動します。

StoreFront 3.5以降では、以下のPowerShellスクリプトを使用して、ストアのサブスクリプションデータを完全消去できます。サービスを停止または開始したり、ファイルを削除したりできる管理者権限でこのPowerShellを実行します。このPowerShellスクリプトは、上記で説明した手動の手順と同様に機能します。

コマンドレットを問題なく実行するには、サーバー上でCitrix Subscriptions Storeサービスが実行されている必要があります。

```
function Remove-SubscriptionData

{

    [CmdletBinding()]

    [Parameter(Mandatory=$False)][String]$Store = "Store"

    $SubsService = "Citrix Subscriptions Store"

    # Path to Subscription Data in StoreFront version 2.6 or higher

    $SubsPath = "C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_$Store\*"

    Stop-Service -displayname $SubsService

    Remove-Item $SubsPath -Force -Verbose

    Start-Service -displayname $SubsService

    Get-Service -displayname $SubsService

}



Remove-SubscriptionData -Store "YourStore"
```

サブスクリプションデータのエクスポート

PowerShellコマンドレットを使用して、ストアサブスクリプションデータのバックアップをタブ区切りのTXTファイル形式で取得できます。

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<yourstore>"

Export-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env:USERPROFILE\Desktop\Subscriptions.txt"
```

複数サーバー展開環境を管理している場合、このPowerShellコマンドレットを、StoreFrontサーバーグループ内の任意のサーバー上で実行できます。サーバーグループの各サーバーは、ピアから同期されたサブスクリプションデータの同一コピーを保持します。Storefrontサーバー間でサブスクリプションの同期に問題がある場合、グループのすべてのサーバーからデータをエクスポートして、比較してください。

サブスクリプションデータの復元

既存のサブスクリプションデータを上書きするには、Restore-STFStoreSubscriptionsを使用します。前述のように、Export-STFStoreSubscriptionsを使用して作成したタブ区切りのTXTファイル形式のバックアップから、ストアのサブスクリプションデータを復元できます。

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<yourstore>"

Restore-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env:USERPROFILE\Desktop\Subscriptions.txt"
```

Restore-STFStoreSubscriptionsについて詳しくは、https://citrix.github.io/storefront-sdk/Citrix.StoreFront.SubscriptionsStore/Restore-STFStoreSubscriptions/#restore-stfstoresubscriptionsを参照してください。

単一のStoreFrontサーバー上でデータを復元する

単一のサーバー展開環境で、Subscriptions Storeサービスをシャットダウンする必要はありません。また、サブスクリプションデータの復元前に既存のサブスクリプションデータを消去する必要もありません。

StoreFrontサーバーグループ上でデータを復元する

サーバーグループにサブスクリプションデータを復元するには、次の手順に従う必要があります。

例：3つのStoreFrontサーバーを含むサーバーグループ環境。

StoreFrontA

StoreFrontB

StoreFrontC

1. 3つのサーバーのいずれかから、既存のサブスクリプションデータのバックアップを作成します。
2. サーバーStoreFrontBおよびStoreFrontCでSubscriptions Storeサービスを停止します。この操作によって、StoreFrontAの更新中、サーバーはサブスクリプションデータを送受信することができなくなります。
3. サーバーStoreFrontBおよびStoreFrontCからサブスクリプションデータを完全消去します。この操作によって、復元されたサブスクリプションデータの不一致が発生しないようにします。
4. Restore-STFStoreSubscriptionsコマンドレットでStoreFrontA上にデータを復元します。Subscriptions Storeサービスを停止したり、StoreFrontAでサブスクリプションデータを完全消去する必要はありません（復元操作中に上書きされます）。
5. サーバーStoreFrontBおよびStoreFrontC上で、Subscriptions Storeサービスを再起動します。これで、このサーバーはStoreFrontAからデータのコピーを受信できます。
6. すべてのサーバー間で同期が開始されるのを待ちます。このために必要な時間は、StoreFrontAに存在するレコード数によって異なります。すべてのサーバーがローカルネットワーク接続であれば、通常同期は迅速に行われます。WAN接続でのサブスクリプションの同期には、多少時間がかかる場合があります。
7. StoreFrontBおよびStoreFrontCからデータをエクスポートして、同期が完了したことを確認します。またはストアサブスクリプションカウンターを表示します。

サブスクリプションデータのインポート

ストアにサブスクリプションデータがない場合、Import-STFStoreSubscriptionsを使用します。このコマンドレットによって、サブスクリプションデータをストア間で転送したり、サブスクリプションデータを新しくプロビジョニングされたStoreFrontサーバーにインポートしたりできます。

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<yourstore>"

Import-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env:USERPROFILE\Desktop\Subscriptions.txt"
```

Import-STFStoreSubscriptionsについて詳しくは、https://citrix.github.io/storefront-sdk/Citrix.StoreFront.SubscriptionsStore/Import-STFStoreSubscriptions/#import-stfstoresubscriptionsを参照してください。

サブスクリプションデータファイルの詳細

サブスクリプションデータファイルは、各行に1つのユーザーサブスクリプションが記載されたテキストファイルです。各行には、以下の値がタブで区切られて記載されます。

…

値は、以下のように定義されます。

- <*user-identifier*>：必須の値です。ユーザーを識別する文字列です。この識別子には、ユーザーのWindowsセキュリティID

が使用されます。

- <*resource-id*>：必須の値です。サブスクライブされるリソースを識別する文字列です。
- <*subscription-id*>：必須の値です。サブスクリプションを一意に識別する文字列です。この値は使用されません（ただし、データファイル内に値が存在する必要はあります）。
- <*subscription-status*>：必須の値です。サブスクリプションの状態（subscribedまたはunsubscribed）です。
- <*property-name*>および<*property-value*>：オプションの値です。0個以上の値と値の組み合わせです。StoreFrontクライアント（通常はCitrix Receiver）によるサブスリプションのプロパティを表します。複数の値を持つプロパティは、同じ名前の複数の「 」ペアで示されます（MyPropが2つの値AとBを持つ場合は「... MyProp A MyProp B ...」など）。

たとえば、次のように指定します。

S-0-0-00-0000000000-0000000000-0000000000-0000 XenApp.Excel 21EC2020-3AEA-4069-A2DD-08002B30309D Subscribed dazzle:position 1

StoreFrontサーバーのディスク上にあるサブスクリプションデータのサイズ

Subscription Datastore Size	
No of Records	Size MB
0	6.02
1000	7.02
10000	40.00
100000	219.00
200000	358.00
500000	784.00
800000	1213.02
1000000	1497.15
1300000	1919.15
1500000	2205.15
1700000	2487.15
2000000	2915.15

インポートおよびエクスポート用のTXTファイルのサイズ

Subscriptions Import/Export.txt	
No of Records	Size MB
0	0.00
1000	0.13
10000	1.30
100000	12.80
200000	25.60
500000	64.10
800000	102.00
1000000	128.00
1300000	166.00
1500000	192.00
1700000	218.00
2000000	256.00

ストアサブスクリプションカウンター

Microsoft Windowsパフォーマンスモニターカウンター（［スタート］>［検索の開始］ボックスに「perfmon」と入力）を使用して、サーバー上のサブスクリプションレコードの合計数、StoreFrontサーバーグループ間で同期されたレコード数などを表示できます。

PowerShellを使用したサブスクリプションカウンターの表示

```
Get-Counter -Counter "\Citrix Subscription Store(1__citrix_store)\Subscription Entries Count (including unpurged deleted records)"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Subscriptions Store Synchronizing"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number Subscriptions Synchronized"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number Subscriptions Transferred"
```

可用性の高いマルチサイトストアのセットアップ

Aug 14, 2017

ここでは次のことについて説明します。

ユーザーマッピングおよびアグリゲーションの構成

詳細構成

サブスクリプション同期の構成

ストアの最適なHDXルーティングの構成

Citrix StoreFront管理コンソールの使用

PowerShellを使用して最適なNetScaler Gatewayルーティングを構成するには

特に地理的に分散した複数の展開環境からリソースを集約するストアについては、展開環境間の負荷分散とフェールオーバー、ユーザーと展開環境のマッピング、および障害回復用の展開環境を構成して、可用性の高いリソースを提供できます。複数の展開環境で個別のNetScaler Gatewayアプライアンスを構成している場合は、ユーザーが各展開環境にアクセスするための最適なアプライアンスを定義できます。

StoreFront 3.5から、StoreFront管理コンソールでは共通のマルチサイトシナリオがサポートされるようになりました。お客様の要件に合う場合は、この管理コンソールを使用することをお勧めします。

StoreFront管理コンソールでは、次の操作を行うことができます。

- **展開環境へのユーザーのマッピング：**Active Directoryグループメンバーシップに基づいて、特定の展開環境へのアクセス権を持つユーザーを制限できます。
- **展開環境の集計：**集計対象のリソースがある展開環境を指定できます。集計された展開環境のリソースは、単一の高可用性リソースとしてユーザーに示されます。
- **展開環境へのゾーンの関連付け：**StoreFrontでは、グローバルな負荷分散構成のNetScaler Gatewayを使用してアクセスされた場合、リソースの起動時に、ゲートウェイゾーンに一致するゾーンの展開環境が優先されます。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. すべてのXenDesktopおよびXenApp展開環境の詳細を使用してストアが正しく構成されていることを確認します。ストアへの展開環境の追加について詳しくは、ストアに表示するリソースの管理」を参照してください。
2. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、 **[Citrix StoreFront]** タイルをクリックします。
3. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、 **[操作]** ペインの **[Delivery Controllerの管理]** をクリックします。
4. 2つ以上のControllerが定義されている場合、 **[ユーザーマッピングおよびマルチサイトアグリゲーション構成]**>［構成］の順にクリックします。
5. **[ユーザーをControllerにマップ]** をクリックして、Delivery Controllerをユーザーが使えるようにするのか画面上で選択します。
6. **[リソースをまとめる]** をクリックしてコントローラーを選択し、 **[アグリゲート]** をクリックしてDelivery Controllerをまとめるかどうかを指定します。Delivery Controllerのアグリゲーションを有効にすると、同じ表示名とパスのDelivery Controllerのアプリケーションおよびデスクトップは、Citrix Receiverに単一のアプリケーション/デスクトップとして表示されます。
7. **[集計済みコントローラーの設定]** チェックボックスのいずれかまたはオンにして、 **[OK]** をクリックします。

   コントローラーの公開_同一のリソース- オンにすると、集計済みセットにあるいずれか1つのみのコントローラーのリソースが列挙されます。オフにすると、（利用できるリソースのユーザーのセット全体を集計するために）集計済みセットにあるすべてのコントローラーのリソースが列挙されます。このオプションをオンにするとリソース列挙時のパフォーマンスが向上します。ただし、リソースのリストが集計済みのすべての展開環境全体で同一であることが確実でない限り、お勧めしません。

   複数のコントローラーでリソースを負荷分散します- オンにすると、利用可能なコントローラーに起動が均一に分散されます。オフにすると、起動はユーザーマッピングダイアログ画面で指定された最初のコントローラーに割り当てられ、その起動が失敗した場合は以降のコントローラーにフェールオーバーします。

多くの一般的なマルチサイトおよび高可用性操作をStoreFront管理コンソールで構成できますが、以前のバージョンのStoreFrontと同じ方法で構成ファイルを使ってStoreFrontを引き続き構成することもできます。

PowerShellを使用するかStoreFront構成ファイルを編集して利用できる追加機能は次のとおりです。

- 集計対象として複数の展開環境グループを指定する機能。
  - 管理コンソールでは展開環境を単一のグループにまとめることしかできませんが、大部分の場合はこれで十分です。
  - 参加していないリソースセットを持つ複数の展開環境があるストアでは、複数グループによりパフォーマンスが向上する場合があります。
- 集計済み展開環境に対して複雑な優先順位を指定する機能。管理コンソールでは、集計済みの展開環境を負荷分散したり、単一のフェールオーバーリストとして使用したりできます。

- 障害回復展開環境（他のすべての展開環境が利用できない時のみアクセスされる展開環境）を定義する機能。

警告：構成ファイルを手動で編集して詳細なマルチサイトオプションを構成すると、構成ミスを防ぐため、Citrix StoreFront管理コンソールで一部のタスクを実行できなくなります。

重要：複数サーバーの展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. 障害回復用の展開環境を含め、すべてのXenDesktopおよびXenApp展開環境の詳細を使用してストアが正しく構成されていることを確認します。ストアへの展開環境の追加について詳しくは、「ストアに表示するリソースを管理するには」を参照してください。
2. テキストエディターを使ってストアのweb.configファイルを開きます。このファイルは通常、C:\inetpub\wwwroot\Citrix\storename\ディレクトリにあります。ここで、storenameはストアの作成時に指定した名前です。
3. ファイル内で次のセクションを検索します。

4. 次のように構成します。

```
        ...

        aggregationGroup="aggregationgroupname">

        ...

        ...

        ...

        ...
```

構成を定義する時に使用する要素は以下のとおりです。

- **userFarmMapping**
  展開環境のグループを指定して、それらの展開環境間の負荷分散とフェールオーバーを定義します。また、障害回復用の展開環境を定義します。指定した展開環境グループにMicrosoft Active Directoryユーザーグループをマップして、リソースへのユーザーアクセスを制御します。
- **groups**
  関連付けたマッピングが適用されるActive Directoryユーザーグループの名前とセキュリティID（SID）を指定します。ユーザーグループ名は、*domain**usergroup*の形式で指定する必要があります。複数のグループを指定する場合、そのすべてのグループに属しているユーザーのみにマッピングが適用されます。すべてのActive Directoryユーザーアカウントのアクセスを有効にするには、グループ名およびSIDに**everyone**を設定します。
- **equivalentFarmSet**
  負荷分散またはフェールオーバーのために集約されるリソースを提供する同等の展開環境のグループと、障害回復用の展開環境のグループを定義します。

  loadBalanceMode属性により、ユーザーがどのように展開環境に割り当てられるかが定義されます。**loadBalanceMode**属性を**LoadBalanced**に設定すると、ユー

ザー接続が均等に分散されるように展開環境が一覧からランダムに選択されます。**loadBalanceMode**属性を**Failover**に設定すると、展開環境が定義した順序で選択されます。これにより、使用される展開環境の数が常に最小になります。集約するソースを提供する同等の展開環境のグループの名前として、アグリゲーショングループ名（aggregationGroup）を指定します。同じアグリゲーショングループに属するすべての展開環境で提供されるリソースが集約されてユーザーに表示されます。特定のアグリゲーショングループの展開環境がほかのグループと集約されないように定義するには、アグリゲーショングループ名を、空の文字列""に設定します。

identical属性は値**true**および**false**を取り、同等の展開環境セット内のすべての展開環境のリソースセットが完全に同一であるかどうかを指定します。展開環境が同一の場合、StoreFrontは、セット内の1つのみのプライマリ展開環境からユーザーのリソースを列挙します。複数の展開環境のリソースに共通部分はあるが同一ではない場合、StoreFrontは、各展開環境から列挙して、ユーザーが利用できるリソースの完全なセットを取得します。負荷分散（起動時）は、展開が同一であるかどうかにかかわらず使用できます。**identical**属性のデフォルト値はfalseです。ただし、StoreFrontのアップグレード時には、アップグレード後に既存の動作が変更されないように**true**に設定されます。

- **primaryFarmRefs**
  リソースの一部もしくは全部が一致する、同等のXenDesktopまたはXenAppサイトのセットを指定します。ここには、ストアに追加済みの展開環境の名前を入力します。入力する展開環境の名前は、ストアに展開環境を追加する時に指定した名前と完全に一致する必要があります。
- **optimalGatewayForFarms**
  特定の展開環境のグループで提供されるリソースにユーザーがアクセスする時に使用される最適なNetScaler Gatewayアプライアンスを定義します。通常、展開環境に最適なアプライアンスは、その展開環境と地理的に同じ場所に配置されます。「最適なNetScaler Gatewayアプライアンス」は、展開環境にアクセスする時に、StoreFrontにアクセスする時に経由するNetScaler Gatewayアプライアンスと異なるアプライアンスを使用する場合のみ定義します。

異なるStoreFront展開環境のストアからユーザーのアプリケーションサブスクリプションが定期的に同期されるように構成するには、いくつかのWindows PowerShellコマンドを実行します。

注：StoreFront管理コンソールとPowerShellコンソールを同時に開くことはできません。StoreFront管理コンソールを閉じてからPowerShellコンソールを開いてください。同様に、PowerShellのすべてのインスタンスを閉じてからStoreFront管理コンソールを開いてください。
重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。
サブスクリプションを同期する場合は、ストア間でDelivery Controller名が一致している必要があります（大文字と小文字は区別されます）。Delivery Controller名が異なると、同期サイト間で異なるサブスクリプションが使用される場合があります。

1. ローカルの管理者アカウントを使ってWindows PowerShellを起動して、コマンドプロンプトで次のコマンドを実行します。これにより、StoreFrontモジュールがインポートされます。
   Import-Module "installationlocation\Management\Cmdlets\UtilsModule.psm1" Import-Module "installationlocation\Management\Cmdlets\ SubscriptionSyncModule.psm1"
   installationlocationはStoreFrontのインストール先フォルダーで、通常C:\Program Files\Citrix\Receiver StoreFront\です。

2. 次のコマンドを入力して、同期するストアを含んでいるリモートのStoreFront展開環境を指定します。
   Add-DSSubscriptionsRemoteSyncCluster -clusterName deploymentname -clusterAddress deploymentaddress
   ここで、deploymentnameはリモートの展開環境を識別するために定義する名前で、deploymentaddressはStoreFrontサーバーまたは負荷分散サーバーグループの外部アクセス可能なアドレスです。

3. 次のコマンドを入力して、同期するリモートストアを指定します。
   Add-DSSubscriptionsRemoteSyncStore -clusterName deploymentname -storeName storename
   ここで、deploymentnameは前の手順でリモート展開環境用に定義した名前であり、storename はローカルストアおよびリモートストアの作成時に指定した名前です。アプリケーションサブスクリプションをストア間で同期するには、両方のストアがそれぞれのStoreFront展開環境で同じ名前を持つ必要があります。

4. 毎日特定の時刻に同期が実行されるように構成するには、次のコマンドを入力します。
   Add-DSSubscriptionsSyncSchedule -scheduleName synchronizationname -startTime hh:mm
   synchronizationnameは作成するスケジュールを識別するために定義する名前です。-startTimeでは、ストア間でサブスクリプションを同期する時刻を指定します。追加の同期時刻を指定するには、このコマンドを繰り返します。

5. 特定の間隔で定期的に同期が実行されるように構成するには、次のコマンドを入力します。
   Add-DSSubscriptionsSyncReoccuringSchedule -scheduleName synchronizationname -startTime hh:mm:ss -repeatMinutes interval
   synchronizationnameは作成するスケジュールを識別するために定義する名前です。-startTimeでは、繰り返しスケジュールを開始する時刻を指定します。intervalでは、同期の実行間隔を分単位で指定します。

6. リモートの展開環境内の各StoreFrontサーバーのMicrosoft Active Directoryドメインマシンアカウントを、現在のサーバー上のローカルWindowsユーザーグループCitrixSubscriptionSyncUsersに追加します。
   これにより、リモートの展開環境のサーバーからローカルの展開環境のサブスクリプションストアサービスにアクセスできるようになります。
   CitrixSubscriptionSyncUsersグループは、手順1でサブスクリプションの同期モジュールをインポートする時に自動的に作成されます。ローカルユーザーグループの変更について詳しくは、http://technet.microsoft.com/ja-jp/library/cc772524.aspxを参照してください。

7. ローカルStoreFront展開環境が複数のサーバーで構成されている場合は、Citrix StoreFront管理コンソールを使用して、グループ内のほかのサーバーに構成の変更を反映させます。
   複数サーバーで構成されるStoreFront展開環境への変更の適用について詳しくは、「サーバーグループの構成」を参照してください。

8. リモートのStoreFront展開環境で手順1~7を繰り返し、リモート展開環境からローカル展開環境へのサブスクリプションの補完的な同期スケジュールを構成します。StoreFront展開環境の同期スケジュールを構成する時は、複数の展開環境で同時に同期が実行されないようにしてください。

9. ストア間でのユーザーのアプリケーションサブスクリプションの同期を開始するには、ローカルおよびリモートの展開環境でサブスクリプションストアサービスを再起動します。これを行うには、各展開環境のサーバー上でWindows PowerShellコマンドプロンプトを開き、次のコマンドを入力します。
Restart-DSSubscriptionsStoreSubscriptionService
10. 既存の同期スケジュールを削除するには、次のコマンドを入力します。その後で展開環境のほかのStoreFrontサーバーに構成の変更を反映させて、サブスクリプションストアサービスを再起動します。
Remove-DSSubscriptionsSchedule -scheduleName synchronizationname
synchronizationnameはスケジュールの作成時に定義した名前です。

11. StoreFront展開環境に構成済みの同期スケジュールを一覧表示するには、次のコマンドを入力します。
Get-DSSubscriptionsSyncScheduleSummary

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

ストアの最適なゲートウェイマッピングを定義する時のファームとゾーンの違い

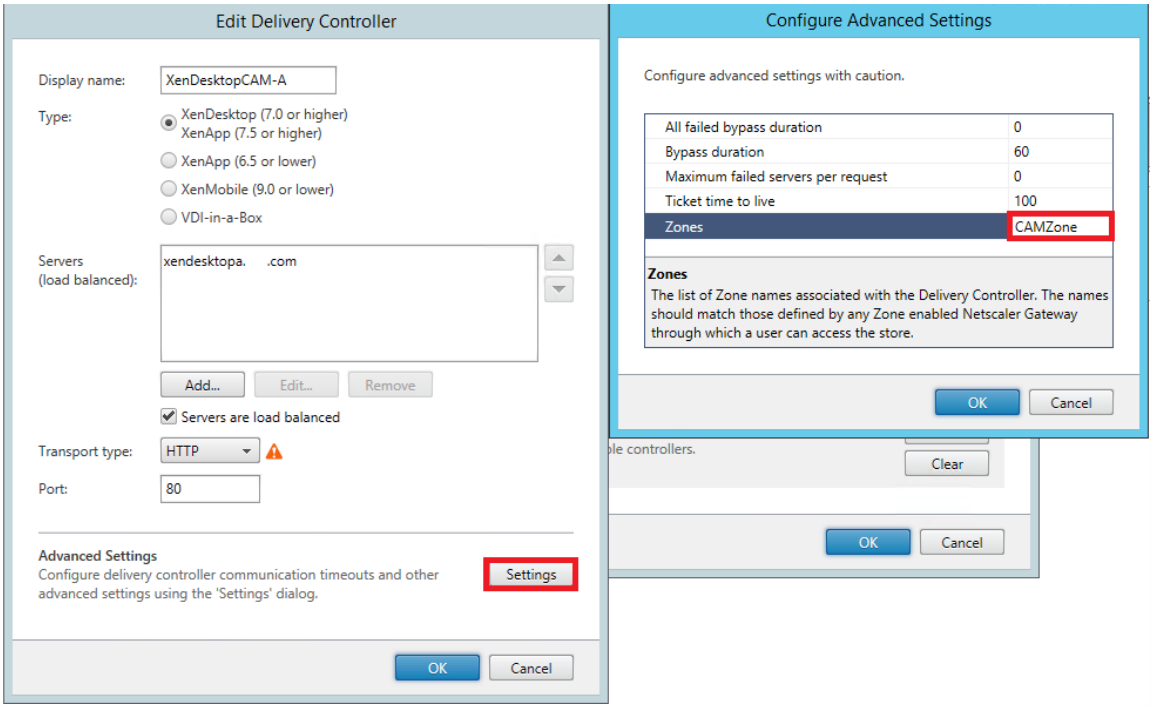
StoreFront 3.5より前にリリースされたバージョンでは、最適なゲートウェイはファームにのみマッピングできました。ゾーンの概念を利用すれば、XenApp 7.8またはXenDesktop 7.8の展開環境を、XenAppまたはXenDesktopコントローラーと公開リソースが存在するデータセンターや地理的な場所に基づいて、複数のゾーンに分割できます。ゾーンは、XenAppまたはXenDesktop 7.8 Studioで定義します。StoreFrontは現在、XenApp 7.8およびXenDesktop 7.8と相互運用できます。StoreFrontで定義されたすべてのゾーンが、XenAppおよびXenDesktopで定義されたゾーン名と正確に一致する必要があります。

このStoreFrontのバージョンでは、定義済みゾーン内に位置するすべてのDelivery Controllerに対して最適なゲートウェイマッピングを作成することもできます。最適なゲートウェイへのゾーンのマッピングは、既によく知っているファームを使用したマッピングの作成とほぼ同義です。その唯一の違いは、ゾーンは通常、もっと多くのDelivery Controllerを含む大規模なコンテナーを表すものであるということです。すべてのDelivery Controllerを最適なゲートウェイマッピングに追加する必要はありません。Controllerを目的のゾーン内に配置するには、それぞれのDelivery Controllerに、既にXenAppまたはXenDesktopに定義されているゾーンと一致するゾーン名のタグを付けるだけです。1つの最適なゲートウェイを複数のゾーンにマッピングすることができますが、通常は単一のゾーンを使用してください。一般に、ゾーンはある地理的な場所にある1つのデータセンターを表します。各ゾーンには少なくとも1つの最適なNetscaler Gatewayがあり、そのNetscaler GatewayがそのゾーンのリソースへのHDX接続に使用されることが想定されます。

ゾーンについて詳しくは、「ゾーン」を参照してください。

ゾーン内に配置するすべてのDelivery Controllerに対して、ゾーン属性を設定します。

1. Windowsの **[スタート]** 画面または［アプリ］画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、 **[操作]** ペインの **[Delivery Controllerの管理]** をクリックします。
3. Controllerを選択し、 **[編集]** をクリックして、 **[Delivery Controllerの編集]** 画面の **[設定]** をクリックします。
4. **[ゾーン]** 行で、2つ目の列をクリックします。
5. **[Delivery Controllerゾーン名]** 画面の **[追加]** をクリックして、ゾーン名を追加します。



ストアのNetScaler Gatewayルーティングを構成して、HDXエンジンから公開リソース（XenDesktop VDA、およびXenAppやXenDesktopの公開アプリケーション）にアクセスするICA接続の処理を最適化します。通常、最適なゲートウェイはサイトと地理的に同じ場所に配置されます。

「最適なNetScaler Gatewayアプライアンス」は、ユーザーがStoreFrontにアクセスする時に最適なゲートウェイが使用されない展開環境でのみ定義します。起動要求がその要求元のゲートウェイ経由で返送する必要がある場合、StoreFrontがこれを自動的に行います。

ファーム使用のシナリオ例

1×UKゲートウェイ -> 1×UK StoreFront	-> UKアプリおよびデスクトップ（ローカル）
	–> USアプリおよびデスクトップ（UKユーザーのフェールオーバーとして）
1×USゲートウェイ -> 1×US StoreFront	-> USアプリおよびデスクトップ（ローカル）
	–> UKアプリおよびデスクトップ（USユーザーのフェールオーバーとして）

UKゲートウェイは、UKでホストされるリソース（UK StoreFrontによるアプリやデスクトップ）へのリモートアクセスを提供します。

UK StoreFrontにはUKおよびUSベースのNetScaler Gatewayが定義されており、Delivery Controllerの一覧にUKおよびUSのファームが含まれています。UKのユーザーは、地理的に同じ場所に配置されたゲートウェイ、StoreFront、およびファームを使用してリモートリソースにアクセスします。UKのリソースが使用不能になった場合は、フェールオーバーとして一時的にUSのリソースにアクセスできるようになります。

最適なゲートウェイルーティング構成を行わない場合、すべてのICA起動要求はリソースの場所がUKでもUSでも起動要求元のUKゲートウェイを経由します。デフォルトでは、起動要求時にその要求元のゲートウェイがStoreFrontにより動的に識別されます。最適なゲートウェイルーティング構成によりこの動作が無視され、USリソースへの接続がUSファームに地理的に近いゲートウェイを経由するようになります。

注：最適なゲートウェイとしてマップできるのは、各サイトのStoreFrontストアについて1つのみです。

ゾーン使用のシナリオ例

1×CAMZone -> 2×UK StoreFront	-> ケンブリッジ（UK）：アプリおよびデスクトップ
	-> フォートローダーデール（US東部）：アプリおよびデスクトップ
	-> バンガロール（インド）：アプリおよびデスクトップ

1×FTLZone -> 2×US StoreFront	-> フォートローダーデール（US東部）：アプリおよびデスクトップ -> ケンブリッジ（UK）：アプリおよびデスクトップ -> バンガロール（インド）：アプリおよびデスクトップ
1×BGLZone -> 2×IN StoreFront	-> バンガロール（インド）：アプリおよびデスクトップ -> ケンブリッジ（UK）：アプリおよびデスクトップ -> フォートローダーデール（US東部）：アプリおよびデスクトップ

図1：次善のNetScaler Gatewayルーティング

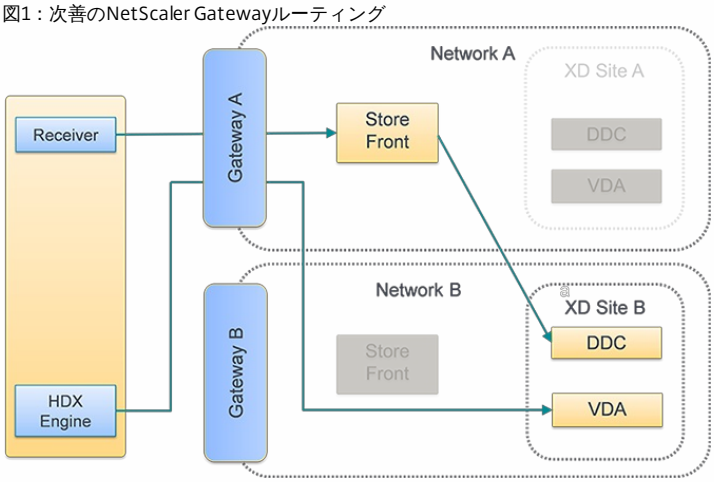
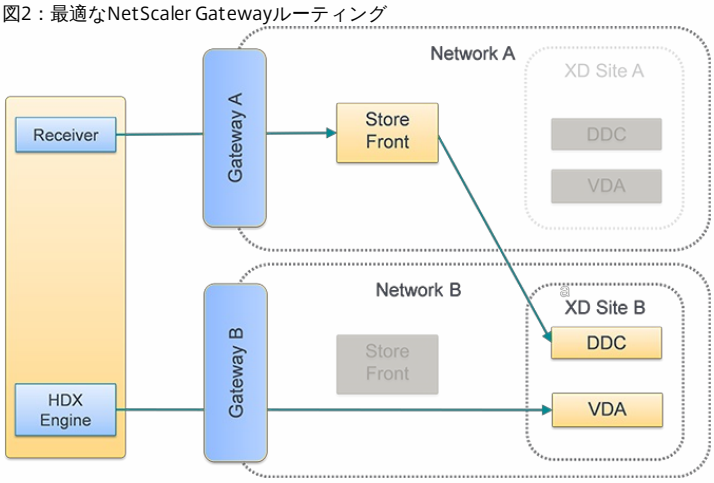
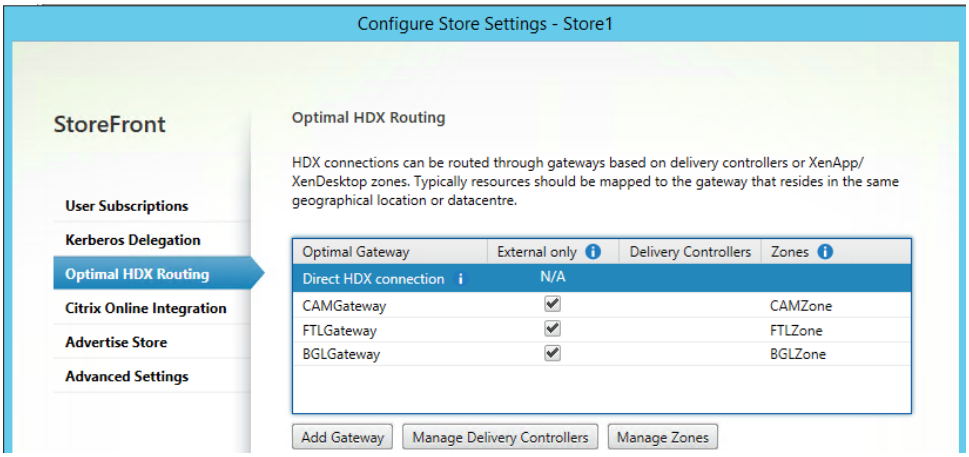


図2：最適なNetScaler Gatewayルーティング



複数の展開環境で個別のNetScaler Gatewayアプライアンスを構成した後に、ユーザーが各展開環境にアクセスするための最適なアプライアンスを定義できます。

1. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、結果ペインでストアを選択します。**[操作]** ペインで、 **[ストア設定の構成]** を選択します。
3. **[設定]** > **[最適なHDXルーティング]** ページで、ゲートウェイを選択します。
4. **[直接アクセス]** チェックボックスを選択すると、**-enabledOnDirectAccess = false**と同等の操作になります。また、［ゲートウェイを使用しない］を選択すると、ファームまたはゾーンで**Set-DSFarmsWithNullOptimalGateway**を使用する場合と同等の操作になります。



［ゲートウェイの追加］

前の手順のオプションの1つは、**［ゲートウェイの追加］**です。**［ゲートウェイの追加］**を選択すると、［NetScaler Gatewayの追加］画面が表示されます。

1. **［全般設定］**画面で、［表示名］、［NetScaler Gateway URL］、および［使用法］または［役割］設定を入力して、パブリックネットワークから接続しているユーザーに対するNetScaler Gateway経由でのストアへのアクセスを構成します。認証不要なストアでは、NetScaler Gatewayを介したリモートアクセスは許可されません。
2. **［Secure Ticket Authority（STA）］**画面で、表示されているオプションを入力します。STAは、XenDesktopおよびXenAppサーバーでホストされ、接続要求に応答してセッションチケットを発行します。セッションチケットは、XenDesktopおよびXenAppリソースへのアクセスを認証および承認するための基本機能です。
3. **［認証設定］**画面で、リモートユーザーによる認証資格情報の提供方法を指定する設定を入力します。

PowerShell APIパラメーター

Parameter	Description
-SiteId（Int）	IISでのサイトIDです。StoreFrontのインストール先のIISでは、通常「1」です。
-ResourcesVirtualPath（String）	最適なゲートウェイマッピングのファームを構成するストアのパスです。 例："/Citrix/Store"
-GatewayName（String）	StoreFrontでNetscaler Gatewayを識別するために設定された名前です。 例1：ExternalGateway 例2：InternalGateway
-Hostnames（String Array）	最適なNetScaler Gatewayアプライアンスの完全修飾ドメイン名（FQDN）とポート番号を指定します。 標準的なvServerポート443の例1：gateway.example.com 非標準的なvServerポート500の例2：gateway.example.com:500
-Farms（String Array）	指定するNetScaler Gatewayアプライアンスを共有し、通常は同じ場所に配置されているXenDesktop、XenApp、App Controllerの展開環境の一覧を指定します。公開リソースを提供する1つまたは複数のDelivery Controllerを持つファームを指定できます。 複数のDelivery Controllerを持つXenDesktopサイトを構成するには、「"XenDesktop"」を指定します。これは単一ファームを表します。 フェールオーバー一覧に複数のDelivery Controllerを指定できます。 例："XenDesktop" XenDesktop-A.example.com XenDesktop-B.example.com XenDesktop-C.example.com
-Zones（String Array）	多数のDelivery Controllerを含む1つまたは複数のデータセンターを指定します。StoreFrontで、Delivery Controllerオブジェクトに、割り当て先となる適切なゾーンのタグを付ける必要があります。
-staUrls（String Array）	STAを実行しているXenDesktop、XenApp、およびVDI-in-a-BoxサーバーのURLの一覧を指定します。複数のファームを使用している場合は、各ファームのSTAサーバーをカンマで区切って入力します。 例："http://xenapp-a.example.com/scripts/ctxsta.dll","http://xendesktop-a.example.com/scripts/ctxsta.dll"
-StasUseLoadBalancing（Boolean）	trueを設定すると、すべてのSTAからセッションチケットがランダムに取得されます。これにより、すべてのSTAで要求が均等に分散されます。 falseを設定すると、構成時の一覧の順序でSTAが選択されます。これにより、使用されるSTAの数が常に最小になります。
-StasBypassDuration	STA要求が失敗した場合に、そのSTAが使用できないとみなされるまでの時間を時間、分、秒で設定します。 例：02:00:00
-EnableSessionReliability（Boolean）	trueを設定すると、Receiverが再接続を試行する間、切断セッションが開いたままになります。複数のSTAを構成した展開環境でセッション画面の保持機能を常に使用できるようにするには、useTwoTickets属性をtrueに設定します。これにより、2つのSTAからチケットが取得されるため、一方のSTAが使用できなくなってもユーザーセッションが中断されなくなります。
-UseTwoTickets（Boolean）	trueを設定すると、2つのSTAからチケットが取得されるため、セッション中に一方のSTAが使用できなくなっても中断されなくなります。 falseを設定すると、単一のSTAサーバーのみが使用されます。
-EnabledOnDirectAccess（Boolean）	trueに設定すると、内部ネットワーク上のローカルユーザーがStoreFrontに直接ログオンする時に、そのファームに定義されている最適なアプライアンスを介してルーティングされるようになります。 falseに設定すると、StoreFrontにNetScaler Gateway経由でアクセスするユーザーを除き、最適なアプライアンスを介してルーティングされません。

PowerShellスクリプトが複数行にまたがる場合は、各行末にバッククォート文字を入力してください。

サンプルコードを実行する前に、Windows PowerShell Integrated Scripting Environment（ISE）にコピーして形式チェッカーを使ってPowershellコードを検証することをお勧めします。

注意

Set-DSOptimalGatewayForFarmsという以前のPowerShellコマンドレットでは、［最適なHDXルーティング］は構成できません。

この問題の回避方法は次のとおりです。

1. Add-DSGlobalV10Gatewayコマンドを使用して、［最適なHDXルーティング］に使用する設定でグローバルゲートウェイを構成し、認証設定のデフォルト値を入力します。
2. Add-DSStoreOptimalGatewayコマンドを使用して、最適なゲートウェイ構成を追加します。

例：

```
Add-DSGlobalV10Gateway -Id 2eba0524-af40-421e-9c5f-a1ccca80715f -Name LondonGateway -Address "http://example" -Logon Domain -SecureTicketAuthorityUrls
@("http://staurl1", "http://staurl2")
```

```
Add-DSStoreOptimalGateway -SiteId 1 -VirtualPath /Citrix/Store1 -GatewayId 2eba0524-af40-421e-9c5f-a1ccca80715f -Farms @("Controller") -EnabledOnDirectAccess $true
```

たとえば、次のように指定します。

ストアInternalのOptimalGatewayForFarmsマッピングを作成または上書きします。

```
& "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\ImportModules.ps1"

Set-DSOptimalGatewayForFarms -SiteId 1 `

        -ResourcesVirtualPath /Citrix/Internal `
        -GatewayName "gateway1" `
        -Hostnames "gateway1.example.com:500" `
        -Farms "XenApp","XenDesktop" `
        -StaUrls "https://xenapp.example.com/scripts/ctxsta.dll","https://xendesktop.example.com/scripts/ctxsta.dll" `
        -StasUseLoadBalancing:$false `
        -StasBypassDuration 02:00:00 `
        -EnableSessionReliability:$false `
        -UseTwoTickets:$false `
        -EnabledOnDirectAccess:$true
```

ゾーンの最適なゲートウェイの構成

例：

ゾーンCAMZoneのOptimalGatewayForFarmsマッピングを作成または上書きします。

```
& "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\ImportModules.ps1"

Set-DSOptimalGatewayForFarms -SiteId 1 `

        -ResourcesVirtualPath /Citrix/Internal `
        -GatewayName "gateway1" `
        -Hostnames "gateway1.example.com:500" `
        -Zones "CAMZone" `
        -StaUrls "https://xenapp.example.com/scripts/ctxsta.dll","https://xendesktop.example.com/scripts/ctxsta.dll" `
        -StasUseLoadBalancing:$false `
        -StasBypassDuration 02:00:00 `
        -EnableSessionReliability:$false `
        -UseTwoTickets:$false `
        -EnabledOnDirectAccess:$true
```

例：

ストアInternalで、OptimalGatewayForFarmsマッピングの一覧を返します。

```
Get-DSOptimalGatewayForFarms -SiteId 1 –ResourcesVirtualPath "/Citrix/Internal"
```

例：

ストアInternalのOptimalGatewayForFarmsマッピングをすべて削除します。

```
Remove-DSOptimalGatewayForFarms -SiteId 1 -ResourcesVirtualPath "/Citrix/Internal"
```

ファームの直接HDX接続の構成

例：

ストアInternalで、特定ファームへのすべてのICA起動要求がゲートウェイを経由せずに送信されるようにします。

