フェデレーション認証サービス 2103

Contents

フェデレーション認証サービス **2103**

June 23, 2023

フェデレーション認証サービス 2103（PDF ダウンロード）

この製品バージョンのドキュメントは最新リリースではありません。最近更新されたコンテンツについては、フェデレーション認証サービスの最新リリースに関するドキュメントを参照してください。

> 注:
>
> PDF から外部サイトへのリンクは正しいサイトに移動しますが、ドキュメント内を移動するリンクは無効になっています。

フェデレーション認証サービス **2103**

November 9, 2021

フェデレーション認証サービス 2103 には、次の新機能が含まれています。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。

Citrix_SmartcardLogon 証明書テンプレートの強化

Citrix_SmartcardLogon 証明書テンプレートのアプリケーションポリシーの拡張に、「クライアント認証」および「スマートカードによるログオン」が含まれるようになりました。[AUTH-812]

パフォーマンスカウンターの向上

Windows パフォーマンスモニターに表示されるカウンター名やカウンター機能など、さまざまな面での FAS パフォーマンスカウンターの向上。「パフォーマンスカウンター」を参照してください。

解決された問題

June 29, 2021

フェデレーション認証サービス 2103 で解決された問題はありません。

既知の問題

June 29, 2021

フェデレーション認証サービス 2103 には既知の問題はありません。

レジストリエントリの変更を伴う回避策については、次の点に注意してください:

> 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、オペレーティングシステム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。

サードパーティ製品についての通知

November 9, 2021

フェデレーション認証サービスのこのリリースには、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:

- Citrix Virtual Apps and Desktops サードパーティ製品についての通知（PDF ダウンロード）
- Non-Commercial Software Disclosures For FlexNet Publisher 2017 (11.15.0.0)（PDF のダウンロード）（英語）
- FLEXnet Publisher Documentation Supplement Third Party および FlexNet Publisher 11.15.0 で使用されるオープンソースソフトウェア（PDF のダウンロード）（英語）

システム要件

September 30, 2021

- フェデレーション認証サービス（FAS）は、次の Windows Server バージョンでサポートされています:
  - Windows Server 2019 の Standard Edition、Datacenter Edition、および Server Core オプション付き
  - Windows Server 2016 の Standard Edition、Datacenter Edition、および Server Core オプション付き

- FAS は、ほかの Citrix コンポーネントを含まないサーバーにインストールすることをお勧めします。
- Windows サーバーはセキュリティ保護されている必要があります。Windows サーバーには登録機関の証明書および秘密キーへのアクセス権限があり、ドメインユーザーに対して自動的に証明書を発行できます。また、これらのユーザー証明書および秘密キーへのアクセス権限もあります。
- FAS PowerShell コマンドレットを使用するには、Windows PowerShell 64 ビットが FAS サーバーにインストールされている必要があります。
- ユーザー証明書を発行するには、Microsoft エンタープライズ証明機関（ルートまたは下位）が必要です。

Citrix Virtual Apps サイトまたは Citrix Virtual Desktops サイトの要件:

- Delivery Controller、Virtual Delivery Agent（VDA）、StoreFront サーバーはすべて現在サポートされているバージョンを使用する必要があります。

  > 注:
  >
  > FAS は XenApp および XenDesktop 7.6 長期サービスリリース（LTSR）ではサポートされていません。

- マシンカタログを作成する前に、フェデレーション認証サービスのグループポリシー構成が適切に VDA に適用されている必要があります。詳しくは、「グループポリシーの構成」セクションを参照してください。

このサービスの展開を計画する場合は、「セキュリティに関する注意事項」セクションを参照してください。

インストールと構成

November 9, 2021

インストールとセットアップの順序

1. フェデレーション認証サービスのインストール（FAS）
2. StoreFront ストアでの FAS プラグインの有効化
3. Delivery Controller の構成
4. グループポリシーの構成
5. FAS 管理コンソールを使用して、以下を行います:
   a) 証明書テンプレートの展開
   b) 証明機関のセットアップ
   c) 証明機関を使用するための FAS の認証
   d) ルールの構成
   e) FAS の Citrix Cloud への接続（オプション）

フェデレーション認証サービスのインストール

セキュリティ上の理由により、フェデレーション認証サービス（FAS）は、ドメインコントローラーや証明機関と同様にセキュリティ保護されている専用サーバーにインストールすることをお勧めします。FAS は次のいずれかの方法でインストールできます:

- Citrix Virtual Apps and Desktops インストーラー（ISO の挿入時に自動実行されるスプラッシュスクリーンの ［フェデレーション認証サービス］ボタンから）を使用、または
- スタンドアロンの FAS インストーラーファイル（Citrix ダウンロードから MSI ファイルでダウンロード）を使用。

以下のコンポーネントをインストールします:

- フェデレーション認証サービス
- 詳細な FAS 構成用のPowerShell スナップインコマンドレット
- FAS 管理コンソール
- FAS のグループポリシーテンプレート（CitrixFederatedAuthenticationService.admx/adml）
- 証明書テンプレートファイル
- パフォーマンスカウンターおよびイベントログ

FAS のアップグレード

インプレースアップグレードで FAS を新しいバージョンにアップグレードできます。アップグレード前に、以下に注意してください:

- インプレースアップグレードを行った場合、FAS サーバーの設定はすべて保持されます。
- FAS をアップグレードする前に、FAS 管理コンソールが閉じていることを確認してください。
- 1 台以上の FAS サーバーを常に利用可能な状態に維持してください。フェデレーション認証サービスに対応した StoreFront サーバーから到達可能なサーバーがない場合、ユーザーはログオンやアプリケーションの起動を行えなくなります。

アップグレードを開始するには、Citrix Virtual Apps and Desktops インストーラーまたはスタンドアロンの FAS インストーラーファイルを使用して FAS をインストールします。

StoreFront ストアでの **FAS** プラグインの有効化

> 注:
>
> FAS を Citrix Cloud でのみ使用する場合は、この手順は必要ありません。

StoreFront ストアで FAS の統合を有効にするには、管理者アカウントで以下の PowerShell コマンドレットを実行します。ストア名が異なる場合は、`$StoreVirtualPath`を変更します。


```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module
$StoreVirtualPath = "/Citrix/Store"
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$auth = Get-STFAuthenticationService -StoreService $store
Set-STFClaimsFactoryNames -AuthenticationService $auth -
    ClaimsFactoryName "FASClaimsFactory"
Set-STFStoreLaunchOptions -StoreService $store -
    VdaLogonDataProvider "FASLogonDataProvider"
```

FAS の使用を停止するには、以下の PowerShell スクリプトを使用します:

```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module
$StoreVirtualPath = "/Citrix/Store"
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$auth = Get-STFAuthenticationService -StoreService $store
Set-STFClaimsFactoryNames -AuthenticationService $auth -
    ClaimsFactoryName "standardClaimsFactory"
Set-STFStoreLaunchOptions -StoreService $store -
    VdaLogonDataProvider ""
```

Delivery Controller の構成

> 注:
>
> FAS を Citrix Cloud でのみ使用する場合は、この手順は必要ありません。

FAS を使用するには、このサービスに接続可能な StoreFront サーバーを信頼するように Citrix Virtual Apps または Citrix Virtual Desktops の Delivery Controller を構成します。PowerShell コマンドレット **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true** を実行します。サイト内の Delivery Controller の数にかかわらず、これを実行するのはサイトごとに一度のみです。

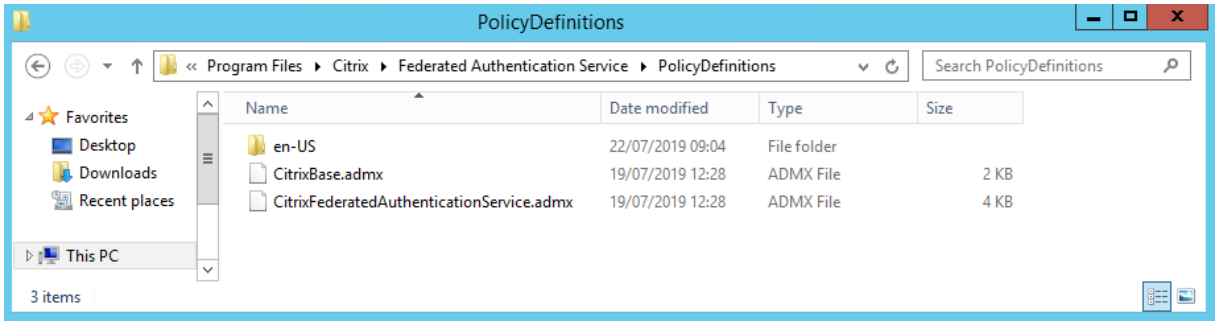
グループポリシーの構成

FAS のインストール後は、インストールで提供されたグループポリシーテンプレートを使用して、グループポリシー内の FAS サーバーの完全修飾ドメイン名（FQDN）を指定する必要があります。

