StoreFront 1912

Contents

StoreFront 1912

January 31, 2020

StoreFront 1912 は、StoreFront の最新リリース（CR）です。このドキュメントには、この最新リリースの機能と構成が反映されています。

StoreFront は、Citrix Virtual Apps and Desktops サイトからアプリケーションとデスクトップを集約して、使いやすい単一のストアとして機能するエンタープライズアプリストアです。StoreFront は Citrix Virtual Apps and Desktops の統合コンポーネントで、さまざまなバージョンの Virtual Apps and Desktops で使用できます。

ユーザーは、Citrix Workspace アプリまたはサポート対象のバージョンの Citrix Receiver を使用して、StoreFront ストアにアクセスできます。特定のバージョンが異なる動作をする場合、またはユーザーインターフェイステキストが両方に言及している場合、記載に従います。それ以外の場合は、ドキュメントは「Citrix Workspace アプリ」を指しています。

以前のリリース

以前のリリースのドキュメントについては、以下を参照してください:

- StoreFront 1909
- StoreFront 1906
- StoreFront 1903
- StoreFront 1811
- StoreFront 3.16
- StoreFront 3.12
- StoreFront 3.0
- 以前のバージョンの StoreFront

Citrix Virtual Apps and Desktops の最新リリース（CR）および長期サービスリリース（LTSR）の製品ライフサイクル戦略は、ライフサイクルマイルストーンで説明しています。StoreFront のライフサイクルについてさらに詳しくは、CTX200356を参照してください。

> 注:
>
> StoreFront の以前のサポートされていないバージョンから最新バージョンの CR へのアップグレードはサポートされていません。CR を使用している場合、常にサポートされている StoreFront 最新リリースバージョンを使用するようにしてください。

新機能

March 2, 2020

StoreFront 1912

StoreFront 1909 には次の新機能があります。修正プログラムについて詳しくは、「解決された問題」を参照してください。

StoreFront プロトコルハンドラーが、**Android** 向け **Workspace** アプリを搭載した **Chrome** デバイスをサポートするようになりました

Chrome デバイスでユーザーが Citrix Receiver for Web サイトを開くと、Android 向け Citrix Workspace アプリ 1912 以降がインストールされている場合、起動時にブラウザーが Android 向け Citrix Workspace アプリを使用して自動的に ICA ファイルを開きます。

Android 向け Citrix Workspace アプリがインストールされているかを判断する Linux のクライアント検出ワークフローは、Chrome ブラウザーが Chrome デバイスで使用されている場合、Windows 向け Citrix Workspace アプリおよび Mac 向け Citrix Workspace アプリの場合と同一の形式になりました。以前のリリースでは、Chrome デバイスのユーザーはダウンロードした ICA ファイルを最初に手動で開く必要がありました。

アプリ保護ポリシーのサポート

StoreFront 1912 は、Citrix Workspace アプリや Citrix Virtual Apps and Desktops Delivery Controller などの他の Citrix コンポーネントもアプリ保護機能をサポートしている場合、セキュリティを強化するアプリ保護ポリシーをサポートします。アプリ保護ポリシーはデリバリーグループレベルで設定され、Citrix Virtual Apps and Desktops がアプリ保護ポリシーを使用するかどうかを決定します。StoreFront 内でアプリ保護機能を手動で有効にする必要があります。StoreFront がアプリ保護ポリシーをサポートする Citrix Workspace アプリから HTTP ヘッダー「X-Citrix-AppProtection-Capable」を含む要求を受信すると、StoreFront はアプリ保護ポリシーをサポートすることを示すスマートアクセスタグを Citrix Virtual Apps and Desktops に自動的に送信します。アプリ保護ポリシーを使用したデリバリーグループの構成について詳しくは、「アプリ保護」を参照してください。

StoreFront サーバーでアプリ保護を有効にするには、StoreFront サーバーで次の PowerShell コマンドを実行します: `Add-STFFeatureState -Name "Citrix.StoreFront.AppProtectionPolicy.Control" -IsEnabled $True`。(複数サーバーの StoreFront 展開環境では、手動でサーバーグループ内のほかのサーバーに変更を反映する必要があります。詳しくは、「サーバーグループへのローカルの変更の反映」を参照してください)。

この機能が **StoreFront** サーバー上で有効になっていることを確認するには、次の PowerShell コマンドを使用します:
`Get-STFFeatureState -Name "Citrix.StoreFront.AppProtectionPolicy.Control`。

デスクトップアプライアンスサイトのサポート終了

ユーザーがデスクトップアプライアンスサイトのデスクトップにアクセスするための StoreFront サポートは、Citrix Virtual Apps and Desktops 7 1811 での廃止が発表されました。このリリースでは、デスクトップアプライアンスサイトはサポートされなくなりました。ドメイン不参加のユースケースでは Citrix Workspace アプリDesktop Lockの使用をお勧めします。

> 警告:
>
> StoreFront 1912 にアップグレードすると、展開内のデスクトップアプライアンスサイトは自動的に削除されます。「StoreFront のアップグレード」を参照してください。

StoreFront PowerShell SDK

StoreFront PowerShell SDK は、バージョン 1912 として再公開されました。PowerShell を使用してデスクトップアプライアンスサイトを作成または管理することはできなくなりました。

解決された問題

January 31, 2020

次の問題は、バージョン 1909 以降で解決されています。

- オンプレミスの StoreFront は、MMC で Web リンクの起動ゲートウェイを追加できません。[WSP-4368]
- LCM-6351: CitrixPrivilegedService_x64.msi の古いレジストリキーは DDC のアップグレード後に削除されませんでした。[WSP-4785]
- StoreFront サーバーに VMware VMTools v10.3.x がインストールされている場合、Citrix Virtual Apps and Desktops 7 1906 メタインストーラーを使用して StoreFront をバージョン 1906 にアップグレードしようとすると失敗します。StoreFront は、スタンドアロン StoreFront 1906 インストーラーでアップグレードできますが、StoreFront 1906 は Windows のプログラムの追加/削除リストに追加されません。[WSP-4895]
- X1.1 Purple UI では、長いアプリ名をカスタマイズして省略することはできなくなりました。[WSP-4899]
- アップグレード履歴に 2.6、3.0.1、3.5、3.8 が含まれる場合、Kerberos の制約付き委任（KCD）サービスが停止状態のときに 3.12 CU* 以降へのアップグレードが失敗することがあります。[WSP-5160]

- http://downloadplugins.citrix.comを更新して、販売終了となった Citrix Receiver の代わりに Citrix Workspace アプリを配信します。[WSP-5303]

既知の問題

January 14, 2020

このリリースの既知の問題は次のとおりです。

- Windows で TLS 1.0 が無効で、Windows Server が.NET Framework 4.5 サーバーを使用している場合、StoreFront Server グループのメンバー間でサブスクリプションを反映できません。デフォルトでは、.NET Framework 4.5 は TLS 1.0 のみを使用します。この問題を回避するには、サーバー上の.NET Framework を 4.7 以降（デフォルトで TLS 1.2 を使用）にアップグレードします。[STF-2413]
- スマートカード認証と Microsoft Edge に関するサードパーティの既知の問題があります。この問題を解決するには、Internet Explorer を使用します。[DNA-47809]
- 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, DNA-22561]
- StoreFront を Windows Server 2012 R2 にインストールすると、Citrix Analytics サービス（CAS）への登録に失敗する場合があります。この問題は、C++ ランタイムソフトウェアコンポーネントがインストールされていないために発生します。StoreFront のスタンドアロンインストーラーでは、これらのコンポーネントはインストールされません。これを回避する簡単な方法として、StoreFront のインストール前または後に、C++ ランタイムをインストールしてください。[WSP-4412]

サードパーティ製品についての通知

March 2, 2020

StoreFront には、次のドキュメントで定義された条件の下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。

StoreFront サードパーティ製品についての通知 （PDF のダウンロード）

システム要件

March 2, 2020

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。

> 注:
>
> 製品終了（EOL）になった古い最新リリースから最近の最新リリースへのアップグレードはサポートされていません。詳しくは、「CTX200356」を参照してください。

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 2019 の Datacenter、および Standard エディション
- 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

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。StoreFront 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の向上は確認されていません。理想的には、サーバーグループ内のすべてのサーバーは同じ場所（データセンター、アベイラビリティゾーン）に存在する必要がありますが、グループ内のサーバー間のリンクが遅延の最小基準を満たしていれば、サーバーグループは同じリージョン内の場所に分散できます。「スケーラビリティ」を参照してください。

StoreFront をインストールする前に、Windows PowerShell（バージョン 4.0 以降）および Microsoft 管理コンソール（バージョン 3.0 以降）を Web サーバーにインストールする必要があります。これらは両方とも Windows Server のデフォルトのコンポーネントです。

StoreFront インストーラーは、StoreFront をインストールする前に次の前提条件がインストールされ有効になっていることを確認します。デフォルトでは、これらの前提条件は OS ごとの機能パッケージとして提供されます。StoreFront インストーラーがこれらの前提条件のいずれかが満たされていない、または無効になっていることを検出した場合、自動的にインストールされ有効になります。

- Microsoft .NET Framework（バージョン 4.5.1 以降）
- Microsoft ASP.NET（バージョン 4.5 以降）

- Microsoft Visual C++ VC141 x64 ランタイム
- Microsoft インターネットインフォメーションサービス（IIS）

  IIS は Web サーバーの「Windows Server」役割によって追加されます。バージョンは選択したオペレーティングシステムによって異なります。StoreFront インストーラーは次の IIS 役割を追加します：

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

  StoreFront の IIS での相対パスが、サーバー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 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るため、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。
- HTML5 向け Citrix Workspace アプリまたは Citrix Receiver および Citrix Workspace アプリのサポート対象バージョンが有効な場合、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。

Microsoft SQL Server を使用したサブスクリプションデータの保存

必要に応じて、Microsoft SQL Server を使用したサブスクリプションデータの保存を行うこともできます。StoreFront でこのオプションがサポートされる Microsoft SQL Server バージョンは、Citrix Virtual Apps and

Desktops でデータベースに関してサポートされる Microsoft SQL Server バージョンと同じです。Citrix Virtual Apps and Desktops の「システム要件」の「データベース」セクションを参照してください。

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。

- Citrix Virtual Apps and Desktops 7 1912 LTSR
- Citrix Virtual Apps and Desktops 7 1909
- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp および XenDesktop 7.15 LTSR *
- XenApp および XenDesktop 7.6 LTSR *

* 長期サービスリリース（LTSR）環境でのこの最新リリース（CR）の使用について、およびその他のよくある質問については、Citrix Knowledge Center の記事を参照してください。

Citrix 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 Citrix Gateway および NetScaler Gateway を使用できます。

- Citrix Gateway 13.0
- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1

HTML5 向け **Citrix Workspace** アプリの要件

Citrix Receiver for Web サイト上で動作する HTML5 向け Citrix Workspace アプリを使用した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、HTML5 向け Citrix Workspace アプリを使用して、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。

- Citrix Virtual Apps and Desktops 7 1912 LTSR
- Citrix Virtual Apps and Desktops 7 1909
- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp および XenDesktop 7.15 LTSR
- XenApp および XenDesktop 7.6 LTSR

> 注:
>
> HTML5 向け Citrix Workspace アプリは、リソースをホストする VDA への安全な接続が構成されている場合にのみ、内部ネットワーク接続を使用してデスクトップとアプリを起動します。アプリとデスクトップをホストする VDA への HTTP 接続は使用できません。

社内ネットワーク外のリモートユーザーが HTML5 向け Citrix Workspace アプリを使用する場合、以下のバージョンの Citrix Gateway および 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。

- Citrix Gateway 13.0
- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1

Citrix Gateway を介した接続では、HTML5 向け Citrix Workspace アプリを使用して、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。

- Citrix Virtual Apps and Desktops 7 1912 LTSR
- Citrix Virtual Apps and Desktops 7 1909
- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp および XenDesktop 7.15 LTSR
- XenApp および XenDesktop 7.6 LTSR

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 Workspace アプリのユーザーは、Citrix Workspace アプリを使用してストアにアクセスしたり、Web ブラウザーから Citrix Receiver for Web サイトにログオンしたりできます。Citrix Workspace アプリ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 HTML5 向け Citrix Workspace アプリを有効にして、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。

Citrix Desktop Lock を実行している 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。

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。

Citrix Workspace アプリを使用して StoreFront ストアにアクセスする

現在サポートされているすべてのバージョンの Citrix Workspace アプリで、内部ネットワーク接続と Citrix Gateway の両方から StoreFront ストアにアクセスできます。Citrix Workspace アプリと Citrix Receiver のライフサイクル日程については、https://www.citrix.com/support/product-lifecycle/milestones/receiver.htmlを参照してください。

Citrix Gateway 経由の StoreFront ストアへの接続は、Citrix Gateway Plug-in、ICA プロキシ、またはクライアントレス VPN（cVPN）を使用して実行できます。「統合ユーザーエクスペリエンス」を参照してください。

Citrix Receiver for Web サイト経由でストアにアクセスする

内部ネットワーク接続と Citrix Gateway の両方から Citrix Receiver for Web サイトにアクセスするには、次のブラウザーの最新バージョンを使用します：

Windows の場合

- Internet Explorer 11
- Microsoft Edge
- Google Chrome
- Mozilla Firefox

Mac の場合

- Safari
- Google Chrome
- Mozilla Firefox

Linux の場合

- Google Chrome
- Mozilla Firefox

Citrix Gateway 経由の接続は、Citrix Gateway Plug-in、ICA プロキシ、またはクライアントレス VPN（cVPN）を使用して実行できます。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 Citrix 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。

Citrix Receiver for Web サイトを介してリソースを起動する

Citrix Receiver for Web サイトは、ネイティブにインストールされた Citrix Workspace アプリ経由で、または HTML5 向け Citrix Workspace アプリ経由での起動をサポートします。上記のブラウザーはすべて HTML5 に準拠しており、HTML5 リソースを起動できます。Receiver for Web の構成によっては、エンドユーザーが 2 つの起動方法を切り替えることができます。

XenApp Services の **URL** 経由でストアにアクセスする

XenApp Services の URL を使用すると、機能が限定された状態で StoreFront ストアにアクセスできます。XenApp Services の URL は、PNAgent 経由の接続のみをサポートする Citrix Receiver 3.4 Enterprise およびそれ以前のクライアントによる接続に対して、後方互換性のあるレガシーサポートを提供します。Citrix Gateway 経由の接続（サポートされる場合）は、Citrix Gateway Plug-in およびクライアントレスアクセスを使用して実行できます。

スマートカードの要件

Citrix Receiver for Windows 4.x、および **Windows** 向け **Citrix Workspace** アプリ **1808** 以降でスマートカードを使用する

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、Citrix Virtual Apps and Desktops ドキュメントの「スマートカード」およびhttp://www.citrix.com/readyを参照してください。

Citrix Gateway で認証する

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 Citrix Gateway を使用できます。

- Citrix Gateway 13.0
- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1

Citrix Analytics Service の要件

Citrix StoreFront を構成して、Citrix Workspace アプリが Citrix Analytics Service にデータを送信できます。構成の詳細は、「Citrix Analytics Service」で説明されています。この機能は、次のシナリオでサポートされています:

- HTML5 対応 Web ブラウザーで Citrix Receiver for Web サイトに移動してアクセスされるストア。ネイティブの Citrix Workspace アプリまたは HTML5 を使用してリソースを起動すると、Citrix Analytics サービスデータが提供されます。
- Windows 向け Citrix Workspace アプリ 1903 以降からアクセスされるストア。
- Linux 向け Citrix Workspace アプリ 1901 以降からアクセスされるストア。

StoreFront の展開計画

January 14, 2020

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。Citrix Virtual Apps and Desktops 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。

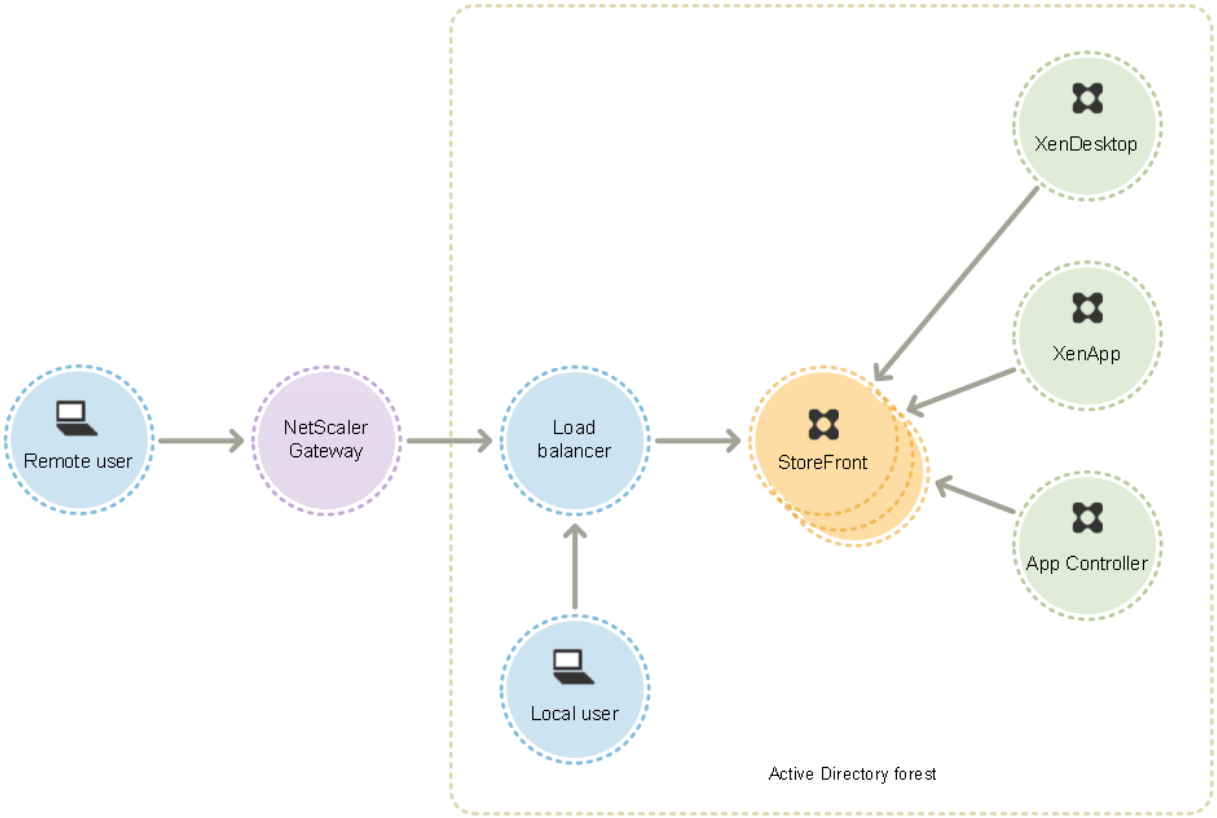
StoreFront は、次のコアコンポーネントにより構成されています。

- 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、Citrix Virtual Apps and Desktops 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 Workspace アプリ、Citrix Receiver for Web サイトおよび 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、「ユーザーアクセスのオプション」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 展開の例を示しています。



負荷分散

複数サーバーの展開環境の場合は、Citrix ADC 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。Citrix ADC 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 ネットワークの負荷分散については、http://technet.microsoft.com/en-us/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 Citrix Virtual Desktops サイトや Citrix Virtual Apps 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、Citrix ADC 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] <
    WebReceiverService> [[-Loopback] <On | Off | OnUsingHttp>] [[-
    LoopbackPortUsingHttp] <Int32>]
```

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
```

> 注:
>
> 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します。

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、Citrix Virtual Apps and Desktops 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 Citrix Gateway が必要です。社内ネットワークの外に Citrix 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 Citrix Gateway を分離します。Citrix 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 Web サイトを作成する方法については、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：アプリケーション用とデスクトップ用の **2** つの **IIS Web** サイト展開を作成するには

```
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 Workspace アプリユーザーの数は、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 Workspace アプリを使用する場合も、Citrix Receiver for Web を使用する場合と同様に、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:
>
> StoreFront サーバーグループの展開は、サーバーグループ内のサーバー間のリンクの遅延が 40 ミリ秒未満（サブスクリプションが無効の場合）または 3 ミリ秒未満（サブスクリプションが有効の場合）のみの場合にサポートされます。理想的には、サーバーグループ内のすべてのサーバーは同じ場所（データセンター、アベイラビリティゾーン）に存在する必要がありますが、グループ内のサーバー間のリンクがこれらの遅延基準を満たしていれば、サーバーグループは同じリージョン内の場所に分散できます。たとえば、1 つのクラウドリージョン内または大都市圏データセンター間のアベイラビリティゾーンにまたがるサーバーグループなどがあります。ゾーン間の遅延はクラウドプロバイダーによって異なることに注意してください。複数の場所にまたがる障害回復構成はお勧めしませんが、高可用性に適している場合もあります。
>
> 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の混在や、言語およびロケール構

> 成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」および「通信のタイムアウト期間および再試行回数」を参照してください。

ユーザーアクセスのオプション

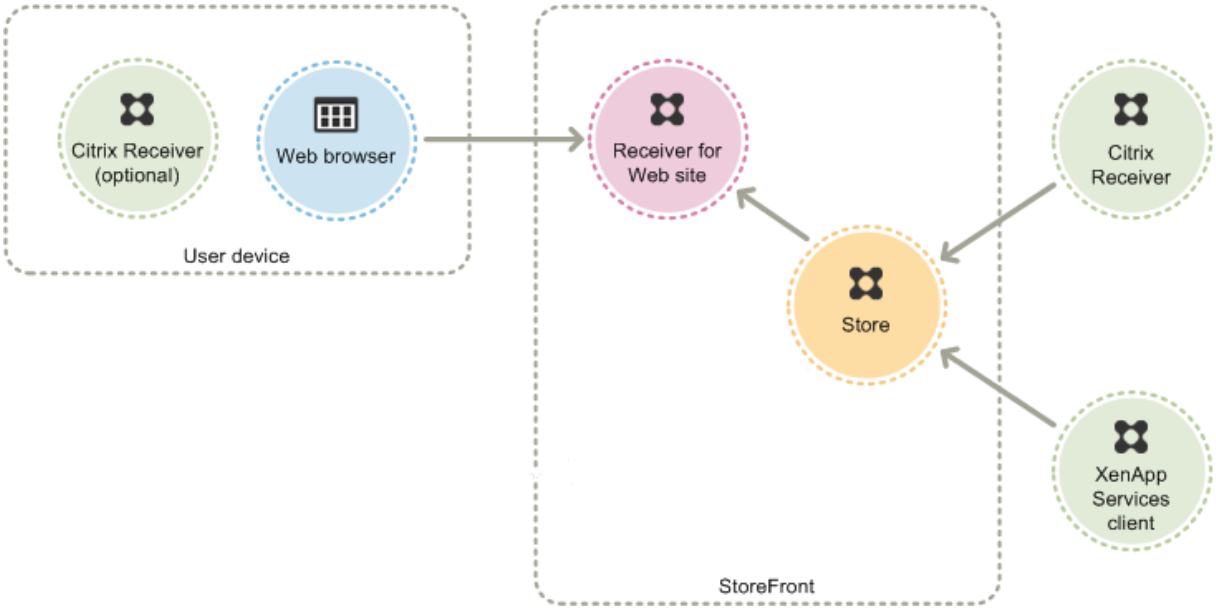
March 2, 2020

ユーザーは、以下の 3 つの方法で StoreFront ストアにアクセスできます。

- Citrix Receiver または Citrix Workspace アプリ - 適切なバージョンの Citrix Receiver または Citrix Workspace アプリのユーザーは、Citrix Receiver または Citrix Workspace アプリ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。これにより、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。
- 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 または Citrix Workspace アプリも必要です。ただし、管理者は、Citrix Receiver または Citrix Workspace アプリ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。新しいストアを作成すると、そのストアの Citrix Receiver for Web サイトがデフォルトで作成されます。
- XenApp Services サイトの 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時に、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 または Citrix Workspace アプリ

Citrix Receiver または Citrix Workspace アプリ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 または Citrix Workspace アプリ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。このドキュメントでは、「Citrix Workspace アプリ」に関する記載は、特に明記されていない限り、サポートされているバージョンの Citrix Receiver にも適用されます。

Citrix Workspace アプリでは、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 Workspace アプリ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 Workspace アプリに返します。これにより、Citrix Workspace アプリでは、ユーザーがデスクトップまたはアプリケーションにアクセスしたときに再ログオンする必要がなくなります。詳しくは、「ビーコンポイントの構成」を参照してください。

Citrix Workspace アプリ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 Workspace アプリ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。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、Citrix Receiver for Windows または Windows 向け Citrix Workspace アプリのドキュメントの「コマンドラインパラメーターを使用した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 Workspace アプリ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、「ユーザー用の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 のユーザーに向けて、Citrix Receiver for Mac または Mac 向け Citrix Workspace アプリの 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 を生成できます。ユーザーが Citrix Workspace アプリ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。

手動構成

Citrix Workspace アプリの構成に慣れているユーザーであれば、Citrix Workspace アプリにストア URL を入力して新しいアカウントを作成できます。詳しくは、Citrix Workspace アプリ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 Workspace アプリをデバイスに初めてインストールするユーザーは、シトリックスの 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 Workspace アプリ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 Citrix 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 Workspace アプリの初回構成時に自分のメールアドレスを入力します。Citrix Workspace アプリ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 Workspace アプリに表示されます。

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 Workspace アプリ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。Citrix Workspace アプリをシトリックス Web サイトからダウンロードするか、内部ネットワーク内でホストされている Citrix Workspace アプリのダウンロードページからダウンロードする場合、ユーザーは Citrix Workspace アプリをインストールして構成するときに、ストアのアクセス詳細を知る必要はありません。メールアドレスによるアカウントの検出は、Citrix Workspace アプリが Receiver for Web サイトなどの他の場所からダウンロードされた場合に使用できます。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 Workspace アプリの初回構成時に、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 Workspace アプリはメールアドレスで指定されたドメインの Microsoft Active Directory DNS 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 Workspace アプリ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 Citrix 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上に StoreFront を展開することもできます。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。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 Workspace アプリは「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、Citrix 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、Subject または 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 Workspace アプリで 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、Citrix Gateway で StoreFront 接続の詳細を構成する必要があります。詳しくは、「メールベースの検出を使用して StoreFront に接続する」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、［管理ツール］フォルダーで［**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、Citrix 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。

   内部 DNS サーバーと外部 DNS サーバーの両方が環境に含まれている場合は、StoreFront サーバーの FQDN を指定する SRV レコードを内部 DNS サーバーに追加し、Citrix Gateway の FQDN を指定する別の SRV レコードを外部サーバーに追加することができます。この構成により、リモートユーザーには Citrix 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. Citrix 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 Citrix 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 Workspace アプリ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 Workspace アプリと 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 Workspace アプリ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 Workspace アプリが検出されない場合は、プラットフォームに適した Citrix Workspace アプリ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 Workspace アプリ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 Workspace アプリ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 または Windows 向け Citrix Workspace アプリ、および Citrix Receiver for Mac または Mac 向け Citrix Workspace アプリ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。

HTML5 向け **Citrix Workspace** アプリ

HTML5 向け Citrix Workspace アプリは 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 HTML5 向け Citrix Workspace アプリを有効にすると、Citrix Workspace アプリ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。HTML5 向けの Citrix Workspace アプリを使用すると、ユーザーは Citrix Workspace アプリをインストールしなくても、HTML5 対応の Web ブラウザー内でデスクトップやアプリケーションに直接アクセスできます。サイトを作成すると、HTML5 向け Citrix Workspace アプリはデフォルトで無効になります。HTML5 向け Citrix Workspace アプリ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。

HTML5 向け Citrix Workspace アプリ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 対応の Web ブラウザーで Citrix Receiver for Web サイトを開きます。HTML5 向け Citrix Workspace アプリ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。

HTML5 向け Citrix Workspace アプリは、内部ネットワーク上のユーザーと Citrix 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、HTML5 向け Citrix Workspace アプリでは、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 HTML5 向け Citrix Workspace アプリをオプションとして選択すると、Citrix 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。HTML5 向け Citrix Workspace アプリを使用する場合は、特定のバージョンの Citrix 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 Citrix Virtual Apps and Desktops で提供されるリソースに HTML5 向け Citrix Workspace アプリでアクセスすることはできません。HTML5 向け Citrix Workspace アプリ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、Citrix Virtual Apps and Desktops 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スデバイスで、ポリシーで指定された HTML5 向け Citrix Workspace アプリ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、HTML5 向け Citrix Workspace アプリ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 HTML5 向け Citrix Workspace アプリ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 HTML5 向け Citrix Workspace アプリを構成することもできます。詳しくは、「HTML5 向け Citrix Workspace アプリ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 URL を生成できます。生成した URL 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 Workspace アプリまたは HTML5 向け Citrix Workspace アプリ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は、サイトの構成、Citrix Workspace アプリをユーザーのデバイスで検出できるかどうか、および HTML5 対応の 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、Citrix 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 Citrix 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 Workspace アプリ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 Citrix 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 Citrix Gateway を使って接続している場合、HTTPS 接続で HTML5 向け Citrix Workspace アプリを使用できます。
- Mozilla Firefox で HTTPS 接続の HTML5 向け Citrix Workspace アプリを使用するには、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。

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 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 Workspace アプリから 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 または Windows 向け Citrix Workspace アプリから 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、Citrix Virtual Apps and Desktops 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、Citrix Receiver for Windowsの最新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。XenApp Services サイトの URL 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。これにより、PNAgent プロトコルのみを使用でき

る Citrix Workspace アプリが 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 Workspace アプリ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 ベースの認証」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デフォルトで有効になっており、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して、ストアにデスクトップとアプリケーションを提供する Citrix Virtual Apps and Desktops 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

January 14, 2020

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と構成」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 Citrix Gateway を使用して Citrix Receiver for Web にアクセスする場合、Citrix 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 Citrix 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 または Linux 向け Citrix Workspace アプリユーザーは、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、Citrix Gateway 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：

- Citrix フェデレーション認証サービスの実装。
- 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 AD FS 2016 の展開」および「Microsoft AD 2016 FS の運用」を参照してください。
  - Microsoft Windows Server 2012 R2
  - Citrix Gateway（IdP として構成）
- 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（4.6 以降）または Windows 向け Citrix Workspace アプリ、または Citrix Receiver for Web。

現在、Citrix Gateway 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 Workspace アプリおよび 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、ドメイン参加 Windows クライアントマシンで Internet Explorer、Microsoft Edge、Mozilla Firefox、Google Chrome によるドメインパススルー認証をサポートします。

ドメインパススルー認証を有効にするには

1. Citrix Receiver for Windows、Windows 向け Citrix Workspace アプリ、または Citrix Online plug-in for Windows をユーザーデバイスにインストールします。パススルー認証が有効になっていることを確認します。
2. 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、
3. 「ドメインパススルー認証の構成」で説明されているように、Citrix Receiver for Windows または Windows 向け Citrix Workspace アプリ上で SSON を構成します。HTML5 向け Citrix Workspace アプリでは、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。
4. Windows のデフォルトの動作は、「イントラネットゾーンで自動ログオン」です。Internet Explorer、Mozilla Firefox、Google Chrome の場合、インターネットオプションを使用して Citrix Receiver for Web サイトをイントラネットサイトとして構成するか、信頼済みゾーンで自動ログオンを有効にします。Microsoft Edge の場合、Citrix Receiver for Web サイトをイントラネットサイトとして構成する必要があります。
5. Mozilla Firefox の場合、ブラウザーの詳細設定を変更して Citrix Receiver for Windows または Windows 向け Citrix Workspace アプリの URI を信頼します。

   > 警告：
   >
   > 詳細設定を誤って編集すると、深刻な問題が発生することがあります。お客様の責任と判断の範囲で編集してください。

   a) Firefox を起動して、アドレスフィールドに **about:config** と入力して、［危険性を承知の上で使用する］を選択します。
   b) 検索ボックスに **ntlm** を入力します。
   c) 「network.automatic-ntlm-auth.trusted-uris」でダブルクリックして、Citrix Receiver for Windows または Windows 向け Citrix Workspace アプリサイトの URL をポップアップダイアログに入力します。
   d) ［**OK**］ をクリックします。

Citrix Gateway からのパススルー

ユーザーは Citrix 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。Citrix 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 Workspace アプリまたは Citrix Receiver for Web サイトを使用して、Citrix Gateway 経由でストアに接続できます。Citrix Gateway での StoreFront の構成について詳しくは、「Citrix Gateway 接続の追加」を参照してください。

StoreFront は、次の Citrix 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によって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 Citrix Gateway にログオンします。トークンコードと暗証番号（PIN）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：Citrix 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、Citrix 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、Citrix 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 Citrix 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、Citrix 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 Citrix 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 Citrix 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 Citrix 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。

Citrix 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 Workspace アプリ内からストアに直接接続できます。Citrix Gateway Plug-in をインストールできないリモートユーザーも、クライアントレスアクセスを使用してパススルー認証により Citrix Workspace アプリ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 Workspace アプリが必要です。

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 Citrix Gateway を構成する必要があります。ユーザーは Citrix 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、Citrix Gateway Plug-in を使用する必要があります。

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

Citrix 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 Citrix 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、Citrix 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 Citrix 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。

Citrix Gateway 展開環境でサポートされる場合は、SmartAccess 機能を使用して、Citrix Virtual Apps and Desktops リソースへのユーザーアクセスを Citrix 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、「Citrix Virtual Apps and Desktops での SmartAccess の機能」を参照してください。

スマートカード

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

スマートカードは、Citrix Virtual Apps and Desktops で提供されるデスクトップとアプリケーションのユーザー認証を StoreFront 経由で行うために使用できます。StoreFront に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。

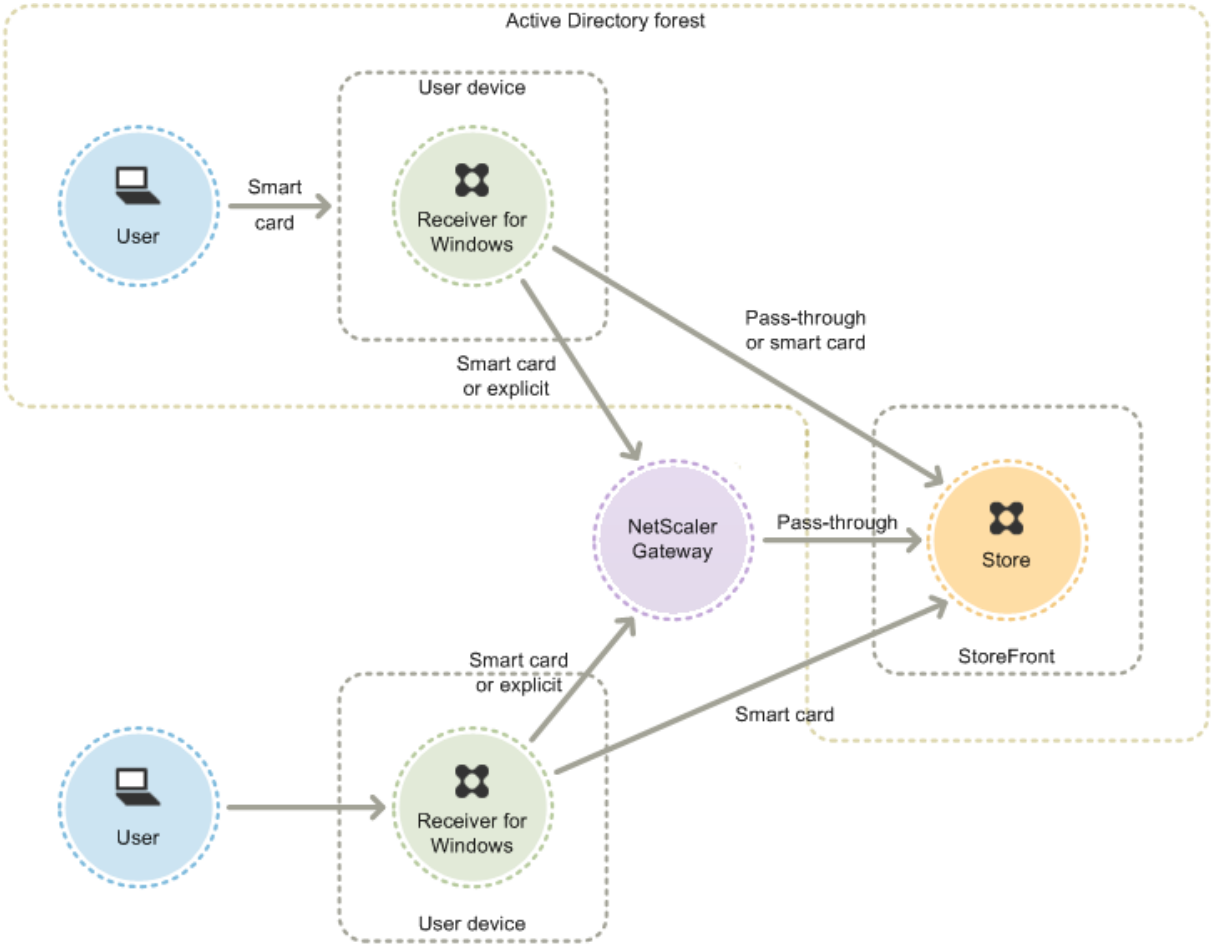
スマートカード認証を有効にする場合、StoreFront サーバーが属している Microsoft Active Directory ドメインか、そのドメインと直接の双方向の信頼関係が設定されているドメインのいずれかにユーザーのアカウントが属している必要があります。双方向の信頼関係を含んでいるマルチフォレスト展開環境がサポートされます。

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 または **Windows** 向け **Citrix Workspace** アプリでのスマートカードの使用

Citrix Receiver for Windows または Windows 向け Citrix Workspace アプリ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 Citrix 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 または Windows 向け Citrix Workspace アプリ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 または Windows 向け Citrix Workspace アプリ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 または Windows 向け Citrix Workspace アプリの認証を受けます。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 または Windows 向け Citrix Workspace アプリ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 Citrix 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、Citrix 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 Citrix Gateway に委任します。さらに Citrix Gateway 仮想サーバーを追加して、リソースへのユーザー接続がその Citrix 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 または Windows 向け Citrix Workspace アプリのパススルー認証も構成する必要があります。

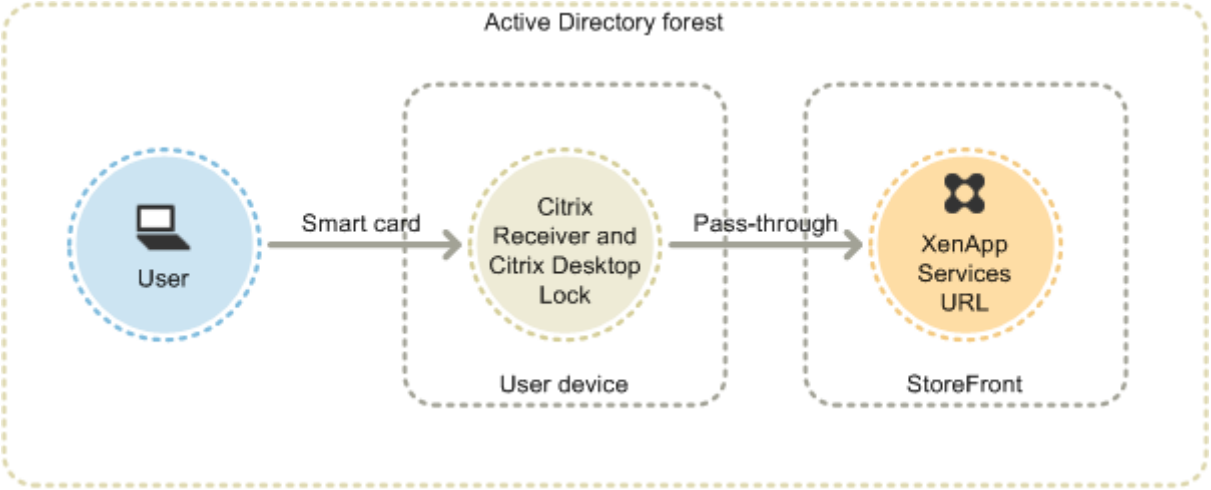
> 注:
>
> Citrix Receiver for Windows または Windows 向け Citrix Workspace アプリをお使いの場合、2 つ目の vServer をセットアップし、最適なゲートウェイルーティング機能を使用することで、アプリおよびデスクトップの起動時に PIN の入力を不要にすることができます。

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 Citrix Gateway にログオンできます。これにより、管理者はユーザーが Citrix 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、Citrix 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 Citrix Gateway に委任します。

XenApp Services サイトでのスマートカードの使用

Citrix Desktop Lock を実行している 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。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自動的に認証され、PIN を再入力する必要はありません。

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。

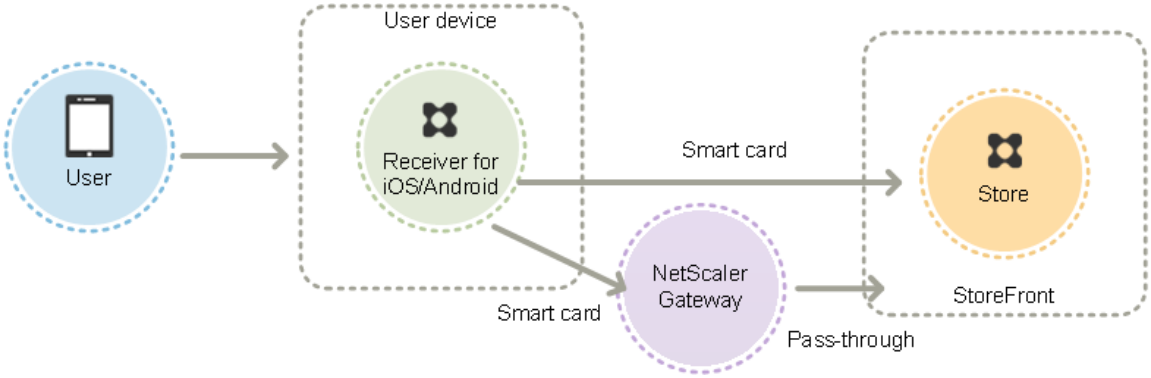
1. 左ペインで［Citrix Receiver for Web］ノードを選択します。
2. スマートカード認証を使用するサイトを選択します。
3. 右ペインで［認証方法の選択］を選択します。
4. ポップアップダイアログボックスでスマートカードのチェックボックスをオンにして、［OK］をクリックします。

ドメイン参加デバイスを使用する Citrix Receiver for Windows または Windows 向け Citrix Workspace アプリユーザーが Citrix Gateway を使用せずにストアにアクセスする場合、Citrix Virtual Apps and Desktops 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 または Windows 向け Citrix Workspace アプリユーザーが Citrix Gateway を使用してストアにアクセスする場合、Citrix Virtual Apps and Desktops 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。

iOS 向け **Citrix Workspace** アプリおよび **Android** 向け **Citrix Workspace** アプリでのスマートカードの使用

iOS 向け Citrix Workspace アプリおよび Android 向け Citrix Workspace アプリ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 Citrix 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 Workspace アプリに対しては、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 Citrix 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、Citrix 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 Citrix Gateway に委任します。さらに Citrix Gateway 仮想サーバーを追加して、リソースへのユーザー接続がその Citrix 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 Citrix 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、Citrix 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 Citrix 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 または **Linux** 向け **Citrix Workspace** アプリでのスマートカードの使用

Citrix Receiver for Linux または Linux 向け Citrix Workspace アプリ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 または Linux 向け Citrix Workspace アプリには入力済みの 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 または Windows 向け Citrix Workspace アプリ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、「スマートカード認証の構成」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、「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 または Linux 向け Citrix Workspace アプリの認証を受けます。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 または Linux 向け Citrix Workspace アプリ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 Citrix 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、Citrix 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 Citrix Gateway に

委任します。さらに Citrix Gateway 仮想サーバーを追加して、リソースへのユーザー接続がその Citrix 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 Citrix Gateway にログオンできます。これにより、管理者はユーザーが Citrix 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、Citrix 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 Citrix Gateway に委任します。

Citrix Receiver for Linux または Linux 向け Citrix Workspace アプリで 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 Workspace アプリ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 Virtual Apps and Desktops 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 Workspace アプリ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`」と入力します。
3. 「`Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True`」と入力します。
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 Citrix 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、Citrix 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ができますが、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 または Windows 向け Citrix Workspace アプリユーザーが Citrix Gateway を使用せずにストアにアクセスする場合、Citrix Virtual Apps and Desktops 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 または Windows 向け Citrix Workspace アプリユーザーが Citrix Gateway を使用してストアにアクセスする場合、Citrix Virtual Apps and Desktops 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 Citrix 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

April 2, 2020

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 Workspace アプリ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 HTML5 向け Citrix Workspace アプリ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 Workspace アプリで起動したリソースは、Citrix 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、Citrix Virtual Apps and Desktops 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の無効化」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。

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、「ユーザーに対するリソースの表示方式の構成」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。Citrix Virtual Desktops 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 Workspace アプリや 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

Citrix Virtual Apps and Desktops 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。Citrix Virtual Apps and Desktops で作成したフォルダーは、Citrix Workspace アプリでカテゴリとして表示されます。たとえば、アプリケーションを種類ごとにグループ化したり、組織内のユーザーの役割ごとにフォルダーを作成したりすることができます。
- 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 Workspace アプリに表示されます。
- 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 Workspace アプリ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 ［すべてのユーザーがアプリを **Citrix Receiver** または **Citrix Workspace** アプリで自動的に利用可能にする］ チェックボックスをオンにします。
- Citrix Virtual Apps and Desktops アプリケーションが Citrix Workspace アプリの［おすすめ］一覧に表示されることで、アプリケーションの宣伝になったり、ユーザーがそのアプリケーションを見つけやすくなったりします。これを行うには、アプリケーションの説明に「`KEYWORDS:Featured`」という文字列を追加します。

  > 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、Citrix Virtual Apps and Desktops でホストされる共有デスクトップがほかの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ると、Citrix Workspace アプリはユーザーを配信済みのアプリケーションにサブスクライブしますが、ショートカットは作成しません。この場合、サブスクライブしたアプリケーションを Citrix Workspace アプリで起動すると、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。
- Citrix Virtual Apps and Desktops では、ユーザーが公開デスクトップで公開アプリケーションを起動する場合、そのデスクトップセッションでアプリケーションを起動するのか、同じデリバリーグループ内の公開アプリケーションとして起動するのかを制御できます。制御には、Broker Service の PowerShell コマンドレットと Citrix Receiver for Windows（vPrefer）のポリシー設定を使用します。この機能は、公開アプリケーションを Citrix Receiver for Windows または Windows 向け Citrix Workspace アプリで起動する場合のみ有効です。公開アプリケーションが Web ブラウザーの StoreFront サイトから起動されている場合、この機能によってアプリケーションをローカルで起動することはできません。以前のリリースでは、「ダブルホップ」のアプリケーションの起動制御で、Studio の`KEYWORDS:Prefer`タグを使用する必要がありました。`KEYWORDS:Prefer`タグは、引き続き使用できます。KEYWORDS と vPrefer の両方の方法が構成されている場合、vPrefer が優先されます。

詳しくは、CTX232210、Citrix Virtual Apps and Desktops ドキュメントの「アプリケーション」、Citrix Receiver for Windowsドキュメントを参照してください。

StoreFront の高可用性とマルチサイト構成

August 29, 2019

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 Citrix Virtual Apps and Desktops 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、複数の Citrix Virtual Apps and Desktops の展開環境で配信されているデスクトップやアプリケーションがすべてストアで集約され、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。

Citrix Virtual Apps and Desktops 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 **Citrix Gateway** ルーティング

同一ストアの複数の展開環境で個別の Citrix 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 Citrix 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 Citrix 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 を経由するネットワークトラフィックを削減するため、展開環境ごとに最適な Citrix 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 Citrix 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 Citrix 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 Citrix 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 Citrix Gateway 経由である必要はありません。この場合、最適な Citrix 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 Citrix Gateway 経由ではなく、直接ルーティングされます。また、Citrix 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 Workspace アプリがネットワーク上の場所にかかわらず Citrix Gateway 経由でストアにアクセスするようにします。

Citrix Gateway のグローバルサーバー負荷分散

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、グローバルサーバー負荷分散用の Citrix 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 Citrix Gateway 仮想サーバーの IP アドレスになります。

Windows ネットワークの負荷分散については、「Citrix ADC 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 Workspace アプリ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

April 2, 2020

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 Citrix Virtual Apps and Desktops 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 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 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。

   Citrix ADC 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。Citrix ADC を使用した負荷分散の構成について詳しくは、「Citrix ADC による負荷分散」を参照してください。

   a) Citrix ADC 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。

   b) 必要に応じて、各 StoreFront サーバーについて個別の HTTP または SSL 負荷分散サービス（StoreFront モニター）を作成します。

   c) 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。

   d) 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。

   e) 仮想サーバーで、クライアント **IP** または **Cookie** 挿入のうちいずれかの方法を使用して永続性を構成します。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 の機能] > [.NET Framework]、[ASP.NET]

   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]

  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 のインストール。

   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 Workspace アプリはストアへの接続に HTTPS を必要とします。StoreFront で HTTPS ホストベース URL を使用できるように IIS を構成するには、デフォルトの Web サイトへの HTTPS バインドを作成し、それを StoreFront サーバー証明書にリンクします。HTTPS バインドを IIS サイトに追加する方法について詳しくは、「StoreFront 展開環境のセキュリティ」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

> 重要
>
> 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。

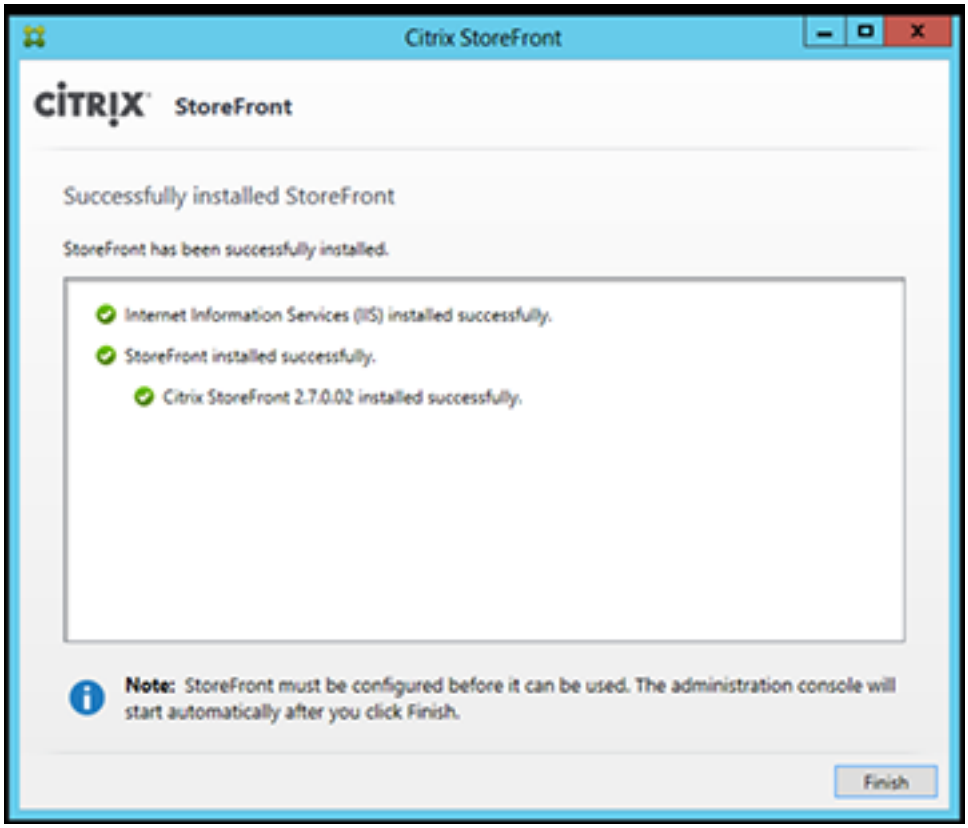
1. ダウンロードページからインストーラーをダウンロードします。
2. ローカルの管理者権限を持つアカウントで StoreFront サーバーにログオンします。
3. 必要な Microsoft .NET Framework がサーバー上にインストールされていることを確認します。
4. CitrixStoreFront-x64.exe を検索し、管理者として実行します。
5. ライセンス契約書を読み、同意することを選択して、［次へ］ をクリックします。
6. ［必須条件の確認］ページが開いた場合は、［次へ］ をクリックします。
7. ［インストールの開始］ページで、インストール対象の必須条件および 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］
   - ［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 の機能］> ［.NET Framework］、［ASP.NET］
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。

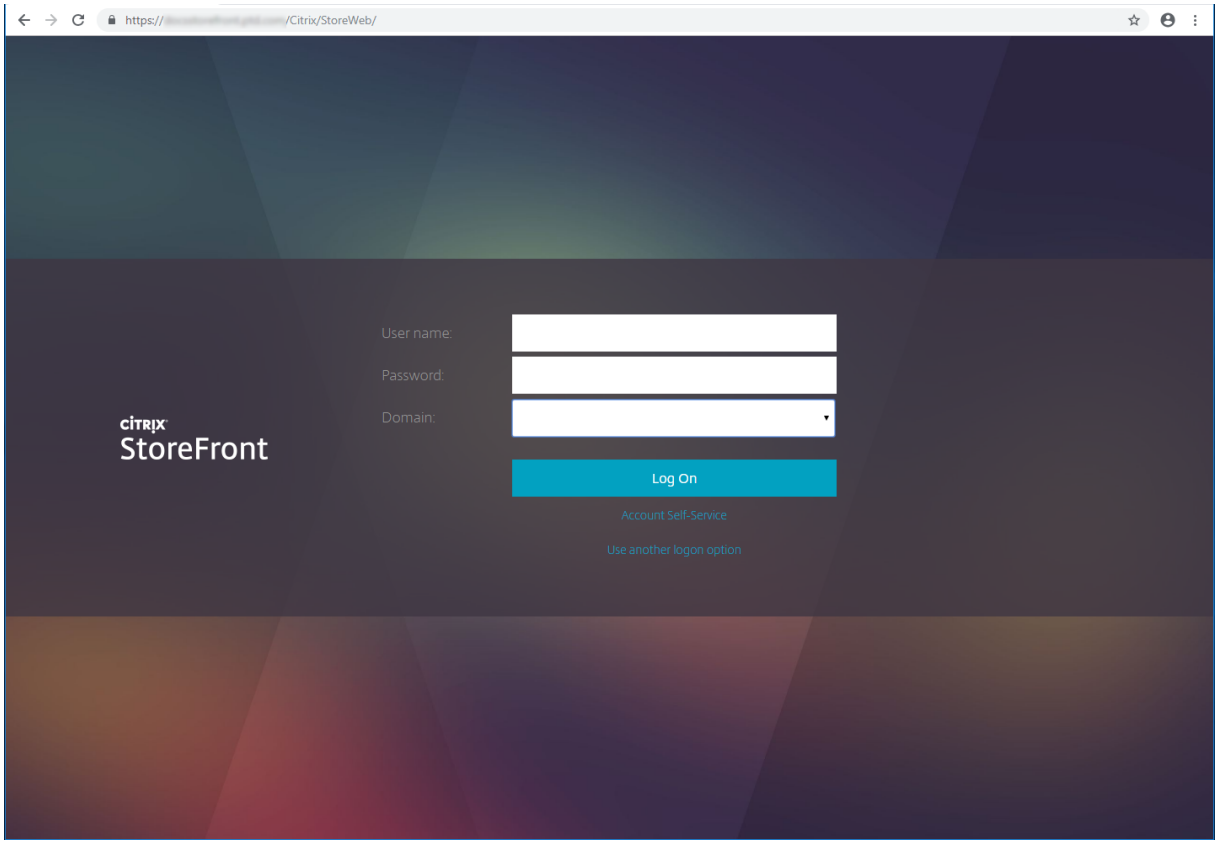
   a)［ベース **URL**］ ボックスで StoreFront サーバーの URL を指定します。
   b)［ストア名］ ページで、ストアの名前を指定して、［次へ］ をクリックします。

［**Delivery Controllers**］ ページで、ストアで使用できるようにするリソースを提供する Citrix Virtual Apps and Desktops 展開環境の詳細を入力します。

1.［トランスポートの種類］ および ［ポート］ を設定し（HTTP とポート 80、または HTTPS とポート 443 など）、［**OK**］ をクリックします。
2.［リモートアクセス］ ページで［なし］を選択します。Citrix 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。
3.［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。例: `example.net/Citrix/StoreWeb/`。ログオンして、Citrix Workspace アプリの新しいユーザーインターフェイスにアクセスします。



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、StoreFront のインストール要件が満たされていることを確認します。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。
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が含まれるフォルダーに移動して、次のコマンドを実行します:

```
CitrixStoreFront-x64.exe [-silent] [-INSTALLDIR
    installationlocation] [-WINDOWS_CLIENT filelocation\filename.
    exe] [-MAC_CLIENT filelocation\filename.dmg]
```

StoreFront とその前提条件のサイレントインストールを実行するには、**-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ります。

デフォルトでは、Citrix Receiver for Web サイトが Windows または Mac OS X デバイスの Citrix Workspace アプリを検出できない場合、プラットフォームに適した Citrix Workspace アプリをシトリックスの Web サイトからダウンロードしてインストールするようメッセージが表示されます。この動作を変更して、Citrix Workspace アプリ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、「ユーザーに対するリソースの表示方式の構成」を参照してください。

この構成を変更する場合は、**-WINDOWS_CLIENT** および **-MAC_CLIENT** 引数を指定して、Citrix Receiver for Windows または Windows 向け Citrix Workspace アプリ、および Citrix Receiver for Mac または Mac 向け Citrix Workspace アプリのインストールファイルをそれぞれ StoreFront 展開の適切な場所にコピーします。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* はインストールファイルの名前を示します。Citrix Receiver for Windows または Windows 向け Citrix Workspace アプリ、Citrix Receiver for Mac または Mac 向け Citrix Workspace アプリのインストールファイルは、Citrix Virtual Apps and Desktops のインストールメディアに含まれています。

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。StoreFront 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。StoreFront の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。StoreFront のアップグレード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、シトリックス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。

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）:

```
Location: HKLM:\Software\Citrix\Telemetry\CEIP
Name: Enabled
Type: REG_DWORD
Value: 0 = disabled, 1 = enabled
```

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 が有効にされているかどうか（True または False）を示す文字列。
Citrix Receiver for Web の HTML 5 設定	各 Receiver for Web サイトの HTML5 Receiver 設定（Always、Fallback、または Off）を示す文字列の一覧。
Citrix Receiver/Citrix Workspace アプリ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（True または False）を示すブール値の一覧。
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」が有効にされているかどうか（ENABLED または DISABLED）を示す文字列の一覧。
ゲートウェイ数	展開環境で構成されている Citrix Gateway の数を表すカウンター。

Citrix Analytics Service

Citrix Cloud をご利用中でオンプレミスの StoreFront 展開環境をお持ちの場合、データが Citrix Cloud の Citrix Analytics Service に送信されるように StoreFront を構成できます。構成後は、Citrix Workspace アプリ（およ

び HTML5 対応 Web ブラウザーからアクセスする Citrix Receiver for Web サイト）から送信されたユーザーイベントを Citrix Analytics が処理します。Citrix Analytics は、ユーザー、アプリケーション、エンドポイント、ネットワーク、データに関する測定値を集約して、ユーザーの行動に関する包括的な識見を提供します。Citrix Analytics のドキュメントでこの機能について確認するには、「StoreFront を使用した Virtual Apps and Desktops サイトへのオンボード」を参照してください。

この機能を構成するには、以下を実行します：

- Citrix Analytics から構成ファイルをダウンロードします。
- Citrix Analytics データを PowerShell を使用してオンプレミスの StoreFront 展開にインポートします。

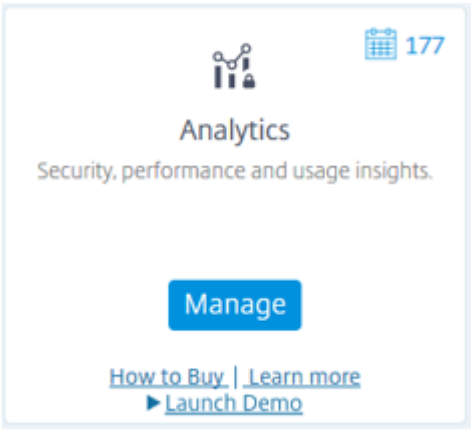
StoreFront の構成後は、Citrix Analytics Service が要求した時に Citrix Workspace アプリが StoreFront のストアからデータを送信できます。

> 重要：
>
> この機能が正しく動作し、Citrix Cloud サービスを消費するには、使用中の StoreFront 展開がポート 443 の次のアドレスと通信できるようにする必要があります：
>
> - `https://*.cloud.com`
> - `https://*.citrixdata.com`

Citrix Analytics から構成ファイルをダウンロードする

> 重要：
>
> 初期構成には、機密情報を含む構成ファイルが必要です。ダウンロード後はファイルを安全に保管してください。このファイルを組織外の人と共有しないでください。構成後、このファイルは削除できます。別のマシンに構成を再適用する必要がある場合は、Citrix Analytics Service 管理コンソールからファイルを再度ダウンロードできます。

1. 管理者アカウントで Citrix Cloud（`https://citrix.cloud.com/`）にログオンします。
2. Citrix Cloud の顧客を選択します。
3. ［管理］をクリックして、Citrix Analytics Service 管理コンソールを開きます。



4. Citrix Analytics Service 管理コンソールで、［**Settings**］**>**［**Data Sources**］を選択します。
5. Virtual App and Desktops カードで、（⊠）メニューアイコン、［**Connect StoreFront deployment**］の順に選択します。
6. ［Connect StoreFront Deployment］ページで ［**Download File**］ を選択して *StoreFrontConfigurationFile.json* ファイルをダウロードします。

構成ファイルの例

```
{

  ”customerId”: ”<yourcloudcustomer>”,
  ”enablementService”: ” https://api.analytics.cloud.com /casvc/<
     yourcloudcustomer>/ctxana/v1/cas/<yourcloudcustomer>/XenDesktop/<
     deviceid>/dsconfigdata”,
  ”cwsServiceKey”: ”PFJTPn …… .. T4=”,
  ”enablementServiceStatus”: ” https://api.analytics.cloud.com /casvc/<
     yourcloudcustomer>/ctxana/v1/cas/storefront/config”,
  ”instanceId”: ”d98f21d0-56e0-11e9-ba52-5136d90862fe”,
  ”name”: ”CASSingleTenant”
 }
```

各項目の意味は次のとおりです。

customerId は、最新の Citrix Cloud の顧客用の一意の ID です。

cwsServiceKey は、最新の Citrix Cloud の顧客を特定する一意のキーです。

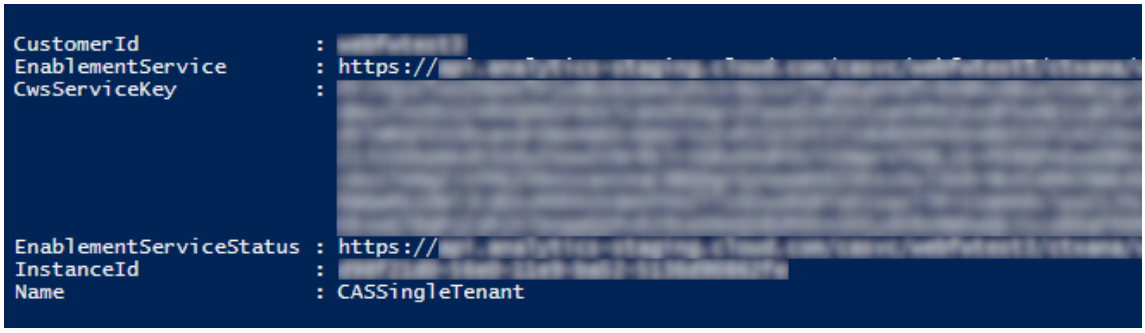
instanceID は、Citrix Workspace アプリから Citrix Analytics に対して送信された要求に署名（セキュリティ保護済み）するために生成された ID です。複数の StoreFront サーバーまたはサーバーグループを Citrix Cloud に登録すると、それぞれに一意の instanceID が割り当てられます。

Citrix Analytics データを **StoreFront** 展開にインポートする

1. *StoreFrontConfigurationFile.json* ファイルをオンプレミスの StoreFront サーバー（または StoreFront サーバーグループのいずれかのサーバー）の適切なフォルダーにコピーします。以下のコマンドは、ファイルがデスクトップに保存されている場合です。
2. PowerShell ISE を開き、［管理者として実行］ を選択します。
3. 次のコマンドを実行します：

```
Import-STFCasConfiguration -Path ”$Env:UserProfile\Desktop\
   StoreFrontConfigurationFile.json”
Get-STFCasConfiguration
```


4. このコマンドはインポートされたデータのコピーを返し、それを PowerShell コンソールに表示します。



> 注:
>
> Windows Server 2012 R2 にインストールされているオンプレミス StoreFront サーバーでは、C++ ランタイムソフトウェアコンポーネントを手動でインストールして CAS に登録できるようにする必要があります。Citrix Virtual Apps and Desktops のインストール中に StoreFront がインストールされる場合、CVAD メタインストーラーが C++ ランタイムコンポーネントをインストールするため、この手順は不要です。C++ ランタイムのない CitrixStoreFront-x64.exe メタインストーラーで StoreFront がインストールされている場合、CAS 構成ファイルのインポート後、Citrix Cloud への登録に失敗する場合があります。

Citrix Analytics のデータを **StoreFront** サーバーグループに伝達する

StoreFront サーバーグループでこれらの操作を実行している場合は、インポートされた Citrix Analytics データをサーバーグループの全メンバーに伝達する必要があります。この手順は、単一の StoreFront サーバー展開では必要ありません。

データを伝達するには、以下のいずれかの方法を使用します:

- StoreFront 管理コンソールを使用します。
- PowerShell コマンドレット **Publish-STFServerGroupConfiguration** を使用します。

StoreFront サーバーグループ **ID** を確認する

Citrix Analytics Service に正常に登録されたかどうかを確認するには、PowerShell を使用して展開の Server-GroupID を検出します。

1. StoreFront サーバー、またはサーバーグループ内の 1 台の StoreFront サーバーにログオンします。
2. PowerShell ISE を開き、［管理者として実行］ を選択します。
3. 次のコマンドを実行します:

```
1 $WebConfigPath = ”C:\Program Files\Citrix\Receiver StoreFront\
     Framework\FrameworkData\Framework.xml”
2 $XMLObject = (Get-Content $WebConfigPath) -as [Xml]
3 $XMLObject.framework.properties.property
```


たとえば、これらのコマンドは次のような出力結果を生成します:

```
name value
---- -----
ClusterId 8b8ff5c8-44ba-46e4-87f0-2df8cff31432
HostBaseUrl https://storefront.example.com/
SelectedIISWebSiteId 1
AdminConsoleOperationMode Full
```

StoreFront から **Citrix Analytics** へのデータの送信を停止する

1. PowerShell ISE を開き、［管理者として実行］ を選択します。
2. 次のコマンドを実行します:

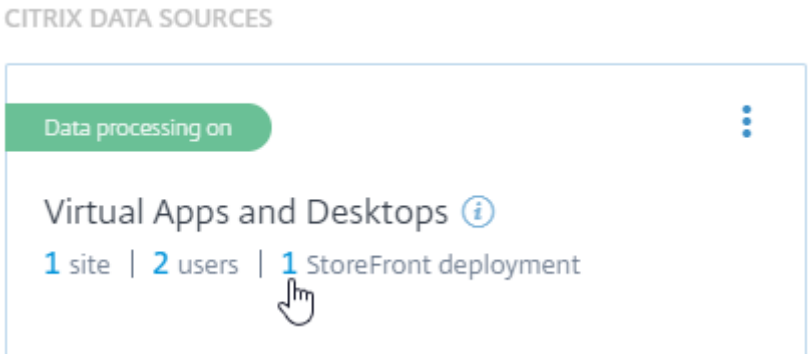
   ```
   Remove-STFCasConfiguration
   ```

   ```
   Get-STFCasConfiguration
   ```

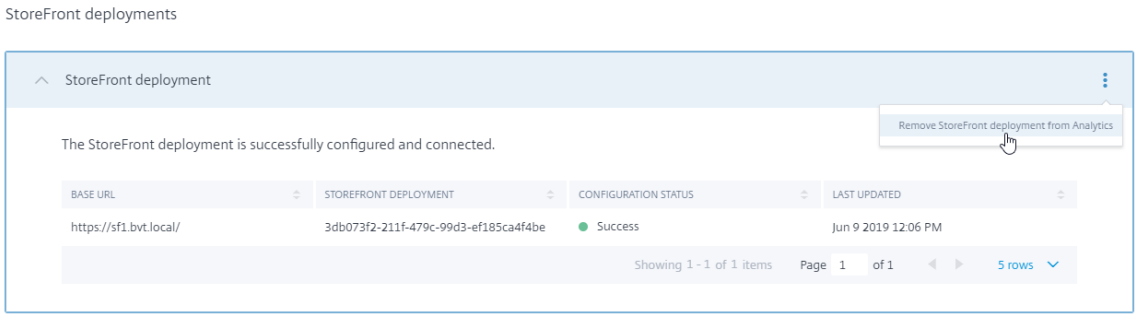
   以前にインポートされた Citrix Analytics データの削除に成功した場合、**Get-STFCasConfiguration** は値を返しません。
3. StoreFront サーバーグループでこれらの操作を実行している場合は、変更を伝達し、インポートされた Citrix Analytics データをサーバーグループの全メンバーから削除する必要があります。サーバーグループ内の 1 台のサーバーで、次のコマンドを実行します:

   ```
   Publish-STFServerGroupConfiguration
   ```
4. 他のサーバーグループメンバーで次のコマンドを実行して、Citrix Analytics 構成がグループ内のすべてのサーバーから正常に削除されたことを確認します:

   ```
   Get-STFCasConfiguration
   ```
5. 管理者アカウントで Citrix Cloud（https://citrix.cloud.com/）にログオンします。
6. Citrix Cloud の顧客を選択します。
7. ［管理］をクリックして、Citrix Analytics Service 管理コンソールを開きます。
8. Citrix Analytics Service 管理コンソールで、［**Settings**］**>**［**Data Sources**］ を選択します。
9. Virtual App and Desktops カードで、StoreFront の展開数を選択します:



10. ホストベース URL および ServerGroupID を参照して削除対象の StoreFront 展開を特定します。
11. （⊠）メニューで、［**Remove StoreFront deployment from Analytics**］ を選択します。



> 注:
>
> サーバー側で構成を削除する一方、Citrix Analytics からは削除しない場合、StoreFront 展開のエントリは Citrix Analytics に残るものの、StoreFront からはデータを受信しません。Citrix Analytics からのみ構成を削除する場合、StoreFront 展開のエントリは次回のアプリプールの再利用時（IIS のリセット時、または自動で 24 時間ごと）に再度追加されます。

Web プロキシを使用して **Citrix Cloud** に接続し、**Citrix Analytics** に登録するように **StoreFront** を構成する

StoreFront が Web プロキシの背後のホスト Web サーバーに配置されている場合、Citrix Analytics への登録は失敗します。StoreFront 管理者が Citrix 展開で HTTP プロキシを使用する場合、インターネットへの StoreFront トラフィックはクラウド内の Citrix Analytics に到達する前に Web プロキシを通過する必要があります。StoreFront は、ホスト OS のプロキシ設定を自動的に使用しません。Web プロキシを介してトラフィックを送信するようストアに指示するには、さらに構成が必要です。ストアの web.config ファイルに新しいセクションを追加して<system.net>プロキシ設定を構成できます。Citrix Analytics へのデータ送信に使用される StoreFront サーバー上のすべてのストアに対してこれを実行します。

方法 **1**: **Powershell** で **1** つまたは複数のストアでプロキシ構成を設定する（推奨）

Powershell スクリプト Config-StoreProxy.ps1 を実行すると、1 つまたは複数のストアでこのプロセスを自動化し、<system.net>を構成する有効な XML が自動的に挿入されます。また、このスクリプトは現在のユーザーの

デスクトップにストアの web.config ファイルのバックアップを作成し、必要な場合変更されていない web.config ファイルを復元できるようにします。

> 注:
>
> スクリプトを複数回実行すると、複数の<system.net>XML のコピーが追加されます。ストアごとに<system.net>のエントリは 1 つのみにする必要があります。複数のコピーを追加すると、ストアのプロキシ構成が正しく機能しなくなります。

1. PowerShell ISE を開き、［管理者として実行］ を選択します。
2. $Stores = @(”Store”,”Store2”)を設定して Web プロキシで構成するストアを含めます。
3. 次のいずれかを指定します:
   - IP アドレス、または
   - Web プロキシの FQDN
4. 次の PowerShell を実行します:

```
$Stores = @(”Store”,”Store2”)
$ProxyIP = ”10.0.0.1”
$ProxyFQDN = ”proxyserver.example.com”
$ProxyPort = 8888

# Set this for every Store using Stores array
function Set-StoreProxyServer() # Tested with both IP and FQDN
{

    [CmdletBinding()]
    param([Parameter(Mandatory=$true,ParameterSetName=”ProxyIP”)][
        Parameter(Mandatory=$true,ParameterSetName=”ProxyFQDN”)][
        array]$Stores,
         [Parameter(Mandatory=$true,ParameterSetName=”ProxyIP”)][
            string]$ProxyIP,
         [Parameter(Mandatory=$true,ParameterSetName=”ProxyFQDN”)][
            string]$ProxyFQDN,
         [Parameter(Mandatory=$true,ParameterSetName=”ProxyIP”)][
            Parameter(Mandatory=$true,ParameterSetName=”ProxyFQDN”)
            ][int]$ProxyPort)

    foreach($Store in $Stores)
    {

        Write-Host ”Backing up the Store web.config file for store
             $Store before making changes...” -ForegroundColor ”
            Yellow”
         Write-Host ”‘n”
```

```
21
22          if(!(Test-Path "$env:UserProfile\desktop$Store"))
23          {
24
25              Write-Host "Creating $env:UserProfile\desktop$Store\
                    directory for backup..." -ForegroundColor "Yellow"
26              New-Item -Path "$env:UserProfile\desktop$Store" -
                    ItemType "Directory" | Out-Null
27              Write-Host "`n"
28           }
29
30
31          Write-Host "Copying c:\inetpub\wwwroot\Citrix$Store\web.
                config to $env:UserProfile\desktop$Store..." -
                ForegroundColor "Yellow"
32          Copy-Item -Path "c:\inetpub\wwwroot\Citrix$Store\web.
                config" -Destination "$env:UserProfile\desktop$Store" -
                Force | Out-Null
33
34          if(Test-Path "$env:UserProfile\desktop$Store\web.config")
35          {
36
37              Write-Host "$env:UserProfile\desktop$Store\web.config
                    file backed up" -ForegroundColor "Green"
38           }
39
40          else
41          {
42
43              Write-Host "$env:UserProfile\desktop$Store\web.config
                    file NOT found!" -ForegroundColor "Red"
44           }
45
46          Write-Host "`n"
47
48          Write-Host "Setting the proxy server to $ProxyAddress for
                Store $Store..." -ForegroundColor "Yellow"
49          Write-Host "`n"
50
51          $StoreConfigPath = "c:\inetpub\wwwroot\Citrix$Store\web.
                config"
52          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
53
54          if([string]::IsNullOrEmpty($ProxyFQDN))
55          {
```

```
56
57              $ProxyServer = ("HTTP://$ProxyIP"+":"+$ProxyPort)
58           }
59
60          else
61          {
62
63              $ProxyServer = ("HTTP://$ProxyFQDN"+":"+$ProxyPort)
64           }
65
66
67          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
68
69          # Create 3 elements
70          $SystemNet = $XMLObject.CreateNode("element","system.net",
                "")
71          $DefaultProxy = $XMLObject.CreateNode("element","
                defaultProxy","")
72          $Proxy = $XMLObject.CreateNode("element","proxy","")
73          $Proxy.SetAttribute("proxyaddress","$ProxyServer")
74          $Proxy.SetAttribute("bypassonlocal","true")
75
76          # Move back up the XML tree appending new child items in
                reverse order
77          $DefaultProxy.AppendChild($Proxy)
78          $SystemNet.AppendChild($DefaultProxy)
79          $XMLObject.configuration.AppendChild($SystemNet)
80
81          # Save the modified XML document to disk
82          $XMLObject.Save($StoreConfigPath)
83
84          Write-Host "Getting the proxy configuration for c:\inetpub
                \wwwroot\Citrix$Store..." -ForegroundColor "Yellow"
85          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
86          $ConfiguredProxyServer = $XMLObject.configuration.'system.
                net'.defaultProxy.proxy.proxyaddress | Out-Null
87          Write-Host ("Configured proxy server for Store $Store"+":
                "+ $ConfiguredProxyServer) -ForegroundColor "Green"
88          Write-Host "`n"
89       }
90
91      Write-Host "Restarting IIS..." -ForegroundColor "Yellow"
92      IISReset /RESTART
93  }
94
```

```
95
96 Set-StoreProxyServer -Stores $Stores -ProxyFQDN $ProxyFQDN -
       ProxyPort $ProxyPort
97 # OR
98 Set-StoreProxyServer -Stores $Stores -ProxyIP $ProxyIP -ProxyPort
       $ProxyPort
```

5. C:\inetpub\wwwroot\Citrix< Store>\web.config で web.config ファイルの最後に新しい<system.net>セクションが含まれていることを確認します。

```
1          </dependentAssembly>
2      </assemblyBinding>
3  </runtime>
4  <system.net>
5      <defaultProxy>
6      <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
           bypassonlocal="true" />
7      </defaultProxy>
8  </system.net>
9  </configuration>
```

6. 「Citrix Analytics データを StoreFront 展開にインポートする」の手順で、Citrix Analytics データをインポートします。

方法 **2**: 手動で **<system.net>** セクションをストアの **web.config** ファイルに追加する

これは、Citrix Analytics にデータを送信するために使用される StoreFront サーバー上のすべてのストアに対して実行する必要があります。

1. ストアの web.config ファイルのバックアップを作成し、C:\inetpub\wwwroot\Citrix< Store>\web.config 以外の別の場所にコピーします。
2. FQDN とポート番号の組み合わせか IP とポート番号の組み合わせを使用して、以下の XML でプロキシ設定を編集します。

   たとえば、FQDN とポート番号の組み合わせでは、以下のような<system.net>要素を使用します:

```
1  <system.net>
2      <defaultProxy>
3      <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
           bypassonlocal="true" />
4      </defaultProxy>
5  </system.net>
```

   たとえば、IP とポート番号の組み合わせでは、以下のような<system.net>要素を使用します:


```
<system.net>
    <defaultProxy>
    <proxy proxyaddress="HTTP://10.0.0.1:8888" bypassonlocal="true
        " />
    </defaultProxy>
</system.net>
```

3. ストアの web.config ファイルの最後に、以下のように適切な<system.net>要素を挿入します:

```
<runtime>
<gcServer enabled="true" />
<assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
    <dependentAssembly>
    <assemblyIdentity name="System.Web.MVC" publicKeyToken="31
        BF3856AD364E35" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-5.0.0.0" newVersion="
        5.0.0.0" />
    </dependentAssembly>
    <dependentAssembly>
    <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30
        ad4fe6b2a6aeed" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-9.0.0.0" newVersion="
        9.0.0.0" />
    </dependentAssembly>
</assemblyBinding>
</runtime>

Insert the <system.net> element here

</configuration>
```

4. 「Citrix Analytics データを StoreFront 展開にインポートする」の手順で、Citrix Analytics データをインポートします。

StoreFront のアップグレード

> 警告:
>
> StoreFront 1912 にアップグレードすると、展開内のデスクトップアプライアンスサイトは自動的に削除されます。デスクトップアプライアンスサイトを保持する必要がある場合は、アップグレードしないでください。代わりに、ドメイン不参加のユースケースではCitrix Workspace アプリ Desktop Lockを使用することをお勧めします。

アップグレードする場合、StoreFront 構成が保存され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。一方、StoreFront のアンインストールは StoreFront および関連サービス、サイト、アプリケーションサブスクリプションデータ（スタンドアロンサーバーの場合）、関連構成を削除します。

ヒント

- 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。
- 製品終了（EOL）になった古い StoreFront の最新リリースから最近の最新リリースへのアップグレードはサポートされていません。詳しくは、「CTX200356」を参照してください。
- StoreFront では、複数の製品バージョンが混在する複数サーバーの展開環境がサポートされないため、サーバー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、ユーザーが展開環境にアクセスできるようにしてください。
- StoreFront は、異なるサーバー OS を含む複数のサーバー展開環境をサポートしていないため、サーバーグループ内のすべてのサーバーは同じ Windows Server OS 上で実行されている必要があります。
- 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。
- 従来のユーザーエクスペリエンスを使用しているすべてのストアは、このバージョンの StoreFront にアップグレードすると、統合エクスペリエンスを使用するように更新されます。「統合ユーザーエクスペリエンス」で説明されている、アップグレードによって導入される新しいエクスペリエンスについてユーザーに周知することをお勧めします。統合エクスペリエンスがカスタマイズされている場合、このバージョンの StoreFront にアップグレード後もカスタマイズした内容は保持されます。カスタマイズした外観が新しい統合エクスペリエンスに最適か確認してください。
- StoreFront のアップグレードを実行する前に、アップグレード前チェックを実行します。アップグレード前チェックが失敗した場合、アップグレードは開始されず、エラーに関する通知が表示されます。StoreFront のインストールは変更されません。エラーの原因を修復してから、アップグレードに戻ります。
- StoreFront のアップグレード自体が失敗すると、既存の StoreFront のインストールで初期構成が失われる可能性があります。StoreFront のインストールを機能する状態に復元してから、アップグレードを再度実行してください。StoreFront を機能する状態に復元するには、次の方法を検討してください：
  - アップグレード前に作成した仮想マシンスナップショットを復元する、
  - アップグレード前にエクスポートした StoreFront 構成をインポートする（StoreFront 構成のエクスポートとインポートを参照）、
  - 「StoreFront のアップグレードの問題に関するトラブルシューティング」のトラブルシューティング方法を実行する。
- Citrix Virtual Apps and Desktops Metainstaller で StoreFront のアップグレードが失敗した場合、ダイアログで報告され関連するエラーログへのリンクが記載されます。

アップグレードの準備

アップグレードを開始する前に、アップグレードの失敗を防ぐために次の手順の実行をお勧めします:

- アップグレード前にバックアップを計画します。
- 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。
- StoreFront 管理コンソールを閉じます。
- すべてのコマンドラインおよび PowerShell 画面を終了します。
- すべての StoreFront 関連のフォルダー(C:\inetpub\wwwroot\Citrix\Store、C:\inetpub\wwwroot\Citrix\StoreWeb など）を閉じます。これにより、Windows エクスプローラーがフォルダーに排他的ロックをかけることを防ぎます。
- サーバーをアップグレードする前にサーバーを再起動して、StoreFront のファイルまたはフォルダーに排他的ロックかかってないことを確認します（Windows エクスプローラーのすべてのインスタンスを閉じるなど、エクスプローラープロセスを再起動するだけでは十分ではありません)。
- サーバー上の他のプログラムを起動せずに、すぐにアップグレードを実行します。
- 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、サーバーをアップグレードします。

スタンドアロンの **StoreFront** サーバーのアップグレード

1. 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ます。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。インストーラーがファイルにアクセスできない場合、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。
2. 仮想マシンスナップショットを作成してサーバーのバックアップを作成します。
3. 既存の StoreFront 構成をエクスポートします（推奨)。
4. このバージョンの StoreFront 用のインストールファイルを実行します。

StoreFront サーバーグループをアップグレードするには

StoreFront サーバーグループのアップグレードでは、いずれかのサーバーを使用して他のサーバーをグループから削除します。削除されたサーバーは、グループに関連する構成を保持しているため、新しいサーバーグループに参加できなくなります。新しいサーバーグループを構築するために再利用する前に、またはスタンドアロンの StoreFront サーバーとして再利用する前に、削除されたサーバーを出荷時のデフォルト設定にリセットするか、または StoreFront に再インストールする必要があります。

サーバーグループをアップグレードする前に、以下を実行します:

- 仮想マシンスナップショットを作成してグループのすべてのサーバーのバックアップを作成します。これにより、アップグレードが計画どおりに行われない場合は、機能している 3 ノードのサーバーグループに簡単に戻すことができます。

- 既存の StoreFront 構成をエクスポートします（推奨）。1 台のサーバーからサーバーグループ構成のみをエクスポートします。サーバー間ですべての変更を伝達していることを前提としているため、サーバーグループ内のすべてのサーバーは同一コピーの構成を維持します。このバックアップにより、簡単に新しいサーバーグループを構築できます。

例 **1**：スケジュールされたメンテナンスダウンタイム中に **3** ノードの **StoreFront** サーバーグループをアップグレードします

スケジュールされたダウンタイム中に、3 台のサーバー A、B、C による StoreFront サーバーグループをアップグレードします。

1. 負荷分散 URL を無効にして、サーバーグループへのユーザーアクセスを無効にします。これにより、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 A を使用して、サーバー B と C をグループから削除します。

   サーバー B と C は、サーバーグループから「孤立」しています。
3. このバージョンの StoreFront のインストールファイルを実行してサーバー A をアップグレードします。
4. サーバー A が正常にアップグレードされたことを確認してください。
5. サーバー B と C で、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。
6. アップグレードされたサーバーグループを作成するために、アップグレードされたサーバー A にサーバー B と C を参加させます。このサーバーグループは、アップグレードされた 1 台のサーバー（A）と 2 台の新しくインストールされたサーバー（B と C）で構成されています。

   既存のサーバーグループへの参加プロセスは自動的にすべての構成データとサブスクリプションデータを新しいサーバー B と C に伝達します。
7. すべてのサーバーが正しく機能していることを確認してください。
8. 負荷分散 URL を有効にして、アップグレードされたサーバーグループへのユーザーアクセスを有効にします。

例 **2**：スケジュールされたダウンタイムなしで **3** ノードの **StoreFront** サーバーグループをアップグレードします

スケジュールされたダウンタイムなしで、3 台のサーバー A、B、C による StoreFront サーバーグループをアップグレードします。

サーバーグループをアップグレードする前に、以下を実行します：

1. **Export-STFStoreSubscriptions** を使用してサーバー A からサブスクリプションデータをエクスポートします。このバックアップは、サーバーがプロセスの後半で工場出荷時設定にリセットされ、サブスクリプションデータと構成データが削除されるため、必要になります。「ストアのサブスクリプションデータの管理」を参照してください。

2. サーバー C に関連した負荷分散サービスを無効にしてサーバー C へのユーザーアクセスを無効にします。これによって、ユーザーはアップグレードプロセス中サーバー C に接続できなくなります。サーバー A と B に関連した負荷分散サービスを有効にして、ユーザーがそれらのサーバーを引き続き使用できるようにします。
3. グループからサーバー C を削除するには、サーバー A を使用します。
   サーバー A と B は、引き続きユーザーのリソースへのアクセスを提供します。サーバー C はサーバーグループから孤立し、工場出荷時設定にリセットされました。
4. **Clear-STFDeployment** を使用して孤立したサーバー C を出荷時のデフォルト設定にリセットします。
5. **Import-STFConfiguration** を使用して、以前にサーバー C にエクスポートしたことがあるStoreFront 構成をインポートします。
6. このバージョンの StoreFront のインストールファイルを実行してサーバー C をアップグレードします。これで、サーバー C は以前のサーバーグループと同じ構成になり、新しいバージョンの StoreFront にアップグレードされます。
7. 以前にサーバー C にエクスポートしたサブスクリプションデータをインポートします。後からこの手順を繰り返す必要はありません。必要なのはサーバー 1 台分のサブスクリプションデータのコピーであり、グループに参加しているその他のサーバーにはデータが伝達されます。
8. サーバー B を使用して手順 2 ～ 6 を繰り返します。この間、ユーザーはサーバー A のリソースにのみアクセスできます。そのためこの手順は、StoreFront サーバーグループの負荷が最小になると予想される、作業の少ない期間に実行するのが最適です。
9. 既存のサーバーグループへの参加プロセスを使用してサーバー B をサーバー C に参加させます。これにより、StoreFront の現在のバージョンで単一サーバー（サーバー A）を、StoreFront の新しいバージョンで新しい 2 ノードサーバーグループ（サーバー B および C）を展開できます。
10. サーバー B と C の両方で負荷分散サービスを有効にして、サーバー A から引き継ぐことができるようにします。
11. ユーザーが新しくアップグレードされたサーバー B および C に接続されるように、サーバー A の負荷分散サービスを無効にします。
12. サーバー A を使用して手順 2 ～ 6 を繰り返します。
    サーバーグループのアップグレードプロセスが完了すると、サーバー A、B、C には、元のグループと同じ構成およびサブスクリプションデータが配置されます。

> 注:
>
> サーバー A が唯一アクセス可能なサーバーである短い期間中に、サブスクリプションが失われる可能性があります（手順 9）。これによって、アップグレード後の新しいサーバーグループに存在するサブスクリプションデータベースが比較的古いものになり、新しいサブスクリプションレコードはすべて失われる可能性があります。
>
> サブスクリプションデータはユーザーがログオンしてリソースを起動できるようにするために不可欠な要素ではないため、これによる機能への影響はありません。ただし、サーバー A が工場出荷時の設定にリセットされ、新しくアップグレードされたグループに参加した後で、ユーザーはリソースを再度サブスクライブする必要が

> あります。ダウンタイムなしで StoreFront 実稼働環境をライブでアップグレードすると、多数ではないものの、いくつかのサブスクリプションレコードが失われる可能性があります。

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。

- 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。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。サーバーグループに 6 台を超えるサーバーを追加することはお勧めしません。

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、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. StoreFront 管理コンソールが開いている場合は閉じます。
3. PowerShell SDK を使用して StoreFront の管理に使用されている可能性のある PowerShell セッションをすべて閉じます。
4. 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。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。
5. ［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。
6. ［**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

April 2, 2020

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。
4. ［次へ］ をクリックしてユーザーを Microsoft Active Directory に認証する認証サービスをセットアップします。

   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 Workspace アプリ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 Workspace アプリ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. ［**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。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、「ストアに Citrix Virtual Apps and Desktops リソースを追加する」の手順に従います。Citrix Virtual Apps and Desktops 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。
7. 必要なリソースをすべてストアに追加したら、［**Delivery 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、パブリック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。

- Citrix 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。ユーザーは ICAProxy またはクライアントレス VPN（cVPN）を使用して Citrix Gateway にログオンするため、Citrix Gateway Plug-in を使用して完全 VPN を確立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（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に Citrix 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 ［**PCitrix 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 Citrix 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。

9. リモートアクセスを有効にした場合、［**Citrix Gateway** アプライアンス］には、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が一覧表示されます。この一覧に Citrix Gateway の展開環境を追加するには、「Citrix 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。展開環境をさらに追加する場合は、必要に応じて手順を繰り返します。
10. ［**Citrix Gateway** アプライアンス］ の一覧で、ユーザーがストアにアクセスできる展開環境を選択します。複数の展開環境を介したアクセスを有効にする場合は、［デフォルトアプライアンス］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、ユーザーがストアにアクセスするための認証方法を選択し、［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。
    - **Citrix Gateway** を介したパススルー：ストアにアクセスする場合、Citrix 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。
      1. ［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。
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、「ストアの構成と管理」を参照してください。

ストアが作成されました。ただし、Citrix Workspace アプリ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、「ユーザーアクセスのオプション」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 サイトの URL 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。

展開環境に複数のサーバーをすばやく追加するには、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への参加オプションを選択します。

ストアに **Citrix Virtual Apps and Desktops** リソースを追加する

Citrix Virtual Apps and Desktops 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. ［**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。［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、展開環境に対してわかりやすい表示名を指定し、［種類］を選択してストアで使用できるようにするリソースの提供方法を指定します。［種類］はデフォルトの「Citrix Virtual Apps and Desktops」になります。XenApp 6.5 は［種類］として使用できますが、2018 年 6 月に製品終了（End of Life：EOL）となったため、現在は拡張サポートプログラムの対象となっています。
3. 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 Citrix Virtual Apps and Desktops および XenApp 6.5 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。Citrix Virtual Apps and Desktops サイトの場合は、Delivery Controller の詳細を指定します。XenApp 6.5 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。

- 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。Citrix Virtual Apps and Desktops 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。
- SSL Relay を使用した XenApp 6.5 サーバーとのセキュリティで保護された接続でデータを送信し、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。Citrix Virtual Apps and Desktops 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 6.5 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］ で指定します。デフォルトのポートは 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。
7. ［**OK**］ をクリックします。Citrix Virtual Apps and Desktops 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。さらに Citrix Virtual Desktops サイトまたは Citrix Virtual Apps ファームを追加するには、上記の手順を繰り返します。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。

Citrix 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、Citrix 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［ストアの作成］ダイアログボックスの ［リモートアクセス］ ページで、［追加］をクリックします。
2. ［Citrix Gateway アプライアンスの追加］ダイアログボックスの ［全般設定］ ページで、Citrix Gateway アプライアンスにわかりやすい表示名を指定します。

   ここで指定する表示名がユーザーの Citrix Workspace アプリに表示されます。そのため、ユーザーが使用するゲートウェイ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、または最も近いゲートウェイ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. [**Citrix Gateway URL**] に、展開環境の Citrix Gateway 仮想サーバーの URL: ポートの組み合わせを入力します。ポートが指定されていない場合は、デフォルトの`https://`ポート 443 が使用されます。URL にポート 443 を指定する必要はありません。

   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. 使用可能なオプションから、Citrix Gateway の [使用法] または [役割] を選択します。

   - 認証および **HDX** ルーティング: Citrix 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: Citrix 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: Citrix 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. すべての展開環境で、Citrix Virtual Apps and Desktops または XenApp 6.5 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 **STA 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、Citrix Virtual Apps and Desktops または XenApp 6.5 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、Citrix Virtual Apps and Desktops または XenApp 6.5 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。Delivery Controller の設定方法に応じて、正しい STA URL（`HTTPS://`や`HTTP://`など）を使用します。また、STA URL は、仮想サーバー上の Citrix Gateway 内で構成されているものと同じである必要があります。

6. Citrix Workspace アプリが自動的に再接続を試みている間、Citrix Virtual Apps and Desktops または XenApp 6.5 が切断されたセッションを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] を選択します。

7. 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] を選択します。セッションの途中で 1 つの STA が使用できなくなっても、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、ユーザーセッションは中断されません。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、Citrix Gateway アプライアンスの仮想サーバーの **IP** アドレス（VIP）を入力します。

   プライベート IP アドレスに NAT されたパブリック IP アドレスではなく、Citrix Gateway 仮想サーバーのプライベート IP アドレスを使用します。ゲートウェイは通常、その URL を介して StoreFront によって識別されます。グローバルサーバー負荷分散（GSLB）を使用している場合、各ゲートウェイに VIP を追加する必要があります。これにより、StoreFront では、同じ URL（GSLB ドメイン名）を個別のゲートウェイとして使用する複数のゲートウェイを識別できます。たとえば、ストアに対して 3 つのゲートウェイを同じ URL（`https://gslb.domain.com`など）で構成できますが、それぞれに固有の VIP（10.0.0.1、10.0.0.2、10.0.0.3 など）が設定されます。

9. Citrix Gateway 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 Workspace アプリ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。

   - 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一覧から代替の認証方法を選択します。

10. Citrix Gateway 用に StoreFront を構成していて、Smart Access を使用する場合は、コールバック **URL** を入力する必要があります。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 Citrix Gateway 認証サービスに接続して、Citrix 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。

    GSLB を使用するときは、各 GSLB ゲートウェイに固有のコールバック URL を設定することをお勧めします。StoreFront は、各 GSLB ゲートウェイ仮想サーバー用に構成されたプライベート VIP への固有のコールバック URL を解決できる必要があります。たとえば、`emeagateway.domain.com`、`usgateway.domain.com`、および`apacgateway.domain.com`は正しいゲートウェイ VIP に解決する必要があります。

11. ［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 Citrix Gateway アプライアンスが追加されます。

    Citrix Gateway アプライアンスに関する構成情報は、ストアの.cr プロビジョニングファイルに保存されます。これにより、Citrix Workspace アプリは、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。

12. このトピック冒頭の「新しい展開環境の作成」の手順 10 に戻ってください。

既存のサーバーグループへの参加

April 2, 2020

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。

グループに追加するサーバーに StoreFront をインストールする前に、次のことを確認してください:

- 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。
- 追加するサーバーの StoreFront の IIS での相対パスは、グループ内のほかのサーバーと同じです。

追加する StoreFront サーバーがサーバーグループに属していて削除された場合、同じサーバーグループまたは異なるサーバーグループに再度追加される前に、出荷時のデフォルト設定にリセットする必要があります。詳しくは、「サーバーを出荷時のデフォルト設定にリセット」を参照してください。

> 重要:
>
> 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. 参加する StoreFront 展開環境のサーバーにログオンし、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。

サーバーを出荷時のデフォルト設定にリセット

June 21, 2019

場合によっては、StoreFront インストールを初期インストール状態にリセットする必要があります。これは、StoreFront サーバーをサーバーグループに再度追加する前などに必要です。

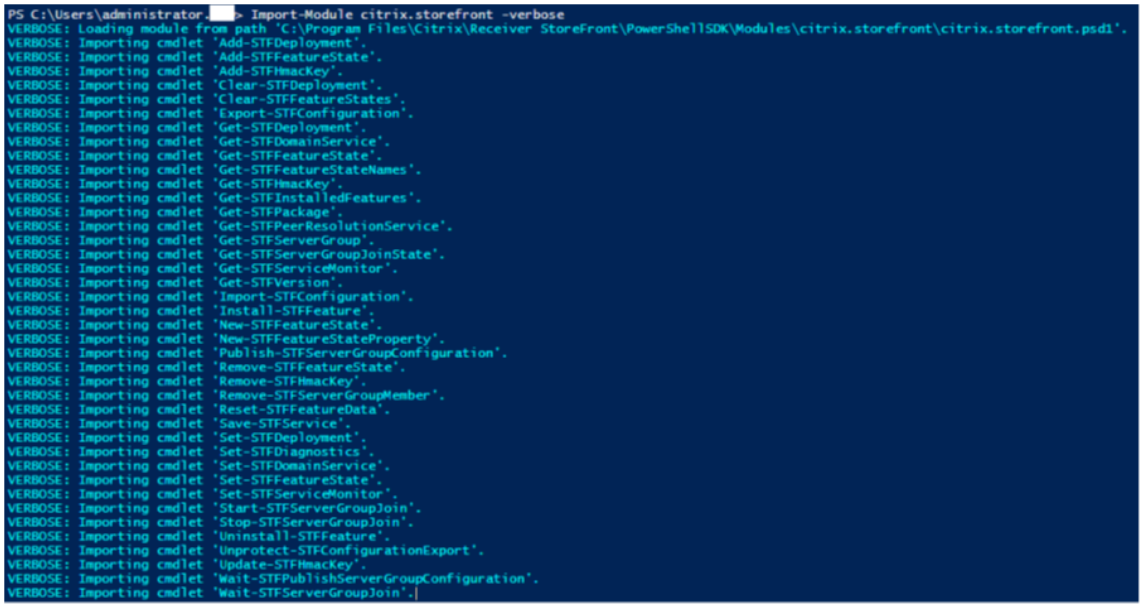
手動でアンインストールおよび再インストールすることはできますが、時間がかかり、予期しない問題を引き起こす可能性があります。代わりに、**Clear-STFDeployment** PowerShell コマンドレットを実行して、StoreFront サーバーを出荷時のデフォルト設定にリセットできます。

1. StoreFront 管理コンソールが閉じられていることを確認してください。
2. PowerShell ISE を開き、［管理者として実行］ を選択します。
3. PowerShell パスを設定します:

```
$env:PSModulePath = [Environment]::GetEnvironmentVariable('
    PSModulePath','Machine')
```

4. Citrix StoreFront モジュールをインポートします。

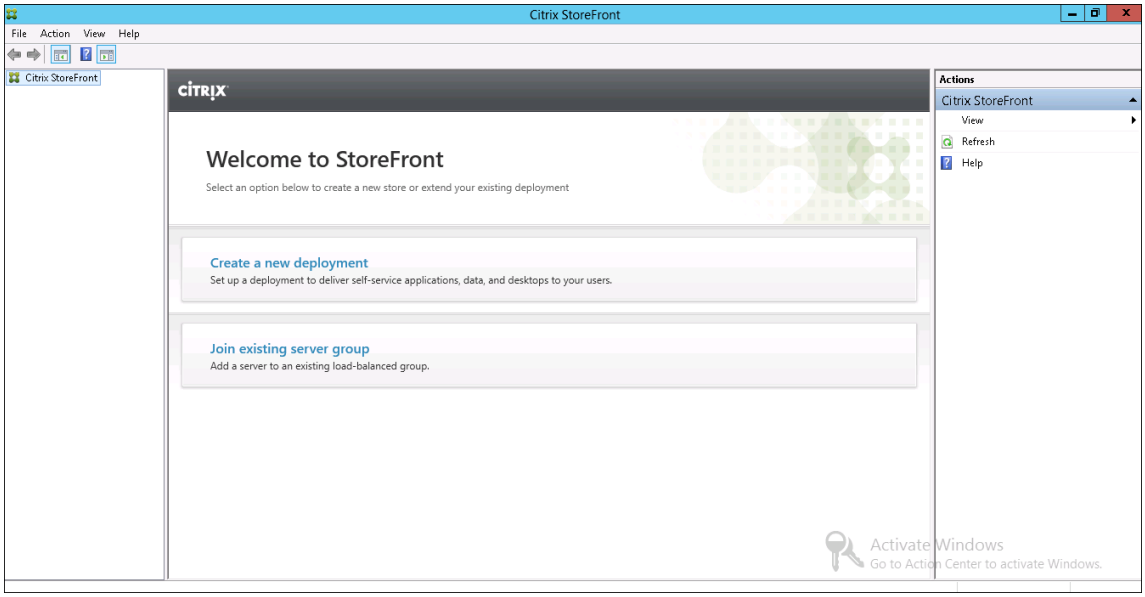
```
Import-Module citrix.storefront -verbose
```



5. モジュールのインポート後、**Clear-STFDeployment** コマンドを実行して StoreFront サーバーをデフォルトの設定にリセットします:

```
Clear-STFDeployment -Confirm $False
```

6. コマンドが正常に完了した後、StoreFront 管理コンソールを開き、すべての設定がリセットされたことを確認します。［新しい展開環境の作成］ または ［既存のサーバーグループへの参加］ を可能にするオプションが利用できるようになります。



Web Interface 機能の StoreFront への移行

March 2, 2020

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、ここでは取り上げません。

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。デスクトップまたは **Web UI** で検索ボックスを無効にするには、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** で検索ボックスを無効にするには、style.css に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）。

Web Interface の機能	StoreFront の同等のもの
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。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 Workspace アプリ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、ヒントの使用は非常に限定されたものになります。カスタムスクリプトを使うとヒントを追加できます。

Web Interface の機能	StoreFront の同等のもの
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 Workspace アプリには異なる 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、タブ付き UI（アプリタブ、デスクトップタブ、コンテンツタブ、（タブ順））	Citrix Workspace アプリ 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。
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 管理コンソールの ［操作］ 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'); }`

Web Interface の機能	StoreFront の同等のもの
ログオン前のウェルカムメッセージ（ロケール前）（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; //Before web login CTXS. Extensions.beforeLogon = function (callback){ doneClickThrough = true; CTXS.ExtensionAPI.showMessage({ messageTitle: ”Welcome!”, messageText: ”Only for \<a href=” http://www.WWc.com” target=”_blank ”\>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(); } } ;`

Web Interface の機能	StoreFront の同等のもの
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** ディレクトリに置いてください。
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 { text-align: center; color: white; font-size: 16px; } ** Example static content using a script: **\$('\##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。

Web Interface の機能	StoreFront の同等のもの
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

April 2, 2020

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。

削除された StoreFront サーバーが、同じサーバーグループまたは異なるサーバーグループに再度追加される前に、出荷時のデフォルト設定にリセットする必要があります。詳しくは、「サーバーを出荷時のデフォルト設定にリセット」を参照してください。

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。構成情報の伝達は手動で開始されるため、グループ内のサーバーが構成変更で更新されるタイミングと状況を制御できます。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:
>
> これにより、伝達中に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。サーバーの構成を更新する場合、変更をグループ内の他のサーバーに反映することで、後で展開の別のサーバーからの変更を反映する場合でもこれらの変更が失われないようにします。

グループ内のサーバー間で反映される情報には、次の項目が含まれます:

- StoreFront 構成を含むすべての web.config ファイルの内容。
- `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\Windows\CitrixWorkspaceAppWeb.exe`や`C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\MAC\CitrixWorkspaceAppWeb.dmg`のような`C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients`の内容。
- `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\contrib`の内容。
- コピーされたイメージや customisation.js ファイルのような`C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\custom folder`の内容。
- 手動でインポートされた証明書失効一覧（CRL）を除く、Citrix Delivery Services 証明書ストアの内容。ローカル CRL の配布について詳しくは、「証明書失効一覧（CRL）のチェック」を参照してください。

> 注:
>
> サブスクリプションデータは、変更の反映メカニズムとは無関係に他のサーバーと同期されます。これは自動的に行われ、変更の反映タスクが開始されることはありません。

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。この場合、HTTPS バインドをデフォルトの Web サイトに追加します。詳しくは、「StoreFront 展開環境のセキュリティ」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 0 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。完了したら、構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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. コントローラーを選択して ［編集］ をクリックし、［**Delivery Controller** の編集］ 画面で ［設定］ をクリックします。
4. ［詳細設定］で ［設定］ をクリックします。
5. ［詳細設定の構成］ダイアログボックスで、次の操作を行います:
   a) ［すべての失敗のバイパス期間］ の行で 2 番目の列をクリックして、すべてのサーバーが応答しなくなった後に Delivery Controller がオフラインと見なされる時間を分単位で入力します。
   b) ［バイパス時間］ の行で 2 番目の列をクリックして、1 つのサーバーが応答しなくなった後にオフラインと見なされる時間を分単位で入力します。

認証と委任の構成

January 14, 2020

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。

方法	詳細
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 Citrix Virtual Apps and Desktops 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、Citrix Virtual Apps and Desktops 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。

方法	詳細
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。

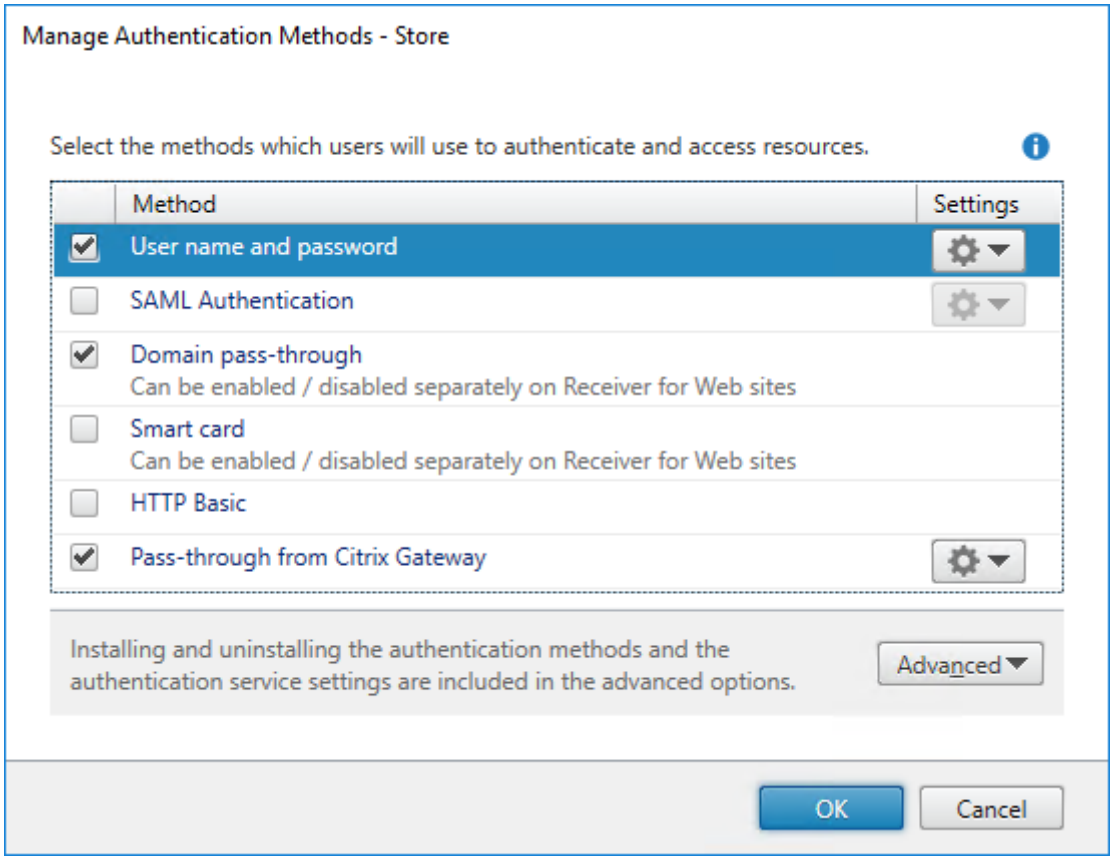
認証サービスの構成

April 2, 2020

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時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］ 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 または Windows 向け Citrix Workspace アプリをユーザーデバイスにインストールする時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］ をオンにします。ユーザーは、ストアにアクセスするときに、スマートカードと PIN を使用して認証されます。
- HTTP 基本認証を有効にするには、［**HTTP** 基本］ 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。
- Citrix Gateway からのパススルー認証を有効にするには、［**Citrix Gateway** からのパススルー］ をオンにします。ユーザーは Citrix 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。

Citrix 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 Citrix 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、［信頼済みドメイン］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］**>**［設定］ の一覧から、［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。ドメイン名を変更するには、［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 Citrix Workspace アプリと 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 Workspace アプリおよび 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 Workspace アプリは、有効期限が切れた時にのみ Citrix Gateway を介したパスワードの変更をサポートします。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、［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］**>**［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。カスタムの通知期間を設定する方法について詳しくは、「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。
    - パスワードの有効期限が切れた場合にのみユーザーがパスワードを変更できるようにするには、［パスワードの有効期限］ 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。これは、Citrix Workspace アプリと Citrix Receiver for Web でサポートされています。

        > 注:
        >
        > 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。

    - ユーザーによるパスワードの変更を禁止する場合は、［ユーザーにパスワードの変更を許可する］ をオンにしないでください。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。
    - ユーザーによるパスワードの変更を禁止する場合は、［ユーザーにパスワードの変更を許可する］ をオンにしないでください。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 Workspace アプリ	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これまで以上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。

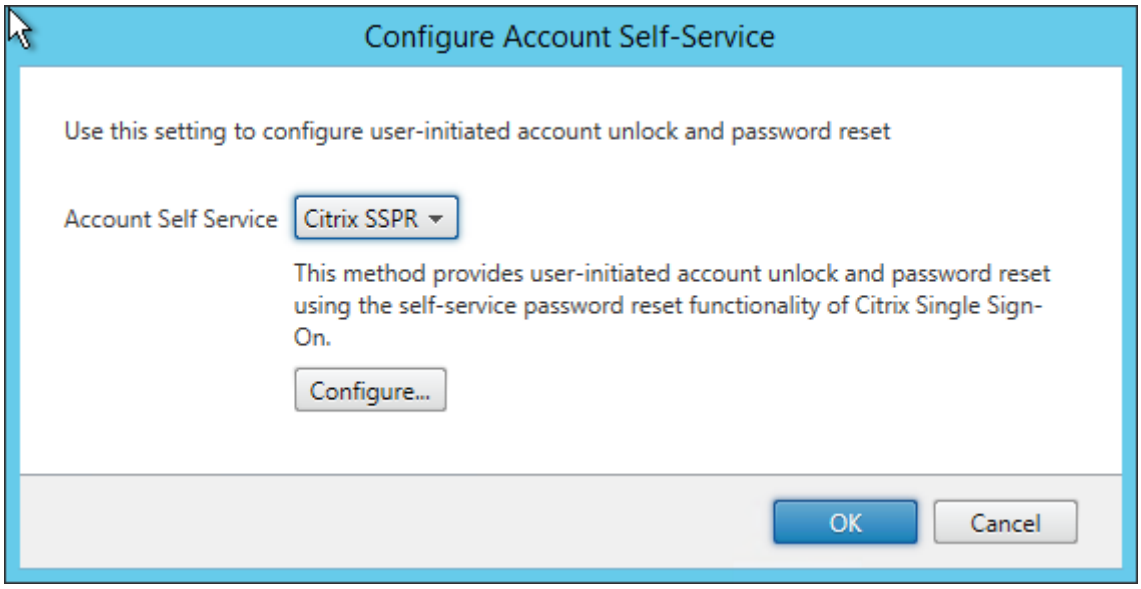
セルフサービスパスワードリセットでは、`username@domain.com`などの UPN ログオンはサポートされません。

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:

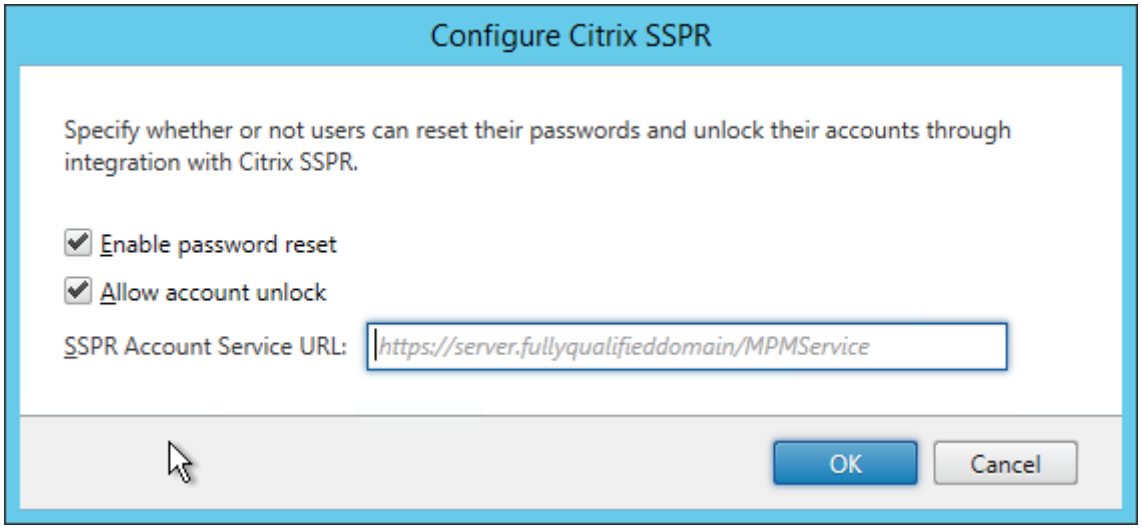
- ストアが、ユーザー名とパスワードによる認証を使用するように構成されている。
- ストアが、1 つのセルフサービスパスワードリセットのみを使用するように構成されている。StoreFront が、複数の同じドメインまたは信頼されているドメイン内にある複数のサーバーファームを使用するように構成されている場合は、これらすべてのドメインの資格情報を受け入れるようにセルフサービスパスワードリセットを構成する必要があります。
- ストアが、ユーザーがパスワードを常時変更できるように構成されている（パスワードのリセット機能を有効にする場合）。
- StoreFront ストアを Receiver for Web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

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。Citrix Virtual Apps and Desktops メディアで入手できます。詳しくは、セルフサービスパスワードリセットのドキュメントを参照してください。

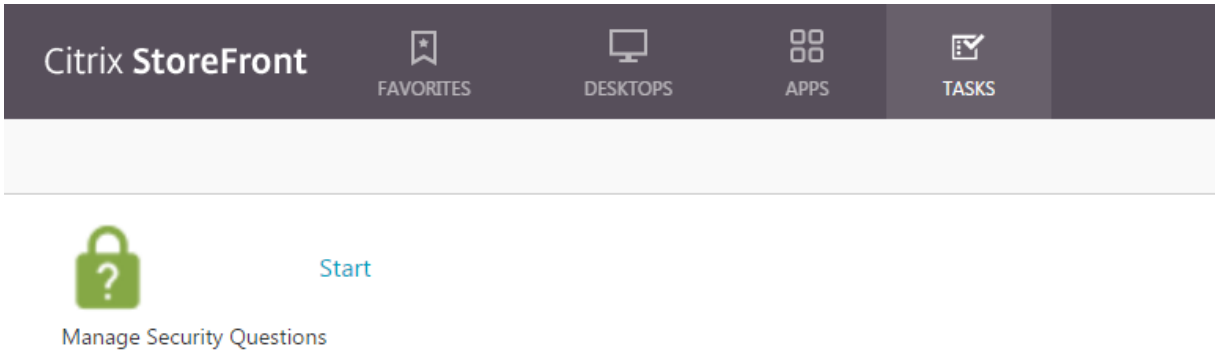
1. Citrix StoreFront 管理コンソールの左ペインで ［ストア］ ノードを選択して、［操作］ ペインの ［認証方法の管理］ **>** ［ユーザー名とパスワード］ をクリックし、ドロップダウンメニューから ［パスワードオプションの管理］ を選択します。
2. パスワードの変更を許可するユーザーを選択し、［**OK**］ をクリックします。
3. ［ユーザー名とパスワード］ ボックスの一覧で ［アカウントセルフサービスの設定］ を選択し、ドロップダウンメニューで ［**Citrix SSPR**］ を選択して ［**OK**］ をクリックします。
4. ユーザーに対して、セルフサ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。



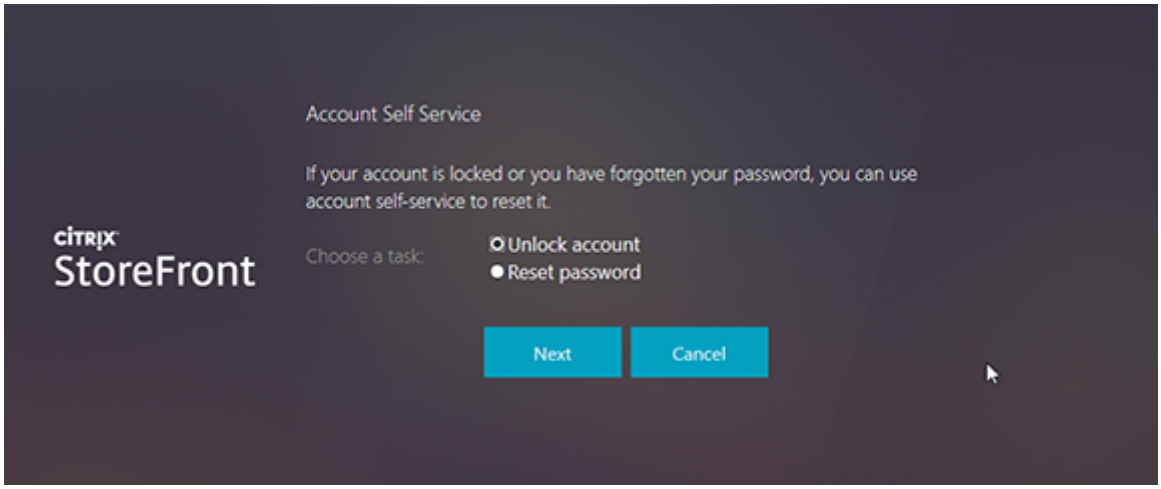
Citrix Workspace アプリまたは Citrix Receiver for Web への次回ユーザーログオン時に、セキュリティ用の質問に対する回答を登録できるようになります。［開始］ をクリックすると、ユーザーが回答を登録する必要のある質問が表示されます。



StoreFront で構成すると、Citrix Receiver for Web のログオン画面にアカウントセルフサービスへのリンクが（他の Citrix Workspace アプリ内のボタンとして）ユーザーに表示されます。

このリンクをクリックすると、一連のフォームが表示されます。最初に ［アカウントのロック解除］ と ［パスワードのリセット］ （どちらも使用可能な場合）のいずれかを選択します。

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に機能的な違いはありません。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 **Citrix Gateway** に委任する

Citrix 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、［Citrix 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 Citrix Gateway に委任した場合、ユーザーはスマートカードを使って Citrix Gateway への認証を実行し、ストアにアクセスするときは自動的にログオンします。スマートカードユーザーのパススルー認証は、管

理者が Citrix 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 Citrix 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。

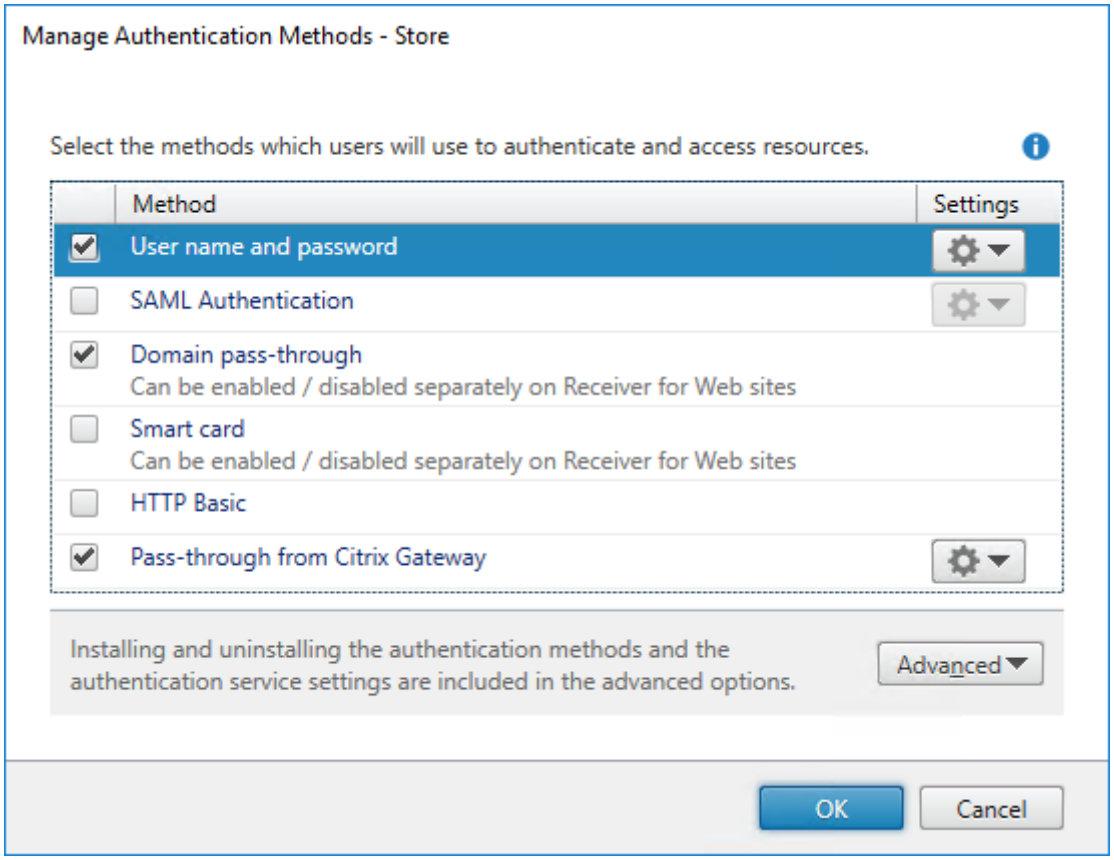
XML サービスベースの認証

April 2, 2020

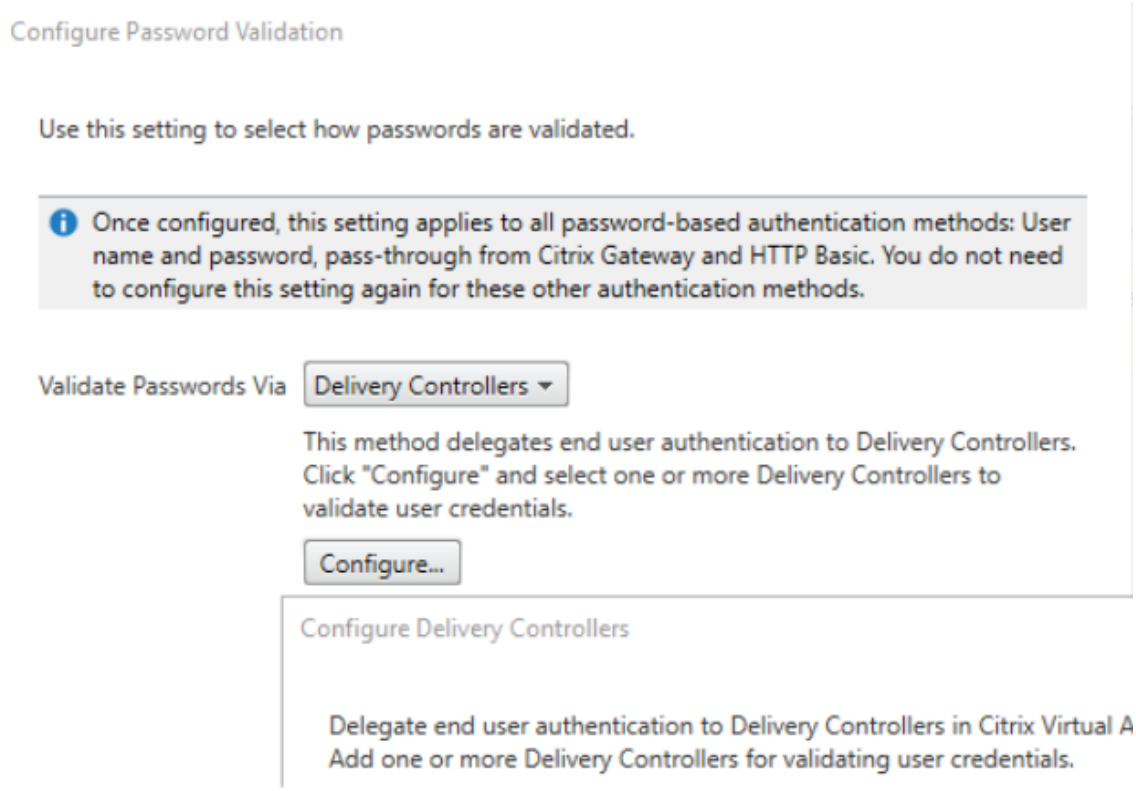
StoreFront が Citrix Virtual Apps and Desktops と同じドメイン内にない場合、また Active Directory の信頼を適切に配置できない場合には、Citrix Virtual Apps and Desktops XML Service を使ってユーザー名とパスワード資格情報を認証するように StoreFront を構成できます。

XML サービスベースの認証の有効化

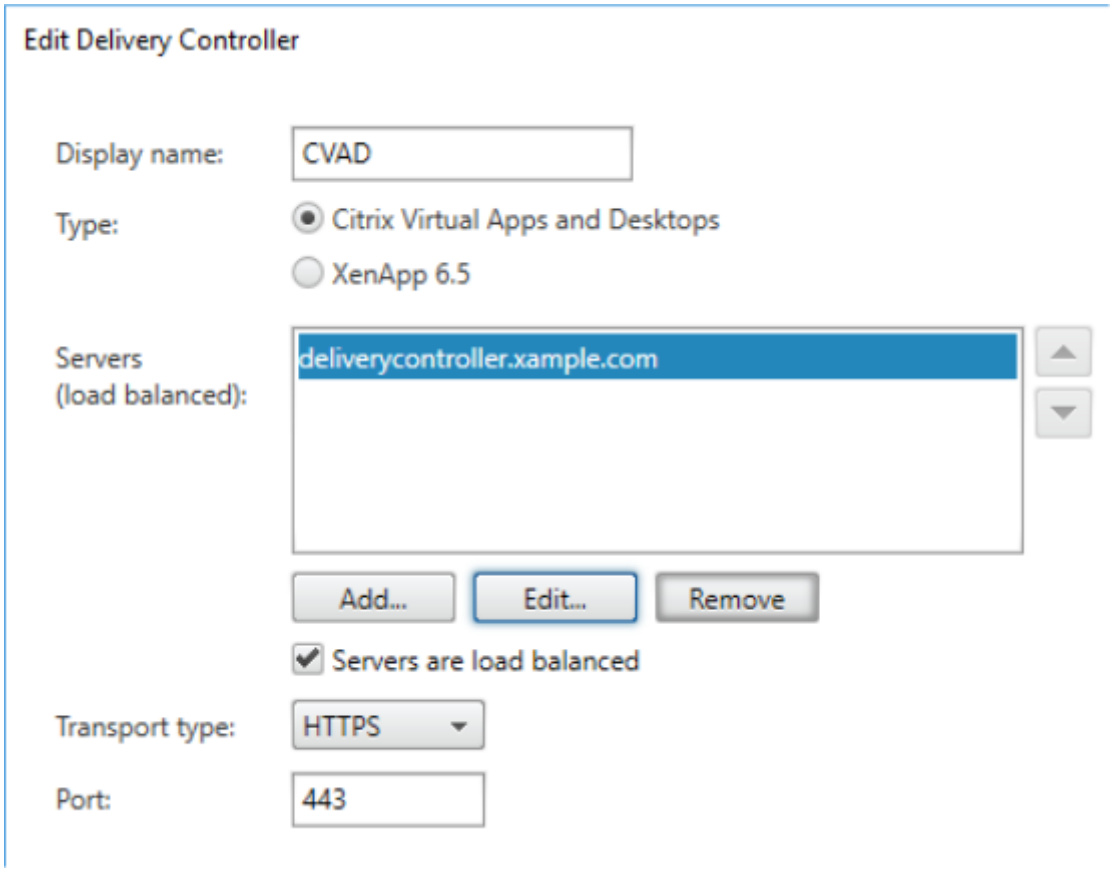
1. Windows の ［スタート］ 画面または ［アプリ］ 画面で、Citrix StoreFront タイルをクリックします。
2. Citrix StoreFront 管理コンソールの左ペインで ［ストア］ ノードを選択して、［操作］ペインの ［認証方法の管理］ をクリックします。
3. ［認証方法の管理］ ページで、［ユーザー名とパスワード］ > ［設定］ ドロップダウンメニューから、［パスワード確認の構成］ を選択します。



4. ［パスワード検証方法］ の一覧から ［**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］ の一覧から、［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

April 2, 2020

> 注:
>
> XenApp 6.5 は製品終了（End of Life：EOL）となり、現在は拡張サポートプログラムの対象となっています。

［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 Citrix Virtual Apps 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 Virtual Apps and Desktops XML Service を実行する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 **Citrix Virtual Apps** サーバーの構成する

各 Citrix Virtual Apps 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 Virtual Apps and Desktops XML Service 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 Virtual Apps and Desktops XML Service を実行する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］ ボックスにドメインコントローラーの名前を入力し、［**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。

- Citrix 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［Citrix 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。
  - Citrix 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 Citrix 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 または Windows 向け Citrix Workspace アプリ（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 または Windows 向け Citrix Workspace アプリ（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、シトリックス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\integratedwin
名前:SSONCheckEnabled
種類:REG_SZ
値:true or false
64 ビットマシンの場合:HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\AuthManagerProtocol
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

March 2, 2020

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 環境のためのスマートカードの構成』ドキュメントでは、Citrix 環境でスマートカードを使用する場合に、特定の種類のスマートカードが使用されるように構成する方法について説明しています。同様の手順がほかのベンダーのスマートカードにも適用されます。

> 注:
>
> この記事では、「Citrix Workspace アプリ」に関する記載は、特に明記されていない限り、サポートされているバージョンの Citrix Receiver にも適用されます。

前提条件

- 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。Citrix Virtual Desktops 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」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。

Citrix Gateway を構成します

- Citrix 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、「証明書のインストールと管理」を参照してください。
- Citrix Gateway 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、「Citrix Gateway にルート証明書をインストールするには」を参照してください。
- 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、「クライアント証明書認証ポリシーの構成およびバインド」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、「ルート証明書を仮想サーバーに追加するには」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 Citrix 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。
- Citrix 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、「Citrix Gateway を介した StoreFront へのアクセス」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 Citrix 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。

StoreFront の構成

- 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 でサーバー証明書を作成する方法については、https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831637(v=ws.11)#create-certificate-wizardを参照してください。HTTPS バインドを IIS サイトに追加する方法について詳しくは、「https://docs.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/hh831632(v=ws.11)」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したり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 Citrix 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。Citrix 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 のインストールと設定」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 Citrix Gateway 経由でストアにアクセスする場合は、認証方法として Citrix Gateway からのパススルーを有効にして、資格情報の検証を Citrix 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 または Windows 向け Citrix Workspace アプリ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 または Windows 向け Citrix Workspace アプリ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 または Windows 向け Citrix Workspace アプリ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 Citrix 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 Citrix 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。
- Citrix Desktop Lock を実行している 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。

ユーザーデバイスの構成

- 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、「デスクトップロックを取り付けるには」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 Workspace アプリ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 Citrix Virtual Apps and Desktops 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 Windows 向け Citrix Workspace アプリ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の使用」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 Windows 向け Citrix Workspace アプリが構成されていることを確認します。ドメインポリシーの場合は、グループポリシー管理コンソールを使用して、Windows 向け Citrix Workspace アプリのグループポリシーオブジェクト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、「スマートカード」を参照してください。

  ［スマートカード認証］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、［PIN にパススルー認証を使用します］チェックボックスをオンにします。さらに、Citrix Virtual Apps and Desktops 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、［ローカルユーザー名とパスワード］ポリシーを有効にして、［すべての ICA 接続にパススルー認証を許可します］チェックボックスをオンにします。詳しくは、「ICA 設定リファレンス」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 Citrix Virtual Apps and Desktops 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 Citrix 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、「ICA 設定リファレンス」を参照してください。

Receiver for Windows または **Windows** 向け **Citrix Workspace** アプリのスマートカードパススルー認証を有効にする

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。Citrix Virtual Apps and Desktops 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.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。完了したら、
> 構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

1. テキストエディターを使ってストアの default.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\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. Citrix Gateway を経由しないでストアにアクセスするユーザーに対して、スマートカードの資格情報でのパススルーを有効にするには、[[アプリケーション]] セクションに次の設定を追加します。

   ```
   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. Citrix Gateway を経由してストアにアクセスするユーザーに対して、スマートカードの資格情報でのパススルーを有効にするには、[アプリケーション] セクションに次の設定を追加します。