```
Set-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath /Citrix/Store -Farms "Farm1","Farm2"
```

例：

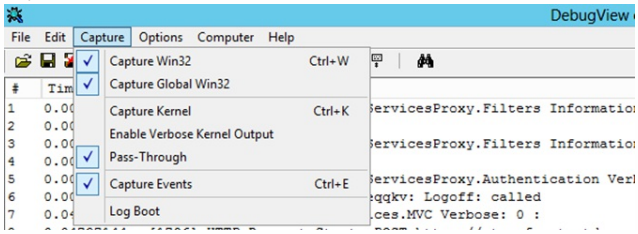
ストアInternalで、ゲートウェイを経由せずにICA起動要求が送信されるファームの一覧を返します。

```
Get-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath "/Citrix/Internal"
```

OptimalGatewayForFarmsマッピングが使用されているかどうかを確認する

1. 次のPowerShellコマンドを実行して、すべてのサーバーグループノードでStoreFrontのトレース機能を有効にします。
   & "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\ImportModules.ps1"

   #トレースはc:\Program Files\Citrix\Receiver Storefront\admin\trace\に出力されます
   Set-DSTraceLevel -All -TraceLevel Verbose
2. StoreFrontサーバーのデスクトップで、Debug Viewツールを開きます。StoreFrontサーバーグループを使用している場合は、起動要求を受信したノードのトレース情報を取得できるように、すべてのノード上でDebug Viewツールを開く必要があります。
3. Capture Global Win32イベントを有効にします。



4. トレース出力をLOGファイルとして保存して、メモ帳などのテキストエディターで開きます。以下のサンプルシナリオを参照して、ログエントリを検索します。
5. ログの確認が終わったら、トレース機能を無効にします。トレース機能を有効にしておくと、StoreFrontサーバー上のディスク領域が消費されます。
   Set-DSTraceLevel -All -TraceLevel Off

最適なゲートウェイのサンプルシナリオ

- 外部クライアントはGateway1にログオンします。ファームFarm2への起動要求が、定義されている最適なゲートウェイGateway2経由で送信されます。
  Set-DSOptimalGatewayForFarms -onDirectAccess=false

  Farm2の最適なゲートウェイとしてGateway2が構成されています。

  Farm2の最適なゲートウェイでは、直接アクセスが無効になっています。

  起動要求は、最適なゲートウェイGateway2を経由します。

- 内部クライアントはStoreFrontを使用してログオンします。ファームFarm1への起動要求が、定義されている最適なゲートウェイGateway1経由で送信されます。
  Set-DSOptimalGatewayForFarms -onDirectAccess=true

  動的に識別されるゲートウェイは要求内にありません。StoreFrontには直接アクセスされます。

  Farm1の最適なゲートウェイとしてGateway1が構成されています。

  Farm1の最適なゲートウェイでは、直接アクセスが有効になっています。

  起動要求は、最適なゲートウェイGateway1を経由します。

- 内部クライアントはGateway1を使用してログオンします。Farm1のリソースの起動要求はいずれのゲートウェイも経由せず、StoreFrontには直接アクセスされます。
  Set-DSFarmsWithNullOptimalGateway

  要求内で動的に識別されるゲートウェイ：Gateway1

  Farm1では、ゲートウェイが使用されません。起動要求が経由するゲートウェイはありません。

NetScaler GatewayおよびNetScalerの統合

Aug 14, 2017

NetScaler GatewayをStoreFrontと一緒に使って、企業ネットワークとNetScalerの外側にいるユーザーにセキュアなリモートアクセスを提供し、負荷分散を実行します。

StoreFrontをNetScaler GatewayおよびNetScalerと統合するには、ゲートウェイとサーバー証明書の使用方法について計画を立てる必要があります。展開環境内のどのCitrixコンポーネントでサーバー証明書を要求するかを検討してください。

- インターネットに接続するサーバーおよびゲートウェイの証明書を外部の証明機関から取得する計画を立ててください。クライアントデバイスでは、内部証明機関により署名された証明書は自動で信頼されない場合があります。
- 外部および内部の両方のサーバー名を用意してください。多くの組織では、example.com（外部用）とexample.net（内部用）というように内部用と外部用の名前空間が分けられています。サブジェクトの別名（SAN）拡張機能を使用すると、これら両種の名前を1つの証明書に含めることができます。これは推奨される構成ではありません。公的証明機関から証明書が発行されるのは、最上位ドメイン（TLD：top-level domain）がIANAに登録されている場合のみです。この場合でも、一般的に使用される内部サーバー名の一部（example.localなど）は使用できないため、外部名と内部名で別々の証明書が必要になることがあります。
- 可能であれば、外部サーバーと内部サーバーには別の証明書を使用してください。ゲートウェイでは、各インターフェイスに異なる証明書をバインドすることで複数の証明書を使用できる場合があります。
- インターネットに接続するサーバーと接続しないサーバー間で証明書を共有しないでください。これらの証明書は、有効期間や失効ポリシーなどが内部証明機関から発行された証明書とは異なる可能性があります。
- 「ワイルドカード」証明書を共有するのは、同等のサービス間のみにしてください。異なる種類のサーバー間（StoreFrontサーバーとその他の種類のサーバーなど）で証明書を共有しないでください。異なる管理下にあるサーバー間やセキュリティポリシーが違うサーバー間で証明書を共有しないでください。 同等のサービスを提供するサーバーの典型的な例は以下のとおりです。
  - StoreFrontサーバーのグループとこれらのサーバー間で負荷分散を実行するサーバー。
  - GSLB内のインターネットに接続するゲートウェイのグループ。
  - 同等のリソースを提供するXenAppおよびXenDesktop 7.x Controllerのグループ。
- ハードウェアセキュリティで保護された秘密キーストレージを用意してください。一部のNetScalerモデルを含むゲートウェイとサーバーでは、ハードウェアセキュリティモジュール（HSM：Hardware Security Module）またはトラステッドプラットフォームモジュール（TPM：Trusted Platform Module）内に秘密キーを格納して保護することができます。セキュリティ上の理由から、こうした構成は、一般に証明書および秘密キーの共有をサポートするようには設定されていません。各コンポーネントのドキュメントを参照してください。 NetScaler Gatewayを使用してGSLBを実装する場合、使用するFQDNがすべて含まれる同一の証明書をGSLB内の各ゲートウェイに設定する必要のある場合があります。

Citrix展開環境のセキュリティ保護について詳しくは、「End-To-End Encryption with XenApp and XenDesktop」ホワイトペーパーおよびXenAppとXenDesktopの「セキュリティ保護」セクションを参照してください。

NetScaler Gateway接続の追加

Aug 14, 2017

ユーザーがストアにアクセスするときに経由するNetScaler Gateway展開環境を追加するには、[NetScaler Gatewayアプライアンスの追加]タスクを使用します。NetScaler Gatewayを経由するストアへのリモートアクセスを構成するには、その前に認証方法としてNetScaler Gatewayからのパススルーを有効にする必要があります。StoreFrontでのWebFront Gatewayの構成について詳しくは、「Using WebFront to Integrate with StoreFront」を参照してください。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、［操作］ペインの［NetScaler Gatewayの管理］をクリックします。
3. **［追加］**をクリックし、［全般設定］で、NetScaler Gateway展開環境にわかりやすい名前を指定します。
   ここで指定する表示名がユーザーのCitrix Receiverに表示されます。そのため、ユーザーが使用するNetScaler Gatewayを判断しやすいように、名前に関連情報を含める必要があります。たとえば、ユーザーが自分のいる場所に最も便利なNetScaler Gatewayを簡単に特定できるように、表示名に地理情報を含めることができます。

4. 展開環境の仮想サーバーまたはユーザーログオンポイント（Access Gateway 5.0の場合）のURLを入力します。展開環境で使用する製品のバージョンを指定します。
   StoreFront展開環境のFQDN（Fully Qualified Domain Name：完全修飾ドメイン名）は一意で、NetScaler Gateway仮想サーバーのFQDNと異なるものである必要があります。StoreFrontとNetScaler Gateway仮想サーバーに同じFQDNを使用することはサポートされていません。

5. 展開環境でAccess Gateway 5.0が実行されている場合は、手順9.に進みます。それ以外の場合は、必要に応じてNetScaler GatewayアプライアンスのサブネットIPアドレスを指定します。サブネットIPアドレスは、Access Gateway 9.3アプライアンスの場合は必須ですが、それより後の製品バージョンではオプションです。
   このサブネットアドレスは、NetScaler Gatewayで内部ネットワークのサーバーと通信するときに、ユーザーデバイスを表すために使用するIPアドレスです。このアドレスは、NetScaler GatewayアプライアンスのマップされたIPアドレスである場合もあります。StoreFrontは、サブネットIPアドレスを使用して、受信要求が信頼されているデバイスから発信されているかどうかを検証します。

6. NetScaler Gateway 10.1～11.0、Access Gateway 10～11.0、またはAccess Gateway 9.3のアプライアンスを追加する場合は、［ログオンの種類］の一覧から、Citrix Receiverユーザー用にアプライアンスで構成した認証方法を選択します。
   NetScaler Gatewayアプライアンスに関する構成情報は、ストアのプロビジョニングファイルに追加されます。これにより、Citrix Receiverは、アプライアンスへの初回接続時に適切な接続要求を送信できるようになります。

   - ユーザーのMicrosoft Active Directoryドメインの資格情報を入力させる場合は、［ドメイン］を選択します。
   - セキュリティトークンから取得するトークンコードを入力させる場合は、［セキュリティトークン］を選択します。
   - ユーザーのドメイン資格情報とセキュリティトークンから取得するトークンコードの両方を入力させる場合は、［ドメインおよびセキュリティトークン］を選択します。
   - テキストメッセージで送信されるワンタイムパスワードを入力させる場合は、［SMS認証］を選択します。
   - スマートカードを挿入してPINを入力させる場合は、［スマートカード］を選択します。

   スマートカードでの認証に問題が生じた場合に代替の認証方法を使用できるようにするには、［スマートカードフォールバック］の一覧から代替の認証方法を選択します。手順2.に進みます。

7. Access Gateway 5.0のアプライアンスを追加する場合は、ユーザーのログオンポイントのホスト（スタンドアロンのアプ

ライアンスまたはクラスターの一部であるAccess Controllerサーバー）を指定します。クラスターを追加する場合は、［次へ］をクリックして手順9.に進みます。

8. NetScaler Gateway 10.1～11.0、Access Gateway 10～11.0、Access Gateway 9.3、またはスタンドアロンAccess Gateway 5.0アプライアンスを追加する場合は、［コールバックURL］ボックスにNetScaler Gateway認証サービスのURLを入力します。URLの標準的な部分は自動的に補完されます。［次へ］をクリックして手順11.に進みます。
   アプライアンスの内部URLを入力します。StoreFrontはNetScaler Gateway認証サービスに接続して、NetScaler Gatewayからの要求の送信元がそのアプライアンスであることを確認します。

9. StoreFrontにAccess Gateway 5.0クラスターを追加する場合は、［アプライアンス］ページでクラスター内のアプライアンスのIPアドレスまたはFQDNを一覧に追加して、［次へ］をクリックします。
10. ［サイレント認証を有効にする］ページで、Access Controllerサーバーで実行されている認証サービスのURLを一覧に追加します。一覧に複数のサーバーのURLを追加すると、その順番に基づいてフェールオーバーされます。［Next］をクリックします。
    StoreFrontでは認証サービスを使用してリモートユーザーが認証されるため、リモートユーザーがストアにアクセスするときに資格情報を再入力する必要はありません。

11. すべての展開環境で、XenDesktopまたはXenAppが提供するリソースをストアで使用できるようにするには、［Secure Ticket Authority（STA）］ページで、STAを実行しているサーバーのURLを一覧に追加します。一覧に複数のSTAのURLを追加すると、その順番に基づいてフェールオーバーされます。
    STAは、XenDesktopおよびXenAppサーバーでホストされ、接続要求に応答してセッションチケットを発行します。セッションチケットは、XenDesktopおよびXenAppリソースへのアクセスを認証および承認するための基本機能です。

12. Citrix Receiverが自動的に再接続を実行する間に、切断したセッションをXenDesktopおよびXenAppで開いたままにするには、［セッション画面の保持を有効にする］チェックボックスをオンにします。複数のSTAを構成した環境でセッション画面の保持機能を常に使用できるようにするには、［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにします。
    ［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにすると、セッションの途中で1つのSTAが使用できなくなってもユーザーセッションが中断されないように、StoreFrontにより2つの異なるSTAからセッションチケットが取得されます。StoreFrontがどちらのSTAにもアクセスできない場合は、単一のSTAを使用するようにフォールバックされます。

13. ［作成］をクリックして、NetScaler Gateway展開環境の詳細を追加します。展開環境が追加されたら、［完了］をクリックします。
    展開環境の詳細を更新する方法について詳しくは、「NetScaler Gateway接続設定の構成」を参照してください。

NetScaler Gatewayを介したストアへのアクセスを提供するには、1つの内部ビーコンポイントと、2つ以上の外部ビーコンポイントが必要です。Citrix Receiverは、ユーザーがローカルネットワークと公共のネットワークのどちらに接続しているのかをビーコンポイントを使用して識別し、適切なアクセス方法を選択します。StoreFrontでは、内部ビーコンポイントとしてデフォルトでサーバーのURLまたは負荷分散URLが使用されます。外部ビーコンポイントは、デフォルトでCitrix社のWebサイト、および管理者が追加した最初のNetScaler Gateway仮想サーバーまたはユーザーログオンポイント（Access Gateway 5.0の場合）のURLが使用されます。ビーコンポイントの変更について詳しくは、「ビーコンポイントを構成」を参照してください。

ユーザーがNetScaler Gatewayを介してストアにアクセスできるようにするには、そのストアのリモートユーザーアクセスを構成する必要があります。

NetScaler Gatewayアプライアンスのインポート

Aug 14, 2017

NetScaler管理コンソールのリモートアクセス設定は、StoreFrontで構成されているものと同じように構成する必要があります。この記事では、NetScalerとStoreFrontを適切に構成して連携させるためにNetScaler Gatewayをインポートする方法について説明します。

- 複数のゲートウェイ仮想サーバーをZIPファイルにエクスポートするには、NetScaler 11.1.51.21以降が必要です。**注：** NetScalerでエクスポートできるゲートウェイ仮想サーバーは、XenAppおよびXenDesktopのウィザードを使用して作成したもののみです。
- NetScalerにより生成されるZIPファイル内のGatewayConfig.jsonファイルに記載されているすべてのSTA（Secure Ticket Authority）サーバーのURLをDNSが解決でき、StoreFrontがアクセスできる必要があります。
- NetScalerで生成されるZIPファイル内のGatewayConfig.jsonファイルには、StoreFrontサーバー上にある既存のCitrix Receiver for WebサイトのURLが含まれている必要があります。バージョン11.1以降のNetScalerは、エクスポート用のZIPファイルの生成前にStoreFrontサーバーにアクセスして既存のストアとCitrix Receiver for Webサイトをすべて列挙し、この処理を自動で行います。
- StoreFrontで、インポートしたゲートウェイを使用して認証できるように、ゲートウェイVPN仮想サーバーのIPアドレスへのDNSのコールバックURLを解決できる必要があります。

    StoreFrontでゲートウェイURLを解決できる場合、使用するコールバックURLとポートの組み合わせは、通常、ゲートウェイURLとポートの組み合わせと同じものにします。

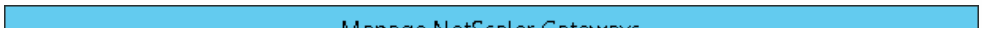
    または

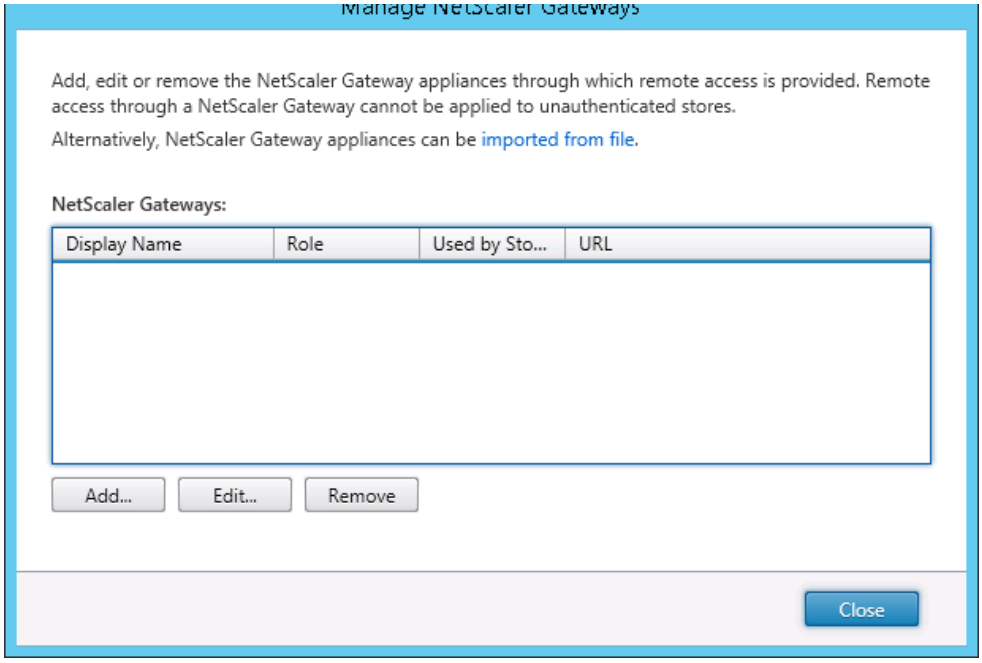
    環境内で外部と内部に違うDNS名前空間を使用する場合は、コールバックURLとポートの組み合わせをゲートウェイURLとポートの組み合わせとは異なるものにしても構いません。ゲートウェイをDMZ内に配置してのURLを使用しており、StoreFrontはプライベートの社内ネットワークに配置してのURLを使用している場合、コールバックURLを使用してDMZ内のゲートウェイ仮想サーバーへポイントバックすることができます。

NetScaler構成ファイルをインポートすることによって、NetScaler Gatewayアプライアンスをインポートすることができます。

> **Important**
>
> 注：NetScalerからインポートされた構成ファイルを手で編集することはできません。

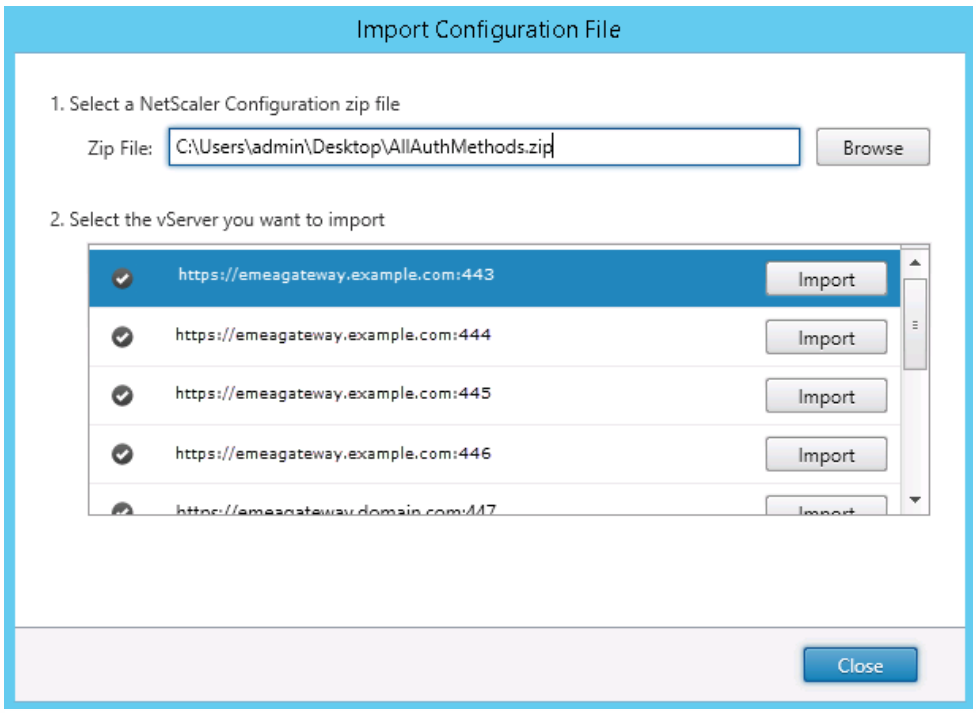
1. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、 **[操作]** ペインの **[NetScaler Gatewayの管理]** をクリックします。
2. ［NetScaler Gatewayの管理］画面で、 **[ファイルからインポート]** リンクをクリックします。





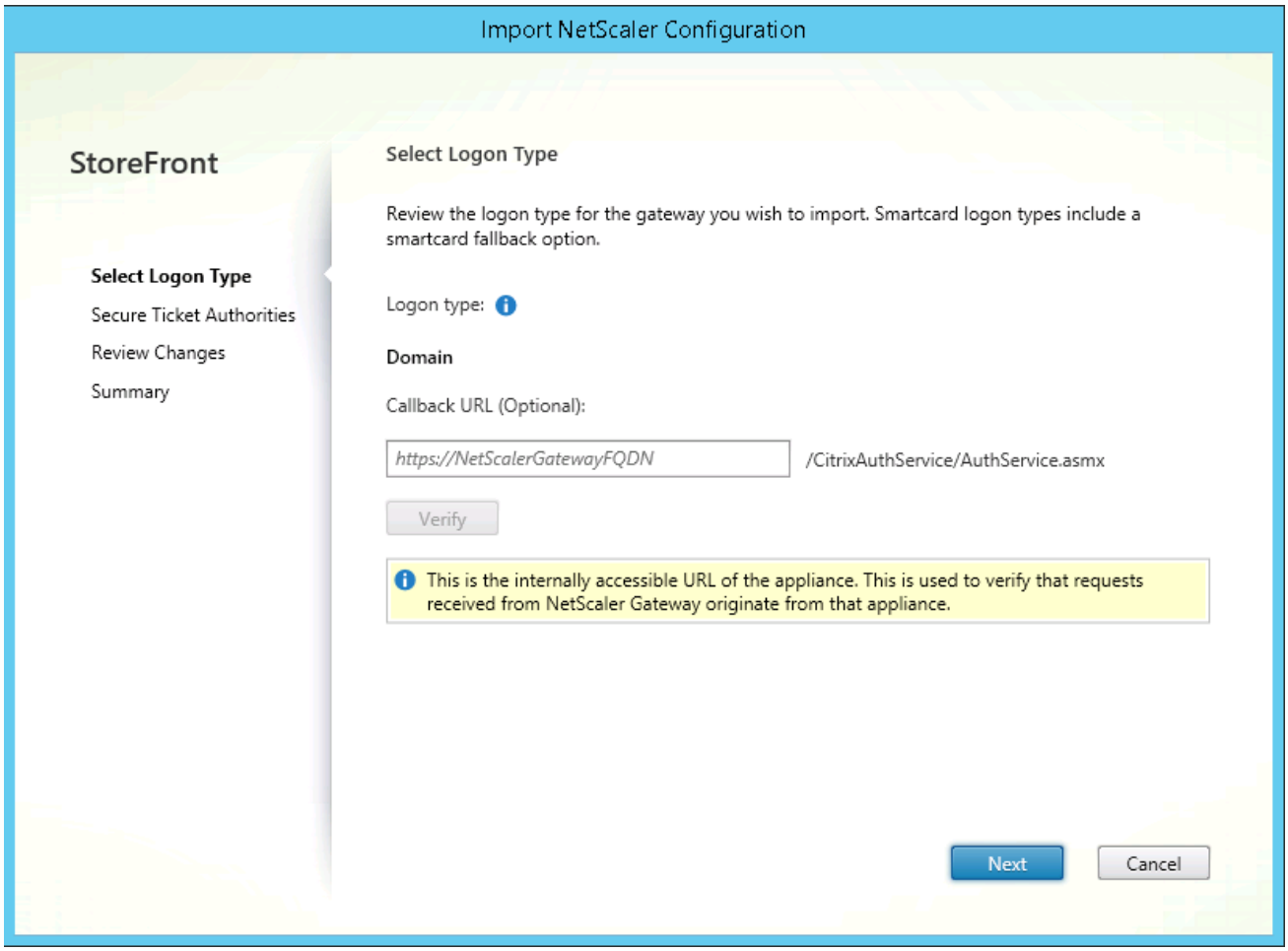
3. 1. NetScaler 構成の zip ファイルを選択してください

4. 選択したZIPファイルに含まれるゲートウェイ仮想サーバーの一覧が表示されます。インポートするゲートウェイ仮想サーバーを選択し、 **[インポート]** をクリックします。仮想サーバーを繰り返してインポートする場合、［インポート］ボタンは［更新］ボタンになります。 **[更新]** をクリックした場合、後でゲートウェイを上書きするか新規に作成することができます。



5. 選択したゲートウェイのログオンの種類を確認し、必要に応じてコールバックURLを指定します。［ログオンの種類］の一覧から、Citrix Receiverユーザー向けにアプライアンス上で構成した認証方法を選択します。ログオンの種類によってはコールバックURLが必要になります（表を参照）。

- [確認] をクリックして、コールバックURLが有効でありStoreFrontサーバーから到達可能であることをチェックします。



コンソールでの［ログオンの種類］	JSONファイルでのLogonType	ｺｰﾙﾊﾞｯｸ URL(必須)(_U):
ドメイン	ドメイン	なし
ドメインおよびセキュリティ トークン	DomainAndRSA	なし
セキュリティトークン	RSA	はい
スマートカード - フォールバックがありません	スマートカードの使用	はい
スマートカード - ドメイン	SmartCardDomain	はい
スマートカード - ドメインおよびセキュリティ トークン	SmartCardDomainAndRSA	はい

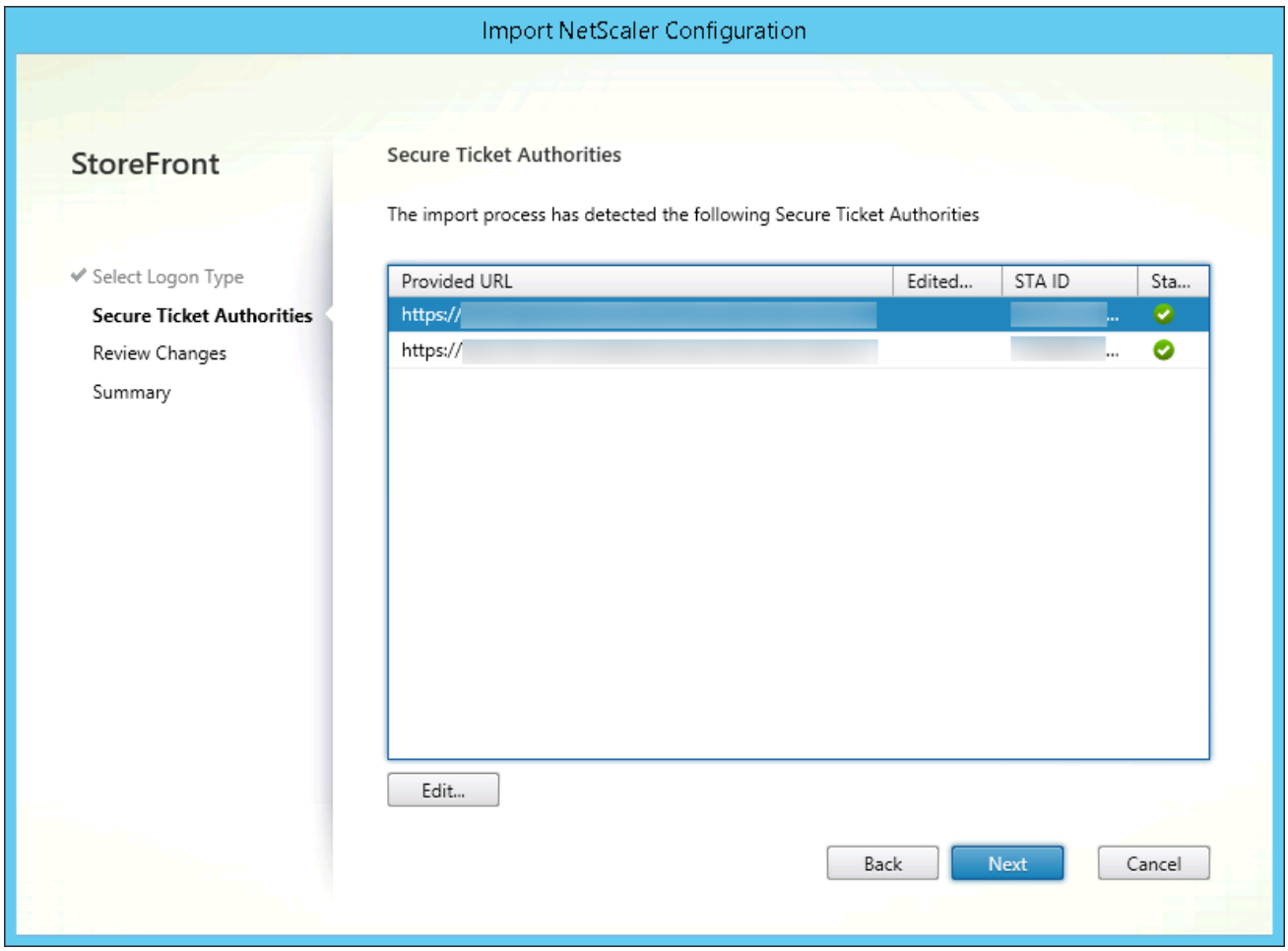
スマートカード - セキュリティ トークン	SmartCardRSA	はい
スマートカード - SMS 認証	SmartCardSMS	はい
SMS 認証	SMS：	はい

コールバックURLが必要な場合、ZIPファイルに記載されているゲートウェイURLに基づいてStoreFrontによりコールバックURLが自動で入力されます。このURLは、NetScaler Gateway仮想サーバーのIPにポイントバックする有効なURLに変更できます。

スマートアクセスを使用する場合、コールバックURLは必須です。

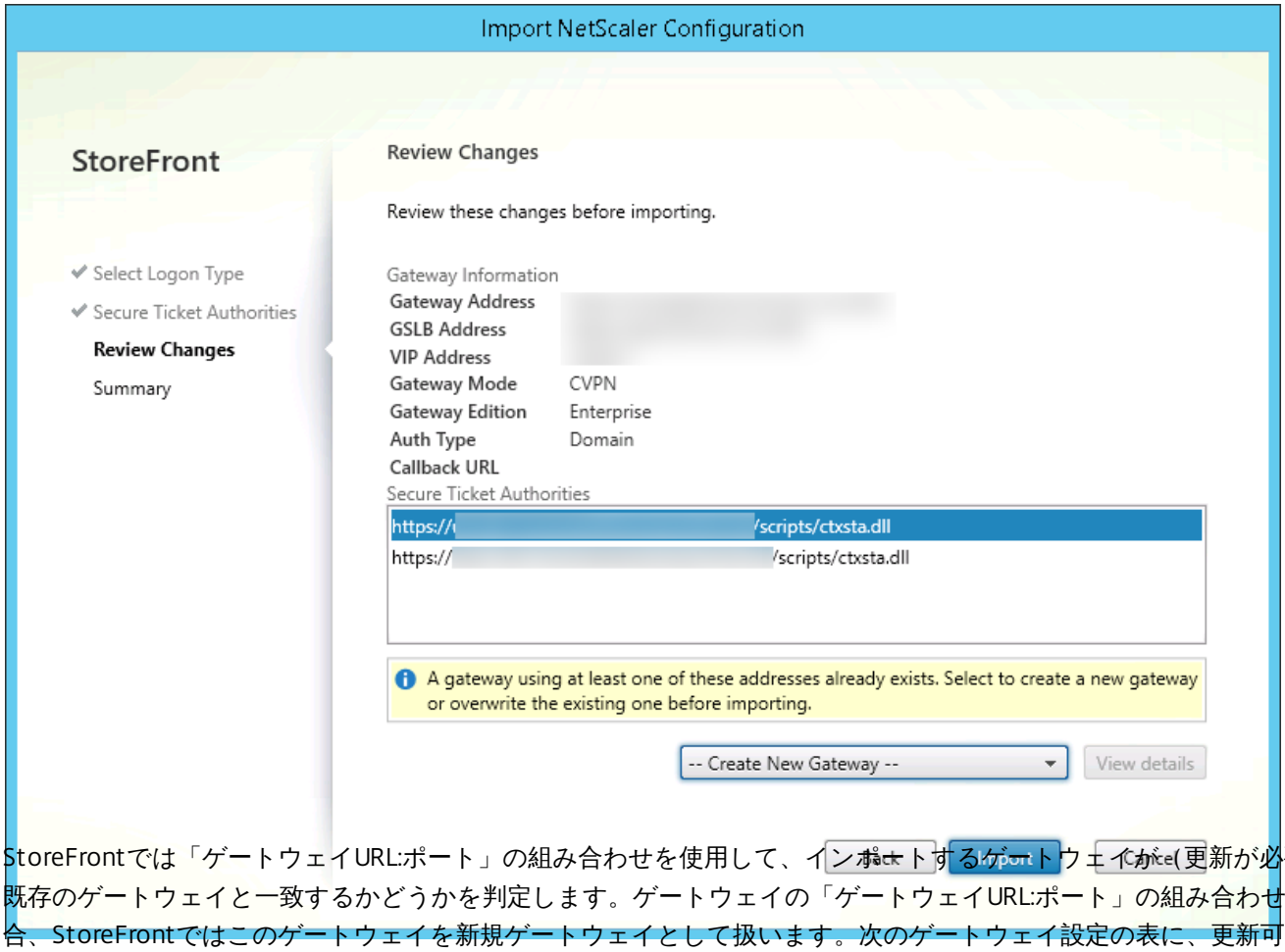
6. [Next] をクリックします。

7. StoreFrontが、ZIPファイルに記載されているすべてのSTA（Secure Ticket Authority）サーバーのURLへDNSを使用してアクセスし、これらのサーバーが動作中のSTAチケット発行サーバーであることを確認します。いずれかのSTA URLが無効である場合、インポートは中断されます。



8. [Next] をクリックします。

9. インポートの詳細を確認します。ゲートウェイURLとポートの組み合わせ（ゲートウェイ:ポート）の同じゲートウェイが既に存在する場合は、ボックスの一覧からゲートウェイを選択して上書きするか、新規ゲートウェイを作成します。



StoreFrontでは「ゲートウェイURL:ポート」の組み合わせを使用して、インポートするゲートウェイが（更新が必要になる）既存のゲートウェイと一致するかどうかを判定します。ゲートウェイの「ゲートウェイURL:ポート」の組み合わせが異なる場合、StoreFrontではこのゲートウェイを新規ゲートウェイとして扱います。次のゲートウェイ設定の表に、更新可能な設定を示します。

ゲートウェイの設定	更新の可否
「ゲートウェイURL:ポート」の組み合わせ	なし
GSLBのURL	はい
Netscalerの信頼証明書と捺印	はい
コールバック URL	はい
Receiver for WebサイトのURL	はい
ゲートウェイのアドレス/VIP	はい
STAのURLおよびSTAのID	はい
すべてのログオンの種類	はい

10. [Import] をクリックします。StoreFrontサーバーがサーバーグループに含まれている場合、インポートしたゲートウェイ設定をグループ内の他のサーバーに反映させるように求めるメッセージが表示されます。

11. [完了] をクリックします。

別の仮想サーバー構成をインポートする場合は、上記の手順を繰り返します。

> **注意**
>
> 別のゲートウェイを使用するようにネイティブCitrix Receiverを構成していない場合、ストアのデフォルトゲートウェイが、ネイティブCitrix Receiverが接続に使用するゲートウェイとなります。ストアのゲートウェイが構成されていない場合、ZIPファイルからインポートされた1番目のゲートウェイが、ネイティブCitrix Receiverが使用するデフォルトゲートウェイになります。後でゲートウェイをインポートしても、ストアに設定済みのデフォルトゲートウェイは変更されません。

Read-STFNetScalerConfiguration

- 現在ログオンしているStoreFront管理者のデスクトップにZIPファイルをコピーします。
- NetScalerのZIPファイルの内容をメモリに読み込み、インデックス値を使用してファイルに含まれる3つのゲートウェイを確認します。

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"
```

Read-STFNetScalerConfigurationコマンドレットを使用して、NetscalerのZIPインポートパッケージからメモリ内に読み込んだ3つのゲートウェイオブジェクトを表示します。

```
$ImportedGateways.Document.Gateways[0]

$ImportedGateways.Document.Gateways[1]

$ImportedGateways.Document.Gateways[2]



GatewayMode          : CVPN
```

```
CallbackUrl           :

GslbAddressUri        : https://gslb.example.com/

AddressUri            : https://emeagateway.example.com/

Address               : https://emeagateway.example.com:443

GslbAddress           : https://gslb.example.com:443

VipAddress            : 10.0.0.1

Stas                  : {STA298854503, STA909374257}

StaLoadBalance        : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType       : Domain

GatewayEdition        : Enterprise

ReceiverForWebSites   : {Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite}



GatewayMode           : CVPN

CallbackUrl           :

GslbAddressUri        : https://gslb.example.com/

AddressUri            : https://emeagateway.example.com/

Address               : https://emeagateway.example.com:444

GslbAddress           : https://gslb.example.com:443

VipAddress            : 10.0.0.2
```

```
Stas                  : {STA298854503, STA909374257}

StaLoadBalance        : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType       : DomainAndRSA

GatewayEdition        : Enterprise

ReceiverForWebSites   : {Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite}



GatewayMode           : CVPN

CallbackUrl           : https://emeagateway.example.com:445

GslbAddressUri        : https://gslb.example.com/

AddressUri            : https://emeagateway.example.com/

Address               : https://emeagateway.example.com:445

GslbAddress           : https://gslb.example.com:443

VipAddress            : 10.0.0.2

Stas                  : {STA298854503, STA909374257}

StaLoadBalance        : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType       :SmartCard

GatewayEdition        : Enterprise

ReceiverForWebSites   : {Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite}
```

コールバックURLを指定せずにImport-STFNetScalerConfigurationを使用する

現在ログインしているStoreFront管理者のデスクトップにZIPファイルをコピーします。 NetScalerのZIPインポートパッケージをメモリに読み込み、インデックス値を使用してファイルに含まれる3つのゲートウェイを確認します。

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"
```

Import-STFNetScalerConfigurationコマンドレットを使用し、必要なゲートウェイインデックスを指定してStoreFrontに新しい3つのゲートウェイをインポートします。 -Confirm:$Falseパラメーターを使用することで、Powershell GUIからゲートウェイのインポートを1つ1つ許可するように求められなくなります。 1度に1つのゲートウェイをインポートする場合、このパラメーターは削除してください。

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -Confirm:$False
```

独自のコールバックURLを指定してImport-STFNetScalerConfigurationを使用する

Import-STFNetScalerConfigurationコマンドレットと-CallbackUrlパラメーターを使用し、任意のコールバックを指定して3つの新しいゲートウェイをStoreFrontへインポートします。

```
```

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.co

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.co

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.co
```

Import-STFNetScalerConfigurationを使用してインポートファイルに格納されている認証方法を上書きし独自のコールバックURLを指定する

- Import-STFNetScalerConfigurationコマンドレットと-CallbackUrlパラメーターを使用し、任意のコールバックを指定して3つの新しいゲートウェイをStoreFrontへインポートします。

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://em

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://em

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://em
```

NetScaler Gateway接続設定の構成

Aug 14, 2017

以下のタスクでは、ユーザーがストアにアクセスするときに経由するNetScaler Gateway環境の詳細を更新します。StoreFrontでのWebFront Gatewayの構成について詳しくは、「Using WebFront to Integrate with StoreFront」を参照してください。

NetScaler Gateway環境の構成を変更する場合は、そのNetScaler Gatewayを経由してストアにアクセスするユーザーに変更内容を通知して、Citrix Receiverの設定を更新させてください。ストアのCitrix Receiver for Webサイトが構成済みの場合、ユーザーはそのサイトから最新のCitrix Receiverプロビジョニングファイルを入手できます。Receiver for Webサイトが構成済みでない場合は、管理者がストアのプロビジョニングファイルをエクスポートしてユーザーに提供します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

ユーザーに表示されるNetScaler Gateway環境の名前を変更し、NetScaler Gatewayインフラストラクチャの仮想サーバー、ユーザーログオンポイントのURL、および展開モードを変更するには、［全般設定の変更］タスクを使用します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、［NetScaler Gatewayの管理］をクリックします。
3. NetScaler Gatewayの展開環境にわかりやすい名前を指定します。
   ここで指定する表示名がユーザーのCitrix Receiverに表示されます。そのため、ユーザーが使用するNetScaler Gatewayを判断しやすいように、名前に関連情報を含める必要があります。たとえば、ユーザーが自分のいる場所に最も便利なNetScaler Gatewayを簡単に特定できるように、表示名に地理情報を含めることができます。

4. 展開環境の仮想サーバーまたはユーザーログオンポイント（Access Gateway 5.0の場合）のURLを入力します。展開環境で使用する製品のバージョンを指定します。
   StoreFront展開環境のFQDN（Fully Qualified Domain Name：完全修飾ドメイン名）は一意で、NetScaler Gateway仮想サーバーのFQDNと異なるものである必要があります。StoreFrontとNetScaler Gateway仮想サーバーに同じFQDNを使用することはサポートされていません。