> 重要:
>
> チケットを要求する StoreFront サーバーおよびチケットを使用する Virtual Delivery Agent（VDA）に、グループポリシーオブジェクトによって適用されるサーバーの自動番号設定を含む、同じ FQDN 構成を行う必要があります。

説明をシンプルにするために、以下の例ではすべてのマシンに適用されるドメインレベルで単一のポリシーを構成していますが、これは必須ではありません。StoreFront サーバー、VDA、および FAS 管理コンソールを実行しているマシンで同じ FQDN の一覧が参照されている限り、FAS は機能します。手順 6 を参照してください。

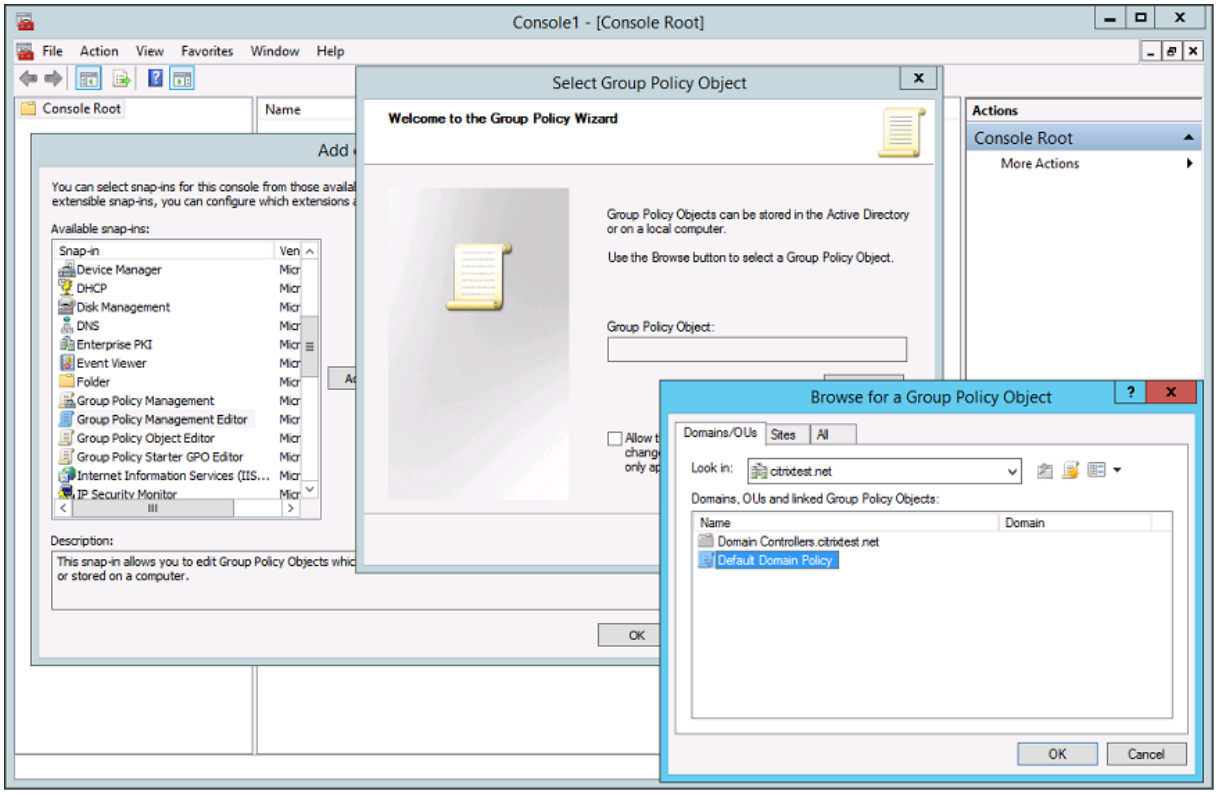
手順 **1**: FAS をインストールしたサーバーで、C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx ファイル、CitrixBase.admx ファイル、および en-US フォルダーを見つけます。