   ```
   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

April 2, 2020

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。完了したら、構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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

January 14, 2020

Citrix StoreFront では、Citrix Virtual Apps and Desktops 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。

タスク	詳細
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 Citrix 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。

タスク	詳細
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 Workspace アプリを構成する場合、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
Citrix 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 Citrix Gateway を介したストアへのアクセスを構成します。
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

April 2, 2020

［ストアの作成］ タスクを使用して、追加のストアを構成します。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。

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、Citrix Gateway 経由でのストアへのリモートアクセスを設定します（任意）。

［ストア名］ページで、［認証されていないユーザーだけにこのストアへのアクセスを許可する］ を選択すると、認証が不要なストアの作成（匿名のストアまたは認証不要なストア）が許可されます。認証が不要なストアを作成すると、［認証方法］ ページおよび ［リモートアクセス］ ページは利用できなくなり、左側の ［サーバーグループノード］ ペインと［操作］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、これが使用できる唯一のオプションです）。

> 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。完了したら、
> 構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

デスクトップとアプリケーションのストアへの追加

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 Workspace アプリ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。［追加］ をクリックします。
5. ［Delivery Controller の追加］ダイアログボックスで表示名を指定します。これにより環境を識別しやすくなります。［種類］ を指定して、ストアで使用可能になったリソースの提供方法を示します。［種類］はデフォルトの「Citrix Virtual Apps and Desktops」になります。XenApp 6.5 は［種類］として使用できますが、2018 年 6 月に製品終了（End of Life：EOL）となったため、現在は拡張サポートプログラムの対象となっています。
6. 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 Citrix Virtual Apps and Desktops および XenApp 6.5 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。Citrix Virtual Apps and Desktops サイトの場合は、Delivery Controller の詳細を指定します。XenApp 6.5 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。
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。
   - 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。Citrix Virtual Apps and Desktops 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。
   - SSL Relay を使用した XenApp 6.5 サーバーとのセキュリティで保護された接続でデータを送信し、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。Citrix Virtual Apps and Desktops 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 6.5 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］で指定します。デフォルトのポートは 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。Citrix Virtual Apps and Desktops 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 ～ 10 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。

11. ［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 Citrix 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ユーザーがストアを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化するには、［リモートアクセスの有効化］をオンにします。
      - Citrix 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。ユーザーは ICAProxy またはクライアントレス VPN（cVPN）を使用して Citrix Gateway にログオンするため、Citrix Gateway Plug-in を使用して完全 VPN を確立する必要はありません。
      - Secure Sockets Layer（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に Citrix 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［**PCitrix 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 Citrix 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。

12. リモートアクセスを有効にした場合は、［**Citrix Gateway** アプライアンス］の一覧で、ユーザーがストアにアクセスできるアプライアンス（展開環境）を選択します。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。一覧で複数のエントリを選択して複数のアプライアンスを介したアクセスを有効にする場合は、［デフォルトアプライアンス］を選択します。さらにアプライアンスを一覧に追加するには、Citrix Gateway を介したストアへのリモートアクセスを有効にするで説明されている手順を実行します。

13. ［認証方法］ページで、ユーザーがストアにアクセスするための認証方法を選択し、［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。
- **Citrix Gateway** を介したパススルー：ストアにアクセスする場合、Citrix 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。
  1. ［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。

14. ［**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 URL を構成し、［作成］ をクリックします。
15. ストアが作成されたら、［完了］をクリックします。

ストアへのアクセス

ストアが作成されました。ただし、Citrix Workspace アプリ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、「ユーザーアクセスのオプション」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。Citrix Desktop Lock を実行している 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]://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。

Citrix Gateway を介したストアへのリモートアクセスを有効にする

前の手順で作成したストアに Citrix 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、［追加］ をクリックします。
2. ［**Citrix Gateway** アプライアンスの追加］ の ［全般設定］ ページで、Citrix Gateway アプライアンスにわかりやすい表示名を指定します。

ここで指定する表示名がユーザーの Citrix Workspace アプリに表示されます。そのため、ユーザーが使用するゲートウェイ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、または最も近いゲートウェイ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. [**Citrix Gateway URL**] に、展開環境の Citrix Gateway 仮想サーバーの URL: ポートの組み合わせを入力します。ポートが指定されていない場合は、デフォルトの`https://`ポート 443 が使用されます。URL にポート 443 を指定する必要はありません。

   StoreFront 展開環境の FQDN（Fully Qualified Domain Name：完全修飾ドメイン名）は一意で、Citrix 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 Citrix 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、Citrix Gateway の ［使用法］または［役割］ を選択します。

   - 認証および **HDX** ルーティング： Citrix 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： Citrix 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： Citrix 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. すべての展開環境で、Citrix Virtual Apps and Desktops または XenApp 6.5 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 STA 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、Citrix Virtual Apps and Desktops または XenApp 6.5 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、Citrix Virtual Apps and Desktops または XenApp 6.5 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。Delivery Controller の設定方法に応じて、正しい STA URL（`HTTPS://`や`HTTP://`など）を使用します。また、STA URL は、仮想サーバー上の Citrix Gateway 内で構成されているものと同じである必要があります。

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 Workspace アプリが自動的に再接続を試みている間、Citrix Virtual Apps and Desktops または XenApp 6.5 が切断されたセッションを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］ を選択します。

8. 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］ を選択します。セッションの途中で 1 つの STA が使用できなくなっても、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、ユーザーセッションは中断されません。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. ［認証設定］ ページで、Citrix Gateway アプライアンスの仮想サーバーの **IP** アドレス（VIP）を入力します。

   プライベート IP アドレスに NAT されたパブリック IP アドレスではなく、Citrix Gateway 仮想サーバーのプライベート IP アドレスを使用します。ゲートウェイは通常、その URL を介して StoreFront によって識別されます。グローバルサーバー負荷分散（GSLB）を使用している場合、各ゲートウェイに VIP を追加する必要があります。これにより、StoreFront では、同じ URL（GSLB ドメイン名）を個別のゲートウェイとして使用する複数のゲートウェイを識別できます。たとえば、ストアに対して 3 つのゲートウェイを同じ URL（`https://gslb.domain.com`など）で構成できますが、それぞれに固有の VIP（10.0.0.1、10.0.0.2、10.0.0.3 など）が設定されます。

10. Citrix Gateway 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 Workspace アプリ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。

    - 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一覧から代替の認証方法を選択します。

11. Citrix Gateway 用に StoreFront を構成していて、Smart Access を使用する場合は、コールバック **URL** を入力する必要があります。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 Citrix Gateway 認証サービスに接続して、Citrix 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。

    GSLB を使用するときは、各 GSLB ゲートウェイに固有のコールバック URL を設定することをお勧めします。StoreFront は、各 GSLB ゲートウェイ仮想サーバー用に構成されたプライベート VIP への固有のコールバック URL を解決できる必要があります。たとえば、`emeagateway.domain.com`、`usgateway.domain.com`、および`apacgateway.domain.com`は正しいゲートウェイ VIP に解決する必要があります。

12. ［作成］ をクリックします。これにより、［リモートアクセス設定］ ダイアログボックスの一覧に Citrix Gateway アプライアンスが追加されます。

    Citrix Gateway アプライアンスに関する構成情報は、ストアの.cr プロビジョニングファイルに保存されます。これにより、Citrix Workspace アプリは、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。

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。完了したら、構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

認証が不要なストアの作成

April 2, 2020

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、［認証されていないユーザー用のストアの作成］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、Citrix 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。完了したら、
> 構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

デスクトップとアプリケーションのストアへの追加

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。

   Citrix Receiver ではストア名が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。［追加］ 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 Citrix Virtual Apps and Desktops または XenApp 6.5 で提供されるかどうかを指定します（XenApp 6.5 は製品終了（EOL）となり、現在は拡張サポートプログラムの対象となっています）。Delivery Controller を追加する時は、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。

   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 6.5 ファームを選択した場合は、ファームの個別サーバーの名前を［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。Citrix Virtual Desktops サイトの場合は、Controller の詳細を指定します。XenApp 6.5 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。

6. ［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。Citrix Virtual Apps and Desktops 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）。

7. 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 接続では 80、HTTPS 接続では 443 が使用されます。Citrix Virtual Apps and Desktops 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。

8. [**OK**] をクリックします。Citrix Virtual Apps and Desktops 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 ～ 9 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 Workspace アプリ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、「ユーザーアクセスのオプション」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、Citrix 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 サイトの URL 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\`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（「Citrix XML Service のポートと信頼を設定する」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

April 2, 2020

ストアで使用される Citrix 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ファイルを提供すると、ユーザーが Citrix Workspace アプリを簡単に構成できるようになります。Citrix Workspace アプリの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。完了したら、
> 構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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

April 2, 2020

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 Workspace アプリを構成する場合、［ストアの非表示］タスクを使って、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。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 Workspace アプリ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。完了したら、
> 構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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

April 2, 2020

Citrix Virtual Apps and Desktops 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、［**Delivery 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。完了したら、

構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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. ［Delivery Controller の管理］ダイアログボックスで、次の手順を実行します：
   a) ［追加］ をクリックして、別の Citrix Virtual Apps and Desktops 環境のデスクトップとアプリケーションをストアに含めます。
   b) ［編集］ をクリックして展開環境の設定を変更します。
   c) 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、Delivery controller 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表示名を指定します。これにより環境を識別しやすくなります。
5. Citrix Virtual Apps and Desktops 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。Citrix Virtual Desktops サイトの場合は、Delivery Controller の詳細を指定します。Citrix Virtual Apps 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。
6. ［サーバーを負荷分散する］ オプションを選択して、Citrix Virtual Apps and Desktops サイトのすべての Delivery Controller 間で負荷が分散されるようにすることをお勧めします。StoreFront は、サーバー一覧からの起動ごとにランダムに Delivery Controller を選択し、Citrix Virtual Apps and Desktops サイトのすべてのサーバー間で負荷を分散します。このオプションが選択されていない場合、サーバー一覧は優先度順のフェールオーバー一覧として機能します。この場合、一覧の最初の Delivery Controller で 100% の起動が発生します。そのサーバーがオフラインになった場合は、一覧の 2 番目の Delivery Controller で 100% の起動が発生し、以降同様に順番に動作します。
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。Citrix Virtual Apps and Desktops 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。
   - Citrix Virtual Apps 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。Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps 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。Citrix Virtual Apps and Desktops 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 ～ 9 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。

Citrix Gateway を介したストアへのリモートアクセスの管理

April 2, 2020

公共のネットワークから接続するユーザーに対して Citrix 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、Citrix 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。完了したら、
> 構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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 管理コンソールの右ペインで［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 Citrix 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ユーザーがストアを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化するには、［リモートアクセスの有効化］ をオンにします。

- Citrix 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。ユーザーは ICAProxy またはクライアントレス VPN（cVPN）を使用して Citrix Gateway にログオンするため、Citrix Gateway Plug-in を使用して完全 VPN を確立する必要はありません。
- Secure Sockets Layer（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に Citrix 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［**PCitrix 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 Citrix 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 ［**Citrix 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。それ以外の場合は、手順 14 に進みます。
5. ［全般設定］ページで、Citrix Gateway アプライアンスにわかりやすい表示名を指定します。

   ここで指定する表示名がユーザーの Citrix Workspace アプリに表示されます。そのため、ユーザーが使用するゲートウェイ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、または最も近いゲートウェイ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. ［**Citrix Gateway URL**］ に、展開環境の Citrix Gateway 仮想サーバーの URL: ポートの組み合わせを入力します。ポートが指定されていない場合は、デフォルトの`https://`ポート 443 が使用されます。URL にポート 443 を指定する必要はありません。
7. 使用可能なオプションから、Citrix Gateway の使用法を選択します。
   - 認証および **HDX** ルーティング： Citrix 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： Citrix 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： Citrix 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。
8. すべての展開環境で、Citrix Virtual Apps and Desktops または XenApp 6.5 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 STA 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、Citrix Virtual Apps and Desktops または XenApp 6.5 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、Citrix Virtual Apps and Desktops または

XenApp 6.5 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。Delivery Controller の設定方法に応じて、正しい STA URL（HTTPS://やHTTP://など）を使用します。また、STA URL は、仮想サーバー上の Citrix Gateway 内で構成されているものと同じである必要があります。

9. 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。

10. Citrix Workspace アプリが自動的に再接続を試みている間、Citrix Virtual Apps and Desktops または XenApp 6.5 が切断されたセッションを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］ を選択します。

11. 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］ を選択します。セッションの途中で 1 つの STA が使用できなくなっても、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、ユーザーセッションは中断されません。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。

12. ［認証設定］ ページで、Citrix Gateway アプライアンスの仮想サーバーの **IP** アドレス（VIP）を入力します。

    プライベート IP アドレスに NAT されたパブリック IP アドレスではなく、Citrix Gateway 仮想サーバーのプライベート IP アドレスを使用します。ゲートウェイは通常、その URL を介して StoreFront によって識別されます。グローバルサーバー負荷分散（GSLB）を使用している場合、各ゲートウェイに VIP を追加する必要があります。これにより、StoreFront では、同じ URL（GSLB ドメイン名）を個別のゲートウェイとして使用する複数のゲートウェイを識別できます。たとえば、ストアに対して 3 つのゲートウェイを同じ URL（https://gslb.domain.comなど）で構成できますが、それぞれに固有の VIP（10.0.0.1、10.0.0.2、10.0.0.3 など）が設定されます。

13. Citrix Gateway 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 Workspace アプリ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。

    - 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一覧から代替の認証方法を選択します。

14. Citrix Gateway 用に StoreFront を構成していて、Smart Access を使用する場合は、コールバック **URL** を入力する必要があります。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 Citrix Gateway 認証サービスに接続して、Citrix 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。

GSLB を使用するときは、各 GSLB ゲートウェイに固有のコールバック URL を設定することをお勧めします。StoreFront は、各 GSLB ゲートウェイ仮想サーバー用に構成されたプライベート VIP への固有のコールバック URL を解決できる必要があります。たとえば、`emeagateway.domain.com`、`usgateway.domain.com`、および`apacgateway.domain.com`は正しいゲートウェイ VIP に解決する必要があります。

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 Citrix Gateway アプライアンスが追加されます。

    Citrix Gateway アプライアンスに関する構成情報は、ストアの.cr プロビジョニングファイルに保存されます。これにより、Citrix Workspace アプリは、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。

16. 必要に応じて手順 4 ～ 13 を繰り返し、［Citrix Gateway アプライアンス］の一覧に Citrix Gateway アプライアンスを追加します。一覧で複数のエントリを選択して複数のアプライアンスを介したアクセスを有効にする場合は、［デフォルトアプライアンス］ を選択します。

17. ［**OK**］ をクリックして構成を保存し、［リモートアクセスの構成］ダイアログボックスを閉じます。

証明書失効一覧（**CRL**）のチェック

March 2, 2020

はじめに

StoreFront で、
CVAD Delivery Controller が使用する TLS 証明書の状態を公開された証明書失効一覧（CRL）を使用して確認するよう構成できます。
次の場合、証明書へのアクセスの取り消しが必要なことがあります:

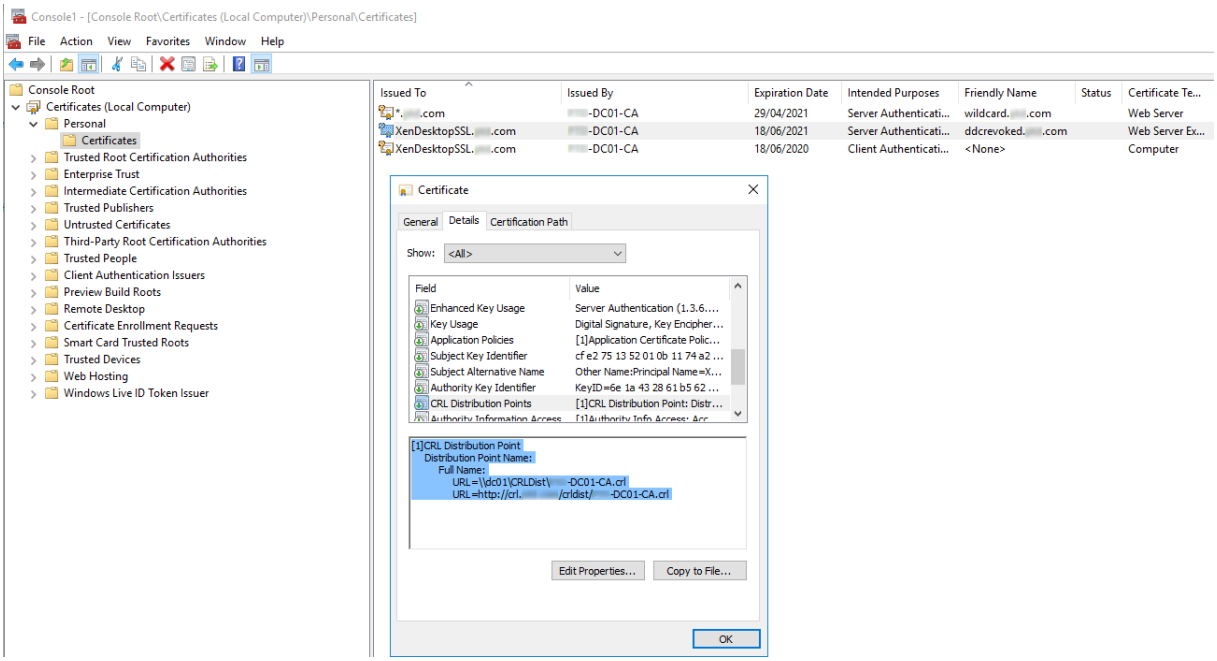
- 秘密キーが侵害された可能性がある
- CA が侵害された
- 所属が変更された
- 証明書が置き換えられた

> 注:
>
> このトピックは、StoreFront と
> Citrix Virtual Apps and Desktop Delivery Controller との間で HTTPS 接続が使用された場合のみ該当し

> ます。Delivery Controller への HTTP 接続
> に証明書は必要ありません。そのため、ここで説明されるストアの
> -CertRevocationPolicy 設定が影響することはありません。
>
> StoreFront は、CRL 配布ポイント
> （CDP）の拡張機能およびローカルにインストールされた証明書失効一覧
> （CRL）を使用した証明書失効チェックをサポートします。StoreFront は完全な CRL のみをサポートしています。デルタ CLR はサポートされていません。

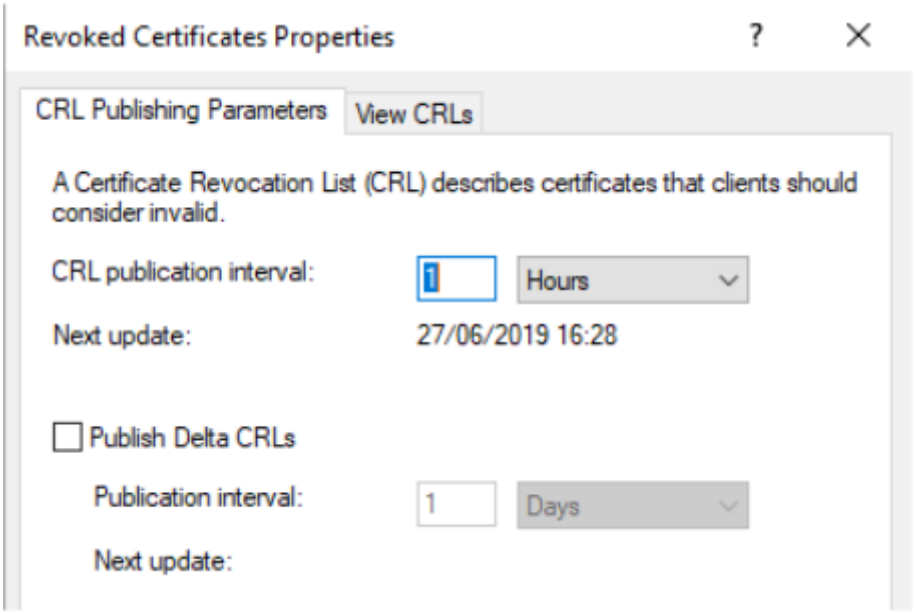
CRL 配布ポイント（**CDP**）拡張機能

Citrix Virtual Apps and Desktops Delivery Controller が使用している証明書が失効し、公開された CRL にシリアル番号が表示されている場合、
StoreFront はこの
Delivery Controller のリソースを列挙しません。StoreFront が失効した証明書を検出するには、
CDP 証明書拡張機能で定義されているいずれかの URL を使用して、公開された
CRL にアクセスする必要があります。



CRL の公開間隔

StoreFront がいち早く Delivery
Controller 上の失効した証明書を検出できるようにするには、CA での CRL の公開期間を短縮する必要があります。
CLR
配布ポイント拡張機能のプロパティを編集して、使用中の公開キー基盤により短い
CRL 公開期間値を設定します。



クライアントの **CRL** キャッシュ

Windows 公開キー基盤のクライアントは、CRL をローカルにキャッシュします。最新の CRL は、ローカルにキャッシュされた
CRL の有効期限が切れるまでダウンロードされません。

証明書失効リスト（**CRL**）への **StoreFront** のアクセス

証明書失効チェックのためには、StoreFront が CRL にアクセスできる必要があります。
StoreFront が CRL を公開する Web サーバーや証明機関（CA）と通信する方法や、
CRL の更新を受信する方法について慎重に確認してください。

Delivery Controller 上の内部エンタープライズ **CA** およびプライベート証明書

プライベート
CA および証明書を使用する場合、StoreFront に必要なのは正しく構成されたエンタープライズ CA と、組織内の内部ネットワークからアクセスできる公開された
CRL です。エンタープライズ CA が CDP 拡張機能を公開するように構成する情報については、Microsoft
ドキュメントを参照してください。CA が
CDP 拡張機能を含むように構成される前に
Delivery Controller 上に存在していた証明書は、再発行が必要な場合があります。

StoreFront サーバーおよび Citrix Virtual Apps and
Desktops サーバーは通常、インターネット接続のない隔離されたプライベートネットワーク上に存在します。この

場合、プライベート CA
を使用する必要があります。

Delivery Controller 上の外部パブリック **CA** およびパブリック証明書

StoreFront サーバーおよび Citrix Virtual Apps and
Desktops Delivery Controller は、パブリック CA によって発行された証明書を使用できます。StoreFront は、CDP 拡張機能で参照された URL を使用して、インターネット経由でパブリック
CA の Web サーバーと通信できる必要があります
。パブリック証明書が失効した後、StoreFront が CDP URL を使用して
CRL のコピーをダウンロードできない場合、StoreFront は
CRL チェックを実行できなくなります。

証明書失効ポリシーの設定

Citrix StoreFront の PowerShell コマンドレット **Get-STFStoreFarmConfiguration**
および **Set-STFStoreFarmConfiguration** を使用して、ストアの証明書失効ポリシーを設定します。
Get-Help Set-STFStoreFarmConfiguration -detailed
を実行すると、PowerShell のヘルプとオプション
-CertRevocationPolicy の例を表示します。これらの StoreFront
PowerShell コマンドレットについて詳しくは、Citrix StoreFront SDK PowerShell Modulesを参照してください。

-CertRevocationPolicy オプションは、以下の値に設定できます:

設定	説明
NoCheck	StoreFront は、Delivery Controller 上の証明書の失効状態をチェックしません。StoreFront は、失効した証明書を使用する Delivery Controller からのリソースを列挙し続けます。これがデフォルトの設定です。
MustCheck	これは最も安全なオプションです。StoreFront は、Delivery Controller 上の証明書の CDP 拡張機能で参照されている URL にアクセスして、CRL の取得を試みます。CRL が利用できない場合、または Delivery Controller で使用されている証明書が失効している場合、StoreFront は Delivery Controller からの列挙に失敗します。URL は、証明書がプライベートの場合は内部 Web サーバーを指し、証明書がパブリック CA によって発行された場合はパブリックインターネット Web サーバーを指します。

設定	説明
FullCheck	StoreFront は、Delivery Controller 証明書の CDP 拡張機能で公開されている URL への接続を試みます。StoreFront がこれらの URL から CRL のコピーの取得に失敗した場合でも、Delivery Controller からのリソースの列挙を許可します。StoreFront が CRL を正常に取得しても、Delivery Controller の証明書が失効している場合、StoreFront はリソースを列挙しません。URL は、証明書がプライベートの場合は内部 Web サーバーを指し、証明書がパブリック CA によって発行された場合はパブリックインターネット Web サーバーを指します。
NoNetworkAccess	StoreFront サーバー上の Citrix Delivery Server 証明書ストアにローカルにインポートされた CRL のみがチェックされます。StoreFront は、CDP 拡張機能で指定された URL への接続を試みません。StoreFront が CRL のローカルコピーの取得に失敗した場合でも、Delivery Controller からのリソースの列挙を許可します。StoreFront が Citrix Delivery Server 証明書ストアから CRL のローカルコピーを正常に取得しても、Delivery Controller の証明書が失効している場合、StoreFront はリソースを列挙しません。

ストアで証明書失効チェックを構成する

ストアの証明書失効ポリシーを設定するには、［管理者として実行］で PowerShell ISE を開いて、次の PowerShell コマンドレットを実行します。複数のストアがある場合、この手順をすべてのストアで繰り返します。-CertRevocationPolicy は、$StoreVirtualPath で指定されたストアに構成されたすべての Delivery Controller に影響を与えるストアレベルの設定です。

```
$SiteID = 1
$StoreVirtualPath = ”/Citrix/Store”
$StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
$StoreVirtualPath
Set-STFStoreFarmConfiguration -StoreService $StoreObject -
    CertRevocationPolicy
”MustCheck”
```


設定が正しく適用されたことを確認する、または現在の
-CertRevocationPolicy 構成を表示するには、次を実行します:

```
(Get-STFStoreFarmConfiguration -StoreService $StoreObject).
    CertRevocationPolicy
```

StoreFront サーバーでローカルにインポートされた CRL を使用する

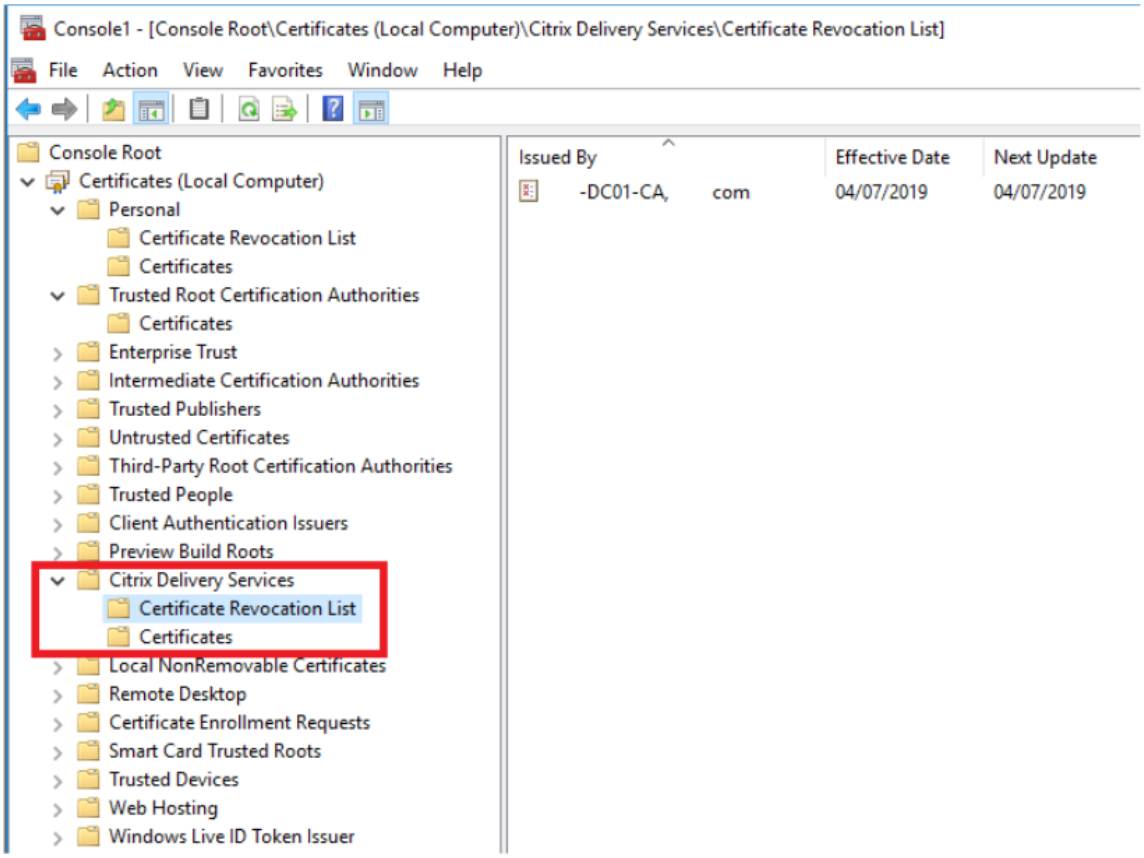
ローカルにインポートされた CRL の使用はサポートされていますが、推奨されていません。
以下はその理由です:

- 大規模な環境では複数の
  StoreFront サーバーグループが関係する可能性があるため、管理や更新が困難になります。
- 証明書が失効するたびにすべての
  StoreFront サーバーの CRL を手動で更新すると、
  Active Directory ドメイン全体で CDP 拡張機能および公開された CRL を使用する場合に比べて、大幅に効率が低下します。

-CertRevocationPolicy が「NoNetworkAccess」に設定されている場合、ローカルでインストールされているまたは更新された
CRL を使用して、CRL
をすべての StoreFront サーバーに効率的に配布できます。

ローカルにインポートされた **CLR** を使用するには

1. CRL を StoreFront サーバーのデスクトップにコピーします。StoreFront サーバーがサーバーグループの一部である場合は、グループ内のすべての
   StoreFront サーバーにコピーします。
2. MMC スナップインを開いて ［ファイル］**>**［スナップインの追加と削除］**>**［証明書］**>**［コンピューターアカウント］**>**［**Citrix Delivery Services** の証明書ストア］ を選択します。
3. 右クリックして ［すべてのタスク］**>**［インポート］ を選択し、.CRL ファイルを参照して
   ［すべてのファイル］**>**［開く］**>**［証明書をすべて次のストアに配置する］**>**［**Citrix Delivery Services**］ を選択します。



PowerShell またはコマンドラインで **CRL** を **Citrix Delivery Service** 証明書ストアに追加するには

1. StoreFront にログインし、
   .CRL ファイルを現在のユーザーのデスクトップにコピーします。
2. PowerShell ISE を開き、［管理者として実行］ を選択します。
3. 以下を実行します:

```
certutil -addstore ”Citrix Delivery Services” ”$env:UserProfile\
    Desktop\Example-DC01-CA.crl”
```

正常に実行されると、次の値が返されます:

```
Citrix Delivery Services
CRL ”CN=Example-DC01-CA, DC=example, DC=com” added to store.
CertUtil: -addstore command completed successfully.
```

このコマンドは、スクリプト経由で自動的に環境のすべての StoreFront
サーバーに CRL を配布する場合に使用できます。

Delivery Controller を使用した **XML** 認証

StoreFront を構成して、ユーザー認証を Citrix Virtual
Apps and Desktops Delivery Controller に委任できます。Delivery Controller の証明書が失効した場合、ユーザーは
StoreFront にサインインできなくなります。認証を担当する
Citrix Virtual Apps
and
Desktops Delivery Controller 上の証明書が失効している場合、Active Directory ユーザーを StoreFront にサインインできなくする必要があるため、これは望ましい動作です。

ユーザー認証を **Delivery Controller** に委任するには

1. 「
   」で説明したように、ストアで証明書失効チェックを構成するストアで証明書の失効を構成します。
2. 「
   」の手順に従って、XML サービスベースの認証Delivery Controller で HTTPS の使用を構成します。

XML 認証サービスで証明書失効チェックを構成する

以下の手順は、展開で XML 認証を使用している場合にのみ必要です
。

> 注:
>
> StoreFront
> では、ストアを認証サービスにマッピングするために 2 つの方法を利用できます。推奨される方法は、ストアと認証サービスの 1 対 1 のマッピングです
> 。この場合、すべてのストアと関連する認証サービスに対して、このセクションの手順を実行する必要があります
> 。
>
> ストアと認証サービスの両方で、証明書失効モードが同じ値に設定されていることを確認してください
> 。また、すべてのストアが同
> 一の認証構成を使用している場合、
> 複数のストアが単一の認証サービスを共有するように構成できます。

認証サービスの PowerShell コマンドレットには
Set-STFStoreFarmConfiguration に相当する値がないため、PowerShell の使用方法は多少異なります
。前述の証明書失効ポリシーの設定と同じ設定を使用します。

1. PowerShell ISE を開き、［管理者として実行］ を選択します。


```
$SiteID = 1
$StoreVirtualPath = ”/Citrix/Store”
$AuthVirtualPath = ”/Citrix/StoreAuth”
```

2. XML 認証で使用されるストアサービス、認証サービス、Delivery Controller を選択します。Delivery Controller
   が既にストアで構成されていることを確認してください。

```
$StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
    $StoreVirtualPath
$FarmObject = Get-STFStoreFarm -StoreService $StoreObject -
    FarmName ”CVAD”
$AuthObject = Get-STFAuthenticationService -SiteID $SiteID -
    VirtualPath $AuthVirtualPath
```

3. 認証サービスの CertRevocationPolicy
   プロパティを直接編集します。

```
$AuthObject.FarmsConfiguration.CertRevocationPolicy = ”FullCheck”
$AuthObject.Save()
Enable-STFXmlServiceAuthentication -AuthenticationService
    $AuthObject -Farm $FarmObject
```

4. 正しい証明書失効モードを設定したことを確認してください。

```
$AuthObject = Get-STFAuthenticationService -SiteID 1 -VirtualPath
    $AuthVirtualPath
$AuthObject.FarmsConfiguration.CertRevocationPolicy
```

Windows イベントビューアーで予想されるエラー

CRL チェックが有効な場合、エラーは
StoreFront サーバーの Windows イベントビューアーで報告されます。

イベントビューアーを開くには:

- StoreFront サーバーで **Run** と入力します。
- **eventvwr** と入力して、Enter キーを押します。
- [アプリケーションとサービス] で、Citrix Delivery Service イベントを探します。

エラー例: ストアが失効した証明書を使用している **Delivery Controller** に接続できない


```
An SSL connection could not be established: An error occurred during SSL
crytography: Access is denied.

This message was reported from the Citrix XML Service at address https://deliverycontrollerTLS.domain.com/scripts/wpnbr.dll.

The specified Citrix XML Service could not be contacted and has been temporarily
removed from the list of active services.
```

エラー例：**Receiver for Web** で **XML** 認証の失敗によりユーザーがログインできない場合

```
認証処理時に予期されない応答が受信されました。

Citrix.DeliveryServicesClients.Authentication.Exceptions.ExplicitAuthenticationFailure,
Citrix.DeliveryServicesClients.Authentication, Version=3.20.0.0,
Culture=neutral, PublicKeyToken=null

General Authentication Failure

ExplicitResult.State: 5

AuthenticationControllerRequestUrl:
https://storefront.example.com/Citrix/StoreWeb/ExplicitAuth/LoginAttempt

ActionType: LoginAttempt

at
Citrix.Web.AuthControllers.Controllers.ExplicitAuthController.GetExplicitAuthResult(ActionType
type, Dictionary‘2 postParams)
```

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

April 5, 2019

StoreFront のインストールプロセスでは、各 StoreFront サーバーに Windows データストアをローカルにインストールして、サブスクリプションデータを管理します。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 Citrix 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 つのストアとそれに対応するサブスクリプションデータストアを含むデフォルトのシナリオでは、ユーザーは同じリソースに 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。

```
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1__Citrix_<
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 Citrix Virtual Apps and Desktops コントローラー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。次に例を示します:


```
<subscriptionsStoreClient enabled="true">
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1
    __Citrix_External" authenticationMode="windows" transferMode="
    Streamed">
<clientCertificate thumbprint="0" />
</clientEndpoint>
</subscriptionsStoreClient>
```

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:

```
<subscriptionsStoreClient enabled="true">
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1
    __Citrix_Internal" authenticationMode="windows" transferMode="
    Streamed">
<clientCertificate thumbprint="0" />
</clientEndpoint>
</subscriptionsStoreClient>
```

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。

ストアのサブスクリプションデータの管理

December 23, 2019

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:
>
> 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時は、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_<StoreName>
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 later

        $SubsPath = ”C:\Windows\ServiceProfiles\NetworkService\AppData\
            Roaming\Citrix\SubscriptionsStore\1__Citrix_$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、次を参照してください。https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Restore-STFStoreSubscriptions/

1 つの 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。これによって、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。

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
     yourstore>"
2
3 Import-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env
     :USERPROFILE\Desktop\Subscriptions.txt"
```

Import-STFStoreSubscriptions について詳しくは、次を参照してください。https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Import-STFStoreSubscriptions/

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。

```
<user-identifier> <resource-id> <subscription-id> <subscription-status> <
property-name> <property-value> <property-name> <property-value> ...
```


各項目の意味は次の通りです：

- <user-identifier>：必須キーで、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>：必須キーで、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>：必須キーで、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>：必須キーで、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。0 個以上のプロパティ名/値の組み合わせです。StoreFront クライアント（通常は Citrix Workspace アプリ）によるサブスク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「<property-name> <property-value>」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）。

例

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するテキストファイルのサイズ

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

ストアの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

```
1 Get-Counter -Counter ”\Citrix Subscription Store(1__citrix_store)\
    Subscription Entries Count (including unpurged deleted records)”
2
3 Get-Counter -Counter ”\Citrix Subscription Store Synchronization\
    Subscriptions Store Synchronizing”
4
5 Get-Counter -Counter ”\Citrix Subscription Store Synchronization\Number
     Subscriptions Synchronized”
6
7 Get-Counter -Counter ”\Citrix Subscription Store Synchronization\Number
     Subscriptions Transferred”
```


Microsoft SQL Server を使用したサブスクリプションデータの保存

April 2, 2020

> 注:
>
> このドキュメントは、MS SQL Server と T-SQL クエリに関する基本的な知識を前提としています。管理者がこのドキュメントを参照するには、SQL Server を問題なく構成、使用、管理できるようにする必要があります。

はじめに

ESENT は、Windows で使用できる埋め込み可能なトランザクションデータベースエンジンです。StoreFront のすべてのバージョンは、デフォルトで組み込みの ESENT データベースの使用をサポートしています。また、ストアが SQL 接続文字列を使用するように構成されている場合、Microsoft SQL Server インスタンスに接続することもできます。

StoreFront を ESENT ではなく SQL を使用するように切り替えることの主な利点は、T-SQL の UPDATE ステートメントを使用して、サブスクリプションレコードを管理、変更、または削除できることです。SQL を使用すると、サブスクリプションデータでわずかな変更が実行されるたびに ESENT サブスクリプションデータ全体をエクスポート、変更、再インポートする必要はありません。

既存のサブスクリプションデータを ESENT から Microsoft SQL Server に移行するには、StoreFront からエクスポートされた ESENT のフラットデータを、一括インポート用の SQL フレンドリーな形式に変換する必要があります。新しいサブスクリプションデータのない新しい展開の場合、この手順は不要です。データ変換手順が必要なのは一度だけです。ここでは、参照している-STF PowerShell SDK が導入されたバージョン 3.5 以降のすべての StoreFront バージョンで使用できる、サポート対象の構成について説明します。

> 注:
>
> ネットワークの停止が原因で StoreFront がサブスクリプションデータを保存するために使用する SQL Server インスタンスへの接続に失敗した場合、StoreFront 展開は利用不能として表示されません。停止は、ユーザーエクスペリエンスを一時的に低下させるだけです。ユーザーは、SQL Server への接続が復元されるまで、お気に入りのリソースを追加、削除、または表示できません。リソースは、停止でも列挙および起動できます。予測される動作は、ESENT の使用中に Citrix Subscription Store サービスが停止する場合と同じです。
>
> ヒント:
>
> リソースが KEYWORDS:Auto または KEYWORDS:Mandatory で構成されていると、ESENT または SQL で両方を使用する場合と同じように動作します。いずれかの KEYWORD がユーザーのリソースに含まれている場合、ユーザーが最初にログオンすると、新しい SQL サブスクリプションレコードが自動的に作成されます。

ESENT および SQL Server の利点

ESENT	SQL
デフォルト。StoreFront を「そのまま」使用するため追加構成は不要です。	非常に管理しやすい。T-SQL クエリを使用してサブスクリプションデータを簡単に操作または更新できます。ユーザーごとのレコードを削除または更新可能。アプリケーション、Delivery Controller、またはユーザーごとに簡単にレコードをカウントできます。企業/組織から離職したユーザーの不要なユーザーデータを簡単に削除できます。管理者がアグリゲーションの使用に切り替えたときや、新しい Delivery Controller がプロビジョニングされたときなど、Delivery Controller の参照を簡単に更新できます。
サブスクリプションの同期と取得スケジュールを使用して、異なるサーバーグループ間でレプリケーションを簡単に構成できます。「サブスクリプション同期の構成」を参照	StoreFront から切り離されているため、StoreFront をアップグレードする前にサブスクリプションデータをバックアップする必要はありません。データは別の SQL Server で維持されます。サブスクリプションのバックアップは StoreFront に依存せず、SQL のバックアップ戦略とメカニズムを使用します。
サブスクリプション管理が不要な場合、SQL は不要です。サブスクリプションデータを更新する必要がない場合、ESENT の方が顧客のニーズに適している可能性が高くなります。	サーバーグループのすべてのメンバーが共有するサブスクリプションデータの単一コピー。サーバー間のデータの違いやデータ同期の問題が発生する可能性が低くなります。

ESENT および **SQL Server** の欠点

ESENT	SQL
サブスクリプションデータを簡単かつきめ細かく管理する簡単な手段はありません。エクスポートされた.txt ファイルでサブスクリプションの操作を行う必要があります。サブスクリプションデータベース全体をエクスポートおよび再インポートする必要があります。場合によっては、何千ものレコードを検索と置換の手法を使用して変更する必要があります。この手法は手間がかかりエラーの可能性も高くなります。	基本的な SQL の専門知識とインフラストラクチャが必要です。SQL ライセンスの購入が必要になる場合があり、StoreFront 展開の総所有コストが増加します。ただし、Citrix Virtual Apps and Desktops データベースインスタンスを StoreFront と共有してコストを削減することもできます。

ESENT	SQL
サーバーグループ内の各 StoreFront サーバーで ESENT データベースのコピーを保持する必要があります。まれに、このデータベースがサーバーグループ内または異なるサーバーグループ間で同期しなくなることがあります。	サーバーグループ間でのサブスクリプションデータのレプリケーションは、重要な展開タスクです。複数の SQL インスタンスと、データセンターごとに各インスタンス間のトランザクションのレプリケーションが必要です。これには、MS SQL の専門知識が必要です。
	ESENT からのデータ移行および SQL フレンドリーな形式への変換が必要です。このプロセスが必要なのは一度だけです。
	追加の Windows サーバーとライセンスが必要になる場合があります。
	StoreFront を展開するための追加手順。

展開シナリオ

> 注:
>
> ユーザーサブスクリプションをサポートするには、StoreFront 内で構成された各ストアに ESENT データベースまたは Microsoft SQL データベースが必要です。サブスクリプションデータの保存方法は、StoreFront 内のストアレベルで設定されます。

管理の複雑さを軽減し、構成ミスのスコープを減らすために、すべてのストアデータベースを同じ Microsoft SQL Server インスタンスに配置することをお勧めします。

すべて同じ接続文字列を使用するように構成されていれば、複数のストアで同じデータベースを共有できます。異なる Delivery Controller を使用していても問題ありません。複数のストアがデータベースを共有することの欠点は、各サブスクリプションレコードがどのストアに対応するかを知る方法がないことです。

複数のストアを持つ単一の StoreFront 展開では、技術的には 2 つのデータストレージ方法の組み合わせが可能です。ESENT を使用するように 1 つのストアを構成し、別のストアでは SQL を使用するように構成できます。これは、管理の複雑さと構成ミスのスコープがあるためお勧めしません。

SQL
Server にサブスクリプションデータを保存する場合、4 つのシナリオがあります:

シナリオ **1**: **ESENT** を使用する単一の **StoreFront** サーバーまたはサーバーグループ（デフォルト）

デフォルトではバージョン 2.0 以降の StoreFront のすべてのバージョンは、フラット ESENT データベースを使用して、サーバーグループのメンバー間でサブスクリプションデータを保存および複製します。サーバーグループの各メンバーは、サブスクリプションデータベースの同一のコピーを保持し、これはサーバーグループの他のすべてのメンバーと同期されます。このシナリオでは、追加の構成手順は必要ありません。このシナリオは、Delivery

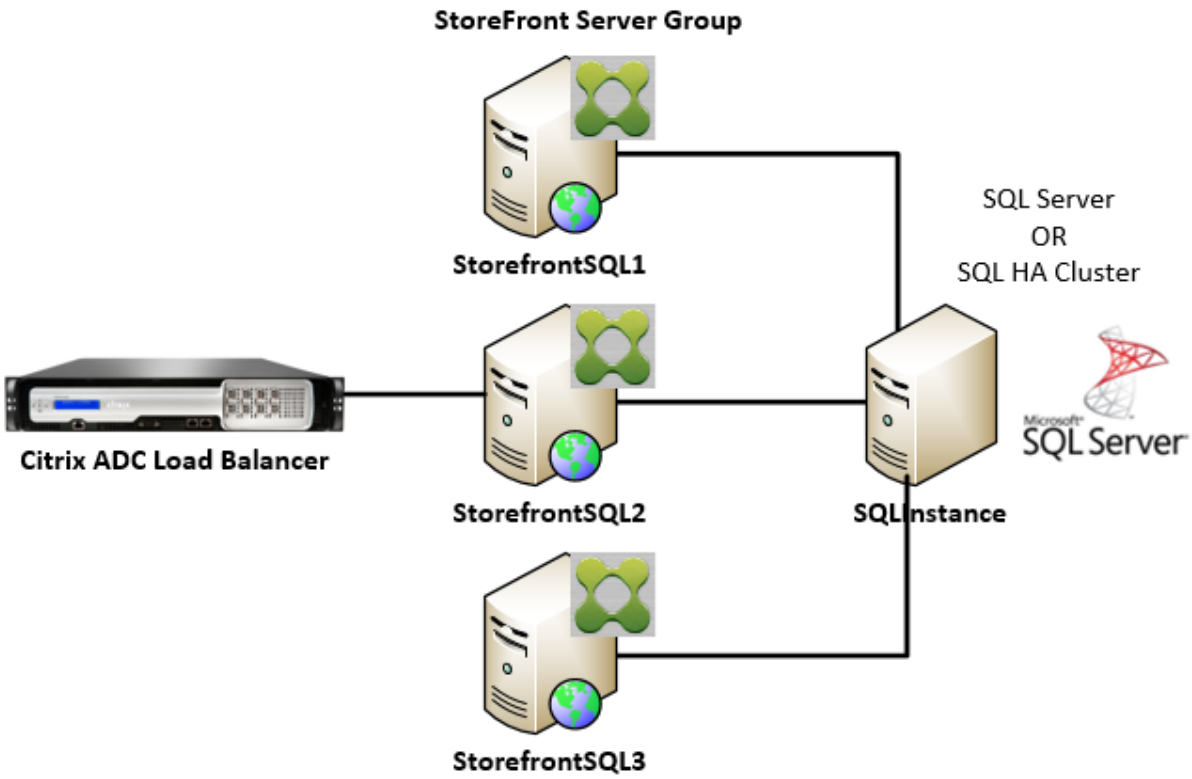
Controller の名前を頻繁に変更しないお客様や、古いユーザーサブスクリプションの削除や更新など、サブスクリプションデータの管理タスクを頻繁に実行する必要がない大半のお客様に適しています。

シナリオ **2**: 単一の **StoreFront** サーバーとローカル **Microsoft SQL Server** インスタンスがインストールされている

StoreFront はローカルにインストールされた SQL Server インスタンスを使用します。両方のコンポーネントは同じサーバー上にあります。このシナリオは、Delivery Controller の名前を頻繁に変更する必要があるお客様や、古いユーザーサブスクリプションの削除や更新など、サブスクリプションデータの管理タスクを頻繁に実行する必要があるものの、高可用性 StoreFront 展開は必要ないお客様のシンプルな単一 StoreFront 展開に適しています。このシナリオは、Microsoft SQL データベースインスタンスをホストするサーバーグループメンバーに単一障害点を作成するため、サーバーグループにはお勧めしません。このシナリオは、大規模なエンタープライズ展開には適していません。

シナリオ **3**: 高可用性用に構成された **StoreFront** サーバーグループおよび専用の **Microsoft SQL Server** インスタンス（推奨）

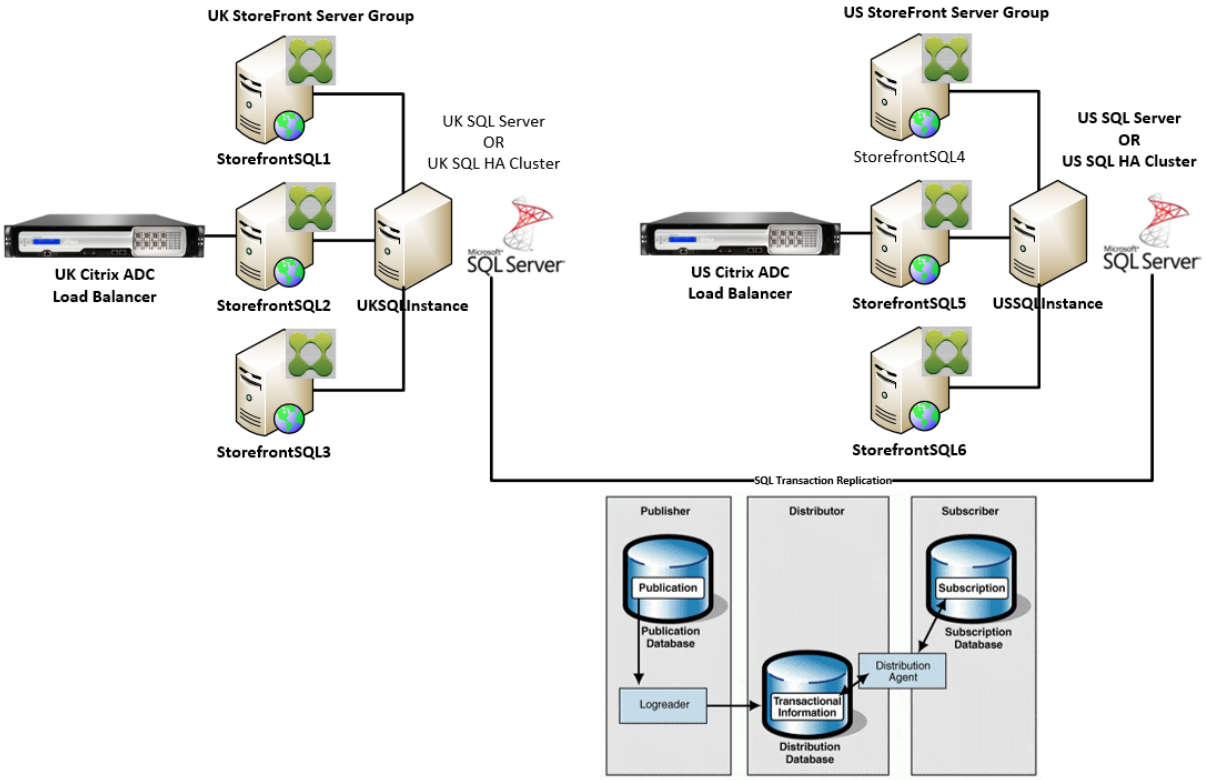
すべての StoreFront サーバーグループメンバーは、同じ専用の Microsoft SQL Server インスタンスまたは SQL フェールオーバークラスターに接続します。これは、Citrix 管理者が Delivery Controller の名前を頻繁に変更する必要性や、古いユーザーサブスクリプションの削除や更新など、サブスクリプションデータの管理タスクを頻繁に実行する必要性があり、高可用性が必要とされる大規模なエンタープライズ展開に適したモデルです。



シナリオ **4**：複数の **StoreFront** サーバーグループ、およびサーバーグループごとの各データセンター内の専用 **Microsoft SQL Server** インスタンス

> 注：
>
> これは高度な構成です。トランザクションレプリケーションに精通した経験豊富な SQL Server 管理者が存在し、正常に展開するために必要なスキルがある場合にのみ実行してください。

これはシナリオ 3 と同様のシナリオですが、異なるリモートデータセンターで複数の StoreFront サーバーグループが必要な状況に応じて拡張されています。Citrix 管理者は、サブスクリプションデータを同じデータセンター内の異なるサーバーグループ間で同期するか、異なるデータセンター内の異なるサーバーグループ間で同期するかを選択できます。データセンター内の各サーバーグループは、冗長性、フェールオーバー、パフォーマンスのために、専用の Microsoft SQL Server インスタンスに接続します。このシナリオでは、Microsoft SQL Server 構成とインフラストラクチャに大幅な追加が必要です。サブスクリプションデータとその SQL トランザクションのレプリケーションは、Microsoft SQL テクノロジに完全に依存しています。



リソース

https://github.com/citrix/sample-scripts/tree/master/storefrontから次のスクリプトをダウンロードできます：

構成スクリプト

- **Set-STFDatabase.ps1** – 各ストアの MS SQL 接続文字列を設定します。StoreFront サーバーで実行します。
- **Add-LocalAppPoolAccounts.ps1** – ローカル StoreFront サーバーのアプリプールに、SQL データベースへの読み取りおよび書き込みアクセスを許可します。SQL Server でシナリオ 2 を実行します。
- **Add-RemoteSFAccounts.ps1** – サーバーグループ内のすべての StoreFront サーバーに、SQL データベースへの読み取りおよび書き込みアクセスを許可します。SQL Server でシナリオ 3 を実行します。
- **Create-StoreSubscriptionsDB-2016.sql** – SQL データベースとスキーマを作成します。SQL Server で実行します。

データの変換およびインポートスクリプト

- **Transform-SubscriptionDataForStore.ps1** – ESENT 内の既存のサブスクリプションデータをインポート用の SQL フレンドリーな形式にエクスポートして変換します。
- **Create-ImportSubscriptionDataSP.sql** – ストアドプロシージャを作成して Transform-SubscriptionDataForStore.ps1 で変換されたデータをインポートします。Create-StoreSubscriptionsDB-2016.sql を使用してデータスキーマを作成後、SQL Server でこのスクリプトを実行します。

SQL Server で StoreFront サーバーのローカルセキュリティグループを構成する

シナリオ **2**: 単一の **StoreFront** サーバーとローカル **Microsoft SQL Server** インスタンスがインストールされている

Microsoft SQL Server で<SQLServer>\StoreFrontServersというローカルセキュリティグループを作成し、IIS APPPOOL\DefaultAppPoolおよびIIS APPPOOL\Citrix Receiver for Webの仮想アカウントを追加してローカルにインストールされた StoreFront が SQL に読み取りおよび書き込みアクセスを許可します。このセキュリティグループは、ストアサブスクリプションデータベーススキーマを作成する.SQL スクリプトで参照されるため、グループ名が一致することを確認してください。

スクリプトAdd-LocalAppPoolAccounts.ps1をダウンロードできます:

Add-LocalAppPoolAccounts.ps1 スクリプトを実行する前に StoreFront をインストールします。このスクリプトは、StoreFront がインストールされ構成されるまで存在しないIIS APPPOOL\Citrix Receiver for Web仮想 IIS アカウントを検出する機能に依存するためです。IIS APPPOOL\DefaultAppPoolは、IIS Web サーバーの役割をインストールすることで自動的に作成されます。

```
# Create Local Group for StoreFront servers on DB Server
$LocalGroupName = "StoreFrontServers"
$Description = "Contains StoreFront Server Machine Accounts or
    StoreFront AppPool Virtual Accounts"

# Check whether the Local Group Exists
```

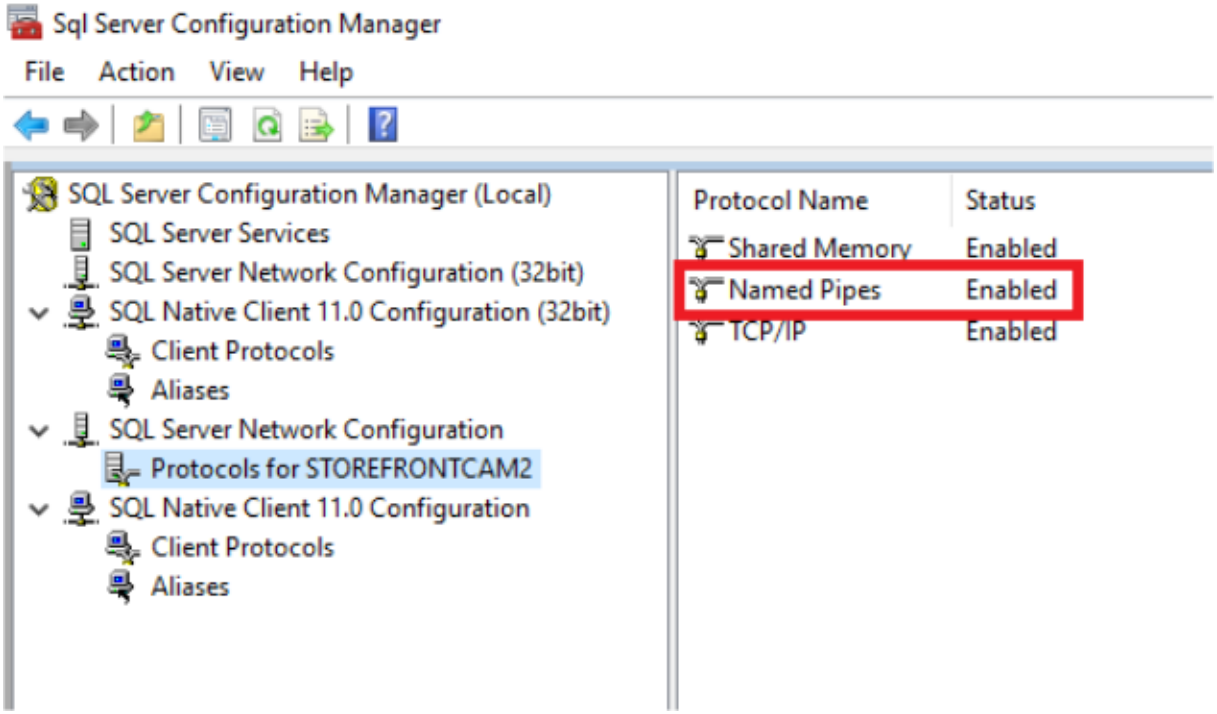


```
6  if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))
7  {
8
9      Write-Host "$LocalGroupName already exists!" -ForegroundColor "
           Yellow"
10  }
11
12 else
13 {
14
15 Write-Host "Creating $LocalGroupName local security group" -
       ForegroundColor "Yellow"
16
17 # Create Local User Group
18 $Computer = [ADSI]"WinNT://$env:ComputerName,Computer"
19 $LocalGroup = $Computer.Create("group",$LocalGroupName)
20 $LocalGroup.setinfo()
21 $LocalGroup.description = $Description
22 $Localgroup.SetInfo()
23 Write-Host "$LocalGroupName local security group created" -
       ForegroundColor "Green"
24  }
25
26 $Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"
27
28 # Add IIS APPPOOL\DefaultAppPool
29 $objAccount = New-Object System.Security.Principal.NTAccount("IIS
       APPPOOL\DefaultAppPool")
30 $StrSID = $objAccount.Translate([System.Security.Principal.
       SecurityIdentifier])
31 $DefaultSID = $StrSID.Value
32
33 $Account = [ADSI]"WinNT://$DefaultSID"
34 $Group.Add($Account.Path)
35
36 # Add IIS APPPOOL\Citrix Receiver for Web
37 $objAccount = New-Object System.Security.Principal.NTAccount("IIS
       APPPOOL\Citrix Receiver for Web")
38 $StrSID = $objAccount.Translate([System.Security.Principal.
       SecurityIdentifier])
39 $WebRSID = $StrSID.Value
40
41 $Account = [ADSI]"WinNT://$WebRSID"
42 $Group.Add($Account.Path)
43
```



```
44  Write-Host ”AppPools added to $LocalGroupName local group” -
        ForegroundColor ”Green”
```

SQL Server 構成マネージャーを使用して、ローカル SQL インスタンス内の名前付きパイプを有効にします。StoreFront と SQL Server のプロセス間通信には名前付きパイプが必要です。

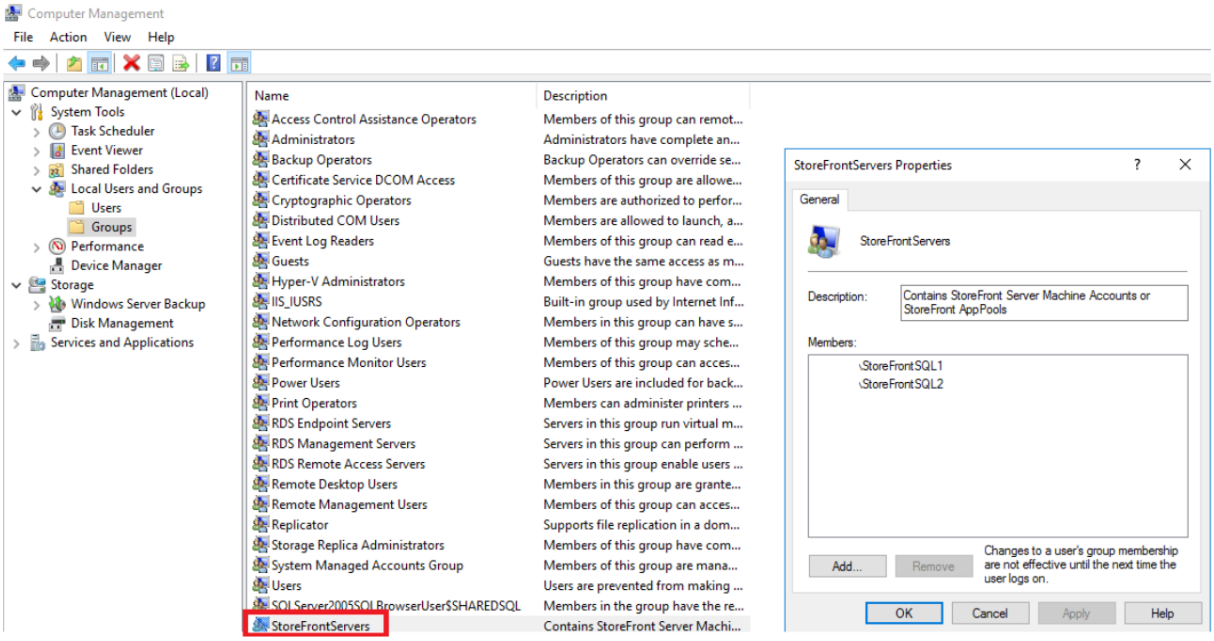


特定のポートまたは動的ポートを使用して SQL Server 接続を許可するように、Windows ファイアウォール規則が正しく構成されていることを確認します。使用中の環境でこれを実行する方法について詳しくは、Microsoft 社のドキュメントを参照してください。

> ヒント:
>
> ローカル SQL インスタンスへの接続に失敗する場合は、localhost または接続文字列で使用される<hostname>が正しい IPv4 アドレスに解決されていることを確認します。Windows は IPv4 の代わりに IPv6 の使用を試み、localhost の DNS 解決は StoreFront および SQL Server の正しい IPv4 アドレスではなく::1 を返すことがあります。この問題を解決するために、場合によってはホストサーバーで IPv6 ネットワークスタックを完全に無効にする必要があります。

シナリオ 3: StoreFront サーバーグループおよび専用の Microsoft SQL Server インスタンス

Microsoft SQL Server で<SQLServer>\StoreFrontServersと呼ばれるローカルセキュリティグループを作成し、StoreFront サーバーグループのすべてのメンバーを追加します。このセキュリティグループは、後から SQL 内にサブスクリプションデータベーススキーマを作成する **Create-StoreSubscriptionsDB-2016.sql** スクリプトで参照されます。



すべての StoreFront サーバーグループのドメインコンピューターアカウントを<SQLServer>\StoreFrontServersグループに追加します。SQL Server が Windows 認証を使用している場合、このグループに登録されている StoreFront サーバーのドメインコンピューターアカウントのみが、SQL でサブスクリプションレコードを読み書きできます。スクリプトAdd-RemoteSFAccounts.ps1で提供される次の PowerShell 関数は、ローカルセキュリティグループを作成し、StoreFrontSQL1 および StoreFrontSQL2 という名前の 2 つの StoreFront サーバーに追加します。

```
function Add-RemoteSTFMachineAccounts
{

[CmdletBinding()]
param([Parameter(Mandatory=$True)][string]$Domain,
[Parameter(Mandatory=$True)][array]$StoreFrontServers)

# Create Local Group for StoreFront servers on DB Server
$LocalGroupName = ”StoreFrontServers”
$Description = ”Contains StoreFront Server Machine Accounts or
    StoreFront AppPool virtual accounts”

# Check whether the Local Security Group already exists
if ([ADSI]::Exists(”WinNT://$env:ComputerName/$LocalGroupName”))
{

    Write-Host ”$LocalGroupName already exists!” -ForegroundColor ”
        Yellow”
 }

```

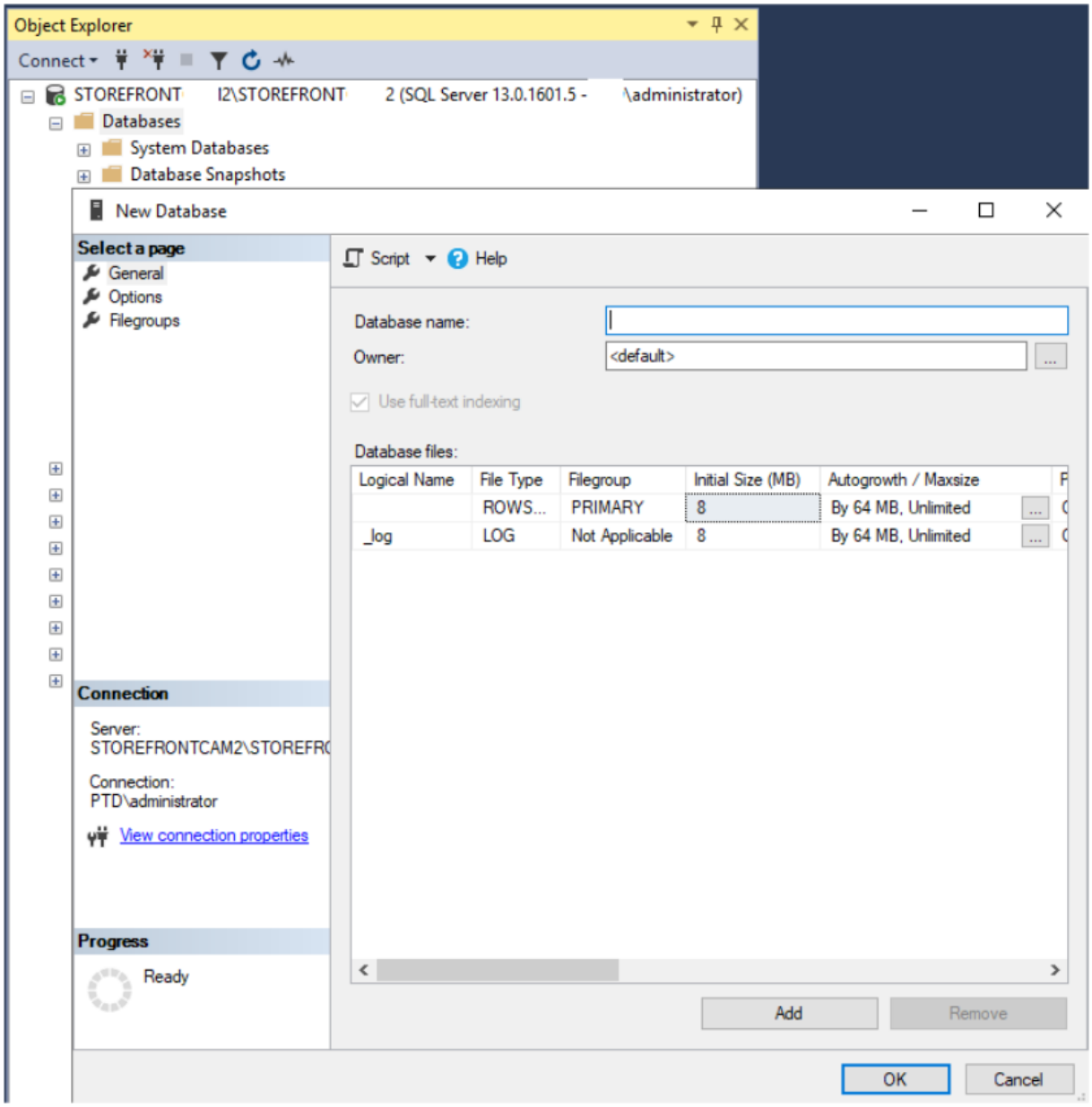


```
19 else
20 {
21
22     Write-Host ”Creating $LocalGroupName local group” -ForegroundColor
       ”Yellow”
23
24     # Create Local Security Group
25     $Computer = [ADSI]”WinNT://$env:ComputerName,Computer”
26     $LocalGroup = $Computer.Create(”group”,$LocalGroupName)
27     $LocalGroup.setinfo()
28     $LocalGroup.description = $Description
29     $Localgroup.SetInfo()
30 Write-Host ”$LocalGroupName local group created” -ForegroundColor ”
       Green”
31  }
32
33 Write-Host ”Adding $StoreFrontServers to $LocalGroupName local group” -
       ForegroundColor ”Yellow”
34
35 foreach ($StoreFrontServer in $StoreFrontServers)
36 {
37
38     $Group = [ADSI]”WinNT://$env:ComputerName/$LocalGroupName,group”
39     $Computer = [ADSI]”WinNT://$Domain/$StoreFrontServer$”
40     $Group.Add($Computer.Path)
41  }
42
43 Write-Host ”$StoreFrontServers added to $LocalGroupName” -
       ForegroundColor ”Green”
44  }
45
46 Add-RemoteSTFMachineAccounts -Domain ”example” -StoreFrontServers @(”
       StoreFrontSQL1”,”StoreFrontSQL2”)
```

Microsoft SQL Server 内でストアごとにサブスクリプションデータベーススキーマを構成する

StoreFront で使用する Microsoft SQL Server に名前付きインスタンスを作成します。使用する SQL のバージョンがインストールされている場所、またはそのデータベースファイルが保存されている場所に対応するように、.SQL スクリプト内のパスを設定します。サンプルスクリプトCreate-StoreSubscriptionsDB-2016.sqlは SQL Server 2016 Enterprise を使用しています。

［データベース］ を右クリックしてから ［新しいデータベース］ を選択し、SQL Server Management Studio（SSMS）を使用して空のデータベースを作成します。



ストアに一致する ［データベース名］ を入力するか、*STFSubscriptions* のような異なる名前を選択します。

スクリプトを実行する前に、StoreFront 展開環境の各ストアでサンプルスクリプトの参照を変更して StoreFront 展開と SQL 展開を一致させます。たとえば、次の項目を変更します:

- 作成する各データベースに`USE [STFSubscriptions]`の StoreFront のストア名と一致する名前を付けます。
- データベースの.mdf ファイルと.ldf ファイルへのパスを、データベースを保存する場所に設定します。

  ```
  C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\
  STFSubscriptions.mdf

  C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\
  ```

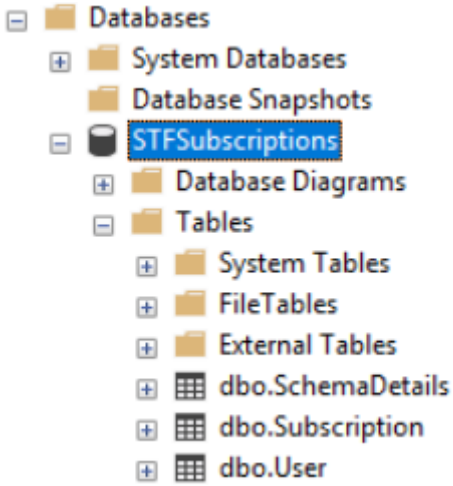