5. 展開環境でAccess Gateway 5.0が実行されている場合は、手順7.に進みます。それ以外の場合は、必要に応じてNetScaler GatewayアプライアンスのサブネットIPアドレスを指定します。サブネットIPアドレスは、Access Gateway 9.3アプライアンスの場合は必須ですが、それより後の製品バージョンではオプションです。
   このサブネットアドレスは、NetScaler Gatewayで内部ネットワークのサーバーと通信するときに、ユーザーデバイスを表すために使用するIPアドレスです。このアドレスは、NetScaler GatewayアプライアンスのマップされたIPアドレスである場合もあります。StoreFrontは、サブネットIPアドレスを使用して、受信要求が信頼されているデバイスから発信されているかどうかを検証します。

6. アプライアンスでNetScaler Gateway 10.1 - 11.0、Access Gateway 10 - 11.0、またはAccess Gateway 9.3を実行している場合は、［ログオンの種類］の一覧から、Citrix Receiverユーザー用にアプライアンスで構成した認証方法を選択します。
   NetScaler Gatewayアプライアンスに関する構成情報は、ストアのプロビジョニングファイルに追加されます。これにより、Citrix Receiverは、アプライアンスへの初回接続時に適切な接続要求を送信できるようになります。

   - ユーザーのMicrosoft Active Directoryドメインの資格情報を入力させる場合は、［ドメイン］を選択します。
   - セキュリティトークンから取得するトークンコードを入力させる場合は、［セキュリティトークン］を選択します。

- ユーザーのドメイン資格情報とセキュリティトークンから取得するトークンコードの両方を入力させる場合は、[ドメインおよびセキュリティトークン]を選択します。
- テキストメッセージで送信されるワンタイムパスワードを入力させる場合は、[SMS認証]を選択します。
- スマートカードを挿入してPINを入力させる場合は、[スマートカード]を選択します。

スマートカードでの認証に問題が生じた場合に代替の認証方法を使用できるようにするには、[スマートカードフォールバック]の一覧から代替の認証方法を選択します。

7. 展開環境でNetScaler Gateway 10.1～11.0、Access Gateway 10～11.0、Access Gateway 9.3、または単一のAccess Gateway 5.0アプライアンスを実行している場合は、NetScaler Gateway認証サービスのURLを［コールバックURL］ボックスに入力します。URLの標準的な部分は自動的に補完されます。
   アプライアンスの内部URLを入力します。StoreFrontはNetScaler Gateway認証サービスに接続して、NetScaler Gatewayからの要求の送信元がそのアプライアンスであることを確認します。

StoreFrontでAccess Gateway 5.0クラスター内のアプライアンスのIPアドレスまたはFQDNを追加、編集、または削除するには、［アプライアンスの管理］タスクを使用します。

Access Gateway 5.0クラスターのAccess Controllerサーバーで実行している認証サービスのURLを追加、編集、または削除するには、［サイレント認証を有効にする］タスクを使用します。一覧に複数のサーバーのURLを入力すると、その順番に基づいてフェールオーバーされます。StoreFrontでは認証サービスを使用してリモートユーザーが認証されるため、リモートユーザーがストアにアクセスするときに資格情報を再入力する必要はありません。

ユーザーセッションチケットを取得するSecure Ticket Authority（STA）の一覧を更新したり、セッション画面の保持機能を構成したりするには、［Secure Ticket Authority］タスクを使用します。STAは、XenDesktopおよびXenAppサーバーでホストされ、接続要求に応答してセッションチケットを発行します。セッションチケットは、XenDesktopおよびXenAppリソースへのアクセスを認証および承認するための基本機能です。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、結果ペインでNetScaler Gateway展開環境を選択します。［操作］ペインの［NetScaler Gatewayの管理］をクリックします。
3. ［追加］をクリックして、STAサーバーのURLを入力します。一覧に複数のSTAのURLを入力すると、その順番に基づいてフェールオーバーされます。URLを変更するには、［Secure Ticket Authority URL］ボックスの一覧でエントリを選択して［編集］をクリックします。特定のSTAからセッションチケットを取得しないようにするには、一覧でURLを選択して［削除］をクリックします。
4. Citrix Receiverが自動的に再接続を実行する間に、切断したセッションをXenDesktopおよびXenAppで開いたままにするには、［セッション画面の保持を有効にする］チェックボックスをオンにします。複数のSTAを構成した環境でセッション画面の保持機能を常に使用できるようにするには、［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにします。
   ［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにすると、セッションの途中で1つのSTAが使用できなくなってもユーザーセッションが中断されないように、StoreFrontにより2つの異なるSTAからセッションチケットが取得されます。StoreFrontがどちらのSTAにもアクセスできない場合は、単一のSTAを使用するようにフォールバックされます。

［操作］ペインで、**［NetScaler Gatewayの管理］**の［削除］タスクを使用して、NetScaler Gateway展開環境の詳細を

StoreFrontから削除します。NetScaler Gateway環境を削除すると、ユーザーはその展開環境を経由してストアにアクセスてきなくなります。

NetScalerによる負荷分散

Aug 14, 2017

ここでは、負荷分散用にNetScalerを使用するために必要な情報について示します。

StoreFrontサーバーグループとNetScaler負荷分散の構成

NetScaler負荷分散およびStoreFrontサーバーに対するSSL証明書の作成

サーバーグループ間のサブスクリプション同期用負荷分散仮想サーバーの作成

負荷分散用StoreFrontサーバーグループの構成

Citrixサービスモニター

同じNetScaler Gatewayアプライアンス上のNetScaler Gatewayおよび負荷分散仮想サーバー

NetScalerを使ってStoreFrontサーバーグループを負荷分散する場合のループバックオプション

負荷分散StoreFrontの展開計画

ここでは、すべてのアクティブな負荷分散構成に2つ以上のStoreFrontサーバーを含むStoreFrontサーバーグループを展開する方法について説明します。また、サーバーグループのすべてのStoreFrontノード間でCitrix Receiver/Citrix Receiver for Webからの受信要求を負荷分散するため、NetScalerアプライアンスを構成する方法と、NetScalerまたはサードパーティのロードバランサーで使用するため新しいStoreFrontモニターを構成する方法について詳しく説明します。

負荷分散構成の例については、後述の「シナリオ1」と「シナリオ2」を参照してください。

テストされた環境

- 単一のサーバーグループ内の4つのWindows Server 2012 R2 StoreFront 3.0ノード。
- 最小接続およびCookieInsert “sticky”負荷分散用に構成された1つのNetScaler 10.5ロードバランサー。
- Fiddler 4.0およびCitrix Receiver for Windows 4.3がインストールされた1つのWindows 8.1テストクライアント。

HTTPSを使用する場合に負荷分散化される展開のSSL証明書要件

「ゲートウェイとサーバー証明書の使用方法の計画」セクションを参照してください。

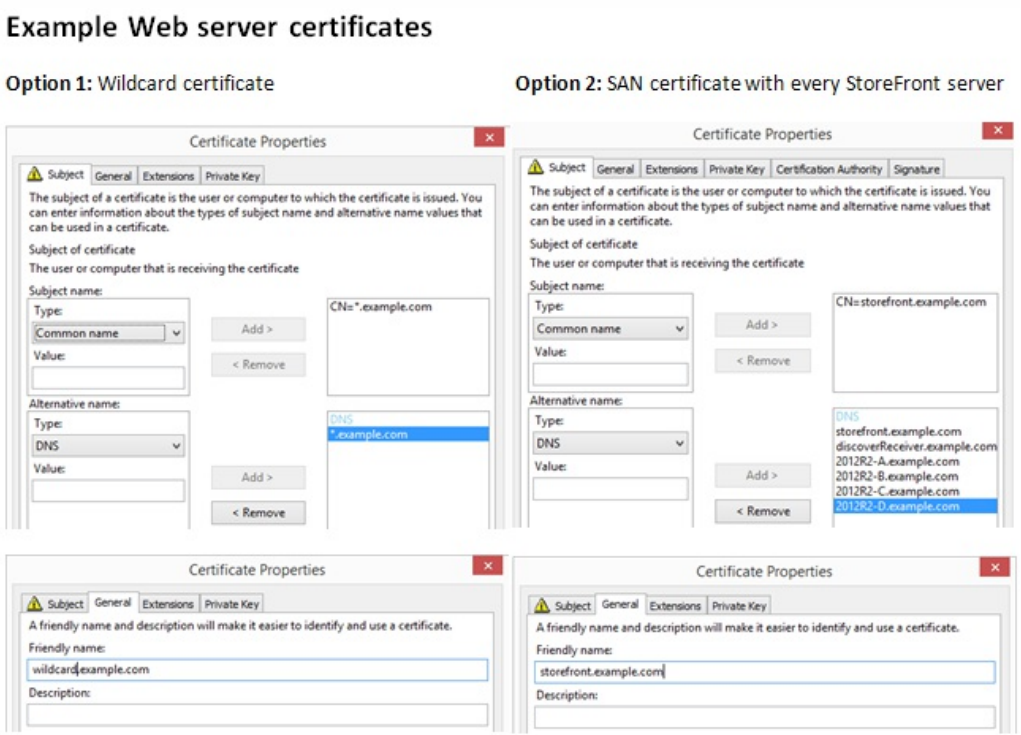
商用証明機関から証明書を購入する、またはエンタープライズCAから発行しようとする前に、次のオプションについて検討します。

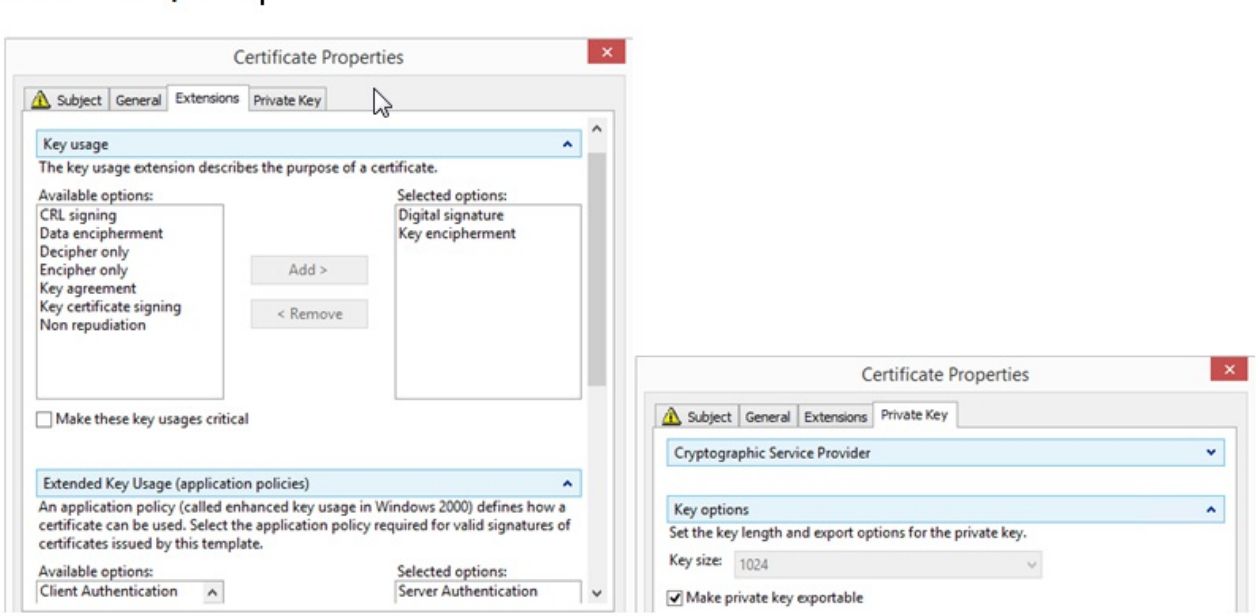
- **オプション1：***.example.comワイルドカード証明書をNetScaler負荷分散仮想サーバーとStoreFrontサーバーグループノードの両方で使用する。これにより構成が簡素化され、将来的には証明書を置き換える必要なく追加のStoreFrontサーバーを増やすことができます。
- **オプション2：**サブジェクトの別名（SAN）が含まれている証明書をNetScaler負荷分散仮想サーバーとStoreFrontサーバーグループノードの両方で使用する。すべてのStoreFrontサーバーの完全修飾ドメイン名（FQDN）と一致する証明書内の追加のSANはオプションですが、これによりStoreFront展開環境に柔軟性がもたらせられるため、推奨されます。メールベースの検出discoverReceiver.example.com用のSANを含めます。

  メールベースの検出の構成については、http://blogs.citrix.com/2013/04/01/configuring-email-based-account-

discovery-for-citrix-receiver/を参照してください。

注： 証明書に関連付けられている秘密キーをエクスポートできない場合は、注：エクスポートする場合、証明書に割り当てられている秘密キーは実行できません。NetScaler負荷分散仮想サーバー上の証明書と、StoreFrontサーバーグループノードの証明書という2つの別個の証明書を使用します。どちらの証明書にもサブジェクトの別名が必要です。





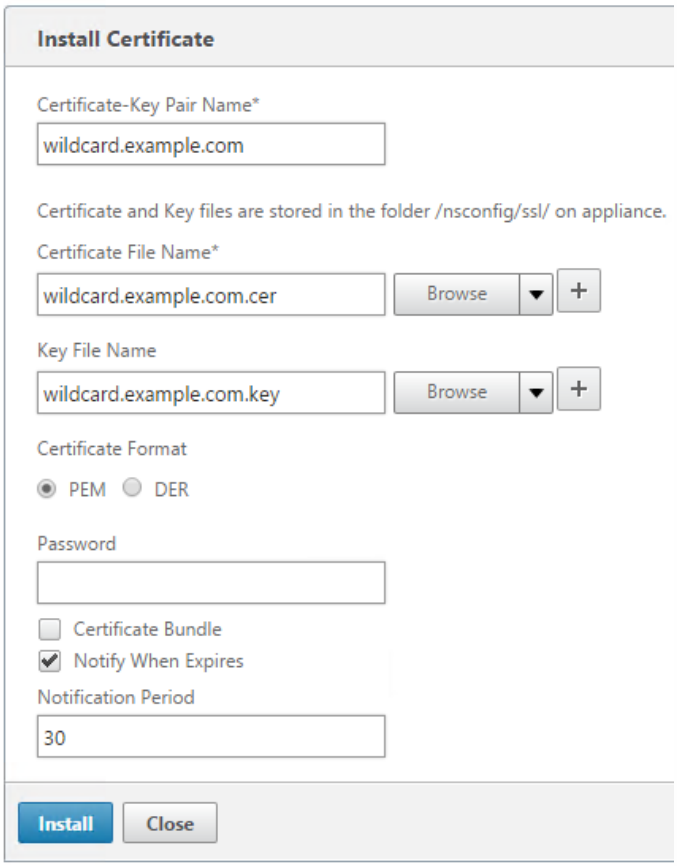
OpenSSLを使った、Windows CAから発行された証明書のNetaScalerアプライアンスへのインポート

- WinSCPは、WindowsマシンからNetScalerファイルシステムへのファイル移動に役立つ無料のサードパーティ製ツールです。インポートする証明書を、NetScalerファイルシステム内の/nsconfig/ssl/フォルダーにコピーします。
- また、NetScaler上でOpenSSLツールを使用して、PKCS12/PFXファイルから証明書とキーを抽出し、NetScalerで使用できるPEM形式で、2つの別々のCERファイルとKEY X.509ファイルを作成することができます。

1. このPFXファイルをNetScaler GatewayアプライアンスまたはVPXの/nsconfig/sslにコピーします。
2. NetScalerコマンドラインインターフェイス（CLI）を開きます。
3. 「Shell」と入力してNetScaler CLIを閉じ、FreeBSDシェルに切り替えます。
4. ディレクトリを変更するために、「cd /nsconfig/ssl」と入力します。
5. openssl pkcs12 -in .pfx -nokeys -out .cerを実行し、画面のメッセージに従ってPFXパスワードを入力します。
6. openssl pkcs12 -in .pfx -nocerts -out .keyを実行し、画面のメッセージに従ってPFXパスワードを入力して、次に秘密キーのPEMパスフレーズを設定してKEYファイルを保護します。
7. ls –alを実行し、/nsconfig/ssl/内にCERファイルとKEYファイルが正常に作成されたことを確認します。
8. 「Exit」と入力してNetScaler CLIに戻ります。

インポート後にNetScalerでSSL証明書の構成

1. NetScaler管理GUIにログオンします。
2. ［Traffic Management］>［SSL］>［SSL Certificates］の順に選択し、［Install］をクリックします。
3. ［Install Certificate］ウィンドウで証明書と秘密キーペア名を入力します。
   - o NetScalerファイルシステムの/nsconfig/ssl/で.cer証明書ファイルを選択します。
   - o 同じ場所から秘密キーを含む.keyファイルを選択します。



StoreFrontサーバーグループ負荷分散用のDNSレコードの作成

選択した共用FQDN用にDNS AおよびPTRレコードを作成します。ネットワーク内のクライアントはこのFQDNを使用して、ロードバランサーを使用するStoreFrontサーバーにアクセスします。

例 - **storefront.example.com**が仮想サーバー仮想IP（VIP）の負荷分散を解決。

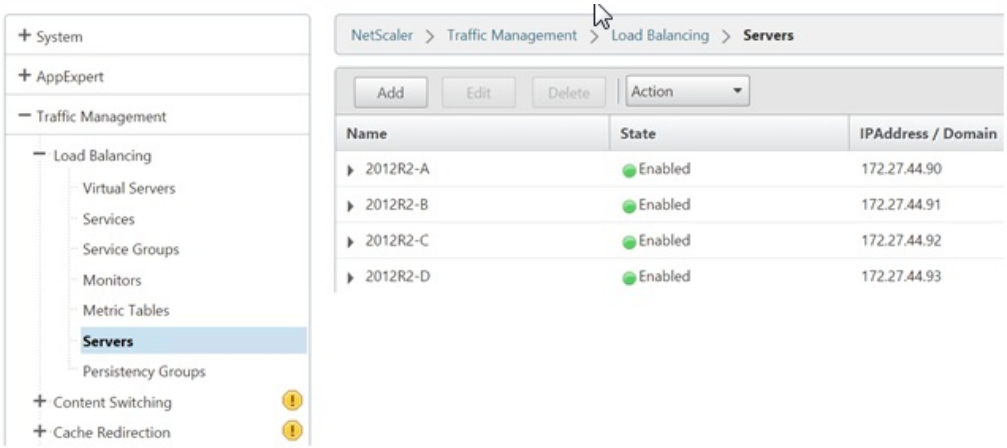
シナリオ1：クライアントとNetScalerロードバランサー間、またNetScalerロードバランサーと2つ以上のStoreFront 3.0サーバー間のエンドツーエンドのHTPPS 443セキュア接続。

このシナリオでは、ポート443を使用する変更されたStoreFrontモニターが使用されます。

1. NetScaler管理GUIにログオンします。
2. **[Traffic Management] > [負荷分散] > [サーバー] > [追加]**の順に選択し、4つのStoreFrontノードをそれぞれ追加して負荷分散させます。

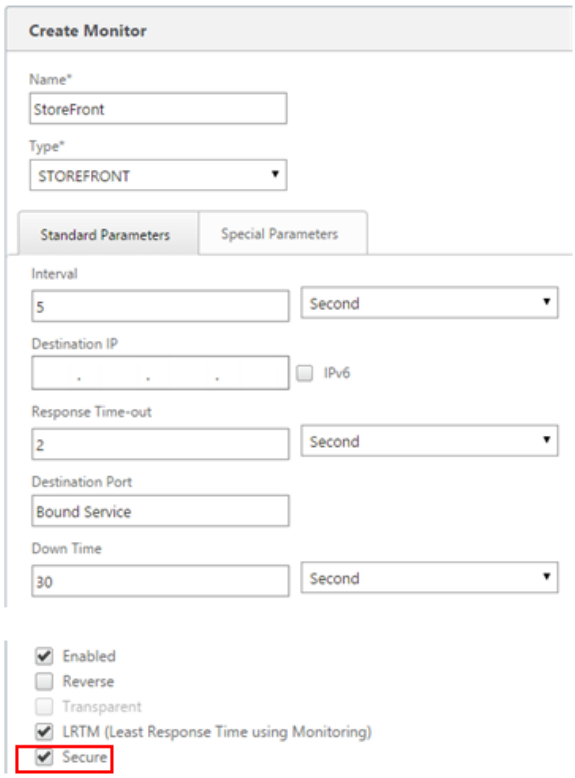
   例 = 4 x 2012R2 StoreFront Nodes called 2012R2-A to –D

3. IPベースのサーバー構成を使用し、各StoreFrontノードのサーバーIPアドレスを入力します。

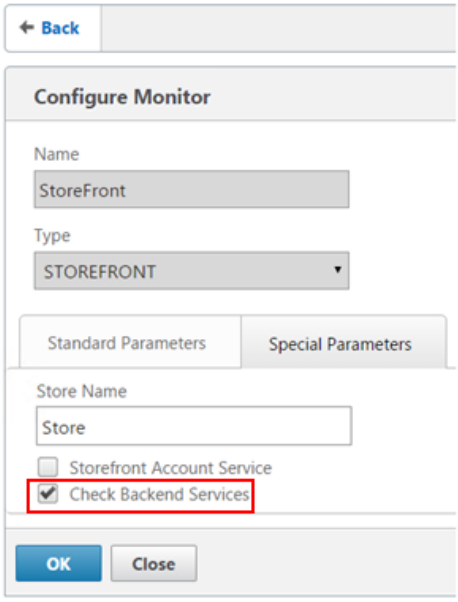


1. NetScaler管理GUIにログオンします。
2. **[Traffic Management] > [負荷分散] > [モニター] > [追加]**の順に選択し、StoreFrontを呼び出す新しいモニターを追加してすべてのデフォルト設定を受け入れます。
3. **[Type]**ドロップダウンの一覧から**[StoreFront]**を選択します。
4. 負荷分散仮想サーバーとStoreFront間でSSL接続を使用している場合は、**[Secure]**チェックボックスをオンにする必要があります。その他の場合はオフのままにします。
5. ［Special Parameters］タブでストア名を指定します。
6. ［Special Parameters］タブで**[Check Backend Services]**チェックボックスをオンにします。このオプションにより、StoreFrontサーバーで監視サービスの実行が有効になります。StoreFrontサーバーで実行するWindowsサービスをプローブしてStoreFrontサービスが監視され、実行中のすべてのStoreFrontサービスの状態が返されます。

Standard Parameters Tab

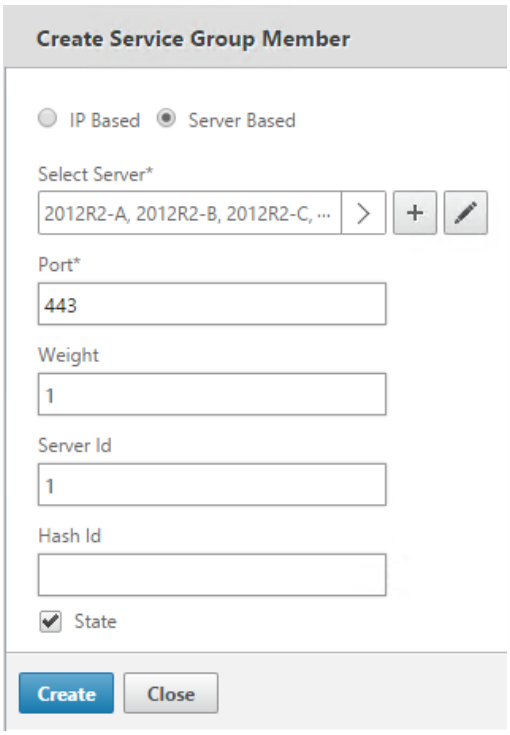


Special Parameters Tab

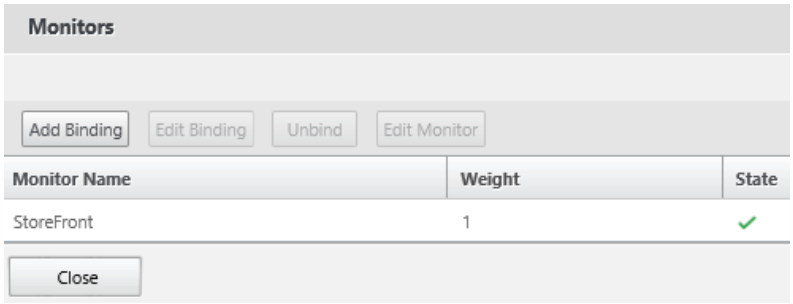


1. サービスグループ内で、右側の［Members］オプションを選択し、サーバーセクションで以前定義したすべてのStoreFrontサーバーノードを追加します。

2. SSLポートを設定し、各ノードに一意のサーバーIDを追加します。

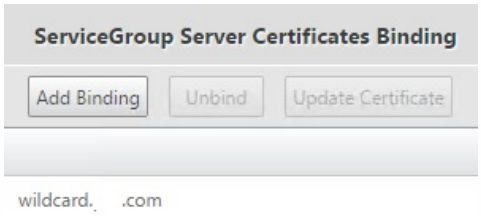


3. ［Monitors］タブで前に作成したStoreFrontモニターを選択します。



4. ［Certificates］タブで、前にインポートしたSSL証明書をバインドします。

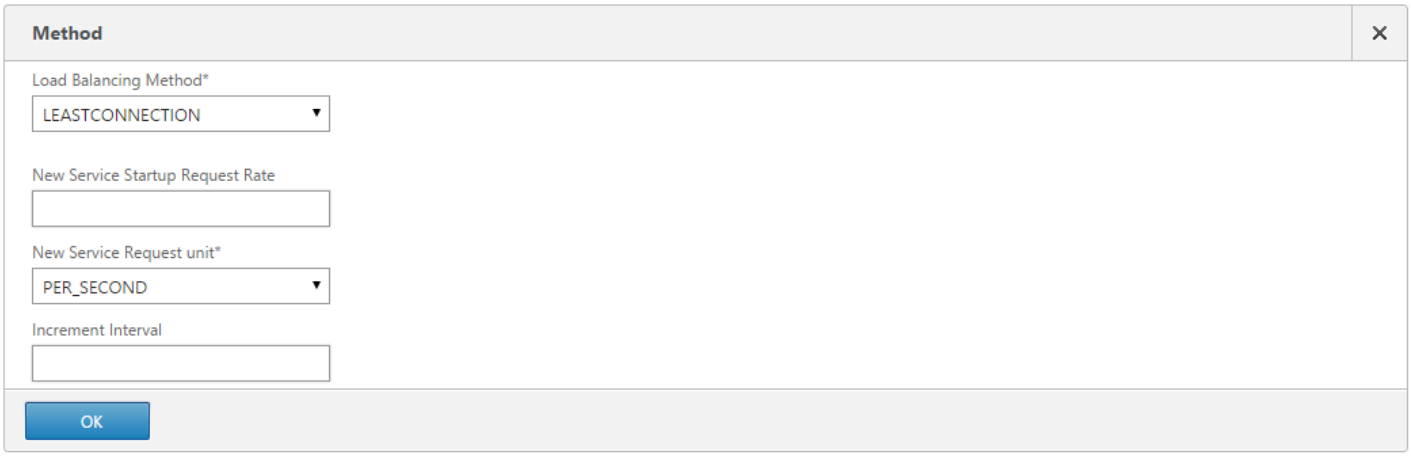
5. 以前にインポートしたSSL証明書の署名に使用されたCA証明書とPKIチェーン信頼の一部の可能性があるそのほかのCAをバインドします。



1. NetScaler管理GUIにログオンします。

2. **[Traffic Management] > [負荷分散] > [仮想サーバー] > [追加]** の順に選択し、新しい仮想サーバーを作成します。

3. 仮想サーバー用の負荷分散方式を選択します。StoreFront負荷分散で共通の選択は、[round robin] または [least connection] です。



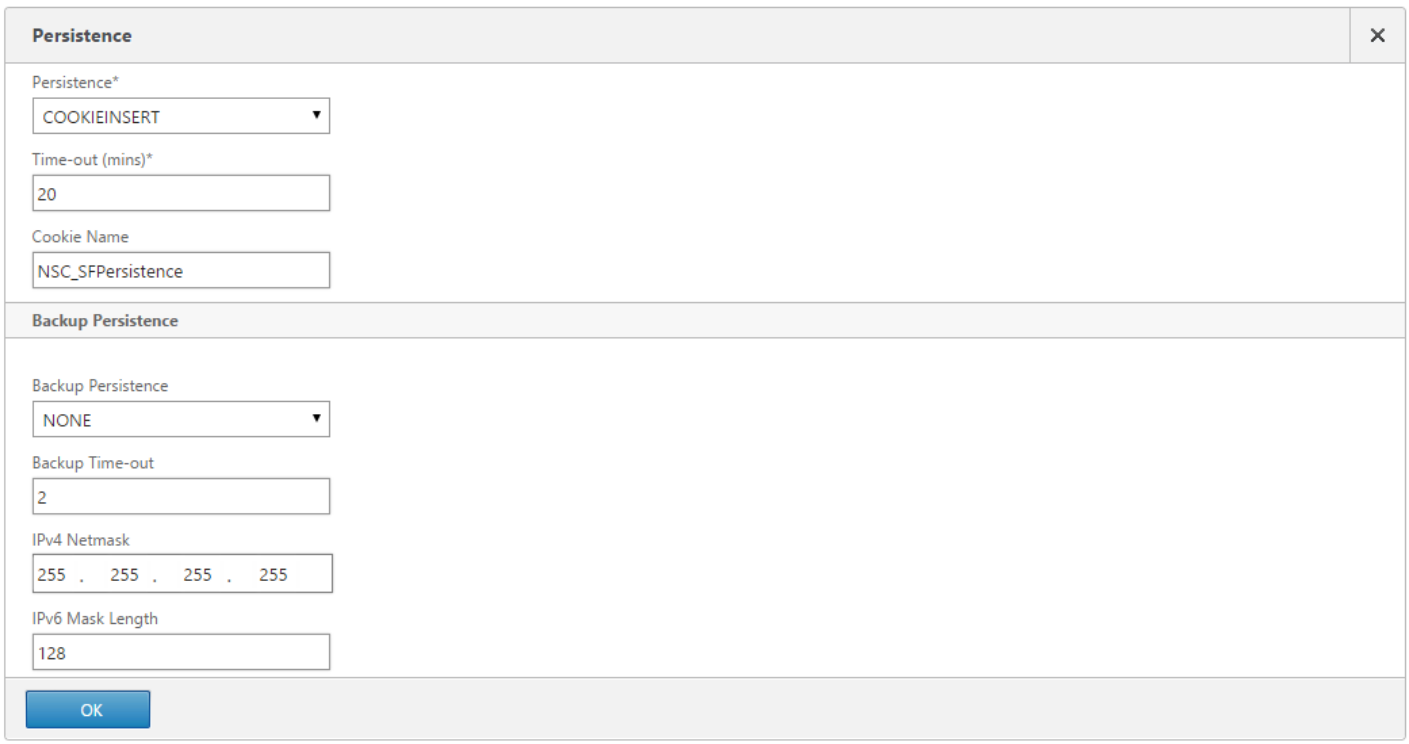
4. 前に作成したService Groupを負荷分散仮想サーバーにバインドします。

5. 以前にサービスグループにバインドしたのと同じSSLおよびCA証明書を負荷分散仮想サーバーにバインドします。

6. 負荷分散仮想サーバーメニュー内から、右側にある [Persistence] を選択して、パーシステンス方式がCookieInsertになるように設定します。

7. cookieに名前を付けます。たとえば、デバッグ時にFiddlerトレースで見つけやすいようにNSC_SFPersistenceという名前を付けます。

8. バックアップパーシステンスを [None] に設定します。



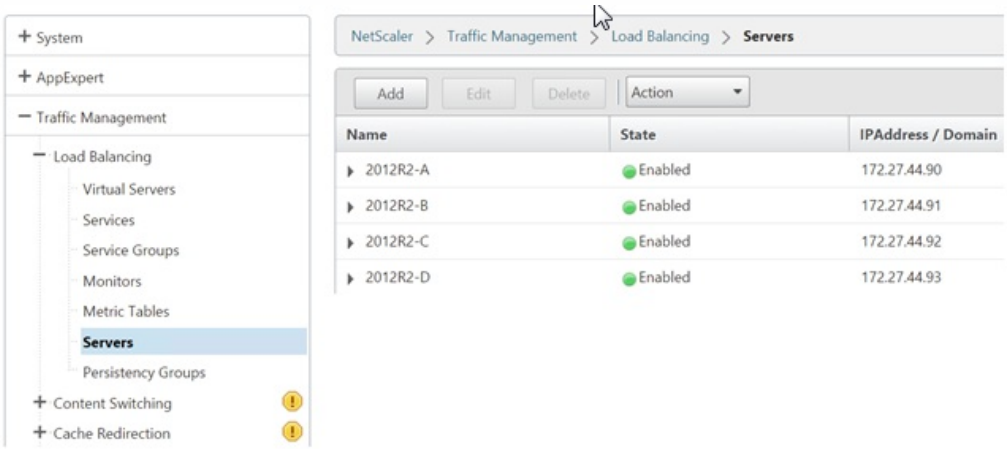
シナリオ2：SSL終了 - クライアントとNetScalerロードバランサー間のHTTPS 443通信、およびロードバランサーとその裏のStoreFront 3.0サーバー間のHTTP 80 接続。

このシナリオでは、ポート8000を使用するデフォルトのStoreFrontモニターが使用されます。

1. NetScaler管理GUIにログオンします。
2. **[Traffic Management] > [負荷分散] > [サーバー] > [追加]** の順に選択し、4つのStoreFrontサーバーをそれぞれ追加して負荷分散させます。

   例 = 4 x 2012R2 Storefront servers called 2012R2-A to -D

3. IPベースのサーバー構成を使用し、各StoreFrontサーバーのサーバーIPアドレスを入力します。



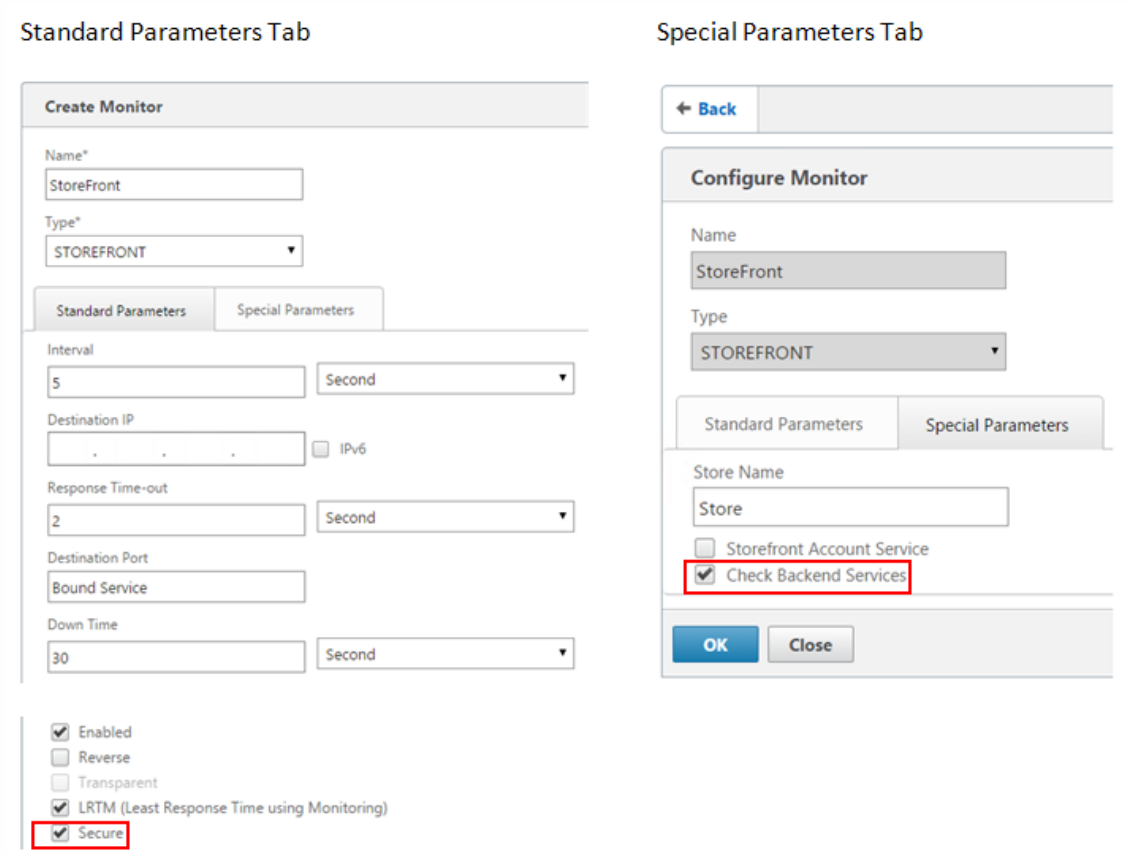
1. NetScaler管理GUIにログオンします。
2. **[Traffic Management] > [Monitors] > [Add]** の順に選択し、StoreFrontを呼び出す新しいモニターを追加します。
3. 新しいモニターの名前を入力し、すべてのデフォルトの設定を受け入れます。
4. **[Type]** ドロップダウンメニューから **[StoreFront]** を選択します。
5. ［Special Parameters］タブでストア名を指定します。
6. ポートに「**8000**」を入力して、各StoreFrontサーバーで作成されるデフォルトのモニターインスタンスと一致させます。
7. ［Special Parameters］タブで **[Check Backend Services]** チェックボックスをオンにします。このオプションにより、StoreFrontサーバーで監視サービスの実行が有効になります。StoreFrontサーバーで実行するWindowsサービスをプローブしてStoreFrontサービスが監視され、実行中のすべてのStoreFrontサービスの状態が返されます。

1. サービスグループ内で、右側のメンバーオプションを選択し、サーバーセクションで以前定義したすべてのStoreFrontサーバーノードを追加します。
2. HTTPポートを80に設定し、各サーバーに一意のサーバーIDを追加します。
3. ［Monitors］タブで前に作成したStoreFrontモニターを選択します。

1. [Traffic Management] > [負荷分散] > [仮想サーバー] > [追加] の順に選択し、新しい仮想サーバーを作成します。
2. 仮想サーバーが使用する負荷分散方式を選択します。StoreFront負荷分散で共通の選択は、[round robin] または [least connection] です。
3. 前に作成したService Groupを負荷分散仮想サーバーにバインドします。
4. 以前にサービスグループにバインドしたのと同じSSLおよびCA証明書を負荷分散仮想サーバーにバインドします。

   注：クライアントがHTTP Cookieを保存できない場合は、以降の要求にHTTP Cookieが含まれなくなり、パーシステンスは適用されません。

5. 負荷分散仮想サーバーメニュー内から [Persistence] を選択して、パーシステンス方式がCookieInsertとなるように設定します。
6. cookieに名前を付けます。たとえば、デバッグ時にFiddlerトレースで見つけやすいようにNSC_SFPersistenceという名前を付けます。
7. バックアップパーシステンスを [None] に設定します。



負荷分散仮想サーバーを作成する前に、次の点について検討します。

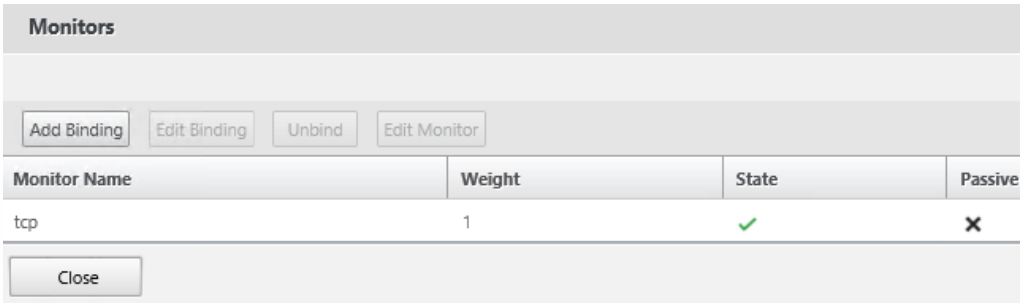
- オプション1：単一の仮想サーバーの作成：ユーザートラフィックのみを負荷分散。公開アプリケーションおよびデスクトップのICA起動のみを実行する場合は、必要なのはこれですべてです（必須、かつ通常はこれが必要なすべてです）。
- オプション2：仮想サーバーペアの作成：公開アプリケーションおよびデスクトップのICA起動を実行するためのユーザー

トラフィックの負荷分散用に1つ、サブスクリプションデータ同期操作の負荷分散用にもう1つ（大規模マルチサイト展開環境の2つ以上の負荷分散されたStoreFrontサーバーグループ間でサブスクリプションデータを反映させる場合にのみ必要）。

地理的に別々の場所にある2つ以上のStoreFrontサーバーグループで構成されるマルチサイト展開環境の場合、定期的にプル戦略を使ってサブスクリプションデータを複製できます。StoreFrontサブスクリプションレプリケーションはTCPポート808を使用するため、既存の負荷分散仮想サーバーをHTTPポート80またはSSL 443で使用することはできません。このサービスに対して高い可用性を提供するには、展開内の各NetScalerで2つ目の仮想サーバーを作成して、各StoreFrontサーバーグループのTCPポート808へ負荷分散します。レプリケーションスケジュールを構成する場合、サブスクリプション同期仮想サーバーの仮想IPアドレスと一致するサーバーグループアドレスを指定します。サーバーグループアドレスは、その場所にあるサーバーグループのロードバランサーのFQDNである必要があります。