手順 **2**: これらをドメインコントローラーにコピーして、C:\Windows\PolicyDefinitions および en-US サブフォルダーに配置します。

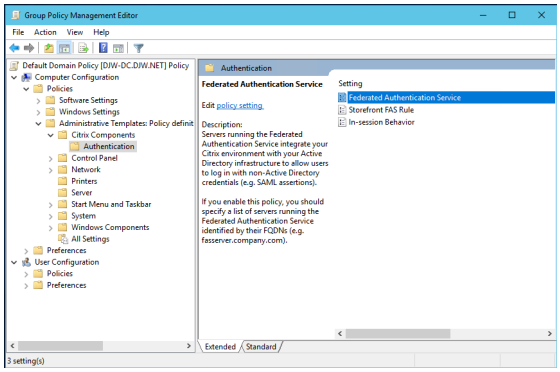
手順 **3**: コマンドラインから Microsoft 管理コンソールを実行します（mmc.exe）。メニューバーから、［ファイル］**>**［スナップインの追加と削除］の順に選択します。グループポリシー管理エディターを追加します。

グループポリシーオブジェクトを入力するための画面が開いたら、［参照］を選択してから［既定のドメインポリシー］を選択します。または、任意のツールを使用して、環境に応じたポリシーオブジェクトを作成して選択することもできます。このポリシーは、影響を受ける Citrix ソフトウェア（VDA、StoreFront サーバー、管理ツール）を実行しているすべてのマシンに適用する必要があります。



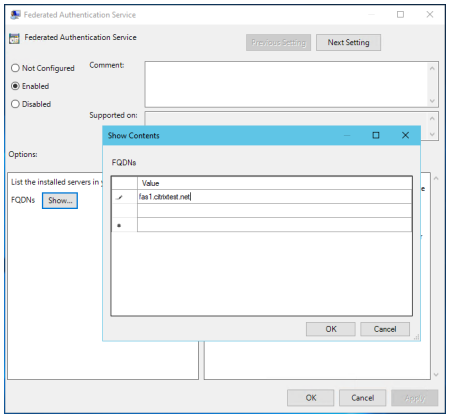
手順 **4**: Computer Configuration/Policies/Administrative Templates/Citrix Components/Authentica-

tion にあるフェデレーション認証サービスポリシーに移動します。



> 注:
>
> フェデレーション認証サービスのポリシー設定は、CitrixBase.admx または CitrixBase.adml テンプレートファイルを PolicyDefinitions フォルダーに追加する際に、ドメイン GPO でのみ使用できます。手順 3 の後、フェデレーション認証サービスのポリシー設定は、[管理用テンプレート] > [Citrix コンポーネント] > [認証] フォルダーに表示されます。

手順 **5**: フェデレーション認証サービスポリシーを開き、[有効] を選択します。これにより、FAS サーバーの FQDN を構成する [表示] ボタンを選択できるようになります。



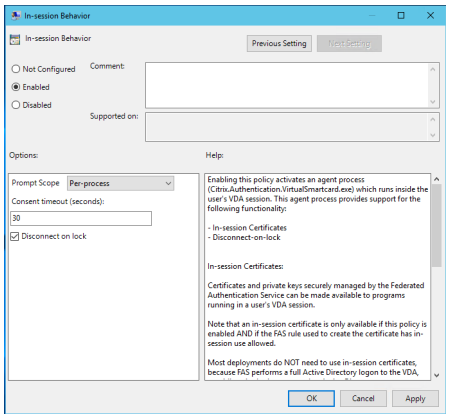
手順 **6**: FAS サーバーの FQDN を入力します。

> 重要:
>
> 複数の FQDN を入力する場合は、VDA、StoreFront サーバー（存在する場合）と FAS サーバー間で一覧の順番が統一されている必要があります。「グループポリシー設定」を参照してください。

手順 **7**: [**OK**] をクリックしてグループポリシーウィザードを終了し、グループポリシーの変更を適用します。変更を反映させるには、マシンを再起動（またはコマンドラインから **gpupdate /force** を実行）する必要がある場合があります。