```
STFSubscriptions.ldf
```

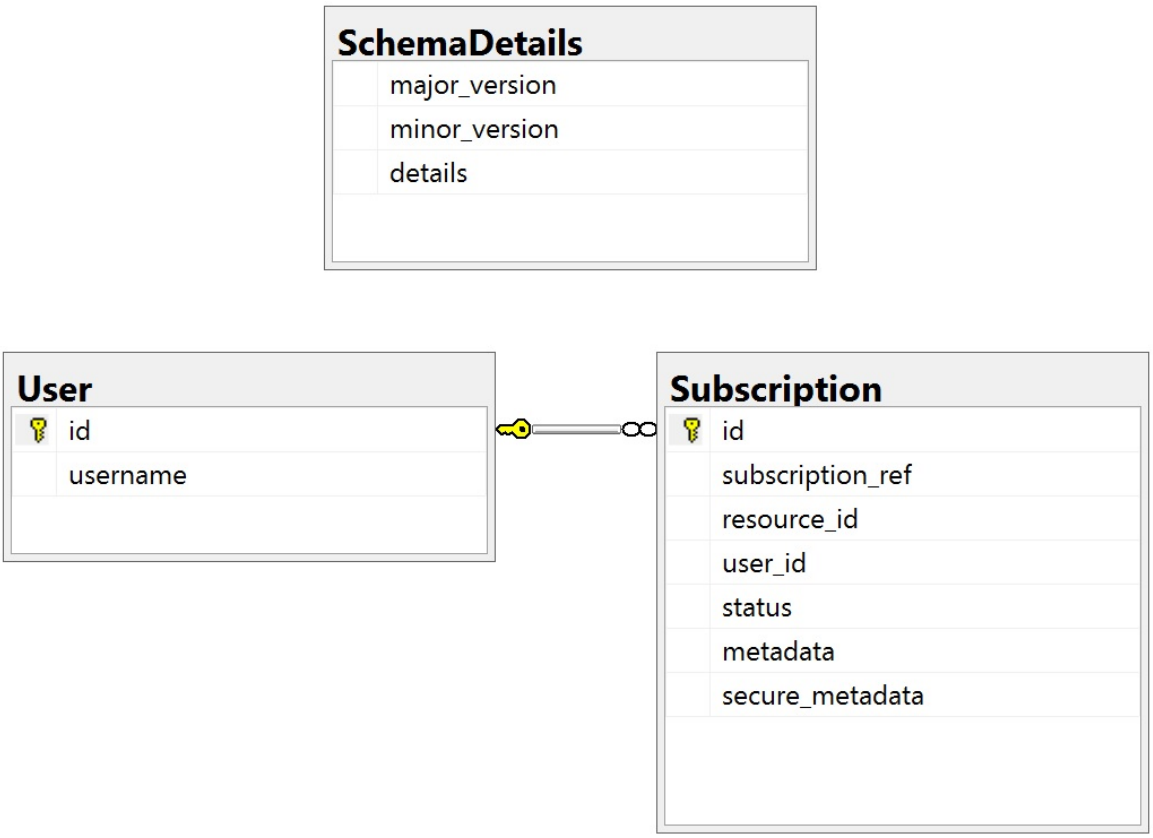
- スクリプト内で SQL Server の名前への参照を設定します:

```
CREATE LOGIN [SQL2016\StoreFrontServers] FROM WINDOWS;

ALTER LOGIN [SQL2016\StoreFrontServers]
```

スクリプトを実行します。スキーマが正常に構成されると、次の 3 つのデータベーステーブルが作成されます: *SchemaDetails*、*Subscription*、*User*。



次のデータベース図は、*Create-StoreSubscriptionsDB-2016.sql* スクリプトが作成したサブスクリプションデータベーススキーマです。



各 **StoreFront** ストアの **SQL Server** 接続文字列を構成する

シナリオ **1**

> ヒント：
>
> ESENT データベースのディスクに保存されている元のサブスクリプションデータは、破棄または削除されません。Microsoft SQL Server から ESENT の使用に戻す場合、ストア接続文字列を削除して、元のデータの使用に切り替えることができます。ストアで SQL が使用されている間に作成された追加のサブスクリプションは ESENT に存在せず、ユーザーにはこれらの新しいサブスクリプションレコードは表示されません。元のサブスクリプションレコードはすべて、引き続き存在します。

ストアでの **ESENT** サブスクリプションを再度有効にするには

PowerShell ISE を開き、［管理者として実行］ を選択します。

-UseLocalStorage オプションを使用して、ESENT サブスクリプションを再度有効にするストアを指定します：

```
$SiteID = 1
$StoreVirtualPath = ”/Citrix/Store1”

```



```
# Sets SQL DB Connection String
$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath
    $StoreVirtualPath

# Removes the SQL DB Connection string and reverts back to using ESENT
Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
    UseLocalStorage
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
```

シナリオ **2**、**3**、**4**

PowerShell ISE を開き、［管理者として実行］ を選択します。

$StoreVirtualPath を使用して接続文字列を設定するストアを指定します。

```
$SiteID = 1
$VirtualPath= "/Citrix/Store1"
$DBName = "Store1"
$DBServer = "SQL2016Ent"
$DBLocalServer = "localhost"
$DBInstance = "StoreFrontInstance"

# For a remote database instance
$ConnectionString = "Server=$DBServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;" Database=$DBName;Trusted_Connection=True;"
```

または

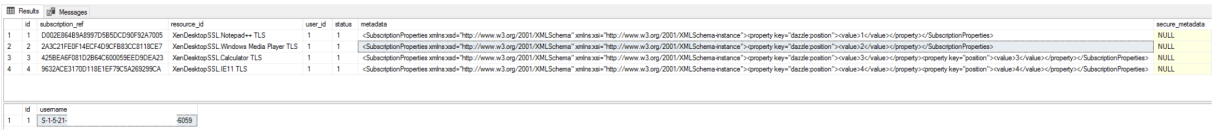
```
# For a locally installed database instance
$ConnectionString = "$DBLocalServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;"

# Sets SQL DB Connection String
$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath "/
    Citrix/Store"
Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
    ConnectionString $ConnectionString
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
```

すべてのストアで SQL 接続文字列を使用するように構成する場合は、展開内のすべてのストアに対してこのプロセスを繰り返します。

ESENT から **Microsoft SQL Server** に既存のデータを移行する

既存の ESENT データを SQL に移行するには、2 段階のデータ変換プロセスが必要です。この一度のみの操作を実行するために役立つ 2 つのスクリプトが提供されています。StoreFront の接続文字列と SQL インスタンスが正しく構成されている場合、新しいサブスクリプションはすべて SQL 内で正しい形式で自動的に作成されます。移行後、過去の ESENT サブスクリプションデータは SQL 形式に変換され、ユーザーは以前にサブスクライブしたリソースも表示できます。

例：同じドメインユーザーの **4** つの **SQL** サブスクリプション



手順 **1 Transform-SubscriptionDataForStore.ps1** スクリプトを使用して、**ESENT** データを一括インポート用の **SQL** フレンドリー形式に変換する

ESENT データを変換する StoreFront サーバーにログインします。

サーバーグループのすべてのメンバーに同じ数のサブスクリプションレコードが含まれている場合、どのメンバーでも使用できます。

PowerShell ISE を開き、［管理者として実行］ を選択します。

スクリプトTransform-SubscriptionDataForStore.ps1を実行すると、<StoreName>.txtファイルが ESENT データベースから現在のユーザーのデスクトップにエクスポートされます。

PowerShell スクリプトは、デバッグを支援し、操作の成功を評価するために処理される各サブスクリプション行に関する詳細なフィードバックを提供します。この処理には時間がかかる場合があります。

変換されたデータはスクリプトが完了した後、現在のユーザーのデスクトップの<StoreName>SQL.txtに書き出されます。このスクリプトは、一意のユーザーレコード数と処理されたサブスクリプションの総数をまとめます。

SQL Server に移行するストアごとにこの処理を繰り返します。

手順 **2 T-SQL** ストアドプロシージャを使用して変換されたデータを一括 **SQL** インポートする

一度に 1 つのストアのデータのみをインポートする必要があります。

手順 1 で作成された<StoreName>SQL.txtファイルを StoreFront サーバーのデスクトップから Microsoft SQL Server のC:\にコピーして、SubscriptionsSQL.txt に名前を変更します。

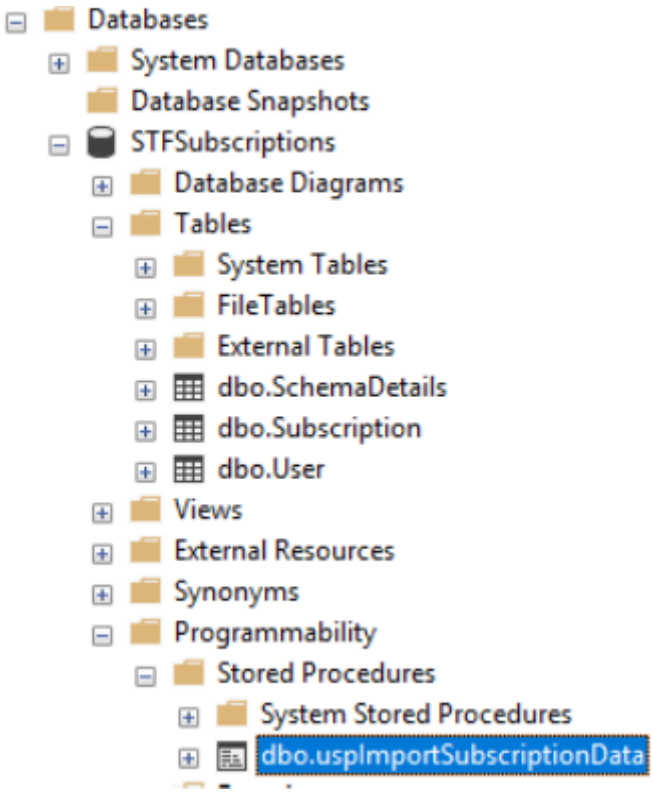
Create-ImportSubscriptionDataSP.sqlスクリプトは T-SQL ストアドプロシージャを作成して、サブスクリプションデータを一括インポートします。一意のユーザーごとに重複するエントリが削除されるため、結果の SQL データは正しく正規化され、正しいテーブルに分割されます。

Create-ImportSubscriptionDataSP.sql を実行する前に、`USE [STFSubscriptions]`を変更してストアドプロシージャを作成するデータベースに一致させます。

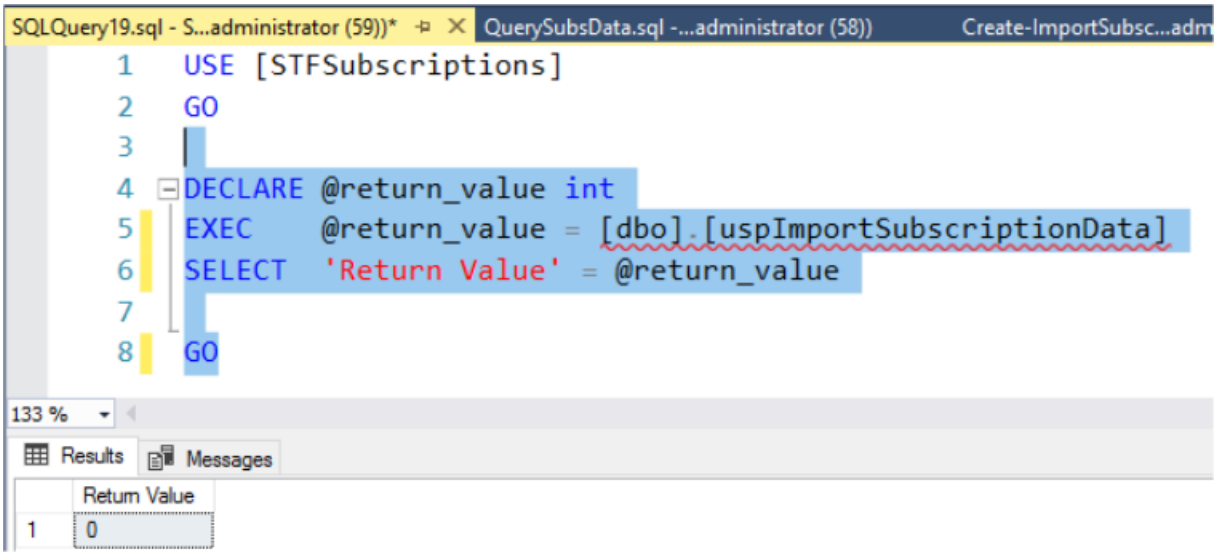
SQL Server Management Studio を使用して *Create-ImportSubscriptionDataSP.sql* ファイルを開き、その中のコードを実行します。このスクリプトは *ImportSubscriptionDataSP* ストアドプロシージャを以前に作成したデータベースに追加します。

ストアドプロシージャが正常に作成されると、SQL コンソールに次のメッセージが表示され、ImportSubscriptionDataSP ストアドプロシージャがデータベースに追加されます:

```
Commands completed successfully.
```



ストアドプロシージャを右クリックして実行し、［ストアドプロシージャの実行］ を選択し ［**OK**］ をクリックします。



戻り値 0 は、すべてのデータが正常にインポートされたことを示します。インポートに関する問題はすべて SQL コンソールに記録されます。ストアドプロシージャが正常に実行された後、サブスクリプションレコードの合計数と以下の 2 つの SQL クエリの結果とともにTransform-SubscriptionDataForStore.ps1が提供する一意のユーザー数を比較します。2 つの合計数は一致する必要があります。

変換スクリプトからのサブスクリプションの総数は、SQL から報告される合計数と一致する必要があります。

```
SELECT COUNT(*) AS TotalSubscriptions
FROM [Subscription]
```

変換スクリプトからの一意のユーザー数は、SQL から報告される User テーブルのレコード数と一致する必要があります。

```
SELECT COUNT(*) AS TotalUsers
FROM [User]
```

変換スクリプトで 100 の一意のユーザーと 1000 の合計サブスクリプションレコードが表示された場合、移行が成功した後、SQL で同じ 2 つの数値が表示される必要があります。

StoreFront にログインして、既存のユーザーがサブスクリプションデータを表示できるかどうかを確認します。ユーザーがリソースをサブスクライブしたり、サブスクリプションを解除したりすると、既存のサブスクリプションレコードが SQL で更新されます。新しいユーザーとサブスクリプションレコードも SQL で作成されます。

手順 **3** インポートされたデータで **T-SQL** クエリを実行する

> 注:
>
> Delivery Controller の名前はすべて大文字と小文字が区別され、StoreFront 内で使用される名前および大文字と小文字に正確に一致する必要があります。


```
-- Get all SQL subscription records
Use [STFSubscriptions]
SELECT * FROM [Subscription]
SELECT * FROM [User]
```

```
-- Get all subscription records for a particular user SID
Use [STFSubscriptions]
SELECT * FROM [Subscription]
INNER JOIN [User]
ON [Subscription].[user_id] = [User].[id]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'

-- Get total number of Subscription records for a particular user SID
Use [STFSubscriptions]
SELECT COUNT(Subscription.id)
FROM [Subscription]
INNER JOIN [User]
ON [Subscription].[user_id] = [User].[id]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'
```

```
-- Get all subscription records for a particular delivery controller
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] LIKE 'DeliveryController.%'

-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'

-- Get all subscription records for a particular application
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] = ' DeliveryController.Application'
```

T-SQL を使用して既存のサブスクリプションレコードを更新または削除する

> 免責:
>
> すべてのサンプル SQL UPDATE および DELETE ステートメントは、完全にお客様の責任において使用されま

> す。Citrix は、提供された例を誤って使用したことによるサブスクリプションデータの損失または偶発的な変更について責任を負いません。以下の T-SQL ステートメントは、簡単な更新を実行できるようにするためのガイドとして提供されています。サブスクリプションの更新または古いレコードの削除を試みる前に、SQL データベースの完全バックアップですべてのサブスクリプションデータのバックアップを作成してください。必要なバックアップの実行に失敗すると、データの損失または破損が発生する可能性があります。独自の T-SQL UPDATE または DELETE ステートメントを実稼働データベースに実行する前に、実際の実稼働データベースから離れてダミーデータまたは実稼働データの冗長コピーでテストします。
>
> 注:
>
> Delivery Controller の名前はすべて大文字と小文字が区別され、StoreFront 内で使用される名前および大文字と小文字に正確に一致する必要があります。

```
-- Update the delivery controller used in all subscriptions.
Use [STFSubscriptions]
UPDATE [Subscription]
SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
    NewDeliveryController.')
WHERE [resource_id] LIKE 'OldDeliveryController.%'

-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
UPDATE [Subscription]
SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
    DefaultAggregationGroup.')
WHERE [resource_id] LIKE 'OldDeliveryController.%'
```

```
-- Delete all subscription records for a particular Delivery Controller
Use [STFSubscriptions]
DELETE FROM [Subscription]
WHERE [resource_id] LIKE 'DeliveryController.%'

-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'

-- Delete all subscription records for a particular application
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] LIKE '%.Application'

-- Delete all subscription records for an application published via a
```

```
    specific delivery controller
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] = 'DeliveryController.Application'
```

```
-- Delete all subscription records for a particular user SID
Use [STFSubscriptions]
DELETE FROM [Subscription]
INNER JOIN [User]
ON [Subscription].[user_id] = [User].[id]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'

Use [STFSubscriptions]
DELETE FROM [User]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'
```

```
-- Delete ALL subscription data from a particular database and reset
    the primary key clustered index to start numbering from 0.
-- USE WITH EXTREME CARE AND NOT ON LIVE PRODUCTION DATABASES.
-- Can be useful whilst debugging data import issues to start with a
    clean database.

Use [STFSubscriptions]
DELETE FROM [Subscription]
DBCC CHECKIDENT ([Subscription], RESEED, 0)
DELETE FROM [User]
DBCC CHECKIDENT ([User], RESEED, 0)
```

上級ストア設定

April 2, 2020

［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。

> 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。完了したら、構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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。

アドレスの解決の種類

［詳細設定］ ページを使って、サーバーから要求する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、次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

フォントスムージングを許可する

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［オン］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］ オプションを選択し、［**OK**］ をクリックします。

セッションの再接続を許可する

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［オン］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］ オプションを選択し、［**OK**］ をクリックしてセッションの再接続を有効にします。

特殊なフォルダーのリダイレクトを許可する

［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］ オプションを選択するか選択解除することで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。

バックグラウンドヘルスチェックポーリング期間

StoreFront は、各 Citrix Virtual Desktops ブローカーや Citrix Virtual Apps サーバー上で定期的にヘルスチェックを実行し、サーバーの可用性に対する断続的な影響を軽減させます。デフォルトは 1 分毎（00:01:00）です。［詳細設定］ 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。

通信のタイムアウト期間

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。

接続タイムアウト

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、初期接続が確立するまでの待機秒数を指定して、［**OK**］ をクリックします。

拡張列挙を有効にする

このオプションでは、複数の Citrix Virtual Apps and Desktops サイトにわたってアプリやデスクトップを列挙する場合、StoreFront が Delivery Controller に対してクエリを同時に実行するか、連続して実行するかを制御できます。同時列挙は、複数サイト間のリソースを集約する場合に、ユーザーのクエリにより高速に応答できるいようにします。（デフォルトで）このオプションが選択されている場合、StoreFront はすべての Delivery Controller に同時に列挙要求を送信し、すべての応答を受信後に応答を集約します。［同時列挙の最大数］ および ［同時列挙の最小ファーム数］ オプションを使用して、この動作を調整できます。

［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］ オプションを選択（または選択解除）し、［**OK**］ をクリックします。

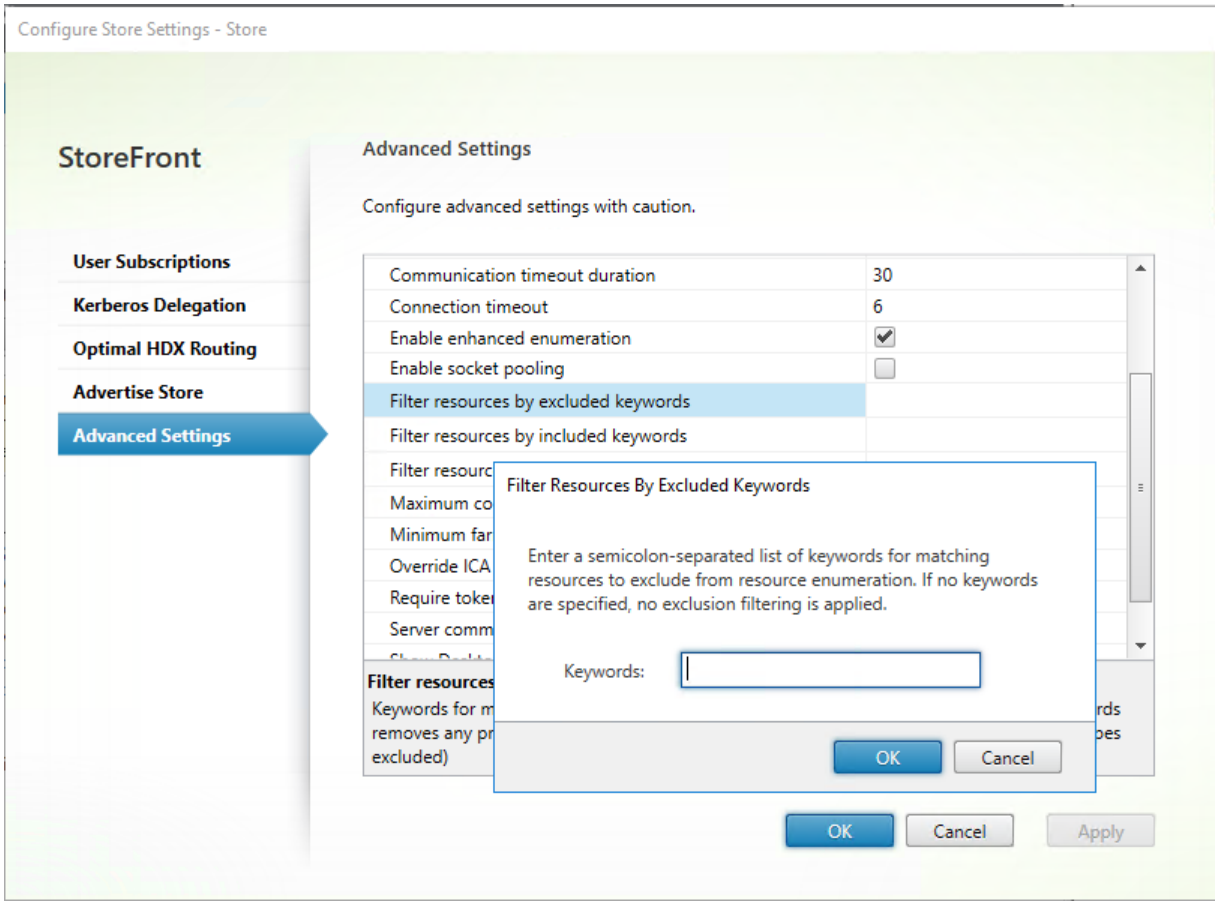
ソケットプール機能を有効にする

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］ オプションを選択して、［**OK**］ をクリックしてソケットプール機能を有効にします。

リソースを除外キーワードでフィルターする

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。



リソースを包含キーワードでフィルターする

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。

リソースを種類でフィルターする

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。

同時列挙の最大数

すべての Delivery Controller に送信する同時要求の最大数を指定します。このオプションは、［拡張列挙を有効にする］ オプションが有効になっている場合に機能します。デフォルト値は 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、数値を入力してから ［**OK**］ をクリックします。

同時列挙の最小ファーム数

同時列挙をトリガーするために必要な Delivery Controller の最小数を指定します。このオプションは、［拡張列挙を有効にする］ オプションが有効になっている場合に機能します。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 クライアント名を上書きする

.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 Workspace アプリによってクライアント名が指定されます。デフォルトは［オフ］です。

［詳細な設定］ タスクを使用し、［**ICA** クライアント名を上書きする］ オプションを選択して、［**OK**］ をクリックします。

トークンの一貫性を要求する

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［オン］です。

［詳細な設定］ タスクを使用し、［トークンの整合性を要求する］ オプション選択して、［**OK**］ をクリックします。

サーバー通信試行回数

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、数値を入力してから ［**OK**］ をクリックします。

デスクトップビューアーを有効にする

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［オフ］です。

［詳細な設定］タスクを使用し、［古いクライアントで **Desktop Viewer** を表示する］オプションを選択して、［**OK**］をクリックします。

Citrix Receiver for Web サイトの管理

January 14, 2020

Citrix Receiver for Web サイトは、アプリストアとして使用される Web サイトです。ユーザーはブラウザーでサイトを開き、Citrix Virtual Apps and Desktops を使用して公開されたアプリケーション、データ、デスクトップに安全にアクセスできます。

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:

タスク	詳細
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。

タスク	詳細
統合ユーザーエクスペリエンス	StoreFront は、統合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。
お勧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。
HTML5 向け Citrix Workspace アプリのブラウザータブ使用の構成	ユーザーが Citrix Receiver for HTML5 または HTML5 向け Citrix Workspace アプリ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見なされます。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

April 2, 2020

管理者が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。既存のストアに Citrix Receiver for Web サイトを追加できます。

> 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。完了したら、
> 構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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。目的の **Web** サイトパスを入力し、［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、［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 Workspace アプリ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 Workspace アプリが検出されない場合は、自分のプラットフォームに適した Citrix Workspace アプリをシトリックスの Web サイトからダウンロードしてインストールするよう求められます。この動作の変更について詳しくは、「Citrix Workspace アプリをインストールしていないユーザーがアクセスしたときのサイトの動作を構成する」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 Workspace アプリをインストールする必要があります。ただし、Receiver for Web サイトの HTML5 向け Citrix Workspace アプリを有効にすると、Citrix Workspace アプリ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

April 2, 2020

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。完了したら、
> 構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

認証方法の選択

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、［認証方法の管理］タスクを使用します。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、［ストア］ペインで変更するストアを選択します。
3. ［ストア］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］ 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］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時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］ 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 または Windows 向け Citrix Workspace アプリをユーザーデバイスにインストールする時にパススルー認証を有効にする必要があります。

     > 注：
     >
     > 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 でのみサポートされます。

   - スマートカード認証を有効にするには、［スマートカード］ をオンにします。ユーザーは、ストアにアクセスするときに、スマートカードと PIN を使用して認証されます。
   - Citrix Gateway からのパススルー認証を有効にするには、［**Citrix Gateway** からのパススルー］ をオンにします。ユーザーは Citrix 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. 認証方法の選択後、［**OK**］ をクリックします。

   認証方法の設定を変更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。

ほかの **Web** サイトにリソースのショートカットを追加する

内部ネットワーク上でホストされている信頼される 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。

リソースのショートカットを生成する前に、Citrix StoreFront 管理コンソールまたは PowerShell を使用して、ホスト Web サイトの URL を「信頼できる URL」一覧に追加する必要があります。信頼できる URL は、Citrix Receiver for Web サイトの web.config ファイルの<trustedUrls>セクションに一覧表示されています。web.config ファイルは通常、C:\inetpub\wwwroot\Citrix\storenameWeb\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。

デフォルトでは、信頼できない Web サイトからのリソースショートカットを起動しようとするユーザーに警告が表示されますが、ユーザーは引き続きリソースの起動を選択できます。これらの警告が表示されないようにするには、［ストア］ペインで ［**Receiver for Web** サイトの管理］、［構成］ で［詳細な設定］ を選択して、［信頼できないショートカットについてメッセージを表示する］ オプションのチェックをオフにします。

管理コンソールを使用して信頼できる **Web** サイトを追加する

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 ブラウザーに表示された 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。

PowerShell を使用して信頼できる **Web** サイトを追加する

https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Citrix.StoreFront.SubscriptionsStore/の説明どおりに **Set-STFWebReceiverApplicationShortcuts** PowerShell コマンドレットを使用して「信頼できる」URL を追加できます。

セッションのタイムアウトの設定

デフォルトでは、Citrix Receiver for Web サイト上のユーザーセッションは、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。

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

[**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。

ユーザーへのプロビジョニングファイルの提供を停止する

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 または Citrix Workspace アプリでストアを自動で構成できます。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（Citrix Gateway 展開環境やビーコンの詳細など）が定義されています。この記事では、「Citrix Workspace アプリ」に関する記載は、特に明記されていない限り、サポートされているバージョンの Citrix Receiver にも適用されます。

［**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/Workspace** アプリの構成を有効にする］ を選択します。

Citrix Workspace アプリをインストールしていないユーザーがアクセスしたときのサイトの動作を構成する

Citrix Workspace アプリ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時の Citrix Receiver for Web サイトの動作を構成するには、［**Citrix Receiver/Workspace** アプリの展開］ 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 Workspace アプリ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 Workspace アプリが検出されない場合は、プラットフォームに適した Citrix Workspace アプリ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場所はシトリックスの Web サイトですが、Citrix Workspace アプリのインストーラーを StoreFront サーバーにコピーして、ユーザーが StoreFront サーバーから直接ダウンロードできるようにすることもできます。

Citrix Workspace アプリをインストールできないユーザーの場合は、Citrix Receiver for Web サイトで HTML5 向け Citrix Workspace アプリを有効にすることができます。HTML5 向け Citrix Workspace アプリを使用すると、Citrix Workspace アプリをインストールしなくても、HTML5 対応の Web ブラウザー内でデスクトップやアプリケーションに直接アクセスできます。内部ネットワーク接続と Citrix Gateway を介した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、HTML5 向け Citrix Workspace アプリ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 Citrix 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 Citrix Virtual Apps and Desktops で提供されるリソースに HTML5 向け Citrix Workspace アプリでアクセスすることはできません。HTML5 向け Citrix Workspace アプリ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、Citrix Virtual Apps and Desktops 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。Citrix Virtual Apps and Desktops は、HTML5 向け Citrix Workspace アプリへの接続にポート 8008 を使用します。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。

StoreFront に直接接続するときに、Citrix Virtual Apps and Desktops リソースが HTML5 向け Citrix Workspace アプリを使用して正常に起動するには、アプリとデスクトップをホストする VDA への TLS 接続を構成

する必要があります。Citrix Gateway を介したリモート接続では、VDA への TLS 接続を設定せずに、HTML5 向け Citrix Workspace アプリを使用してリソースを起動できます。

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。［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/Workspace** アプリの展開］ を選択して、［展開オプション］ を指定します。
   - ［常に **Receiver for HTML5** を使用］ を選択して、毎回 Citrix Workspace アプリのダウンロードとインストールを要求されることなく、HTML5 対応 Web ブラウザーでサイトが常にリソースにアクセスできるようにします。このオプションを選択すると、HTML5 対応 Web ブラウザーを使用しているユーザーは、常に HTML5 向け Citrix Workspace アプリ経由でサイトのデスクトップやアプリケーションにアクセスできます。HTML5 対応 Web ブラウザーを使用していないユーザーは、リソースにアクセスできません。ローカルにインストールされている Citrix Workspace アプリからのアクセスは無効になっています。
   - ［ローカルの **Receiver** が使用できない場合は **Receiver for HTML5** を使用する］ を選択して、Citrix Workspace アプリ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サイトに表示されるようにし、インストールできない場合は HTML5 向け Citrix Workspace アプリが使用できるようにします。この場合、Citrix Workspace アプリ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 Workspace アプリ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。
   - ［ローカルにインストール］ を選択して、常にローカルにインストールされた Citrix Workspace アプリからアクセスするようにします。ユーザは使用しているプラットフォームに対応した Citrix Workspace アプリをダウンロードしてインストールするよう求められます。HTML5 対応 Web ブラウザー経由のアクセスは無効になっています。
     - ［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 Workspace アプリを使用できない場合は、Citrix Receiver for Web によりユーザーは Citrix Workspace アプリ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 ではログオン時に Citrix Workspace アプリクライアントをアップグレードするかどうかをユーザーが選択できます。ユーザーはアップグレードをスキップすることもでき、Citrix Receiver for Web のブラウザーの Cookie が消去されない限り、アップグレードを求めるメッセージが再度表示されることはありません。この機能を有効にするには、StoreFront サーバー上で Citrix Workspace アプリファイルを使用できるようにしてください。
     - ドロップダウンリストからソースを選択します。

Citrix Workspace アプリの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

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 Workspace アプリ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 Workspace アプリが検出されない場合は、シトリックスの Web サイトから、または StoreFront サーバーから適切なインストーラーをダウンロードして、自分のプラットフォームに適した Citrix Workspace アプリをダウンロードしてインストールするように求められます。

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/Workspace** アプリの展開］ と ［**Receiver/Workspace** アプリのソース］ を選択し、インストールファイルを参照します。

ログオン後にプロンプトを実行して **Citrix Workspace** アプリをインストールする

Citrix Receiver for Web では、StoreFront にログオンする前に、最新の Citrix Workspace アプリがユーザーのコンピューターにインストールされていない場合は、インストールするように求められます。構成により異なりますが、インストール済みの Citrix Workspace アプリ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. ［詳細の設定］ を選択し、［ログオン後に **Citrix Receiver/Workspace** アプリのインストールメッセージを表示］ をオンにします。

Citrix Receiver for Web サイトの削除

［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。

統合ユーザーエクスペリエンスのサポート

April 2, 2020

> 注:
>
> 「StoreFront」（この名称に変更はありません）は、Citrix Virtual Apps and Desktops サイトからアプリケーションとデスクトップを集約して、使いやすい単一のストアとして機能するエンタープライズアプリストアです。Citrix Receiver のテクノロジーは Citrix Workspace アプリに含まれるようになりました。現在、製品と製品ドキュメントで移行作業が行われています。統合エクスペリエンスで「Citrix Receiver」を使用するなど、

> 製品内コンテンツには古い名称が含まれる場合があります。この移行の間はご迷惑をおかけしますが、何卒ご容赦願います。新しい名前について詳しくは、https://www.citrix.com/about/citrix-product-guide/を参照してください。

StoreFront は、統合ユーザーエクスペリエンスをサポートします。統合エクスペリエンスにより、集中管理された HTML5 ユーザーエクスペリエンスがすべての Web およびネイティブ Citrix Workspace アプリで体感できます。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 を使用して作成されたストアでは、統合エクスペリエンスが使用されます。

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。

Javascript と CSS を使ってCitrix Receiver for Web ページをカスタマイズ。

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:
>
> XenApp 6.x を使用している場合、［クライアントへのストリーム配信］ または ［可能な場合はストリーム配信、それ以外の場合はサーバーからアクセス］ に設定されているアプリケーションは、統合エクスペリエンスを有効にしてもサポートされません。

Citrix Receiver for Web の **Web** サイトの作成

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。

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

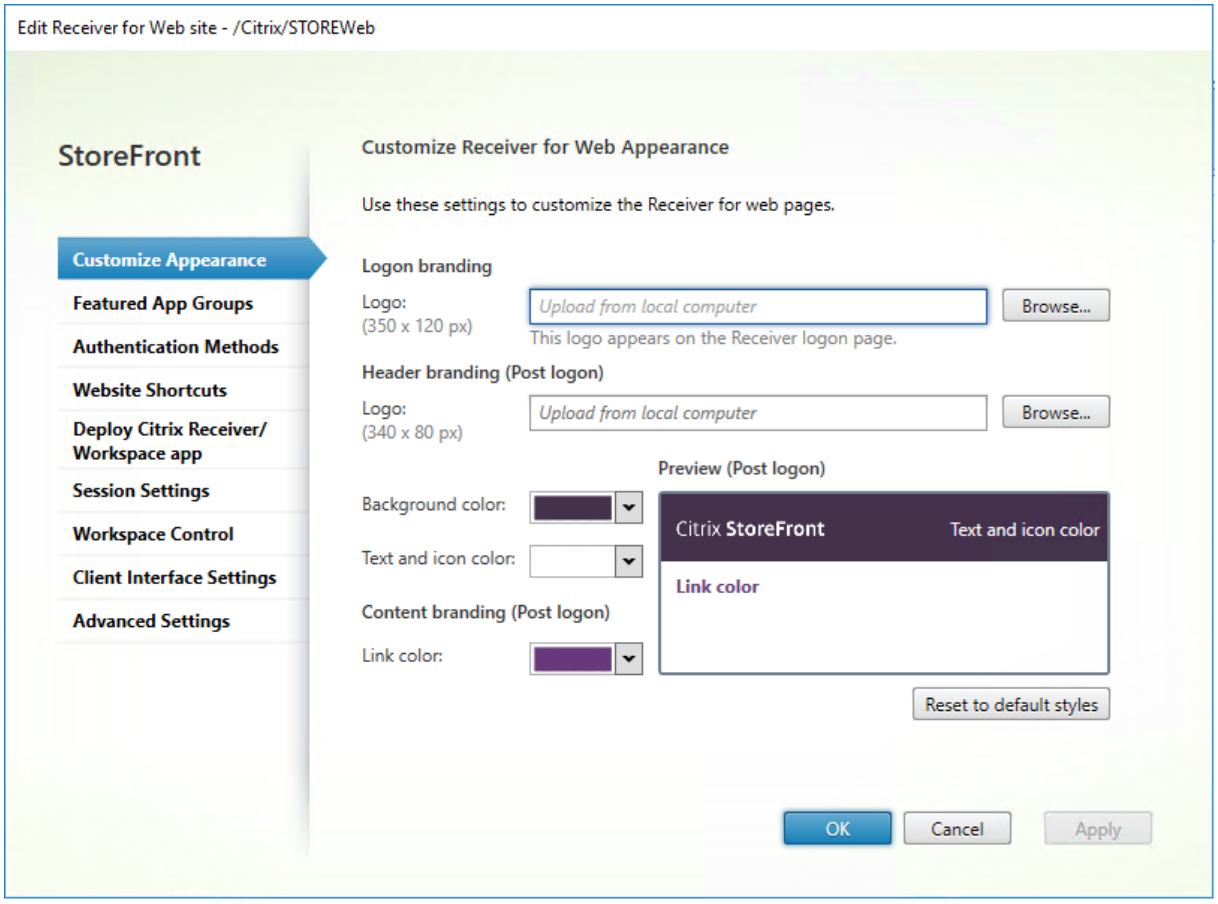
StoreFront を使って新しいストアが作成されると、Citrix Receiver for Web サイトが自動的に作成され、ストアに割り当てられます。Citrix Receiver for Web サイトは統合エクスペリエンスを使用します。ストアに複数の Receiver for Web サイトがある場合、ユーザーが Citrix Workspace アプリを使用してストアにアクセスしたときにどの Receiver for Web サイトを表示するかを選択する必要があります。

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、中央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。作成された Citrix Receiver for Web の Web サイトがない場合は、Receiver for Web サイトの追加ウィザードへのリンクを含むメッセージが表示されます。
3. ユーザーがこのストアにアクセスしたときに Citrix Workspace アプリクライアントが表示するデフォルトの Receiver for Web サイトを選択します。
4. ［**OK**］ をクリックします。

Citrix Receiver の外観のカスタマイズ

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. ［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。



Javascript と **CSS** による追加のカスタマイズ

> 注:
>
> このセクションの例では、C:\inetpub\wwwroot\Citrix\StoreWeb\custom などにある *script.js* ファイルに Javascript を追加し、同じディレクトリの *style.css* ファイルに CSS を追加します。

Receiver for Web のログインページに静的ヘッダーを追加

ここで「静的」とは、ウェルカムメッセージや会社名などの固定のテキストのことです。ニュースメッセージやサーバーの状態などのように変化する場合は、Receiver for Web のログインページに動的ヘッダーを追加します。

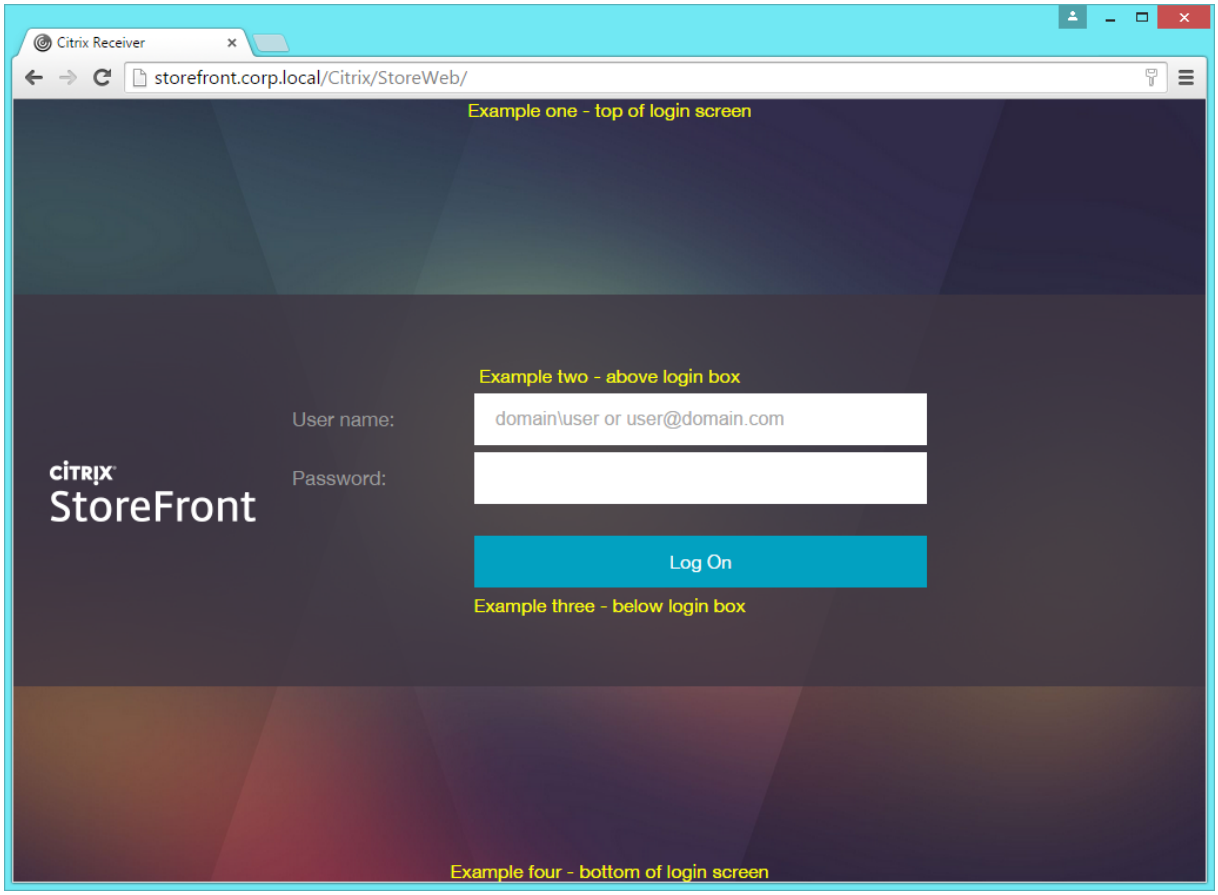
次の JavaScript の行を使用して、4 か所に静的テキストを追加できます:

```
$('.customAuthHeader').html("Example one - top of login screen");
$('.customAuthTop').html("Example two - above login box");
$('.customAuthBottom').html("Example three - below login box");
$('.customAuthFooter').html("Example four - bottom of login screen");
```

テキストをわかりやすくするために、custom.css に次のスタイルを追加します:

```
.customAuthHeader,
.customAuthFooter,
.customAuthTop,
.customAuthBottom
{

 font-size:16px;
 color:yellow;
 text-align: center;
 }
```

これにより、以下のような結果になります:



HTML 形式を使用するには、4 行の javascript を次の内容に置き換えます:

```
1 $('.customAuthHeader').html("<b>Example one</b> - top of login screen"
    );
2 $('.customAuthTop').html("<div style='background:black'>Example two -
    above login box</div>");
3 $('.customAuthBottom').html("<i>Example three - below login box</i>");
4 $('.customAuthFooter').html("<img src='logo.png'>Example four - bottom
     of login screen");
```

> 注:
>
> 例の 4 行目は、カスタムディレクトリの画像の名称が *logo.png* の場合です。

Receiver for Web のログインページに動的ヘッダーを追加

ここで「動的」とは、キャッシュされるのではなく、コンテンツが毎回読み込まれて表示されることを意味します。Web ブラウザーは可能な限りコンテンツをキャッシュしますが、Citrix Workspace アプリは常に UI をキャッシュし、常に以前キャッシュされた UI を読み込みます。つまり、サービスの状態などで以前の例を使用すると、意図した内容を取得できません。

コンテンツを動的に読み込んでページに挿入するためには、代わりに Ajax 呼び出しを使用する必要があります。このためには、以下の手順を実行します:

1. サーバーの*customweb* ディレクトリでページ内のコンテンツを取得する便利なユーティリティ関数を定義し、ページに追加します。これによって、上記の.html の例と同じことが行われます。カスタムページには、テキストまたは HTML スニペットを含めることができます。*customweb* ディレクトリを使用します。これは、(\custom ディレクトリ同様) StoreFront サーバーグループのすべてのサーバーにコピーされますが、ダウンロードされたりキャッシュされることはありません。

2. この関数が適切な時点で呼び出されるようにします。関数の呼び出しが早すぎると、Citrix Workspace アプリで問題が発生します。これは、構成が完全に読み込まれる前にスクリプトが実行されるためです。こうした操作に適切なタイミングは **beforeDisplayHomeScreen** です (ただし、ログインページにコンテンツを表示する場合は、代わりに **beforeLogin** を使用します)。以下のコードは両方のケースを処理し、Web およびネイティブクライアントに適しています。

完全なスクリプトは次のとおりです:

```
function setDynamicContent(txtFile, element) {

   CTXS.ExtensionAPI.proxyRequest({

      url: ”customweb/”+txtFile,
      success: function(txt) {
 $(element).html(txt); }
  }
 );
 }


var fetchedContent=false;
function doFetchContent(callback)
{

  if(!fetchedContent) {

    fetchedContent = true;
    setDynamicContent(”ReadMe.txt”, ”#customScrollTop”);
   }

  callback();
 }


CTXS.Extensions.beforeDisplayHomeScreen = doFetchContent;
CTXS.Extensions.beforeLogon = doFetchContent;
```


これによって、デフォルトでは不要な情報も含まれる*customweb**readme.txt* からコンテンツを読み込みます。独自のファイル（*status.txt*）を追加して、より有用な結果を得られるようにスクリプトの呼び出しを調整します。

ログイン前後にクリックスルー免責事項を表示する

以下は、*script.js* ファイルで既に例として提供されていますが、コメント解除が必要です。このコードには 2 つのバージョンがあります。1 つ目は Web ブラウザーのログイン前に実行され、2 つ目はネイティブクライアントのメイン UI 表示前に実行されます。ログイン後のメッセージのみが必要な場合は、最初の関数を削除します。ただし、ログイン前メッセージのみを使用するのは適切ではありません。その理由は、このログインフローが Web ブラウザーでのみ表示され、ネイティブクライアントでは表示されないためです。Web ブラウザーでのみ表示されている場合でも、ユーザーが Citrix Gateway からアクセスしている時は、このログインフローは表示されません。

```
var doneClickThrough = false;

// Before web login
CTXS.Extensions.beforeLogon = function (callback) {

  doneClickThrough = true;
  CTXS.ExtensionAPI.showMessage({

    messageTitle: ”Welcome!”,
    messageText: ”Only for WWCo Employees”,
    okButtonText: ”Accept”,
    okAction: callback
   }
 );
 }
 ;

// Before main screen (both web and native)
CTXS.Extensions.beforeDisplayHomeScreen = function (callback) {

  if (!doneClickThrough) {

    CTXS.ExtensionAPI.showMessage({

      messageTitle: ”Welcome!”,
      messageText: ”Only for WWCo Employees”,
      okButtonText: ”Accept”,
      okAction: callback
     }
 );
   }
```



```
  else {

    callback();
   }

}
;
```

クリックスルー免責事項ボックスを拡張する

CTXS.ExtensionAPI.showMessage() で使用されるメッセージボックスは事前にスタイルが定義されています。このスタイルを拡張して、その他のメッセージでも対応できるようにできます。次の関数例を script.js に追加して、後からスタイルを再度縮小できます。さらに大きいボックスが必要な場合は、**showLargeMessage()** を **CTXS.ExtensionAPI.showMessage()** の代わりに呼び出します。

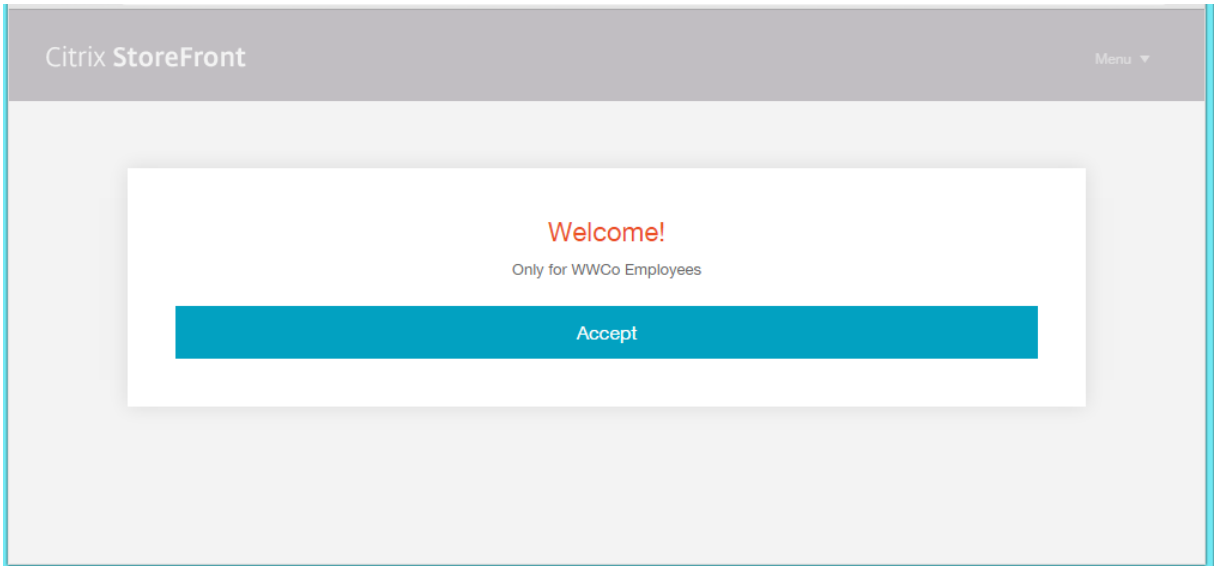
```
function mkLargeMessageExitFn(origfn)
{

  if(origfn) {

    return function() {

      origfn();
      window.setTimeout(function() {
 $('body').removeClass('largeMessage'); }
 ,500);
     }
 ;
   }

 }


function showLargeMessage(details)
{

  $('body').addClass('largeMessage');
  details.cancelAction = mkLargeMessageExitFn(details.cancelAction);
  details.okAction = mkLargeMessageExitFn(details.okAction);
  CTXS.ExtensionAPI.showMessage(details);
 }
 ;
```

これによって、大きなメッセージが表示されている時、マーカークラスが追加されます。ボックスを閉じると、（不要な「ジャンプ」を回避するために）少し遅れてこのマーカークラスが削除されます。

このマーカークラスの存在に基づいてボックスのサイズを調整するための CSS を追加します。たとえば、custom\style.css で以下を実行します：

```
.largeTiles .largeMessage .messageBoxPopup
{

  width:800px;
 }
```

これによって、messageBoxPopup が大きな UI に表示され、largeMessage フラグが設定されます。その幅は 800 ピクセルです。既存のコードで確実にセンタリングされます（携帯電話などの小さな UI では、デフォルトのメッセージボックスは既に最大幅です）。



さらに多くのテキストを表示するには、custom\style.css に次を追加してフォントサイズを縮小するか、スクロール可能なコンテンツを追加するします。

```
.largeTiles .largeMessage .messageBoxText
{

  font-size:10px;
 }
```

クリックスルー免責事項ボックスをスクロール可能にする

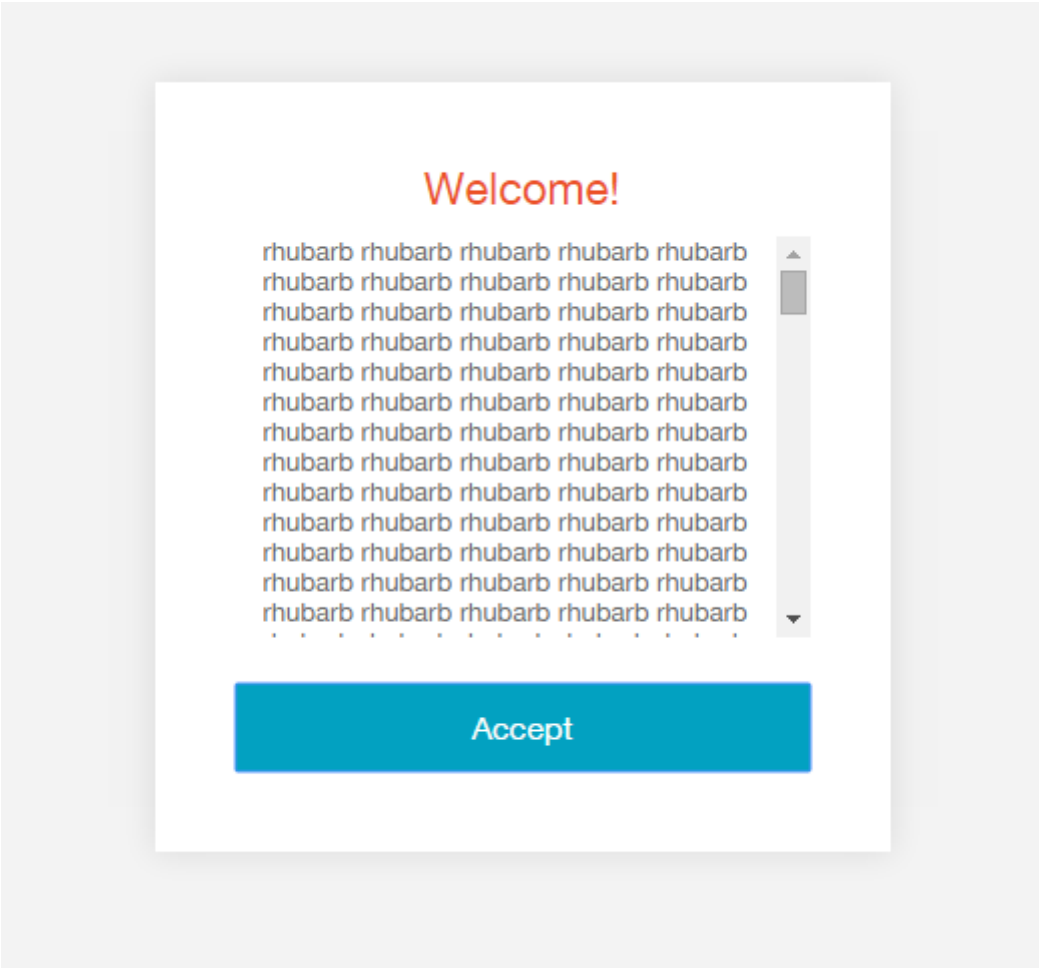
showMessage を呼び出すと、単なる文字列ではなく HTML を渡してスタイルを追加できます。このためには、以前の showMessage の呼び出し例における messageText を次のように置き換えます：


```
    CTXS.ExtensionAPI.showMessage({

          messageTitle: ”Welcome!”,
          messageText: ”&lt;div class=’disclaimer’&gt;rhubarb rhubarb
              rhubarb ... rhubarb rhubarb&lt;/div&gt;”,
          okButtonText: ”Accept”,
          okAction: callback  }
);
```

次に、style.css に以下を追加します:

```
.disclaimer {

    height: 200px;
    overflow-y: auto;
}
```

これにより、以下のような結果になります:



各ページにフッターを追加

これを指定するためのカスタム領域がもう 1 つあります。次の Javascript の行を追加してその内容を設定できます:

```
$('#customBottom').html("For ACME Employees Only");
```

style.css でスタイルを定義します。position:**static**を設定して、スクロール領域が正しく機能するようにします。

```
#customBottom
{

 text-align:center;
 font-size:30px;
 position:static;
 }
```

> 注:
>
> スクリプトを使用してこの領域のサイズを動的に変更する場合は、**CTXS.ExtensionAPI.resize()** コマンドを呼び出して、Citrix Workspace アプリに変更が加えられたことを認識させる必要があります。

ユーザーがアプリタブに移動する場合、フォルダービューをデフォルトにする

このためには、「ビュー変更」イベントを監視します。「ストア」（アプリビューの内部名）へのビューが変更されると、ルートフォルダーに移動します。以下は、注意事項です:

- **onViewChange** イベントが発火した場合（ストアビューの変更中）、ビューは描画を完了しません。したがって、すぐにフォルダーに移動すると、ストアビューの初期化コードが使用したコードの後に実行されるため、実行した作業を元に戻すだけです。これを回避するには、現在のスタックが元に戻された後にコードが実行されるように、1 ミリ秒の遅延を追加します。
- 「whitespace」という単語を含む 3 行は、最初の［すべてのアプリケーション］の UI の上に大きなカスタム領域を配置することによって画面外に表示されるようにします。これにより、フォルダーが表示される前の［すべてのアプリケーション］ビューのちらつきが収まります。

通常どおり、script.js に次のコードを追加します:

```
$('#customScrollTop').append('&lt;div class="whitespace"&gt;&lt;/div&gt
    ;');

CTXS.Extensions.onViewChange = function(view) {

  if (view == "store") {

```



```
    $('.whitespace').height(5000);
    window.setTimeout(function() {

      CTXS.ExtensionAPI.navigateToFolder("/");
      $('.whitespace').height(0);
     }
, 1);
  }

}
;
```

［すべてのアプリケーション］からおすすめカテゴリにも表示されるアプリを非表示にする

このために、以下のコードを使用できます。まずバンドル内のすべてのアプリを記憶し、「すべてのアプリの表示」一覧からそれらを削除します。

```
var bundleApps = [];

CTXS.Extensions.sortBundleAppList = function(apps,bundle, defaultfn) {

  for (var i = 0; i &lt; apps.length; i++) {

    bundleApps.push(apps[i]);
   }

  defaultfn();
 }
 ;

CTXS.Extensions.filterAllAppsDisplay = function(allapps) {

  for (var i = 0; i &lt; allapps.length; i++) {

    if ($.inArray(allapps[i], bundleApps) != -1) {

      allapps.splice(i, 1);
      i--;
     }

   }

 }
 ;
```

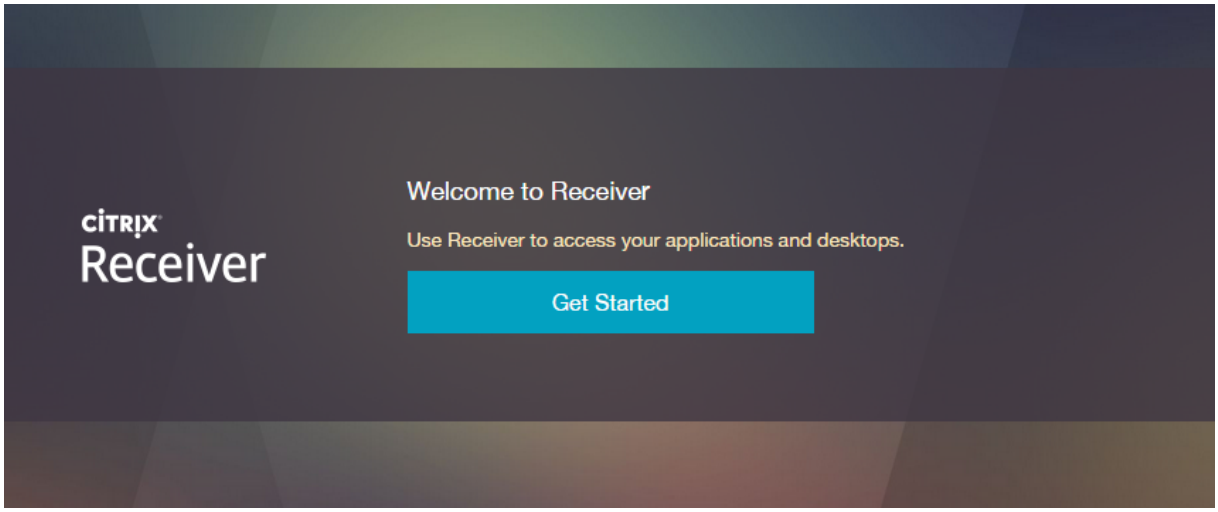
このカスタマイズを使用する場合は、ユーザーが混乱しないように、「All Apps」というテキスト文字列を「Other Apps」に変更することをお勧めします。このためには、カスタムディレクトリの *strings.en.js* ファイルを編集し、**AllAppsTitle** のタグを追加します。たとえば、変更を黄色で表示する場合、以下のようになります:

```
(function ($) {

  $.localization.customStringBundle(”en”, {

    <span style=”background-color: yellow;”>AllAppsTitle: ”Other Apps”
        ,</span>
    Example1: ”This is an example”,
    Example2: ”This is another example”
 }
 );
 }
 )(jQuery);
```

デフォルトの **UI** テキストを変更する

ラベルの名前が判明している場合、UI で使用されているテキストを変更できます。たとえば、Google Chrome の Receiver for Web で使用される「Install」画面を「Get Started」に変更するには、次のようにカスタム文字列を追加します:

```
(function ($) {

  $.localization.customStringBundle(”en”, {

    <span style=”background-color: yellow;”>Install: ”Get Started”,</
        span>
    Example1: ”This is an example”,
    Example2: ”This is another example”
 }
 );
 }
 )(jQuery);
```

変更するラベルの名前を見つけるには、以下を実行します：

1. StoreFront サーバーでディレクトリ C:\inetpub\wwwroot\citrix\StoreWeb\receiver\js\localization\en を探します（ストア名が「Store」の場合）。
2. メモ帳でファイル *ctxs.strings_something.js* を開きます。
3. 変更する文字列を探します。注：このファイルを直接編集する代わりに、「install」例でのようにカスタムディレクトリの上書き値を作成します。

おすすめカテゴリの背景画像を変更する

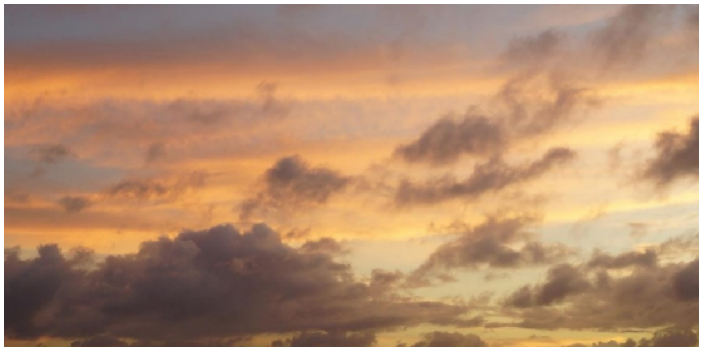
> 重要：
>
> サーバー上の画像を上書きしないでください。クライアントは変更を認識できないため、既に画像をダウンロードしたクライアントを混乱させることになります。また、これによってアップグレードで問題が発生したり、失敗したりします。

独自の画像を*custom* ディレクトリに追加し、CSS を参照として追加できます。おすすめカテゴリ（内部の名称は「bundle」）ごとに 2 つの画像を使用します：

- 最初の画像はカルーセルのタイルとして使用されます。
- 2 番目の画像は、詳細ページのヘッダーの背景画像として使用されます。この画像は画面の幅いっぱいに引き伸ばされ、下端の方はぼかしが追加されます。

画面ごとに異なる画像を使用できます。詳細ページで同じ画像を使用し、背景の高さを 2 倍にすると、画像の上半分だけが表示されます。画像は詳細ページ上で引き伸ばされるため、変形しても問題がない画像を使用してください。

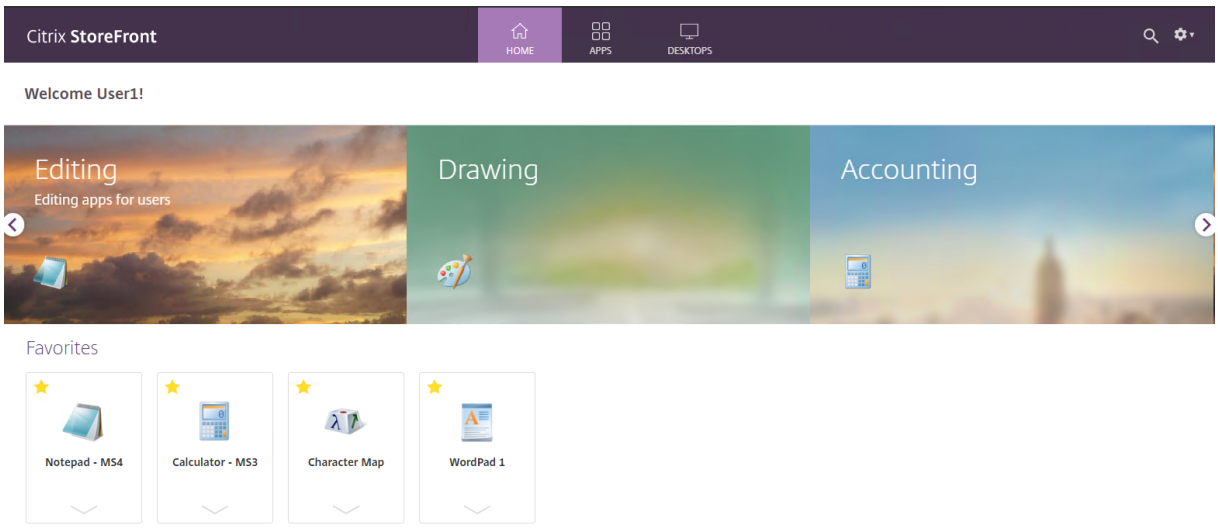
最初の bundle のクラスは「appBundle1」、2 番目は「appBundle2」で、「appBundle8」まで使用できます。以下の例では「clouds.png」を使用しています。これは、以下の画像を右クリックしてダウンロードできます：

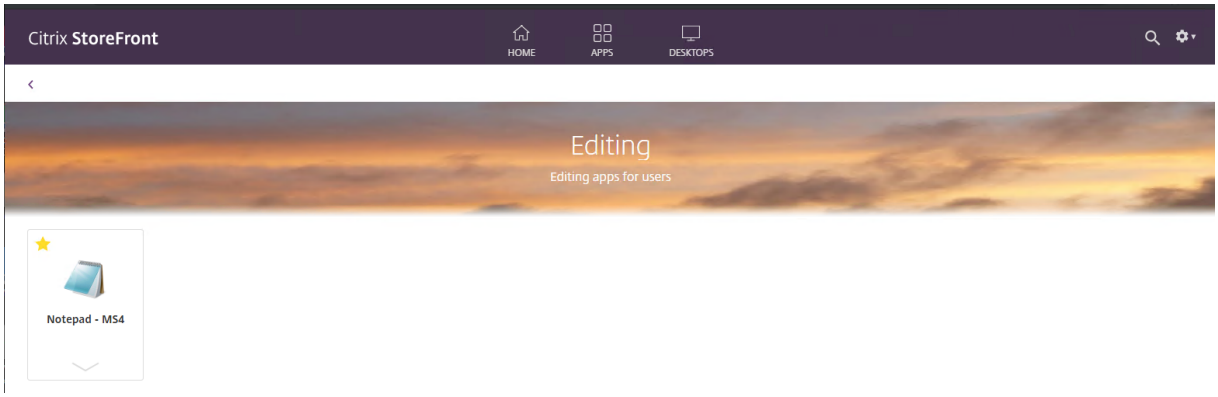


1. *\custom* ディレクトリに画像を保存します。他の画像と同様の約 520×256 ピクセルのサイズにしてください（必要に応じて拡大縮小します）。
2. style.css に以下を追加します：

```
.appBundle1 {

  background-image: url('clouds.png');
 }


.bundleDetail.appBundle1 {

  background-image: url('clouds.png');
  background-size: 100% 200%;
 }
```

これにより、以下のような結果になります：





会社のロゴがぼやけないようにする

Receiver for Web は標準（「低 DPI」）の画面と、1 インチあたりのピクセル数が多い、新しい高画質（「高 DPI」）画面の両方を正しく処理する必要があります。たとえば、Apple Retina の画面は、Retina 以外の画面の 2 倍の解像度です。ノートブック PC では、画面は通常、同サイズの「標準」のピクセル数に対して 1.5 倍、2 倍、または 3 倍のこともあります。現時点では、最も一般的なのは 2 倍であり、解像度の違いが最も明確になるため、Citrix Workspace アプリは大半の画像アセットを 2 つの解像度で保有しています。標準の画面用の 100×100 ピクセルの画像と、2 倍の解像度用の 200×200 ピクセルです。

StoreFront 管理コンソールからロゴ画像をアップロードするときは、2 倍の画像であることを確認してください。つまり、標準画面の約 2 倍の幅と高さの「スペース」になります（1 倍でアップロードされた画像を 2 倍に拡大することはできません）。標準画面の「スペース」は 170×40 ピクセルであるため、アップロードするロゴ画像は約 340×80 ピクセルにする必要があります。

StoreFront はロゴのコピーを作成し、それを半分のサイズに縮小します。この画像は低 DPI ディスプレイで使用されます。

この場合、画像の詳細の半分が破棄されるため、画像がぼやけることもあります。ただし、ロゴは明瞭度が高くシンプルであることが多いため、ぼやけることはほぼありません。ロゴでこの問題が発生した場合は、次の回避策を使用します：

1. 1 倍サイズ、2 倍サイズの 2 つのバージョンのロゴを作成し、*\custom* ディレクトリに保存します。
2. *custom\style.css* を編集して、2 つの異なる画像を参照できるようにします。次のようになります：

```
<span style="color: green;">/* The following section of the file is
    reserved for use by StoreFront. \*/</span>
<span style="color: green;">/\* CITRIX DISCLAIMER: START OF MANAGED
    SECTION. PLEASE DO NOT EDIT ANY STYLE IN THIS SECTION \*/</span>
<span style="color: green;">/\* CITRIX DISCLAIMER: END OF MANAGED
    SECTION. \*/</span>
<span style="color: green;">/\* You may add custom styles below this
    line. */</span>

```



```
.logo-container {

    background-image: url('mylogo_x1.png');
    background-size: 169px 21px;
 }


.highdpi .logo-container {

    background-image: url('mylogo_x2.png');
    background-size: 169px 21px;
 }
```

> 注:
>
> - これらのカスタムスタイルが「managed section」内にないことを確認してください。「managed section」内にあると、上書きされるか、StoreFront 管理コンソールを混乱させることになります。
> - 両方のスタイルは同じ背景サイズを指定します。これは、サイズが「論理的な」単位で指定されており、2 倍画像の場合、背景サイズは実際のロゴの幅と高さの半分になるためです。

背景画像を設定する

> 注:
>
> 統合エクスペリエンスは、シンプルな白の背景用に設計されています。背景画像は邪魔になることが多いためです。そのため、背景画像を追加する場合は、明度の高いシンプルな画像を使用します。この画像に対応できるよう、必要に応じてフォントを調整してください。

例 **1**: アップロードされた画像への **CSS** リファレンス

custom.css を次のように変更します:

```
.storeViewSection {

   background: url('images/background.jpg') no-repeat center center
      fixed;
   background-size: cover;
 }
```

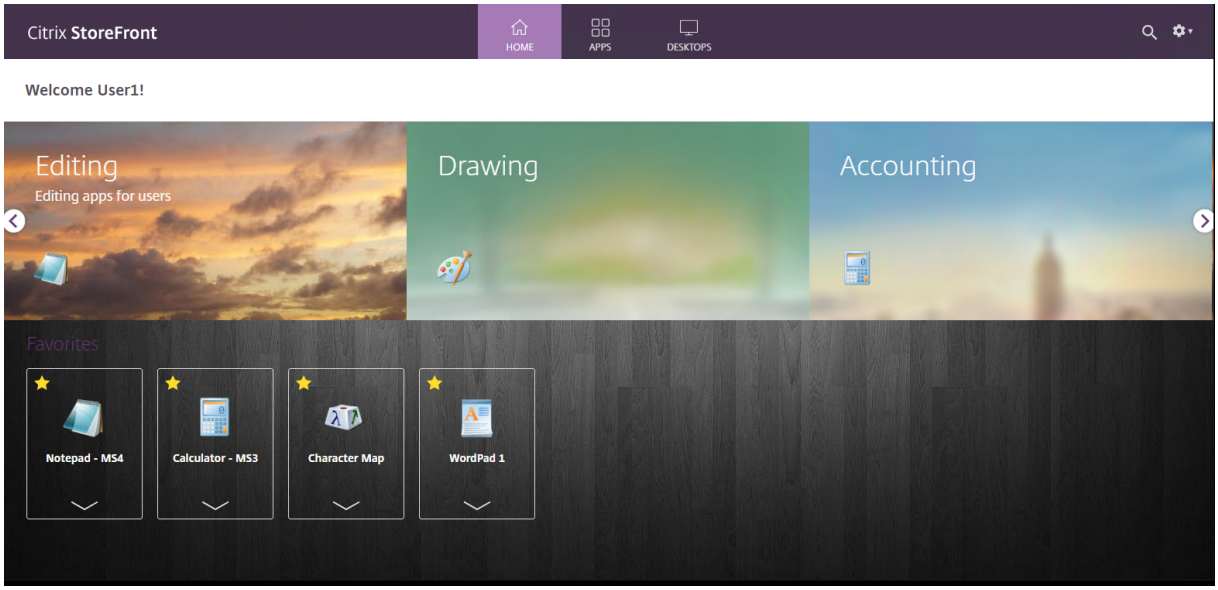
> 注:
>
> background-size:cover; ステートメントは、一部の古いブラウザーでは機能しません。

例 **2**: 微調整による既存の画像への **CSS** リファレンス

custom.css を次のように変更します:

```
.storeViewSection {

   background: url('../media/bg_bubbles.jpg') no-repeat center center
      fixed;
    background-size: cover;
    color: white;
 }


// Tweak fonts
.smallTiles .storeapp .storeapp-name,
.largeTiles .storeapp .storeapp-name {

    color: white;
 }


// Tweak bundle area so it doesn't clash as badly
.largeTiles .applicationBundleContainer {

    background-color: rgba(255, 255, 255, 0.4);
    margin-top: 0;
    padding-top: 25px;
 }


.smallTiles .applicationBundleContainer {

    background-color: rgba(255, 255, 255, 0.4);
    margin-top: 0;
    padding-top: 14px;
 }
```

これにより、以下のような結果になります:



コード内のエラーを見つける

デバッグには、いくつかの方法があります。必ず最初にブラウザーを試してください。これは Citrix Workspace アプリでカスタマイズをデバッグするよりもはるかに簡単です。ページ URL で「?」や「#」の後に次の引数を追加して、一度に複数の文字列をつなぎ合わせることができます。次に例を示します:

```
1 http://storefront.wwco.net/Citrix/StoreWeb/#-tr-nocustom
```

-errors - 通常、コードで発生する可能性があるエラーを回避しようとしますが、代わりにエラーを明確にすることもできます。この引数は、エラーが発生した時にアラートボックスを表示します。

-debug - この引数は、カスタマイズコードの例外処理を無効にします。これは、最近のブラウザーに組み込まれた開発ツール（Google Chrome や Internet Explorer の F12 など）で役に立ち、例外を自身でデバッグできます。

-nocustom - この引数は、スクリプトと CSS カスタマイズを無効にします。これは、Citrix Workspace アプリが機能していない場合に、エラーが何らかの作業の結果かを確認する時に役に立ちます。

-tr - この引数は、個別のブラウザータブで Citrix Workspace アプリの UI コードのトレースを提供します（**CTXS.ExtensionAPI.trace()** の呼び出しで追加するトレースなど）。

統合ユーザーエクスペリエンス

ここでは統合エクスペリエンスの機能と外観について説明します。

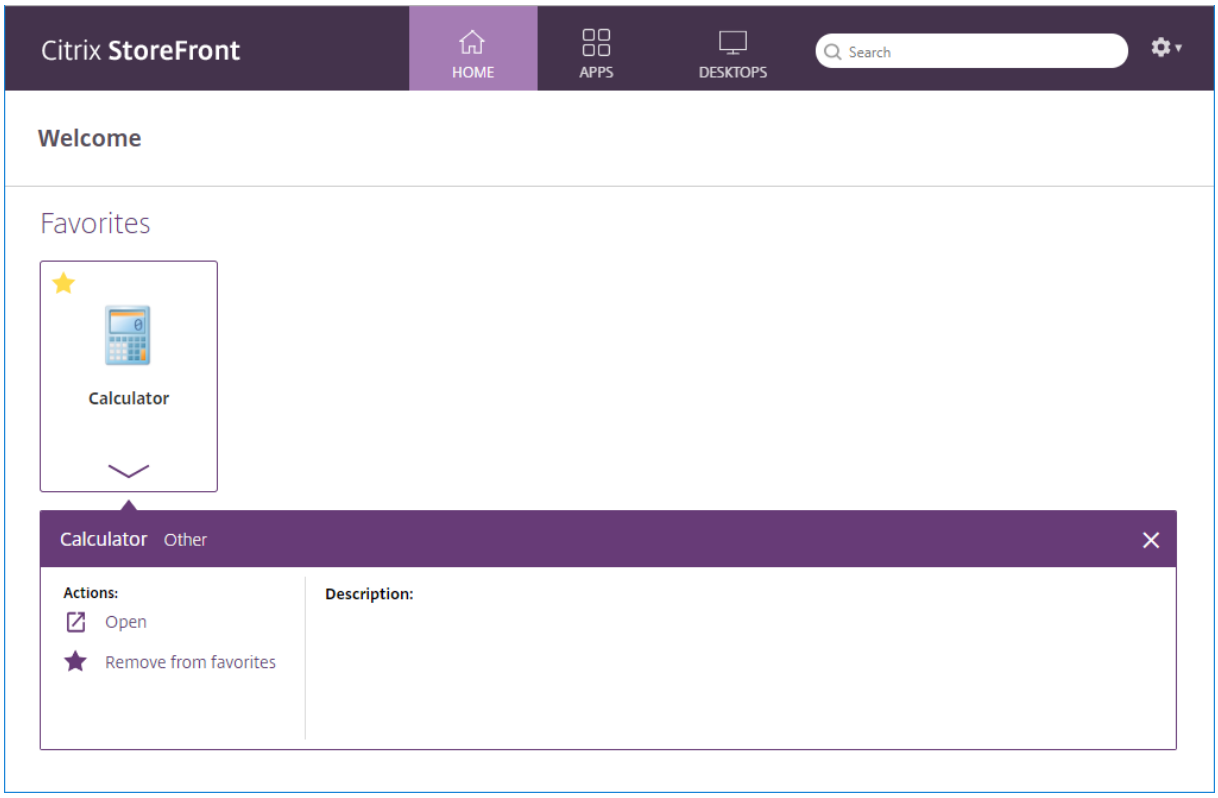
カードのレイアウト

ストアのアプリは、「カード」レイアウトで表示されます。各カードの下のパネルを展開して、詳細および操作を表示できます。

> 注:
>
> 統合エクスペリエンスでは、ユーザーがドラッグアンドドロップでアプリケーションを再配置することはできません。

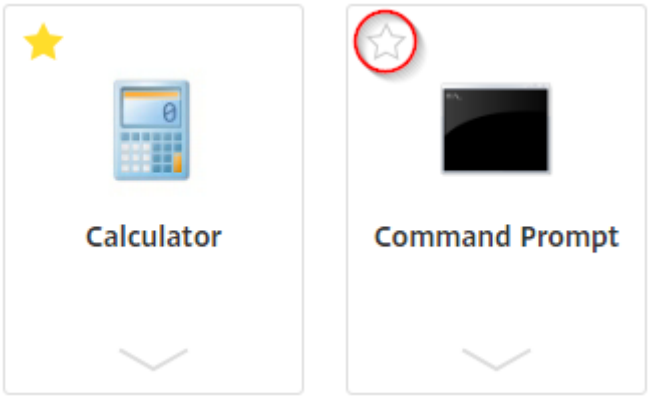
ホーム

ホームにはお気に入りが表示されます。



お気に入り

アイテムをお気に入りに登録するには、星をクリックまたはタップします:



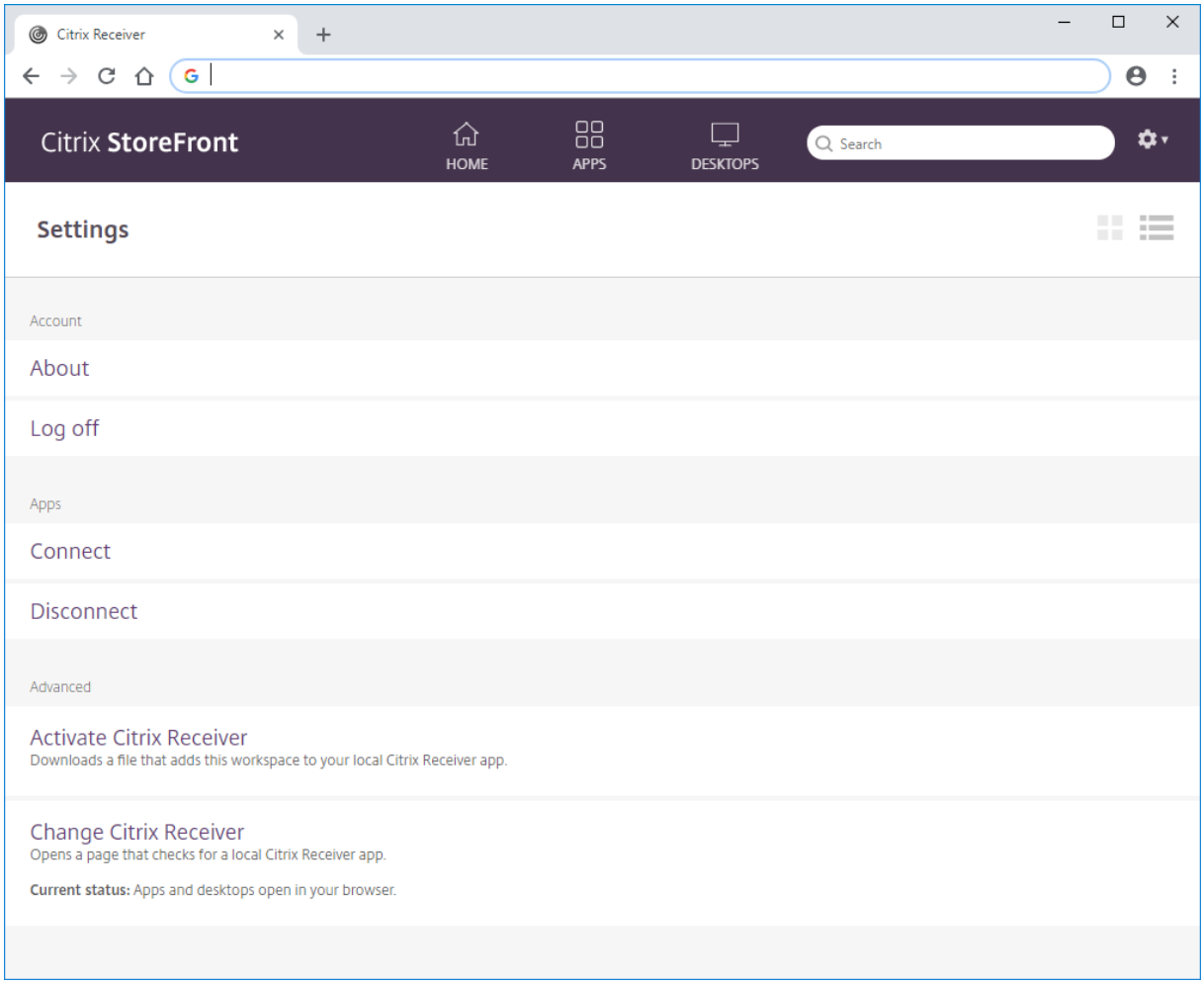
検索

すべてのアプリ、デスクトップ、カテゴリを横断して検索します:

設定

ドロップダウンメニューのアクセス設定です:

メニューには、Active Directory の表示名を使用したユーザー名が表示されます。表示名が空白の場合（推奨されていません）、ドメインとアカウント名が表示されます。メニューを使用して［設定］ページを開き、Citrix Workspace アプリのバージョンを確認するかログオフします。



設定では、切断されたセッションを再開したり、現在のすべてのセッションを切断したり、ログアウトしたりできます。カードレイアウトまたは一覧レイアウトの設定ページを表示します：

接続。切断されたセッションを再開します。

切断。現在のすべてのセッションを切断し、ログオフします。

Citrix Receiver のアクティブ化：このストアをローカルの Citrix Workspace アプリに追加するファイルをダウンロードします。

Citrix Receiver の変更：ローカルの Citrix Workspace アプリを確認するページを開きます。これによってユーザーがローカルにインストールされた Citrix Workspace アプリを使用したリソースの起動と HTML5 ブラウザーでのリソースの起動とを切り替えることもできます。

お勧めのアプリケーションの作成および管理

April 2, 2020

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、営業部にお勧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ア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勧めのアプリケーションを定義できます。

[お勧めのアプリケーショングループ] タスクを使って、お勧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。完了したら、
> 構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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 ［**Receiver for Web** サイトの管理］>［構成］ の順にクリックします。
3. ［お勧めのアプリケーショングループ］ を選択します。
4. ［お勧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、お勧めのアプリケーショングループ名、説明（任意）、背景、およびお勧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。

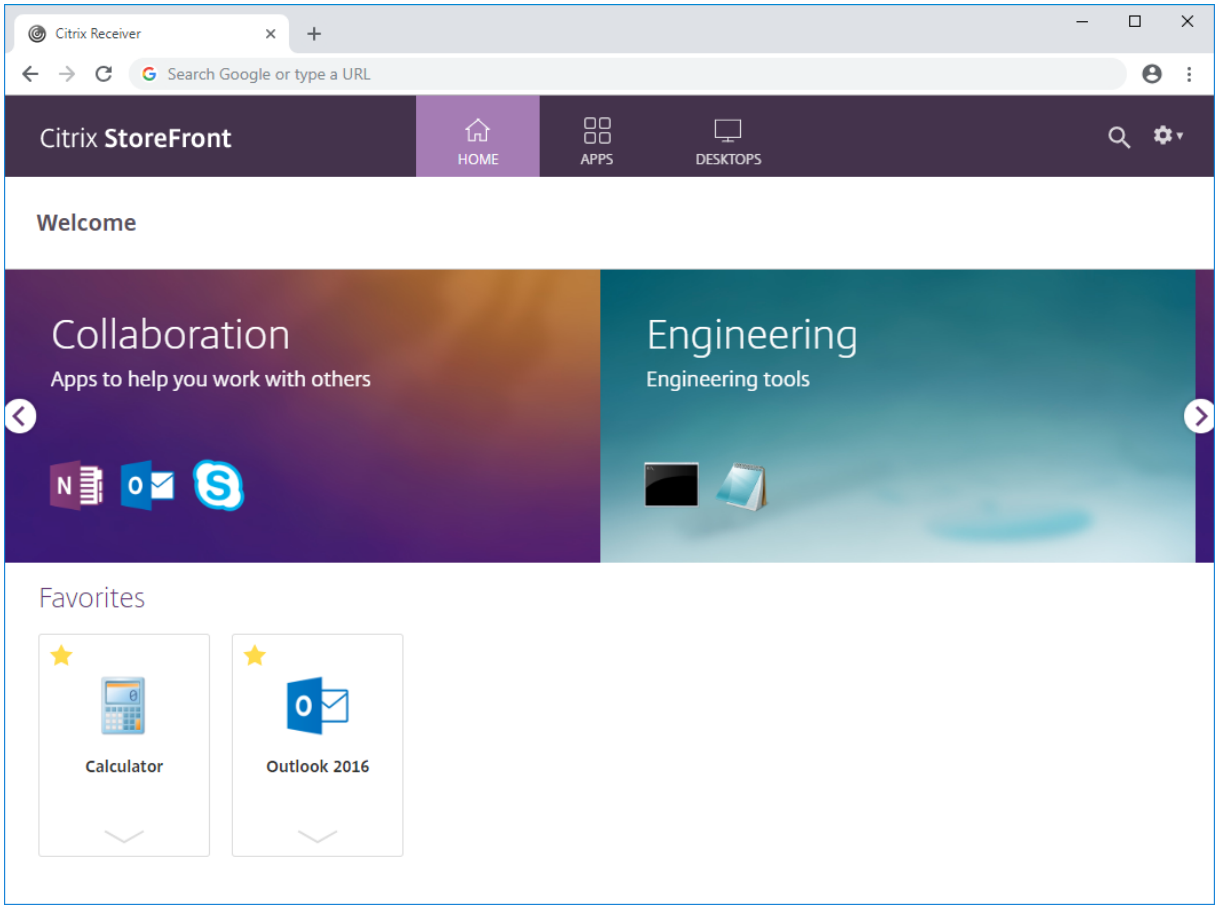
オプション	説明
キーワード	Studio でキーワードを定義します。
アプリケーションカテゴリ	Studio でアプリケーションカテゴリを定義します。

オプション	説明
アプリケーション名	アプリケーション名を使ってお勧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、お勧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。

例:

2 つのお勧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

April 2, 2020

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。完了したら、構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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

HTML5 向け Citrix Workspace アプリのブラウザータブ使用の構成

April 2, 2020

デフォルトでは、HTML5 向け Citrix Workspace アプリ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 HTML5 向け Citrix Workspace アプリ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。完了したら、構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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/Workspace** アプリの展開］ を選択します。
4. ［展開オプション］ リストから ［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

April 2, 2020

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見なされます。［セッション設定］ タスクを使ってデフォルトの設定を変更します。

> 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。完了したら、構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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、中央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。

セッションタイムアウトの構成

StoreFront でセッションタイムアウトが適切に構成されていない場合、ユーザーに次のタイムアウトメッセージが表示されることがあります。「操作が行われないため、セッションがタイムアウトしました。」セッションのタイムアウト値をリセットして、ユーザーの使用パターンに応じて非アクティブタイマーの値を増加させることができます。

StoreFront でセッションタイムアウトを設定するには、次の手順を実行します:

StoreFront のセッションタイムアウト値を増やす

1. StoreFront で **c:\inetpub\wwwroot\Citrix<StoreWeb>** に移動します。
2. 次のエントリを特定します: `web.config`ファイルの **<sessionState timeout="20"/>**。
3. **`sessionState timeout`** を必要な値（分）に変更します。

認証サービスのトークンの最大有効期間を増やす

Citrix Receiver for Web のセッションタイムアウト値を 1 時間を超えて増やす場合、その値に応じて ［認証サービス］ でトークンの最大有効期間も増やす必要があります。

Citrix Workspace アプリのセッションタイムアウトを増やす

1. StoreFront サーバーにインストールされた Citrix Workspace アプリで、ストアの認証サービスのパスに移動します。最新のバージョンの StoreFront では、このパスは**`c:\inetpub\wwwroot\Citrix\<Store>Auth`**です（ストアが複数ある場合、これは多数の認証サービスのうちの 1 つです）。

   以前のバージョンの StoreFront では、このパスは**`c:\inetpub\wwwroot\Citrix\Authentication`**です（認証サービス間で共有されている場合とサーバー上で唯一のパスの場合があります）。

2. `web.config`ファイルで次のエントリを特定します: **<defaultLifetime="01:00:00" maxLifetime="01:00:00">**。

3. **maxLifetime** を必要な値に変更します。

> 注:
>
> Windows 向け Citrix Workspace アプリと Linux 向け Citrix Workspace アプリ。現在のセッションからログアウトすると、バックグラウンドに Citrix Virtual Apps and Desktops が表示されることがあります。ただし、StoreFront のセッションタイムアウト後、アプリやデスクトップをクリックした場合、再度資格情報を入力する必要があります。

認証トークンの有効期間を増やす

必要なタイムアウト値が 8 時間を超える場合、Citrix Receiver for Web のweb.configファイルを編集して、［認証トークンの有効期間］を増やします:

1. StoreFront で **c:\inetpub\wwwroot\Citrix<StoreWeb>** に移動します。
2. 次のエントリを特定します: **<authentication tokenLifeTime=”08:00:00”method=”Auto”/>**
3. **tokenLifeTime** を必要な値に変更します。

IIS の再起動

- **iisreset** コマンドを実行して変更を適用します。このコマンドを実行することで、ユーザーを Citrix Receiver for Web からログオフさせます。現在の ICA セッションに影響を与えることはありません。

> 注:
>
> 完了した有効期間の形式は.d.hh:mm:ss[.ff]です。最大有効期間は、24 時間に限定されません。

そのほかの情報の入手先

- Citrix ブログ - Receiver for Web のアイドルタイムアウト（英語）
- セキュリティトークンサービス API（英語）

ユーザーアクセスの構成

April 2, 2020

XenApp Services サイトを介した接続のサポート

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。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時に、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。完了したら、構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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。

   XenApp Services サイトの URL 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の再接続を無効または有効にする

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、Citrix Workspace アプリ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含まれています。この機能は、StoreFront コンソールまたは PowerShell を使用して管理します。

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. ［詳細設定］ を選択し、［セッションの再接続を許可する］ 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てから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 HKEY_LOCAL_MACHINE:\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] <Int64>] [[-VirtualPath] <String> ]
[[-IsAllowed] <Boolean>]
```

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
```

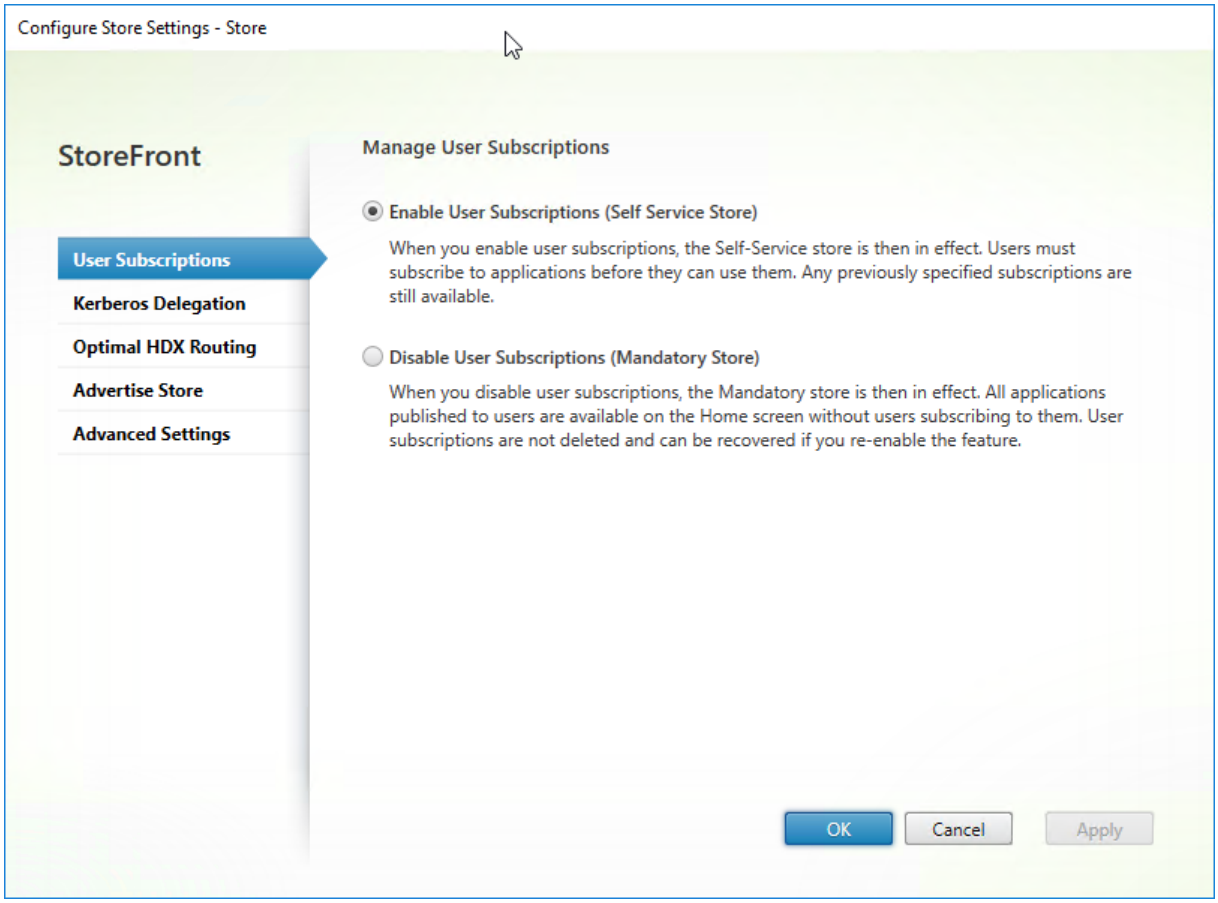
ユーザーサブスクリプションの構成

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 Workspace アプリでユーザーに［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時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時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/<yourstore>”
Set-STFStoreService -StoreService $StoreObject -LockedDown $True -Confirm:$False
```

Get-STFStoreService について詳しくは、次を参照してください。https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Get-STFStoreService/

StoreFront を構成してウィンドウモードでアプリケーションおよびデスクトップを起動

August 29, 2019

アプリケーションの起動は、環境での StoreFront の可用性にシームレスに依存します。アプリケーションおよびデスクトップのシームレスオプションを無効にする場合は、代わりにウィンドウモードでの起動を検討してください。

以下は、公開アプリケーションの「メモ帳」の例です。Citrix Virtual Apps and Desktops のアプリケーションセットで表示された公開アプリケーションの正確な名前を使用します。

> 注:
>
> ICA ファイルの大半の設定は大文字小文字を区別しません（例外：DesiredHRES設定およびDesiredVRES設定）。ウィドウモードのアプリバージョンを適用する場合、ブラウザー名を使用して StoreFront サーバー上にある *default.ica* ファイルのアプリを参照します。Delivery Controller で PowerShell を使用してアプリケーションのブラウザー名を確認します：
>
> ```
> >>asnp citrix*
> ```
>
> ```
> >>Get-BrokerApplication -ApplicationName
> ```

StoreFront を構成するには

1. StoreFront サーバーの\inetpub\wwwroot\Citrix\StoreName\App_Dataディレクトリにある default.ica ファイルを編集します。
2. default.ica ファイルでは、次の行を探します：[ApplicationServers] application=。
3. application=の後に行を作成し、次のパラメーターを追加します：

```
[Notepad]
TWIMode=Off
DesiredHRES=1024
DesiredVRES=768
```

4. ファイルを保存します。

Citrix Virtual Apps and Desktops 7.x および StoreFront 3.x の公開デスクトップの場合

1. StoreFront サーバーのC:\inetpub\wwwroot\Citrix\storeWebディレクトリ内の *web.config* ファイルを編集します。
2. web.config ファイルで、次の行を探します：showDesktopViewer=''**true**''。
3. 値を **True** から **False** に変更します。
4. クライアント側で、または AD-GPMC で、管理用テンプレートファイルを使用して（オペレーティングシステムによってreceiver.admまたはreceiver.admx\receiver.admlに）、次のポリシーを構成します：
   - [**Computer configuration**] > [**Citrix Components**] > [**Citrix Receiver**] > [**User Experience**] > [**Client Display Settings**]：**Enable**
   - シームレスウィンドウ：**False**
   - ウィンドウの幅：**<As per requirement>**、ウィンドウの高さ：**<As per requirement>**

注

DeisredHRESおよびDesiredVRESは、必要な解像度（800x600 や 1024x768 など）に設定できます。

パーセント表示の画面サイズでアプリケーションを実行する必要がある場合、TWIMode=Offの設定後にScreenPercent=90行を追加すると、画面サイズが 90% に設定されます。これは、XenApp Services サイトでも設定できます。サイト（Inetpub\wwwroot\Citrix\PNAgent\conf）のconfフォルダー上で対象ファイルを編集してください。

10.x クライアントを使用して**default**.icaまたはtemplate.icaファイルを編集する場合、TWIMode=Off行のみを追加します。公開アプリケーションのプロパティからHRESおよびVRES設定が取得されます。または、ユーザーがアプリケーションを起動するときに ICA ファイルに重複したエントリがあるというエラーメッセージが表示されます。

可用性の高いマルチサイトストアのセットアップ

April 2, 2020

> 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。完了したら、構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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 Citrix 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。

ユーザーマッピングおよびアグリゲーションの構成

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。
- 集約する展開環境：集約するリソースがある展開環境を指定できます。集約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。
- ゾーンを展開環境に関連付ける：グローバルな負荷分散構成の Citrix Gateway でアクセスする場合、StoreFront は、リソースを起動するときにゲートウェイゾーンに一致するゾーンの展開環境を優先します。

1. すべての Citrix Virtual Apps and Desktops 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 つ以上のコントローラー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集合体構成］、［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. ［リソースを集約する］ をクリックして、複数の展開環境からリソースを集約します。Delivery Controller を集約する場合、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 Workspace アプリ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。
   a) Delivery Controller を集約するには、複数のコントローラーを選択して ［集約］ をクリックします。
   b) ［集約済みコントローラーの設定］ オプションを選択します：

      コントローラーが同一のリソースを公開します - オンにすると、集約済みセットにあるいずれか 1 つのコントローラーのリソースのみが列挙されます。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約するために）集約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約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。
7. ［ユーザーマッピングおよびマルチサイト集合体構成］ダイアログボックスで、［**OK**］ をクリックします。
8. ［Delivery Controller の管理］ダイアログボックスで、［**OK**］ をクリックします。

詳細構成

StoreFront 管理コンソールで、多くの一般的なマルチサイトおよび高可用性操作を構成できます。PowerShell を使用するか、StoreFront 構成ファイルを編集して、StoreFront を構成することもできます。これにより次の追加機能が提供されます：

- 集約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。
- 集約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、集約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。

1. 障害回復用の展開環境を含め、すべての Citrix Virtual Apps and Desktops 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. 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。

```
<resourcesWingConfigurations>
<resourcesWingConfiguration name=”Default” wingName=”Default” />
</resourcesWingConfigurations>
```

4. 次のように構成します。

```
<resourcesWingConfigurations>
<resourcesWingConfiguration name=”Default” wingName=”Default”>
<userFarmMappings>
<clear />
<userFarmMapping name=”user_mapping”>
<groups>
<group name=”domain\usergroup” sid=”securityidentifier” />
<group ... />
...
</groups>
<equivalentFarmSets>
<equivalentFarmSet name=”setname” loadBalanceMode=”{
 LoadBalanced | Failover }
 ”
aggregationGroup=”aggregationgroupname”>
<primaryFarmRefs>
<farm name=”primaryfarmname” />
<farm ... />
...
</primaryFarmRefs>
<backupFarmRefs>
<farm name=”backupfarmname” />
<farm ... />
...
</backupFarmRefs>
```

```
</equivalentFarmSet>
<equivalentFarmSet ... >
...
</equivalentFarmSet>
</equivalentFarmSets>
</userFarmMapping>
<userFarmMapping>
...
</userFarmMapping>
</userFarmMappings>
</resourcesWingConfiguration>
</resourcesWingConfigurations>
```

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 Citrix Virtual Apps and Desktops 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とき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ときに使用される最適な Citrix 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 Citrix 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 Citrix 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。

サブスクリプション同期の構成

異なる StoreFront 展開環境のストアからユーザーの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。

サブスクリプションの同期を確立するときは、同期するストア間で構成された Delivery Controller を同一の名前にする必要があります。Delivery Controller の名前は大文字と小文字が区別されます。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。集約されたリソースからサブスクリプションを同期する場合、両方のストアで使用されるアグリゲーショングループの名前も一致している必要があります。Delivery Controller 名とアグリゲーショングループ名では大文字と小文字が区別されます。たとえば、*XenDesktop7* と *Xendesktop7* は異なります。

1. ローカル管理者権限を持つアカウントを使用して、Windows PowerShell ISE を起動します。
2. 毎日特定の時刻に同期が行われるように構成するには、次のコマンドを実行します。

```
$RepeatMinutes = 30
Add-STFSubscriptionSynchronizationSchedule -StartTime (Get-Date -
    Format t) -RepeatMinutes $RepeatMinutes
```

-StartTime を使用して同期スケジュールの開始時間を指定します。**(Get-Date -Format t)** を使用すると、同期スケジュールはすぐに開始します。*10:00* のように指定すると、指定した時間に定期的に開始します。

-RepeatMinutes は、スケジュールを実行する頻度を設定します。たとえば、*30* では 30 分ごとにスケジュールを実行し、*180* では 3 時間ごとにスケジュールを実行します。2 つのサーバーグループが互いにサブスクリプションデータを同時に取得しないように、プルスケジュールをずらすことをお勧めします。たとえば、各サーバーグループから 60 分ごとにデータを取得するスケジュールは、次のように構成されます。サーバーグループ 1 が、サーバーグループ 2 から 01:00、02:00、03:00 のようなスケジュールでデータを取得します。

サーバーグループ 2 は、サーバーグループ 1 から 01:30、02:30、03:30 のようなスケジュールでデータを取得します。

3. 同期させるストアを含むリモート StoreFront 展開を指定するには、次のコマンドを入力します。StoreFront サーバーグループが存在するデータセンターごとにこれを構成して、他のリモートデータセンターからサブスクリプションデータを取得できるようにする必要があります。次の米国および英国のデータセンターの例を参照してください:

   - 米国データセンターの StoreFront サーバーで実行して、英国データセンターのサーバーからデータを取得します:

   ```
   $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/
       Citrix/Store"
   Add-STFSubscriptionSynchronizationSource -FriendlyName "
       SyncFromUKStore" -StoreService $StoreObject -
       RemoteStoreFrontAddress "UKloadbalancedStoreFront.example.
       com"
   ```

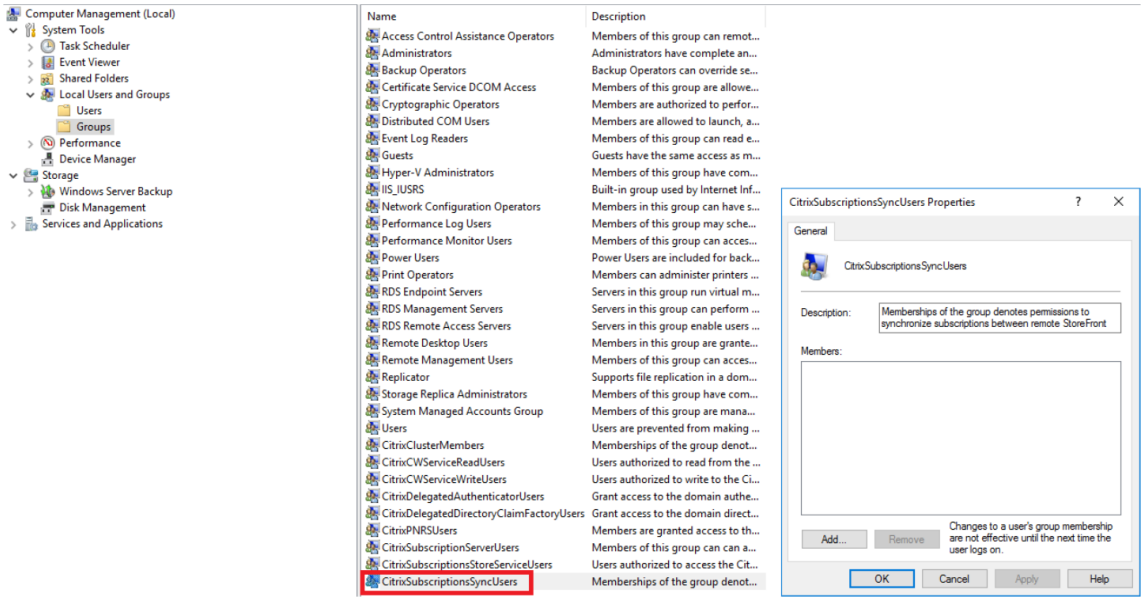
   - 英国データセンターの StoreFront サーバーで実行して、米国データセンターのサーバーからデータを取得します:

   ```
   $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/
       Citrix/Store"
   Add-STFSubscriptionSynchronizationSource -FriendlyName "
       SyncFromUSStore" -StoreService $StoreObject -
       RemoteStoreFrontAddress "USloadbalancedStoreFront.example.
       com"
   ```

   ここで、*FriendlyName* 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、*RemoteStoreFrontAddress* は StoreFront サーバーまたは負荷分散サーバーグループの FQDN です。アプリケーションサブスクリプションを複数のストア間で同期するには、同期されるすべて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. 現在のサーバー上のローカル Windows ユーザーグループ CitrixSubscriptionSyncUsers に、リモート展開の各 StoreFront サーバーの Microsoft Active Directory ドメインマシンアカウントを追加します。

   これにより、同期スケジュールを構成すると、現在のサーバーは、CitrixSubscriptionSyncUsers に表示されているリモートサーバーから新規または更新されたサブスクリプションデータを取得できます。ローカルユーザーグループの変更については、http://technet.microsoft.com/en-us/library/cc772524.aspxを参照してください。



5. 正常にスケジュールを構成した後、Citrix StoreFront 管理コンソールまたは以下の Powershell を使用して、サブスクリプション同期スケジュールとソースをグループ内の他のすべてのサーバーに反映します。

```
Publish-STFServerGroupConfiguration
```

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。

6. 既存のサブスクリプション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、展開環境のほかの StoreFront サーバーに構成の変更を反映させます。

```
Clear-STFSubscriptionSynchronizationSchedule
```

7. 特定のサブスクリプション同期ソースを削除するには、次のコマンドを実行し、展開環境のほかの StoreFront サーバーに構成の変更を反映させます。

```
Remove-STFSubscriptionSynchronizationSource -FriendlyName ”
    SyncFromUKStore”
```

8. すべての既存のサブスクリプション同期ソースを削除するには、次のコマンドを入力し、展開環境のほかの StoreFront サーバーに構成の変更を反映させます。

```
Clear-STFSubscriptionSynchronizationSource
```

9. StoreFront 展開用に現在構成されているサブスクリプション同期スケジュールを一覧表示するには、次のコマンドを実行します。

```
Get-STFSubscriptionSynchronizationSchedule
```


10. StoreFront 展開用に現在構成されているサブスクリプション同期ソースを一覧表示するには、次のコマンドを実行します。

```
Get-STFSubscriptionSynchronizationSource
```

ストアの最適な **HDX** ルーティングの構成

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、Citrix Virtual Apps and Desktops の展開環境を、Citrix Virtual Apps and Desktops 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。Citrix Virtual Apps and Desktops Studio でゾーンを定義します。StoreFront は、Citrix Virtual Apps and Desktops と相互運用できます。StoreFront で定義されたすべてのゾーンが、Citrix Virtual Apps and Desktops 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。

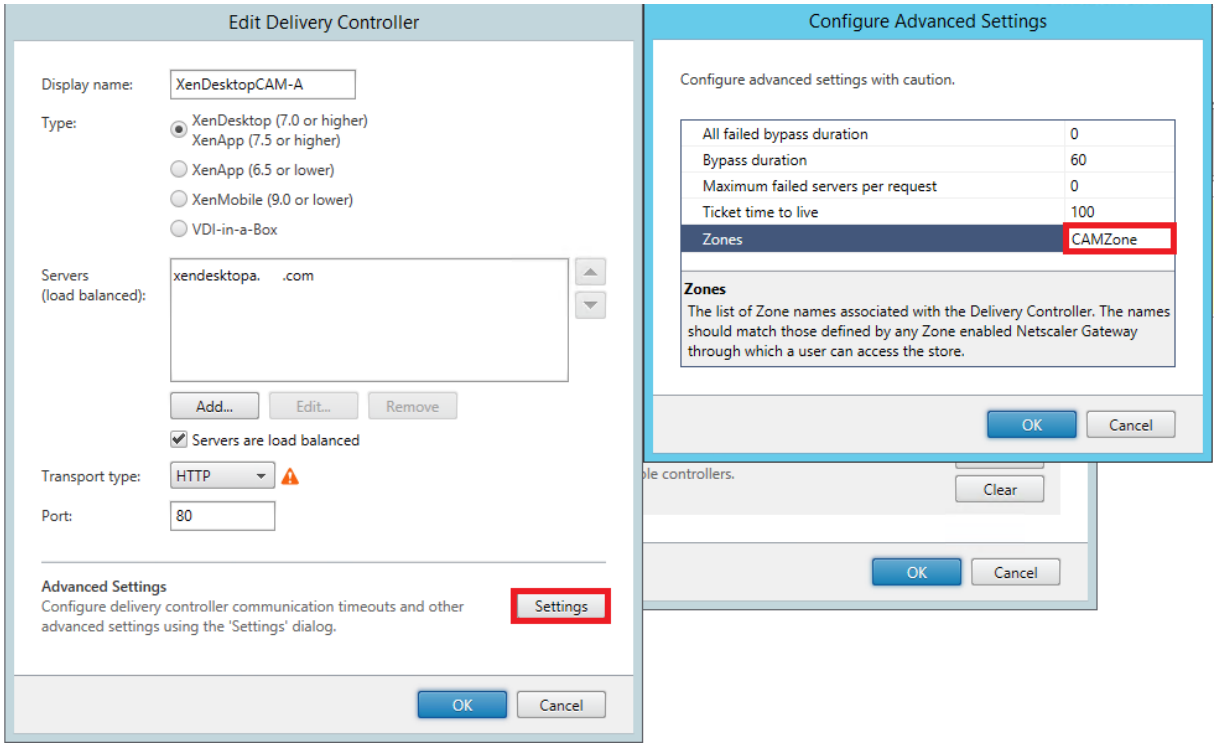
StoreFront では、定義済みゾーン内に位置するすべての Delivery Controller に対して最適なゲートウェイマッピングを作成することもできます。最適なゲートウェイへのゾーンのマッピングは、既によく知っているファームを使用したマッピングの作成とほぼ同義です。その唯一の違いは、ゾーンは通常、もっと多くの Delivery Controller を含む大規模なコンテナを表すものであるということです。すべての Delivery Controller を最適なゲートウェイマッピングに追加する必要はありません。Controller を目的のゾーン内に配置するには、それぞれの Delivery Controller に、既に Citrix Virtual Apps and Desktops 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 Citrix Gateway があり、その Citrix Gateway がそのゾーン内のリソースへの 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。

Delivery Controller のゾーンへの配置

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. コントローラーを選択して ［編集］ をクリックし、［**Delivery Controller** の編集］ 画面で ［設定］ をクリックします。
4. **Zones** 行で、2 番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。



最適な Citrix 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 や Citrix Virtual Apps and Desktops の公開アプリケーションなど）にアクセスする ICA 接続の処理を最適化します。通常、サイトの最適なゲートウェイは、同じ地理的な場所に配置されます。

「最適な Citrix 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。起動要求を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 の StoreFront を使用して、アプリやデスクトップなどの UK がホストするリソースへのリモートアクセスを提供します。

UK の StoreFront には、UK および US ベース両方の定義された Citrix Gateway と、Delivery Controller 一覧に UK および US Controller があります。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がない場合、すべての ICA 起動は、リソースが地理的にどこに位置しているかにかかわらず、起動要求を行った 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: 最適ではないゲートウェイルーティング

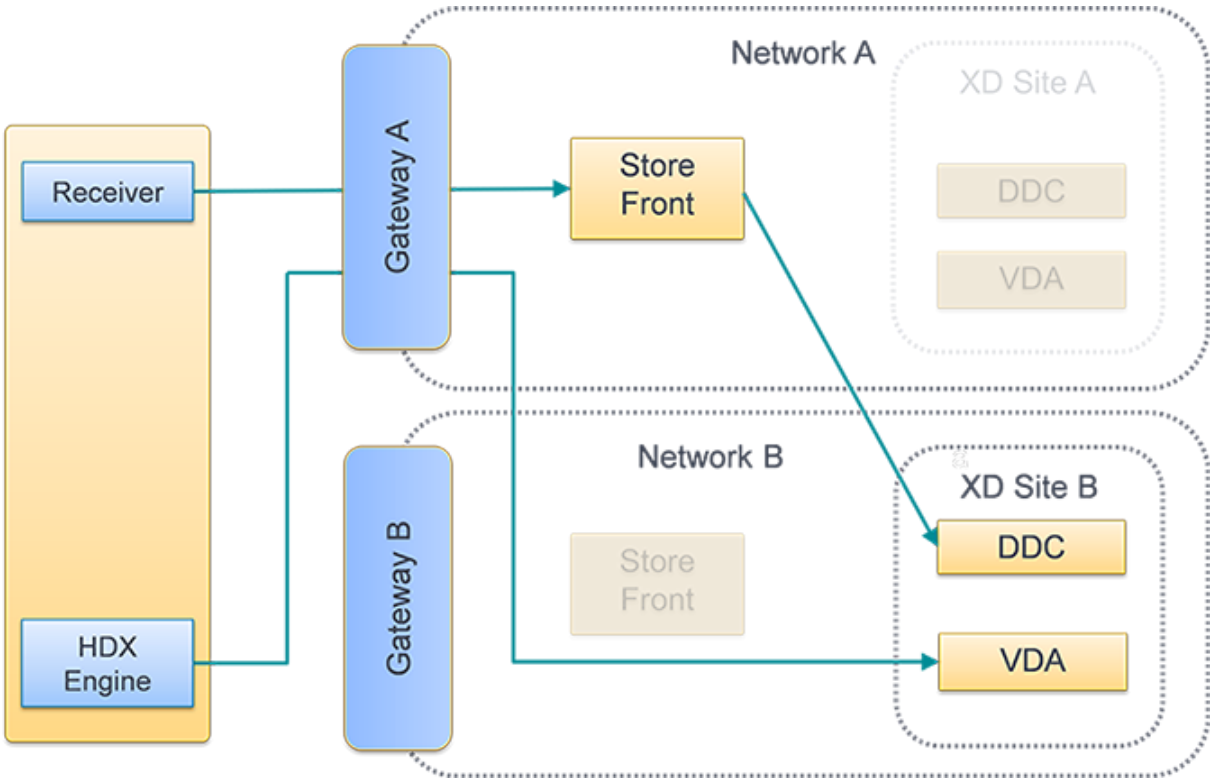
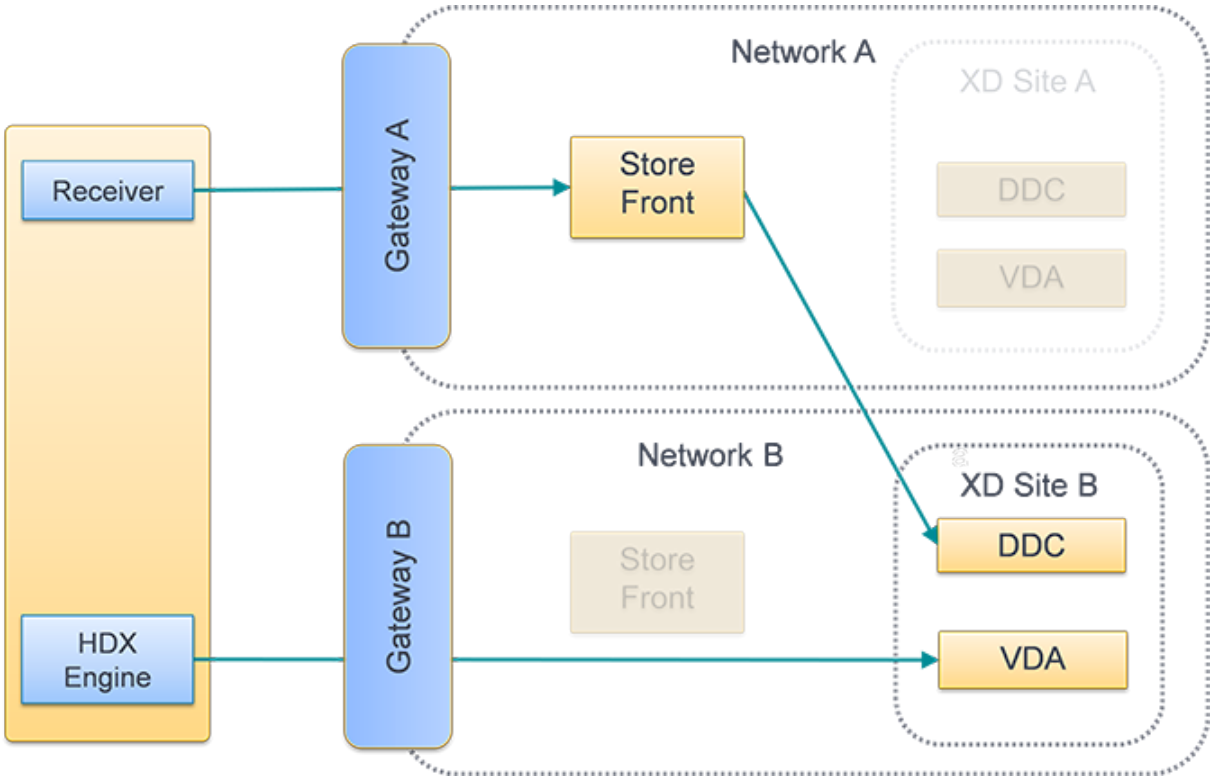


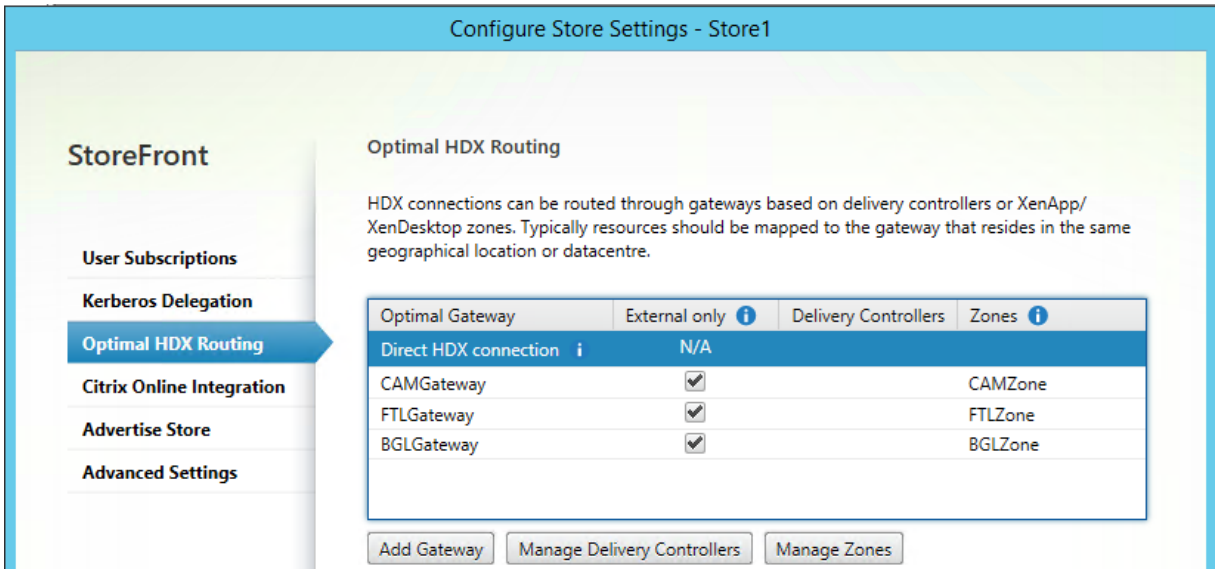
図 2：最適なゲートウェイルーティング



Citrix StoreFront 管理コンソールの使用

複数の展開環境で個別の Citrix Gateway アプライアンスを構成した後、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オンにすることは **-enabledOnDirectAccess = false** の使用と同等であり、［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に **Set-DSFarmsWithNullOptimalGateway** を使用した場合と同等の操作です。



新しい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、［Citrix Gateway の追加］画面が表示されます。

1. ［全般設定］ 画面で、［表示名］、［Citrix 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 Citrix 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、Citrix 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、Citrix Virtual Apps and Desktops 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、Citrix Virtual Apps and Desktops 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、リモートユーザーが認証資格情報を提供する方法を指定する設定を入力します。

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

PowerShell API パラメーター

-SiteId (Int)—Site ID within IIS. 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 Citrix 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 Citrix Gateway アプライアンスの完全修飾ドメイン名（FQDN）とポート番号を指定します。

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 Citrix 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 Citrix Virtual Apps and Desktops の展開環境の一覧を指定します。ファームには、公開リソースを提供する 1 つ以上の Delivery Controller を含めることができます。

複数の Delivery Controller を持つ Citrix Virtual Desktops 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 Citrix Virtual Apps and Desktops サーバーの URL 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 が使用できないと見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** に設定した場合：StoreFront に Citrix 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。

> ヒント：
>
> 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。

ファームの最適なゲートウェイの構成

> 注：
>
> **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
```

例

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”
Configure direct HDX connections for farms
```

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

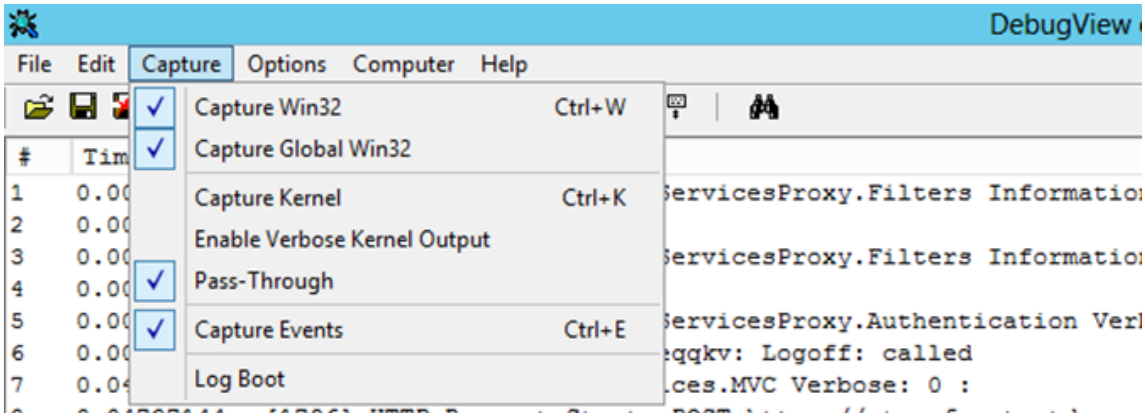
1. 次の PowerShell コマンドを実行して、すべてのサーバーグループノードで StoreFront のトレース機能を有効にします。

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

```



```
#Traces output is to c:\Program Files\Citrix\Receiver Storefront\
    admin\trace\
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

```
-  External client logs on **Gateway1**. Launch is directed through the
    designated optimal gateway **Gateway2** for the farm **Farm2**.

‘Set-DSOptimalGatewayForFarms -onDirectAccess=false‘

Farm2 is configured to use the optimal gateway Gateway2.

Farm2 has optimal gateway on direct access disabled.

The optimal gateway Gateway2 will be used for the launch.

-  Internal client logs on using StoreFront. Launch is directed through
    the designated optimal gatewayGateway1 for the farm Farm1.

```



```
‘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 is configured to use the optimal gateway Gateway1.

Farm1 has optimal gateway on direct access enabled.

The optimal gateway Gateway1 will be used for the launch.

-  Internal client logs on using Gateway1. 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‘

Dynamically identified gateway in request: Gateway1

Farm1 is configured to not use a gateway. 起動要求が経由するゲートウェイはありません。
```

Citrix Gateway および Citrix ADC との統合

January 14, 2020

Citrix Gateway を StoreFront と一緒に使って、企業ネットワークと Citrix ADC 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。

ゲートウェイとサーバー証明書の使用方法の計画

StoreFront を Citrix Gateway および Citrix ADC 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 Citrix Virtual Apps and Desktops コントローラーのグループ。
- 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 Citrix ADC 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。Citrix 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 Citrix Virtual Apps and Desktops』ホワイトペーパーおよび Citrix Virtual Apps and Desktops の「セキュリティ」セクションを参照してください。

Citrix Gateway VIP で認証が無効な場合の **StoreFront** ログオンの構成

Citrix Gateway VIP で認証が無効な場合に StoreFront にログオンします。この手順は次の 2 つのシナリオで機能します：
内部ネットワーク。X-Citrix-Gateway ヘッダーが StoreFront に渡される場合、Citrix Gateway の認証が無効で、STA が使用できないため、リモートの場所からアプリを起動できません。
Citrix Receiver for Web。Citrix Gateway VIP で認証が有効になっていない場合、Receiver クライアントは認証しません。

StoreFront サーバーでの変更

1. ［トークンの一貫性を要求する］ フィールドを無効にします：
   - StoreFront 3.0

a) ストアの Web サイトの`web.config`ファイルを編集します。たとえば、StoreFront ストア名が`NoAuth`の場合、StoreFront サーバーの`web.config`ファイルのパスは **inetpub\wwwroot\Citrix\NoAuth** です。

a) `web.config`ファイル内の次の行を特定し、値を True から False に変更します。
変更前:
`<resourcesGateways requireTokenConsistency="true">`
。変更後:
`<resourcesGateways requireTokenConsistency="false">`。

> 注:
>
> StoreFront 3.x の GUI で ［トークンの一貫性を要求する］ はチェックボックスです。詳しくは、「上級ストア設定」を参照してください。

b) `web.config`ファイルを保存して IIS サービスを再起動します。

2. **Citrix StoreFront** 管理コンソールを開きます。
3. ［**Receiver for Web** サイトの管理］ をクリックします。
4. 対応する Citrix Receiver for Web サイトを選択し、［構成］をクリックし、［認証方法］を選択します。
5. ［**Citrix Gateway** からのパススルー］ オプションをオフにしてください。

> 注:
>
> Citrix Gateway と［リモートアクセスの有効化］は StoreFront サーバーで設定されているものとします。

Citrix Gateway での変更

1. Citrix Gateway 仮想サーバーを開きます。
2. ［**Authentication**］ タブをクリックして ［**Enable Authentication**］ チェックボックスをオフにしてください。
3. 関連するセッションポリシーを、Citrix Gateway 仮想サーバーにバインドします。
4. 接続をテストします。

Citrix Gateway 接続の追加

April 2, 2020

［Citrix Gateway アプライアンスの追加］タスクを使用して、ユーザーがストアにアクセスするときに経由する Citrix Gateway 展開環境を追加します。Citrix 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 Citrix 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 Citrix Gateway の構成について詳しくは、「WebFront を使用した StoreFront との統合」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。完了したら、
> 構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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 ［**Citrix 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、Citrix Gateway 展開環境にわかりやすい表示名を指定します。

   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 Citrix 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、Citrix 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 Citrix 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 Citrix 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、Citrix 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、Citrix 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. Citrix Gateway 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 Workspace アプリ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。

   Citrix 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 Workspace アプリは、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 8 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）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. Citrix Gateway またはスタンドアロンの 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 Citrix 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 Citrix Gateway 認証サービスに接続して、Citrix 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。［次へ］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、Citrix Virtual Apps and Desktops 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、Citrix Virtual Apps and Desktops 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、Citrix Virtual Apps and Desktops 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 Virtual Apps and Desktops 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 Citrix Workspace アプリ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、Citrix 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、「Citrix Gateway 接続設定の構成」を参照してください。

Citrix 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 Workspace アプリは、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、デフォルトでシトリックスの Web サイト、および管理者が追加した最初の Citrix 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、「ビーコンポイントの構成」を参照してください。

ユーザーが Citrix 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。

Citrix Gateway のインポート

January 31, 2020

Citrix Gateway 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、Citrix Gateway と StoreFront を適切に構成して連携させるために Citrix Gateway 仮想サーバーをインポートする方法について説明します。

要件

- 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:
  >
  > Citrix ADC アプライアンスは、Citrix Virtual Apps and Desktops ウィザードを使用して作成されたゲートウェイ仮想サーバーのみをエクスポートできます。

- Citrix ADC アプライアンスにより生成される 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。
- Citrix ADC アプライアンスで生成される 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 Citrix ADC 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

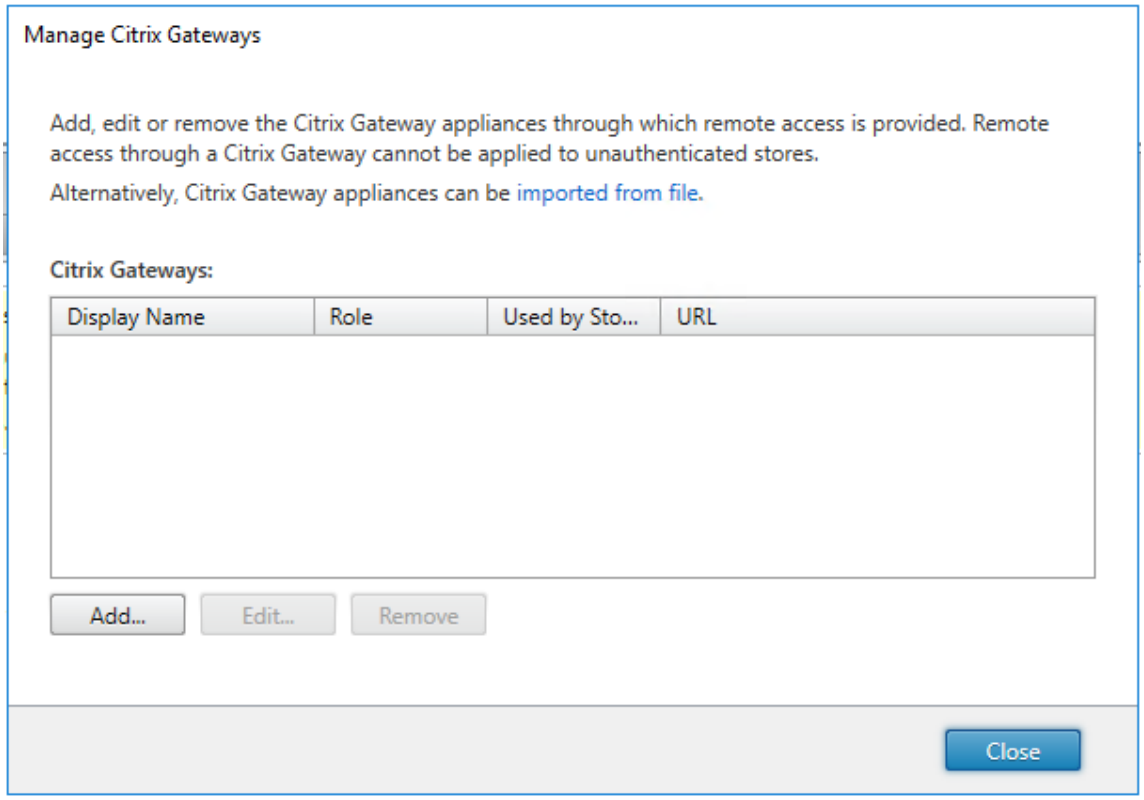
  環境内で外部と内部に違う DNS 名前空間を使用する場合は、コールバック URL とポートの組み合わせをゲートウェイ URL とポートの組み合わせとは異なるものにしても構いません。ゲートウェイを DMZ 内に配置して<example.com>の URL を使用しており、StoreFront はプライベートの社内ネットワークに配置して<example.local>の URL を使用している場合、<example.local>コールバック URL を使用して DMZ 内のゲートウェイ仮想サーバーへポイントバックすることができます。

コンソールを使用して **Citrix Gateway** をインポートする

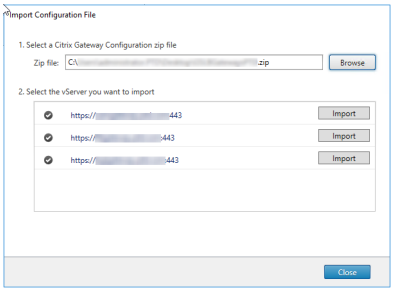
同じインポートファイルを使用して、1 つ以上の Citrix Gateway 仮想サーバー構成をインポートできます。異なる Citrix ADC アプライアンスからの複数のゲートウェイ仮想サーバーがある場合は、複数のインポートファイルを使用する必要があります。

> 重要:
>
> Citrix Gateway からエクスポートされた構成ファイルを手動で編集することはできません。

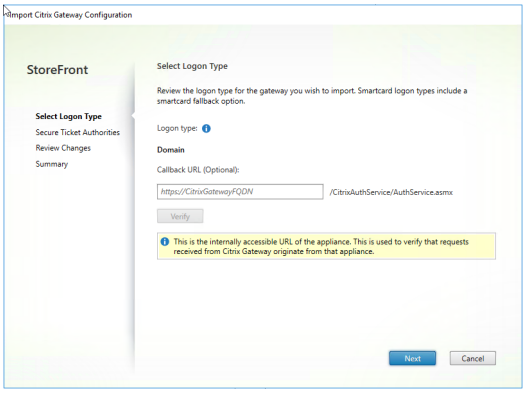
1. Citrix StoreFront 管理コンソールの左ペインで［ストア］を選択して、［操作］ペインの［**Citrix Gateway** の管理］ をクリックします。
2. ［Citrix Gateway の管理］画面で、［ファイルからインポート］ リンクをクリックします。



3. Citrix Gateway 仮想サーバー構成ファイルを参照します。
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 Workspace アプリ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。

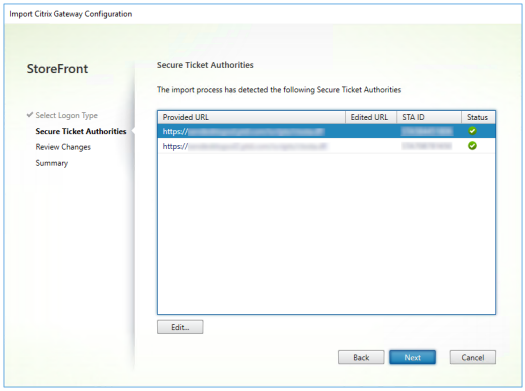


コンソールでのログオンタイプ	**JSON** ファイルでの **LogonType**	コールバック **URL** が必須
ドメイン	ドメイン	いいえ
ドメインおよびセキュリティトークン	DomainAndRSA	いいえ
セキュリティトークン	RSA	はい
スマートカード - フォールバックがありません	SmartCard	はい
スマートカード - ドメイン	SmartCardDomain	はい
スマートカード - ドメインおよびセキュリティトークン	SmartCardDomainAndRSA	はい
スマートカード - セキュリティトークン	SmartCardRSA	はい
スマートカード - SMS 認証	SmartCardSMS	はい
SMS 認証	SMS	はい

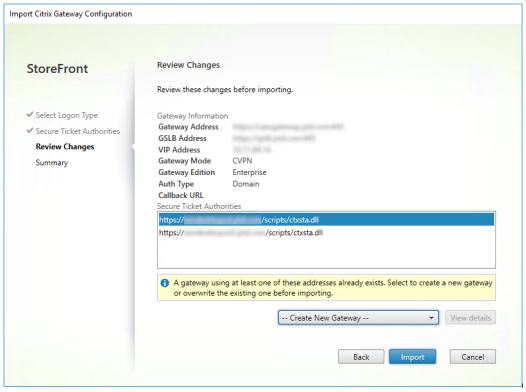
コールバック URL が必須な場合、ZIP ファイルに記載されているゲートウェイ URL に基づいて StoreFront によりコールバック URL が自動で入力されます。この URL は、適切な Citrix Gateway VIP にポイントバックする有効な URL に変更できます。GSLB ゲートウェイの場合、インポートするゲートウェイごとに固有のコールバック URL が必要です。

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. ［次へ］ 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. ［次へ］ 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 URL: 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	いいえ
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

ゲートウェイの設定	更新の可否
すべてのログオンの種類	はい

10. ［インポート］ 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:
>
> 別のゲートウェイを使用するように Citrix Workspace アプリ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、Citrix Workspace アプリ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、Citrix Workspace アプリ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。

PowerShell を使用して複数の Citrix Gateway をインポートする

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。
- Citrix Gateway 仮想サーバー構成ファイルの 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 }
```



```
54
55  StaLoadBalance          : True
56  CertificateThumbprints : {
57  F549AFAA29EBF61E8709F2316B3981AD503AF387 }
58
59  GatewayAuthType         :SmartCard
60  GatewayEdition          : Enterprise
61  ReceiverForWebSites     : {
62  Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
        ReceiverForWebSite }
```

CallbackURL を指定しない **Import-STFNetScalerConfiguration**

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。Citrix Gateway 構成の 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。