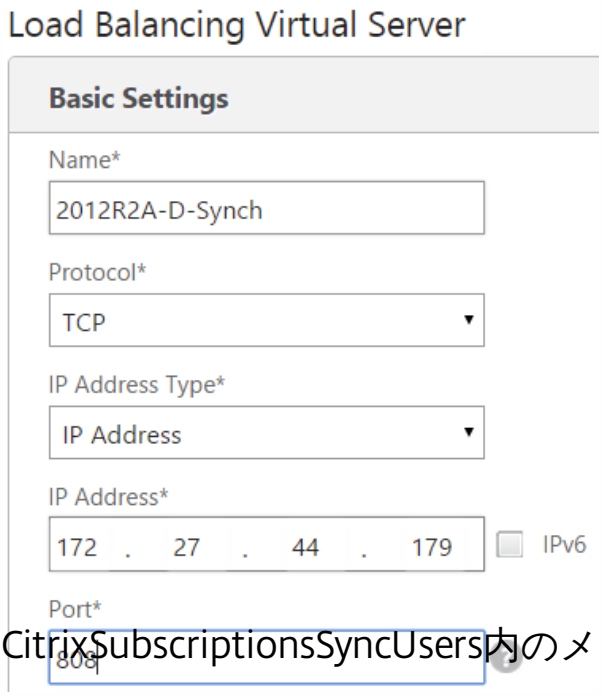
サブスクリプション同期用のサービスグループの構成

1. NetScaler管理GUIにログオンします。
2. [Traffic Management] > [Service Groups] > [Add] の順に選択し、新しいサービスグループを追加します。
3. プロトコルを [TCP] に変更します。
4. サービスグループ内で、右側の [Members] オプションを選択し、サーバーセクションで以前定義したすべてのStoreFrontサーバーノードを追加します。
5. [Monitors] タブで、TCPモニターを選択します。



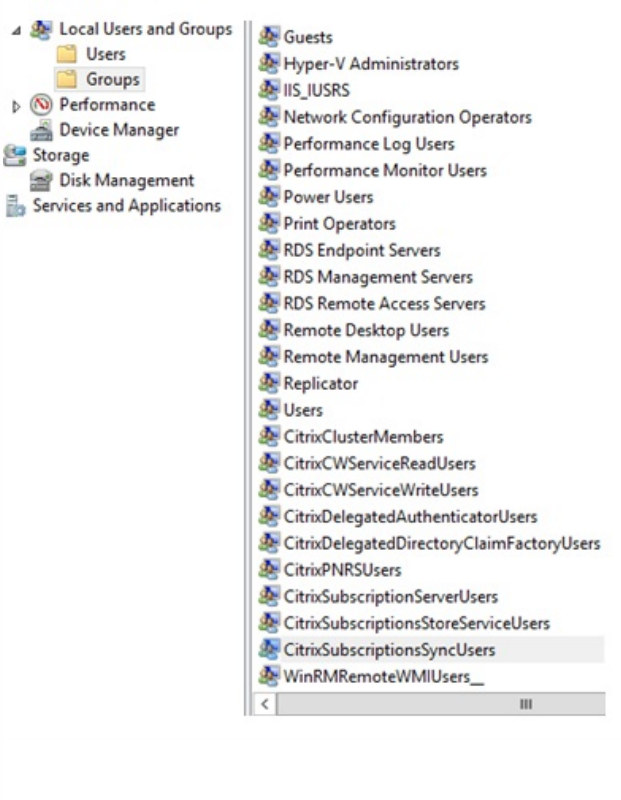
サーバーグループ間のサブスクリプション同期用負荷分散仮想サーバーの作成

1. NetScaler管理GUIにログオンします。
2. [Traffic Management] > [Service Groups] > [Add] の順に選択し、新しいサービスグループを追加します。
3. 負荷分散の手法に [round robin] を設定します。
4. プロトコルを [TCP] に変更します。
5. ポート番号には443ではなく、「808」と入力します。



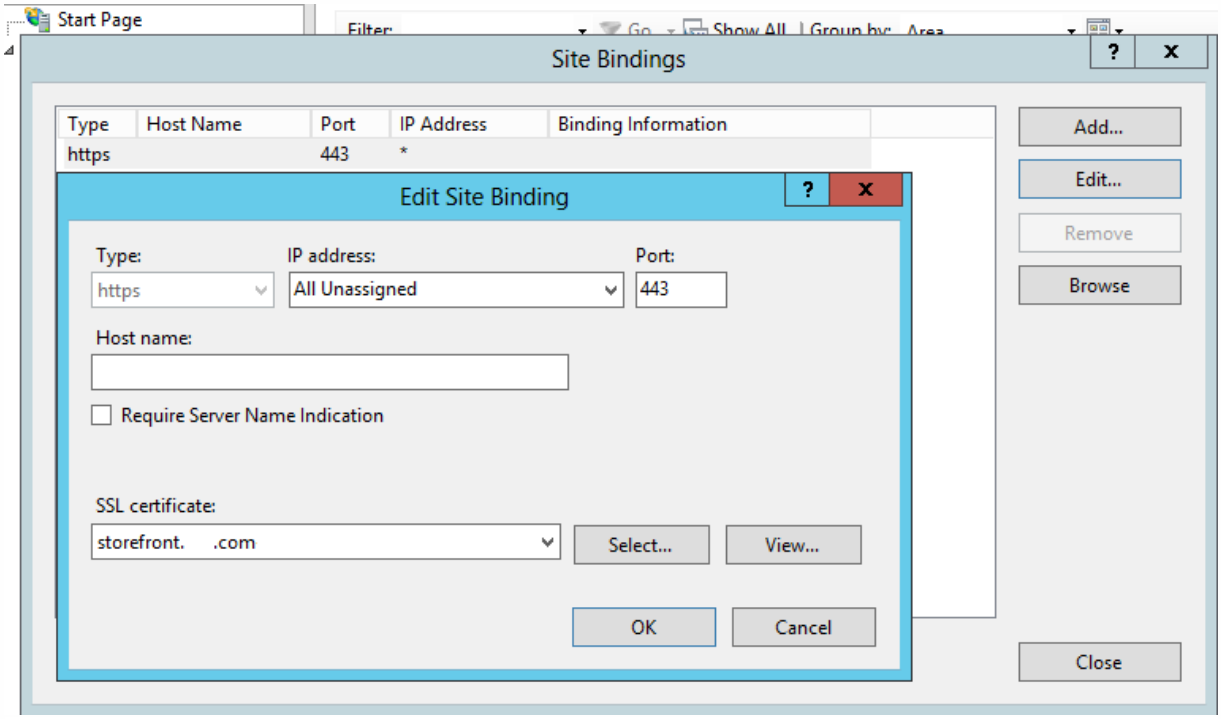
CitrixSubscriptionsSyncUsers内のメンバーシップ

For **StoreFront server A** at **Location A** to request and pull subscription data from **server B** at a different location, server A must be a member of the **CitrixSubscriptionsSyncUsers** local security group on server B. The **CitrixSubscriptionsSyncUsers** local group contains an access control list of all remote StoreFront servers authorized to pull subscription data from a particular server. 双方向サブスクリプション同期の場合、サブスクリプションデータをプルするため、サーバーBもサーバーAの**CitrixSubscriptionsSyncUsers** セキュリティグループのメンバーである必要があります。



1. NetScaler負荷分散仮想サーバー上に展開されたのと同じ証明書と秘密キーをサーバーグループ内のすべてのStoreFrontノードにインポートします。

2. すべてのStoreFrontノードのIISにHTTPSバインドを作成し、そこにこれより前にインポートした証明書をバインドします。



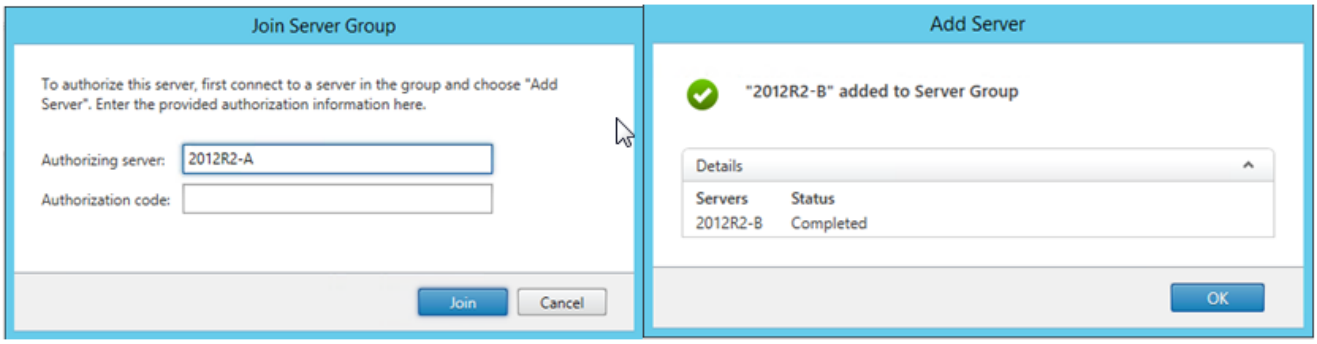
3. サーバーグループのすべてのノードにStoreFrontをインストールします。

4. StoreFrontをインストール間に、プライマリノードのホストベースURLがサーバーグループのすべてのメンバーによって使用される共有FQDNとなるように設定します。共通名（CN）またはサブジェクトの別名（SAN）として負荷分散されたFQDNを含む証明書を使用する必要があります。

「NetScaler負荷分散およびStoreFrontサーバーに対するSSL証明書の作成」を参照してください。

5. 初期StoreFront構成が完了したら、各ノードを順番にプライマリノードを使用するサーバーグループに参加させます。

6. 参加サーバーに対して [サーバーグループ] > [サーバーの追加] > [Copy the Authorization Code] の順に選択します。



7. プライマリノードからグループ内のすべてのほかのサーバーグループノードに構成を反映させます。

8. ロードバランサーの共有FQDNにアクセスして解決できるクライアントを使って、負荷分散サーバーグループをテストします。

StoreFrontが依存しているWindowsサービスが適切に稼働しているかを確認する実行状態の外部監視を有効にするには、**Citrixサービスモニター**Windowsサービスを使用します。このサービスはほかのサービスには依存せず、ほかの重要なStoreFrontサービスの障害を監視して報告できます。モニターにより、StoreFrontサーバー展開の相対的な稼働状態をNetScalerなどほかのCitrixコンポーネントによって外部的に判断することができます。サードパーティソフトウェアは、StoreFrontモニターのXML応答を使用して、必要なStoreFrontサービスの状態を監視できます。

StoreFrontの展開後、HTTPおよびポート8000を使用するデフォルトのモニターが作成されます。

注：StoreFront展開内に存在できるのは、モニターの単一のインスタンスのみです。

プロトコルとポートをHTTPS 443に変更など、既存のデフォルトのモニターに対して何らかの変更を加えるには、3つのPowerShellコマンドレットを使ってStoreFrontモニターサービスURLを表示して再構成します。

デフォルトのサービスモニターを削除し、HTTPSおよびポート443を使用するものに置き換える

1. プライマリStoreFrontサーバーでPowerShell Integrated Scripting Environment（ISE）を開き、以下のコマンドを実行してデフォルトモニターをHTTPS 443に変更します。

    次のように入力します。「Set-DSDerviceMonitorFeature –ServiceUrlhttps://localhost:443/StorefrontMonitor」

    Set-STFServiceMonitor -ServiceUrl $ServiceUrl

    Get-STFServiceMonitor

2. 変更が完了したら、StoreFrontサーバーグループ内の外のすべてのサーバーに変更を反映させます。

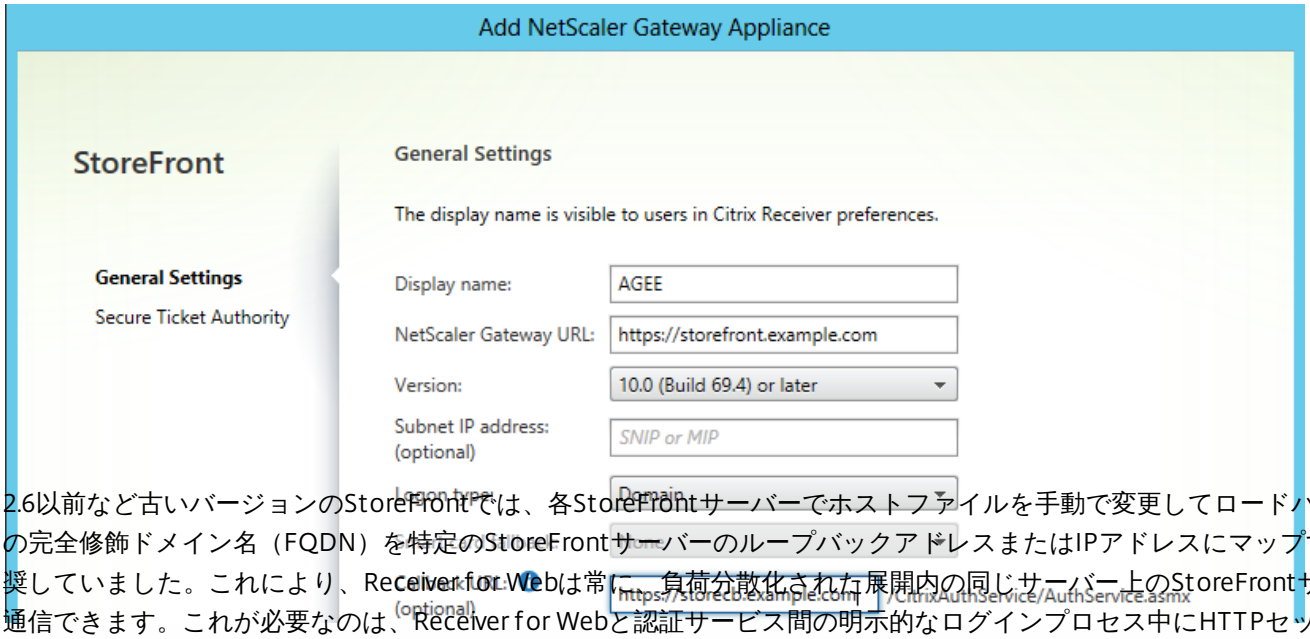
3. 新しいモニターでクイックテストを実行するには、StoreFrontサーバー、またはStoreFrontサーバーへネットワークアクセスするほかの任意のマシンでブラウザーに次のURLを入力します。ブラウザーは、すべてのStoreFrontサービスの状態についてXMLサマリーを返します。

    https://:443/StoreFrontMonitor/GetSFServicesStatus

同じNetScalerアプライアンス上に構成済みのNetScaler Gateway仮想サーバーと負荷分散仮想サーバーがある場合、内部ドメインユーザーがNetScaler Gateway仮想サーバーを経由するのではなくStoreFront負荷分散ホストベースURLに直接アクセスしようとすると問題が発生することがあります。

この場合、StoreFrontはユーザーのソースIPアドレスとNetScaler GatewayのサブネットIPアドレス（SNIP）とを相関するものとするため、エンドユーザーがNetScaler Gatewayで既に認証されたとStoreFrontにより見なされてしまいます。このためStoreFrontは、ユーザーにドメイン資格情報を使ってログオンするよう求めるのではなく、AGBasicプロトコルを使ってNetScaler Gatewayサイレント認証を実行しようとします。この問題を避けるには、次に示すようにSNIPアドレスを省いてAGBasicでなく、ユーザー名とパスワードの認証が使用されるようにします。

StoreFrontサーバーグループでのNetscaler Gatewayの構成



2.6以前など古いバージョンのStoreFrontでは、各StoreFrontサーバーでホストファイルを手動で変更してロードバランサーの完全修飾ドメイン名（FQDN）を特定のStoreFrontサーバーのループバックアドレスまたはIPアドレスにマップするよう推奨していました。これにより、Receiver for Webは常に、負荷分散化された展開内の同じサーバー上のStoreFrontサービスと通信できます。これが必要なのは、Receiver for Webと認証サービス間の明示的なログインプロセス中にHTTPセッションが作成され、Receiver for WebがベースFQDNを使用してStoreFrontサービスと通信するためです。ベースFQDNがロードバランサーに対して解決された場合は、ロードバランサーは潜在的にグループ内の別のStoreFrontサーバーにトラフィックを送信でき、認証エラーが発生することになります。これによって、Receiver for Webはそれと同じサーバー上にあるストアサービスへアクセスしようとする場合を除き、ロードバランサーをバイパスしません。

PowerShellを使ってループバックオプションを設定できます。ループバックを有効にすると、サーバーグループ内の各StoreFrontサーバーにホストファイルエントリを作成する必要がなくなります。

Receiver for Web web.configファイルの例：

PowerShellコマンドの例：

```
& "c:\program files\Citrix\receiver storefront\scripts\ImportModules.ps1"

Set-DSLoopback -SiteId 1 -VirtualPath "/Citrix/StoreWeb" -Loopback "OnUsingHttp" -LoopbackPortUsingHttp 81
```

-Loopback パラメーターには3つの値を設定できます。

値	コンテキスト
On： URLのホストを127.0.0.1に変更します。スキーマおよびポート（指定されている場合）は変更されません。	SSL終了ロードバランサーが使用されている場合は使用できません。
OnUsingHttp： ホストを127.0.0.1に、スキーマをHTTPに変更し、ポートを**loopbackPortUsingHttp**属性に構成されている値に変更します。	ロードバランサーがSSL終了である場合のみ使用します。ロードバランサーとStoreFrontサーバー間の通信はHTTPで行います。-loopbackPortUsingHttp属性を使って、HTTPポートを明示的に構成できます。

Off： 要求内のURLはいかなる方法によっても変更されません。	トラブルシューティングに使用します。Fiddlerのようなツールは、ループバックを“On”に設定している場合、Citrix Receiver for WebとStoreFront Services間のトラフィックをキャプチャできません。

1つのNetScaler Gatewayに2つのURLを構成する

Aug 14, 2017

StoreFrontでは、管理コンソールの［NetScaler Gatewayの管理］の［追加］または［編集］からNetScaler GatewayのURLを1つだけ追加できます。また、［NetScaler Gatewayの管理］の［ファイルからインポート］で、NetScaler Gatewayのパブリック URLとGSLB（Global Server Load Balancing：グローバルサーバー負荷分散）のURLの両方を追加することもできます。

この記事では、PowerShellコマンドレットとStoreFront PowerShell SDKでオプションパラメーターの-gslburlを使用して、ゲートウェイのGslbLocation属性を設定する方法について説明します。これにより、StoreFrontでのNetScaler Gatewayの管理が簡素化されます。

1. **GSLBと複数のNetScaler Gateway**：GSLBと複数のNetScaler Gatewayを使用して、大規模なグローバルCitrix展開の2つまたは複数の場所にある公開リソースへのリモート接続の負荷を分散します。
2. **単一のNetScaler Gatewayでのパブリックまたはプライベート URLの使用**: パブリックURLによる外部アクセスとプライベートURLによる内部アクセスに対し、同一のNetScaler Gatewayを使用します。

これは高度な機能です。GSLBの概念に慣れていない場合は、この記事の最後にある関連情報のリンクを参照してください。

このアーキテクチャには次の長所があります。

- 単一のゲートウェイオブジェクトで2つのURLを同時に使用できます。
- 管理者がユーザーの使用するゲートウェイURLと一致するようにStoreFrontゲートウェイオブジェクトを再構成しなくても、ユーザーは2つの異なるURLを切り替えてNetScaler Gatewayにアクセスできます。
- 複数のGSLBゲートウェイを使用する場合のStoreFrontゲートウェイ構成のセットアップと検証テスト時間が短縮されます。
- 外部アクセスと内部アクセスの両方に、DMZ内部のStoreFrontに含まれる同一のNetScaler Gatewayを使用できます。
- 最適なゲートウェイルーティングで両方のURLを使用できます。詳しくは、「可用性の高いマルチサイトストア構成のセットアップ」を参照してください。

> ## Important
>
> -gslburlパラメーターを使用して2番目のゲートウェイURLを構成する前に、配置済みのサーバー証明書と組織でのDNS解決の実行方法について確認することをお勧めします。NetScalerおよびStoreFrontの展開環境で使用するURLはすべて、サーバー証明書に記載されている必要があります。 サーバー証明書について詳しくは、「ゲートウェイとサーバー証明書の使用方法の計画」を参照してください。

DNS

- **分割 DNS** 大企業では、一般にスプリットDNSが使用されています。スプリットDNSでは、パブリックとプライベートのDNSの解決に異なる名前空間とDNSサーバーを使用しています。既存のDNSインフラストラクチャでこれがサポートされるかどうかを確認してください。
- **公開リソースへの外部および内部アクセス用の単一のURL**: 社内ネットワークの内部および外部からの公開リソースへのアクセスで同一のURLを使用するかどうか、またはexample.comとexample.netのような2つの異なるURLを認めるかどうかを検討します。

サーバー証明書

このセクションでは、2つのゲートウェイURLを使用する場合のサーバー証明書の展開例を示します。

- **StoreFrontの負荷分散展開環境のサーバー証明書の例**

  プライベート署名済みのワイルドカードサーバー証明書に、*.storefront.example.netというFQDNを含めます。

  または

  プライベート署名済みのSANサーバー証明書に、3台のStoreFrontサーバーの負荷分散に必要なFQDNをすべて含めます。

  loadbalancer.storefront.example.net

  server1.storefront.example.net

  server2.storefront.example.net

  server3.storefront.example.net

  Storefrontサーバーグループのホストのベースurlを、ロードバランサーのIPアドレスに対して解決される共有FQDNに設定します。

  loadbalancer.storefront.example.net

- **XenAppおよびXenDesktop 7.xのDelivery Controllerグループ向けのサーバー証明書の例**

  プライベート署名済みのワイルドカードサーバー証明書に、*.xendesktop.example.netというFQDNを含めます。

  または

  プライベート署名済みのSANサーバー証明書に、4つのControllerが含まれるXenDesktopサイトに必要なFQDNをすべて含めます。

  XD1A.xendesktop.example.net

  XD1B.xendesktop.example.net

  XD2A.xendesktop.example.net

  XD2B.xendesktop.example.net

- **スプリットDNSを使用して内外部の両方からアクセスされるNetScaler Gatewayのサーバー証明書の例**

  外部と内部両方のアクセス用のプライベート署名済みSANサーバー証明書に、外部と内部両方のFQDNを含めます。

  gateway.example.com

  gateway.example.net

- **外部からアクセスされるすべてのGSLBゲートウェイ向けのサーバー証明書の例**

  GSLBを経由した外部アクセス用のパブリック署名済みSANサーバー証明書に、次のFQDNを含めます。

  gslbdomain.example.com

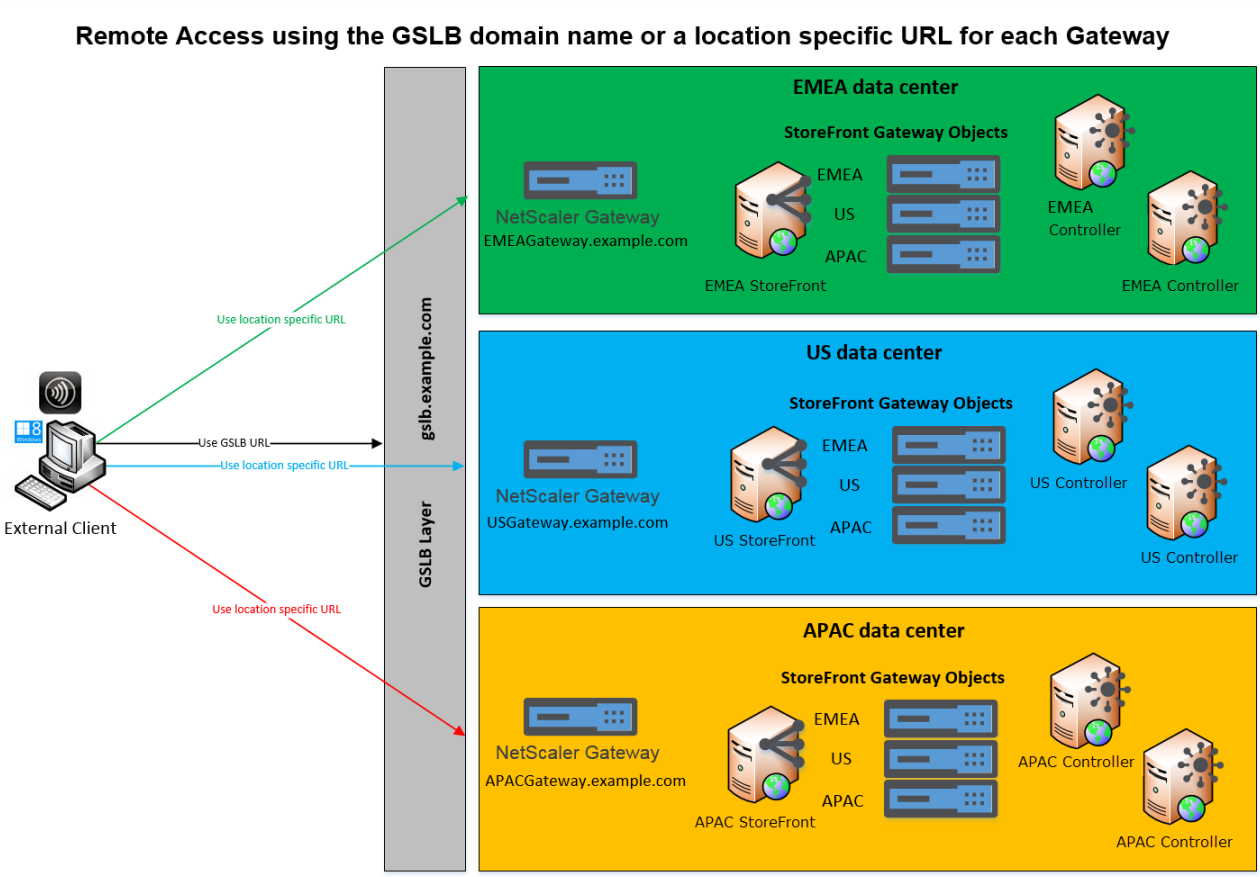
emeagateway.example.com

usgateway.example.com

apacgateway.example.com

これにより、ユーザーはGSLBを使用して最も近いゲートウェイにアクセスするか、一意のFQDNを使用して任意の場所にあるゲートウェイを選択することができます。

管理者がGSLBと複数のNetScaler Gatewayを使用して、大規模なグローバルCitrix展開の2つまたは複数の場所にある公開リソースへのリモート接続の負荷を分散します。

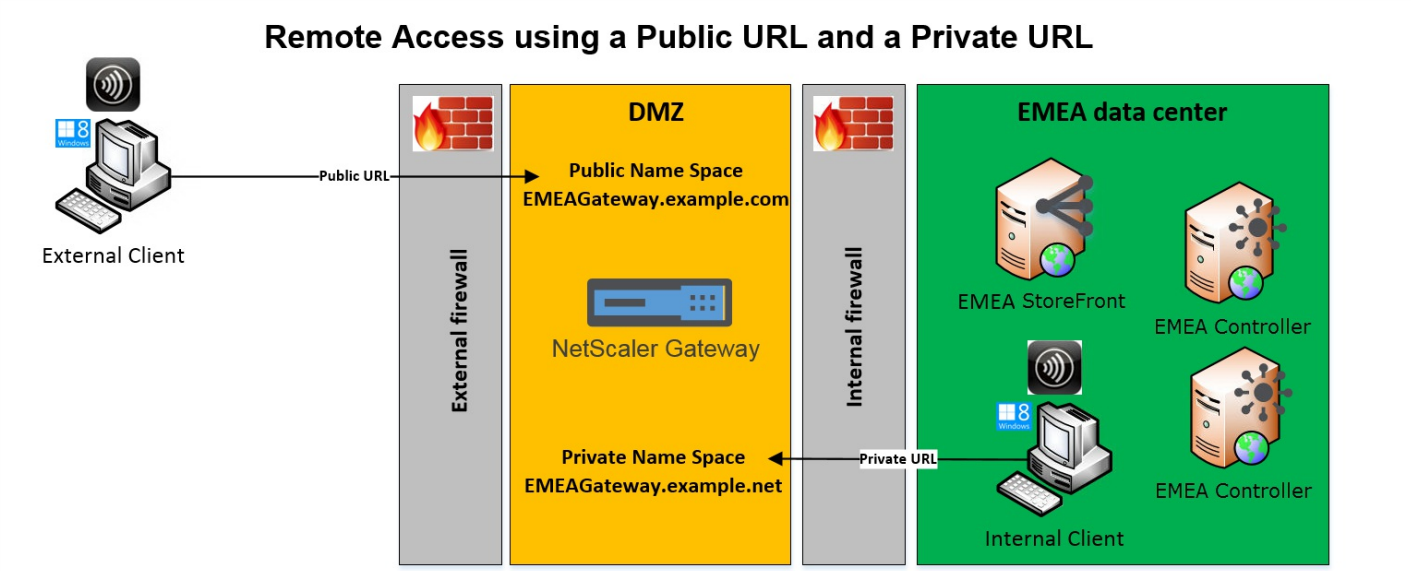


この例の構成は次のとおりです。

- それぞれの場所またはデータセンターに、1つまたは複数のゲートウェイ、1台または複数台のStoreFrontサーバー、その場所の公開リソースを提供する1つ以上のXenAppおよびXenDesktopのコントローラーを含めています。
- グローバル展開環境内のGSLB NetScaler上で構成されている各GSLBが、ゲートウェイVPN仮想サーバーとしています。この環境内のStoreFrontサーバーはすべて、GSLBレイヤーを構成するNetScaler Gateway仮想サーバーすべてを含むように構成する必要があります。
- GSLB NetScaler Gatewayはアクティブ/アクティブモードで使用していますが、1箇所でネットワーク接続、DNS、ゲートウェイ、StoreFrontサーバー、またはXenAppおよびXenDesktopのコントローラーに障害が発生した場合はフェールオーバーを実施することもできます。GSLBサービスが利用不能になると、ユーザーは自動で別のゲートウェイに接続されます。

- リモート接続が確立されると、外部クライアントは、GSLBの構成済み負荷分散アルゴリズム（ラウンドトリップ時間（RTT）や静的近接度）に基づいて最も近いゲートウェイに接続されます。
- 各ゲートウェイの一意のURLにより、ユーザーは使用するゲートウェイの場所固有のURLを選択して、リソースの起動先になるデータセンターを手動で指定することができます。
- GSLBまたはDNSの委任が意図したとおりに動作しなくなった場合は、GSLBをバイパスすることができます。GSLB関連の問題が解決されるまで、ユーザーは場所固有のURLを使用してすべてのデータセンターのリモートリソースに引き続きアクセスできます。

管理者は、パブリックURLによる外部アクセスとプライベートURLによる内部アクセスの両方で、同一のNetScaler Gatewayを使用します。



この例の構成は次のとおりです。

- 管理者は、クライアントが内部にある場合でも、公開リソースへのアクセスおよびHDXの起動トラフィックがNetScaler Gatewayを経由して渡されるように設定します。
- NetScalerはDMZ内に配置されています。
- DMZの両側には、2つのファイアウォールを経由したNetScaler Gatewayへの2つの異なるネットワークルートが配置されています。
- 公開される外部名前空間は、内部の名前空間とは異なります。

StoreFrontゲートウェイオブジェクト上の**GslbLocation**属性を設定するには、**Add-STFRoamingGateway**および**Set-STFRoamingGateway**の各PowerShellコマンドレットで-gslburlパラメーターを指定します。次に例を示します。

```
Add-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://emeagateway.example.com" -GSLBurl "https://gslb.example.com"

Set-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://emeagateway.example.com" -GSLBurl "https://gslb.example.com"

Get-STFRoamingGateway -Name "EMEAGateway" (returns just the EMEA gateway object)

Or

Get-STFRoamingGateway (returns all gateway object configured in StoreFront)
```

ユースケース#1では**GslbLocation**をNULLに設定して、「EMEAGateway」からGSLBurlを削除できます。以下のPowerShellは、メモリに保存されたゲートウェイオブジェクト$EMEAGatewayを変更します。次に、**Set-STFRoamingGatway**が$EMEAGatewayに設定され、StoreFront構成を更新しGSLBurlを削除できます。

```
$EMEAGateway = Get-STFRoamingGateway

$EMEAGateway.GslbLocation = $Null

Set-STFRoamingGateway -Gateway $EMEAGateway
```

ユースケース1では、**Get-STFRoamingGateway**を使用すると以下のゲートウェイが返されます。

```
Name: EMEAGateway

 Location: https://emeagateway.example.com/ (Unique URL for the EMEA Gateway)

GslbLocation: https://gslb.example.com/ (GSLB URL for all three gateways)



Name: USGateway

 Location: https://USgateway.example.com/ (Unique URL for the US Gateway)

GslbLocation: https://gslb.example.com/ (GSLB URL for all three gateways)



Name: APACGateway

 Location: https://APACgateway.example.com/ (Unique URL for the APAC Gateway)

GslbLocation:  https://gslb.example.com/ (GSLB URL for all three gateways)
```

ユースケース2では、Get-STFRoamingGatewayを使用すると以下のゲートウェイが返されます。

```
Name: EMEAGateway

Location: https://emeagateway.example.com/ (Public URL for the Gateway)

GslbLocation: https://emeagateway.example.net/ (Private URL for the Gateway)
```

ユースケース1では、Get-STFStoreRegisteredOptimalLaunchGatewayを使用すると最適なゲートウェイルーティングが返されます。

```
$StoreObject = Get-STFStoreService -SiteId 1 -VirtualPath "/Citrix/<YourStore>"

Get-STFStoreRegisteredOptimalLaunchGateway -StoreService $StoreObject



Hostnames:      {emeagateway.example.com, gslb.example.com}

Hostnames:      {usgateway.example.com, gslb.example.com}

Hostnames:      {apacgateway.example.com, gslb.example.com}
```

各ゲートウェイのGSLB URLまたは内部URLはローミングサービスのweb.configファイルに格納されている

StoreFrontの管理コンソールでは、各ゲートウェイのGSLB URLまたは内部URLは表示されませんが、すべてのGSLBゲートウェイについて、StoreFrontサーバーのC:\inetpub\wwwroot\Citrix\Roaming\にあるローミングサービスのweb.configファイルを開くと構成済みのGSLBLocationパスを確認できます。

ユースケース1：ローミングweb.configファイルのゲートウェイ

ユースケース2： ローミングweb.configファイルのゲートウェイ

DFA用のNetScalerおよびStoreFrontの構成

Aug 14, 2017

拡張認証機能により、NetScalerおよびStoreFrontのフォームベース認証を拡張するための単一のカスタマイズポイントが提供されます。拡張認証SDKを使用した認証ソリューションを実現するには、NetScalerとStoreFrontの間にDelegated Forms Authentication（DFA）を構成する必要があります。DFAプロトコルを使用すると、資格情報検証などの認証フォームの生成と処理をほかのコンポーネントに委任することができます。たとえば、NetScalerは認証をStoreFrontに委任し、StoreFrontはサードパーティの認証サーバーまたは認証サービスとやりとりします。

- NetScalerとStoreFrontの間の通信を確実に保護するには、HTTPプロトコルの代わりにHTTPSプロトコルを使用します。
- クラスター展開環境では、すべてのノードに同じサーバー証明書をインストールし、IIS HTTPSバインドを構成してから、構成手順を実行する必要があります。
- StoreFrontでHTTPSを構成するときは、NetScalerにStoreFrontのサーバー証明書の発行者を信頼された証明書機関として設定する必要があります。

- すべてのノードにサードパーティの認証プラグインをインストールしてから、これらのノードをクラスターに追加します。
- 1つのノードですべてのDFA関連設定を構成し、その内容をほかのノードに反映させます。「DFAの有効化」を参照してください。

StoreFrontにはCitrixの事前共有キー設定を設定するGUIがないので、PowerShellコンソールを使用してDFAをインストールします。

1. DFAをインストールします。DFAはデフォルトではインストールされないので、PowerShellコンソールを使用してインストールする必要があります。
   PS C:\Users\administrator.PTD.000> cd 'C:\Program Files\Citrix\Receiver StoreFront\Scripts' PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> & .\ImportModules.ps1 Adding snapins Importing
2. Citrix Trusted Clientを追加します。StoreFrontとNetScalerの間で共有秘密キー（パスフレーズ）を構成します。パスフレーズとクライアントIDは、NetScalerで構成したものと同一である必要があります。
   PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Add-DSCitrixPSKTrustedClient -clientId netscaler.fqdn.com -passphrase secret
3. DFA Conversation Factoryを設定して、すべてのトラフィックをカスタムフォームにルーティングします。Conversation Factoryを見つけるには、C:\inetpub\wwwroot\Citrix\Authentication\web.configでConversationFactoryを検索します。以下の例を参照してください。

4. PowerShellで、DFA Conversation Factoryを設定します。この例では、ExampleBridgeAuthenticationに設定しています。
   PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Set-DSDFAProperty -ConversationFactory ExampleBridgeAuthentication

PowerShellの引数では大文字と小文字が区別されません。-ConversationFactoryisは–conversationfactoryと同意です。

サードパーティの認証プラグインはStoreFrontの機能に影響を与えるので、すべてのサードパーティの認証プラグインをアンインストールしてから、StoreFrontをアンインストールします。

異なるドメインを使用した認証

Aug 14, 2017

組織によっては、サードパーティの開発者や契約社員に実稼働環境で公開リソースへのアクセスをポリシーで禁止している場合があります。ここでは、NetScaler Gateway経由で1つのドメインに認証することでテスト環境での公開リソースへのアクセスを許可する方法を説明します。これによって、異なるドメインを使用してStoreFrontおよびReceiver for Webサイトへの認証を実行できます。ここで説明されたNetScaler Gateway経由の認証は、Receiver for Webサイト経由でログオンするユーザーが対象です。この認証方法は、ネイティブのデスクトップまたはモバイルCitrix Receiverのユーザーは使用できません。

ここでは、production.comという実稼働ドメインとdevelopment.comというテストドメインを使用します。

production.comドメイン

この例では、production.comドメインを以下のようにセットアップします。

- production.comのLDAP認証ポリシーが構成されたNetScaler Gateway。
- production\testuser1アカウントおよびパスワードを使用してゲートウェイ経由で認証。

development.comドメイン

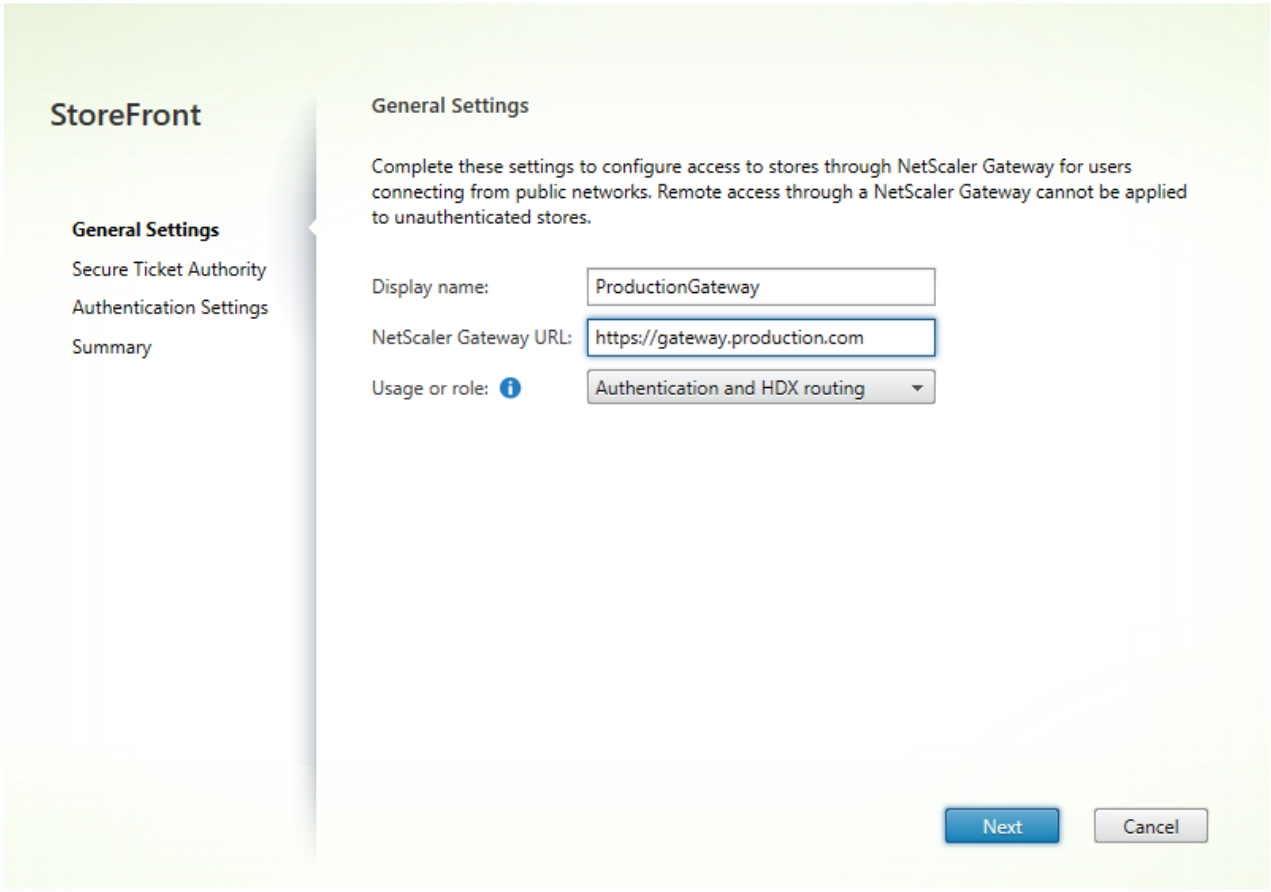
この例では、development.comドメインを以下のようにセットアップします。