In-session Behavior

このポリシーはセッション内証明書、承認、ロック時の切断をサポートするユーザーの VDA セッションでエージェントプロセスをアクティブ化します。セッション内証明書はこのポリシーが有効かつ証明書の作成に使用される FAS ルールでセッション内使用が許可されている場合のみ使用できます。「ルールの構成」を参照してください。



Enable によってこのポリシーが有効になり FAS エージェントプロセスがユーザーの VDA セッションで実行できます。

Disable によってこのポリシーが無効になり FAS エージェントプロセスが実行を停止します。

メッセージのスコープ　このポリシーが有効な場合、**Prompt Scope** によってアプリケーションでセッション内証明書を使用を許可するかというメッセージをユーザーに表示する方法を制御できます。3 つのオプションがあります。

- **No consent required**—このオプションはセキュリティメッセージを無効にし、ユーザーが操作する必要なく秘密キーが使用されます。
- **Per-process consent**—実行中のプログラムごとに個別に承認メッセージが表示されます。
- **Per-session consent**—ユーザーが一度［**OK**］をクリックすると、セッションのすべてのプログラムに適用されます。

承認のタイムアウト　このポリシーが有効になると、**Consent Timeout** によって承認が表示される期間を秒単位で制御できます。たとえば、5 分ごとに 300 秒間メッセージが表示される、などです。この値が 0 の場合、秘密キーの操作ごとにユーザーにメッセージが表示されます。

ロック時の切断　このポリシーを有効にすると、ユーザーが画面をロックしたときにセッションが自動的に切断されます。この機能では「スマートカードの取り出し時の切断」ポリシーと同様の動作になるため、ユーザーが Active Directory ログオン資格情報を持っていない場合に便利です。