```
1  $ImportedGateways = Read-STFNetScalerConfiguration -path "$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。

```
1  ```
2  Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
       GatewayIndex 0 -Confirm:$False
3  Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
       GatewayIndex 1 -Confirm:$False
4  Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
       GatewayIndex 2 -Confirm:$False
5  ```
```

任意の **CallbackURL** を指定する **Import-STFNetScalerConfiguration**

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 URL 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。

```
1  $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
       USERPROFILE\desktop\GatewayConfig.zip"
2
```



```
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.com:443 -
    Confirm:$False
4
5 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.com:444 -
    Confirm:$False
6
7 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.com:445 -
    Confirm:$False
```

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、任意の **CallbackURL** を指定

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 URL 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。

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"
2
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:443" -Confirm:$False
4
5 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:444" -Confirm:$False
6
7 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:445" -Confirm:$False
```

Citrix Gateway 接続設定の構成

April 2, 2020

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 Citrix Gateway 環境の詳細を更新します。StoreFront での Citrix Gateway の構成について詳しくは、「WebFront を使用した StoreFront との統合」を参照してください。

Citrix Gateway 環境の構成を変更する場合は、その Citrix 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 Workspace アプリ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 Citrix Workspace アプリの最新の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。完了したら、
構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

Citrix Gateway の全般的な設定の変更

ユーザーに表示される Citrix Gateway 環境の名前を変更し、Citrix 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、［Citrix Gateway の管理］をクリックします。
3. Citrix 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 Workspace アプリに表示されます。そのため、ユーザーが使用する展開環境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 Citrix 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、Citrix 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 Citrix 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 Citrix 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。

   このサブネットアドレスは、Citrix 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、Citrix 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. アプライアンスが Citrix Gateway を実行している場合、［ログオンの種類］の一覧から、Citrix Workspace アプリ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。

Citrix 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 Workspace アプリは、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 Citrix Gateway またはスタンドアロンの Access Gateway 5.0 アプライアンスを実行している場合は、Citrix 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 Citrix Gateway 認証サービスに接続して、Citrix 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。

Access Gateway 5.0 アプライアンスの管理

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 Controller を経由するサイレントユーザー認証の有効化

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。

Secure Ticket Authority の管理

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、Citrix Virtual Apps and Desktops 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、Citrix Virtual Apps and Desktops 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 Citrix Gateway 展開環境を選択します。［操作］ペインの［Citrix 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 Virtual Apps and Desktops 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 Citrix Workspace アプリ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。

Citrix Gateway 展開環境の削除

［操作］ ペインで、［**Citrix Gateway** の管理］ の［削除］タスクを使用して、Citrix Gateway 展開環境の詳細を StoreFront から削除します。Citrix 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できなくなります。

Citrix ADC アプライアンスによる負荷分散

March 2, 2020

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。サーバーグループの StoreFront ノード間で Citrix Workspace アプリと Citrix Receiver for Web からの受信要求を負荷分散するため、Citrix ADC アプライアンスを構成する方法について詳しく説明します。この記事では、Citrix ADC アプライアンスで使用するために StoreFront モニターを構成する方法についても説明します。

このセクションの例は、次の環境でテストされています:

- 単一のサーバーグループ内に 4 つの Windows Server 2012 R2 StoreFront 3.x ノード。
- 最小接続および「変動しない」（CookieInsert）負荷分散用に構成された Citrix ADC アプライアンス 12.1 ロードバランサー 1 つ。
- Citrix Workspace アプリがインストールされた Windows 10 テストクライアント 1 台。

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」のセクションを確認します。

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証明機関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。

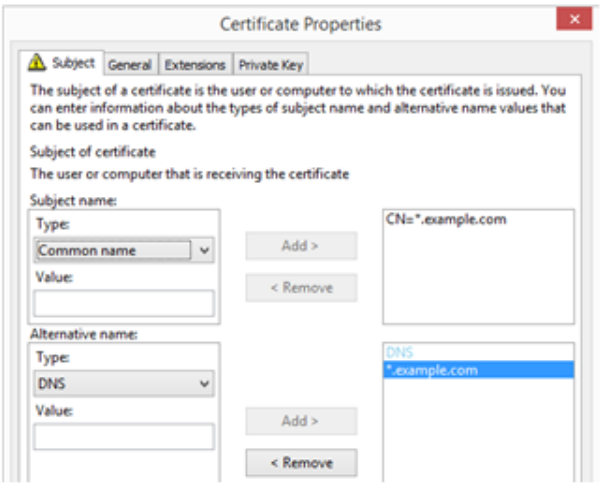
- オプション **1**: **.example.com* ワイルドカード証明書を Citrix ADC アプライアンス負荷分散仮想サーバーと StoreFront サーバーグループノードの両方で使用する。これにより構成が簡素化され、将来的には証明書を置き換える必要なく追加の StoreFront サーバーを増やすことができます。
- オプション **2**: サブジェクトの別名（SAN）を含む証明書を Citrix ADC アプライアンス負荷分散仮想サーバーと StoreFront サーバーグループノードの両方で使用する。すべての StoreFront サーバーの完全修飾ドメイン名（FQDN）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されるため、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。

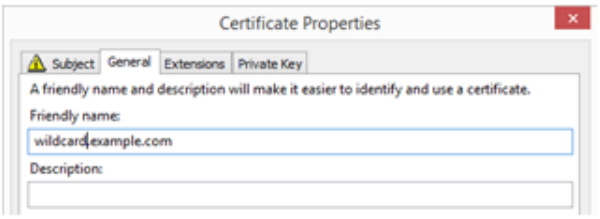
メールアドレスによる検出の構成について詳しくは、以下を参照してください。http://blogs.citrix.com/2013/04/01/configuring-email-based-account-discovery-for-citrix-receiver/

> 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。次の 2 つの別個の証明書を使用します: Citrix ADC アプライアンス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。どちらの証明書にもサブジェクトの別名が必要です。

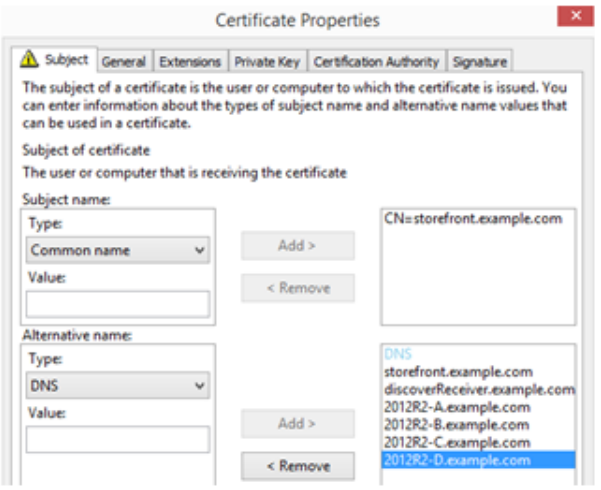
Example Web server certificates

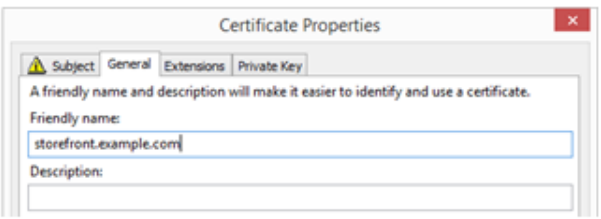
Option 1: Wildcard certificate



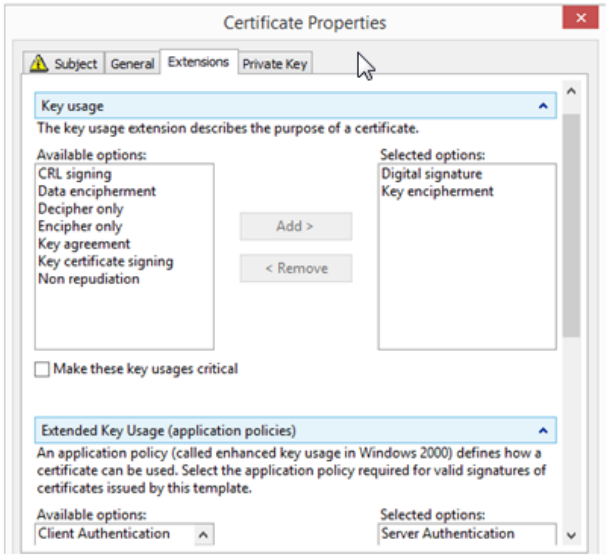


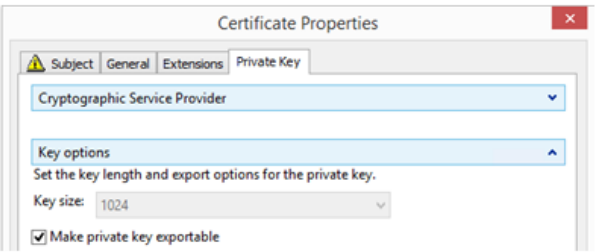
Option 2: SAN certificate with every StoreFront server





Common Properties





Citrix ADC アプライアンス負荷分散および **StoreFront** サーバーに対する **SSL** 証明書の作成

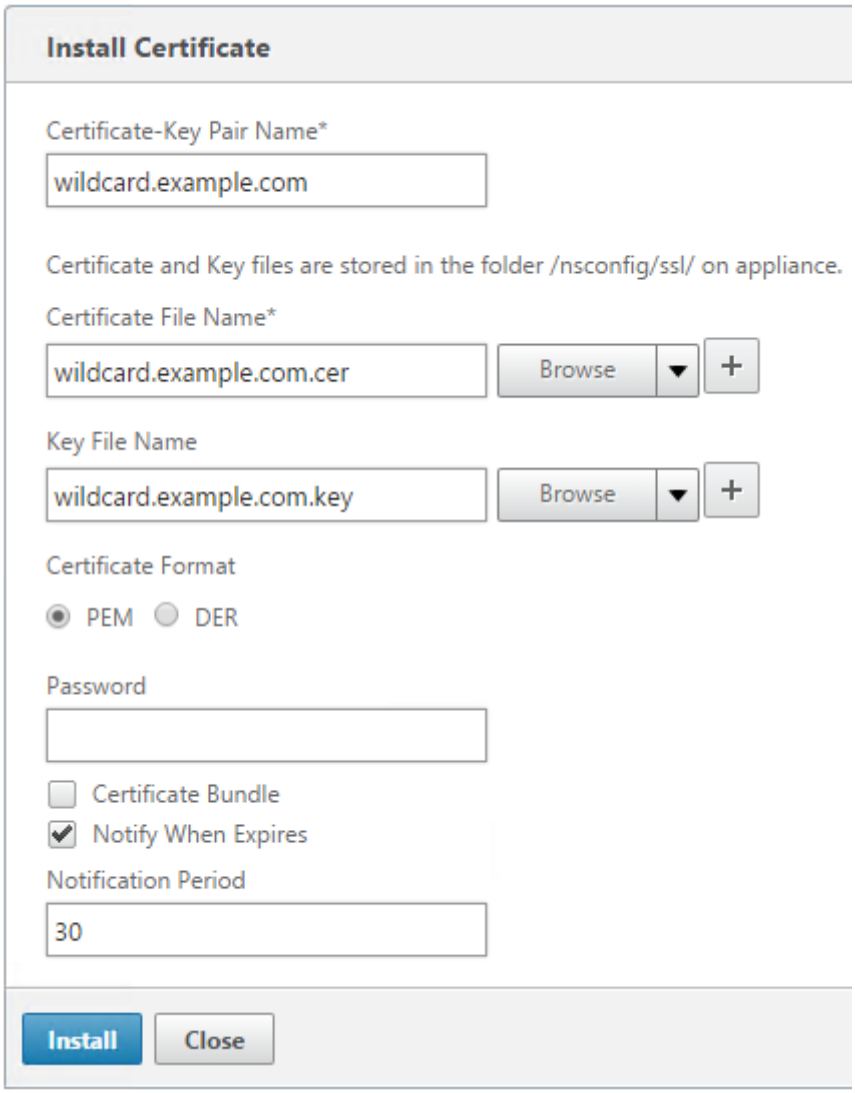
Windows 証明機関から発行された証明書の **Citrix ADC** アプライアンスへのインポート

- WinSCP は、Windows マシンから Citrix ADC アプライアンス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、Citrix ADC アプライアンス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、Citrix ADC アプライアンスで OpenSSL ツールを使用して *PKCS12* または *PFX* ファイルから証明書とキーを抽出し、Citrix ADC で使用できる X.509 の CER ファイルと KEY ファイルを PEM 形式で個別に作成することもできます。

1. この PFX ファイルを Citrix ADC アプライアンスまたは VPX の */nsconfig/ssl* にコピーします。
2. Citrix ADC アプライアンスの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 Citrix ADC アプライアンス CLI を閉じ、FreeBSD シェルに切り替えます。
4. `cd /nsconfig/ssl/`を使用してディレクトリを変更します。
5. `openssl pkcs12 -in <imported cert file>.pfx -nokeys -out <certfilename>.cer`を実行します。PFX のパスワードの入力を求めるメッセージが表示されたら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、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、Citrix ADC アプライアンス CLI に戻ります。

インポート後の **Citrix ADC** アプライアンスでのサーバー証明書の構成

1. Citrix ADC アプライアンス管理 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。
   - Citrix ADC アプライアンス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。
   - 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`が負荷分散仮想サーバーの仮想 IP（VIP）に解決されます。

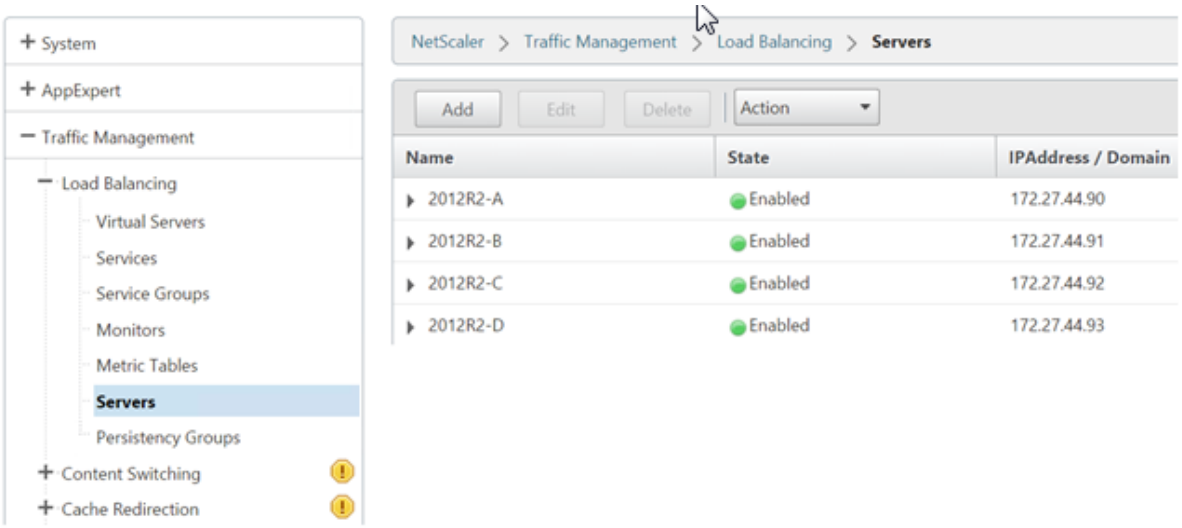
シナリオ **1**：クライアントと **Citrix ADC** アプライアンスロードバランサー間、および **Citrix ADC** アプライアンスロードバランサーと複数の **StoreFront 3.x** サーバー間のエンドツーエンドの **HTTPS 443** セキュア接続

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。

個々の **StoreFront** サーバーノードの **Citrix ADC** アプライアンスロードバランサーへの追加

1. Citrix ADC アプライアンス管理 GUI にログオンします。
2. [**Traffic Management**] > [**Load Balancing**] > [**Servers**] > [**Add**] 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 ノード（2012R2-A ～ 2012R2-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。

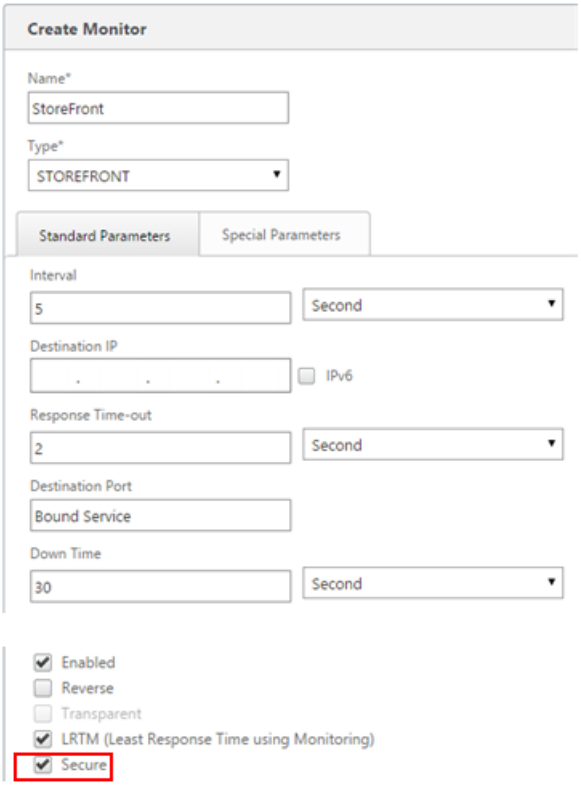


StoreFront モニターを定義して、サーバーグループ内のすべての **StoreFront** ノードをチェックします

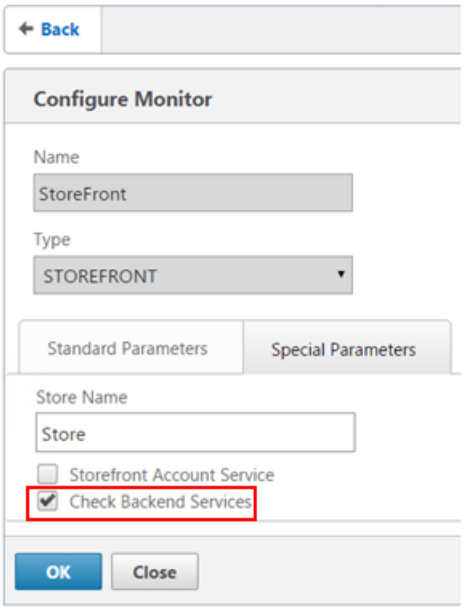
1. Citrix ADC 管理 GUI にログオンします。
2. [**Traffic Management**] > [**Load Balancing**] > [**Monitors**] > [**Add**] の順に選択し、*StoreFront* を呼び出す新しいモニターを追加し、すべてのデフォルトの設定を受け入れます。
3. [**Type**] ドロップダウンの一覧から [**StoreFront**] を選択します。
4. 負荷分散仮想サーバーと StoreFront 間で HTTPS 接続を使用している場合は、[**Secure**] オプションを選択する必要があります。その他の場合は選択しません。
5. [**Special Parameters**] タブで [**Store Name**] を入力します。
6. [**Special Parameters**] タブで [**Check Backend Services**] オプションを選択します。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、次のサービスの状態が返されます:

   - W3SVC（IIS）
   - WAS（Windows プロセスアクティブ化サービス）
   - CitrixCredentialWallet
   - CitrixDefaultDomainService

Standard Parameters Tab

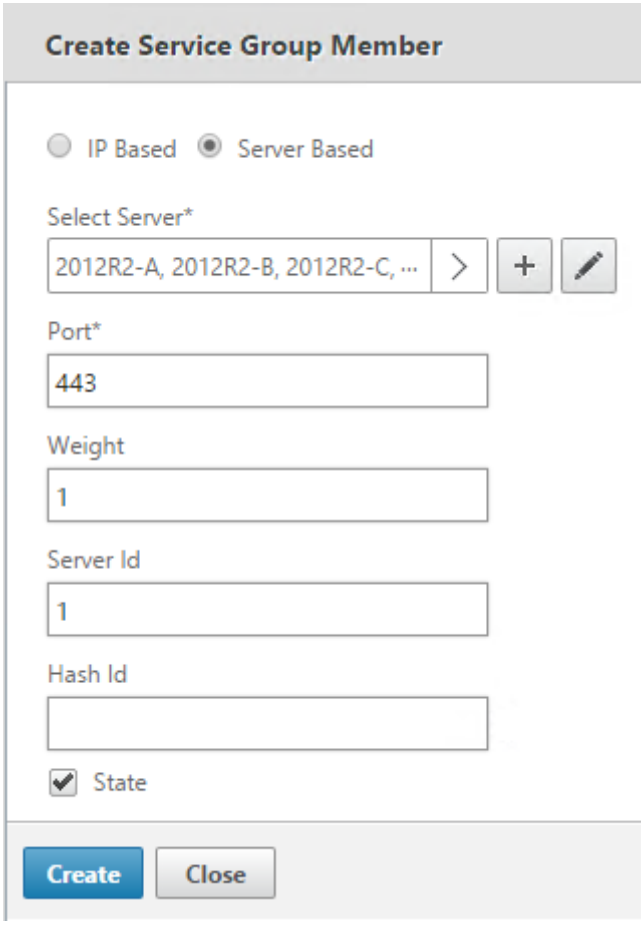


Special Parameters Tab

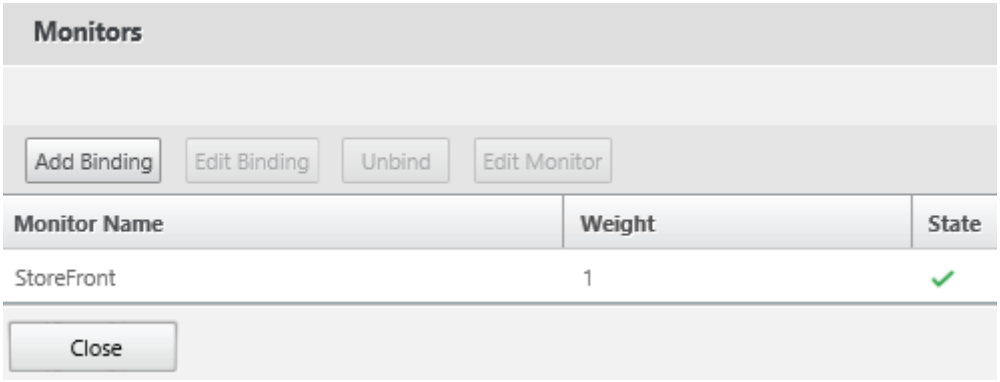


すべての **StoreFront** サーバーを含む **HTTPS 443** サービスグループの作成

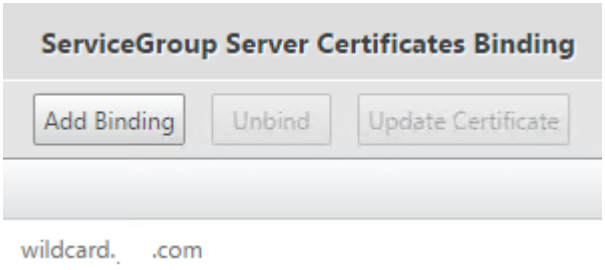
1. サービスグループ内で、右側の［**Members**］オプションを選択し、サーバーセクションで以前定義したすべての StoreFront サーバーノードを追加します。
2. TLS ポートを設定し、追加する各ノードに一意のサーバー ID を指定します。



3. [**Monitors**] タブで前に作成した StoreFront モニターを選択します。

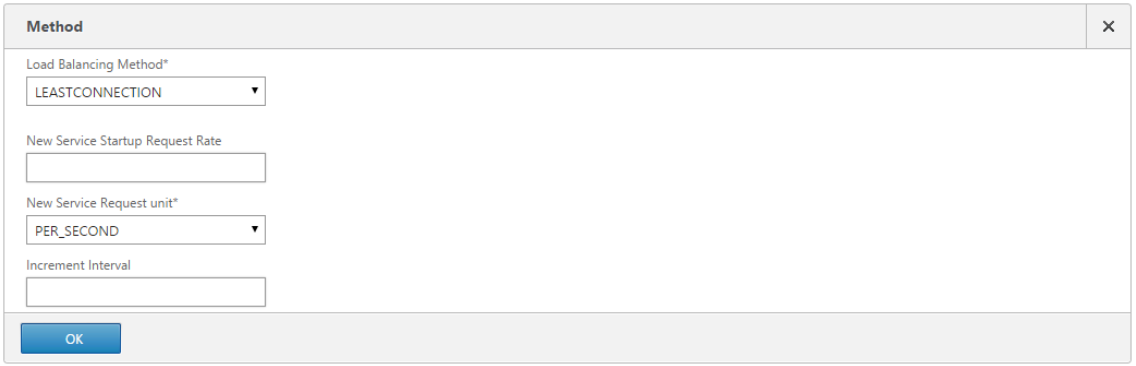


4. [**Certificates**] タブで、前にインポートした SSL 証明書をバインドします。
5. 以前にインポートしたサーバー証明書の署名に使用された CA 証明書と、PKI チェーン信頼の一部の可能性があるそのほかの CA をバインドします。

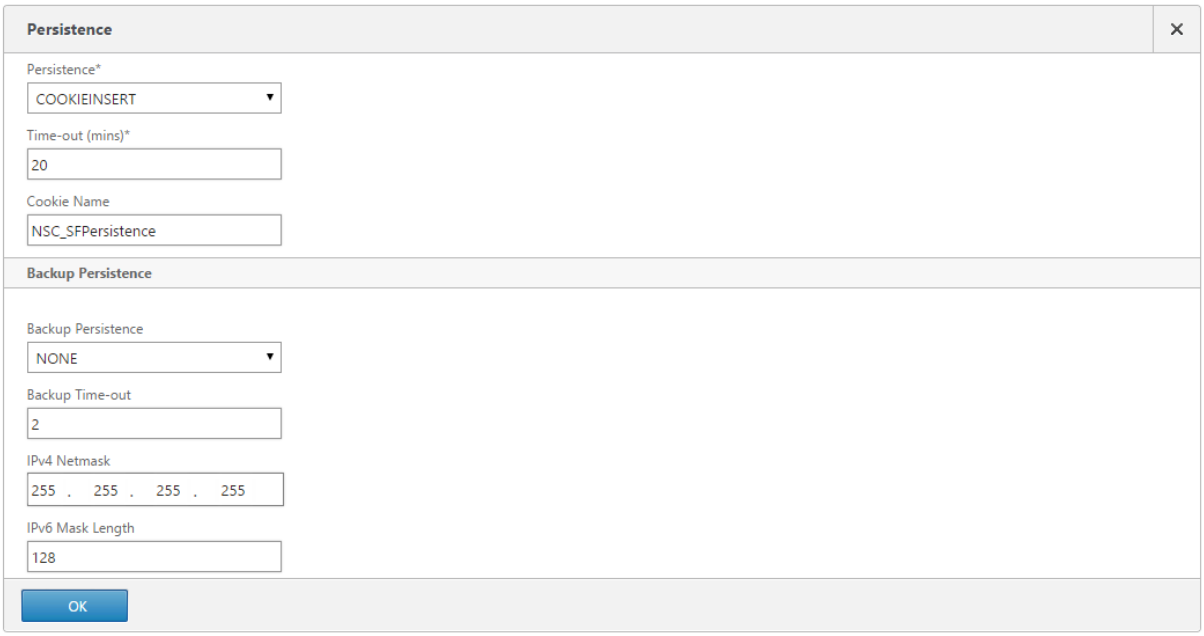


ユーザートラフィック用負荷分散仮想サーバーの作成

1. Citrix ADC アプライアンス管理 GUI にログオンします。
2. [**Traffic Management**] > [**Load Balancing**] > [**Virtual Servers**] > [**Add**] 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。例えば、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**: **HTTPS** 終了 **-** クライアントと **Citrix ADC** 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.x** 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。

個々の **StoreFront** サーバーの **Citrix ADC** ロードバランサーへの追加

1. Citrix ADC 管理 GUI にログオンします。
2. [**Traffic Management**] **>** [**Load Balancing**] **>** [**Servers**] **>** [**Add**] 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 サーバー（2012R2-A ～ 2012R2-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。

HTTP 8000 StoreFront モニターを定義して、サーバーグループ内のすべての **StoreFront** サーバーをチェックします

1. Citrix ADC 管理 GUI にログオンします。
2. [**Traffic Management**] **>** [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**] 一覧で [**StoreFront**] を選択します。
5. [**Special Parameters**] タブで [**Store Name**] を入力します。
6. [**Destination Port**] に「8000」と入力して、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**] オプションを選択します。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。

すべての **StoreFront** サーバーを含む **HTTP 80** サービスグループの作成

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. 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。

ユーザートラフィック用 **SSL** 終了負荷分散仮想サーバーの作成

1. [**Traffic Management**] > [**Load Balancing**] > [**Virtual Servers**] > [**Add**] 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、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。
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。

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。

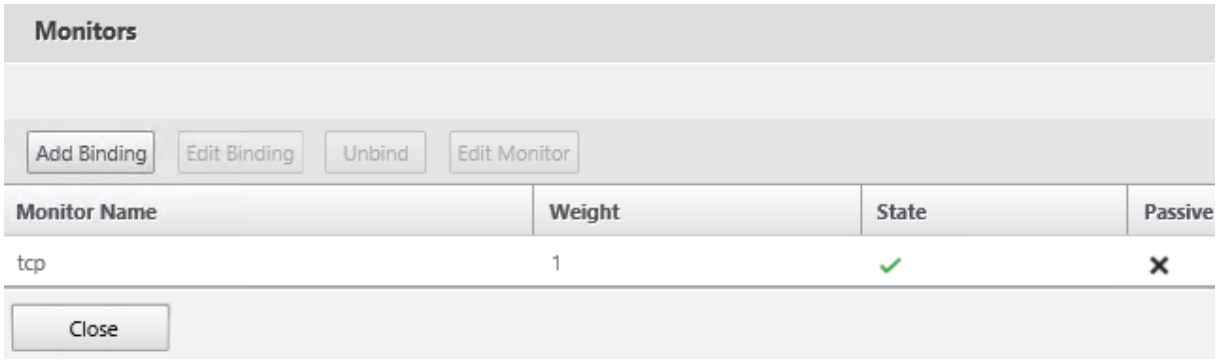
- オプション **1**: 単一の仮想サーバーの作成: ユーザートラフィックのみを負荷分散。公開アプリケーションおよびデスクトップの ICA 起動のみを実行する場合は、必要なのはこれですべてです（必須、かつ通常はこれが必要なすべてです）。

- 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、定期的な取得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 Citrix ADC アプライアンスで 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

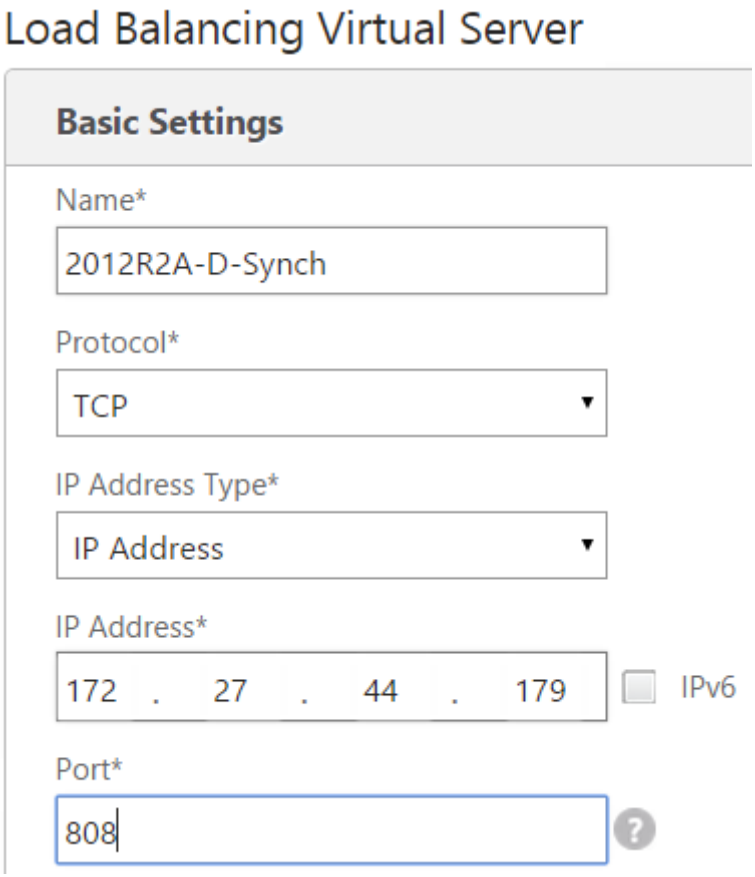
1. Citrix ADC アプライアンス管理 GUI にログオンします。
2. [**Traffic Management**] > [**Service Groups**] > [**Add**] の順に選択し、新しいサービスグループを追加します。
3. プロトコルを [**TCP**] に変更します。
4. サービスグループ内で、右側の [**Members**] オプションを選択し、サーバーセクションで以前定義したすべての StoreFront サーバーノードを追加します。
5. [**Monitors**] タブで、TCP モニターを選択します。



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

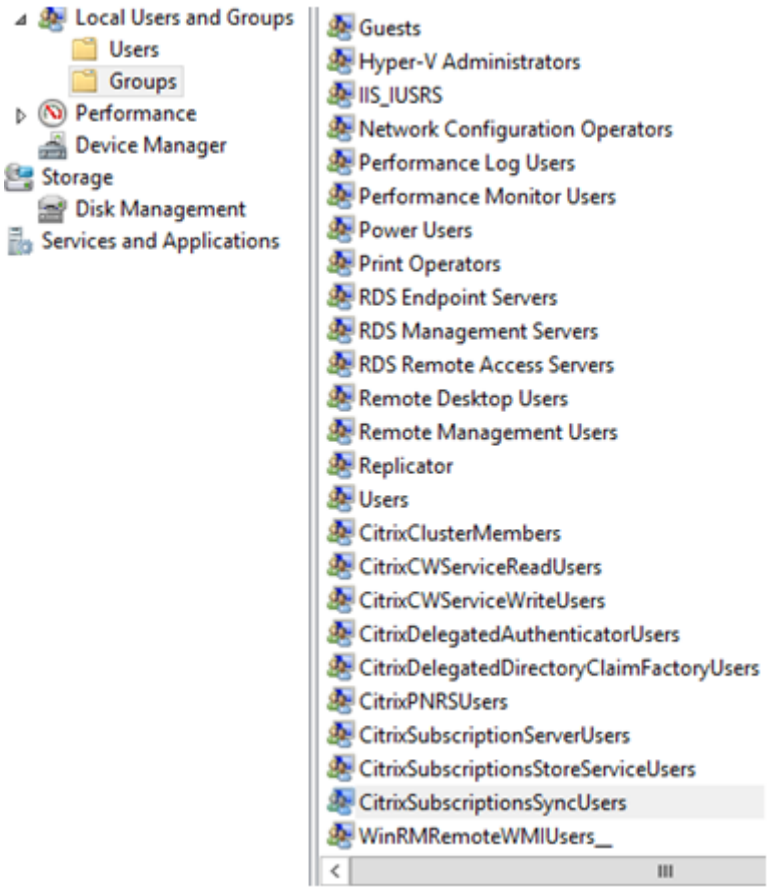
1. Citrix ADC アプライアンス管理 GUI にログオンします。
2. [**Traffic Management**] > [**Service Groups**] > [**Add**] の順に選択し、新しいサービスグループを追加します。
3. 負荷分散方式を [**round robin**] に設定します。
4. プロトコルを [**TCP**] に変更します。

5. ポート番号には **443** ではなく、「**808**」と入力します。



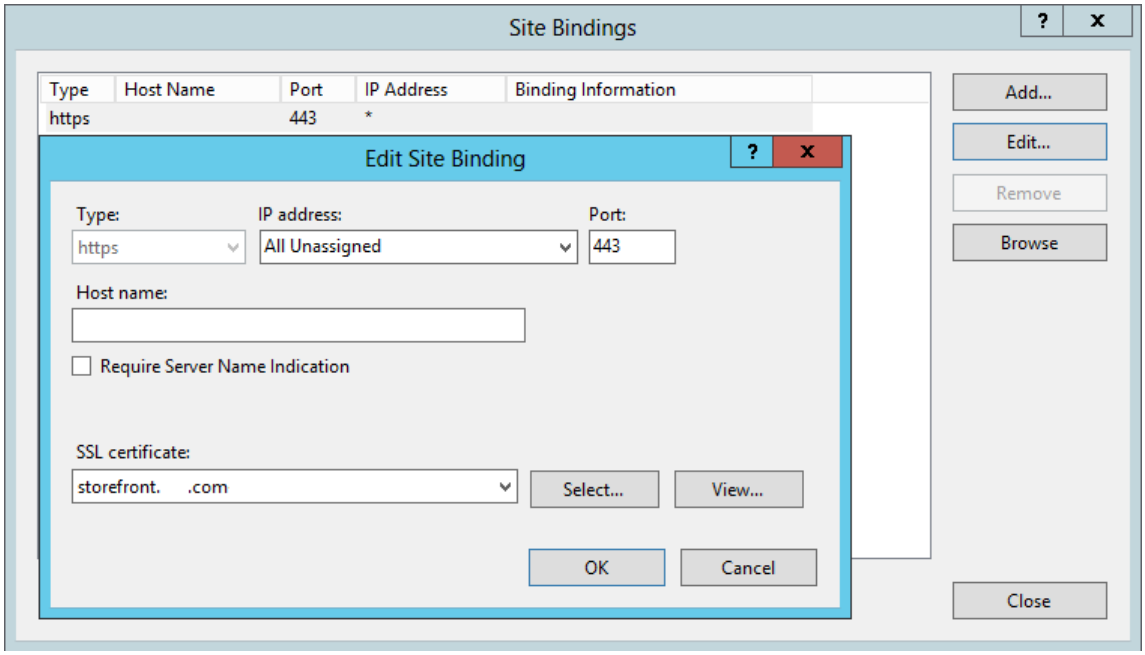
CitrixSubscriptionsSyncUsers 内のメンバーシップ

場所 **A** にある **StoreFront** サーバー **A** について、別の場所にあるサーバー **B** のサブスクリプションデータを要求および取得するには、サーバー A はサーバー B 上の **CitrixSubscriptionsSyncUsers** ローカル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。**CitrixSubscriptionsSyncUsers** ローカルグループには、特定のサーバーからのサブスクリプションデータを取得するため認証されたすべてのリモート StoreFront サーバーのアクセス制御リストが含まれます。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取得するため、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。



シナリオ **1**: **Citrix ADC** と **StoreFront** 間で **HTTPS** を使用して **StoreFront** サーバーグループを構成

1. Citrix ADC アプライアンス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。

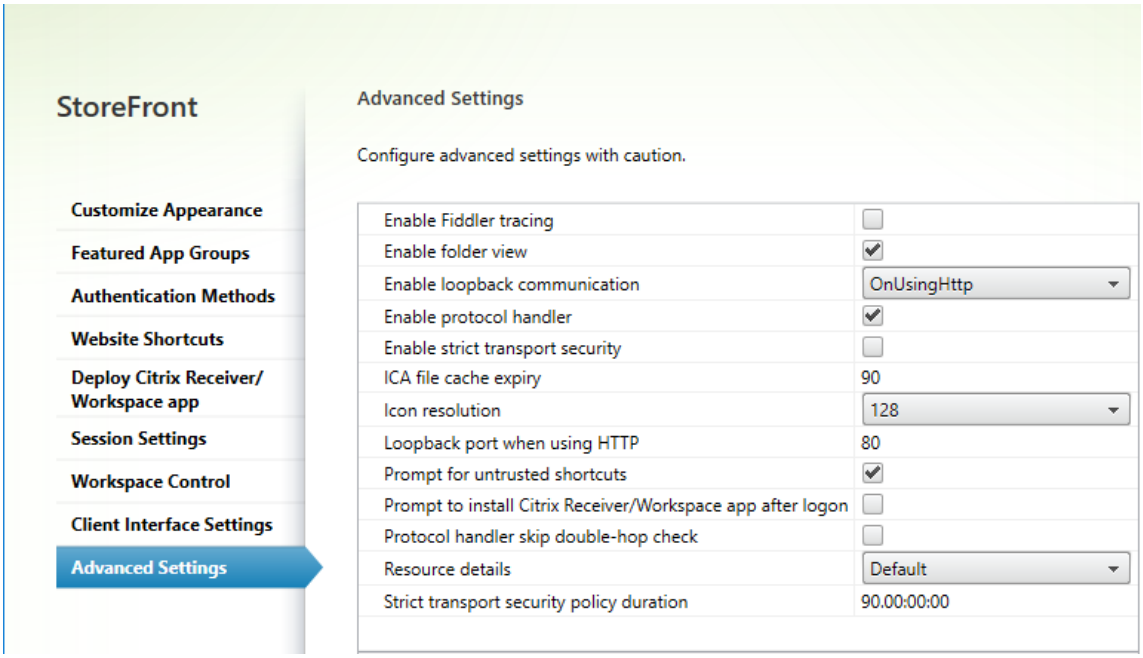


3. Citrix ADC ロードバランサーと StoreFront 間で HTTPS を使用している場合、共通名（CN）またはサブジェクトの別名（SAN）として負荷分散された FQDN を含む証明書を使用する必要があります。

   「Citrix ADC アプライアンス負荷分散および 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。

シナリオ **2**：**Citrix ADC** と **StoreFront** 間で **HTTP** を使用して **StoreFront** サーバーグループを構成

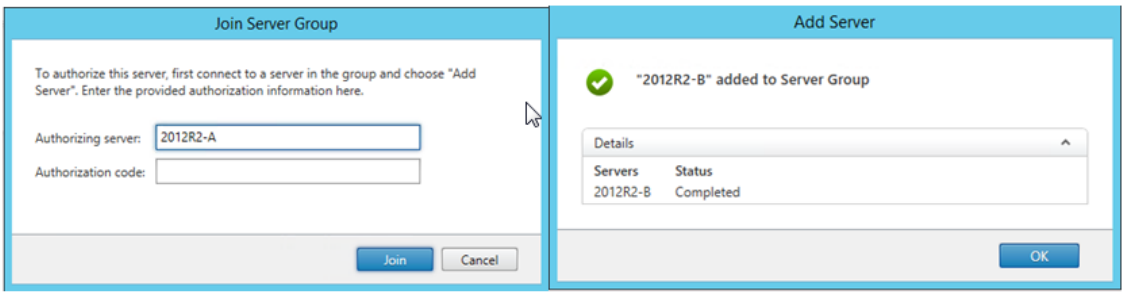
1. 既に存在する場合は、すべての StoreFront ノードから IIS の HTTPS バインドを削除します。
2. HTTP バインドが IIS に存在し、ポート 80 を使用するように設定されていることを確認してください。
3. 以下のように Receiver for Web 内でループバック設定で **OnUsingHTTP** とポート **80** を構成します。この手順は、ネイティブの Citrix Workspace アプリと Receiver for Web 間のクライアント検出を成功させるために不可欠です。



シナリオ **1** と **2** の両方に共通の手順

1. 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。
2. StoreFront のインストール時に、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。この URL は、シナリオ 1 と 2 の両方で`https://storefrontlb.domain.com`であり、Citrix ADC 負荷分散仮想サーバーの完全修飾ドメイン名に一致する必要があります。

   「Citrix ADC アプライアンス負荷分散および 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。
3. 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。
4. 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。



5. 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。

6. 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。

Citrix サービスモニター

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 Citrix ADC アプライアンスなどほかの 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 1 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、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。

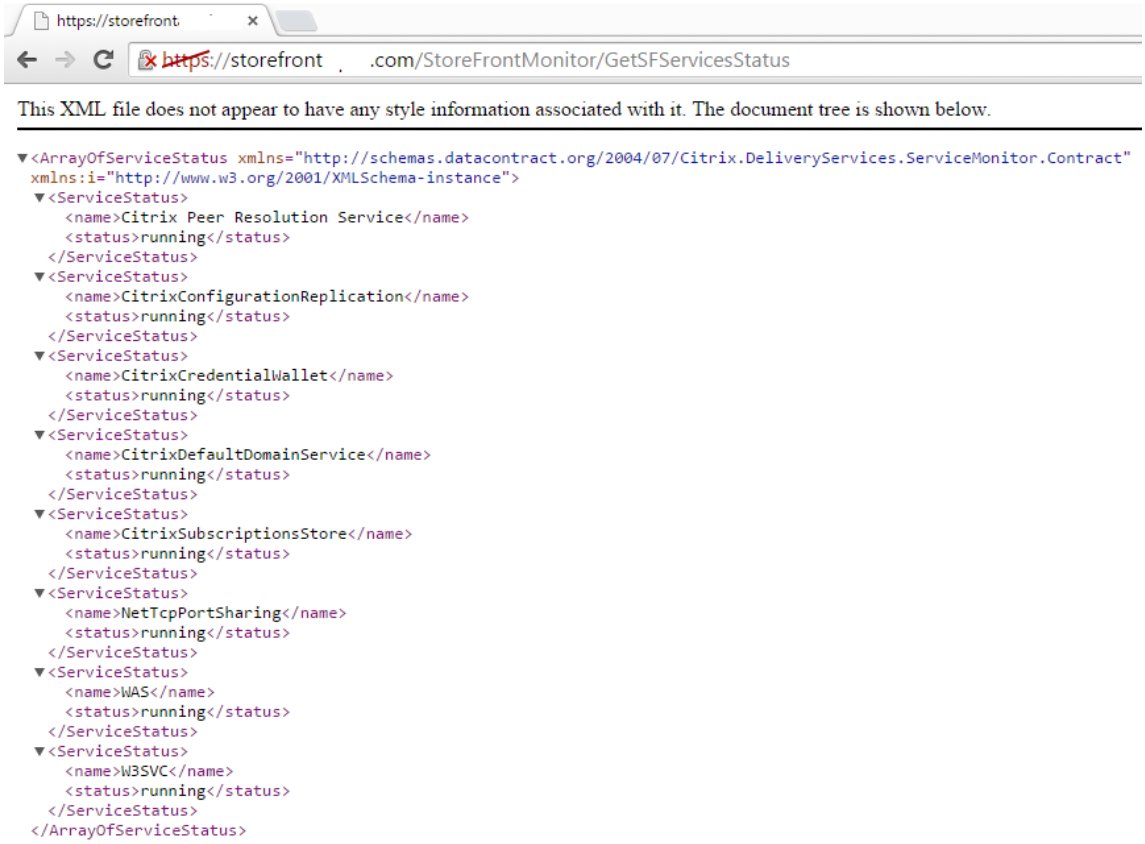
デフォルトのサービスモニターを削除し、**HTTPS** およびポート **443** を使用するものに置き換える

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。

```
$ServiceUrl = ”https://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://<loadbalancingFQDN>:443/StoreFrontMonitor/GetSFServicesStatus`

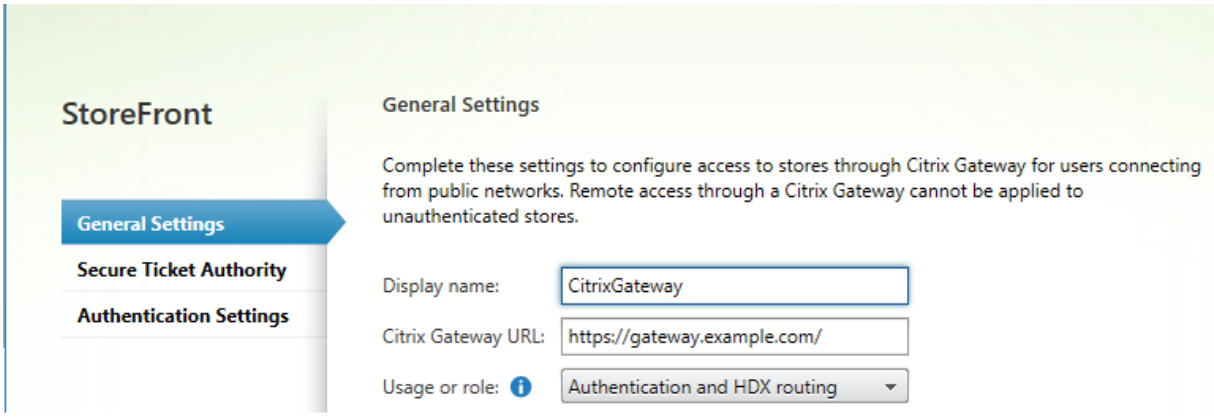


同じ **Citrix ADC** アプライアンス上の **Citrix Gateway** および負荷分散仮想サーバー

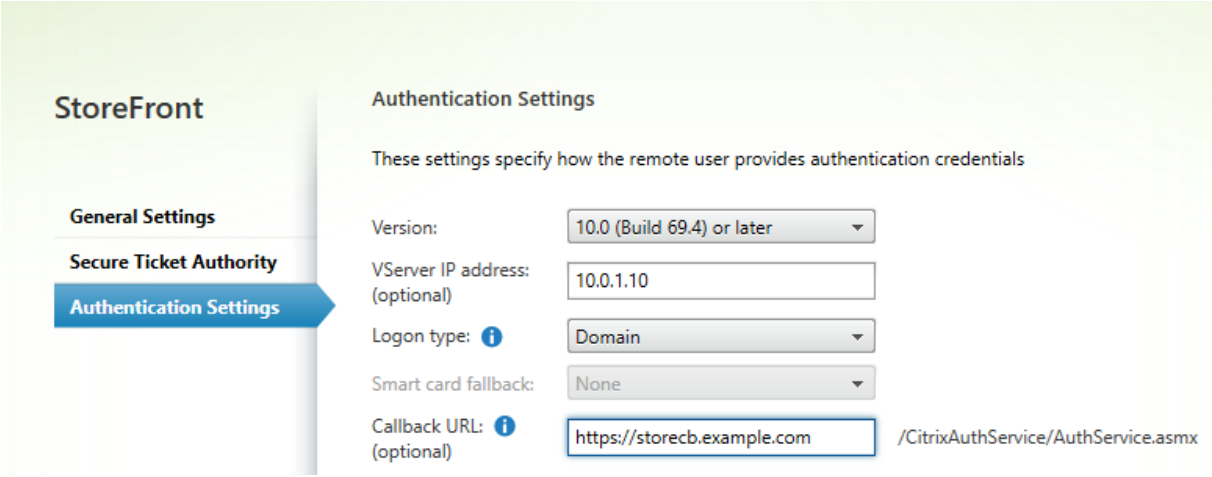
同じ Citrix ADC アプライアンス上に構成済みの Citrix Gateway 仮想サーバーと負荷分散仮想サーバーがある場合、内部ドメインユーザーが Citrix Gateway 仮想サーバーを経由するのではなく StoreFront 負荷分散ホストベース URL に直接アクセスしようとすると問題が発生することがあります。

この場合、StoreFront はユーザーのソース IP アドレスと Citrix Gateway のサブネット IP アドレス（SNIP）とを互いに関係づけるため、エンドユーザーは Citrix 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 Citrix Gateway サイレント認証を実行しようとします。この問題を回避するには、次に示すように SNIP アドレスを省くか VIP を入力して、AGBasic ログオンプロトコルでなくユーザー名とパスワードによる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 **Citrix Gateway** の構成



Citrix Gateway VIP で［VServer IP address］フィールドに入力します。同じ Citrix ADC アプライアンスに負荷分散仮想サーバーがある場合、Citrix Gateway で SNIP を使用しないでください。



Citrix ADC アプライアンスを使って **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

PowerShell を使ってループバックオプションを設定できます。

Receiver for Web web.config ファイルの例

```
<communication attempts="2" timeout="00:01:00" loopback="On"
    loopbackPortUsingHttp="80">
```

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。	TLS 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 TLS 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、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 Citrix Gateway に 2 つの URL を構成する

September 10, 2019

StoreFront では、管理コンソールの［**Citrix Gateway** の管理］の［追加］ または ［編集］ から Citrix Gateway の URL を 1 つだけ追加できます。また、［**Citrix Gateway** の管理］の［ファイルからインポート］ で、Citrix 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、次のユースケースで、StoreFront での Citrix Gateway の管理が簡素化されます:

1. **GSLB** と複数の **Citrix Gateway**。GSLB と複数の Citrix 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 **Citrix 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 Citrix Gateway を使用します。

これは高度な機能とトピックです。StoreFront ゲートウェイとグローバルサーバー負荷分散（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 Citrix 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 Citrix 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。最適なゲートウェイルーティングについて詳しくは、「可用性の高いマルチサイトストアのセットアップ」を参照してください。

2 つのゲートウェイ **URL** を使用する場合の展開に関する検討事項

- ゲートウェイ URL FQDN は、StoreFront 管理コンソール内の各ゲートウェイに対して表示されます。各ゲートウェイの GSLBURL プロパティは、PowerShell コマンドレットを使用した場合にのみ表示されます。
- ゲートウェイ URL は、ネイティブの Citrix Receiver および Citrix Workspace アプリによって認証に使用されます。
- ゲートウェイ URL は、ストアおよびゲートウェイ情報を使用して Citrix Receiver および Citrix Workspace アプリを構成するために使用されるプロビジョニングファイル（receiver.cr）内の場所タグに含まれます。
- 提供されている Powershell を使用して、ストアおよびローミングの web.config ファイルを変更します。この操作は手動で行わないでください。

> 重要:
>
> -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してください。Citrix Gateway 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
```

スプリット **DNS** を使用して内部と外部の両方からアクセスされる **Citrix 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

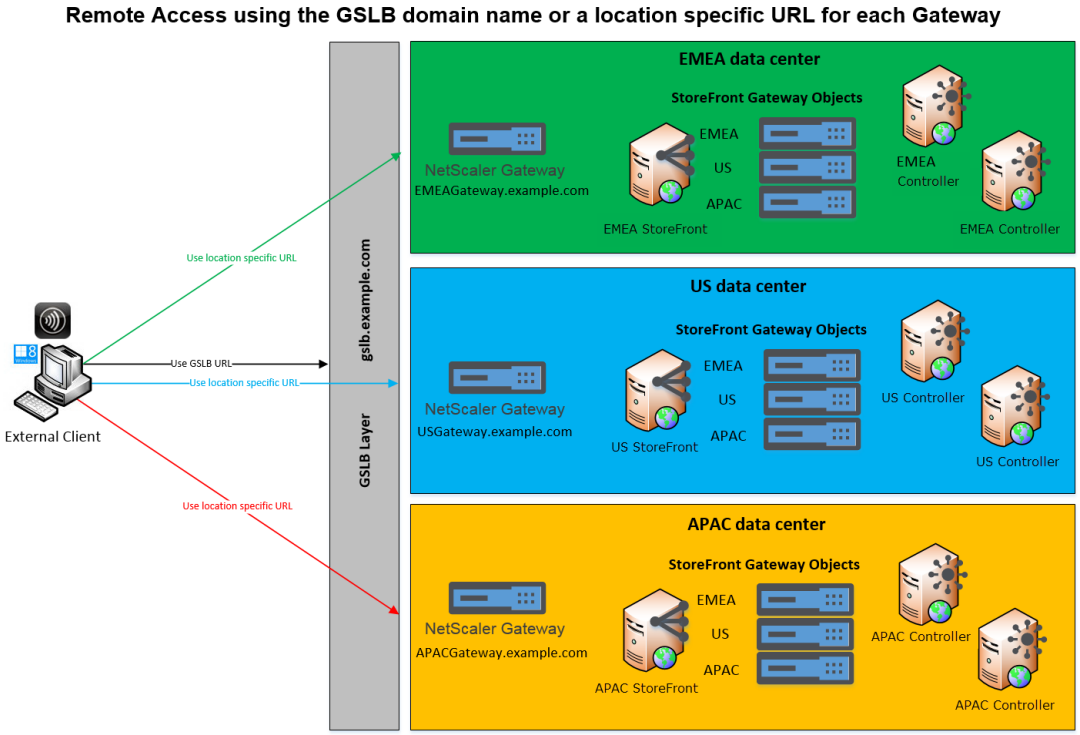
GSLB を経由した外部アクセス用のパブリック署名済み SAN サーバー証明書に、次の FQDN を含めます。

```
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。

ユースケース 1：Receiver for Web：GSLB および複数の Citrix Gateway

管理者が GSLB と複数の Citrix 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 Citrix ADC アプライアンス上で構成されている各 GSLB は、ゲートウェイ VPN 仮想サーバーとして機能しています。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 Citrix 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 Citrix 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 Citrix Virtual Apps and Desktops 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。

ユースケース 1：**Receiver for Web** と、**Citrix Receiver** または **Citrix Workspace** アプリ：**GSLB** および複数の **Citrix Gateway**

ゲートウェイ属性

ネイティブの Citrix Receivers または Citrix Workspace apps アプリで GSLB を使用するには、**Add-STFRoamingGateway**（作成）または **Set-STFRoamingGateway**（変更）を使用して、次の属性を指定します：

-GatewayUrl - すべての GSLB ゲートウェイの共有 FQDN として設定

-GSLBurl - ゲートウェイごとに固有のゲートウェイ FQDN として設定

> 注：
>
> 直観に反しているように思えるかもしれませんが、これはこの Web ユースケースには影響しません。これにより、ネイティブの Citrix Receiver または Citrix Workspace アプリが、エンドポイント`https://storefront.domain.com/citrix/<storename>/discovery`にアクセスすることによって検出された検出ドキュメント内で GSLB が使用する共有 FQDN を確実に受け取ることができます。また、StoreFront の ［プロビジョニングファイルのエクスポート］ コマンドによってエクスポートされたプロビジョニングファイル（receiver.cr）に、共有 GSLB FQDN が確実に含まれるようにすることもできます。

プロビジョニングファイルの例

`-GatewayUrl https://gslb.domain.com`を使用したサンプルファイル 1。これにより、ネイティブの Citrix Receiver または Citrix Workspace アプリは GSLB を使用してゲートウェイに接続できるようになります。

```
<?xml version="1.0" encoding="utf-8"?>
<Services version="1.0"
    xmlns="http://www.citrix.com/ServiceRecord">
    <Service type="store">
        <SRID>167659780</SRID>
        <Name>Store</Name>
        <Address>https://storefront.domain.com/Citrix/Store/discovery</Address>
        <Gateways>
            <Gateway Name="EMEAGateway" Default="true" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
            <Gateway Name="USGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
            <Gateway Name="APACGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
        </Gateways>
        <Beacons>
            <Internal>
                <Beacon>https://storefront.domain.com/</Beacon>
            </Internal>
            <External>
                <Beacon>https://emeagateway.domain.com</Beacon>
                <Beacon>https://usgateway.domain.com</Beacon>
                <Beacon>https://apacgateway.domain.com</Beacon>
                <Beacon>http://gslb.domain.com</Beacon>
            </External>
        </Beacons>
    </Service>
</Services>
```

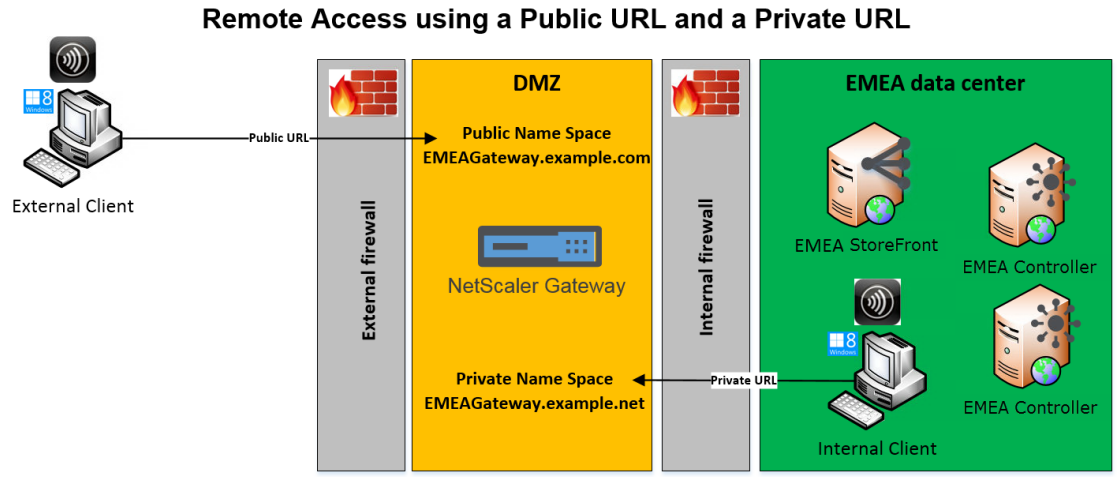

-GatewayUrl https://emeagateway.domain.com, https://usgateway.domain.com and https://apacgateway.domain.comを使用したサンプルファイル 2。これにより、ネイティブの Citrix Receiver または Citrix Workspace アプリは固有の URL を使用してゲートウェイに接続できるようになります。

```
<?xml version="1.0" encoding="utf-8"?>
<Services version="1.0"
    xmlns="http://www.citrix.com/ServiceRecord">
    <Service type="store">
        <SRID>167659780</SRID>
        <Name>Store</Name>
        <Address>https://storefront.domain.com/Citrix/Store/discovery</Address>
        <Gateways>
            <Gateway Name="EMEAGateway" Default="true" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://emeagateway.domain.com/</Location>
            </Gateway>
            <Gateway Name="USGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://ftlgateway.domain.com/</Location>
            </Gateway>
            <Gateway Name="APACGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://bglgateway.domain.com/</Location>
            </Gateway>
        </Gateways>
        <Beacons>
            <Internal>
                <Beacon>https://storefront.domain.com/</Beacon>
            </Internal>
            <External>
                <Beacon>https://emeagateway.domain.com</Beacon>
                <Beacon>https://usgateway.domain.com</Beacon>
                <Beacon>https://apacgateway.domain.com</Beacon>
                <Beacon>http://gslb.domain.com</Beacon>
            </External>
        </Beacons>
    </Service>
</Services>
```

共有 FQDN は、ネイティブの Citrix Receiver および Citrix Workspace アプリによる認証に使用されます。

ユースケース 2: 単一の **Citrix Gateway** でのパブリックまたはプライベート **URL** の使用

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 Citrix 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 Citrix Gateway を経由して渡されるように設定します。
- Citrix Gateway は DMZ 内にあります。
- DMZ の両側には、2 つのファイアウォールを経由した Citrix 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。

PowerShell コマンドレット例

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:

```
1 Add-STFRoamingGateway -Name ”EMEAGateway” -GatewayUrl ”https://
    emeagateway.example.com” -GSLBurl ”https://gslb.example.com” -
    SubnetIPAddress ”10.0.0.1” -CallbackUrl ”https://emeagateway.example
    .com” -LogonType ”DomainAndRSA” -SmartCardFallbackLogonType ”None” -
    Version ”Version10_0_69_4” -SecureTicketAuthorityUrls ”https://emea-
    controller.example.com/scripts/ctxsta.dll,https://us-controller.
    example.com/scripts/ctxsta.dll,https://apac-controller.example.com/
    scripts/ctxsta.dll”
2 Set-STFRoamingGateway -Name ”EMEAGateway” -GatewayUrl ”https://
    emeagateway.example.com” -GSLBurl ”https://gslb.example.com”
3 Get-STFRoamingGateway -Name ”EMEAGateway” (returns just the EMEA
    gateway object)
4 Or
5 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-STFRoamingGateway** が $EMEAGateway に設定され、StoreFront 構成を更新し GSLBurl を削除できます。

```
1 $EMEAGateway = Get-STFRoamingGateway
2 $EMEAGateway.GslbLocation = $Null
3 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:

```
1 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** ファイルに保存されます

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。

使用例＃ **1**: ローミング中のゲートウェイ **web.config** ファイル

```
<gateway id="cca13269-18c1-10fd-a0df-7931b3897aa8" name="EMEAGateway"
    default="false" edition="Enterprise" version="Version10_0_69_1" auth
    ="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.1" rwmode
    ="NONE" deployment="Appliance" callbackurl=https://emeagateway.
    example.com/CitrixAuthService/AuthService.asmx sessionreliability="
    true" requesttickettwosta="false" stasUseLoadBalancing="false"
    stasBypassDuration="01:00:00">
<location path="https://emeagateway.example.com/" /><gslbLocation path=
    "https://gslb.example.com/" /><clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.com/scripts/ctxsta.dll"
     />
<location path="https://us-controller.example.com/scripts/ctxsta.dll"
    />
<location path="https://apac-controller.example.com/scripts/ctxsta.dll"
     />
</secureticketauthorityurls>
</gateway>

<gateway id="b8ec720c-d85e-1889-8188-1cf08a2cf762" name="USGateway"
    default="false" edition="Enterprise" version="Version10_0_69_1" auth
    ="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.2" rwmode
    ="NONE" deployment="Appliance" callbackurl="https://usgateway.
    example.com/CitrixAuthService/AuthService.asmx" sessionreliability="
    true" requesttickettwosta="false" stasUseLoadBalancing="false"
    stasBypassDuration="01:00:00"><location path="https://usgateway.
    example.com/" /><gslbLocation path="https://gslb.example.com/" /><
    clusternodes>
```



```
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.com/scripts/ctxsta.dll" />
<location path="https://us-controller.example.com/scripts/ctxsta.dll" />
<location path="https://apac-controller.example.com/scripts/ctxsta.dll" />
</secureticketauthorityurls>
</gateway>

<gateway id="c57117b5-e111-1eed-9117-a1ffa1c8100e" name="APACGateway" default="false" edition="Enterprise" version="Version10_0_69_1" auth="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.3" rwmode="NONE" deployment="Appliance" callbackurl="https://apacgateway.example.com/CitrixAuthService/AuthService.asmx" sessionreliability="true" requesttickettwosta="false" stasUseLoadBalancing="false" stasBypassDuration="01:00:00"><location path="https://apacGateway.example.com/" /><gslbLocation path="https://gslb.example.com/" /><clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.com/scripts/ctxsta.dll" />
<location path="https://us-controller.example.com/scripts/ctxsta.dll" />
<location path="https://apac-controller.example.com/scripts/ctxsta.dll" />
</secureticketauthorityurls>
</gateway>
```

使用例＃ **2**：ローミング中のゲートウェイ **web.config** ファイル

```
<gateway id="cca13269-18c1-10fd-a0df-7931b3897aa8" name="EMEAGateway"
    default="false" edition="Enterprise" version="Version10_0_69_1" auth
    ="Domain" smartcardfallback="None" ipaddress="10.0.0.1" rwmode="NONE
    " deployment="Appliance" callbackurl="https://emeagateway.example.
    com/CitrixAuthService/AuthService.asmx" sessionreliability="true"
    requesttickettwosta="false" stasUseLoadBalancing="false"
    stasBypassDuration="01:00:00">
<location path="https://emeagateway.example.com/" />
<gslbLocation path=" https://emeagateway.example.net/" />
<clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.net/scripts/ctxsta.dll"
    />
</secureticketauthorityurls>
</gateway>
```

関連情報

開発者用のドキュメントで、Citrix StoreFront SDK PowerShell Modulesを参照してください。

DFA 用の Citrix ADC および StoreFront の構成

July 9, 2019

拡張認証機能により、Citrix ADC アプライアンスおよび 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、Citrix ADC アプライアンスと 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、Citrix Gateway 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。

Citrix Gateway での DFA の構成については、CTX200383を参照してください。

インストールに関する推奨事項

- Citrix ADC アプライアンスと 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、Citrix ADC アプライアンスに 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。

StoreFront クラスターインストールに関する注意事項

- 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。

DFA の有効化

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 modules
Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.
    DeliveryServices.ConfigurationProvider.dll'
Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.
    DeliveryServices.ConfigurationProvider.dll'

PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Install-
    DSDFAServer
Id                              : bf694fbc-ae0a-4d56-8749-
    c945559e897a
ClassType                       : e1eb3668-9c1c-4ad8-bbae-
    c08b2682c1bc
FrameworkController             : Citrix.DeliveryServices.Framework
    .FileBased.FrameworkController
```



```
ParentInstance                  : 8dd182c7-f970-466c-ad4c-27a5980f716c
RootInstance                    : 5d0cdc75-1dee-4df7-8069-7375d79634b3
TenantId                        : 860e9401-39c8-4f2c-928d-34251102b840
Data                            : {
  }

ReadOnlyData                    : {
 [Name, DelegatedFormsServer], [Cmdlet, Add-DSWebFeature], [Snapin, Citrix.DeliverySer
                                   vices.Web.Commands], [Tenant, 860e9401-39c8-4f2c-928d-34251102b840] }

ParameterData                   : {
 [FeatureClassId, e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc], [ParentInstanceId, 8dd182c7-f
                                   970-466c-ad4c-27a5980f716c], [TenantId, 860e9401-39c8-4f2c-928d-34251102b840] }

AdditionalInstanceDependencies : {
 b1e48ef0-b9e5-4697-af9b-0910062aa2a3 }

IsDeployed                      : True
FeatureClass                    : Citrix.DeliveryServices.Framework.Feature.FeatureClass
```

2. Citrix Trusted Client を追加します。StoreFront と Citrix ADC アプライアンス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、Citrix ADC アプライアンス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 を探します。次に表示例を示します。

```
<example connectorURL="http://Example.connector.url:8080/adapters-sf-aaconnector-webapp">
   <routeTable order="1000">
```



```
3          <routes>
4            <route name="StartExampleAuthentication" url="Example-
                 Bridge-Forms/Start">
5              <defaults>
6                <add param="controller" value="
                     ExplicitFormsAuthentication" />
7                <add param="action" value="AuthenticateStart" />
8                <add param="postbackAction" value="Authenticate" />
9                <add param="cancelAction" value="CancelAuthenticate"
                      />
10               <add param="conversationFactory" value="
                     ExampleBridgeAuthentication" />
11               <add param="changePasswordAction" value="
                     StartChangePassword" />
12               <add param="changePasswordController" value="
                     ChangePassword" />
13               <add param="protocol" value="CustomForms" />
14             </defaults>
15           </route>
```