- StoreFront、XenAppおよびXenDesktop 7.0以降、VDAをすべてdevelopment.comドメインに配置。
- production\testuser1アカウントおよびパスワードを使用してCitrix Receiver for Webサイトに認証。
- 2つのドメインの間には、信頼関係はありません。

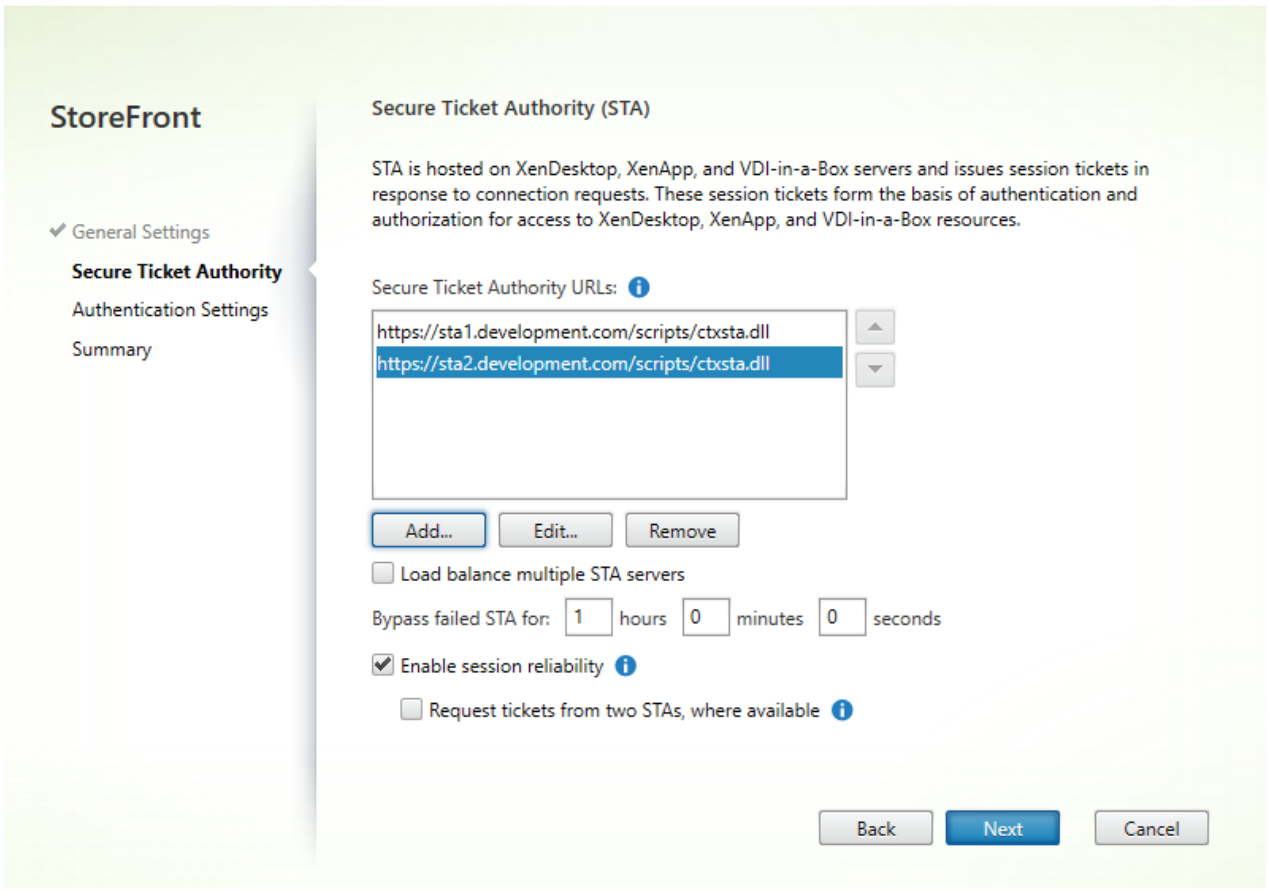
ストアのNetScaler Gatewayを構成するには：

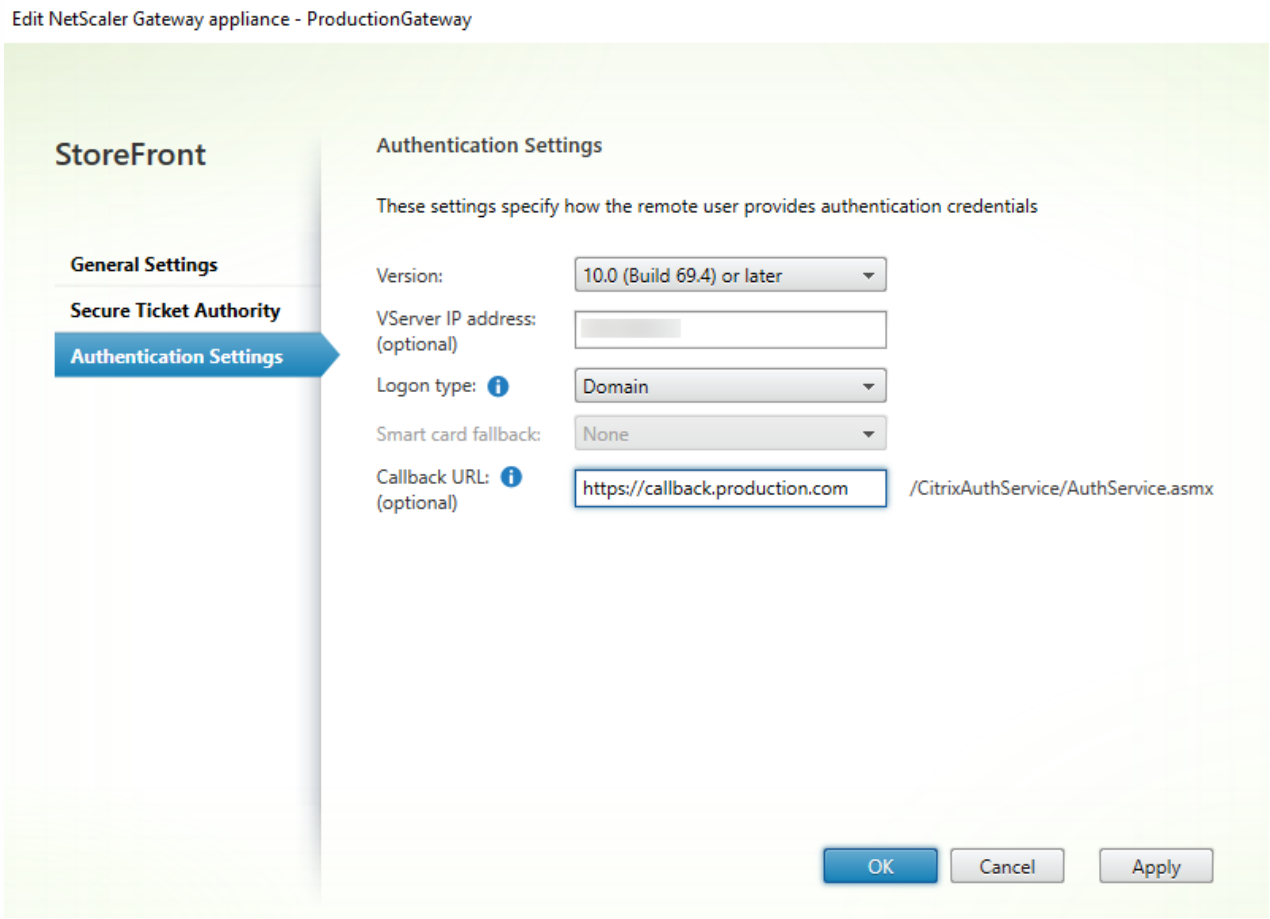
1. Citrix StoreFront管理コンソールの左ペインで **[ストア]** を選択して、 **[操作]** ペインの **[NetScaler Gatewayの管理]** をクリックします。
2. ［NetScaler Gatewayの管理］画面で、 **[追加]** をクリックします。
3. 全般設定、Secure Ticket Authority、認証手順を完了します。

Add NetScaler Gateway Appliance



Add NetScaler Gateway Appliance

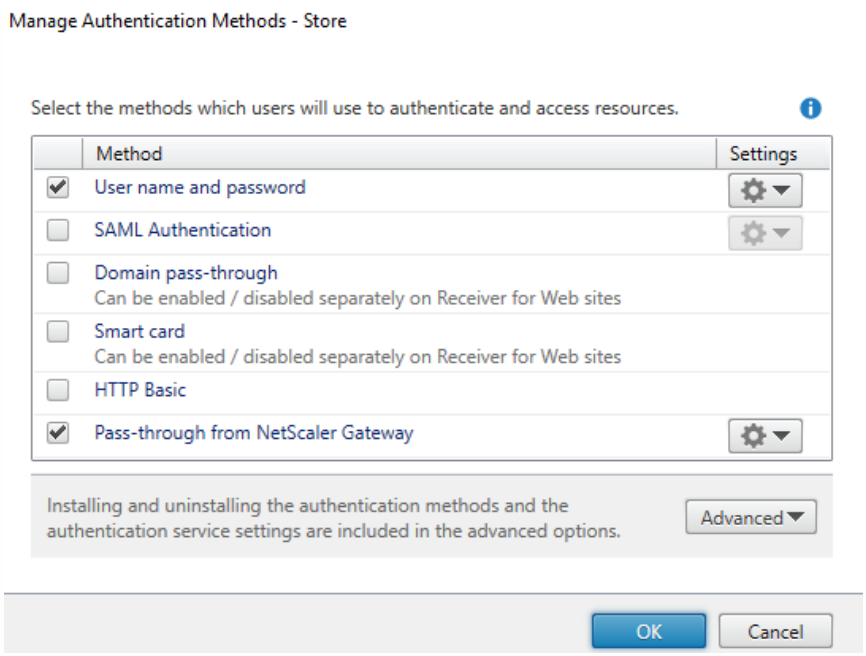




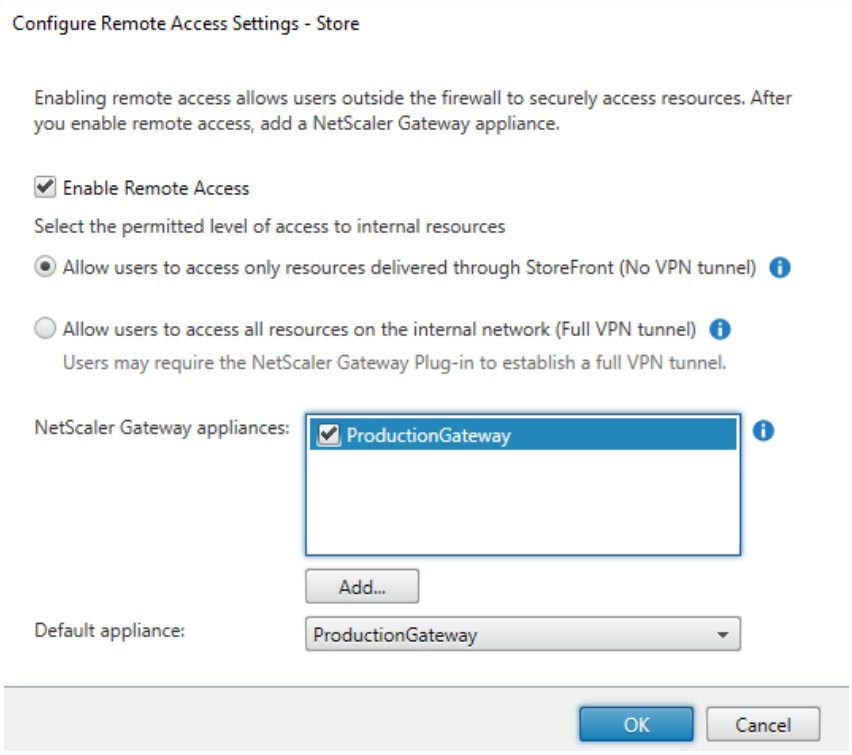
注意

両方のドメインで使用中のDNSサーバーが他方のドメインのFQDNを解決できるよう、DNS条件付きフォワーダーの追加が必要な場合があります。NetScalerは、production.comのDNSサーバーを使用して、development.comドメインでSTAサーバーのFQDNを解決できるようにする必要があります。StoreFrontは、development.comのDNSサーバーを使用して、production.comドメインでコールバックURLを解決できるようにする必要があります。または、development.comのFQDNを使用して、NetScaler Gateway vServer virtual IP（VIP）として解決することもできます。

1. Citrix StoreFront管理コンソールの左ペインで **[ストア]** を選択して、 **[操作]** ペインの **[認証方法の管理]** をクリックします。
2. ［認証方法の管理］画面で、 **[NetScaler Gatewayからのパススルー]** を選択します。
3. **[OK]** をクリックします。

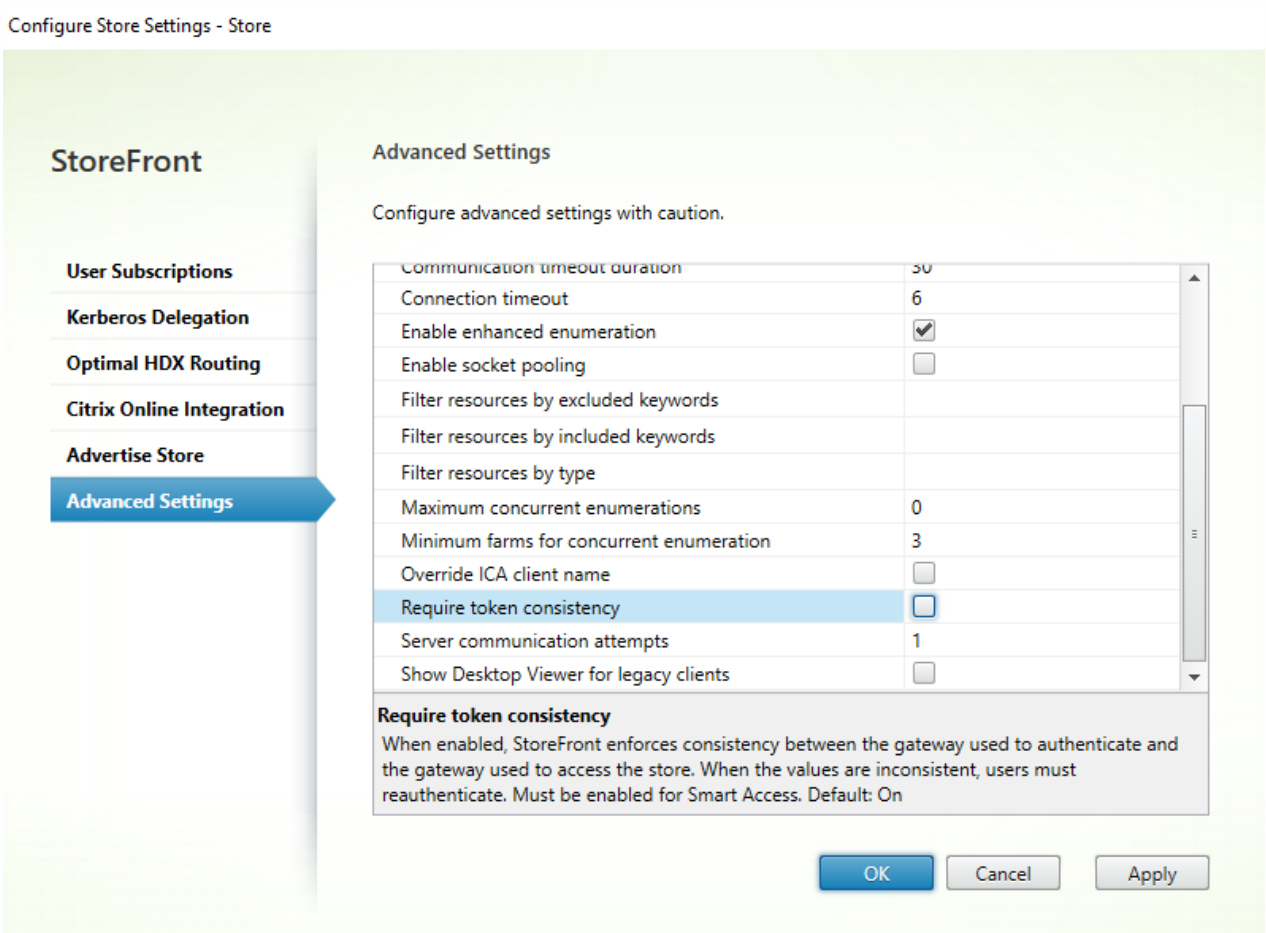


1. Citrix StoreFront管理コンソールの左ペインで **[ストア]** を選択して、結果ペインでストアを選択します。 **[操作]** ペインで **[リモートアクセス設定の構成]** をクリックします。
2. **[リモートPCアクセスを有効にする]** を選択します。
3. NetScaler Gatewayがストアに登録されたことを確認します。NetScaler Gatewayが登録されていないと、STAチケット発行機能は機能しません。



1. Citrix StoreFront管理コンソールの左ペインで **[ストア]** を選択して、結果ペインでストアを選択します。 **[操作]** ペインで、 **[ストア設定の構成]** を選択します。

2. ［ストア設定の構成］ページで、**［詳細な設定］**を選択します。
3. **［トークンの一貫性を要求する］**チェックボックスをオフにします。詳しくは、「上級ストア設定」を参照してください。
4. **［OK］**をクリックします。



注意

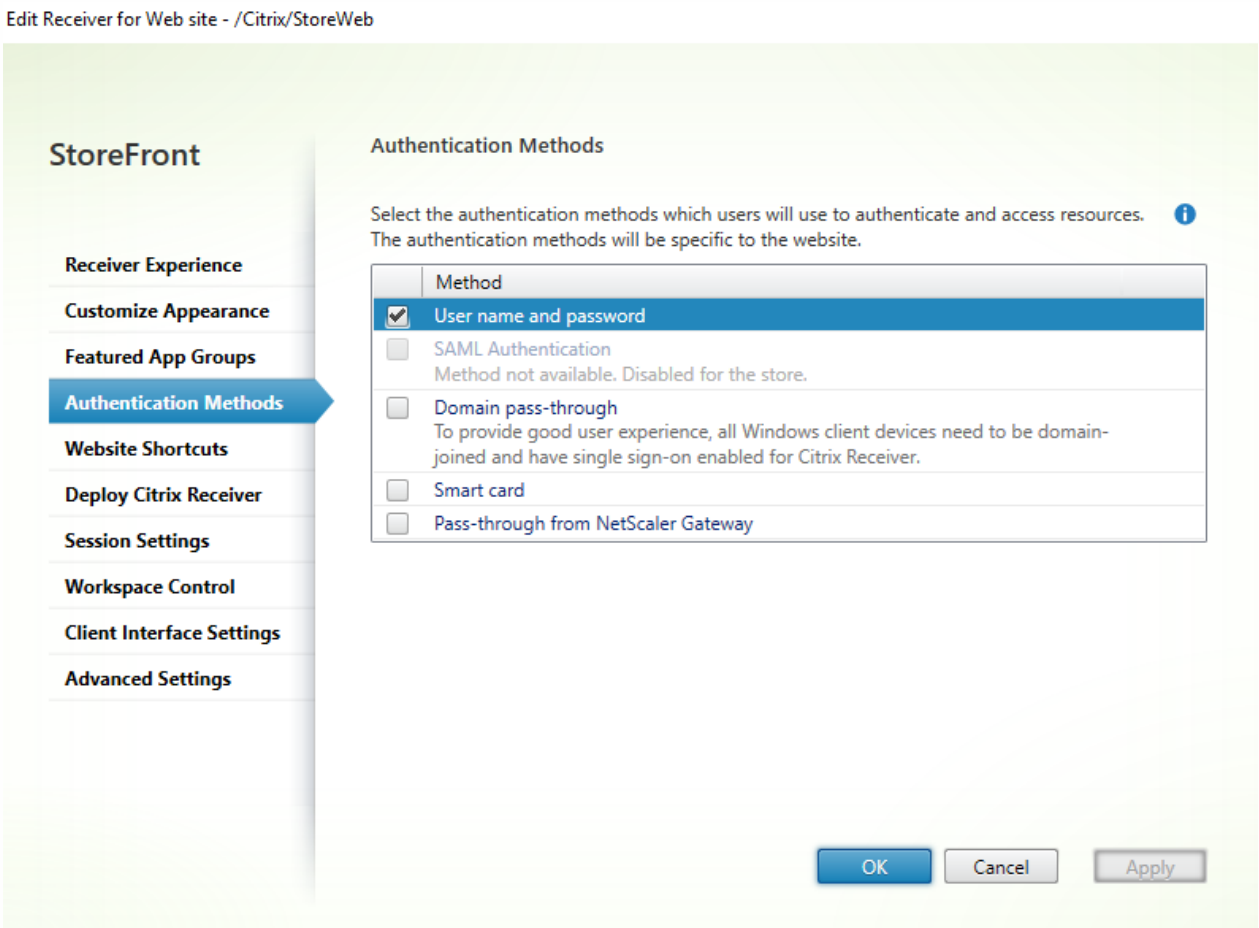
［トークンの一貫性を要求する］設定はデフォルトでオンになっています。この設定を無効にすると、NetScaler End Point Analysis（EPA）SmartAccess機能が停止します。SmartAccessについて詳しくは、CTX138110を参照してください。

Important

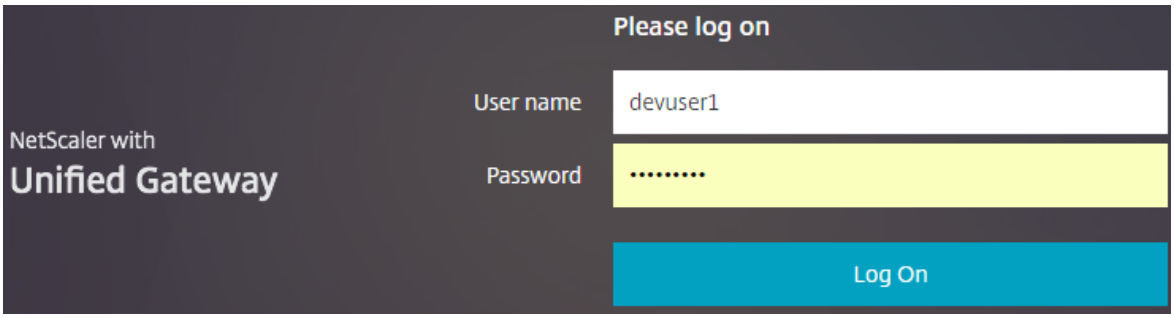
NetScaler Gatewayからのパススルーを無効にすると、Receiver for WebがNetScalerから渡されたproduction.comドメインの誤った資格情報を使用しないようにできます。NetScaler Gatewayからのパススルーを無効にすると、Receiver for Webがユーザーに資格情報の入力を求めます。これらの資格情報は、Netscaler Gatewayでログオンする場合に使用する資格情報とは異なります。

1. Citrix StoreFront管理コンソールの左ペインで、**［ストア］**を選択します。

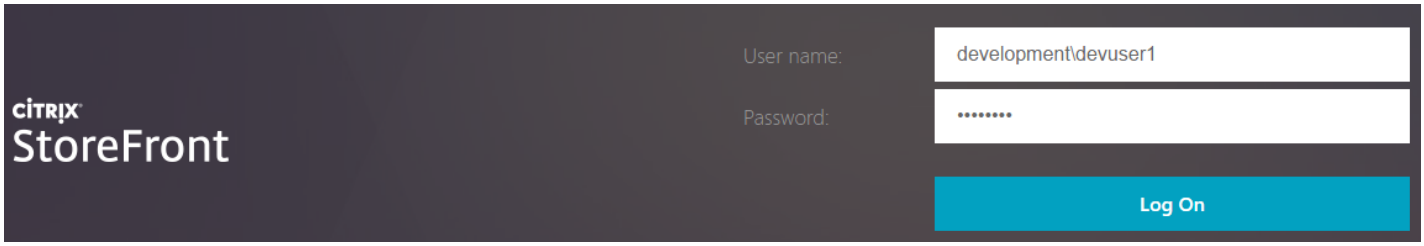
2. 変更するストアを選択します。
3. ［操作］ペインで［Receiver for Webサイトの管理］をクリックします。
4. 認証方法で、［NetScaler Gatewayからのパススルー］チェックボックスをオフにします。
5. ［OK］をクリックします。



テストのために、production.comユーザー名およびパスワードを使用して、NetScaler Gatewayにログオンします。



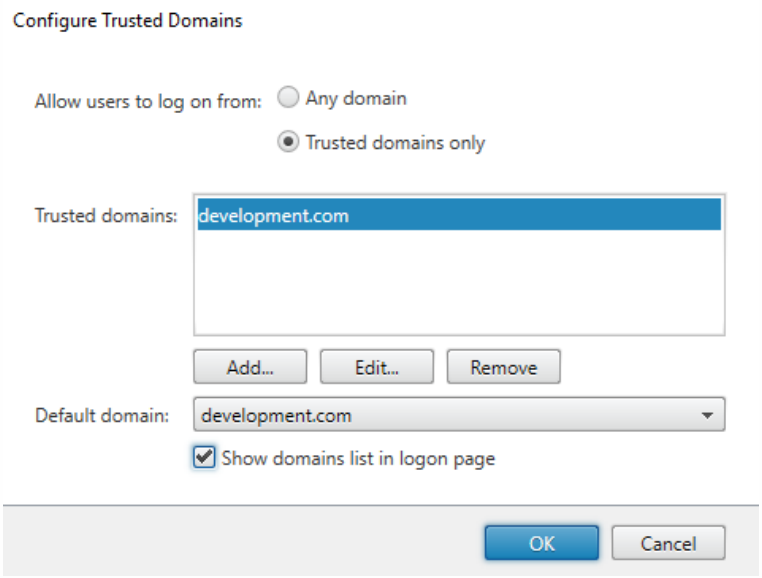
ログオン後、ユーザーはdevelopment.comの資格情報を入力するよう求められます。

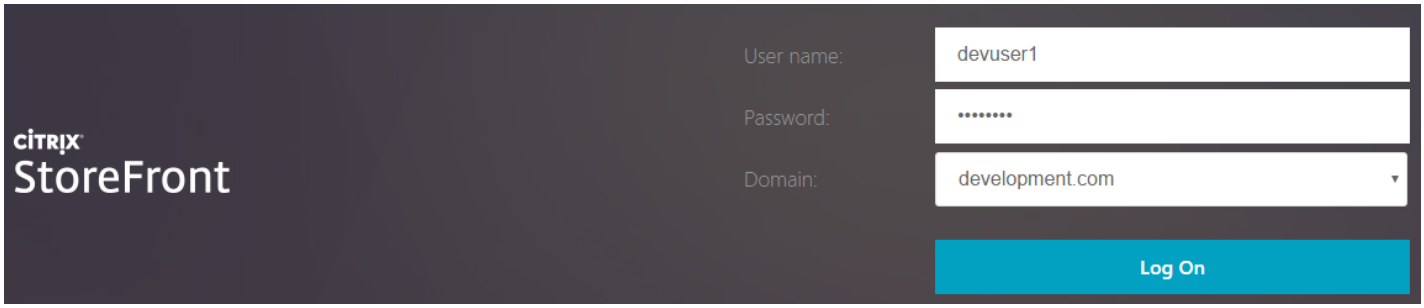


この設定はオプションですが、これによってNetScaler Gateway経由の認証で誤ったドメインの入力を回避できる場合があります。

両方のドメインで同じユーザー名を使用する場合、誤ったドメインを入力する可能性が高くなります。慣れていないユーザーが、NetScaler Gateway経由でログオンする時、ドメインの入力を省略することもあります。その後、Receiver for Webサイトにログオンするよう求められると、ドメインでドメイン\ユーザー名の入力を忘れる可能性があります。

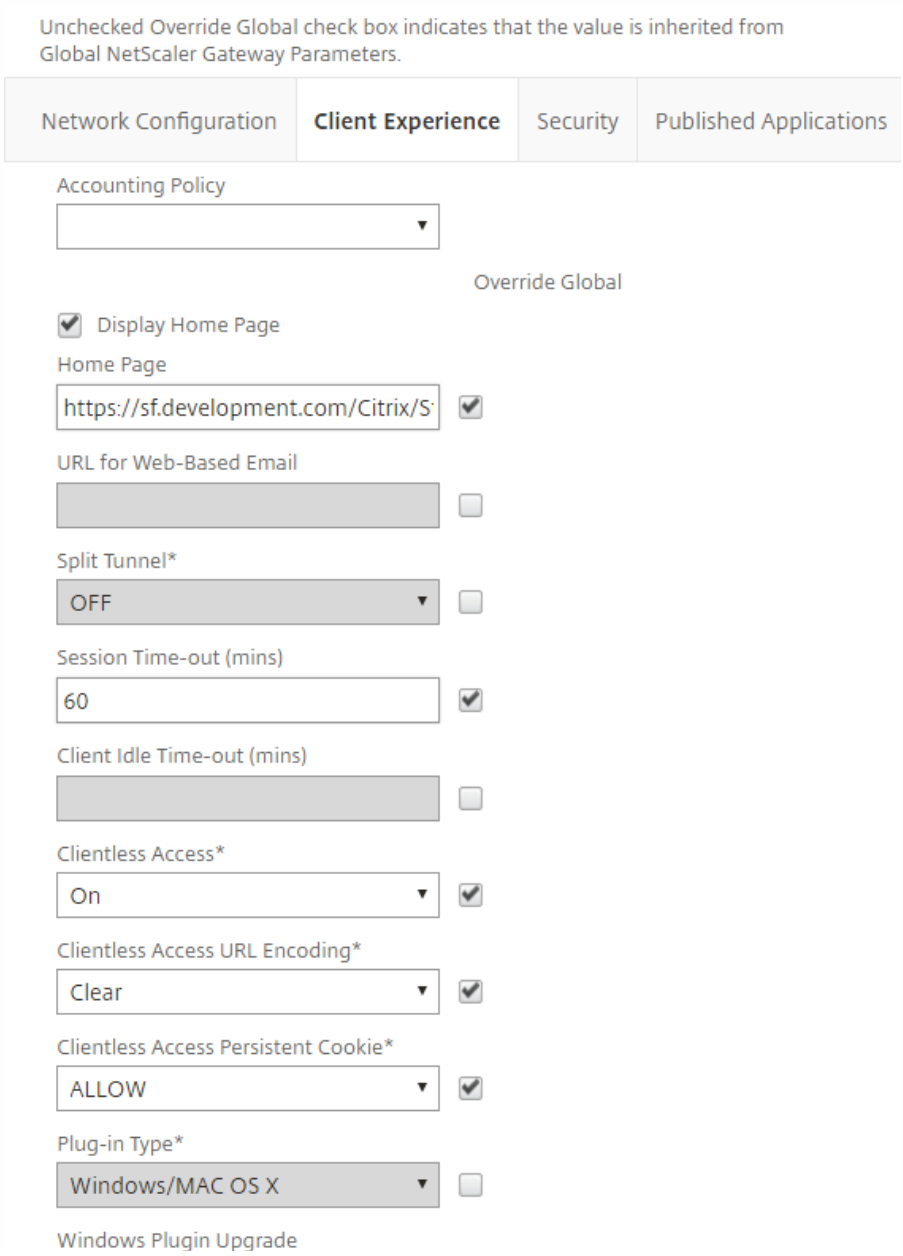
1. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、 **[操作]** ペインの **[認証方法の管理]** をクリックします。
2. **[ユーザー名とパスワード]** の横の下向き矢印を選択します。
3. **[追加]** を選択して、development.comを信頼済みドメインとして追加し、**[ログオンページにドメイン一覧を表示する]** チェックボックスをオンにします。
4. **[OK]** をクリックします。

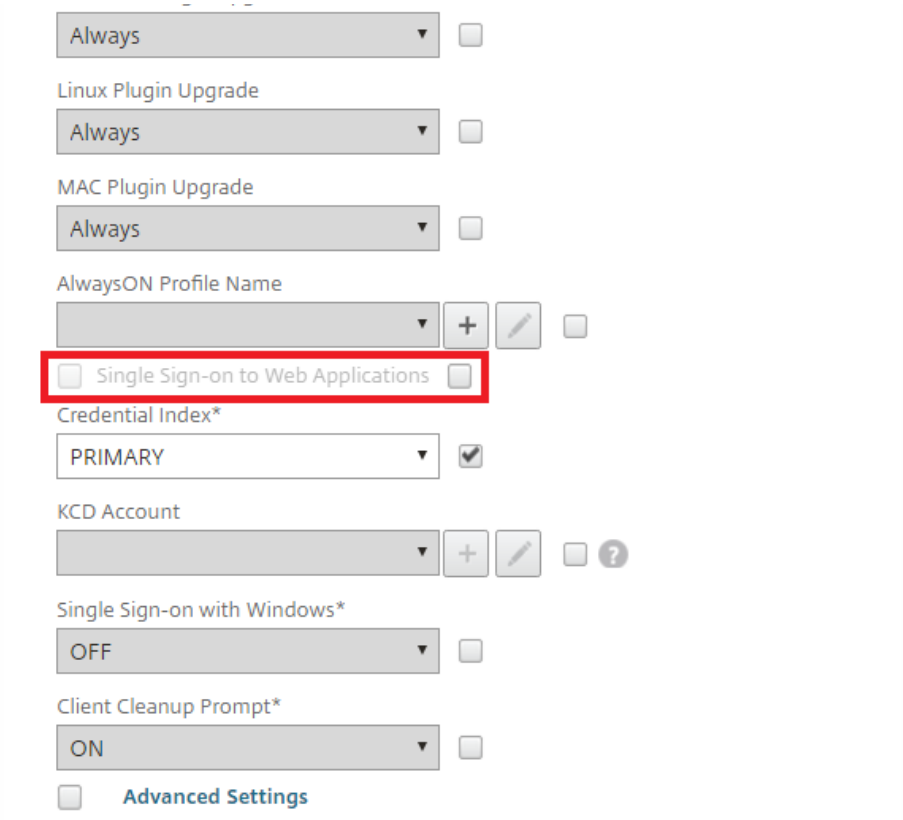


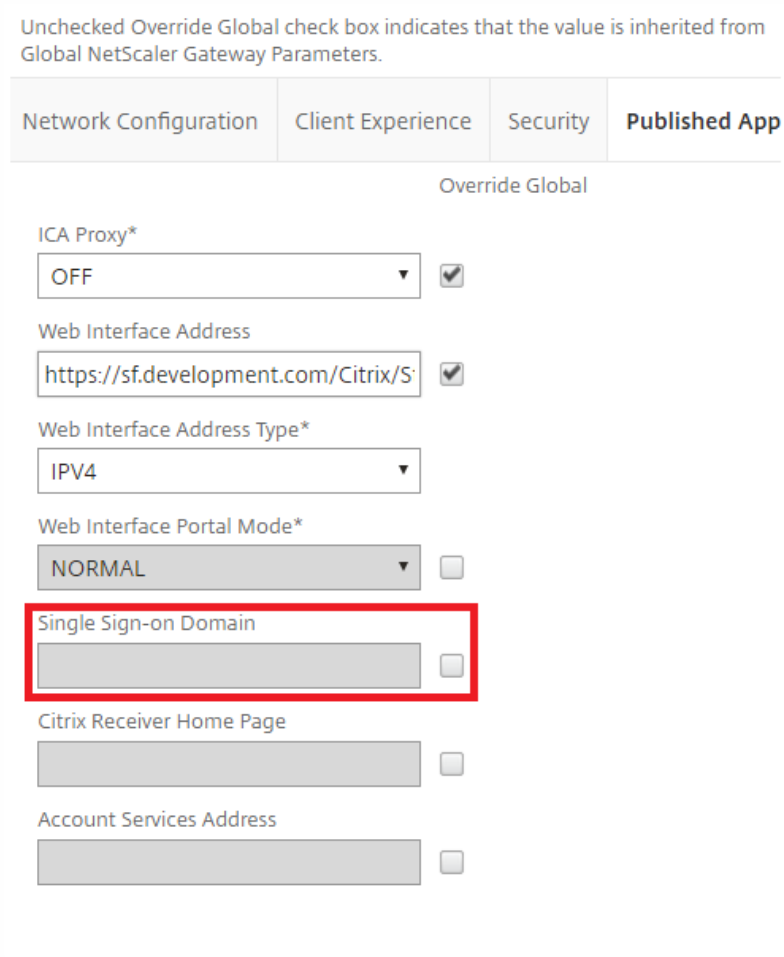


> **注意**
>
> この認証方法では、ブラウザーのパスワードキャッシュ機能は使用しないでください。2つの異なるドメインアカウントに異なるパスワードがある場合、パスワードキャッシュによって操作が複雑になる可能性があります。

- NetScalerセッションポリシーでWebアプリケーションへのシングルサインオン機能が有効になっていると、NetScalerからReceiver for Webに送信された正しくない資格情報は無視されます。これは、Receiver for Webで **[NetScaler Gatewayからのパススルー]** 認証方法が無効になっているためです。このオプションがどのように設定されていても、Receiver for Webは資格情報を求めます。
- NetScalerの［Client Experience］および［Published Applications］タブでシングルサインオンを指定しても、ここで説明された動作は影響を受けません。







ビーコンポイントの構成

Aug 14, 2017

ビーコンポイントとして使用する、内部ネットワークの内側と外側のURLを指定するには、[ビーコンの管理]タスクを使用します。Citrix Receiverは、ユーザーがローカルネットワークと公共のネットワークのどちらに接続しているのかをビーコンポイントを使用して識別します。ユーザーがデスクトップやアプリケーションにアクセスすると、そのリソースを提供するサーバーがそのユーザーの位置情報に基づいて適切な接続詳細をCitrix Receiverに返します。これにより、ユーザーがデスクトップやアプリケーションにアクセスするときに再ログオンする必要がなくなります。

たとえば、内部ビーコンポイントにアクセス可能な場合、そのユーザーはローカルネットワークに接続していると認識されます。これに対し、Citrix Receiverで内部ビーコンポイントにアクセスできず、2つの外部ビーコンポイントからの応答を受信した場合、そのユーザーは社内ネットワークの外からインターネット経由で接続していると認識されます。この場合、このユーザーはデスクトップやアプリケーションにNetScaler Gateway経由で接続する必要があります。ユーザーがデスクトップやアプリケーションにアクセスすると、そのリソースを提供するサーバーが、使用されるべきNetScaler Gatewayアプライアンスの詳細を提供します。このため、ユーザーがそのNetScaler Gatewayアプライアンスにログオンする必要はありません。

StoreFrontでは、内部ビーコンポイントとしてデフォルトでサーバーのURLまたは負荷分散URLが使用されます。外部ビーコンポイントは、デフォルトでCitrix社のWebサイト、および管理者が追加した最初のNetScaler Gateway仮想サーバーまたはユーザーログオンポイント（Access Gateway 5.0の場合）のURLが使用されます。

ビーコンポイントの設定を変更する場合は、そのビーコンポイントをユーザーに通知してCitrix Receiverの設定を変更させる必要があります。ストアのReceiver for Webサイトが構成済みの場合、ユーザーはそのサイトから最新のCitrix Receiverプロビジョニングファイルを入手できます。Citrix Receiver for Webサイトが構成済みでない場合は、管理者がストアのプロビジョニングファイルをエクスポートしてユーザーに提供します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、［操作］ペインの［ビーコンの管理］をクリックします。
3. 内部ビーコンポイントとして使用するURLを指定します。
   - StoreFront展開環境でサーバーのURLまたは負荷分散URLを使用するには、［サービスURLを使用する］を選択します。
   - 別のURLを使用するには、［ビーコンアドレスを指定する］を選択して、内部ネットワーク内の可用性の高いURLを入力します。
4. 外部ビーコンポイントのURLを入力するには、［追加］をクリックします。ビーコンポイントを変更するには、［外部ビーコン］ボックスの一覧でURLを選択して［編集］をクリックします。ビーコンポイントとしてそのアドレスが使われないようにするには、一覧でURLを選択して［削除］をクリックします。
   公共のネットワーク上で解決でき、可用性の高い外部ビーコンポイントを少なくとも2つ指定する必要があります。ビーコンURLは、http://domainなどの簡略化されたNetBIOS名ではなく、http://domain.comなどの完全修飾ドメイン名にする必要があります。これにより、内部ネットワークとユーザーの間に、ホテルやインターネットカフェなど、インターネットペイウォール（有料の壁）があるかどうかをCitrix Receiverで判別できるようになります。インターネットペイウォールがある場合、すべての外部ビーコンポイントが同じプロキシに接続されます。