> 注:
>
> ロック時の切断ポリシーは、VDA 上のすべてのセッションに適用されます。

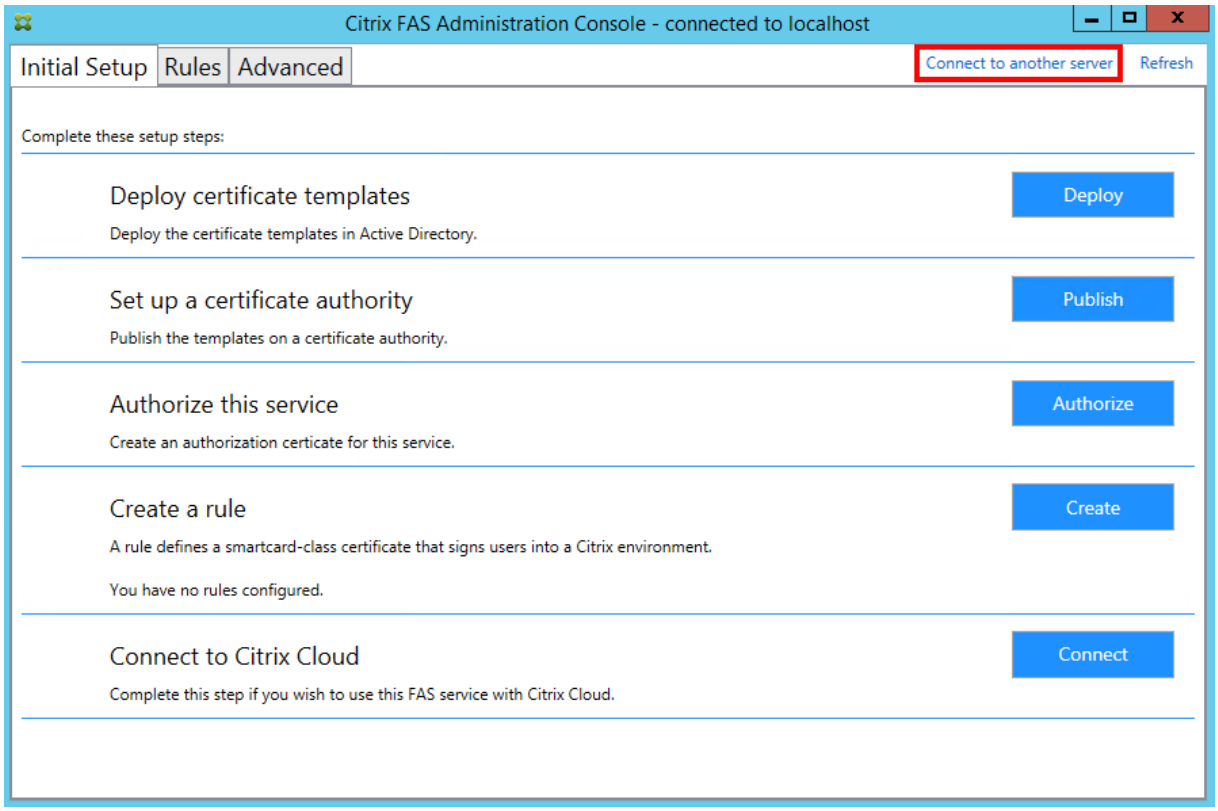
フェデレーション認証サービス管理コンソールの使用

> 注:
>
> 大半の展開には FAS 管理コンソールが適していますが、PowerShell インターフェイスにはより詳細なオプションもあります。FAS PowerShell コマンドレットについて詳しくは、「PowerShell コマンドレット」を参照してください。

FAS 管理コンソールは FAS の一部としてインストールされます。[スタート] メニューにアイコン（Citrix Federated Authentication Service）が配置されます。

管理コンソールの初回使用時は、証明書テンプレートの展開、証明機関のセットアップ、および FAS への証明機関の使用権限の付与を行う手順が表示されます。一部の手順は、OS 構成ツールを使用して手動で完了することもできます。

FAS 管理コンソールは、デフォルトでローカルの FAS サービスに接続されます。必要に応じ、コンソールの右上に表示される ［**Connect to another server**］を使用してリモートサービスに接続できます。

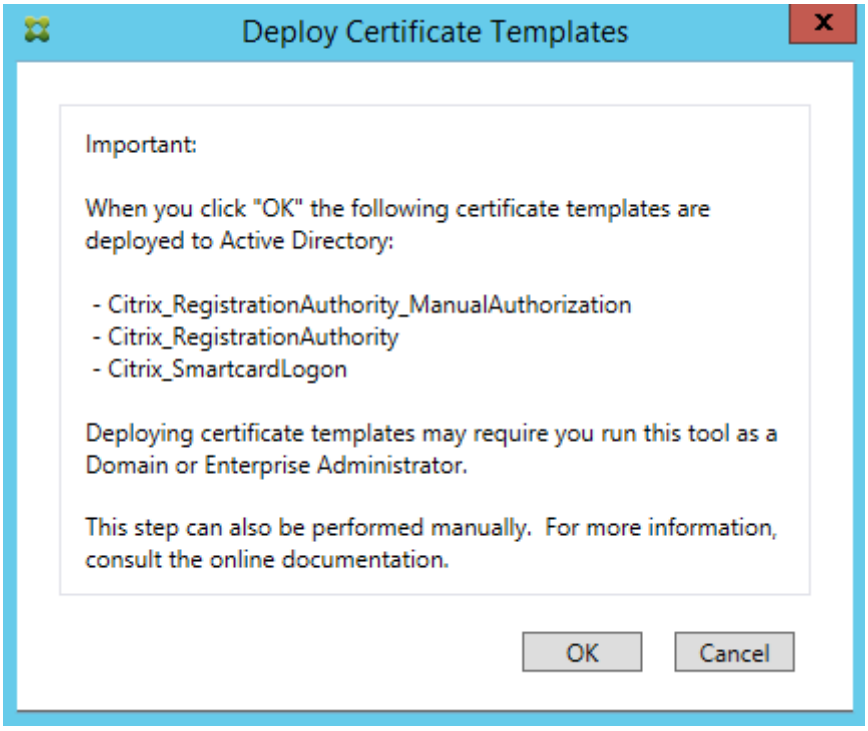


証明書テンプレートの展開

他のソフトウェアとの相互運用性の問題を避けるため、FAS では、独自の目的で使用する 3 つの Citrix 証明書テンプレートが用意されています。

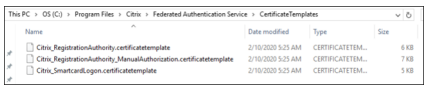
- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

これらのテンプレートは、Active Directory で登録する必要があります。[**Deploy**] をクリックしてから、[**OK**] をクリックします。



テンプレートの構成は、以下のフォルダーに FAS と一緒にインストールされた、拡張子「.certificatetemplate」の XML ファイル内にあります:

C:\Program Files\Citrix\Federated Authentication Service\CertificateTemplates



これらのテンプレートファイルをインストールする権限がない場合は、テンプレートファイルを Active Directory 管理者に渡してください。

テンプレートが含まれるフォルダーから以下の PowerShell コマンドを実行すると、テンプレートを手動でインストールできます:

```
1      $template = [System.IO.File]::ReadAllBytes("$Pwd\
          Citrix_SmartcardLogon.certificatetemplate")
```



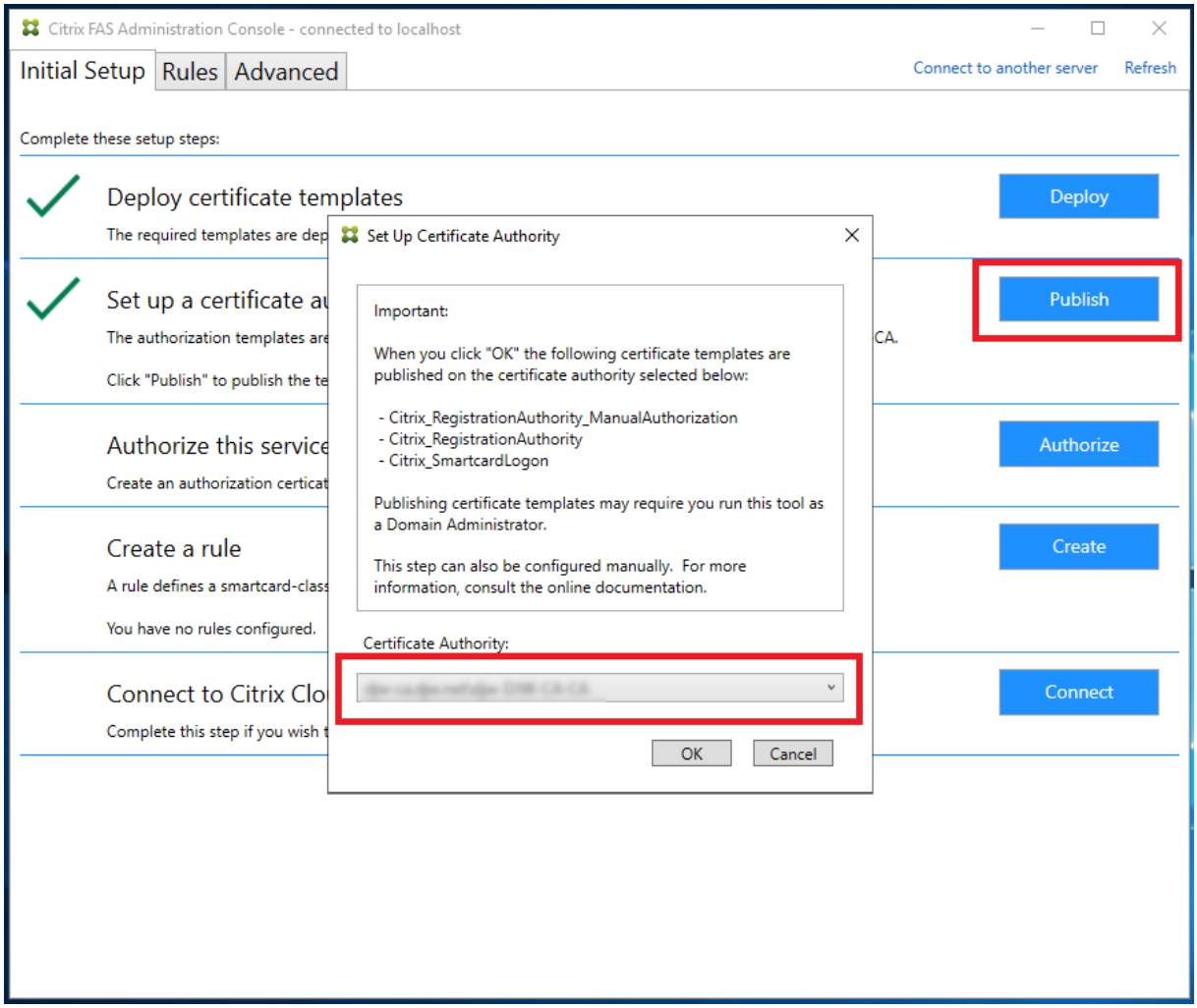
```
2     $CertEnrol = New-Object -ComObject X509Enrollment.
         CX509EnrollmentPolicyWebService
3     $CertEnrol.InitializeImport($template)
4     $comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)
5     $writabletemplate = New-Object -ComObject X509Enrollment.
         CX509CertificateTemplateADWritable
6     $writabletemplate.Initialize($comtemplate)
7     $writabletemplate.Commit(1, $NULL)
```