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。

```
1 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。

StoreFront のアンインストール

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

December 23, 2019

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、Citrix 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 Citrix 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 または Citrix Workspace アプリのユーザーは使用できません。

テスト環境のセットアップ

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 Citrix 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:

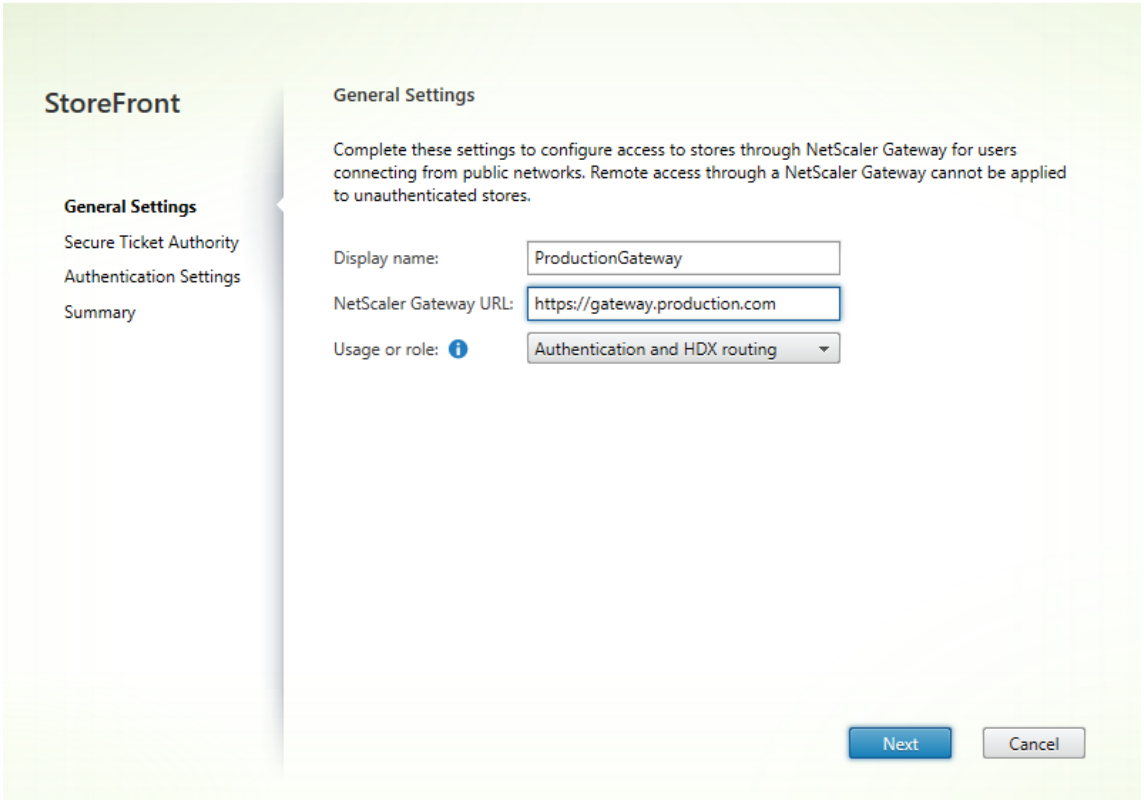
- StoreFront、Citrix Virtual App and Desktops、および VDA はすべて`development.com`ドメイン上にあります。
- production\testuser1 アカウントおよびパスワードを使用して Citrix Receiver for Web サイトに認証。
- 2 つのドメインの間には、信頼関係はありません。

ストアの **Citrix Gateway** の構成

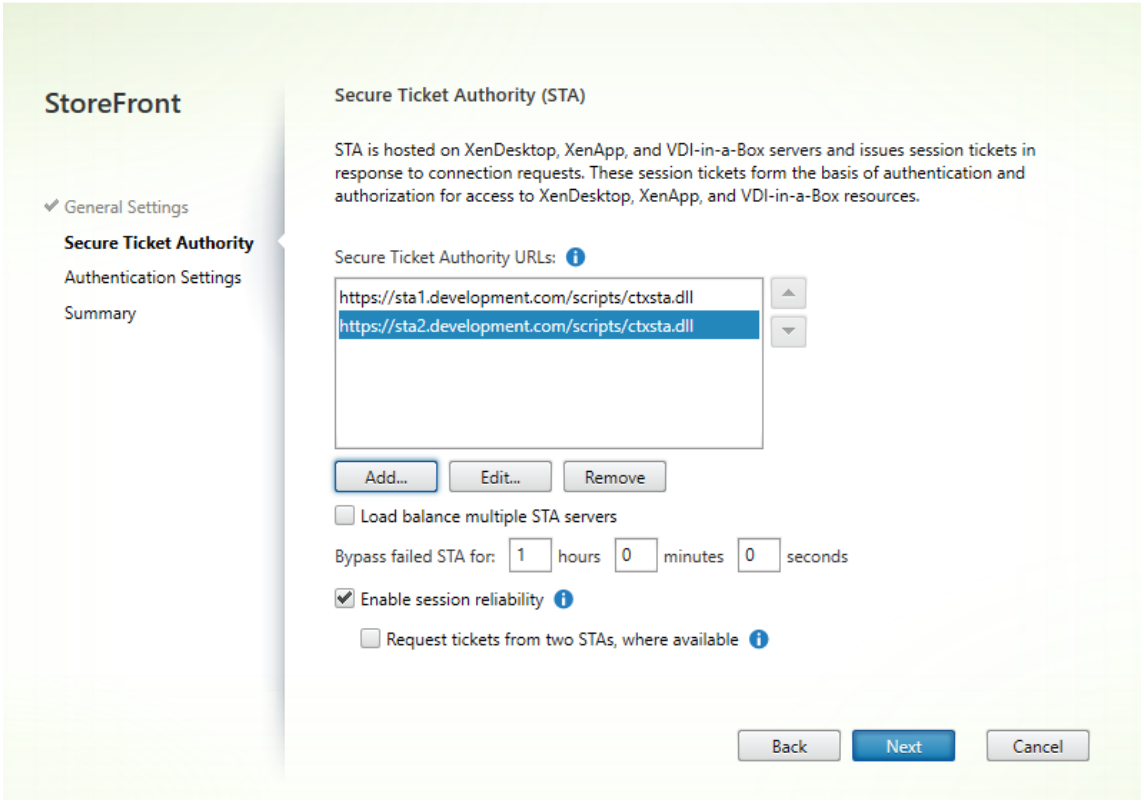
ストアの Citrix Gateway を構成するには:

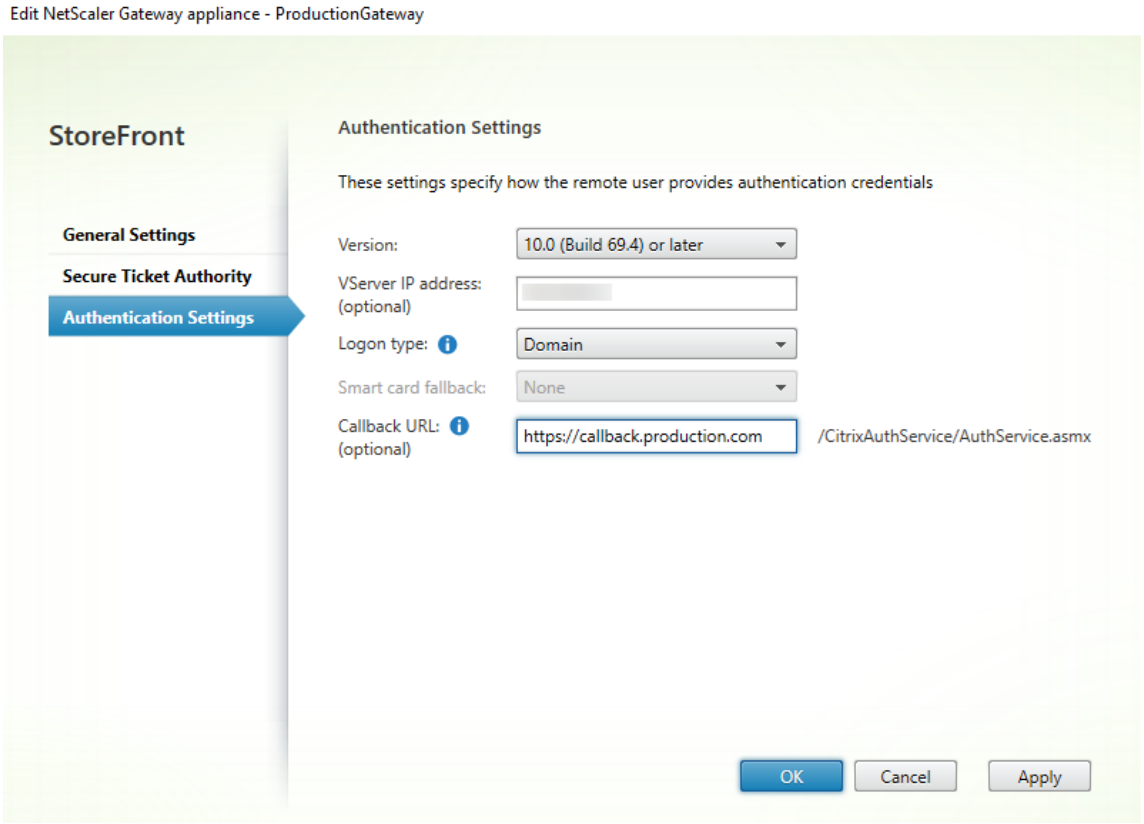
1. Citrix StoreFront 管理コンソールの左ペインで［ストア］を選択して、［操作］ペインの［**Citrix Gateway** の管理］ をクリックします。
2. ［Citrix Gateway の管理］画面で、［追加］ をクリックします。
3. 全般設定、Secure Ticket Authority、認証手順を完了します。

Add NetScaler Gateway Appliance



Add NetScaler Gateway Appliance

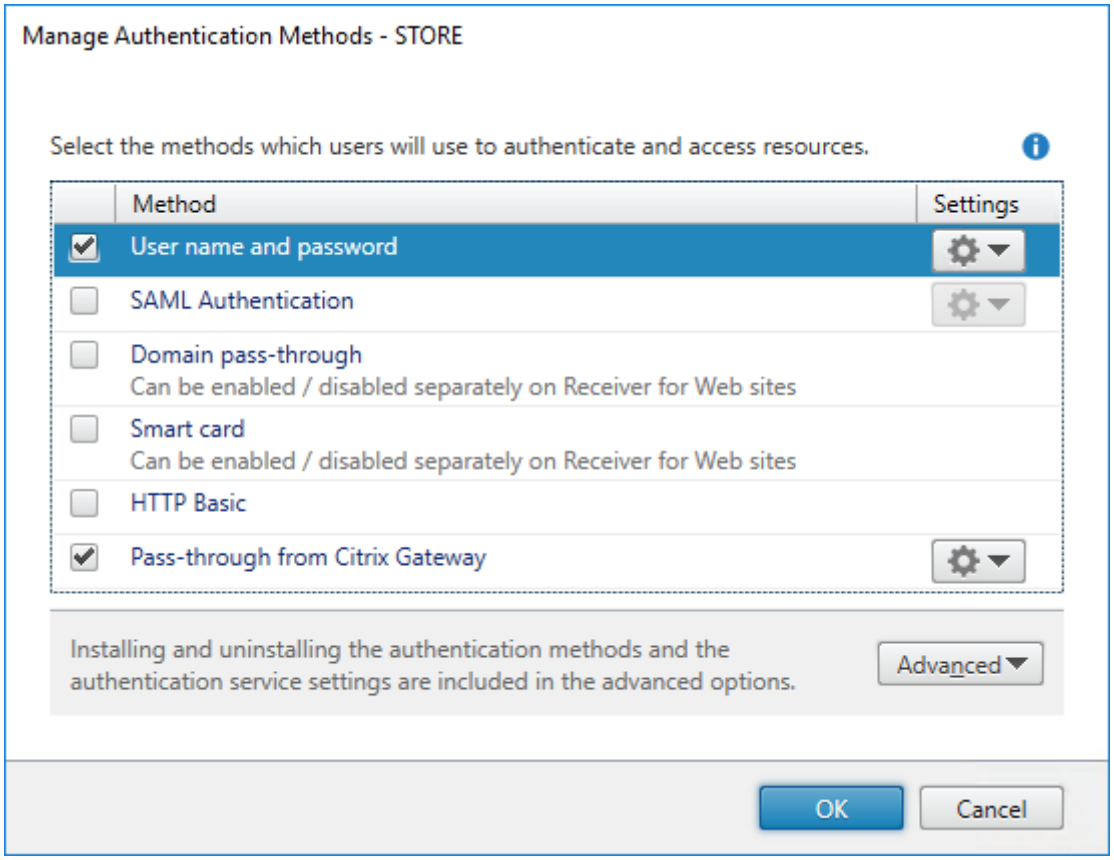




> 注:
>
> 両方のドメインで使用中の DNS サーバーが他方のドメインの FQDN を解決できるよう、DNS 条件付きフォワーダーの追加が必要な場合があります。Citrix ADC アプライアンスは、`production.com`の DNS サーバーを使用して、`development.com`ドメインで STA サーバーの FQDN を解決できるようにする必要があります。StoreFront は、`development.com`の DNS サーバーを使用して、`production.com`ドメインでコールバック URL を解決できるようにする必要があります。または、`development.com`の FQDN を使用して、Citrix Gateway 仮想サーバー virtual IP（VIP）として解決することもできます。

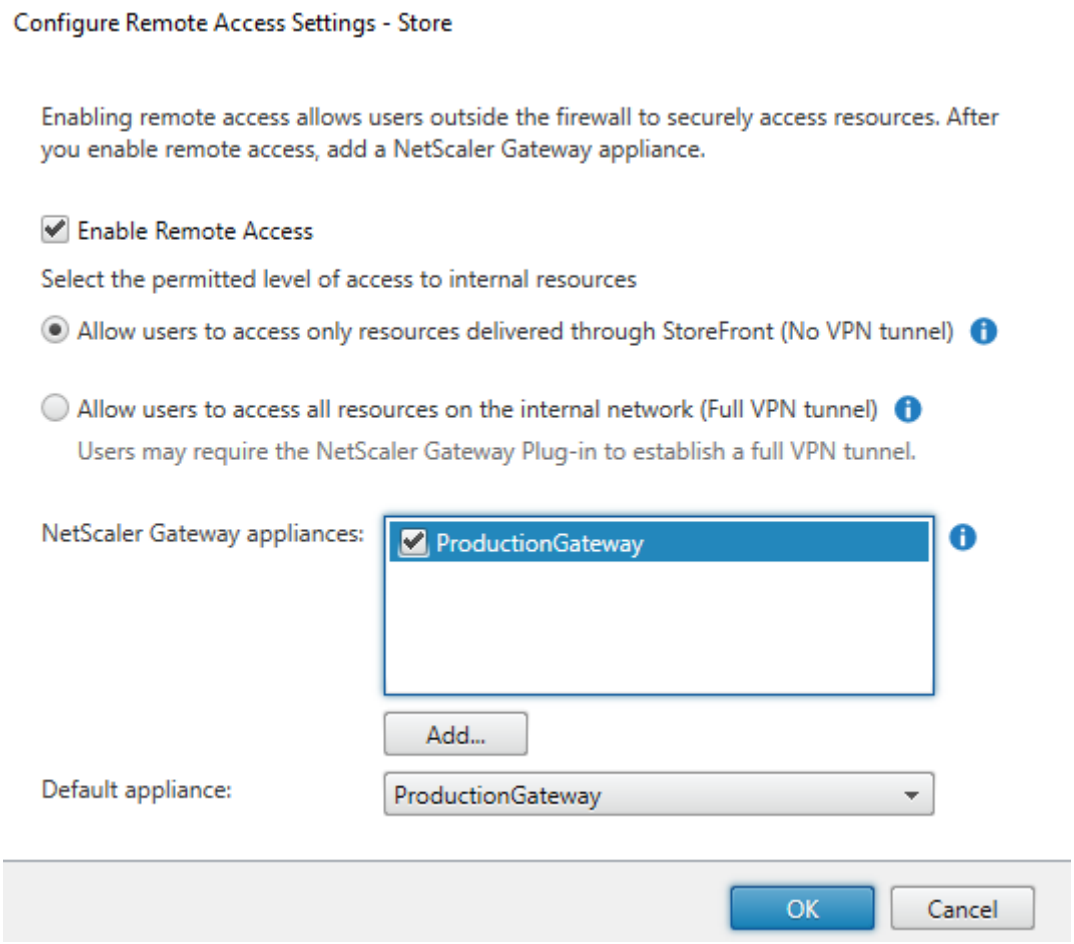
Citrix Gateway からのパススルーを有効にする

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. ［認証方法の管理］ 画面で、 ［**Citrix 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。



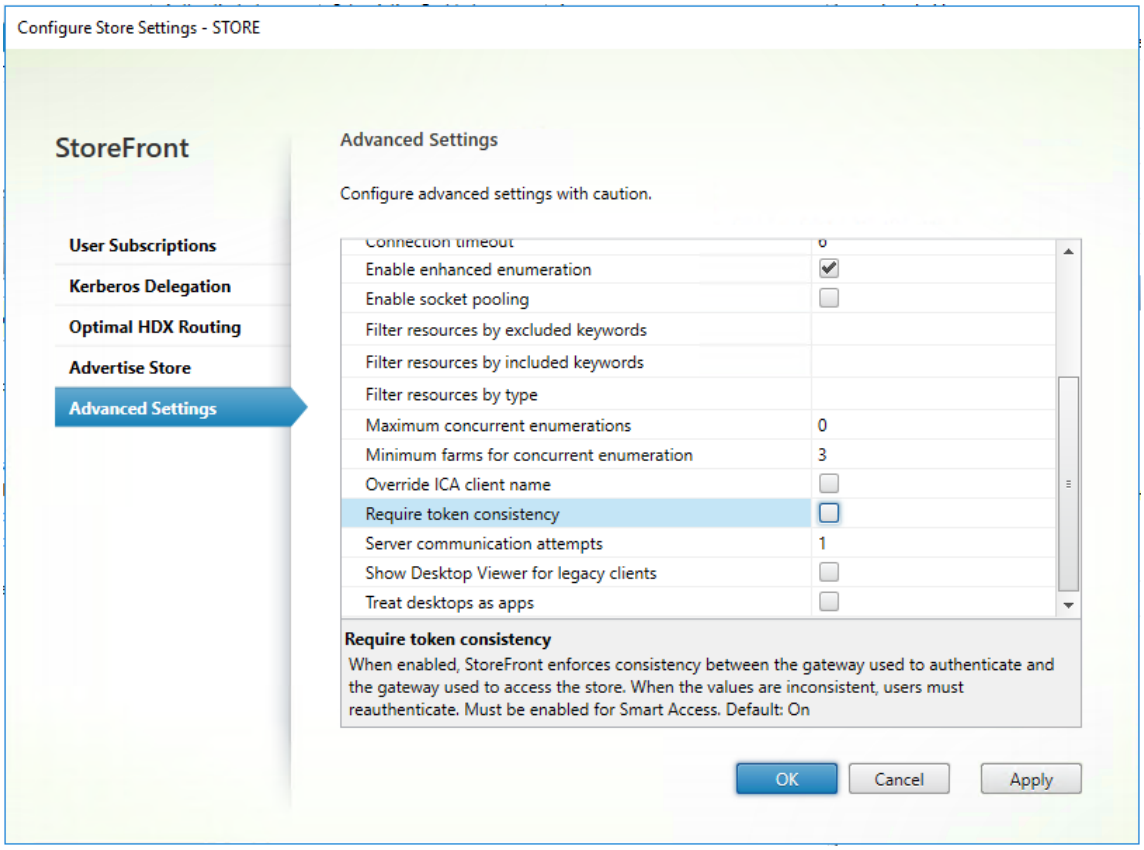
NetScaler Gateway を使用したリモートアクセスをストアで構成する

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、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. ［リモートアクセスの有効化］ を選択します。
3. Citrix Gateway がストアに登録されたことを確認します。Citrix 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。



トークンの一貫性を無効にする

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、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. ［トークンの整合性を要求する］ 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。

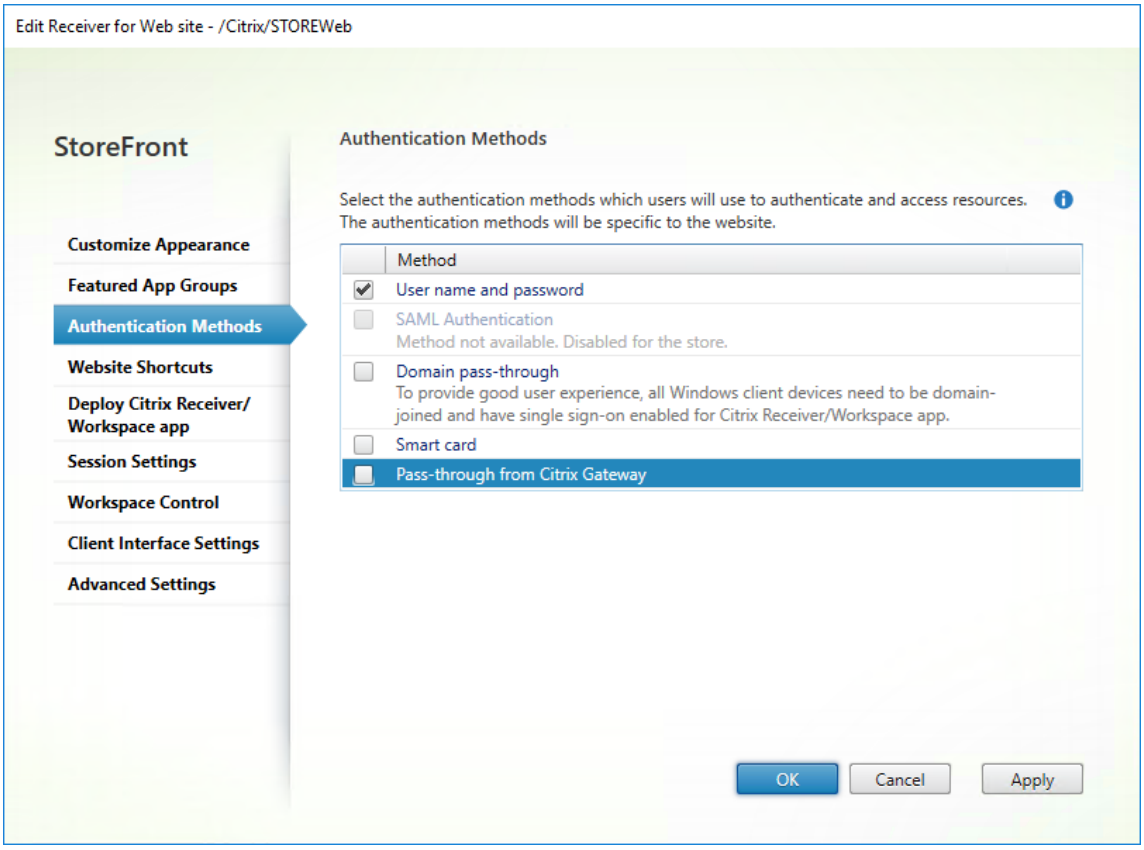


> 注:
>
> [トークンの一貫性を要求する] 設定はデフォルトでオンになっています。この設定を無効にすると、Citrix ADC End Point Analysis (EPA) SmartAccess 機能が停止します。SmartAccess について詳しくは、CTX138110を参照してください。

Receiver for Web サイトで **Citrix Gateway** からのパススルーを無効にする

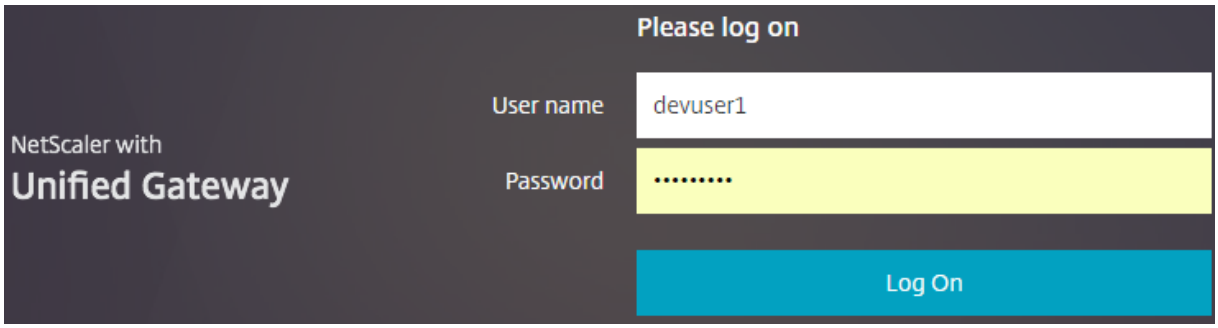
> 重要:
>
> Citrix Gateway からのパススルーを無効にすると、Receiver for Web が Citrix ADC アプライアンスから渡された`production.com`ドメインの誤った資格情報を使用しないようにできます。Citrix Gateway からのパススルーを無効にすると、Receiver for Web がユーザーに資格情報の入力を求めます。これらの資格情報は、Citrix Gateway でログオンする場合に使用する資格情報とは異なります。

1. Citrix StoreFront 管理コンソールの左ペインで [ストア] ノードを選択します。
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、[**Citrix Gateway** からのパススルー] をオフにします。
5. [**OK**] をクリックします。

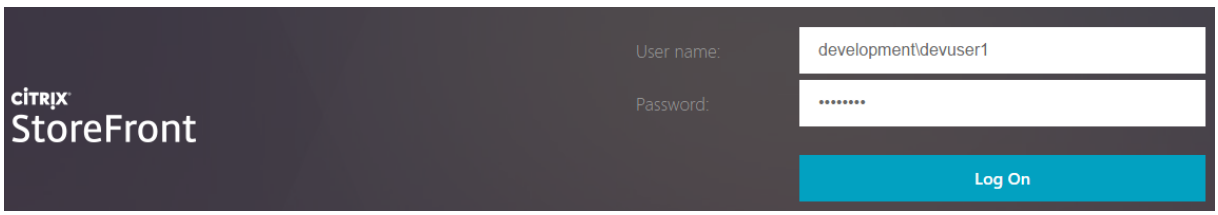


`production.com` ユーザー名およびパスワードを使用して NetScaler Gateway にログオンする

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。

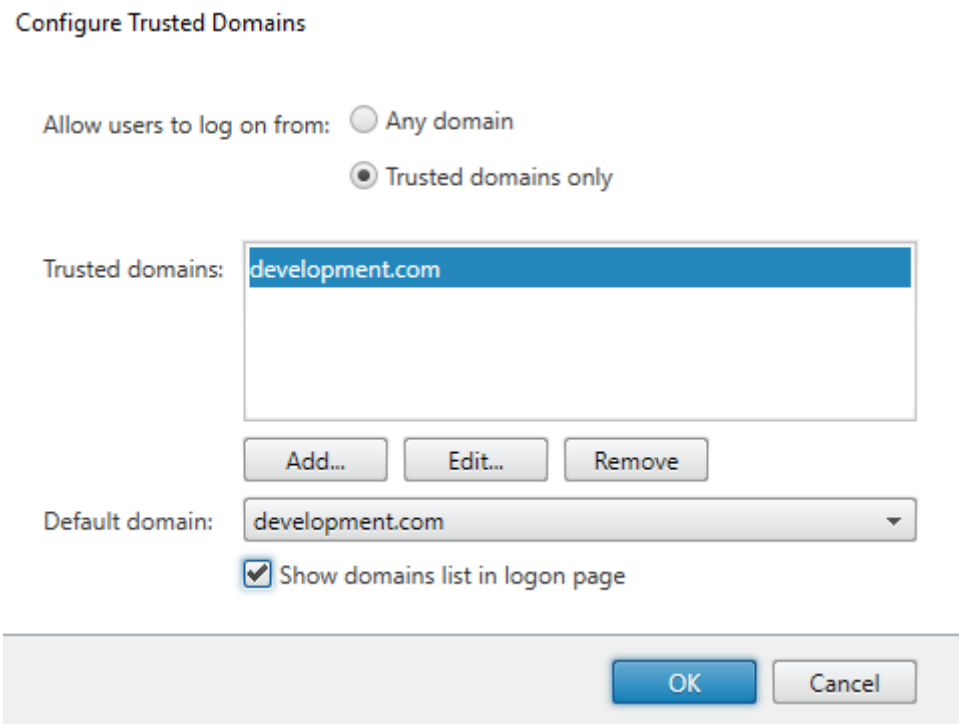


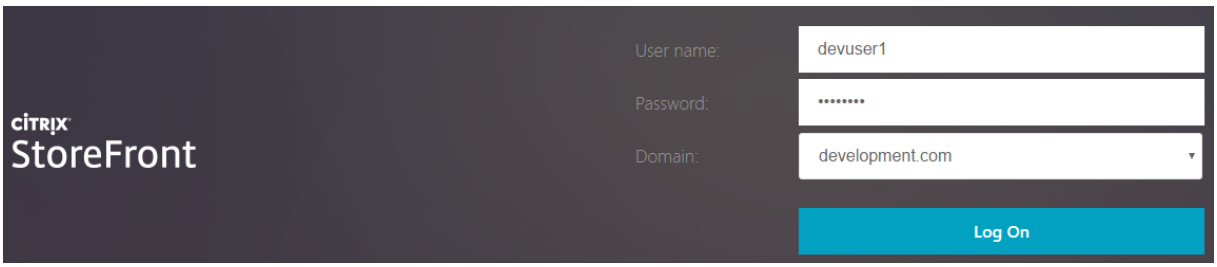
StoreFront で信頼済みドメインドロップダウンリストを追加する（オプション）

この設定はオプションですが、これによって Citrix 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、Citrix 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。

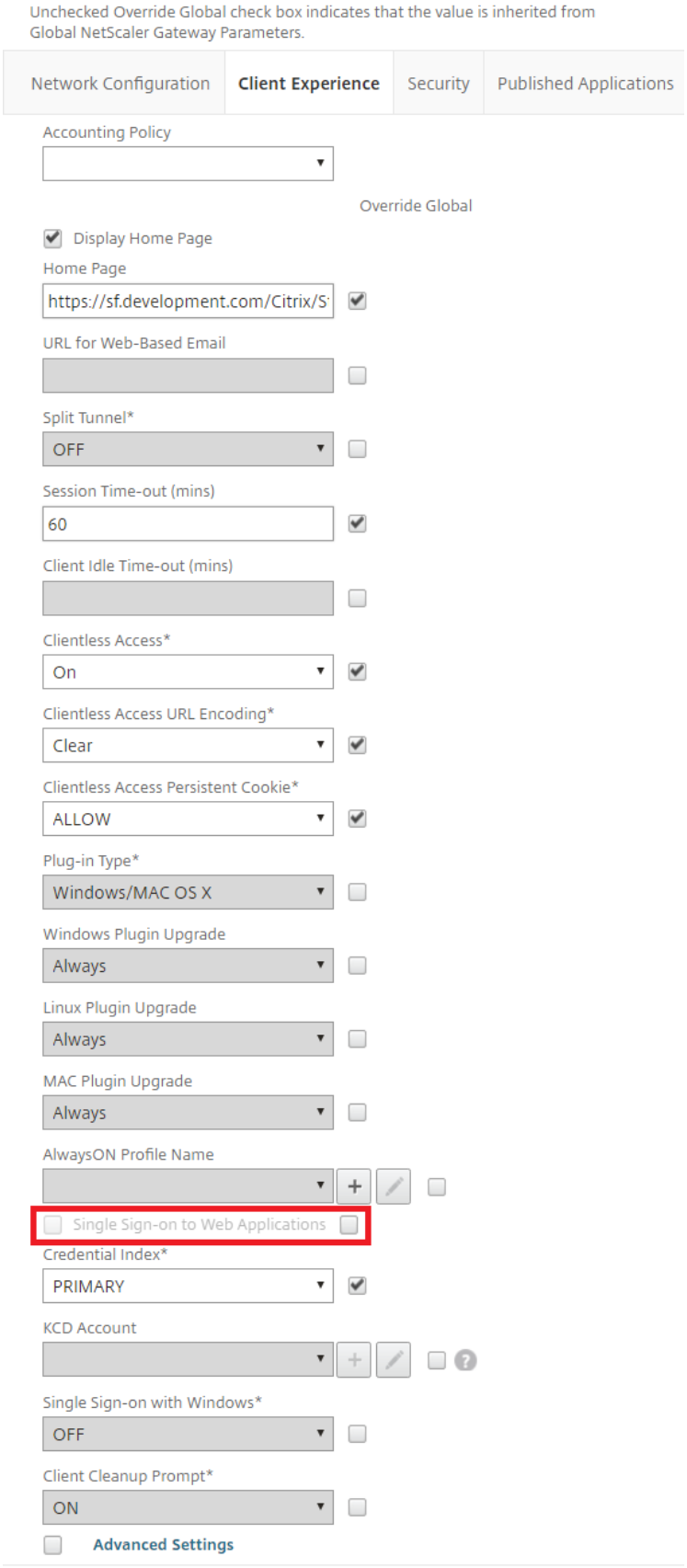


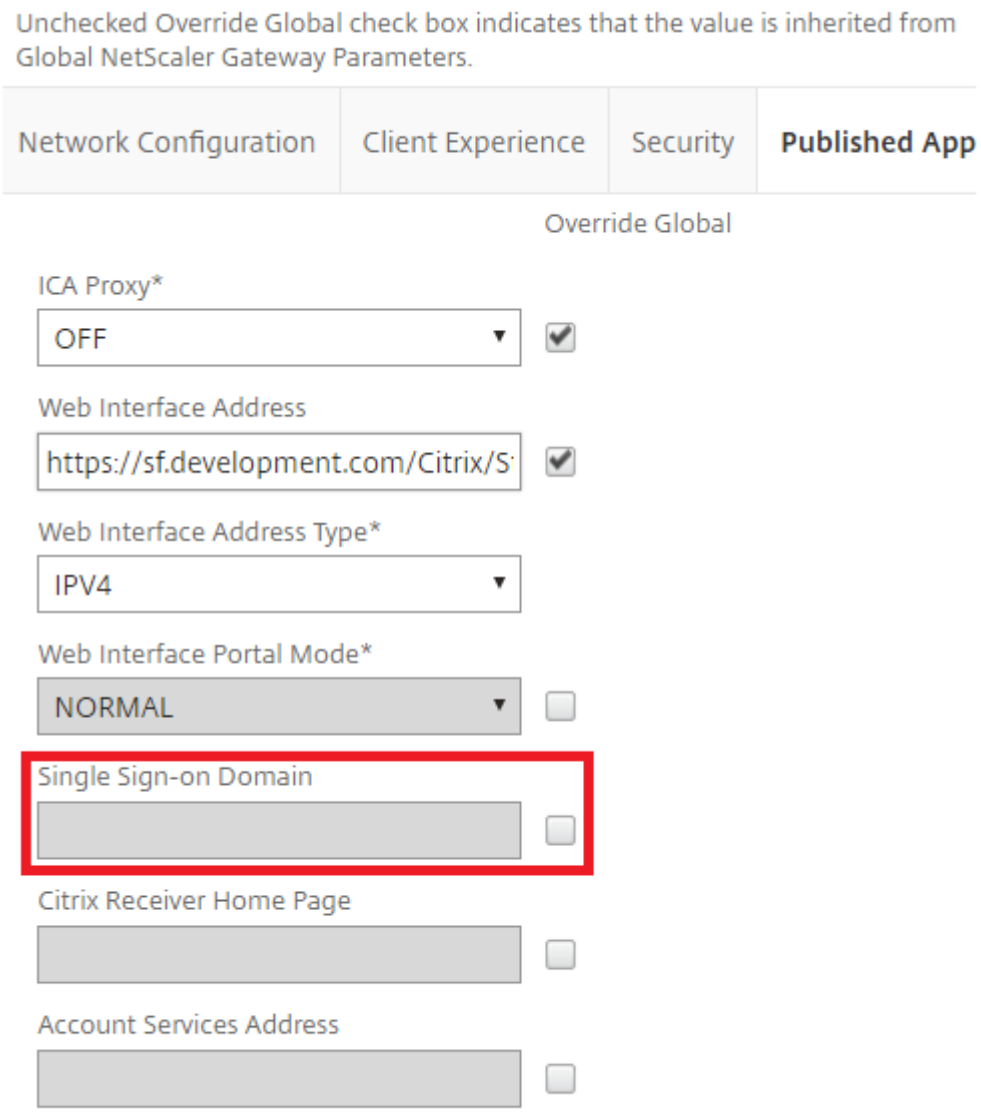


> 注:
>
> この認証方法では、ブラウザーのパスワードキャッシュ機能は使用しないでください。2 つの異なるドメインアカウントに異なるパスワードがある場合、パスワードキャッシュによって操作が複雑になる可能性があります。

Citrix Gateway のクライアントレス **VPN**（**CVPN**）セッションの操作ポリシー

- Citrix Gateway 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、Citrix ADC アプライアンスから 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 ［**Citrix 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。
- Citrix ADC アプライアンスの［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

April 2, 2020

[ビーコンの管理] タスクを使用して、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 を指定します。Citrix Workspace アプリは、ユーザーがローカルネットワークとパブリック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 Workspace アプリに返します。これにより、ユーザーがデスクトップまたはアプリケーションにアクセスしたとき

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 Workspace アプリ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。このため、ユーザーは Citrix Gateway 経由でデスクトップやアプリケーションに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 Citrix 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、デフォルトでシトリックスの Web サイト、および管理者が追加した最初の Citrix 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 Workspace アプリ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 Citrix Workspace アプリの最新の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。完了したら、
> 構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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://example`などの簡略化された NetBIOS 名ではなく、`http://example.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 Workspace アプリ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。

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

December 23, 2019

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 Citrix 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 Workspace アプリ用の **StoreFront** ビーコン

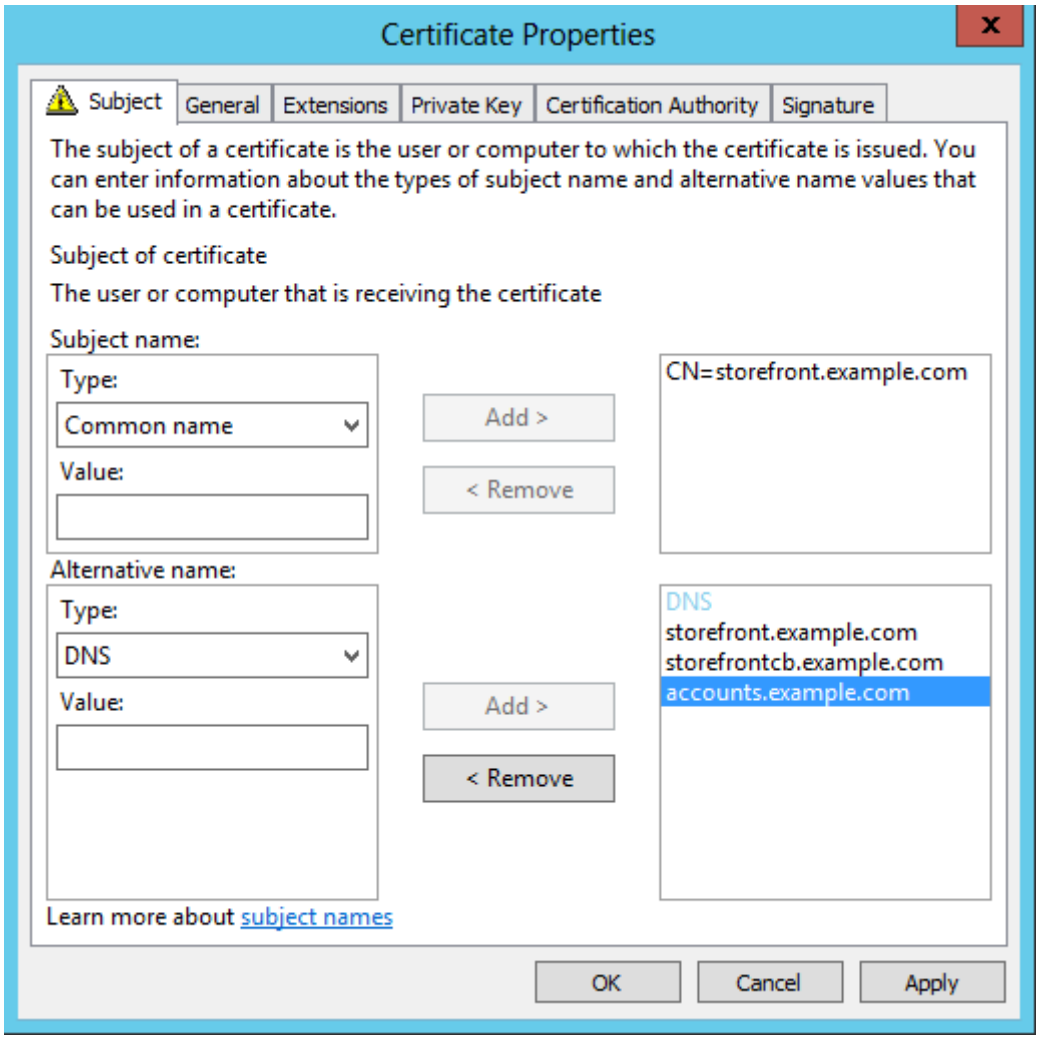
Citrix Workspace アプリは、ユーザーがローカルネットワークとパブリックネットワークのどちらに接続しているのかをビーコンポイントを使用して識別します。ユーザーがデスクトップやアプリケーションにアクセスすると、そのリソースを提供するサーバーがそのユーザーの位置情報に基づいて適切な接続詳細を Citrix Workspace アプリに返します。これにより、ユーザーがデスクトップまたはアプリケーションにアクセスしたときに再ログオンする必要がなくなります。ビーコンポイントの構成については、「ビーコンポイントの構成」を参照してください。

> 注:
>
> この記事では、「Citrix Workspace アプリ」に関する記載は、特に明記されていない限り、サポートされているバージョンの Citrix Receiver にも適用されます。

Citrix Gateway 仮想サーバーと **SSL** 証明書の構成

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 Citrix 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。会社の証明機関（CA）の代わりにサードパーティのルート CA（Verisign など）を使用してゲートウェイ証明書に署名すると、外部クライアントはゲートウェイ仮想サーバーにバインドされている証明書を自動的に信頼します。サードパーティのルート CA（Verisign など）を使用する場合、追加のルート CA 証明書を外部クライアントにインポートする必要はありません。

Citrix 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。



Citrix 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 Citrix 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. サードパーティ CA（Verisign など）または組織における会社のルート 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）

証明機関（**CA**）を使用した **Citrix Gateway** 仮想サーバーの **SSL** 証明書の署名

必要に応じて、次の 2 種類の CA 署名入り証明書のいずれかを選択することができます。

- サードパーティの CA 署名付き証明書 - Citrix 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 証明書ストアにルート 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 の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、Citrix 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。ネイティブ Receiver がインストールされたポータブルデバイス（iPhone や iPad など）を使用する場合は、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

- iOS デバイスのローカルストレージには通常アクセスできないため、iOS デバイスでは電子メールの添付ファイルを使用して X.509 証明書の CER ファイルをインポートします。
- 同様に Android デバイスでも X.509（.CER）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、Citrix 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 **Citrix Gateway** に発行した証明書のインポート

WinSCP は、Windows マシンから Citrix 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、Citrix 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。Citrix Gateway で OpenSSL ツールを使用して PKCS12 または PFX ファイルから証明書とキーを抽出し、Citrix Gateway で使用できる X.509 の CER ファイルと KEY ファイルを PEM 形式で個別に作成できます。

1. この PFX ファイルを Citrix Gateway アプライアンスまたは VPX の/nsconfig/ssl にコピーします。
2. Citrix 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、Citrix Gateway のコマンドラインインターフェイスを終了します。
4. ディレクトリを変更するために、`cd /nsconfig/ssl`を使用します。
5. `openssl pkcs12 -in <imported cert file>.pfx -nokeys -out <certfilename>.cer`を実行します。PFX のパスワードの入力を求めるメッセージが表示されたら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. Citrix 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。

Citrix Receiver for Windows、または **Citrix Receiver for Mac**、**Citrix Gateway** のセッションポリシー

REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS

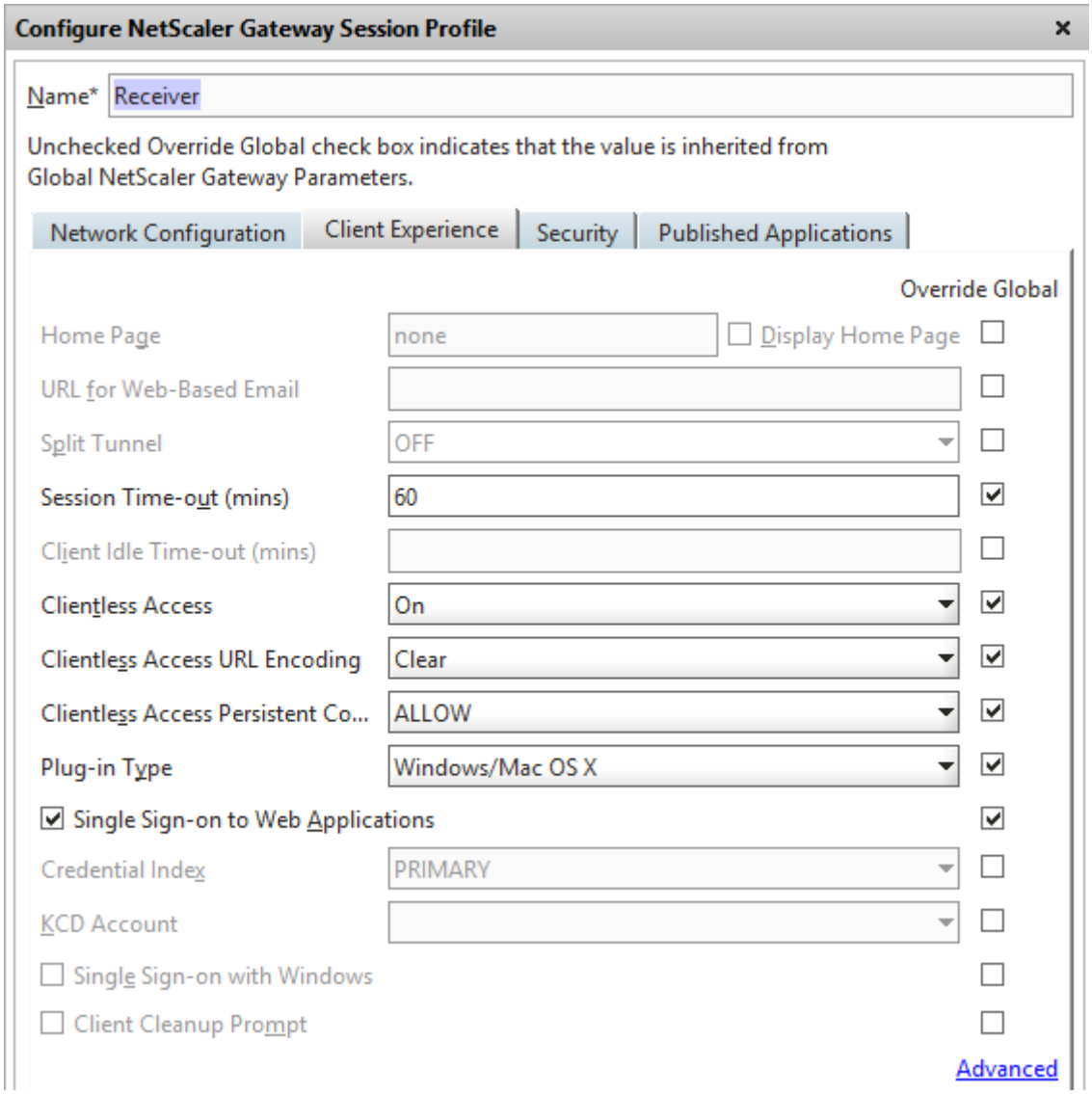
Receiver for Web 用 **Gateway** セッションポリシー

REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS

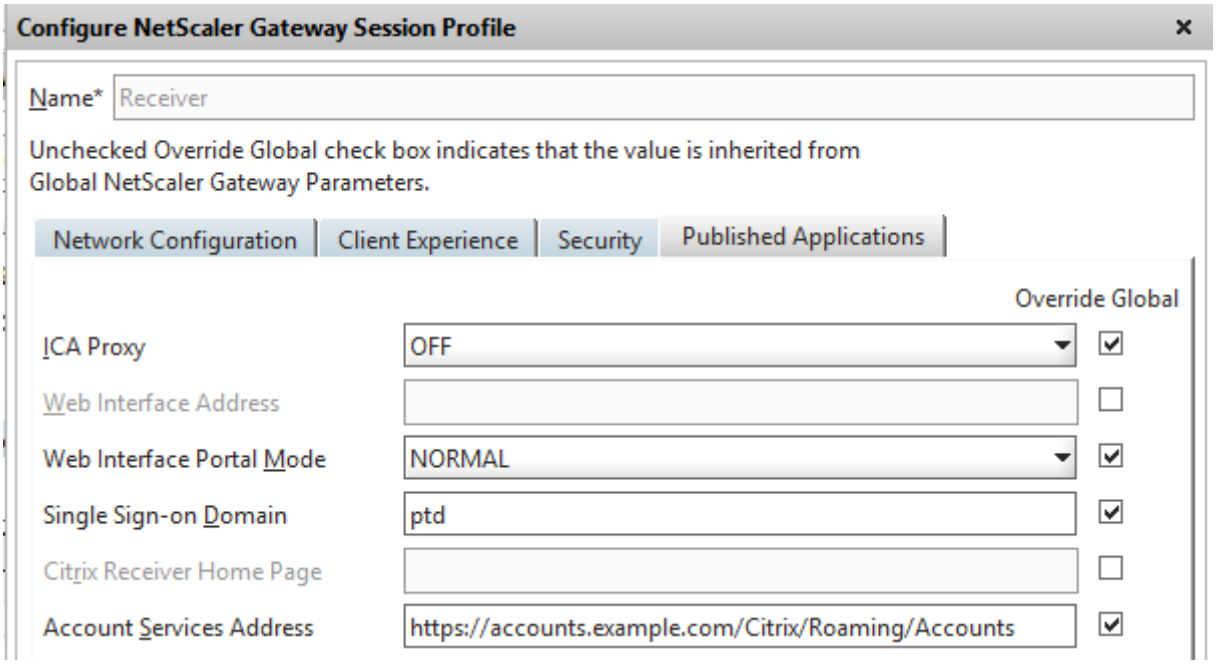
cVPN と SmartAccess の設定

SmartAccess を使用している場合、Citrix 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

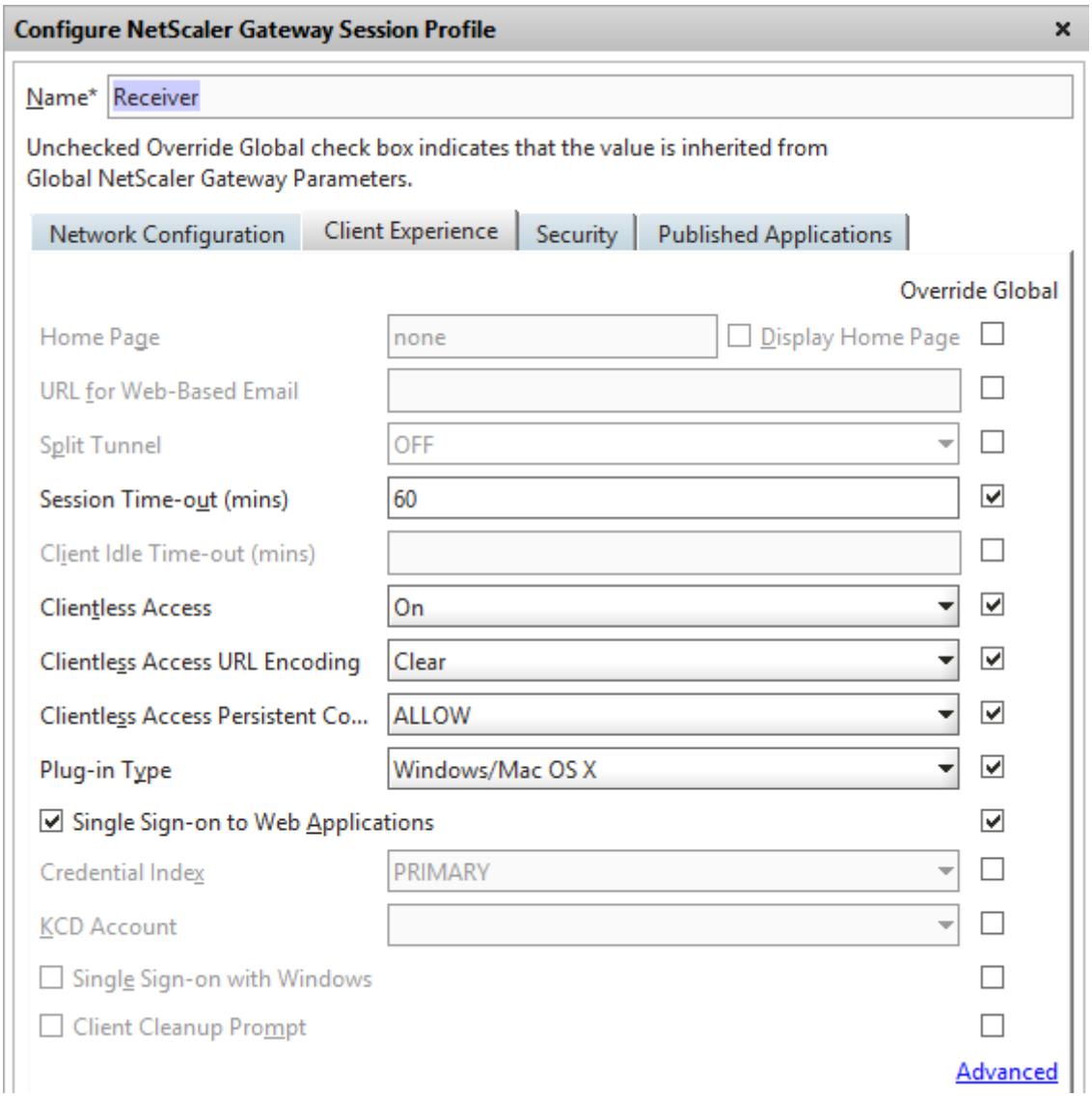


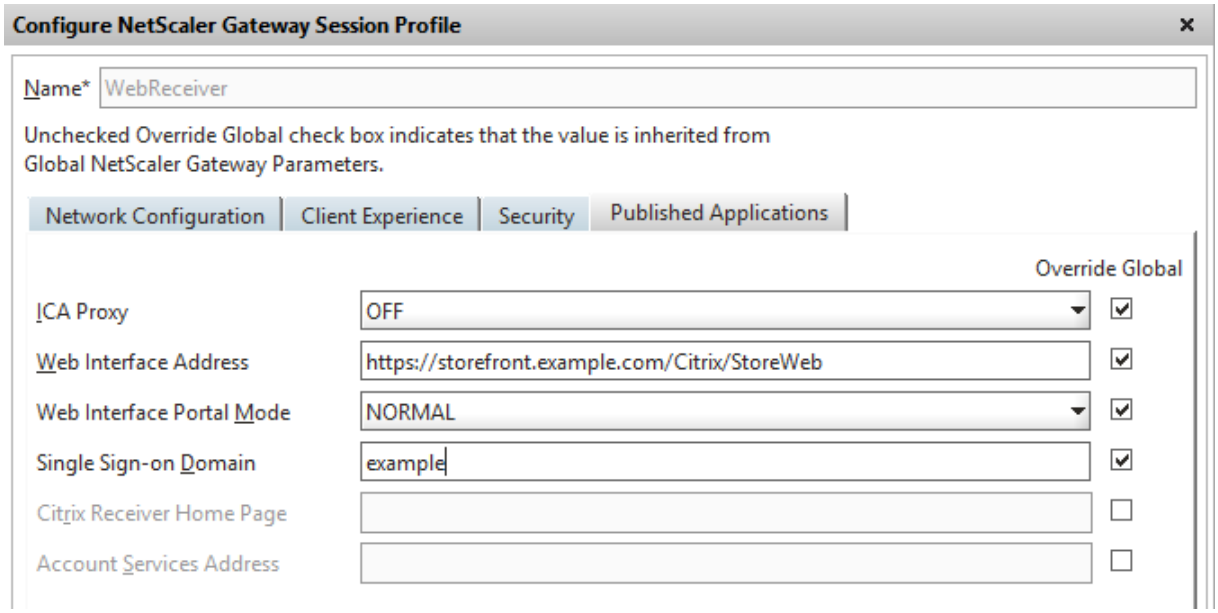
セッションプロファイルのアカウントサービス URL を`https://accounts.example.com/Citrix/Roaming/Accounts`に設定します（`https://storefront.example.com/Citrix/Roaming/Accounts`ではありません）。



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

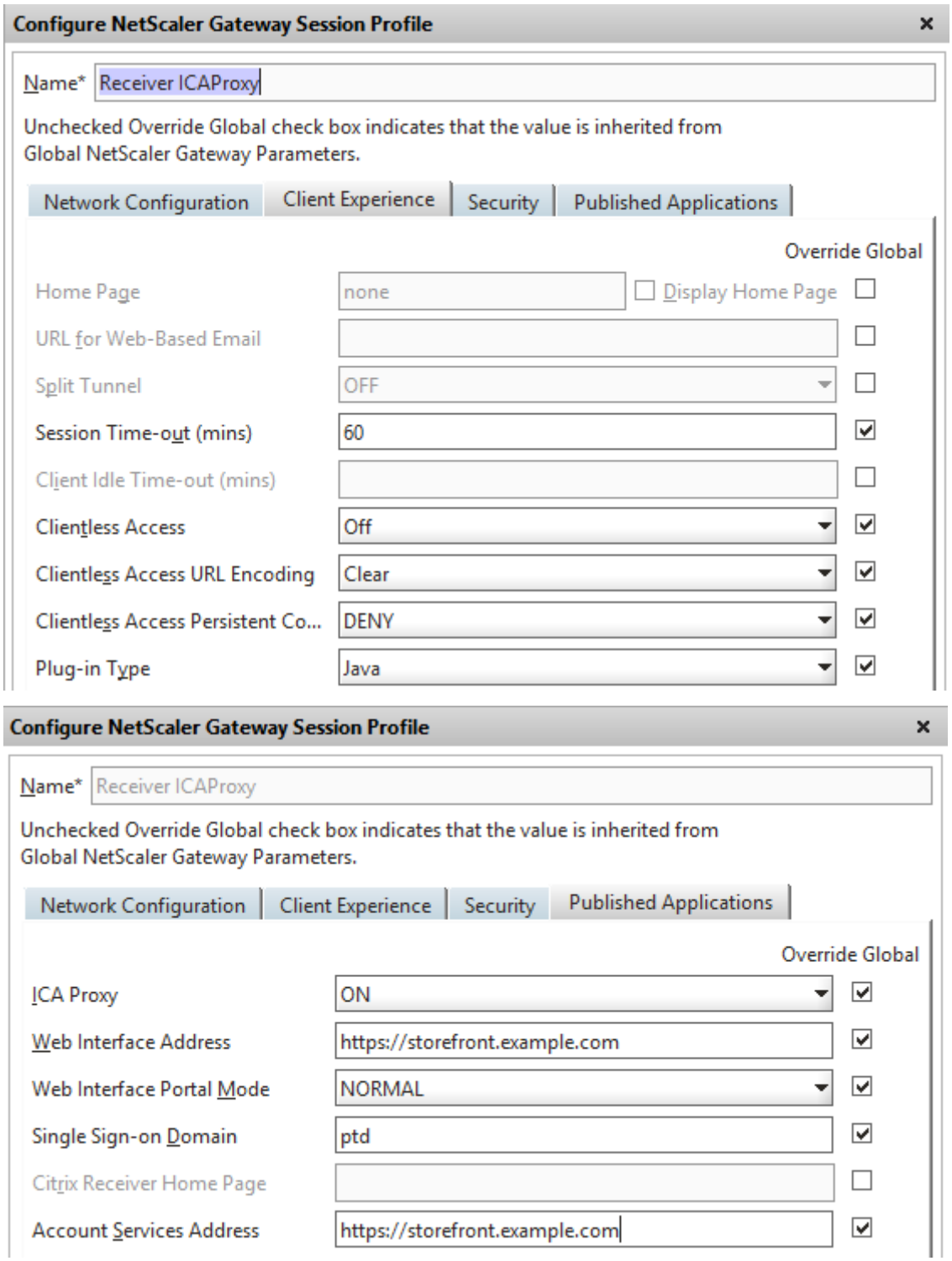




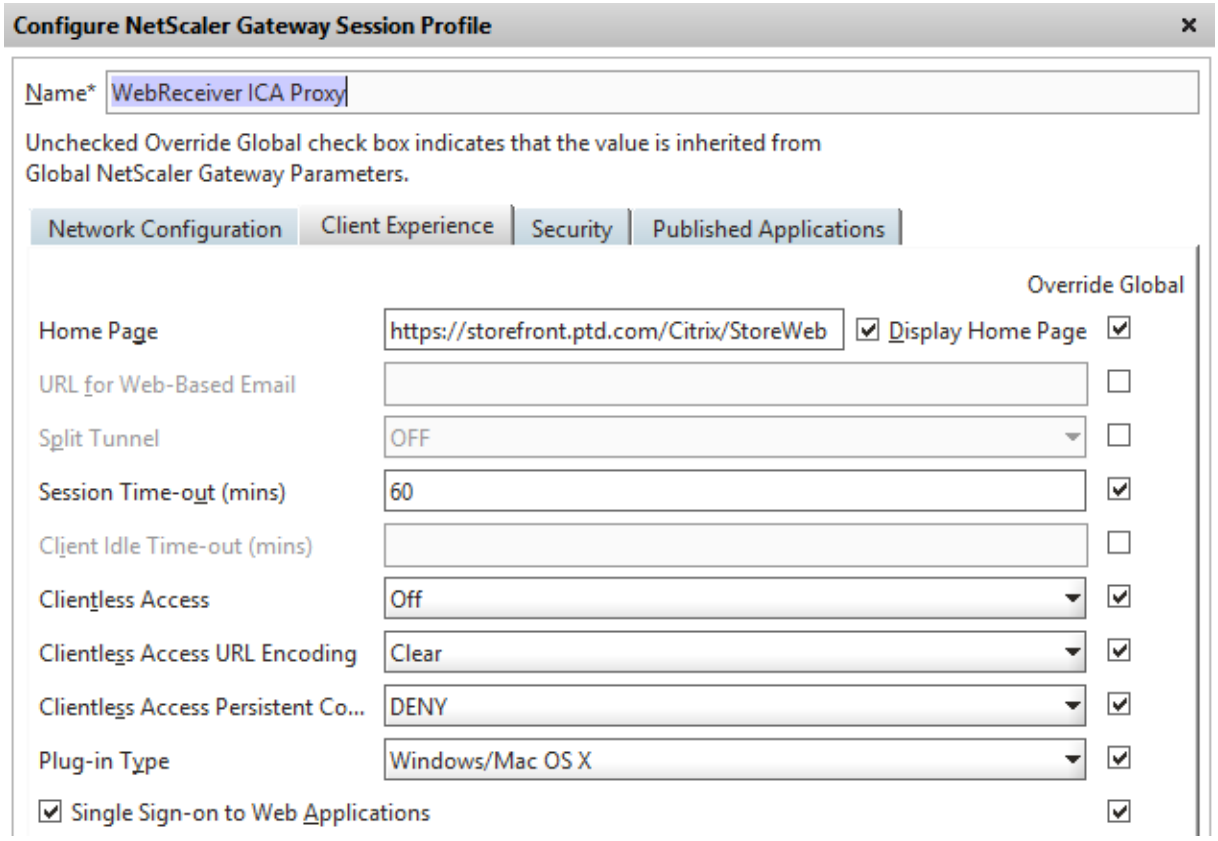
ICA プロキシと基本モードの設定

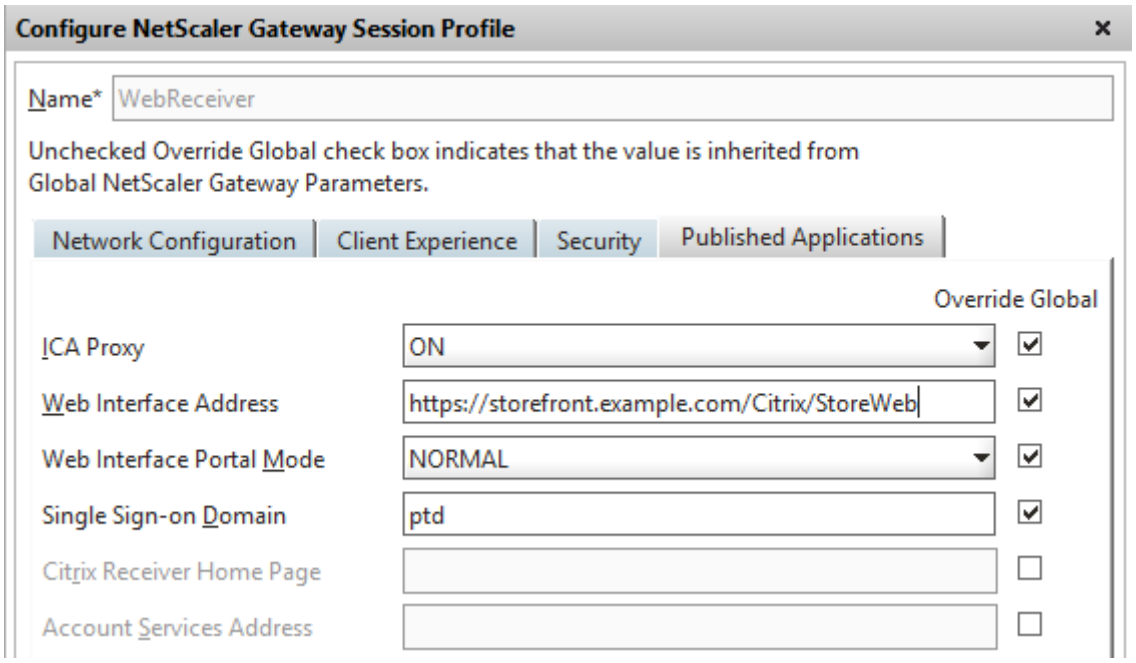
ICA プロキシを使用している場合、Citrix Gateway 仮想サーバーのプロパティページで、基本モードを有効にします。1 つの Citrix ADC プラットフォームライセンスのみが必要です。

Receiver のプロファイル



Receiver for Web のプロファイル





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

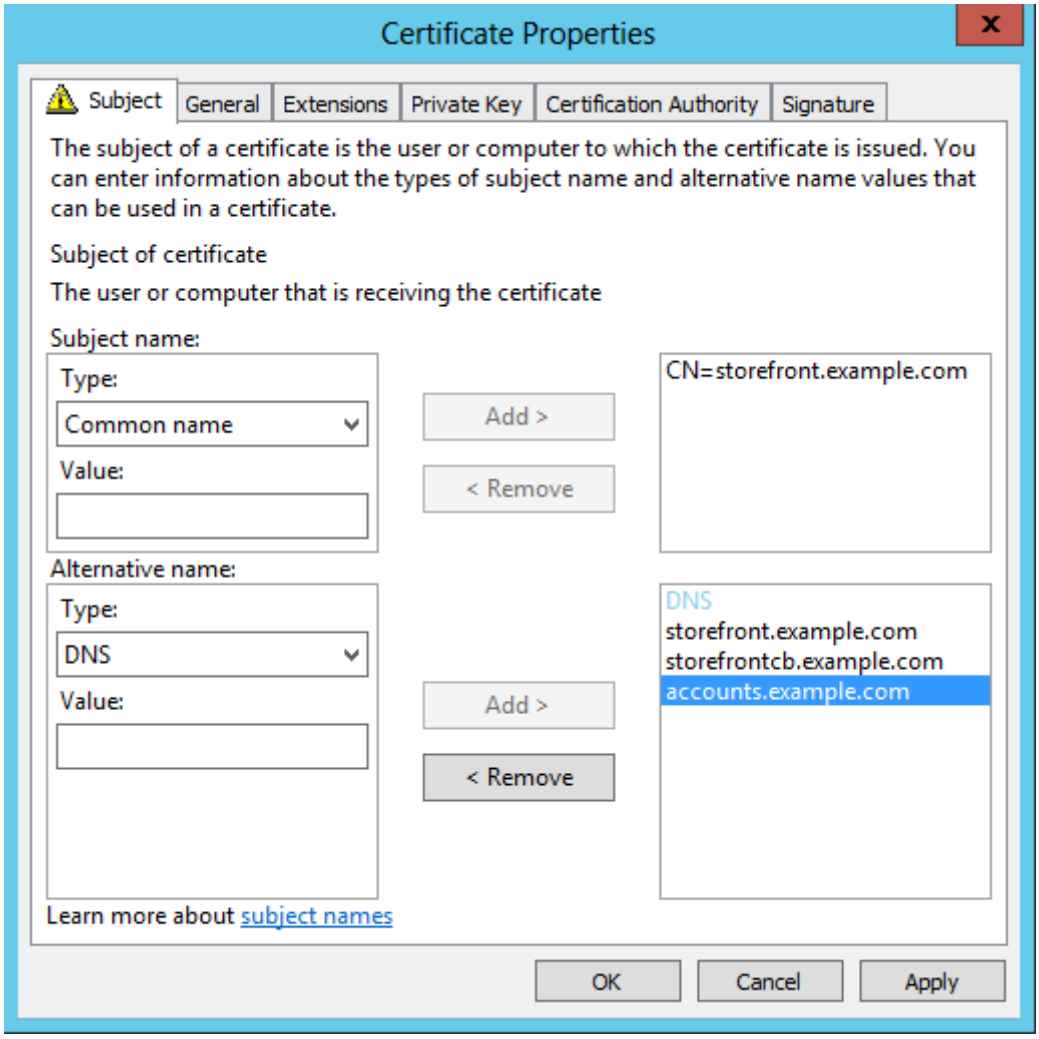
ストアをホストする StoreFront クラスターまたは単一の StoreFront IP が作成されている場合は、Citrix Gateway 仮想サーバーに解決される共有 FQDN が StoreFront のロードバランサーにも直接解決される必要があります。

内部 **DNS**：**3** つの **DNS A** レコードを作成します

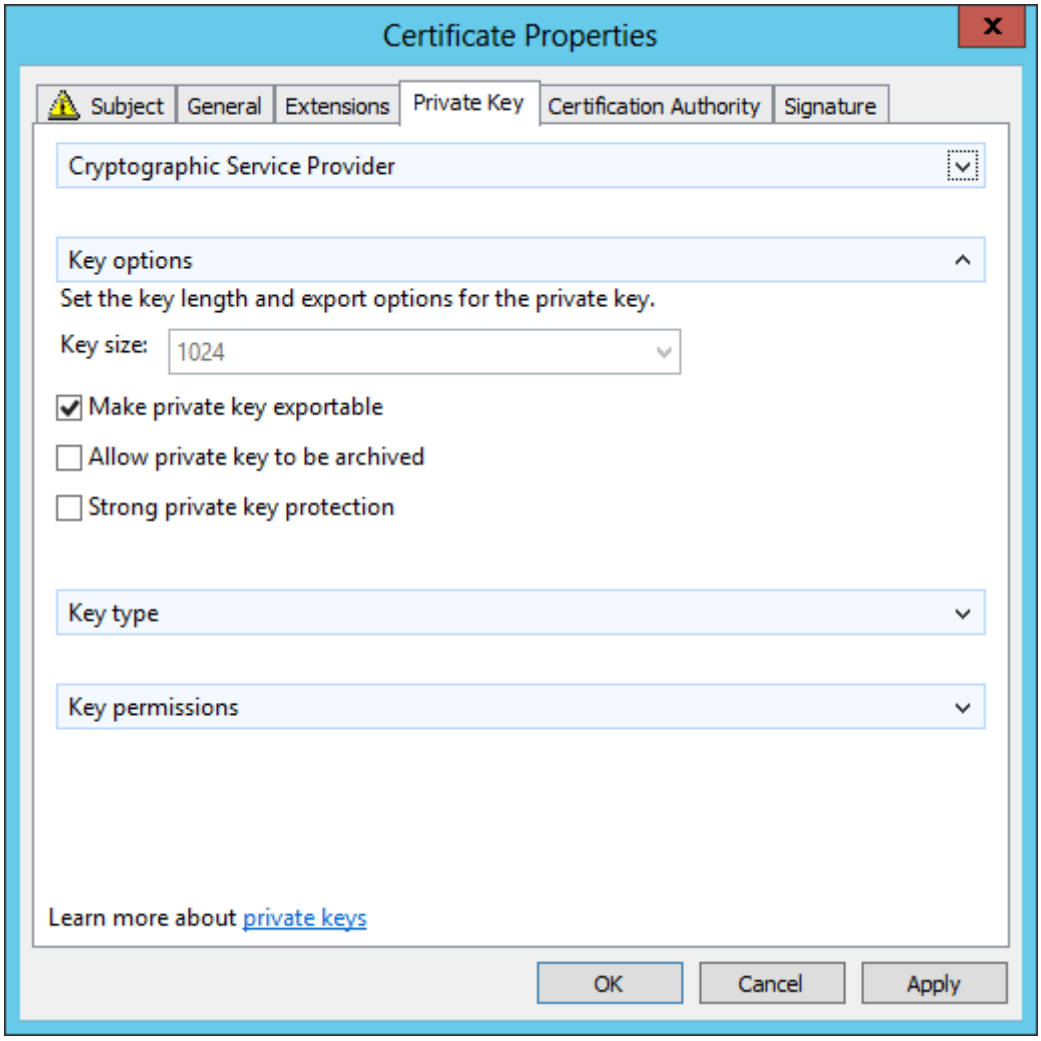
- storefront.example.com が StoreFront のロードバランサーまたは単一の StoreFront サーバー IP に解決される必要があります。
- storefrontcb.example.com がゲートウェイの仮想サーバーの仮想 IP に解決される必要があるので、DMZ と会社のローカルネットワークの間にファイアウォールがある場合は、これを許可します。
- accounts.example.com — storefront.example.com の DNS エイリアスとして作成します。StoreFront クラスターのロードバランサー IP または単一の StoreFront 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**

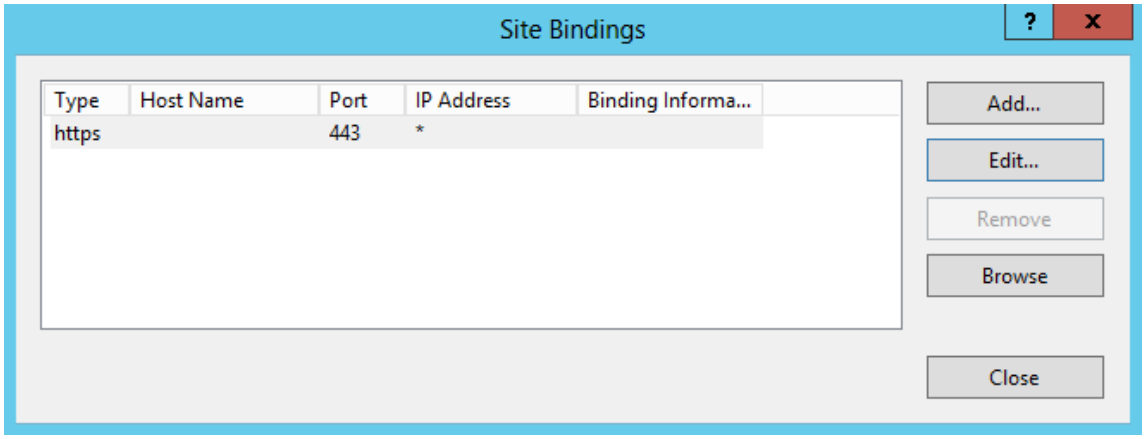
1. StoreFront をインストールする前に、StoreFront サーバーまたはサーバーグループ用の適切な証明書を作成します。
2. 共有 FQDN を［Common name］フィールドと［DNS］フィールドに追加します。これが、先に作成した Citrix Gateway 仮想サーバーにバインドされた SSL 証明書で使用される FQDN と一致することを確認します。または、Citrix Gateway 仮想サーバーにバインドされているものと同じ証明書を使用します。
3. 別の SAN としてアカウントエイリアス（`accounts.example.com`）を証明書に追加します。SAN で使用するアカウントエイリアスは、前述のネイティブ **Receiver** の **Gateway** セッションのポリシーおよびプロファイルの手順で使用したエイリアスです。



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。

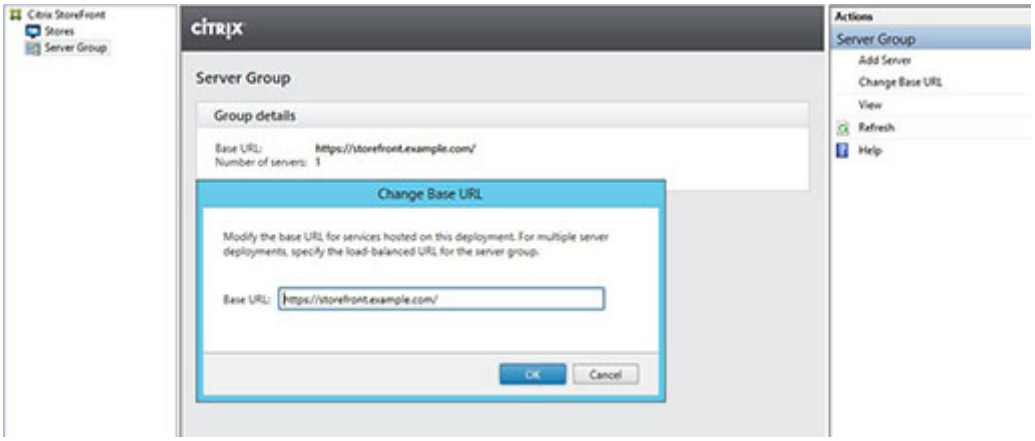


5. サードパーティ CA（Verisign など）、会社のルート CA、または中間 CA を使用して証明書に署名します。
6. 秘密キーを含めて、この証明書を PFX 形式でエクスポートします。
7. 証明書と秘密キーを StoreFront サーバーにインポートします。Windows NLB StoreFront クラスターを展開している場合は、すべてのノードにこの証明書をインポートします。Citrix ADC 負荷分散仮想サーバーなどの代替ロードバランサーを使用している場合は、そこに証明書をインポートします。
8. StoreFront サーバーの IIS で HTTPS バインドを作成し、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`



サーバーのベース **URL** を **HTTP** から **HTTPS** に変更

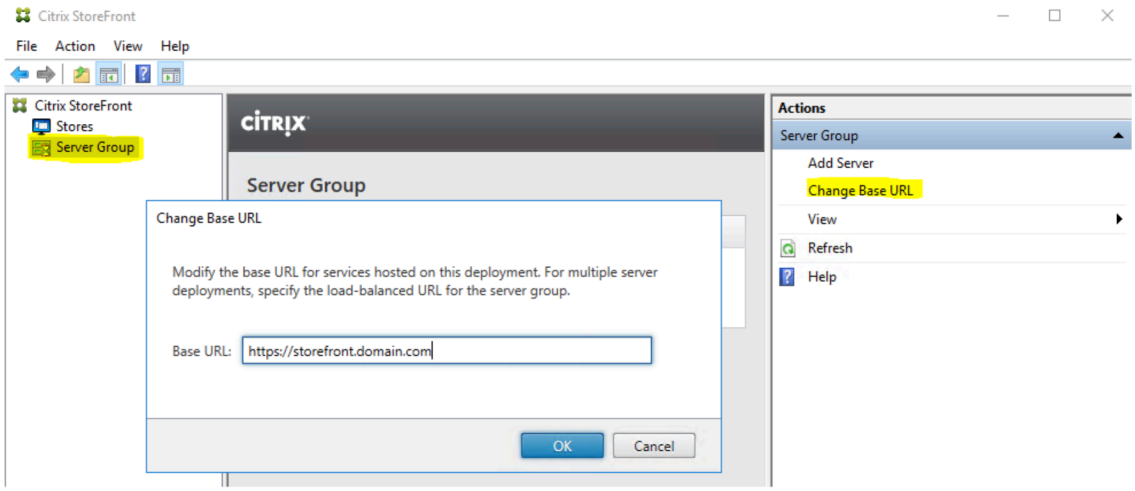
ホストのベース URL オプションは、Citrix StoreFront で単一サーバー展開またはサーバーグループ展開を構成するときに使用できます。これは、サーバー証明書なしで Citrix StoreFront をインストールおよび構成しているお客様にご利用いただけます。証明書をインストールした後、StoreFront とそのサービスがセキュアな接続を使用していることを確認します。

> 注:
>
> IT 管理者は、この手順を実行する前に、Citrix StoreFront サーバーにサーバー証明書を生成してインストールする必要があります。さらに、新しい接続を保護するには、HTTPS（ポート 443）に IIS バインドを作成す

> る必要があります。

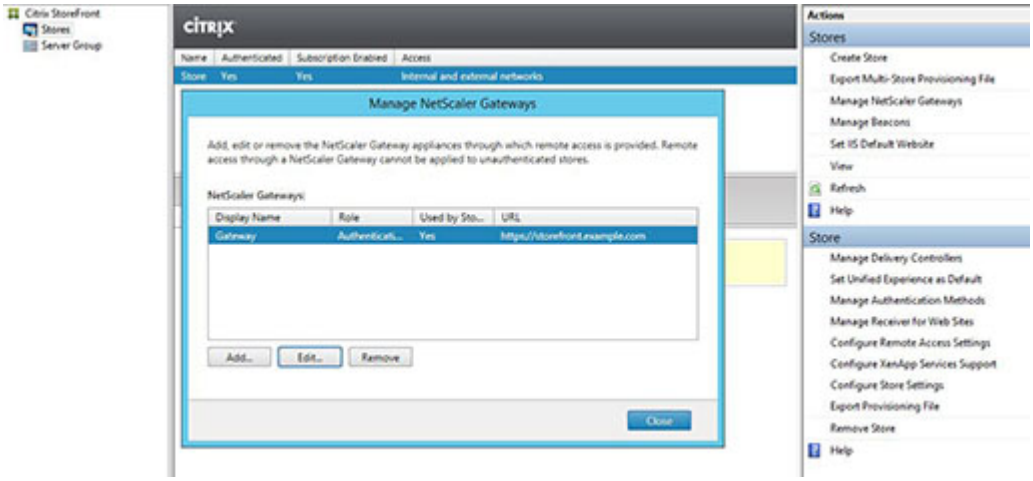
StoreFront 3.x のベース URL を変更するには、以下の手順を実行します:

1. StoreFront で、左ペインの ［サーバーグループ］ をクリックします。
2. 右ペインの ［ベース **URL** の変更］ をクリックします。
3. ベース URL を入力し、 ［**OK**］ をクリックします。

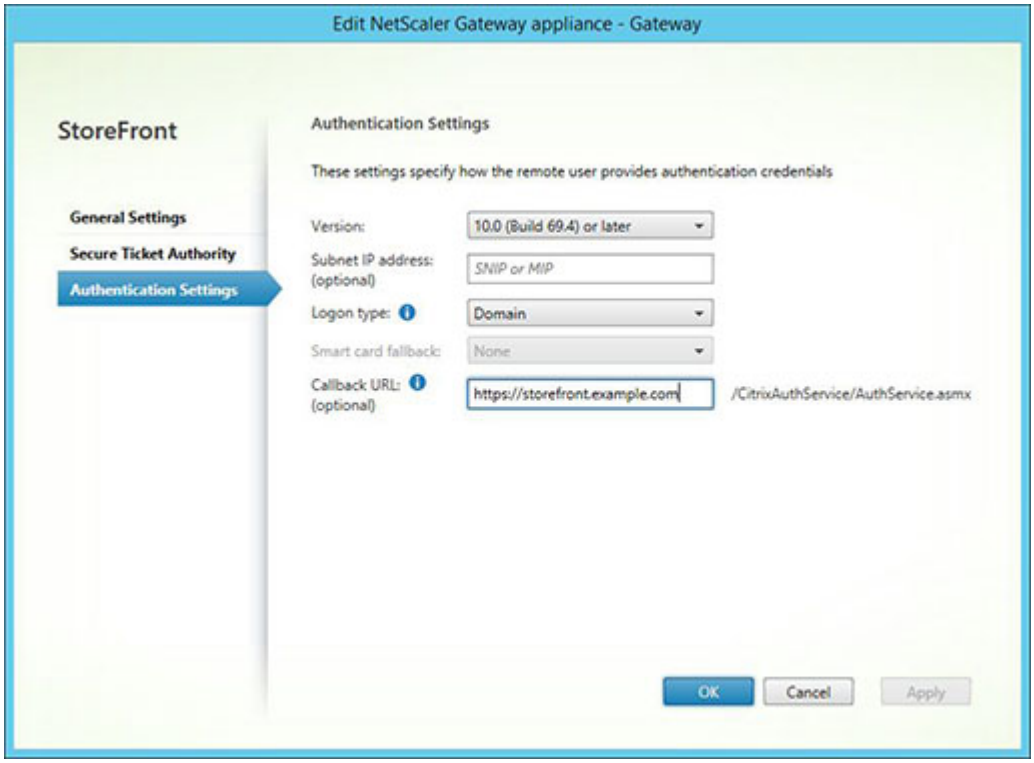


StoreFront サーバーでの **Gateway** の構成：**storefront.example.com**

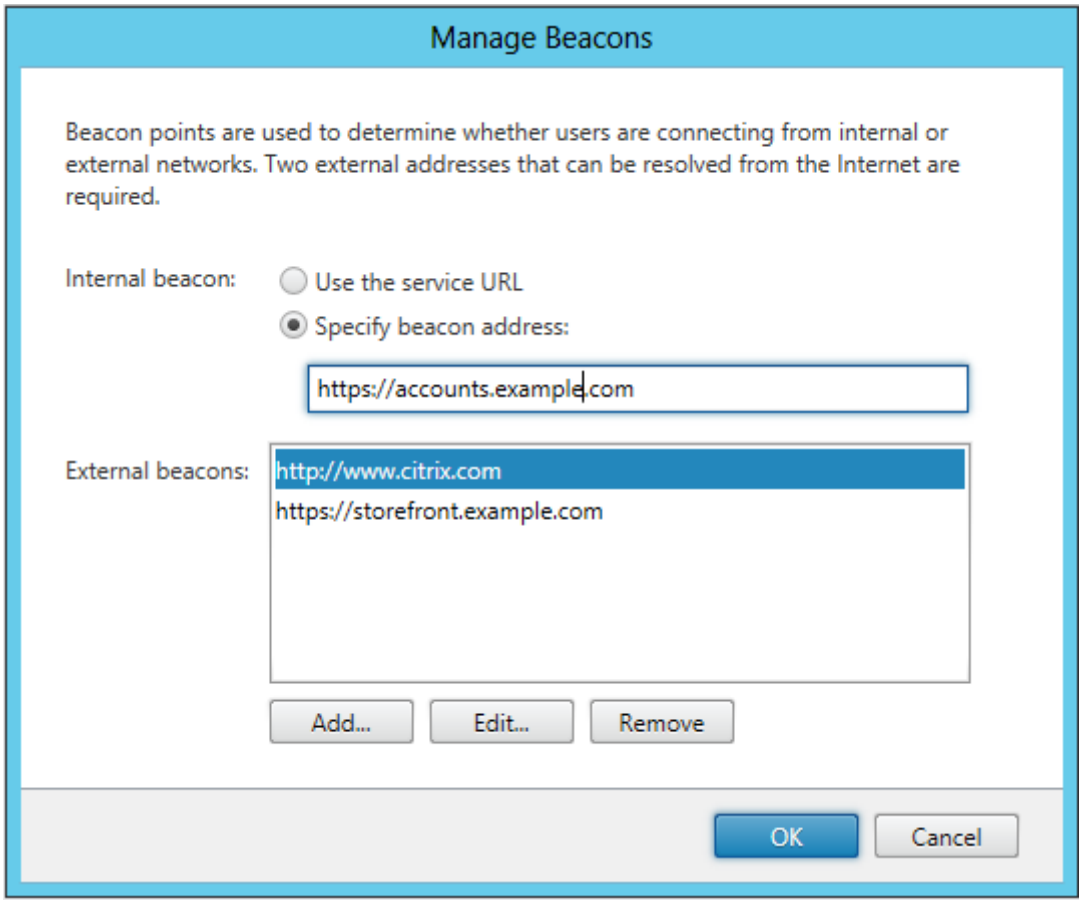
1. ［ストア］ ノードで、 ［**Citrix Gateway** の管理］ を ［操作］ ペインでクリックします。
2. サーバー名を変更するには、一覧から ［ゲートウェイ］ を選択し、 ［編集］ をクリックします。



3. ［全般設定］ ページで共有 FQDN を ［**Citrix 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 Citrix 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。



FQDN を使用した検出のサポート

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<allowedAudiences>エントリを追加します。このファイルには<allowedAudiences>エントリが 2 つあります。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<allowedAudience>エントリを追加する必要があります。

1. <service id> セクションで、<allowedAudiences> 文字列を見つけます。以下のようにaudience="https://accounts.example.com/"の行を追加します。web.config ファイルを保存して閉じます。