詳細構成

Aug 14, 2017

StoreFrontコンソールにより、PowerShell、証明書プロパティ、または構成ファイルを使って構成できる詳細オプションを有効にできます。

デスクトップアプライアンスサイトの構成	デスクトップアプライアンスサイトを作成、削除、および変更します。
ストアに内部および外部アクセスするための単一のFQDNの作成	会社のネットワーク内外のクライアント用に単一の完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）を作成することで、そのネットワーク内、およびネットワーク外からNetScaler Gateway経由でリソースにアクセスするユーザーの使い勝手を簡素化します。
リソースフィルターの構成	リソースの種類やキーワードを使用して、列挙されるリソースを指定します。

デスクトップアプライアンスサイトの構成

Aug 14, 2017

以下のタスクでは、デスクトップアプライアンスサイトを作成、削除、および変更する方法について説明します。サイトを作成または削除するには、Windows PowerShellコマンドを実行します。デスクトップアプライアンスサイトの設定を変更するには、サイトの構成ファイルを編集します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。
注：StoreFront管理コンソールとPowerShellコンソールを同時に開くことはできません。StoreFront管理コンソールを閉じてからPowerShellコンソールを開いてください。同様に、PowerShellのすべてのインスタンスを閉じてからStoreFront管理コンソールを開いてください。

1つのデスクトップアプライアンスサイトから複数のストアにアクセスすることはできません。管理者は、単一のストアを作成してユーザーすべてのリソースをドメイン不参加のデスクトップアプライアンスで提供できます。または、異なるデスクトップアプライアンスサイトにアクセスする個別のストアを作成して、ユーザーのデスクトップアプライアンスが適切なサイトに接続するように構成します。

1. ローカルの管理者アカウントを使ってWindows PowerShellを起動して、コマンドプロンプトで次のコマンドを実行します。これにより、StoreFrontモジュールがインポートされます。
   & "installationlocation\Scripts\ImportModules.ps1"
   installationlocationはStoreFrontのインストール先フォルダーで、通常C:\Program Files\Citrix\Receiver StoreFront\です。
2. 新しいデスクトップアプライアンスサイトを作成するには、次のコマンドを入力します。
   Install-DSDesktopAppliance -FriendlyName sitename -SiteId iisid -VirtualPath sitepath -UseHttps {$False | $True} -StoreUrl storeaddress [-EnableMultiDesktop {$False | $True}] [-EnableExplicit {$True
   ここで、<sitename>でこのデスクトップアプライアンスサイトに対するわかりやすい名前を指定します。iisidは、StoreFrontをホストしているMicrosoftインターネットインフォメーションサービス（IIS）サイトの数値IDを指定します。この値は、インターネットインフォメーションサービス（IIS）マネージャーコンソールから取得します。<sitepath>は、IIS内でサイトを作成する相対パスを指定します（/Citrix/DesktopApplianceなど）。デスクトップアプライアンスサイトのURLでは大文字と小文字が区別されることに注意してください。

   -UseHttpsでは、StoreFrontをHTTPS用に構成する（True）かしない（False）か指定します。

   デスクトップアプライアンスコネクタサイトで使用されるストアサービスの絶対URLを指定するにはStoreUrl <storeaddress>を使用します。この値は、管理コンソールの［ストア］ノードの概要に表示されます。

   デフォルトでは、ユーザーがデスクトップアプライアンスサイトにログオンすると、そのユーザーが使用できる最初のデスクトップが自動的に起動します。このデスクトップアプライアンスサイトでユーザーが複数のデスクトップから使用するものを選択できるようにするには、-EnableMultiDesktopをTrueに設定します。

   新しいサイトを作成すると、指定ユーザー認証がデフォルトで有効になります。指定ユーザー認証を無効にするには、-EnableExplicitを$Falseに設定します。スマートカード認証を有効にするには、-EnableSmartCardを$Trueに設定します。スマートカードパススルー認証を有効にする場合は、-EnableSmartCardと-EnableEmbeddedSmartCardSSOの両方を$Trueに設定する必要があります。指定ユーザーのスマートカード認証または指定ユーザーのスマートカードパススルー認証を有効にすると、ユーザーはまずスマートカードによるログオンが求められますが、スマートカードに問題がある場合は指定ユーザー認証に切り替わります。

   オプションの引数で構成する設定は、デスクトップアプライアンスサイトを作成した後でもサイトの構成ファイルを編集して変更できます。

   たとえば、次のように指定します。

   IISのDefault Web Siteの仮想パス/Citrix/DesktopAppliance1にデスクトップアプライアンスサイトを作成します。

   ```
   Install-DSDesktopAppliance `

   -FriendlyName DesktopAppliance1 `

   -SiteId 1 `

   -VirtualPath /Citrix/DesktopAppliance1 `

   -UseHttps $false `

   -StoreUrl https://serverName/Citrix/Store `

   -EnableMultiDesktop $true `

   -EnableExplicit $true `

   -EnableSmartCard $true `

   -EnableEmbeddedSmartCardSSO $false
   ```

3. 既存のデスクトップアプライアンスサイトを削除するには、次のコマンドを入力します。
   Remove-DSDesktopAppliance -SiteId iisid -VirtualPath sitepath
   ここで、<iisid>はStoreFrontをホストするIISサイトの数値IDで、<sitepath>はIIS内でのデスクトップアプライアンスサイトの相対パスです（/Citrix/DesktopApplianceなど）。
4. StoreFront展開環境で現在使用できるデスクトップアプライアンスサイトの一覧を表示するには、次のコマンドを入力します。
   Get-DSDesktopAppliancesSummary

デスクトップアプライアンスサイトは、指定ユーザー認証、スマートカード認証、スマートカードパススルー認証をサポートします。デフォルトでは、指定ユーザー認証が有効になります。指定ユーザーのスマートカード認証または指定ユーザーのスマートカードパススルー認証を有効にした場合のデフォルトの動作では、まずスマートカードによるログオンが求められます。スマートカードでログオンできない場合は、資格情報を入力してログオンできます（指定ユーザー認証）。すべてのStoreFront URLへのHTTPS接続に対してクライアント証明書が必要となるようにIISを構成した環境では、ユーザーがスマートカードでログオンできない場合に指定ユーザー認証でログオンできません。デスクトップアプライアンスサイトの認証方法を構成するには、サイトの構成ファイルを編集します。

1. テキストエディターを使ってデスクトップアプライアンスサイトのweb.configファイルを開きます。このファイルは通常、C:\inetpub\wwwroot\Citrix\storenameDesktopApplianceディレクトリにあります。ここで、storenameはストアの作成時に指定した名前です。
2. ファイル内で次の要素を検索します。

3. サイトの指定ユーザー認証を無効にするには、enabled属性の値をfalseに変更します。
4. ファイル内で次の要素を検索します。

5. スマートカード認証を有効にするには、enabled属性の値をtrueに設定します。スマートカードパススルー認証を有効にするには、useEmbeddedSmartcardSso属性の値もtrueに設定する必要があります。PIN入力画面の表示がタイムアウトするまでの時間を時間、分、秒で設定するには、embeddedSmartcardSsoPinTimeout属性を使用します。PIN入力画面がタイムアウトするとログオン画面に戻ります。PIN入力画面を再び表示するには、スマートカードをいったん取り出してから再挿入する必要があります。デフォルトのタイムアウト時間は20秒です。

デフォルトでは、ユーザーがデスクトップアプライアンスサイトにログオンすると、そのユーザーに提供されているデスクトップのうち（アルファベット順で）最初のデスクトップが自動的に起動します。ストアで複数のデスクトップをユーザーに提供する場合は、デスクトップアプライアンスサイトに複数のデスクトップを表示して、ユーザーが選択できるように構成できます。これらの設定を変更するには、サイトの構成ファイルを編集します。

1. テキストエディターを使ってデスクトップアプライアンスサイトのweb.configファイルを開きます。このファイルは通常、C:\inetpub\wwwroot\Citrix\storenameDesktopApplianceディレクトリにあります。ここで、storenameはストアの作成時に指定した名前です。
2. ファイル内で次の要素を検索します。
3. ユーザーがデスクトップアプライアンスサイトにログオンしたときにストアで使用できるすべてのデスクトップを表示して選択できるようにするにはshowMultiDesktop属性の値をtrueに変更します。

ストアに内部および外部アクセスするための単一のFQDNの作成

Aug 14, 2017

注：この機能をネイティブのReceiverで使用するには、以下のバージョンが必要です。

- Windows Receiver 4.2
- Receiver for Mac 11.9

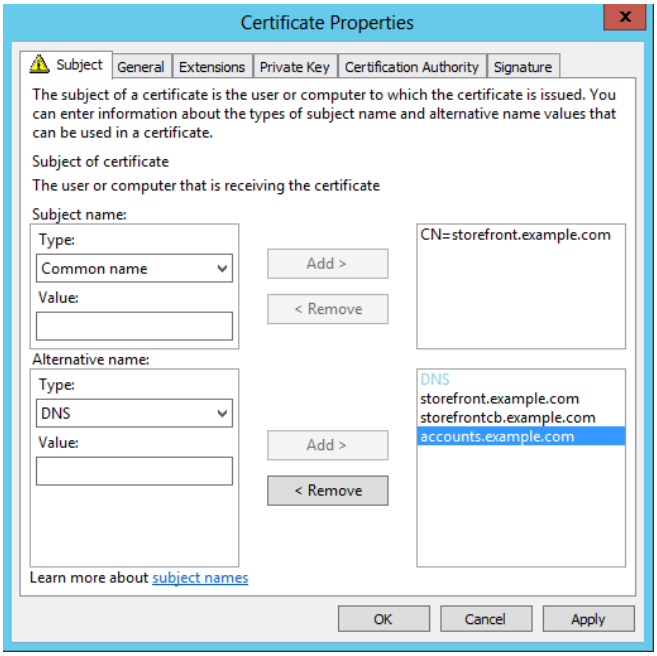
会社のネットワーク内外のクライアント用に単一の完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）を作成することで、そのネットワーク内、およびネットワーク外からNetScaler Gateway経由でリソースにアクセスするユーザーの使い勝手を簡素化することができます。

単一のFQDNを作成すると、ユーザーが各プラットフォーム用のReceiverを簡単に構成できるようになりますネットワーク内からアクセスする場合もインターネット経由で外部からアクセスする場合も、ユーザーが覚える必要のあるURLは1つのみになります。

Citrix Receiverは、ユーザーがローカルネットワークと公共のネットワークのどちらに接続しているのかをビーコンポイントを使用して識別します。ユーザーがデスクトップやアプリケーションにアクセスすると、そのリソースを提供するサーバーがそのユーザーの位置情報に基づいて適切な接続詳細をCitrix Receiverに返します。これにより、ユーザーがデスクトップやアプリケーションにアクセスするときに再ログオンする必要がなくなります。ビーコンポイントの構成については、「ビーコンポイントを構成」を参照してください。

外部のクライアントが会社のネットワーク外からリソースにアクセスしようとしたときに、共有FQDNはDMZの外部ファイアウォールルーターインターフェイスのIP、またはNetScaler Gateway仮想サーバーのIPに解決されます。SSL証明書の［Common Name］（一般名）フィールドと［Subject Alternative Name］（SAN：サブジェクトの別名）フィールドに、ストアの外部アクセスに使用する共有FQDNが含まれていることを確認します。ゲートウェイ証明書への署名に、会社の証明機関（Certification Authority：CA）ではなくVerisign社などのサードパーティのルートCAを使用すると、すべての外部クライアントは、NetScaler Gateway仮想サーバーの証明書を自動的に信頼します。Verisign社などのサードパーティのルートCAを使用する場合は、外部クライアントに追加のルートCA証明書をインポートする必要はありません。

NetScaler GatewayとStoreFrontサーバーの両方に対して、共有FQDNの一般名を使用して単一の証明書を展開する場合は、リモート検出をサポートするかどうかを検討します。サポートする場合は、証明書がSANの仕様に準拠していることを確認してください。



NetScaler Gateway仮想サーバーの証明書の例：storefront.example.com

1. 共有FQDN、コールバックURL、およびアカウントエイリアスURLが、SANとして［DNS］フィールドに含まれていることを確認します。
2. 証明書と秘密キーをNetScaler Gatewayにインポートできるように、秘密キーがエクスポート可能になっていることを確認します。
3. Default AuthorizationがAllowと設定されていることを確認します。
4. Verisign社などのサードパーティのCA、または会社のルートCAを使用して証明書に署名します。

2ノードサーバーグループのSANの例：

storefront.example.com（必須）

storefrontcb.example.com（必須）

accounts.example.com（必須）

storefrontserver1.example.com（オプション）

storefrontserver2.example.com（オプション）

NetScaler Gateway仮想サーバーのSSL証明書の署名

要件に応じて、2つの種類のCA署名付き証明書を選択できます。

- サードパーティのCA署名付き証明書 - NetScaler Gateway仮想サーバーの証明書が信頼されたサードパーティによって署名されている場合は、外部クライアントの信頼されたルートCA証明書ストアにCA証明書をコピーする必要はほとんどありません。Windowsクライアントには、一般的なほとんどの署名機関のルートCA証明書が付属しています。使用できる商用のサードパーティCAの例としては、DigiCert、Thawte、Verisignなどがあります。ただし、iPad、iPhone、Androidタブレットや電話などのモバイルデバイスには、ルートCAをデバイスにコピーして、NetScaler Gateway仮想サーバーを信頼するように構成することが必要な場合があります。
- 会社のルートCA署名付き証明書 — これを選択する場合は、すべての外部クライアントの信頼されたルートCAストアに会社のルートCA証明書をコピーする必要があります。iPhoneやiPadなどのポータブルデバイスにネイティブのReceiverをインストールしている場合は、これらのデバイスでセキュリティプロファイルを作成します。

ポータブルデバイスへのルート証明書のインポート

- 通常、iOSデバイスのローカルストレージにアクセスすることはできないので、iOSデバイスではメールの添付ファイルを使用して.CER x.509証明書ファイルをインポートします。
- Androidデバイスにも同じ.CER x.509形式が必要です。証明書は、デバイスのローカルストレージまたはメールの添付ファイルからインポートできます。

外部DNS：storefront.example.com

組織のインターネットサービスプロバイダーによって提供されるDNS解決によって、DMZの外部境界に位置するファイアウォールルーターの外部に対するIPや、NetScaler Gateway仮想サーバーの仮想IPが解決されるようにします。

スプリットビューDNS

- スプリットビューDNSを正しく構成すると、DNS要求の送信元アドレスに応じてクライアントに正しいDNS Aレコードが送信されます。
- 公共ネットワークと社内ネットワーク間を移動するクライアントのIPアドレスは、それに応じて変更されます。クライアントがstorefront.example.comを照会すると、そのときの接続先ネットワークに応じて適切なAレコードを受信します。

Windows CAがNetScaler Gatewayに発行した証明書のインポート

WinSCPは、WindowsマシンからNetScaler Gatewayファイルシステムへのファイル移動に役立つ無料のサードパーティツールです。インポートする証明書を、NetScaler Gatewayファイルシステム内の/nsconfig/ssl/フォルダーにコピーします。NetScaler Gateway上でOpenSSLツールを使用して、証明書とキーをPKCS12/PFXファイルから抽出し、NetScaler Gatewayで使用できるPEM形式で、2つの別々のCERファイルとKEY X.509ファイルを作成することができます。

1. このPFXファイルをNetScaler GatewayアプライアンスまたはVPXの/nsconfig/sslにコピーします。
2. NetScaler Gatewayのコマンドラインインターフェイスを開きます。
3. FreeBSDシェルに切り替えるために、Shellと入力して、NetScaler Gatewayのコマンドラインインターフェイスを終了します。
4. フォルダーを変更するために、cd /nsconfig/sslと入力します。
5. openssl pkcs12 -in <imported cert file>.pfx -nokeys -out <certfilename>.cerを実行し、画面のメッセージに従ってPFXパスワードを入力します。
6. openssl pkcs12 -in <imported cert file>.pfx -nocerts -out <keyfilename>.keyを実行します。
7. 画面のメッセージに従ってPFXパスワードを入力し、次に、秘密キーのPEMパスフレーズを設定してKEYファイルを保護します。
8. /nsconfig/ssl/内にCERファイルとKEYファイルが正常に作成されたことを確認するには、ls –alを実行します。
9. NetScaler Gatewayのコマンドラインインターフェイスに戻るために、Exitと入力します。

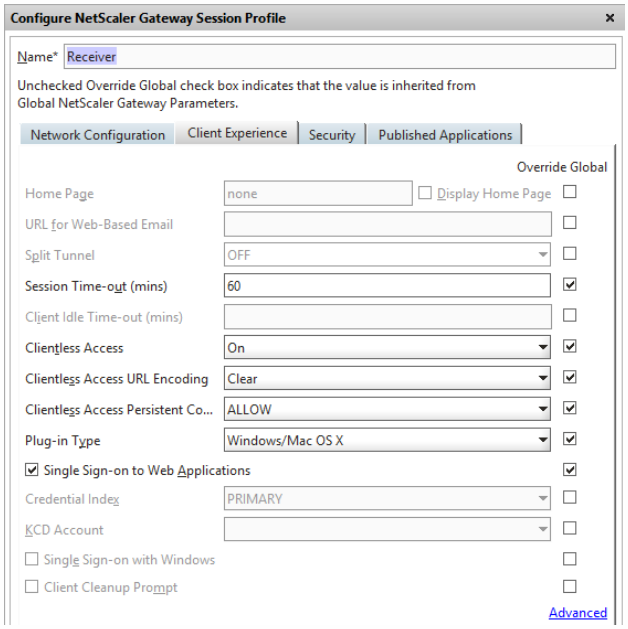
REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS

REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS

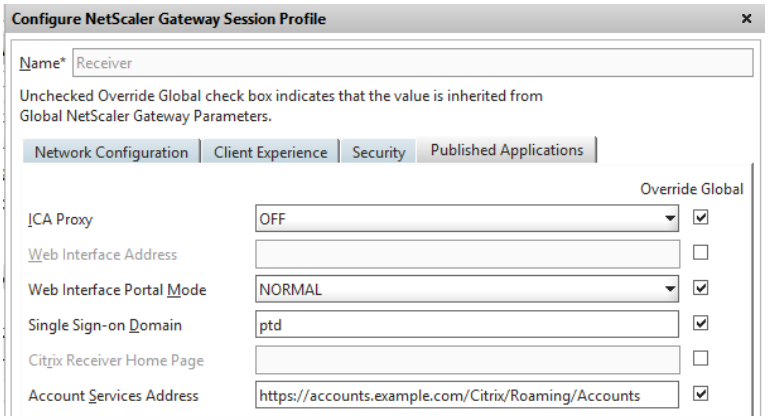
cVPNとSmartAccessの設定

SmartAccessを使用している場合、NetScaler Gateway仮想サーバーのプロパティページで、SmartAccessモードを有効にします。この場合、リモートリソースに同時にアクセスするすべてのユーザー用のユニバーサルライセンスが必要です。

Receiverのプロファイル

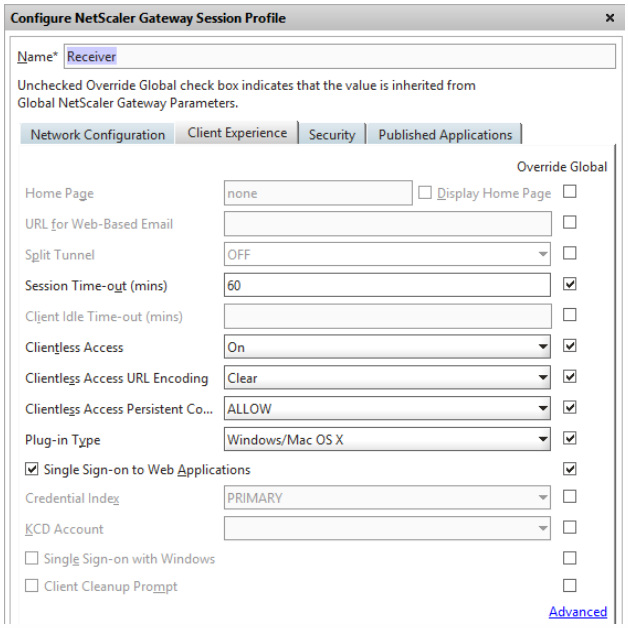


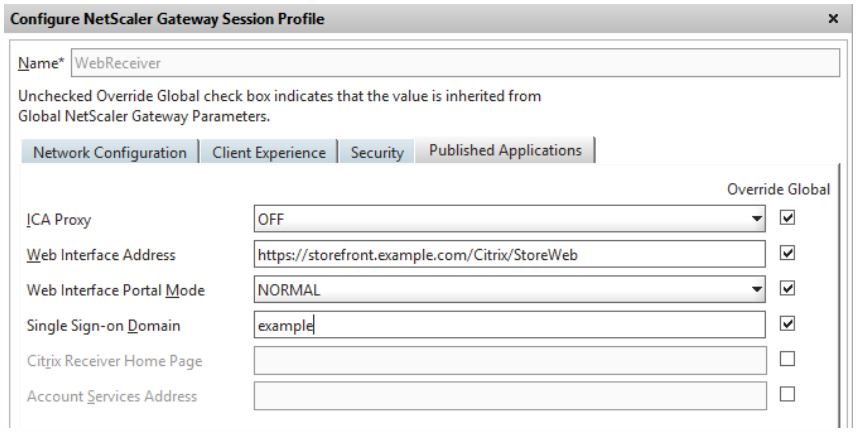
セッションプロファイルアカウントサービスのURLとして、https://storefront.example.com/Citrix/Roaming/Accountsではなくhttps://accounts.example.com/Citrix/Roaming/Accountsを構成します。



また、StoreFrontサーバーの認証用およびローミング用の各web.configファイルにも、このURLを追加の<allowedAudiences>として追加します。詳しくは、後述の「StoreFrontサーバーのホストベースURL、ゲートウェイ、SSL証明書の構成」を参照してください。

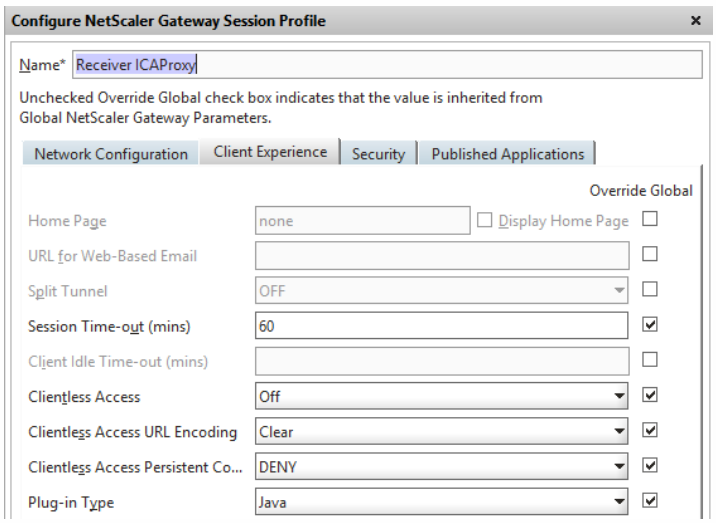
Receiver for Webのプロファイル

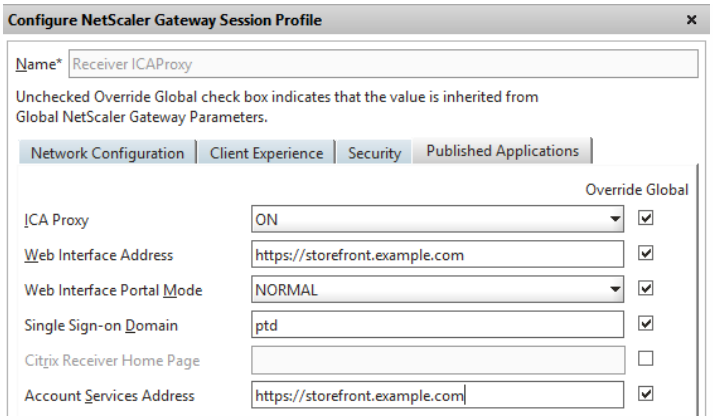




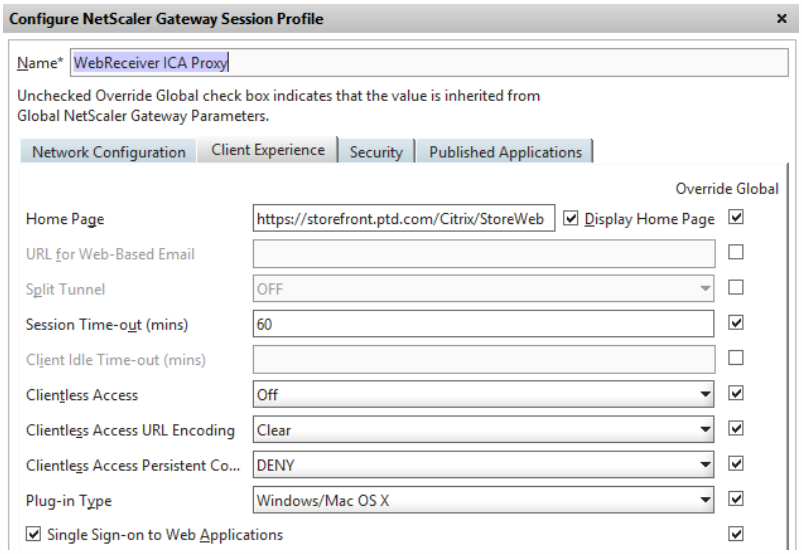
ICAプロキシを使用している場合、NetScaler Gateway仮想サーバーのプロパティページで、基本モードを有効にします。1つのNetscalerプラットフォームライセンスのみが必要です。

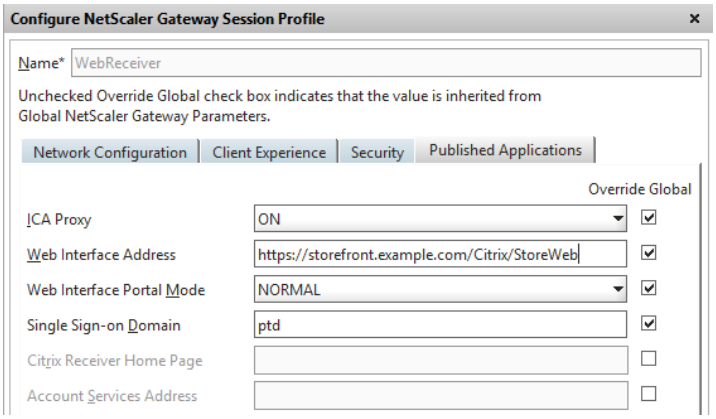
Receiverのプロファイル





Receiver for Webのプロファイル





ストアをホストするStoreFrontクラスターまたは単一のStoreFront IPが作成されている場合は、NetScaler Gateway仮想サーバーに解決される共有FQDNがStoreFrontのロードバランサーにも直接解決される必要があります。

内部DNS：3つのDNS Aレコードを作成します。

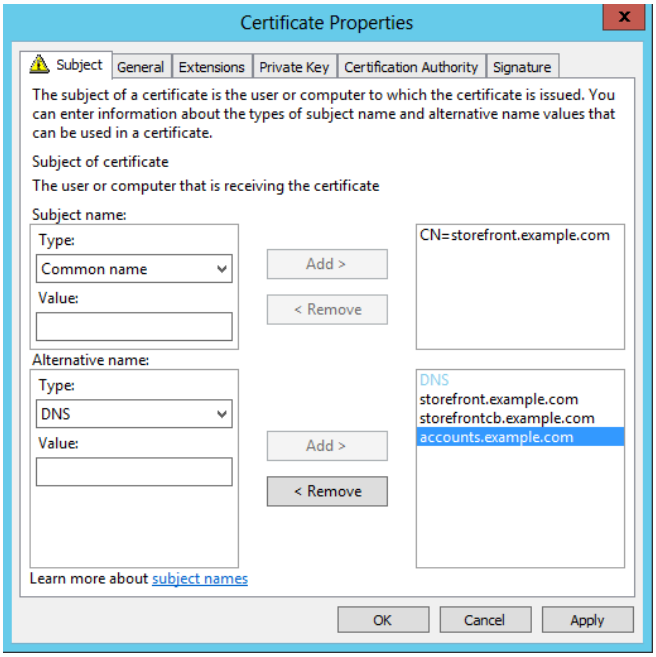
- storefront.example.comがStoreFrontのロードバランサーまたは単一のStoreFrontサーバーIPに解決される必要があります。
- storefrontcb.example.comがゲートウェイの仮想サーバーの仮想IPに解決される必要があるので、DMZと会社のローカル

ネットワークの間にファイアウォールがある場合は、これを許可します。

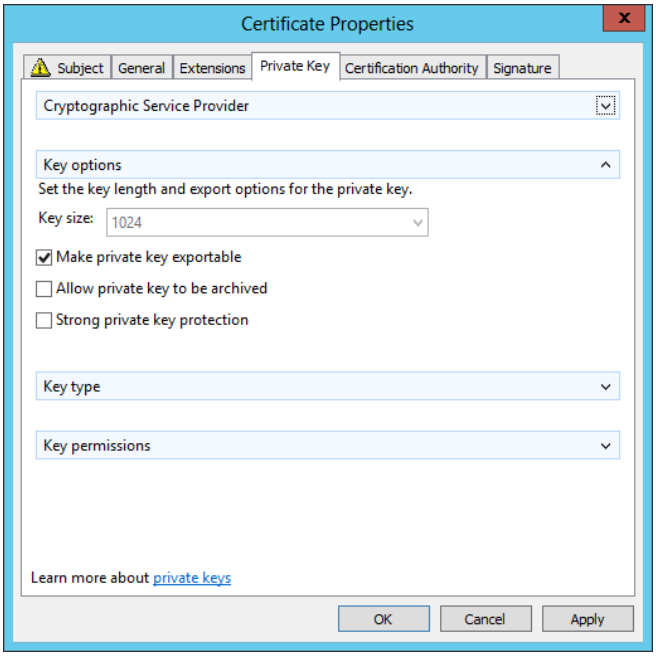
- accounts.example.com — storefront.example.comのDNSエイリアスとして作成します。StoreFrontクラスターのロードバランサーIPまたは単一のStoreFrontサーバーIPにも解決されます。

StoreFrontサーバー証明書の例：storefront.example.com

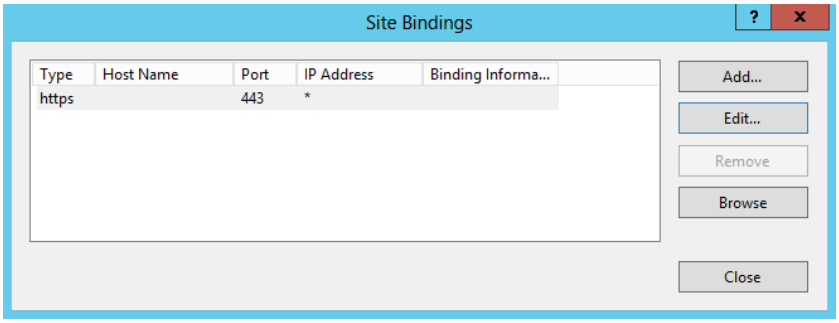
1. StoreFrontをインストールする前に、StoreFrontサーバーまたはサーバーグループ用の適切な証明書を作成します。
2. 共有FQDNを［Common name］フィールドと［DNS］フィールドに追加します。これが、先に作成したNetScaler Gateway仮想サーバーのSSL証明書で使用されるFQDNと一致することを確認します。または、NetScaler Gateway仮想サーバーと同じ証明書を使用します。
3. 別のSANとしてアカウントエイリアス（accounts.example.com）を証明書に追加します。SANで使用されるアカウントエイリアスは、前述の手順（「**ネイティブReceiver Gatewayのセッションポリシーとプロファイル**」）の［Configure NetScaler Gateway Session Profile］画面で使用したものであることに注意してください。



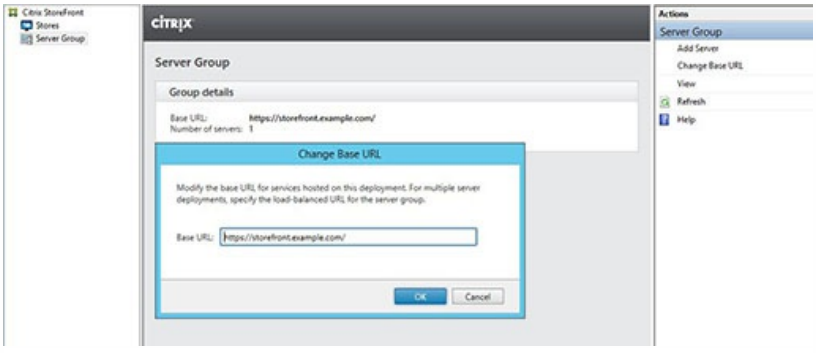
4. 秘密キーをエクスポート可能にして、証明書を別のサーバーまたは複数のStoreFrontサーバーグループノードに転送できるようにします。



5. VeriSign社などのサードパーティのCA、会社のルートCA、または中間CAを使用して証明書に署名します。
6. 秘密キーを含めて、この証明書をPFX形式でエクスポートします。
7. 証明書と秘密キーをStoreFrontサーバーにインポートします。Windows NLB StoreFrontクラスターを展開している場合は、すべてのノードにこの証明書をインポートします。NetScaler LB仮想サーバーなどの代替ロードバランサーを使用している場合は、そこに証明書をインポートします。
8. StoreFrontサーバーのIISでHTTPSバインドを作成し、インポートしたSSL証明書をバインドします。



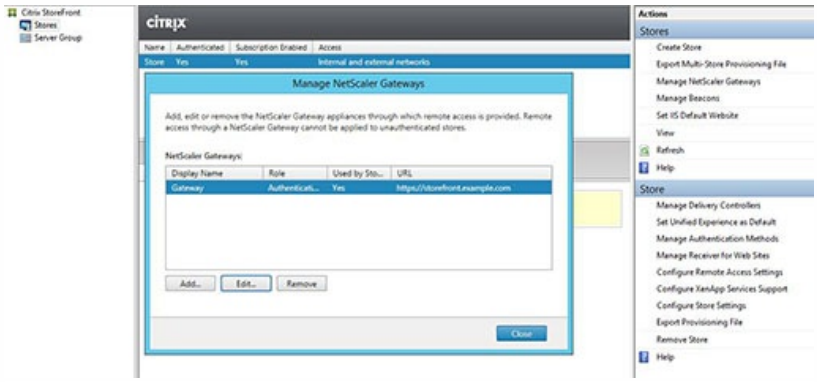
9. StoreFrontサーバーで、選択済みの共有FQDNに一致するように、ホストベースURLを構成します。
   注： StoreFrontでは、証明書内のSAN一覧で最後のSANが常に自動的に選択されます。通常、自動的に選択されたものをそのまま使用できますが、StoreFront管理者は必要に応じて変更することもできます。有効なHTTPS://<FQDN>が証明書内にSANとして存在する場合、ホストベースURLをそのいずれかに手動で設定することができます。（例：https://storefront.example.com）



StoreFrontサーバーでのゲートウェイの構成：storefront.example.com

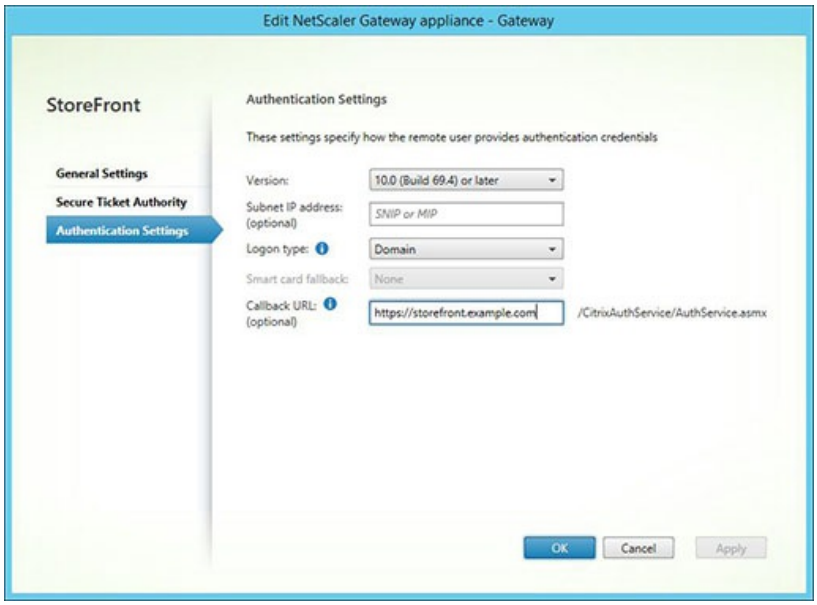
1. [ストア] ノードで、 [NetScaler Gatewayの管理] を [操作] ペインでクリックします。

2. サーバー名を変更するには、一覧から [ゲートウェイ] を選択し、 [編集] をクリックします。



3. [全般設定] ページで共有FQDNを [NetScaler Gateway URL] フィールドに入力します。

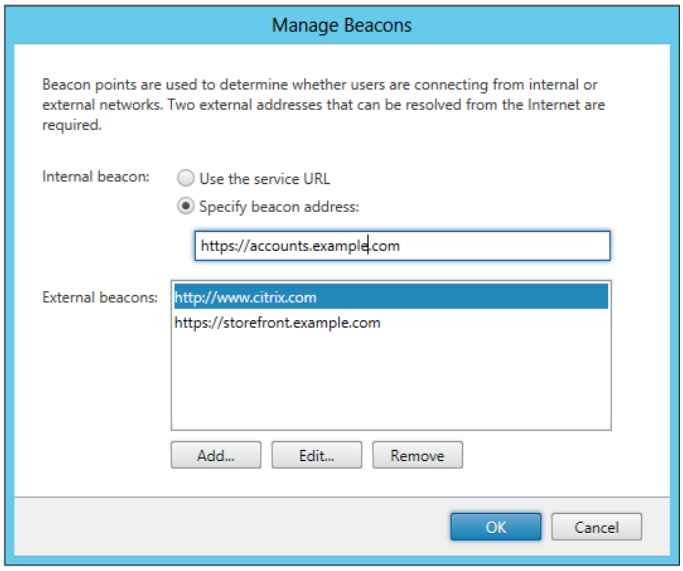
4. [認証設定] タブを選択し、コールバックFQDNを [コールバックURL] フィールドに入力します。



5. [Secure Ticket Authority] タブを選択し、Secure Ticket Authority（STA）サーバーが [ストア] ノード内で既に構成されているDelivery Controllerの一覧と一致するか確認します。

6. このストアのリモートアクセスを有効にします。

7. 内部ビーコンにアカウントエイリアス（accounts.example.com）を手動で設定します。これは、ゲートウェイ外部からの解決が不可能なものである必要があります。このFQDNは、StoreFrontホストベースURLとNetScaler Gateway仮想サーバーで共有される外部ビーコン（storefront.example.com）とは異なるものである必要があります。内部ビーコンと外部ビーコンが同じものになってしまうので、共有FQDNは使用しないでください。



8. FQDNによる検出をサポートするには、次の手順に従います。プロビジョニングファイルの構成が十分である場合、またはReceiver for Webのみを使用する場合は、次の手順を省略できます。

C:\inetpub\wwwroot\Citrix\Authentication\web.configに追加のエントリを追加します。認証用web.configファイルには2つのエントリがあります。Authentication Token Producer用である、ファイル内の最初のエントリのみに、追加のを追加する必要があります。

9. 要素を検索します。以下のようなエントリを見つけ、**太字**で示されている行を追加し、保存して、web.configファイルを閉じます。

.....

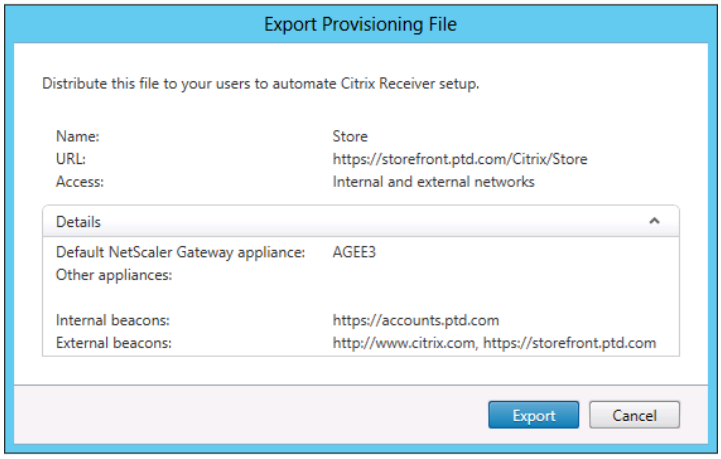
.....

9.**C:\inetpub\wwwroot\Citrix\Roaming\web.config**で、以下のようなエントリを見つけ、**太字**で示されている行を追加し、保存して、web.configファイルを閉じます。

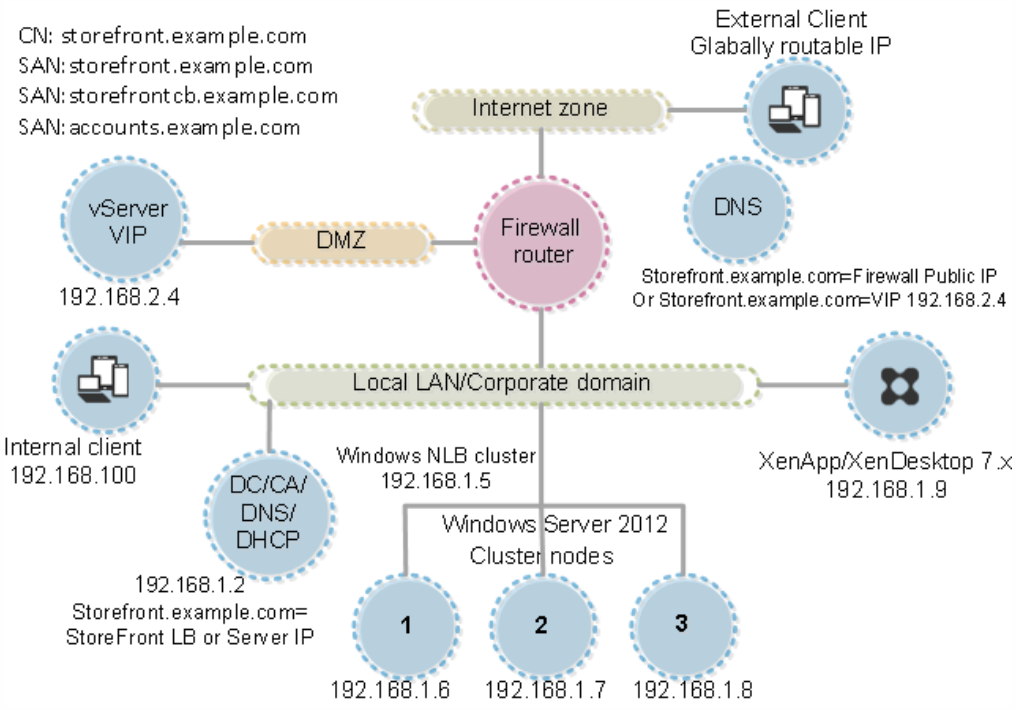
.....

.....

または、ストアのネイティブReceiver CRプロビジョニングファイルをエクスポートすることができます。こうすることで、初回使用時にネイティブReceiverの構成が不要になります。このファイルをすべてのReceiver for WindowsおよびReceiver for Macクライアントに配布します。



Receiverがインストール済みでCRファイルが関連付けられている場合、プロビジョニングファイルをダブルクリックすると自動的にインポートされます。



リソースフィルターの構成

Aug 14, 2017

ここでは、リソースの種類やキーワードを使用して、列挙されるリソースを指定する方法について説明します。管理者は、このフィルター機能と、Store Customization SDKで提供されるより高度なカスタマイズ方法を組み合わせて使用できます。SDKでは、ユーザーに表示されるアプリやデスクトップを制御したり、アクセス条件を変更したり、起動パラメーターを設定したりできます。詳しくは、Store Customization SDKを参照してください。

注：StoreFront管理コンソールとPowerShellコンソールを同時に開くことはできません。StoreFront管理コンソールを閉じてからPowerShellコンソールを開いてください。同様に、PowerShellのすべてのインスタンスを閉じてからStoreFront管理コンソールを開いてください。

フィルターを構成するには、StoresModuleで定義されているPowerShellコマンドレットを使用します。必要なモジュールをロードするには、以下のPowerShellスニペットを使用します。

```
$dsInstallProp = Get-ItemProperty ` -Path HKLM:\SOFTWARE\Citrix\DeliveryServicesManagement -Name InstallDir $dsInstallDir = $dsInstallProp.InstallDir & $dsInstallDir\..\Scripts\ImportModules.ps1
```

リソースを種類でフィルタリングするには、以下のコマンドを使用します。このコマンドにより、列挙するリソースの種類が指定されます。指定した種類以外のリソースは列挙されません。以下のコマンドレットを使用します。

Set-DSResourceFilterType：リソースの種類による列挙フィルターをセットアップします。

Get-DSResourceFilterType：StoreFrontで列挙されるリソースの種類の一覧を取得します。

注：リソースの種類は、キーワードよりも先に適用されます。

これにより、キーワードをベースにリソースをフィルターします。たとえば、XenDesktop、またはXenAppのリソースをフィルターします。キーワードは、各リソースの説明フィールドの文字列から生成されます。

このフィルターでは、列挙対象のリソースまたは列挙から除外するリソースを指定できます。列挙するリソースを指定するフィルターでは、キーワードに一致するリソースのみが列挙され、一致しないリソースは列挙されません。列挙から除外するリソースを指定するフィルターでは、キーワードに一致するリソースが列挙されなくなります。以下のコマンドレットを使用します。

Set-DSResourceFilterKeyword：リソースのキーワードによる列挙フィルターをセットアップします。

Get-DSResourceFilterKeyword：リソースのキーワードの一覧を取得します。

以下のキーワードは予約されており、このフィルターで使用することはできません。

- 自動
- 固定

各キーワードについて詳しくは、「ユーザーエクスペリエンスの最適化」と「アプリケーション配信の構成」を参照してください。

次のコマンドにより、ワークフローリソースが列挙対象から除外されます。

```
Set-DSResourceFilterKeyword -SiteId 1 -VirtualPath "/Citrix/Store" -ExcludeKeywords @("WFS")
```

次のコマンドにより、アプリケーションのみが列挙されます。

```
Set-DSResourceFilterType -SiteId 1 -VirtualPath "/Citrix/Store" -IncludeTypes @("Applications")
```

構成ファイルを使用した構成

Aug 14, 2017

構成ファイルを使用して、Citrix StoreFront管理コンソールでは設定できないCitrix StoreFrontおよびCitrix Receiver for Webの追加設定を構成できます。

構成できるCitrix StoreFront設定には、次のものがあります。

- ICAファイル署名の有効化
- ファイルタイプの関連付けの無効化
- Citrix Receiverのログオンダイアログボックスのカスタマイズ
- Receiver for Windowsでのパスワードおよびユーザー名のキャッシュ機能の無効化

構成できるCitrix Receiver for Web設定には次のものがあります。

- ユーザーに対するリソースの表示方式
- ［マイアプリケーション］フォルダービューの無効化

構成ファイルを使ったStoreFrontの構成

Aug 14, 2017

ここでは、Citrix StoreFront管理コンソールを使用して実行できない付加的な構成タスクについて説明します。

ICAファイル署名の有効化

ファイルタイプの関連付けの無効化

Citrix Receiverのログオンダイアログボックスのカスタマイズ

Citrix Receiver for Windowsでのパスワードおよびユーザー名のキャッシュ機能の無効化

StoreFrontには、ICAファイルにデジタル署名を追加するオプションが用意されています。これにより、この機能をサポートするバージョンのCitrix Receiverで、ICAファイルが信頼されるサーバーからのものであることを検証できるようになります。StoreFrontでファイルの署名を有効にすると、ユーザーがアプリケーションを起動するときに生成されるICAファイルが、StoreFrontサーバーの個人証明書ストアにある証明書を使用して署名されます。StoreFrontサーバーのオペレーティングシステムでサポートされる任意のハッシュアルゴリズムを使ってICAファイルを署名できます。クライアントソフトウェアがこの機能をサポートしない場合やICAファイルの署名用に構成されていない場合、デジタル署名は無視されます。署名処理に失敗した場合は、デジタル署名なしでICAファイルが生成され、Citrix Receiverに送信されます。未署名のファイルを受け入れるかどうかは、Receiver側での構成により決定されます。

StoreFrontのICAファイルの署名機能で使用する証明書には秘密キーが含まれ、許可された有効期間内である必要があります。証明書にキー使用法エクステンションが含まれる場合は、デジタル署名での使用が許可されている必要があります。拡張キー使用法エクステンションが含まれる場合は、コード署名またはサーバー認証ように設定されている必要があります。

ICAファイルを署名する場合、商用の証明機関または組織内の独自の証明機関から取得したコード署名またはSSL署名証明書を使用することをお勧めします。証明機関から適切な証明書を取得できない場合は、サーバー証明書のような既存のSSL証明書を使用するか、新しいルート証明機関証明書を作成してユーザーデバイスに配布することができます。

ストアのICAファイルの署名機能はデフォルトでは無効になっています。ICAファイルの署名機能を有効にするには、ストアの構成ファイルを編集してからWindows PowerShellコマンドを実行します。Citrix Receiver側でICAファイルの署名機能を有効にする方法について詳しくは、「ICAファイルに署名して信頼されていないサーバー上のアプリケーションやデスクトップが起動しないようにする」を参照してください。

注：StoreFront管理コンソールとPowerShellコンソールを同時に開くことはできません。StoreFront管理コンソールを閉じてからPowerShellコンソールを開いてください。同様に、PowerShellのすべてのインスタンスを閉じてからStoreFront管理コンソールを開いてください。
重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. ICAファイルの署名に使用する証明書が、現在のユーザーの証明書ストアではなく、StoreFrontサーバー上のCitrixデリバリーサービスの証明書ストアで使用可能になっていることを確認します。
2. テキストエディターを使ってストアのweb.configファイルを開きます。このファイルは通常、C:\inetpub\wwwroot\Citrix\storename\ディレクトリにあります。このstorenameはストアの作成時に指定した名前です。
3. ファイル内で次のセクションを検索します。
   ...
4. 次に示すように、署名に使用する証明書の詳細を追加します。
   certificateid" thumb="certificatethumbprint" /> ...
   ここで、certificateidはストアの構成ファイル内で証明書を識別するための値で、certificatethumbprintはハッシュアルゴリズムにより生成される証明書データのダイジェスト（または拇印）です。
5. ファイル内で次の要素を検索します。
6. ストアのICAファイルの署名を有効にするには、enabled属性の値をTrueに変更します。さらに、certificateId属性の値を、証明書を識別するために使用したID、つまり手順4.のcertificateidに設定します。
7. SHA-1以外のハッシュアルゴリズムを使用する場合は、必要に応じてhashAgorithm属性の値をsha256、sha384、またはsha512に設定します。
8. ローカルの管理者アカウントを使ってWindows PowerShellを起動して、コマンドプロンプトで次のコマンドを実行します。これにより、ストアが秘密キーにアクセスできるようになります。
   Add-PSSnapin Citrix.DeliveryServices.Framework.Commands $certificate = Get-DSCertificate "certificatethumbprint" Add-DSCertificateKeyReadAccess -certificate $certificates[0] -accountName “IIS
   ここでcertificatethumbprintは、ハッシュアルゴリズムにより 生成される証明書データのダイジェストです。

ストアのファイルタイプの関連付けは、デフォルトで有効になっています。このため、ユーザーがユーザーデバイス上で開いたローカルファイルは、サブスクライブ済みのアプリケーションで表示されます。ファイルタイプの関連付けを無効にするには、ストアの構成ファイルを編集します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. テキストエディターを使ってストアのweb.configファイルを開きます。このファイルは通常、C:\inetpub\wwwroot\Citrix\storename\ディレクトリにあります。このstorenameはストアの作成時に指定した名前です。
2. ファイル内で次の要素を検索します。
3. ストアのファイルタイプの関連付けを無効にするには、enableFileTypeAssociation属性の値をoffに変更します。

Citrix Receiverユーザーがストアにログオンするときのダイアログボックスには、デフォルトでタイトルが表示されません。このダイアログボックスをカスタマイズして、タイトルに「ログオンしてください」などのメッセージを表示することができます。Citrix Receiverのログオンダイアログボックスにタイトル文字列を表示するには、認証サービス用のファイルを編集します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. テキストエディターを使って認証サービス用のUsernamePassword.tfrmファイルを開きます。このファイルは通常、C:\inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\フォルダーにあります。
2. ファイル内で次の行を検索します。
   @* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
3. この行のコメントを解除します。これを行うには、次のように最初の「@*」と最後の「*@」を削除します。
   @Heading("ExplicitAuth:AuthenticateHeadingText")
   これにより、Citrix Receiverユーザーがこのストアにログオンしたときに、デフォルトのタイトル文字列である「Please log on」または「ログオンしてください」などが表示されます。

4. タイトル文字列を変更するには、テキストエディターを使って認証サービス用のExplicitAuth.resxファイルを開きます。このファイルは通常、C:\inetpub\wwwroot\Citrix\Authentication\App_Data\resources\フォルダーにあります。
5. ファイル内で次の要素を検索します。要素内の文字列を編集します。これにより、このストアのログオンダイアロボックスのタイトルが変更されます。
   My Company Name
   ほかのロケールにいるユーザー用にCitrix Receiverのログオンダイアログボックスのタイトルの文字列を変更するには、対象となる言語版のExplicitAuth.resxファイルを編集します。languagecode
   ここで、languagecodeは「ja」などのロケールIDです。

Citrix Receiver for Windowsのデフォルトでは、ユーザーがStoreFrontストアにログオンしたときのパスワードがキャッシュされます。Citrix Receiver for Windowsでパスワードのキャッシュ機能を無効にするには、認証サービスのファイルを編集します（この設定はCitrix Receiver for Windows Enterpriseには適用されません）。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. テキストエディターを使用して、inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\UsernamePassword.tfrmファイルを開きます。
2. ファイル内で次の行を検索します。
   @SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey: "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked: ControlValue("SaveCredentials"))
3. この行を次のようにコメント化します。
   これにより、この認証サービスのストアにCitrix Receiver for Windowsを使用してログオンするユーザーは、毎回パスワードの入力が必要になります。この設定は、Citrix Receiver for Windows Enterpriseには適用されません。

> **警告**
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsのインストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

デフォルトで、Citrix Receiver for Windowsでは姓が自動的に抽出されて入力されます。ユーザー名フィールドへの自動抽出を無効にするには、ユーザーデバイスでレジストリを編集します。

1. REG_SZ値の HKLM\SOFTWARE\Citrix\AuthManager\RememberUsernameを作成します。
2. 値を「false」に設定します。

構成ファイルを使ったCitrix Receiver for Webサイトの構成

Aug 14, 2017

ここでは、Citrix StoreFront管理コンソールを使用して実行できない、Citrix Receiver for Webサイトの付加的な構成タスクについて説明します。

Citrix Receiver for Webサイトからデスクトップとアプリケーションの両方にアクセスできる場合、デフォルトでデスクトップとアプリケーションが別々のビューで表示されます。サイトにログオンすると、最初にデスクトップビューが表示されます。ユーザーがアクセスできるデスクトップが1つのみの場合、アクセス可能なアプリケーションがあるかどうかにかかわらず、ユーザーのログオン時にそのデスクトップが自動的に起動します。これらの設定を変更するには、サイトの構成ファイルを編集します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. テキストエディターを使ってCitrix Receiver for Webサイトのweb.configファイルを開きます。このファイルは通常、C:\inetpub\wwwroot\Citrix\storenameWeb\フォルダーにあります。ここで、storenamestorenameはストアの作成時に指定した名前です。
2. ファイル内で次の要素を検索します。

3. ユーザーがアクセス可能なデスクトップやアプリケーションを非表示にするには、showDesktopsView属性（デスクトップ）およびshowAppsView属性（アプリケーション）の値をfalseに変更します。デスクトップビューとアプリケーションビューの両方が有効な場合は、defaultView属性の値をappsに設定すると、ユーザーがサイトにログオンしたときに最初にアプリケーションビューが表示されます。
4. ファイル内で次の要素を検索します。

5. デスクトップの自動起動を無効にするには、autoLaunchDesktop属性の値をfalseに変更します。これにより、ユーザーがアクセスできるデスクトップが1つのみの場合でも、ログオン時にデスクトップが自動的に起動しなくなります。autoLaunchDesktop属性がtrueの場合、使用可能なデスクトップが1つのみのユーザーがログオンしてもアプリケーションには再接続されません（ワークスペースコントロールが有効になっていても再接続されません）。

注：Citrix Receiver for Webサイトによるデスクトップの自動起動を有効にするには、Internet Explorerでサイトにアクセスするユーザーは［ローカルイントラネット］または［信頼済みサイト］のゾーンにサイトを追加する必要があります。

Citrix Receiver for Webのデフォルトでは、認証不要なストア（匿名ユーザー用）と必須ストア（ユーザーがサブスクライブしなくてもすべての公開アプリケーションがホーム画面に追加される）の［マイアプリケーション］フォルダービューが表示されます。このビューにはアプリケーションがフォルダー階層で表示され、フォルダーパスの情報も表示されます。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. テキストエディターを使ってCitrix Receiver for Webサイトのweb.configファイルを開きます。このファイルは通常、C:\inetpub\wwwroot\Citrix\storenameWeb\フォルダーにあります。ここで、storenameはストアの作成時に指定した名

前です。
2. ファイル内で次の要素を検索します。
3. enableAppsFolderView属性の値をfalseに変更します。これにより、Citrix Receiver for Webの［マイアプリケーション］フォルダービューが無効になります。

StoreFront展開環境のセキュリティ

Aug 14, 2017

このトピックでは、StoreFrontの展開および構成時に使用すべき、システムのセキュリティを保護するための機能について説明します。

制限されたIIS構成でStoreFrontを構成できます。これはデフォルトのIIS構成ではありません。

一覧にない**ファイル拡張子**
を禁止することができます。

StoreFrontでは、要求のフィルタリングに、次のファイル拡張子が必要です。

- （空白の拡張子）
- .appcache
- .aspx
- .cr
- .css
- .dtd
- gif
- .htm
- .html
- ICA
- .ico
- .jpg
- .js
- png
- .svg
- .txt
- .xml

Citrix Receiver for WebでCitrix Receiverのダウンロード/アップグレードが有効になっている場合、次のファイル拡張子も必要です。

- .dmg
- .exe

Citrix Receiver for HTML5が有効になっている場合、次のファイル拡張子も必要です。

- .eot
- .ttf
- .woff

StoreFrontは要求のフィルタリングに、次のHTTP動詞が必要です。次の一覧にない動詞を禁止できます。

- GET
- POST
- HEAD

StoreFrontは次を必要としません。

- ISAPIフィルター
- ISAPI拡張
- CGIプログラム
- FastCGIプログラム

> **Important**
>
> - StoreFrontには完全な信頼が必要です。グローバル.NET信頼レベルを［High］またはそれ以下に設定しないでください。
> - StoreFrontでは、サイトごとに別個のアプリケーションプールはサポートされません。このサイト設定は変更しないでください。

StoreFrontがインストールされると、そのアプリケーションプールには**[サービスとしてログオン]** のログオン権限と **[プロセスのメモリ クォータの増加]** 、 **[セキュリティ監査の生成]** 、 **[プロセス レベル トークンの置き換え]** の権限が付与されます。これはアプリケーションプールが作成された時の通常のビヘイビアーです。

通常、これらのユーザー権利を変更する必要はありません。これらの権限はStoreFrontでは使用されず自動的に無効になります。

StoreFrontをインストールすると、次のWindowsサービスが作成されます。

- Citrix Configuration Replication（NT SERVICE\CitrixConfigurationReplication）
- Citrix Cluster Join（NT SERVICE\CitrixClusterService）
- Citrix Peer Resolution（NT SERVICE\Citrix Peer Resolution Service）
- Citrix Credential Wallet（NT SERVICE\CitrixCredentialWallet）
- Citrix Subscriptions Store（NT SERVICE\CitrixSubscriptionsStore）
- Citrix Default Domain Services（NT SERVICE\CitrixDefaultDomainService）

XenApp 6.5にStoreFront Kerberos制約付き委任を構成すると、Citrix StoreFront Protocol Transitionサービス（NT SERVICE\SYSTEM）が作成されます。このサービスには、Windowsサービスに通常付与されない権限が必要です。

上記の「ユーザー権利の構成」セクションの一覧にあるStoreFront Windowsサービスは、NETWORK SERVICE IDでログオンするように構成されます。Citrix StoreFront Protocol Transitionサービスは、SYSTEMとしてログオンします。この構成は変更しないでください。

StoreFrontのインストールにより、次のサービスが管理者セキュリティグループに追加されます。

- Citrix Configuration Replication（NT SERVICE\CitrixConfigurationReplication）
- Citrix Cluster Join（NT SERVICE\CitrixClusterService）

StoreFrontが正しく動作して次の操作を行うには、これらのグループメンバーシップが必要です。

- 証明書の作成、エクスポート、インポート、削除、および証明書へのアクセス権限の設定
- Windowsレジストリの読み取りおよび書き込み

- Global Assembly Cache（GAC）でのMicrosoft .NET Frameworkアセンブリの追加および削除
- フォルダーProgram Files\Citrix\<*StoreFrontLocation*>へのアクセス
- IISアプリプールIDおよびIIS Webアプリケーションの追加、変更、削除
- ローカルセキュリティグループおよびファイアウォールルールの追加、変更、削除
- WindowsサービスとPowerShellスナップインの追加および削除
- Microsoft Windows Communication Framework（WCF）エンドポイントの登録

上記操作の一覧は、StoreFrontの更新プログラムで告知なく変更されることがあります。

StoreFrontをインストールすると、以下のセキュリティグループも作成されます。

- CitrixClusterMembers
- CitrixCWServiceReadUsers
- CitrixCWServiceWriteUsers
- CitrixDelegatedAuthenticatorUsers
- CitrixDelegatedDirectoryClaimFactoryUsers
- CitrixPNRSUsers
- CitrixStoreFrontPTServiceUsers
- CitrixSubscriptionServerUsers
- CitrixSubscriptionsStoreServiceUsers
- CitrixSubscriptionsSyncUsers内のメンバーシップ

StoreFrontは、これらのセキュリティグループのメンバーシップを保持します。メンバーシップはStoreFront内でのアクセス制御のために使用され、ファイルやフォルダーなどのWindowsリソースには適用されません。このグループメンバーシップは変更しないでください。

サーバー証明書

StoreFrontでは、コンピューターの識別とTransport Layer Security（TLS）通信の保護のためにサーバー証明書を使用します。ICAファイルの署名機能を有効にする場合は、StoreFrontで証明書を使用してICAファイルをデジタル署名することもできます。

Citrix Receiverを初めてデバイスにインストールするユーザーに対してメールアドレスによるアカウント検出を有効にするには、StoreFrontサーバー上に有効なサーバー証明書をインストールする必要があります。ルート証明書へのチェーンのすべてが有効である必要もあります。ユーザーエクスペリエンスを向上させるには、SubjectまたはdiscoverReceiverのSubject Alternative Nameエントリの証明書をインストールする必要があります。domain。ここでdomainはユーザーのメールアカウントを含むMicrosoft Active Directoryドメインです。このドメインのワイルドカード証明書を使用することもできますが、そのような証明書の使用が社内のセキュリティポリシーで許可されていることを確認してください。ユーザーのメールアカウントを含んでいるドメイン用のほかの証明書を使用することもできますが、ユーザーがCitrix ReceiverでStoreFrontサーバーに最初に接続したときに、証明書に関する警告が表示されます。上記以外の証明書を使用してメールアドレスによるアカウント検出機能を使用することはできません。詳しくは、「メールアドレスによるアカウント検出を構成する」を参照してください。

ユーザーがアカウントを構成するときに、Citrix ReceiverにストアのURLを入力する場合（つまりメールアドレスによるアカウント検出機能を使用しない場合）は、StoreFrontサーバー上の証明書がそのサーバーに対してのみ有効で、ルート証明書へのチェーンが有効である必要があります。

トークン管理の証明書

認証サービスとストアのそれぞれに、トークン管理のための証明書が必要です。認証サービスまたはストアを作成すると、StoreFrontにより自己署名証明書が生成されます。StoreFrontにより生成される自己署名証明書をほかの用途で使用しないてください。

Citrix Delivery Servicesの証明書

StoreFrontは、カスタムのWindows証明書ストア（Citrix Delivery Services）に、いくつかの証明書を保持しています。Citrix Configuration Replicationサービス、Citrix Credential Walletサービス、およびCitrix Subscriptions Storeサービスは、これらの証明書を使用します。クラスター内の各StoreFrontサーバーは、これらの証明書のコピーを持っています。これらのサービスはセキュアな通信にTLSを使用せず、これらの証明書はTLSサーバー証明書として使用されません。これらの証明書は、StoreFrontストアの作成時またはStoreFrontのインストール時に作成されます。このWindows証明書ストアのコンテンツは変更しないでください。

コード署名証明書

StoreFrontでは、\Scriptsのフォルダー内にいくつかのPowerShellスクリプト（.ps1）が含まれています。デフォルトのStoreFrontインストールでは、これらのスクリプトは使用されません。これらのスクリプトにより、特殊で低頻度のタスクの構成手順が簡素化されます。スクリプトは署名されているため、StoreFrontでPowerShell実行ポリシーをサポートできるようになります。**AllSigned**ポリシーをお勧めします。（PowerShellスクリプトの実行が妨げられるため、**Restricted**ポリシーはサポートされません）。StoreFrontでは、PowerShell実行ポリシーは変更されません。

StoreFrontでは信頼できる発行元ストアにコード署名証明書はインストールされませんが、Windowsでコード署名証明書を自動的に追加することができます。これは、PowerShellスクリプトが**Always run**オプションで実行されることで可能になります。（**Never run**オプションを選択すると、信頼されていない証明書ストアに証明書が追加され、StoreFront PowerShellスクリプトは実行されません）。コード署名証明書が信頼された発行元ストアに追加されると、Windowsは有効期限を確認しなくなります。StoreFrontタスクが完了したら、信頼できる発行元ストアからこの証明書を削除できます。

実稼働環境では、StoreFrontとサーバーの間で通信されるデータを保護するために、インターネットプロトコルセキュリティ（IPsec）またはHTTPSプロトコルを使用することをお勧めします。IPsecは、インターネットプロトコルの標準機能拡張のセットです。インターネットプロトコルは、データ整合性と再生の保護により通信の認証と暗号化の機能を提供します。IPsecはネットワーク層のプロトコルセットであるため、上位レベルのプロトコルでそのままIPSecを使用できます。HTTPSは、SSL（Secure Sockets Layer）およびTLS（Transport Layer Security）プロトコルを使用して強力なデータ暗号化機能を提供します。

StoreFrontサーバーとXenAppサーバー間のデータトラフィックを保護するには、SSL Relayを使用します。SSL Relayはホスト認証とデータ暗号化を実行する、XenAppのデフォルトのコンポーネントです。

StoreFrontとユーザーデバイスの間の通信は、NetScaler GatewayおよびHTTPSで保護することをお勧めします。StoreFrontでHTTPSを使用するには、認証サービスおよび関連付けられたストアを提供するMicrosoftインターネットインフォメーションサービス（IIS）インスタンスでHTTPSを構成する必要があります。IISでHTTPSが構成されていない場合、StoreFrontの通信にHTTPが使用されます。実稼働環境では、StoreFrontへのすべてのユーザー接続が保護されるようにしてください。

StoreFrontと同じWebドメイン（ドメイン名とポート）にWebアプリケーションを展開すると、これらのWebアプリケーションの脆弱性によりStoreFront展開環境全体のセキュリティが低下する可能性があります。セキュリティ境界を分離してセキュリティを強化するため、Webアプリケーションと異なるWebドメインにStoreFrontを展開することをお勧めします。

StoreFrontには、サーバー上の特定の証明書を使用してICAファイルをデジタル署名するオプションがあり、この機能をサポートするバージョンのCitrix Receiverでは、ファイルの発行元を信頼できるかどうかを検証できます。SHA-1やSHA-256など、StoreFrontサーバーのオペレーティングシステムでサポートされるどのハッシュアルゴリズムでも、ICAファイルを署名できます。詳しくは、「ICAファイル署名の有効化」を参照してください。

Active Directoryドメインの資格情報でReceiver for Webサイトにログオンするユーザーが必要に応じてパスワードを変更できるように設定することができます。ただし、その認証サービスを使用するストアにアクセスできるすべてのユーザーに、慎重に扱うべきセキュリティ機能が公開されることになります。組織のセキュリティポリシーにより、ユーザーパスワード変更機能が内部使用のみに制限される環境では、社内ネットワークの外側からそれらのストアにアクセスできないことを確認してください。認証サービスを作成したときのデフォルトの構成では、パスワードが失効しても、ユーザーはパスワードを変更できません。詳しくは、「ユーザーエクスペリエンスの最適化」を参照してください。

セキュリティ強化のため、自分が管理していないサーバーからコンテンツまたはスクリプトをロードするカスタマイズは行わないでください。コンテンツまたはスクリプトは、カスタマイズを行うCitrix Receiver for Webサイトのカスタムフォルダーにコピーしてください。StoreFrontがHTTPS接続用に構成されている場合、カスタムコンテンツやカスタムスクリプトへのリンクもすべてHTTPSを使用していることを確認してください。

StoreFront構成のエクスポートとインポート

Aug 14, 2017

StoreFront展開環境の構成全体をエクスポートできます。これには、単一サーバー環境とサーバーグループ構成の両方が含まれます。既存の展開環境がインポートサーバーに既に存在している場合、現在の構成が消去されてから、バックアップアーカイブ内に含まれている構成で置き換えられます。ターゲットサーバーがクリーンな工場出荷時のデフォルトインストールの場合、バックアップ内に保存されているインポートされた構成を使用して新しい環境が作成されます。エクスポートされた構成のバックアップは、単一の.zipアーカイブ形式（暗号化されていない場合）または.ctxzip形式（作成時にバックアップファイルの暗号化を選択した場合）です。

StoreFront構成のエクスポートおよびインポート時の検討事項

StoreFrontバックアップの暗号化と暗号化解除に使用されるPowerShell資格情報オブジェクト

PowerShellコマンドレット

構成のエクスポートおよびインポート例

- バックアップアーカイブに含まれているホストベースURLを使用しますか。またはインポートサーバーで使用する新しいホストベースURLを指定しますか。
- 現在Citrixが公開している認証SDKの例（Magic Word Authenticationなど）またはサードパーティの認証カスタマイズを使用していますか。使用している場合は、これらのパッケージをすべてのインポートサーバーにインストールしてから、追加の認証方式を含む構成をインポートする必要があります。必要な認証SDKパッケージがどのインポートサーバーにもインストールされていない場合、構成のインポートは失敗します。構成をサーバーグループにインポートする場合は、グループのすべてのメンバーに認証パッケージをインストールします。
- 構成のバックアップを暗号化または暗号化解除できます。エクスポートおよびインポートPowerShellコマンドレットはどちらのユースケースもサポートします。
- 暗号化されたバックアップ（.ctxzip）は後から暗号化解除できますが、StoreFrontは暗号化されていないバックアップファイル（.zip）を再暗号化できません。暗号化されたバックアップが必要な場合は、選択したパスワードを含むPowerShell資格情報オブジェクトを使用してもう一度エクスポートを実行します。
- StoreFrontが現在インストールされているIIS（エクスポート元サーバー）におけるWebサイトのSiteIDは、バックアップされたStoreFront構成をリストアするIIS（インポート先サーバー）におけるターゲットWebサイトのSiteIDに一致する必要があります。

PowerShell資格情報オブジェクトには、Windowsアカウントのユーザー名とパスワードの両方が結合されています。PowerShell資格情報オブジェクトにより、パスワードがメモリ内で保護されます。

> ## 注意
>
> 構成バックアップのアーカイブを暗号化するには、暗号化と暗号化解除を実行するためのパスワードのみ必要です。資格情報オブジェクト内に保存されているユーザー名は使用されません。エクスポートサーバーおよびインポートサーバーの両方で使用される、PowerShellセッション内の同じパスワードを含む資格情報オブジェクトを作成する必要があります。資格情報オブジェクト内では、どのユーザーでも指定できます。

PowerShellでは、新しい資格情報オブジェクトを作成するときにユーザーを指定する必要があります。便宜上、このコード例では現在ログオンしているWindowsユーザーのみ取得します。

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential($User,$Password)
```

Export-STFConfiguration

パラメーター	説明
-TargetFolder（String）	バックアップアーカイブへのエクスポートパス。 例："$env:userprofile\desktop\"
-Credential（PSCredentialオブジェクト）	エクスポート中に暗号化された.ctxzipバックアップアーカイブを作成する資格情報オブジェクトを指定します。 PowerShell資格情報オブジェクトには、暗号化と暗号化解除に使用されるパスワードが含まれます。**-Credential**を**-NoEncryption**パラメーターと一緒に使用しないでください。 例：$CredObject
-NoEncryption（スイッチ）	バックアップアーカイブを暗号化されていない.zipにすることを指定します。 **-NoEncryption**を**-Credential**パラメーターと一緒に使用しないでください。
-ZipFileName（String）	StoreFront構成のバックアップアーカイブの名前。.zipや.ctxzipなどのファイル拡張子を追加しないでください。ファイル拡張子は、エクスポート中に**-Credential**または**-NoEncryption**のどちらのパラメーターを指定したかによって自動的に追加されます。 例："backup"
-Force（ブール型）	このパラメーターは、バックアップアーカイブを、指定されたエクスポート先にある既存のバックアップファイルと同じファイル名で自動的に上書きします。

Important

StoreFront 3.5にあった**-SiteID**パラメーターは、バージョン3.6で廃止されました。バックアップアーカイブに含まれる**SiteID**が常に使用されるようになったため、インポートを実行するときにSiteIDを指定する必要はなくなりました。SiteIDが、インポート先サーバーのIIS内ですでに構成されている既存のStoreFront Webサイトに一致することを確認します。**SiteID 1**から**SiteID 2**への（またはその逆）構成のインポートはサポートされません。

Import-STFConfiguration

パラメーター	説明
-ConfigurationZip（String）	インポートするバックアップアーカイブへのフルパス。ファイル拡張子も含めます。暗号化されていない場合は.zip、暗号化されたバックアップアーカイブの場合は.ctxzipを使用します。 例："$env:userprofile\desktop\backup.ctxzip"
-Credential（PSCredentialオブジェクト）	インポート中に暗号化されたバックアップを暗号化解除する資格情報オブジェクトを指定します。 例：$CredObject
-HostBaseURL（String）	このパラメーターが含まれると、指定したホストベースURLがエクスポートサーバーのホストベースURLの代わりに使用されます。 例："https://.example.com"

Unprotect-STFConfigurationBackup

パラメーター	説明
-TargetFolder（String）	バックアップアーカイブへのエクスポートパス。 例："$env:userprofile\desktop\"
-Credential（PSCredentialオブジェクト）	このパラメーターを使用して暗号化されたバックアップアーカイブの暗号化されていないコピーを作成します。暗号化解除に使用するパスワードを含むPowerShell資格情報オブジェクトを指定します。 例：$CredObject
-EncryptedConfigurationZip（String）	暗号化解除する暗号化されたバックアップアーカイブのフルパス。ファイル拡張子.ctxzipを指定する必要があります。 例："$env:userprofile\desktop\backup.ctxzip"
-OutputFolder（String）	暗号化された（.ctxzip）バックアップアーカイブから暗号化されていないコピー（.zip）を作成するパス。元の暗号化されたバックアップのコピーは保持され、再使用できます。暗号化されていないコピーのファイル名とファイル拡張子は指定しないでください。

	例："$env:userprofile\desktop\"
-Force（ブール型）	このパラメーターは、バックアップアーカイブを、指定されたエクスポート先にある既存のバックアップファイルと同じファイル名で自動的に上書きします。

現在のPowerShellセッションへのStoreFront SDKのインポート

StoreFrontサーバーでPowerShell Integrated Scripting Environment（ISE）を開き、以下を実行します。

```
$SDKModules = 'C:\Program Files\Citrix\Receiver StoreFront\PowerShellSDK\Modules\Citrix.StoreFront'
Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose
Import-Module "$SDKModules.Authentication\Citrix.StoreFront.Authentication.psd1" -verbose
Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1" -verbose
Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -verbose
Import-Module "$SDKModules.WebReceiver\Citrix.StoreFront.WebReceiver.psd1" -verbose
Import-Module "$SDKModules.SubscriptionsStore\Citrix.StoreFront.SubscriptionsStore.psd1" -verbose
```

単一サーバーのシナリオ

サーバーAで既存の構成の暗号化されていないバックアップを作成し、それを同じ環境に復元する。

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -zipFileName "backup" -NoEncryption
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.zip"
```

サーバーAで既存の構成の暗号化されたバックアップを作成し、それを同じ環境に復元する。

```
#PowerShell資格情報オブジェクトの作成
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential($User,$Password)
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -zipFileName "backup" -Credential $CredObject
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject
```

既存の暗号化されたバックアップアーカイブの保護を解除する。

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential($User,$Password)
Unprotect-STFConfigurationExport -encryptedConfigurationZip "$env:userprofile\desktop\backup.ctxzip" -credential
$CredObject -outputFolder "c:\StoreFrontBackups" -Force
```

サーバーAで既存の構成をバックアップし、サーバーBの新しい工場出荷時のデフォルト環境に復元する。

サーバーBは新しい環境ですが、サーバーAと共存することを目的にしています。サーバーBは新しい工場出荷時のデフォルトのStoreFront環境でもあります。

1. PowerShell資格情報オブジェクトを作成し、サーバーA構成の暗号化されたコピーをエクスポートします。
2. バックアップの暗号化に使用した同じパスワードを使用してサーバーBでPowerShell資格情報オブジェクトを作成します。
3. **-HostBaseURL**パラメーターを使用してサーバーAの構成を暗号化解除し、サーバーBにインポートします。

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" –Credential $CredObject -
HostBaseURL "https://serverB.example.com"
```

サーバーAで既存の構成をバックアップし、それを使用してサーバーBの既存の環境を上書きする。

サーバーBは、古い構成を使用する既存の環境です。 サーバーAの構成を使用してサーバーBを更新します。サーバーBはサーバーAと共存させるためのものです。**-HostBaseURL**パラメーターを指定します。

1. PowerShell資格情報オブジェクトを作成し、サーバーA構成の暗号化されたコピーをエクスポートします。
2. バックアップの暗号化に使用した同じパスワードを使用してサーバーBでPowerShell資格情報オブジェクトを作成します。
3. **-HostBaseURL**パラメーターを使用してサーバーAの構成を暗号化解除し、サーバーBにインポートします。

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" –Credential $CredObject -
HostBaseURL "https://serverB.example.com"
```

新しいサーバーOSにアップグレードしたり、古いStoreFront環境の使用を停止する場合などと同じホストベースURLを使用して既存の環境のクローンを作成する。

2012R2サーバーBは、古い2008R2サーバーAの代わりとなる新しい環境です。インポート中に**HostBaseURL**パラメーターを使用しないでください。サーバーBは新しい工場出荷時のデフォルトのStoreFront環境でもあります。

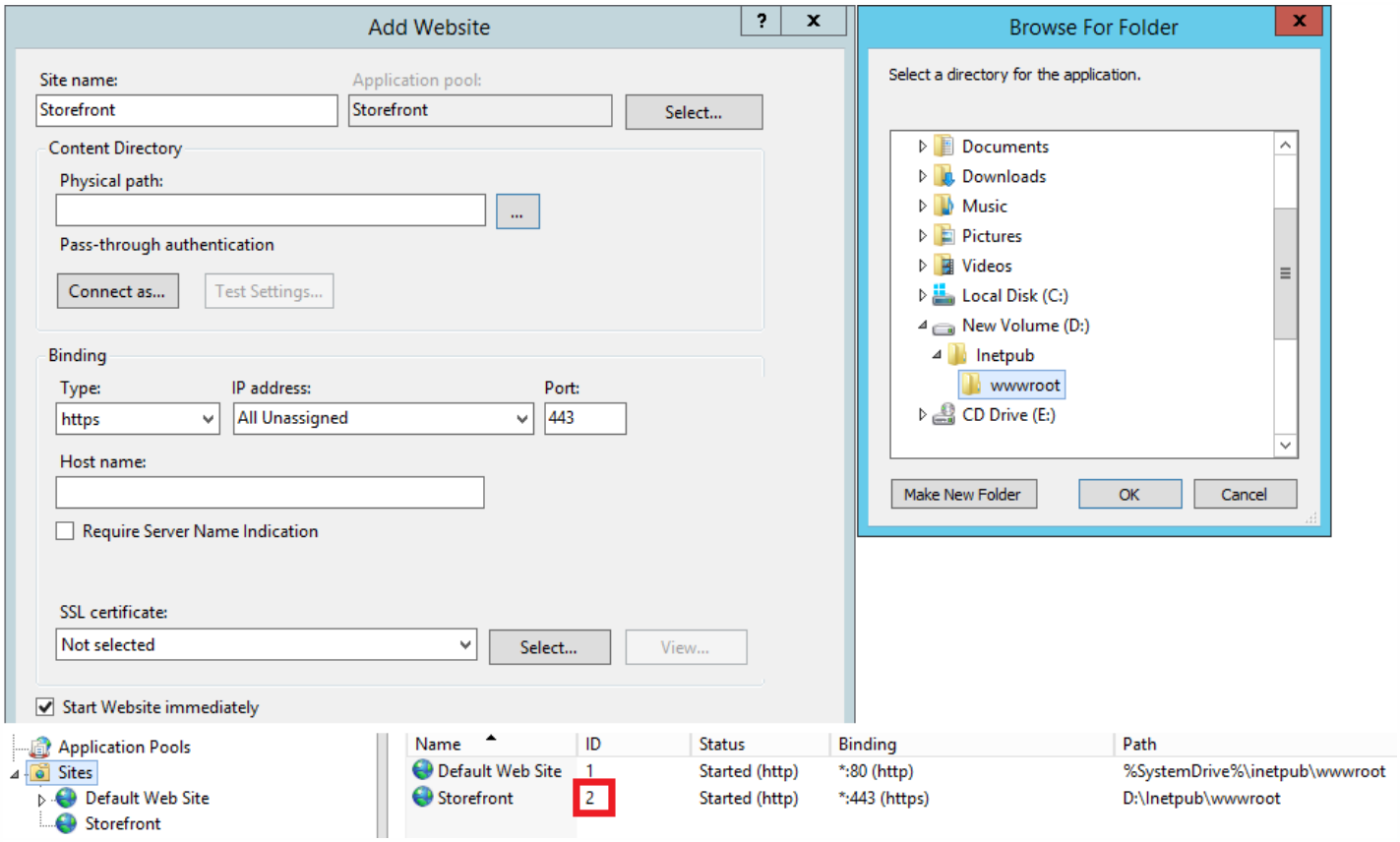
1. PowerShell資格情報オブジェクトを作成し、2008R2サーバーA構成の暗号化されたコピーをエクスポートします。
2. バックアップの暗号化に使用した同じパスワードを使用して2012R2サーバーBでPowerShell資格情報オブジェクトを作成します。
3. **-HostBaseURL**パラメーターを使用せずに、2008R2サーバーA構成を暗号化解除して2012R2サーバーBにインポートします。

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" –Credential $CredObject -
HostBaseURL "https://serverB.example.com"
```