```
1 <service id="abd6f54b-7d1c-4a1b-a8d7-14804e6c8c64" displayName="
     Authentication Token Producer">
2 ...
3 <allowedAudiences>
4 <add name="https-storefront.example.com" audience="https://
     storefront.example.com/" />
```

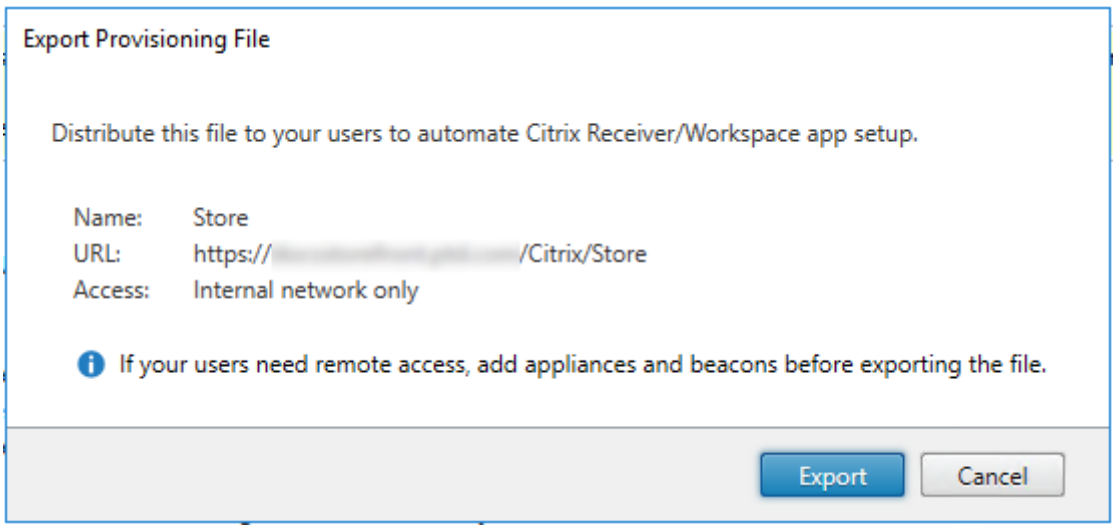


```
5 <add name="https-accounts.example.com" audience="https://accounts.
     example.com/" />
6 </allowedAudiences>
```

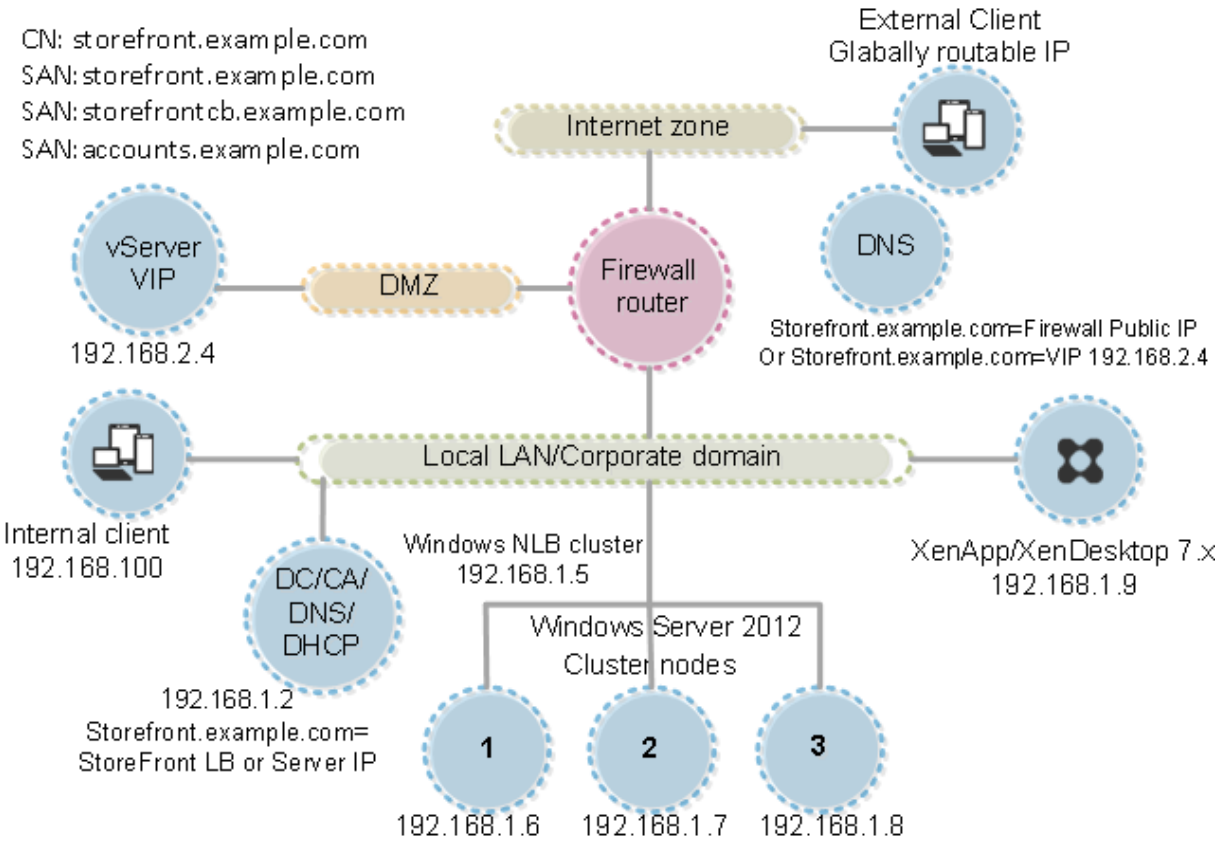
2. *C:\inetpub\wwwroot\Citrix\Roaming\web.config* で <tokenManager> セクションを見つけ、以下のようにaudience="https://accounts.example.com/"の行を追加します。web.config ファイルを保存して閉じます。

```
1 <tokenManager>
2 <services>
3 <clear />
4 ...
5 </trustedIssuers>
6 <allowedAudiences>
7 <add name="https-storefront.example.com" audience="https://
     storefront.example.com/" />
8 <add name='https-accounts.example.com" audience="https://accounts.
     example.com/" />
9 </allowedAudiences>
10 </service>
11 </services>
12 </tokenManager>
```

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もできます。これにより、Citrix Workspace アプリの初回使用時の設定が不要になります。このファイルをすべての Windows および MAC Citrix Workspace アプリクライアントに配布します。



Citrix Workspace がクライアントにインストールされいてる場合、CR ファイルタイプが認識され、プロビジョニングファイルをダブルクリックするとインポートが開始されます。



詳細構成

January 14, 2020

StoreFront コンソール、PowerShell、証明書プロパティ、または構成ファイルを使って、以下の詳細オプションを構成できます。

タスク	詳細
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。

リソースフィルターの構成

June 21, 2019

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、Citrix StoreFront SDK PowerShell Modules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。

フィルターの構成

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
```

種類によるフィルタリング

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。

キーワードによるフィルタリング

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、Citrix Virtual Apps and Desktops 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

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」および「アプリケーション配信の構成」を参照してください。

例

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

January 14, 2020

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 Workspace アプリログオンダイアログボックスのカスタマイズ
- Windows 向け Citrix Workspace アプリ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

April 2, 2020

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。

> 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。完了したら、
> 構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

ICA ファイル署名の有効化

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 Workspace アプリで、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の拡張が含まれる場合、キーをデジタル署名に使用できるようにする必要があります。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用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 Workspace アプリで 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。

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 サーバーの Citrix Delivery Services 証明書ストアで使用でき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。

```
<certificateManager>
    <certificates>
        <clear />
        <add ... />
        ...
    </certificates>
</certificateManager>
```

4. 署名に使用する証明書の詳細を含めます。

```
<certificateManager>
    <certificates>
        <clear />
        <add id=”certificateid” thumb=”certificatethumbprint” />
        <add ... />
    ...
    </certificates>
</certificateManager>
```

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。

```
<icaFileSigning enabled=”False” certificateId=”” hashAlgorithm=”
    sha1” />
```

6. 有効な属性の値を True に変更して、ストアの ICA ファイルの署名を有効にします。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 hashAlgorithm 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 APPPOOL\Citrix Delivery Services Resources”
```

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。

ファイルタイプの関連付けの無効化

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。

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。

```
<farmset ... enableFileTypeAssociation=”on” ... >
```

3. enableFileTypeAssociation 属性の値を off に変更して、ストアでのファイルタイプの関連付けを無効にします。

Citrix Workspace アプリログオンダイアログボックスのカスタマイズ

デフォルトでは、ユーザーがストアにログオンしても、ログオンダイアログボックスにタイトル文字列は表示されません。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。ログオンダイアログボックスにタイトル文字列が表示されるようにし、表示内容をカスタマイズするには、認証サービスのファイルを編集します。

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\ディレクトリにあります。
2. ファイル内で次の行を見つけます。

```
@* @Heading(”ExplicitAuth:AuthenticateHeadingText”) *@
```

3. 先頭の **\@*** と末尾の ***@** を削除して、このステートメントのコメントを解除します。

```
@Heading(”ExplicitAuth:AuthenticateHeadingText”)
```

これにより、Citrix Workspace アプリ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の *ExplicitFormsCommon.xx.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\reso ィレクトリにあります。

5. ファイル内で次の要素を検索します。<value> 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グボックスのタイトルが変更されます。

```
<data name="AuthenticateHeadingText" xml:space="preserve">
    <value>My Company Name</value>
</data>
```

ほかのロケールにいるユーザー用に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.languagecode.resx* ファイルを編集します。ここで **languagecode** は、ロケール識別子です。

Windows 向け Citrix Workspace アプリ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

Windows 向け Citrix Workspace アプリのデフォルトでは、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 または Windows 向け Citrix Workspace アプリ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）。

1. テキストエディターを使って、inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\UsernamePasswor ファイルを開きます。

2. ファイル内で次の行を見つけます。

```
@SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey:
    "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked:
    ControlValue("SaveCredentials"))
```

3. 次のようにステートメントにコメントします。

```
<!-- @SaveCredential(id: @GetTextValue("saveCredentialsId"),
    labelKey: "ExplicitFormsCommon:SaveCredentialsLabel",
    initiallyChecked: ControlValue("SaveCredentials")) -->
```

これにより、この認証サービスのストアに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、シトリックス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] フィールドの自動入力を無効にするには、ユーザーデバイスでレジストリを次のように編集します:

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

January 31, 2020

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。

> 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。完了したら、
> 構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

ユーザーに対するリソースの表示方式の構成

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。

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\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。

```
1 <uiViews showDesktopsView="true" showAppsView="true" defaultView="
    desktops" />
```


3. デスクトップとアプリケーションが（サイトから使用可能な場合でも）ユーザーに表示されないようにするには、それぞれ **showDesktopsView** 属性と **showAppsView** 属性の値を 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。

```
<userInterface ... autoLaunchDesktop="true">
```

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。

［マイアプリケーション］フォルダービューの無効化

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\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。

```
<userInterface enableAppsFolderView="true">
```

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

April 2, 2020

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。

Microsoft インターネットインフォメーションサービス（**IIS**）の構成

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。

ファイル拡張子

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 Workspace アプリのダウンロード/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

HTML5 向け Citrix Workspace アプリ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

MIME の種類

以下のファイルの種類に対応する MIME の種類を削除できます。

- .exe
- .dll
- .com
- .bat
- .csh

要求のフィルタリング

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
- ヘッド

その他の **Microsoft IIS** 設定

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

> 重要:
>
> - IIS 認証規則を構成しないでください。StoreFront は直接認証サポートし、IIS 認証を使用したり、サポートしたりしません。
> - StoreFront サイトの SSL 設定で ［**Client certificates: Require**］ を選択しないでください。StoreFront のインストールでは、この設定で StoreFront サイトの適切なページを構成します。
> - StoreFront には Cookie が必須であるため、［Use Cookies］設定を選択する必要があります。［cookieless/Use URI］設定は選択しないでください。
> - 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。ただし、アプリケーションプールのアイドル状態のタイムアウト値と、アプリケーションプールが使用する仮想メモリの量は設定できます。

ユーザー権利の構成

> 注:
>
> Microsoft IIS は、StoreFront がインストールされると有効化されます。Microsoft IIS により、組み込みグ

> ループ IIS_IUSRS にはバッチジョブとしてログオンするログオン権限、および認証後にクライアントを偽装する特権が付与されます。これは Microsoft IIS がインストールされるときの通常動作です。これらのユーザー権利は変更しないでください。詳しくは、Microsoft のドキュメントを参照してください。

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、およびプロセスレベルトークンの置き換えの特権が付与されます。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。対象となるアプリケーションプールは、Citrix 構成 API、Citrix Delivery Services リソース、Citrix Delivery Services 認証、Citrix Receiver for Web 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。これらの特権は 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特権が必要です。

サービス設定の構成

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。この構成は変更しないでください。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。

グループメンバーシップの構成

StoreFront サーバーグループを構成すると、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）このサービスはグループに属するサーバーでのみ表示され、参加処理中にのみ実行されます。

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

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。

StoreFront での証明書

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 Workspace アプリ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 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 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 Workspace アプリで 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 Workspace アプリにストアの 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でください。

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 は、*<InstallDirectory>*\Scripts のフォルダーに多数の PowerShell スクリプト（.ps1）を含みます。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ていません）。StoreFront は PowerShell 実行ポリシーを変更しません。

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。

StoreFront の通信

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 Citrix Virtual Apps 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、Citrix Virtual Apps のデフォルトのコンポーネントです。

StoreFront をホストする Web サーバーで TLS 1.0 および 1.1 のサポートを無効にすることをお勧めします。グループポリシーオブジェクト経由でこれを適用する必要があり、これによって StoreFront サーバーで必要なレジストリ設定を作成し古いプロトコル（TLS 1.0 や TLS 1.1 など）を無効にします。Microsoft のTLS/SSL Settingsも参照してください。

StoreFront とユーザーデバイスの間の通信は、Citrix 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 のセキュリティ境界による分離

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 経由の SaaS および Web アプリの配信

StoreFront ストア経由で SaaS および Web アプリケーションをユーザーに安全に配信できます。Citrix Cloud と StoreFront 用のアクセス制御 Sync ユーティリティを使用することで、これらのアプリにセキュリティ強化ポリシーおよび Web コンテンツの制限ポリシーを適用してユーザーやネットワークをマルウェアやデータ漏洩から保護できます。ユーザーは通常どおり StoreFront ストアにアクセスして、Citrix Cloud で構成した SaaS および Web アプリを起動します。詳しくは、「StoreFront での SaaS および Web アプリのアクセス制御」を参照してください。

ICA ファイルの署名

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 Workspace アプリでは、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。

ユーザーによるパスワードの変更

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。

StoreFront サーバーのベース URL を HTTP から HTTPS に変更

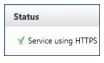
StoreFront とユーザーデバイス間の通信を HTTPS で保護するには、Microsoft インターネットインフォメーションサービス（IIS）で HTTPS を構成する必要があります。最初に SSL 証明書をインストールおよび構成せずに Citrix StoreFront をインストールおよび構成した場合、StoreFront は通信に HTTP を使用します。

後から SSL 証明書をインストールして構成する場合は、次の手順を実行して StoreFront とそのサービスが HTTPS 接続を使用するようにしてください。

例:

ベース **URL** を **HTTPS** に変更する前:

ベース **URL** を **HTTPS** に変更した後:



1. StoreFront サーバーの 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:
    a) 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 SSL サーバー証明書をインポートします。
    b) HTTPS（443）経由で IIS バインドをデフォルトの Web サイトに追加します。

詳しい手順については、CTX200292を参照してください。

2. Citrix StoreFront 管理コンソールの左側のペインで ［サーバーグループ］ を選択します。
3. ［操作］ペインの ［ベース **URL** の変更］ を選択します。
4. ベース URL を入力し、 ［**OK**］ をクリックします。

カスタマイズ

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。

セキュリティに関する詳細

> 注:
>
> この情報は予告なく変更されることがあります。

規制上の理由から、StoreFront のセキュリティスキャンを実行することをお勧めします。上記の設定オプションを使用することで、セキュリティスキャンの検出結果の一部をレポートから除外することができます。

セキュリティスキャナーと StoreFront の間にゲートウェイが介在している場合、検出結果のあるものは StoreFront 自体ではなくゲートウェイに関連する発見である可能性があります。セキュリティスキャンのレポートでは通常これらの発見は区別されません（たとえば、TLS 構成）。そのため、セキュリティスキャンレポートの技術的な説明により誤解が生じるおそれがあります。

セキュリティスキャンレポートを解釈するときは、次の点に注意してください:

- StoreFront の HTML ページにはクリックジャッキングに対する防御（コンテンツセキュリティポリシーまたは X-Frame-Options 応答ヘッダー）が搭載されていない場合があります。ただし、それらの HTML ページは静的コンテンツのみで構成されているため、クリックジャック攻撃の影響はそれほどありません。
- Microsoft IIS のバージョンと ASP.NET を使用していることが、HTTP ヘッダーを見るとわかるようになっています。ただしこの情報は、それらのテクノロジを基盤とする StoreFront を利用していることから明らかな事実ではあります。
- StoreFront はアプリケーションやデスクトップを起動するときに、トークンを使用してクロスサイトリクエストフォージェリ（CSRF）を防御します。このトークンは、Secure や HttpOnly という情報を明示せずに Cookie として応答に埋め込まれて送信されます。その後要求に含まれた状態で送信されるときに、このトークンは URL のクエリ文字列の一部として送信されます。ただし、StoreFront は HTTP 要求の認証に関してこのメカニズムに依存しません。
- StoreFront ではオープンソースのコンポーネントである jQuery を使用しています。ここで使用されているバージョンは jQuery 1.3.2 です。jQuery オープンソースプロジェクトによると、jQuery 1.12.0 で行った変

更により、特定の形式のクロスサイト要求に対する潜在的な脆弱性が軽減されているということです。この変更は jQuery 自体の脆弱性を軽減するものではなく、アプリケーションロジックが悪用される可能性を減らすためのものです。これと関連のある、NetScaler と StoreFront で共通して使用されている Receiver for Web 機能のアプリケーションロジックでは、問題となっているクロスドメイン要求の特定の形式を使用しておらず、この脆弱性の影響を受けません。同様にこの軽減措置による効果もありません。

この軽減措置は、互換性の理由からその後の jQuery 1.12.3 で撤廃されています。シトリックスのアプリケーションロジックはこの措置による影響を受けていないため、jQuery 1.12.4 を使用するバージョンの NetScaler および StoreFront でも措置が撤廃されたことによって大きな影響は受けていません。

StoreFront 構成のエクスポートとインポート

April 2, 2020

> 注:
>
> インポートできるのは、対象の StoreFront インストールと同じバージョンの StoreFront 構成のみです。

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。

構成のエクスポートとインポートを使用できるシナリオ

- StoreFront 展開環境は動作し、信頼できる状態の場合のみバックアップが作成されます。構成を変更した場合は、古いバックアップを置き換えるために新しいバックアップを作成する必要があります。backup.zip ファイルのファイルハッシュが変更を妨げるため、既存のバックアップを変更することはできません。
- StoreFront をアップグレードする前に障害回復用のバックアップを作成します。
- 既存のテスト用 StoreFront 展開を複製して実稼働環境に配置します。
- 実稼働環境をテスト環境に複製することにより、ユーザー承認環境を作成します。
- OS の移行中（ホスト OS を 2008R2 から 2019 にアップグレードするなど）に、StoreFront を移動します。
- 複数のデータセンターを持つ大企業など、複数地域での展開で追加のサーバーグループを構築します。

StoreFront 構成のエクスポートおよびインポート時の検討事項

- 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 コマンドレット

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。**-Credential** パラメーターを**-NoEncryption** 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”

パラメーター	説明
-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。

> 重要:
>
> 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 内で既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://<importingserver>.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\`

パラメーター	説明
-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。

構成のエクスポートおよびインポート例

現在の **PowerShell** セッションへの **StoreFront** コマンドレットのインポート

StoreFront サーバーで PowerShell Integrated Scripting Environment（ISE）を開き、以下を実行します。

```
1 $env:PSModulePath = [Environment]::GetEnvironmentVariable('PSModulePath
    ','Machine')
2 $SDKModules = 'C:\Program Files\Citrix\Receiver StoreFront\
    PowerShellSDK\Modules\Citrix.StoreFront'
3 Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose
4 Import-Module "$SDKModules.Authentication\Citrix.StoreFront.
    Authentication.psd1" -verbose
5 Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1" -
    verbose
6 Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -
    verbose
7 Import-Module "$SDKModules.WebReceiver\Citrix.StoreFront.WebReceiver.
    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

バックアップするサーバーの構成をエクスポートします。

```
1 Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -
    zipFileName "backup" -NoEncryption
```

backup.zip ファイルを安全な場所にコピーします。このバックアップを障害回復で使用して、サーバーを以前の状態に復元できます。

```
1 Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://storefront.example.com"
```

サーバー **A** の既存の構成をバックアップし、サーバー **B** に復元して既存のサーバーのクローンを作成する

バックアップするサーバーの構成をエクスポートします。

```
1 Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -
    zipFileName "backup" -NoEncryption
```

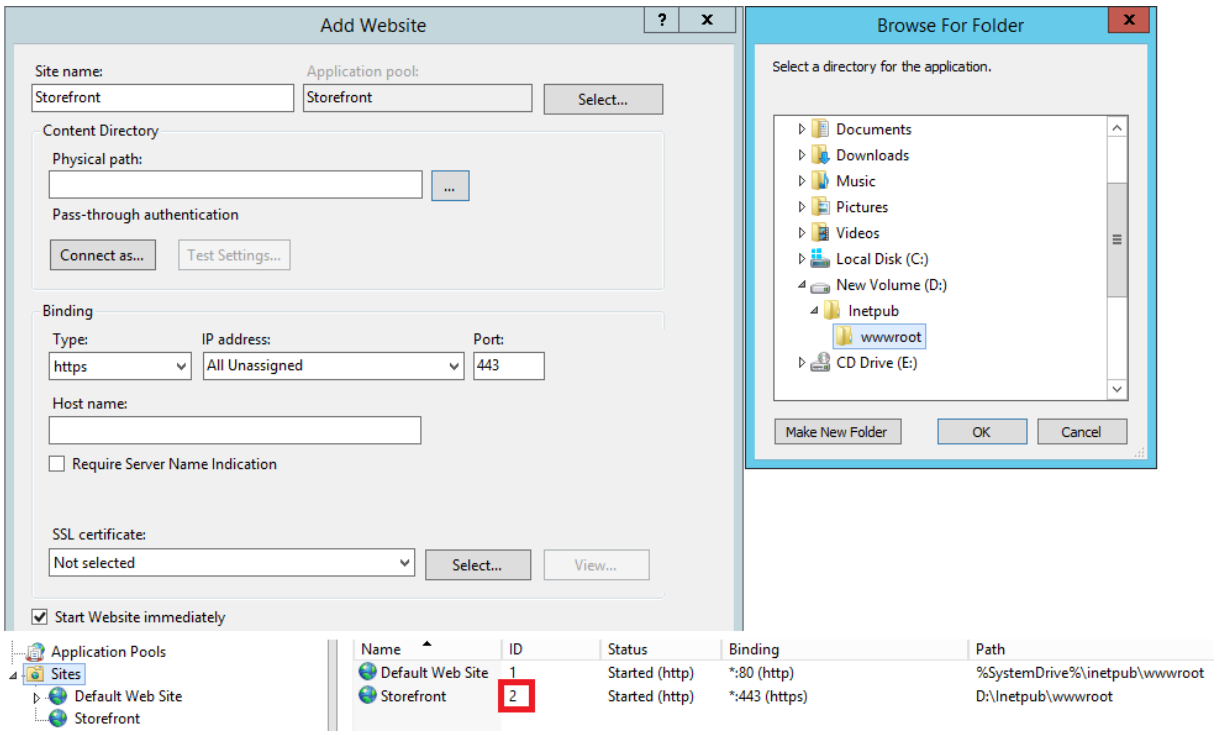
backup.zip ファイルをサーバー B のデスクトップにコピーします。

```
1 Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -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 という新しい Web サイトが、**SiteID = 2** を使用する IIS 内で構成されています。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. サーバー A の構成のコピーをエクスポートします。
2. サーバー B で、**SiteID 2** を使用する **StoreFront** という新しい Web サイトを IIS で構成します。
3. サーバー A の構成をサーバー 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 構成のインポート先 Web サイトに一致する必要があります。

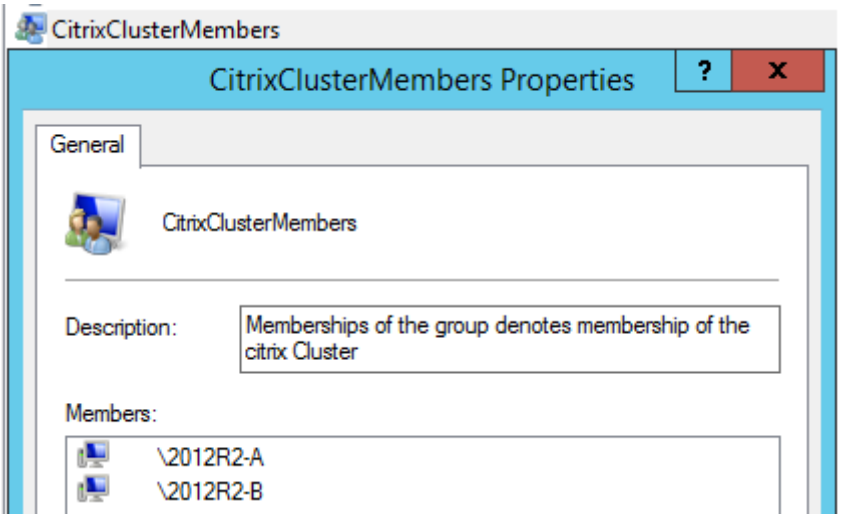
```
Import-STFConfiguration -configurationZip ”$env:userprofile\desktop\
backup.ctxzip”-HostBaseURL ”https://serverB.example.com”
```

サーバーグループシナリオ

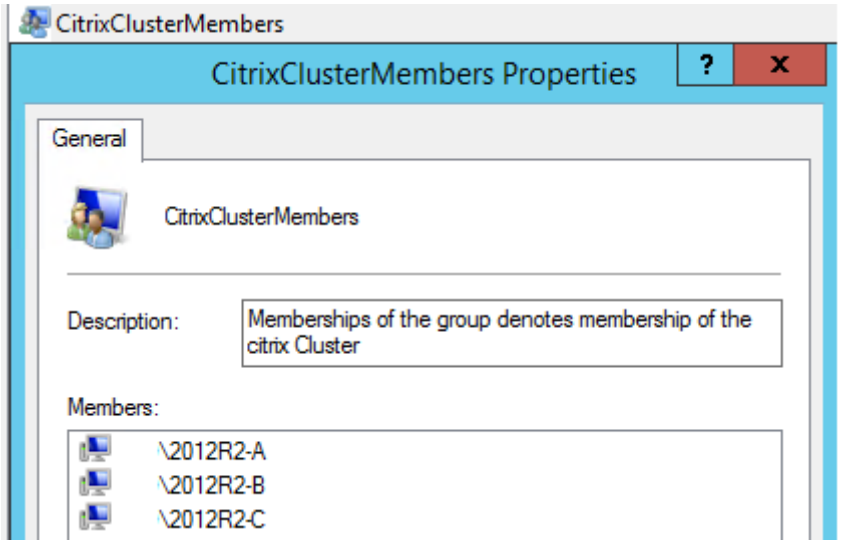
シナリオ **1**: 既存のサーバーグループ構成をバックアップし、後でそのバックアップを同じサーバーグループ環境で復元する

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。



1. 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。



1. 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。
2. 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”-HostBaseURL ”https://servergroup1.example.com”
```

3. 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 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"-HostBaseURL "https://servergroup2.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"-NoEncryption -HostBaseURL "https://servergroup2.example.
   ```



```
    com”
```

サーバー構成の暗号化されたバックアップを作成

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:
>
> 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。PowerShell セッション内に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。これは、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 ユーザーを取得します。

エクスポートサーバーの Powershell セッション内で PowerShell 資格情報オブジェクトを作成します。

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = ”Pa55w0rd”
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential(
    $User,$Password)
```

暗号化された zip ファイルである backup.ctxzip に構成をエクスポートします。

```
Export-STFConfiguration -targetFolder ”$env:userprofile\desktop\” -
    zipFileName ”backup” -Credential $CredObject
```

インポートサーバーの Powershell セッション内で同一の PowerShell 資格情報オブジェクトを作成します。

```
Import-STFConfiguration -configurationZip ”$env:userprofile\desktop\
    backup.ctxzip” -Credential $CredObject -HostBaseURL ”https://
    storefront.example.com”
```

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)

```



```
6 Unprotect-STFConfigurationExport -encryptedConfigurationZip "$env:
    userprofile\desktop\backup.ctxzip" -credential $CredObject -
    outputFolder "c:\StoreFrontBackups" -Force
```

StoreFront SDK

January 14, 2020

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：このバージョンでは、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、Citrix 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 3.6 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。

> 重要：
>
> 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 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、次のように入力します:

   ```
   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 サンプル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。このためには、以下の手順を実行します:
   - 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
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	説明
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。
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：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"
    )
```



```
16      # Import StoreFront modules. Required for versions of
            PowerShell earlier than 3.0 that do not support
            autoloading
17      Import-Module Citrix.StoreFront
18      Import-Module Citrix.StoreFront.Stores
19      Import-Module Citrix.StoreFront.Authentication
20      Import-Module Citrix.StoreFront.WebReceiver
```

- 指定の **$StoreVirtualPath** をベースとして認証および Citrix Receiver for Web サービスの仮想パスを自動化します。仮想パスは常に IIS のパスであるため、**$StoreVirtualPath** は **$StoreIISpath** と同じです。したがって Powershell では、「/Citrix/Store」、「/Citrix/StoreWeb」または「/Citrix/StoreAuth」のような値が使用されます。

```
1   # Determine the Authentication and Receiver virtual path to use
        based of the Store
2   $authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"
3   $receiverVirtualPath = "$($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。

```
1   # Determine if the deployment already exists
2   $existingDeployment = Get-STFDeployment
3   if(-not $existingDeployment)
4   {
5
6       # Install the required StoreFront components
7       Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -
            Confirm:$false
8    }
9
10  elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)
11  {
12
13      # The deployment exists but it is configured to the desired
            hostbase url
14      Write-Output "A deployment has already been created with the
            specified hostbase url on this server and will be used."
15   }
16
17  else
18  {
19
20      Write-Error "A deployment has already been created on this
            server with a different host base url."
```

```
21    }
```

- 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。

```
1  # Determine if the authentication service at the specified
       virtual path exists
2  $authentication = Get-STFAuthenticationService -VirtualPath
       $authenticationVirtualPath
3  if(-not $authentication)
4  {
5
6      # Add an Authentication service using the IIS path of the
           Store appended with Auth
7      $authentication = Add-STFAuthenticationService
           $authenticationVirtualPath
8   }
9
10 else
11 {
12
13     Write-Output ”An Authentication service already exists at the
           specified virtual path and will be used.”
14  }
```

- 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）。

```
1  # Determine if the store service at the specified virtual path
       exists
2  $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
3  if(-not $store)
4  {
5
6  # Add a Store that uses the new Authentication service configured
       to publish resources from the supplied servers
7  $store = Add-STFStoreService -VirtualPath $StoreVirtualPath -
       AuthenticationService $authentication -FarmName $Farmtype -
       FarmType $Farmtype -Servers $FarmServers -LoadBalance
       $LoadbalanceServers ‘
8          -Port $Port -SSLRelayPort $SSLRelayPort -TransportType
               $TransportType
9   }
10
11 else
```



```
{

    Write-Output "A Store service already exists at the specified virtual path and will be used. Farm and servers will be appended to this store."
    # Get the number of farms configured in the store
    $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.Count
    # Append the farm to the store with a unique name
    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。

```
# Determine if the receiver service at the specified virtual path exists
$receiver = Get-STFWebReceiverService -VirtualPath $receiverVirtualPath
if(-not $receiver)
{

    # Add a Receiver for Web site so users can access the applications and desktops in the published in the Store
    $receiver = Add-STFWebReceiverService -VirtualPath $receiverVirtualPath -StoreService $store
 }

else
{

    Write-Output "A Web Receiver service already exists at the specified virtual path and will be used."
 }
```

- ストアに対して XenApp サービスを有効にして、古い Citrix Receiver または Citrix Workspace アプリクライアントは公開アプリケーションに接続できます。

```
# Determine if PNA is configured for the Store service
$storePnaSettings = Get-STFStorePna -StoreService $store
if(-not $storePnaSettings.PnaEnabled)
{
```

```
5
6   # Enable XenApp services on the store and make it the default for
        this server
7   Enable-STFStorePna -StoreService $store -AllowUserPasswordChange
        -DefaultPnaService
8    }
```

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。

```
1   Param(
2       [Parameter(Mandatory=$true)]
3       [Uri]$HostbaseUrl,
4       [Parameter(Mandatory=$true)]
5       [long]$SiteId = 1,
6       [string]$Farmtype = ”XenDesktop”,
7       [Parameter(Mandatory=$true)]
8       [string[]]$FarmServers,
9       [string]$StoreVirtualPath = ”/Citrix/Store”,
10      [bool]$LoadbalanceServers = $false,
11      [int]$Port = 80,
12      [int]$SSLRelayPort = 443,
13      [ValidateSet(”HTTP”,”HTTPS”,”SSL”)]
14      [string]$TransportType = ”HTTP”,
15      [Parameter(Mandatory=$true)]
16      [Uri]$GatewayUrl,
17      [Parameter(Mandatory=$true)]
18      [Uri]$GatewayCallbackUrl,
```



```
19      [Parameter(Mandatory=$true)]
20      [string[]]$GatewaySTAUrls,
21      [string]$GatewaySubnetIP,
22      [Parameter(Mandatory=$true)]
23      [string]$GatewayName
24  )
25  Set-StrictMode -Version 2.0
26
27  # Any failure is a terminating failure.
28  $ErrorActionPreference = 'Stop'
29  $ReportErrorShowStackTrace = $true
30  $ReportErrorShowInnerException = $true
31  # Import StoreFront modules. Required for versions of PowerShell
       earlier than 3.0 that do not support autoloading
32  Import-Module Citrix.StoreFront
33  Import-Module Citrix.StoreFront.Stores
34  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。

```
1  # Create a simple deployment by invoking the SimpleDeployment
       example
2  $scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
       Definition -Parent
3  $scriptPath = Join-Path $scriptDirectory "SimpleDeployment.ps1"
4  & $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
       FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
       Farmtype $Farmtype `
5       -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。

```
1  # Determine the Authentication and Receiver sites based on the
       Store
2  $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
3  $authentication = Get-STFAuthenticationService -StoreService
       $store
4  $receiverForWeb = Get-STFWebReceiverService -StoreService $store
```

- Citrix 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。

```
# Get the Citrix Receiver for Web CitrixAGBasic and ExplicitForms
    authentication method from the supported protocols
# Included for demonstration purposes as the protocol name can be
    used directly if known
$receiverMethods = Get-
   STFWebReceiverAuthenticationMethodsAvailable | Where-Object {
 $_ -match "Explicit" -or $_ -match "CitrixAG"  }

# Enable CitrixAGBasic in Receiver for Web (required for remote
   access)
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。

```
# Get the CitrixAGBasic authentication method from the protocols
   installed.
# Included for demonstration purposes as the protocol name can be
    used directly if known
$citrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-
   Object {
 $_ -match "CitrixAGBasic"  }

# Enable CitrixAGBasic in the Authentication service (required
   for remote access)
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。

```
# Add a new Gateway used to access the new store remotely
Add-STFRoamingGateway -Name "NetScaler10x" -LogonType Domain -
   Version Version10_0_69_4 -GatewayUrl $GatewayUrl '
-CallbackUrl $GatewayCallbackUrl -SecureTicketAuthorityUrls
   $GatewaySTAUrls
# Get the new Gateway from the configuration (Add-
   STFRoamingGateway will return the new Gateway if -PassThru is
   supplied as a parameter)
$gateway = Get-STFRoamingGateway -Name $GatewayName
# If the gateway subnet was provided then set it on the gateway
   object
if($GatewaySubnetIP)
{
```

```
9
10      Set-STFRoamingGateway -Gateway $gateway -SubnetIPAddress
            $GatewaySubnetIP
11   }
12
13  # Register the Gateway with the new Store
14  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。

```
1   Param(
2       [Parameter(Mandatory=$true)]
3       [Uri]$HostbaseUrl,
4       [long]$SiteId = 1,
5       [string]$Farmtype = ”XenDesktop”,
6       [Parameter(Mandatory=$true)]
7       [string[]]$FarmServers,
8       [string]$StoreVirtualPath = ”/Citrix/Store”,
9       [bool]$LoadbalanceServers = $false,
10      [int]$Port = 80,
11      [int]$SSLRelayPort = 443,
12      [ValidateSet(”HTTP”,”HTTPS”,”SSL”)]
13      [string]$TransportType = ”HTTP”,
14      [Parameter(Mandatory=$true)]
15      [Uri]$GatewayUrl,
16      [Parameter(Mandatory=$true)]
```



```
17      [Uri]$GatewayCallbackUrl,
18      [Parameter(Mandatory=$true)]
19      [string[]]$GatewaySTAUrls,
20      [string]$GatewaySubnetIP,
21      [Parameter(Mandatory=$true)]
22      [string]$GatewayName,
23      [Parameter(Mandatory=$true)]
24      [Uri]$OptimalGatewayUrl,
25      [Parameter(Mandatory=$true)]
26      [string[]]$OptimalGatewaySTAUrls,
27      [Parameter(Mandatory=$true)]
28      [string]$OptimalGatewayName
29  )
30  Set-StrictMode -Version 2.0
31  # Any failure is a terminating failure.
32  $ErrorActionPreference = 'Stop'
33  $ReportErrorShowStackTrace = $true
34  $ReportErrorShowInnerException = $true
35  # Import StoreFront modules. Required for versions of PowerShell
        earlier than 3.0 that do not support autoloading
36  Import-Module Citrix.StoreFront
37  Import-Module Citrix.StoreFront.Stores
38  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。

```
1  # Create a remote access deployment
2  $scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
       Definition -Parent
3  $scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.
       ps1"
4  & $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
       FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
       Farmtype $Farmtype `
5       -LoadbalanceServers $LoadbalanceServers -Port $Port  -
           SSLRelayPort $SSLRelayPort -TransportType $TransportType `
6       -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。

```
1  # Add a new Gateway used for remote HDX access to desktops and
       apps
2  $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。

```
1  # Get the Store configured by SimpleDeployment.ps1
2  $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
3  # Register the Gateway with the new Store for launch against all
       of the farms (currently just one)
4  $farmNames = @($store.FarmsConfiguration.Farms | foreach {
5   $_.FarmName  }
6  )
7  Register-STFStoreOptimalLaunchGateway -Gateway $gateway -
       StoreService $store -FarmName $farmNames
```

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 認証は、StoreFront 管理コンソールで構成できます（「認証サービスの構成」を参照するか、以下の PowerShell コマンドレットを使用します：

- Export-STFSamlEncryptionCertificate
- Export-STFSamlSigningCertificate
- Import-STFSamlEncryptionCertificate
- Import-STFSamlSigningCertificate
- New-STFSamlEncryptionCertificate
- New-STFSamlIdPCertificate
- New-STFSamlSigningCertificate

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://<storefront host>/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。

```
1  Get-Module ”Citrix.StoreFront*” -ListAvailable | Import-Module
2
```



```
# 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/FederationMetadata.xml

# 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.xml"
```

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。

```
# 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：

```
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

January 31, 2020

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\StoreFront* 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 管理コンソールが自動的にトレース情報を記録します。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。完了したら、
> 構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

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、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。

   ```
   <logger duplicateInterval=”00:01:00”duplicateLimit=”10”>
   ```

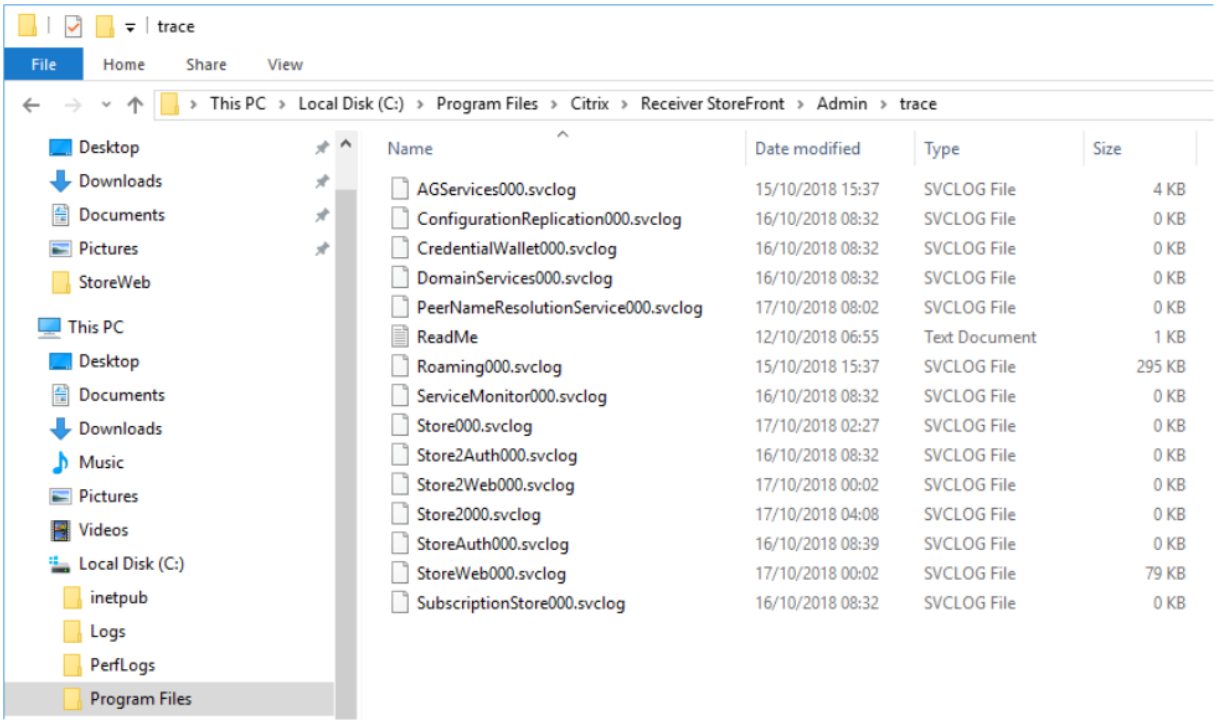
   StoreFront のデフォルトでは、重複するログエントリの数が 1 分あたり 10 件までに制限されます。
3. duplicateInterval 属性の値を変更して、重複エントリの監視期間を時間、分、秒で設定します。duplicateLimit 属性の値を変更して、指定した監視期間内に記録される重複エントリの数を設定します。この数を超えるとログ調整が実行されます。

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。

デバッグのトレースを有効にするには

> 重要:
>
> 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 コンソール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。

トレースの出力は c:\Program Files\Citrix\Receiver StoreFront\admin\trace に送信されます。



> 注：
>
> `Get-Help Set-STFDiagnostics -detailed`を実行して Powershell のヘルプおよび手順と Set-STFDiagnostics コマンドレットの使用方法の手順を入手します。

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。その後次の必須パラメーターを指定してトレースを有効または無効にします。

- **-All**。フラグは、すべてのインスタンスおよびサービスでトレースを更新する必要があることを示しています。
- **-TraceLevel**。トレースの詳細レベルが低い順に次の値が-TraceLevel に許可されています：Off、Error、Warning、Info、Verbose。大量のデータが生成されるため、トレースは StoreFront のパフォーマンスに重大な影響を与える可能性があります Info レベルまたは Verbose レベルの使用は、トラブルシューティングで指定された場合を除いてはお勧めしません。

オプションのパラメーター：

- **-FileSizeKb**。トレースファイルのサイズ（KB）。
- **-FileCount**。ディスク上で同時に保持できるトレースファイルの数。
- **-confirm:$False**。Windows のプロンプトが表示されないようにして、毎回 StoreFront コマンドレットを実行できるようにします。

例

デバッグのために、すべてのデバイスで Verbose レベルのトレースを有効にするには：

```
1 Set-STFDiagnostics -All -TraceLevel ”Verbose” -confirm:$False
```


すべてのサービスで Verbose レベルのトレースを無効にして、トレースレベルをデフォルト値設定に戻すには:

```
Set-STFDiagnostics -All -TraceLevel ”Error” -confirm:$False
```

Set-STFDiagnostics コマンドレットについて詳しくは、StoreFront PowerShell SDKのドキュメントを参照してください。

launch.ica ファイルのログ作成を有効にするには

launch.ica ファイルの情報をクライアントコンピューターに保存して、複数の問題をトラブルシューティングします。launch.ica ファイルは、Citrix Web Interface または Citrix StoreFront サーバーで生成されます。

launch.ica ファイルのログ作成を有効にするには、次の手順を完了します:

1. レジストリエディターを使用して次のレジストリキーを参照します:

   32 ビットシステム: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging

   64 ビットシステム: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging

2. 次の 2 つの文字列キー値を設定します:

   - LogFile=「ログファイルへのパス」
   - LogICAFile=true

   次に例を示します:

   ```
   LogFile=C:\ica\ica.log
   LogICAFile=true
   ```

そのほかの情報の入手先

> 注:
>
> トラブルシューティング目的以外で環境で ICA ファイルを使用する場合について詳しくは、CTX200126を参照してください。

StoreFront のアップグレードの問題に関するトラブルシューティング

以下の手順を使用して、StoreFront のアップグレードの問題をトラブルシューティングします。

アップグレード前の準備

1. すべての StoreFront サーバーのバックアップが存在することを確認してください。
2. StoreFront の製品終了となったバージョンからアップグレードしようとしていないことを確認してください。詳しくは、「CTX200356」を参照してください。
3. サポートされているバージョンの StoreFront から最新バージョンにのみアップグレードしていることを確認してください。
4. StoreFront サーバーが StoreFront サーバーグループの一部である場合は、グループ内のすべてのサーバーを順番にアップグレードする必要があります。StoreFront サーバーグループの同時アップグレードはサポートされていません。
5. *C:\inetpub\wwwroot\citrix* またはそのサブディレクトリ内の *thumbs.db* ファイルを削除します。この手順を完了するには、隠しファイルを表示します：［フォルダーオプション］**>**［表示］ で ［隠しファイル、隠しフォルダー、および隠しドライブを表示する］ オプション選択し、［保護されたオペレーティングシステムファイルを表示しない（推奨）］ オプションを選択解除します。
6. アップグレード手順を開始する前に、ウイルス対策ソフトウェアを無効にしてください。
7. アップグレード中のサーバーがロードバランサーから削除されていること、およびアクティブなユーザーセッションが接続されていないことを確認します。
8. アップグレードを実行する前に StoreFront サーバーを再起動します。
9. 次のサービスを手動で停止します：
   - CitrixConfigurationReplication
   - CitrixCredentialWallet
   - CitrixDefaultDomainService
   - CitrixPeerResolutionService
   - CitrixSubscriptionsStore
10. StoreFront 管理コンソールが閉じられていることを確認してください。

アップグレードが失敗した場合

1. *C:\Windows\Temp\StoreFront* で最新の *CitrixMsi*.log* を開き、例外エラーがないか確認します。

   Thumbs.db Access の例外：原因は *C:\inetpub\wwwroot\citrix* およびそのサブディレクトリ内の *thumbs.db* ファイルです。検出されたすべての *thumbs.db* ファイルを削除します。

   Cannot get exclusive file access \in use の例外：利用可能な場合スナップショット/バックアップを復元するか、サーバーを再起動し、すべての StoreFront サービスを手動で停止します。

   Service cannot be started の例外：利用可能な場合スナップショット/バックアップを復元するか、（クライアントプロファイルではなく）.NET framework 4.5 のフルバージョンをインストールします。

2. *CitrixMsi*.log* に例外エラーがない場合、サーバーの ［イベントビューアー］**>**［デリバリーサービス］ で上記の例外エラーメッセージが含まれるエラーがないか確認します。対応するアドバイスを実行します。

3. イベントビューアーに例外エラーがない場合、Admin ログの *C:\ProgramFiles\Citrix\Receiver StoreFront\logs* で上記の例外エラーメッセージが含まれるエラーがないか確認します。対応するアドバイスを実行します。

手動で **StoreFront** を削除するには

> 警告:
>
> 手動で StoreFront を削除すると、既存の情報がすべて消去されます。

手動で StoreFront を削除するには、以下を実行します:

1. StoreFront のアンインストール。
2. Web サーバーの役割を削除します。
3. *C:\Program Files\Citrix\Receiver StoreFront* フォルダーを削除します。
4. *C:\Program Files\Citrix\StoreFront Install* のすべてのサブディレクトリを削除します。
5. *C:\Inetpub* フォルダーを削除します。

StoreFront を再インストールできるようになりました。

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States