StoreFrontはIISのカスタムのWebサイトに既に展開されている。この構成を別のカスタムWebサイト環境に復元する。

サーバーAではStoreFrontをIIS内の通常のデフォルトのWebサイトではなくカスタムのWebサイトの場所に展開しています。IIS内に作成された2つ目のWebサイトのIIS SiteIDは2です。StoreFront Webサイトの物理パスは、d:\など別のシステム以外のドライブまたはデフォルトのc:\システムドライブに置くことができますが、1を超えるIIS SiteIDを使用する必要があります。

StoreFrontと呼ばれる新しいWebサイトがIIS内に構成され、**SiteID = 2**が使用されています。StoreFrontは、ドライブd:\inetpub\wwwrooot\の物理パスでIIS内のカスタムWebサイトに既に展開されています。



1. PowerShell資格情報オブジェクトを作成し、サーバーA構成の暗号化されたコピーをエクスポートします。
2. サーバーBでは、**StoreFront**と呼ばれる新しいWebサイトでIISを構成します。このサイトで**SiteID 2**を使用します。
3. バックアップの暗号化に使用した同じパスワードを使用してサーバーBでPowerShell資格情報オブジェクトを作成します。
4. **-HostBaseURL**パラメーターを使用してサーバーAの構成を暗号化解除し、サーバーBにインポートします。バックアップに含まれるサイトIDを使用し、このIDがStoreFront構成をインポートするターゲットWebサイトに一致する必要があります。

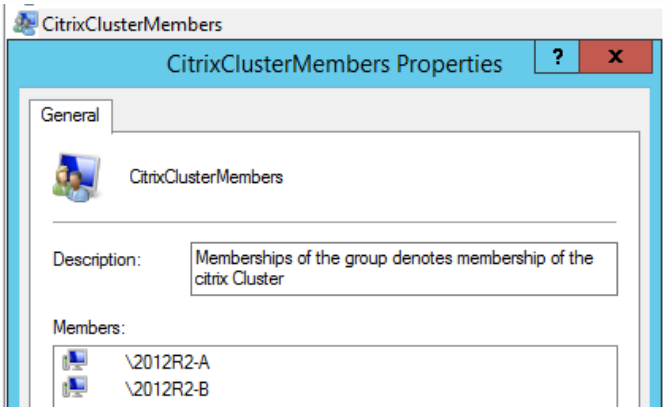
```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" –Credential $CredObject -HostBaseURL "https://serverB.example.com"
```

サーバー グループ シナリオ

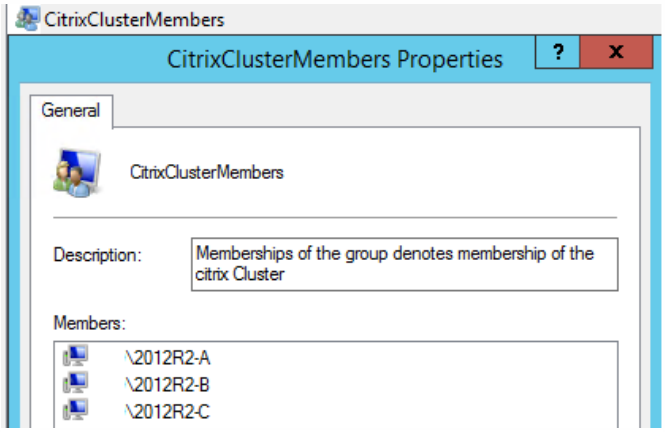
シナリオ1：既存のサーバーグループ構成をバックアップし、後でそのバックアップを同じサーバーグループ環境で復元する。

前の構成バックアップは、2つのStoreFrontサーバー（2012R2-Aと2012R2-B）のみがサーバーグループのメンバーであるときに取得されました。バックアップアーカイブ内には、元のサーバー2012R2-Aと2012R2-Bのみを含む、バックアップが取得された時点の**CitrixClusterMembership**のレコードが含まれます。StoreFrontサーバーグループ環境では、ビジネス上の需要に伴い、元のバックアップが取得された時点よりサイズが増え続けています。したがって、追加のノード2012R2-Cがサーバーグループに追加されています。バックアップに保持されているサーバーグループの基になるStoreFront構成は変更されていません。2つの元のサーバーグループノードのみを含む古いバックアップがインポートされている場合でも、3つのサーバーの現在のCitrixClusterMembershipを維持する必要があります。インポート中に、現在のクラスターメンバーシップが保持されて、構成がプライマリサーバーに正常にインポートされた後にライトバックされます。元のバックアップが取得された後にサーバーグループノードがサーバーグループから削除された場合、インポートでは現在のCitrixClusterMembershipも保持されます。

1. サーバーグループ1の構成を2012R2-Aからエクスポートします。2012R2-Aはサーバーグループ全体を管理するために使用されるプライマリサーバーです。



2. 後で、追加のサーバー2012R2-Cを既存のサーバーグループに追加します。



3. サーバーグループの構成を既知の前の作業状態に復元する必要があります。StoreFrontでは、インポートプロセスの実行中に3つのサーバーの現在のCitrixClusterMembershipがバックアップされ、インポートの成功後に復元されます。

4. サーバーグループ1の構成をノード2012R2-Aにインポートして戻します。

Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" –Credential $CredObject -HostBaseURL "https://serverB.example.com"

5. 新しくインポートした構成をサーバーグループ全体に反映して、インポート後にすべてのサーバーの構成が一致するようにします。

シナリオ2：既存の構成をサーバーグループ1からバックアップし、そのバックアップを使用して別の工場出荷時のデフォルト環境に新しいサーバーグループを作成する。ほかの新しいサーバーグループメンバーを新しいプライマリサーバーに追加できる。

新しい2つのサーバー2012R2-Cと2012R2-Dを含むサーバーグループ2が作成されます。サーバーグループ2の構成は既存環境のサーバーグループ1の構成に基づきます。サーバーグループ1にも2つのサーバー2012R2-Aと2012R2-Bが含まれています。バックアップアーカイブに含まれるCitrixClusterMembershipは、新しいサーバーグループの作成時には使用されません。現在のCitrixClusterMembershipが常にバックアップされ、インポートの成功後に復元されます。インポートされた構成を使用して

新しい展開環境を作成すると、追加サーバーが新しいグループに加わるまでは、CitrixClusterMembershipセキュリティグループには1つのインポートサーバーのみが含まれます。サーバーグループ2は新しい環境で、サーバーグループ1と共存することを目的としています。-HostBaseURLパラメーターを指定します。サーバーグループ2は、新しい工場出荷時のデフォルトStoreFront環境を使用して作成されます。

1. サーバーグループ1の構成を2012R2-Aからエクスポートします。2012R2-Aはサーバーグループ全体を管理するために使用されるプライマリサーバーです。

2. サーバーグループ1の構成をノード2012R2-Cの工場出荷時のデフォルト環境にインポートします。2012R2-Cは新しいサーバーグループ2のプライマリサーバーです。

Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" –Credential $CredObject -HostBaseURL "https://serverB.example.com"

3. 新しいサーバーグループ2環境の一部となる追加のサーバーを追加します。サーバーグループ1からサーバーグループ2の新しいすべてのメンバーに新しくインポートされた構成が自動的に反映されます。これは新しいサーバーが追加されたときの標準の追加プロセスの一部になります。

シナリオ3：既存の構成をサーバーグループAからバックアップし、そのバックアップを使用して既存のサーバーグループBの構成を上書きする。

サーバーグループ1とサーバーグループ2は既に2つの個別のデータセンターに存在します。多くのStoreFront構成の変更はサーバーグループ1で行われ、もう一方のデータセンターのサーバーグループ2に適用する必要があります。サーバーグループ1の変更をサーバーグループ2に移植できます。サーバーグループ2のバックアップアーカイブ内で**CitrixClusterMembership**を使用しないでください。インポート中に**HostBaseURL**パラメーターを指定します。サーバーグループ2のホストベースURLは、サーバーグループ1で現在使用されている同じFQDNに変更できません。サーバーグループ2は既存の環境です。

1. サーバーグループ1の構成を2012R2-Aからエクスポートします。2012R2-Aはサーバーグループ全体を管理するために使用されるプライマリサーバーです。

2. サーバーグループ1の構成をノード2012R2-Cの工場出荷時のデフォルト環境にインポートします。2012R2-Cは新しいサーバーグループ2のプライマリサーバーです。

Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" –Credential $CredObject -HostBaseURL "https://serverB.example.com"

ストア フロントの SDK

Aug 14, 2017

Citrix StoreFrontは、多くのMicrosoft Windows PowerShellのバージョン3.0モジュールをベースとしたSDKを提供しています。このSDKにより、StoreFront MMCコンソールと同じタスクだけでなく、コンソールだけでは実行できないタスクも実行できます。

SDKについては、StoreFront SDKを参照してください。

StoreFront 3.0と現在のStoreFront SDKの主な違い

- **高レベルのSDKの例**：このバージョンは、スクリプトを実行してStoreFront展開をすばやく簡単に自動化できる高レベルのSDKスクリプトを提供します。高レベルの例を特定の要件に合わせて調整できるため、1つのスクリプトを実行して新しい展開を作成することができます。
- **新しい低レベルSDK**：ドキュメント化された低レベルStoreFront SDKを提供して、NetScaler Gatewayによるリモートアクセス同様にストア、認証方法、Citrix Receiver for Webおよび統合Citrix Receiverサイトを含む展開の構成を有効にします。
- **後方互換性**：StoreFront 3.0以前のAPIをStoreFront 3.1でも使用できるため、既存のスクリプトを新しいSDKに徐々に移行できます。

> ### Important
>
> StoreFront 3.0との後方互換性は、可能な限り保持されています。ただし新しいスクリプトを書く場合は、StoreFront 3.0 SDKは古く、削除される予定のため新しい**Citrix.StoreFront.***モジュールを使用することをお勧めします。

SDKの使用

このSDKは、さまざまなStoreFrontコンポーネントをインストールおよび構成する場合に、インストールウィザードにより自動的にインストールされた多くのPowerShellスナップインで構成されています。

コマンドレットにアクセスして実行するには

1. PowerShell 3.0のシェルを開きます。
   StoreFrontサーバーのローカルの管理者グループのメンバーを使って、シェルまたはスクリプトを実行する必要があります。

2. スクリプト内でSDKコマンドレットを使用するには、PowerShellで実行ポリシーを設定する必要があります。
   PowerShell実行ポリシーについて詳しくは、Microsoft社のドキュメントを参照してください。

3. Windows PowerShellコンソールで**Add-Module**コマンドを使って、必要なモジュールをPowerShell環境に追加します。たとえば、次のように入力します。
   Import-Module Citrix.StoreFront
   すべてのコマンドレットをインポートするには、次のコマンドを実行します。

```
Get-Module -ListAvailable | Where-Object { $_.Name.StartsWith("Citrix.StoreFront") } | Import-Module
```

インポートが完了すると、各コマンドレットとそのヘルプにアクセスできます。

SDKの導入

スクリプトを作成するには、次の手順を実行します。

1. StoreFrontによって**%ProgramFiles%\Citrix\Receiver StoreFront\PowerShellSDK\Examples**フォルダー内にインストールされた指定のSDKの例の一つを実行します。
2. 独自のスクリプトのカスタマイズを容易にするため、サンプル スクリプトをレビューして、各部の実行内容について把握します。詳しくは、スクリプトの実行内容についての詳細を説明している使用例を参照してください。
3. 例のスクリプトをより実際の環境に応じて編集します。これを行うには、次の操作を行います。
   - PowerShell ISEまたは同様のツールを使ってスクリプトを編集します。
   - 変数を使って、再使用または変更するための値を割り当てます。
   - 不要なコマンドを削除します。
   - StoreFrontコマンドレットはプレフィックスSTFにより識別することができます。
   - Get-Helpコマンドレットを使って、特定のコマンド上により詳細な情報のためのコマンドレット名および-Fullパラメーターを指定します。

例

注：SDKに拡張や修正が追加されていることがあるため、例のスクリプトをコピーして貼り付けるのではなく、説明されている手順を実際に実行することをお勧めします。

例	説明
<例：簡素な展開の作成>	スクリプト：単一のXenDesktopサーバーで構成されたStoreFront Controllerのある簡素な展開を作成します。
<例：リモートアクセス展開の作成>	スクリプト：以前のスクリプト上に構築して、展開にリモートアクセスを追加します。
<例：最適な起動ゲートウェイがあるリモートアクセス展開の作成>	スクリプト：以前のスクリプト上に構築して、ユーザーエクスペリエンスをより良いものに吸うため、優先する最適な起動ゲートウェイを追加します。
<例：デスクトップアプライアンスサイトがある展開の作成>	スクリプト：デスクトップアプライアンスサイトで構成された簡素な展開を作成します。

例：簡素な展開の作成

次の例では、1つのXenDesktop Controllerで構成された簡素な展開の作成方法を示します。

まず、「SDKの導入」で説明されている手順を実行しておく必要があります。StoreFront展開を自動化するスクリプトの作成について説明した手法を使って、この例をカスタマイズできます。

注：SDKに拡張や修正が追加されていることがあるため、このドキュメントのスクリプト例をコピーして貼り付けるのではなく、このドキュメントで説明されている手順を実際に実行することをお勧めします。

スクリプトの理解

ここでは、StoreFrontにより生成されるスクリプトの各部で何を実行しているかについて説明します。これを理解することで、スクリプトを目的に応じてカスタマイズできるようになります。

- エラー処理要件を設定し、必要なStoreFrontモジュールをインポートします。より新しいバージョンのPowerShellではインポートの必要はありません。

```
Param(
  [Parameter(Mandatory=$true)]
  [Uri]$HostbaseUrl,
  [long]$SiteId = 1,
  [ValidateSet("XenDesktop","XenApp","AppController","VDIinaBox")]
  [string]$Farmtype = "XenDesktop",
  [Parameter(Mandatory=$true)]
  [string[]]$FarmServers,
  [string]$StoreVirtualPath = "/Citrix/Store",
  [bool]$LoadbalanceServers = $false,
  [int]$Port = 80,
  [int]$SSLRelayPort = 443,
  [ValidateSet("HTTP","HTTPS","SSL")]
  [string]$TransportType = "HTTP"
)

#StoreFrontモジュールをインポートする。自動読み込みがサポートされていないバージョン3.0以前のPowerShel
で必須。

Import-Module Citrix.StoreFront
Import-Module Citrix.StoreFront.Stores
Import-Module Citrix.StoreFront.Authentication
Import-Module Citrix.StoreFront.WebReceiver
```

- 認証の仮想パスおよび指定の**$StoreVirtualPath**をベースとしたCitrix Receiver Webサービスを自動化します。

```
#ストアに基づいて使用する認証およびReceiverの仮想パスを決定する
$authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"
$receiverVirtualPath = "$($StoreVirtualPath.TrimEnd('/'))Web"
```

- 必要なStoreFrontサービスの追加準備に備えて新しい展開を作成します（まだ存在していない場合）。-

Confirm:$falseは、展開を進めることができることを確認する要件を無効にします。

```
#展開が既に存在するかどうかを確認する

$existingDeployment = Get-STFDeployment

if(-not $existingDeployment)

{

  #必要なStoreFrontコンポーネントのインストール

  Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -Confirm:$false

}

elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)

{

  #展開は存在するが目的のホストベースURLに構成されていた場合

  Write-Output "このサーバーでは指定されたホストベースURLで展開が既に作成されていたため、この展開を使用します。"

}

else

{

  Write-Error "このサーバーでは違うホストベースURLを使用して展開が既に作成されています。"

}
```

- 新しい認証サービスを指定された仮想パスで作成します（パスに認証サービスが存在しない場合）。ユーザー名とパスワードを使ったデフォルトの認証方法が有効です。

```
#指定した仮想パスに認証パスが存在するかどうかを確認

$authentication = Get-STFAuthenticationService -VirtualPath $authenticationVirtualPath

Authentication :

{

  #ストアのIISパスの末尾にAuthを付けて認証サービスを追加する

  $authentication = Add-STFAuthenticationService $authenticationVirtualPath

}

else

{

  Write-Output "指定した仮想パスには既に認証サービスが存在しているため、このサービスを使用します。"
```



```
}
```

- 新しい認証サービスを指定された仮想パスで作成します（パスに認証サービスが存在しない場合）。ユーザー名とパスワードを使ったデフォルトの認証方法が有効です。

```
#指定した仮想パスに認証パスが存在するかどうかを確認

$authentication = Get-STFAuthenticationService -VirtualPath $authenticationVirtualPath

Authentication :

{

  #ストアのIISパスの末尾にAuthを付けて認証サービスを追加する

  $authentication = Add-STFAuthenticationService $authenticationVirtualPath

}

else

{

  Write-Output "指定した仮想パスには既に認証サービスが存在しているため、このサービスを使用します。"

}
```

- 指定された仮想パスで、配列**$XenDesktopServers**で定義されたサーバーがある1つのXenDesktop Controllerで構成された新しいストアサービスを作成します（まだ存在していない場合）。

```
#指定した仮想パスにストアサービスが存在するかどうかを確認する

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

if(-not $store)

{

#指定したサーバーの公開リソースに対して構成されている新規認証サービスを使用するストアを追加する

$store = Add-STFStoreService -VirtualPath $StoreVirtualPath -AuthenticationService $authentication -FarmName $Farmtype -FarmType $Farmtype -Servers $FarmServers -LoadBalance $LoadbalanceServers `

-LoadbalanceServers $LoadbalanceServers -Port $Port -SSLRelayPort $SSLRelayPort -TransportType $TransportType

}

else

{

  Write-Output "指定した仮想パスには既にストアサービスが存在しているため、このストアサービスを使用します。ファームとサーバーはこのストアに追加されます。"

  #ストアで構成されているファームの数を取得する
```



```
    $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.Count

    #一意の名前を指定してストアにファームを追加する

    Add-STFStoreFarm -StoreService $store -FarmName "Controller$($farmCount + 1)" -FarmType $Farmtype -Servers $FarmServers -LoadBalance $LoadbalanceServers -Port $Port `

        -SSLRelayPort $SSLRelayPort -TransportType $TransportType

}
```

- 指定のIIS仮想パスでCitrix Receiver for Webサービスを追加して、上記で作成されたストアで公開されたアプリケーションにアクセスします。

```
#指定した仮想パスにReceiverサービスが存在するかどうかを確認する

$receiver = Get-STFWebReceiverService -VirtualPath $receiverVirtualPath

if(-not $receiver)

{

    #Store内で公開されているアプリケーションおよびデスクトップにユーザーがアクセスできるようにReceiver for Webサイトを追加する

    $receiver = Add-STFWebReceiverService -VirtualPath $receiverVirtualPath -StoreService $store

}

else

{

    Write-Output "指定した仮想パスには既にWeb Receiverサービスが存在しているため、このWeb Receiverサービスを使用します。"

}
```

- ストアに対してXenAppサービスを有効にして、古いCitrix Receiverクライアントは公開アプリケーションに接続できます。

```
#ストアサービスでPNAが構成されているかどうかを確認する

$storePnaSettings = Get-STFStorePna -StoreService $store

if(-not $storePnaSettings.PnaEnabled)

{

  #ストアでXenAppサービスを有効化してこのサーバーのデフォルト設定にする

  Enable-STFStorePna -StoreService $store -AllowUserPasswordChange -DefaultPnaService

}
```

例：リモートアクセス展開の作成

次の例は以前のスクリプト上に構築して、リモートアクセスのある展開を追加します。

まず、「SDKの導入」で説明されている手順を実行しておく必要があります。StoreFront展開を自動化するスクリプトの作成について説明した手法を使って、この例をカスタマイズできます。

注：SDKに拡張や修正が追加されていることがあるため、このドキュメントのスクリプト例をコピーして貼り付けるのではなく、このドキュメントで説明されている手順を実際に実行することをお勧めします。

スクリプトの理解

ここでは、StoreFrontにより生成されるスクリプトの各部で何を実行しているかについて説明します。これを理解することで、スクリプトを目的に応じてカスタマイズできるようになります。

- エラー処理要件を設定し、必要なStoreFrontモジュールをインポートします。より新しいバージョンのPowerShellではインポートの必要はありません。

```
Param(
  [Parameter(Mandatory=$true)]
  [Uri]$HostbaseUrl,
  [Parameter(Mandatory=$true)]
  [long]$SiteId = 1,
  [string]$Farmtype = "XenDesktop",
  [Parameter(Mandatory=$true)]
  [string[]]$FarmServers,
  [string]$StoreVirtualPath = "/Citrix/Store",
  [bool]$LoadbalanceServers = $false,
  [int]$Port = 80,
  [int]$SSLRelayPort = 443,
  [ValidateSet("HTTP","HTTPS","SSL")]
  [string]$TransportType = "HTTP",
  [Parameter(Mandatory=$true)]
  [Uri]$GatewayUrl,
  [Parameter(Mandatory=$true)]
  [Uri]$GatewayCallbackUrl,
  [Parameter(Mandatory=$true)]
  [string[]]$GatewaySTAUrls,
```

```
    [string]$GatewaySubnetIP,

    [Parameter(Mandatory=$true)]

    [string]$GatewayName

)

Set-StrictMode -Version 2.0


#エラーが発生した場合は常に停止する。

$ErrorActionPreference = 'Stop'

$ReportErrorShowStackTrace = $true

$ReportErrorShowInnerException = $true

#StoreFrontモジュールをインポートする。自動読み込みがサポートされていないバージョン3.0以前のPowerShellで必須。

Import-Module Citrix.StoreFront

Import-Module Citrix.StoreFront.Stores

Import-Module Citrix.StoreFront.Roaming
```

- 以前のサンプルスクリプトを呼び出して、内部アクセスのStoreFront展開を作成します。ベース展開が拡張され、リモートアクセスがサポートされます。

```
#SimpleDeploymentサンプルを呼び出して簡単な展開を作成する

$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition -Parent

$scriptPath = Join-Path $scriptDirectory "SimpleDeployment.ps1"

& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -Farmtype $Farmtype `

-LoadbalanceServers $LoadbalanceServers -Port $Port -SSLRelayPort $SSLRelayPort -TransportType $TransportType
```

- リモートアクセスがサポートされるように更新する必要があるため、簡素な展開で作成されたサービスを取得します。

```
#ストアに基づいて認証およびReceiverのサイトを決定する

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$authentication = Get-STFAuthenticationService -StoreService $store

$receiverForWeb = Get-STFWebReceiverService -StoreService $store
```

- NetScaler Gatewayを使用したリモートアクセスで必要なCitrix Receiver for Webサービス上で、CitrixAGBasicを有効にします。サポートされているプロトコルからCitrix Receiver for WebのCitrixAGBasicおよびExplicitForms認証方法を取得します。

サポートされているプロトコルからCitrix Receiver for WebのCitrixAGBasicおよびExplicitForms認証方法を取得します。

#プロトコル名は既知の場合使用可能なためデモ用に記載

$receiverMethods = Get-STFWebReceiverAuthenticationMethodsAvailable | Where-Object { $_ -match "Explicit" -or $_ -match "CitrixAG" }

#Receiver for WebでCitrixAGBasicを有効化する（リモートアクセスに必要）

Set-STFWebReceiverService $receiverForWeb -AuthenticationMethods $receiverMethods

- 認証サービスでCitrixAGBasicを有効にします。これはリモートアクセスで必要です。

  #インストール済みのプロトコルからCitrixAGBasic認証方法を取得する。

  #プロトコル名は既知の場合使用可能なためデモ用に記載

  $citrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-Object { $_ -match "CitrixAGBasic" }

  #認証サービスでCitrixAGBasicを有効化する（リモートアクセスに必要）

  Enable-STFAuthenticationServiceProtocol -AuthenticationService $authentication -Name $citrixAGBasic

- 新しいリモートアクセスゲートウェイを、オプションのサブネットIPアドレスを指定して追加し、リモートでアクセスするストアに登録します。

  #新しいストアへのリモートアクセス用の新規ゲートウェイを追加する

  Add-STFRoamingGateway -Name "NetScaler10x" -LogonType Domain -Version Version10_0_69_4 -GatewayUrl $GatewayUrl '

  -CallbackUrl $GatewayCallbackUrl -SecureTicketAuthorityUrls $GatewaySTAUrls

  #構成から新規ゲートウェイを取得する（Add-STFRoamingGatewayではパラメーターとして-PassThruを指定した場合新規ゲートウェイが返される）

  $gateway = Get-STFRoamingGateway -Name $GatewayName

  #ゲートウェイサブネットが指定済みの場合ゲートウェイオブジェクトにこのサブネットを設定する

  if($GatewaySubnetIP)

  {

  Set-STFRoamingGateway -Gateway $gateway -SubnetIPAddress $GatewaySubnetIP

  }

  #新規ストアにゲートウェイを登録する

  Register-STFStoreGateway -Gateway $gateway -StoreService $store -DefaultGateway

例：最適な起動ゲートウェイがあるリモートアクセス展開の作成

次の例は以前のスクリプト上に構築して、オプションの起動ゲートウェイリモートアクセスのある展開を追加します。

まず、「SDKの導入」で説明されている手順を実行しておく必要があります。StoreFront展開を自動化するスクリプトの作成について説明した手法を使って、この例をカスタマイズできます。

注：SDKに拡張や修正が追加されていることがあるため、このドキュメントのスクリプト例をコピーして貼り付けるのではなく、このドキュメントで説明されている手順を実際に実行することをお勧めします。

スクリプトの理解

ここでは、StoreFrontにより生成されるスクリプトの各部で何を実行しているかについて説明します。これを理解することで、スクリプトを目的に応じてカスタマイズできるようになります。

- エラー処理要件を設定し、必要なStoreFrontモジュールをインポートします。より新しいバージョンのPowerShellではインポートの必要はありません。

```
Param(
  [Parameter(Mandatory=$true)]
  [Uri]$HostbaseUrl,
  [long]$SiteId = 1,
  [string]$Farmtype = "XenDesktop",
  [Parameter(Mandatory=$true)]
  [string[]]$FarmServers,
  [string]$StoreVirtualPath = "/Citrix/Store",
  [bool]$LoadbalanceServers = $false,
  [int]$Port = 80,
  [int]$SSLRelayPort = 443,
  [ValidateSet("HTTP","HTTPS","SSL")]
  [string]$TransportType = "HTTP",
  [Parameter(Mandatory=$true)]
  [Uri]$GatewayUrl,
  [Parameter(Mandatory=$true)]
  [Uri]$GatewayCallbackUrl,
  [Parameter(Mandatory=$true)]
  [string[]]$GatewaySTAUrls,
  [string]$GatewaySubnetIP,
  [Parameter(Mandatory=$true)]
```

[string]$GatewayName,

[Parameter(Mandatory=$true)]

[Uri]$OptimalGatewayUrl,

[Parameter(Mandatory=$true)]

[string[]]$OptimalGatewaySTAUrls,

[Parameter(Mandatory=$true)]

[string]$OptimalGatewayName

)

Set-StrictMode -Version 2.0

#エラーが発生した場合は常に停止する。

$ErrorActionPreference = 'Stop'

$ReportErrorShowStackTrace = $true

$ReportErrorShowInnerException = $true

#StoreFrontモジュールをインポートする。自動読み込みがサポートされていないバージョン3.0以前のPowerShellで必須。

Import-Module Citrix.StoreFront

Import-Module Citrix.StoreFront.Stores

Import-Module Citrix.StoreFront.Roaming

- リモートアクセス展開スクリプト内に呼び出し、基本展開を構成し、リモートアクセスを追加します。

  例：リモートアクセス展開の作成

  $scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition -Parent

  $scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.ps1"

  & $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -Farmtype $Farmtype `

  -LoadbalanceServers $LoadbalanceServers -Port $Port -SSLRelayPort $SSLRelayPort -TransportType $TransportType

  -GatewayUrl $GatewayUrl -GatewayCallbackUrl $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -GatewayName $GatewayName

- 優先的で最適な起動ゲートウェイを追加し、構成済みゲートウェイの一覧からそれを取得します。

  #デスクトップおよびアプリへのリモートHDXアクセス用の新規ゲートウェイを追加する

  $gateway = Add-STFRoamingGateway -Name $OptimalGatewayName -LogonType UsedForHDXOnly -GatewayUrl


```
$OptimalGatewayUrl -SecureTicketAuthorityUrls $OptimalGatewaySTAUrls -PassThru
```

- 最適なゲートウェイを使用するためにストアサービスを取得し、ゲートウェイをファームからの起動に割り当てて登録します。

```
#SimpleDeployment.ps1で構成されているストアを取得する

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

#すべてのファーム（現時点では1つのみ）に対して起動されるように新規ストアへゲートウェイを登録する

$farmNames = @($store.FarmsConfiguration.Farms | foreach { $_.FarmName })

Register-STFStoreOptimalLaunchGateway -Gateway $gateway -StoreService $store -FarmName $farmNames
```

例：デスクトップアプライアンスサイトがある展開の作成

次の例は、簡素な展開例上に構築して、デスクトップアライアンスサイトがある展開を追加します。

まず、「SDKの導入」で説明されている手順を実行しておく必要があります。StoreFront展開を自動化するスクリプトの作成について説明した手法を使って、この例をカスタマイズできます。

注：SDKに拡張や修正が追加されていることがあるため、このドキュメントのスクリプト例をコピーして貼り付けるのではなく、このドキュメントで説明されている手順を実際に実行することをお勧めします。

スクリプトの理解

ここでは、StoreFrontにより生成されるスクリプトの各部で何を実行しているかについて説明します。これを理解することで、スクリプトを目的に応じてカスタマイズできるようになります。

- エラー処理要件を設定し、必要なStoreFrontモジュールをインポートします。より新しいバージョンのPowerShellではインポートの必要はありません。

```
Param(
  [Parameter(Mandatory=$true)]
  [Uri]$HostbaseUrl,
  [long]$SiteId = 1,
  [string]$Farmtype = "XenDesktop",
  [Parameter(Mandatory=$true)]
  [string[]]$FarmServers,
  [string]$StoreVirtualPath = "/Citrix/Store",
  [bool]$LoadbalanceServers = $false,
  [int]$Port = 80,
  [int]$SSLRelayPort = 443,
  [ValidateSet("HTTP","HTTPS","SSL")]
```

```
    [string]$TransportType = "HTTP",
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$GatewaySTAUrls,
    [string]$GatewaySubnetIP,
    [Parameter(Mandatory=$true)]
    [string]$GatewayName,
    [Parameter(Mandatory=$true)]
    [Uri]$OptimalGatewayUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$OptimalGatewaySTAUrls,
    [Parameter(Mandatory=$true)]
    [string]$OptimalGatewayName
)
Set-StrictMode -Version 2.0
#エラーが発生した場合は常に停止する。
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
#StoreFrontモジュールをインポートする。自動読み込みがサポートされていないバージョン3.0以前のPowerShellで必須。
Import-Module Citrix.StoreFront
Import-Module Citrix.StoreFront.Stores
Import-Module Citrix.StoreFront.Roaming
```

- デスクトップアプライアンスのパスを、$StoreVirtualPathのパスに自動で設定します。

```
$desktopApplianceVirtualPath = "$($StoreIISPath.TrimEnd('/'))Appliance"
```

- 簡素な展開スクリプト内に呼び出して、必須サービスがあるデフォルトの展開を構成します。

  例：リモートアクセス展開の作成

  $scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition -Parent

  $scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.ps1"

  & $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -Farmtype $Farmtype `

  -LoadbalanceServers $LoadbalanceServers -Port $Port -SSLRelayPort $SSLRelayPort -TransportType $TransportType

  -GatewayUrl $GatewayUrl -GatewayCallbackUrl $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -GatewayName $GatewayName

- ストアサービスを取得して、デスクトップアプライアンスサイトに使用します。**Add-STFDesktopApplianceService**コマンドレットを使って、MultiDesktopおよび明示的ユーザー名およびパスワード認証がある新しいサイトを追加します。

  $store = Get-STFStoreService -VirtualPath $StoreVirtualPath

  #ストアサービスで公開されているデスクトップを使用して新しいデスクトップアプライアンスサイトを作成する

  Add-STFDesktopApplianceService -VirtualPath $desktopApplianceVirtualPath -StoreService $store -EnableExplicit

例： SAML認証用にIDプロバイダーとサービスプロバイダー（StoreFront）間でメタデータを交換する

SAML認証の構成は、StoreFront管理コンソール内（「認証サービスの構成」を参照）で、または Export-STFSamlEncryptionCertificate、Export-STFSamlSigningCertificate、Import-STFSamlEncryptionCertificate、Import-STFSamlSigningCertificate、New-STFSamlEncryptionCertificate、New-STFSamlIdPCertificate、New-STFSamlSigningCertificateの各PowerShellコマンドレットを使用して行うことができます。

Update-STFSamlIdPFromMetadataコマンドレットを使用すると、IDプロバイダーとサービスプロバイダー（今回はStoreFront）の間でメタデータ（ID、証明書、エンドポイントなどの構成）を交換できます。

StoreFrontストアの名前が「Store」であり。専用の認証サービスが設定されている場合、そのメタデータエンドポイントは次のようになります。

https:///Citrix/StoreAuth/SamlForms/ServiceProvider/Metadata

IDプロバイダーでメタデータのインポートがサポートされている場合、このプロバイダーを上記URLへポイントすることができます。**注：** この操作はHTTPSを介して行う必要があります。

StoreFrontでIDプロバイダーのメタデータを消費するには、次のPowerShellコマンドレットを使用します。

```
-command
```

コピー

```
Get-Module "Citrix.StoreFront*" -ListAvailable | Import-Module



# Remember to change this with the virtual path of your Store.

$StoreVirtualPath = "/Citrix/Store"



$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store



# To read the metadata directly from the Identity Provider, use the following:

# Note again this is only allowed for https endpoints

Update-STFSamlIdPFromMetadata -AuthenticationService $auth -Url https://example.com/FederationMetadata/2007-06/FederationMetada



# If the metadata has already been download, use the following:

# Note: Ensure that the file is encoded as UTF-8

Update-STFSamlIdPFromMetadata -AuthenticationService $auth -FilePath "C:\Users\exampleusername\Downloads\FederationMetadata.x
```

例：SAML認証用の指定されたストアのメタデータおよびACSエンドポイント一覧を作成する

次のスクリプトを使用して、指定されたストアのメタデータおよびACS（Assertion Consumer Service）エンドポイントの一覧を作成できます。

```
-command
```
コピー

```
# Change this value for your Store

$storeVirtualPath = "/Citrix/Store"



$auth = Get-STFAuthenticationService -Store (Get-STFStoreService -VirtualPath $storeVirtualPath)

$spId = $auth.AuthenticationSettings["samlForms"].SamlSettings.ServiceProvider.Uri.AbsoluteUri

$acs = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.VirtualPath + "/SamlForms/AssertionConsumerService")

$md = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.VirtualPath + "/SamlForms/ServiceProvider/Metadata")

$samlTest = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.VirtualPath + "/SamlTest")

Write-Host "SAML Service Provider information:

Service Provider ID: $spId

Assertion Consumer Service: $acs

Metadata: $md

Test Page: $samlTest"
```

出力例

```
-command
```
コピー

```
SAML Service Provider information:

Service Provider ID: https://storefront.example.com/Citrix/StoreAuth

Assertion Consumer Service: https://storefront.example.com/Citrix/StoreAuth/SamlForms/AssertionConsumerService

Metadata: https://storefront.example.com/Citrix/StoreAuth/SamlForms/ServiceProvider/Metadata

Test Page: https://storefront.example.com/Citrix/StoreAuth/SamlTest
```

StoreFrontのトラブルシューティング

Aug 14, 2017

StoreFrontのインストール時やアンインストール時に、インストーラーによりC:\Windows\Temp\フォルダーに以下のログファイルが作成されます。これらのログファイルには、作成元のコンポーネントと日時を示すファイル名が付けられます。

- Citrix-DeliveryServicesRoleManager-*.log：StoreFrontのインタラクティブインストール時に作成されます。
- Citrix-DeliveryServicesSetupConsole-*.log：StoreFrontのサイレントインストール時、インタラクティブアンインストール時、およびサイレントアンインストール時に作成されます。
- CitrixMsi-CitrixStoreFront-x64-*.log：StoreFrontのインタラクティブインストール時、サイレントインストール時、インタラクティブアンインストール時、およびサイレントアンインストール時に作成されます。

StoreFrontの認証サービス、ストア、およびReceiver for Webサイトのイベントは、Windowsイベントログに書き込まれます。生成されたイベントはStoreFrontのアプリケーションログに書き込まれます。このログを表示するには、イベントビューアーで［アプリケーションとサービスログ］>［Citrix Delivery Services］または［Windowsログ］>［アプリケーション］の順に選択します。単一イベントに対して同じログエントリが何度も書き込まれないようにするには、認証サービス、ストア、およびReceiver for Webサイトの構成ファイルを編集してログ調整を構成します。

Citrix StoreFront管理コンソールでは、トレース情報が自動的に記録されます。デフォルトではほかの操作のトレースは無効になっており、手作業で有効にする必要があります。Windows PowerShellコマンドにより作成されるログファイルは、StoreFrontのインストール先フォルダーにある\Admin\logs\フォルダー内に保存されます。このインストール先フォルダーは通常、C:\Program Files\Citrix\Receiver StoreFront\です。このログファイルの名前は、実行されたコマンド処理、対象、および実行順序を識別するための日時で構成されます。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

ログ調整を構成するには

1. 認証サービス、ストア、またはReceiver for Webサイトのweb.configファイルをテキストエディターで開きます。これらのファイルは通常、それぞれC:\inetpub\wwwroot\Citrix\Authentication\、C:\inetpub\wwwroot\Citrix\storename\、およびC:\inetpub\wwwroot\Citrix\storenameWeb\フォルダーにあります。ここで、storenameはストアの作成時に指定した名前です。
2. ファイル内で次の要素を検索します。
   StoreFrontのデフォルトでは、重複するログエントリの数が1分あたり10件までに制限されます。
3. duplicateInterval属性の値を変更して、重複エントリの監視期間を時間、分、秒で設定します。duplicateLimit属性の値を変更して、指定した監視期間内に記録される重複エントリの数を設定します。この数を超えるとログ調整が実行されます。

ログ調整が実行されると、指定した数を超える重複ログエントリが抑制され、それを示す警告メッセージが記録されます。監視期間が経過すると、ログ調整が解除され、それを示す情報メッセージが記録されます。

トレースを有効にするには

注意：StoreFront管理コンソールとPowerShellコンソールを同時に開くことはできません。StoreFront管理コンソールを閉じてからPowerShellコンソールを開いてください。同様に、PowerShellのすべてのインスタンスを閉じてからStoreFront管理コンソールを開いてください。

1. ローカルの管理者アカウントを使ってWindows PowerShellを起動して、コマンドプロンプトで次のコマンドを実行してサーバーを再起動します。これにより、トレースが有効になります。

```
Add-PSSnapin Citrix.DeliveryServices.Framework.Commands Set-DSTraceLevel -All -TraceLevel Verbose
```

TraceLevelに指定できる値は、トレースの詳細度の低いものから順に Off、Error、Warning、Info、Verboseです。StoreFrontでは、Errorトレースメッセージが自動的に記録されます。大量のデータが生成される可能性があるため、トレースはStoreFrontのパフォーマンスに大きな影響を与える可能性があります。このため、特に必要な場合を除き、InfoやVerboseを指定しないことをお勧めします。

Set-DSTraceLevelコマンドレットのオプションの引数は次のとおりです。
-FileCount：トレースファイルの数を指定します（デフォルトは、3）
-FileSizeKb：各トレースファイルの最大サイズを指定します（デフォルトは、1000）
-ConfigFile <ファイル名>：すべてではなく特定の構成ファイルを構成できる-Allの代わりとなるものです。たとえば、c:\inetpub\wwwroot\Citrix\<ストア名>\web.configの-ConfigFile値は、<ストア名>という名前のストアに対するトレースを設定します。

2. トレースを無効にするには、コマンドプロンプトで以下のコマンドを実行してサーバーを再起動します。
```
Add-PSSnapin Citrix.DeliveryServices.Framework.Commands Set-DSTraceLevel -All -TraceLevel Off
```

トレースを有効にすると、StoreFrontのインストール先フォルダーにある\Admin\Trace\フォルダー内にトレース情報が自動的に書き込まれます。このインストール先フォルダーは、C:\Program Files\Citrix\Receiver StoreFront\です。