Active Directory 証明書サービスのセットアップ

Citrix 証明書テンプレートのインストール後は、これらのテンプレートを 1 つまたは複数の Microsoft エンタープライズ証明機関サーバーで公開する必要があります。Active Directory 証明書サービスの展開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。

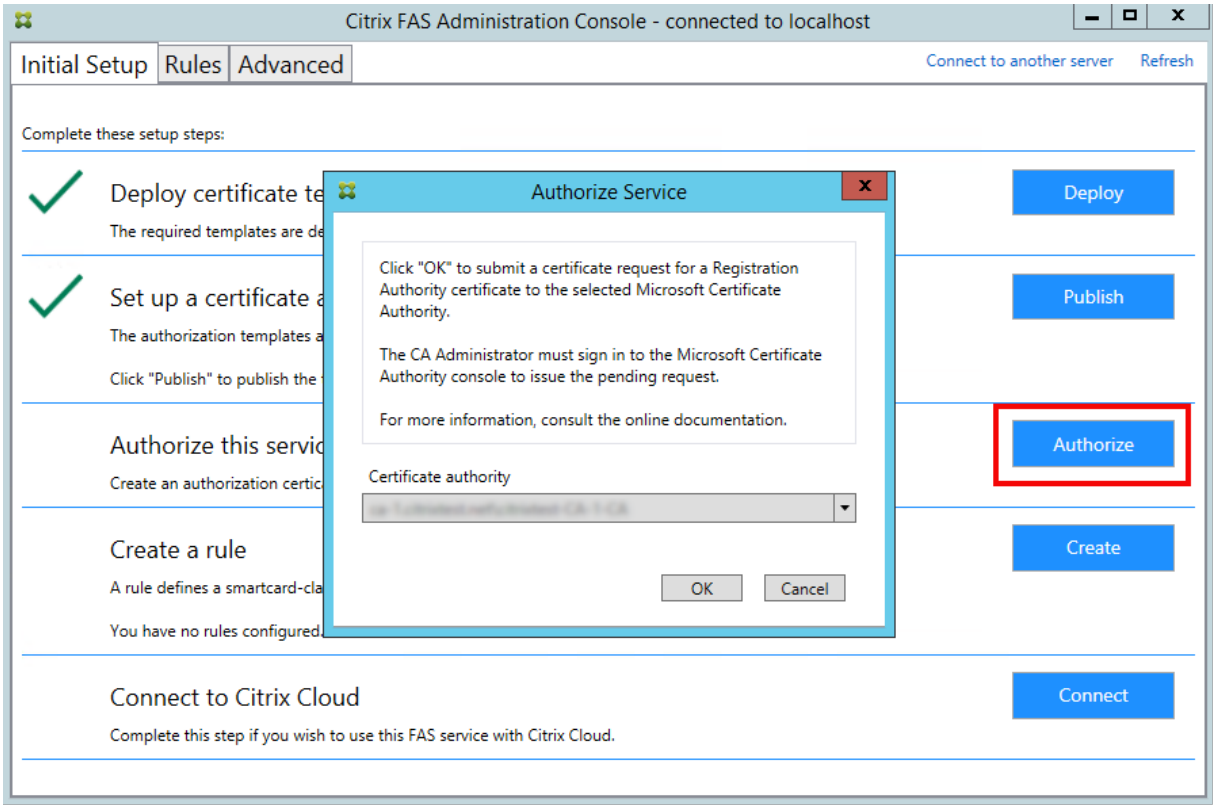
どのサーバーでもテンプレートが公開されていない場合は、**Set Up Certificate Authority** を使用して公開できます。これは、証明機関の管理権限のあるユーザーとして実行する必要があります。

(証明書テンプレートは、Microsoft 証明機関コンソールを使用して公開することもできます。)



フェデレーション認証サービスへの権限付与

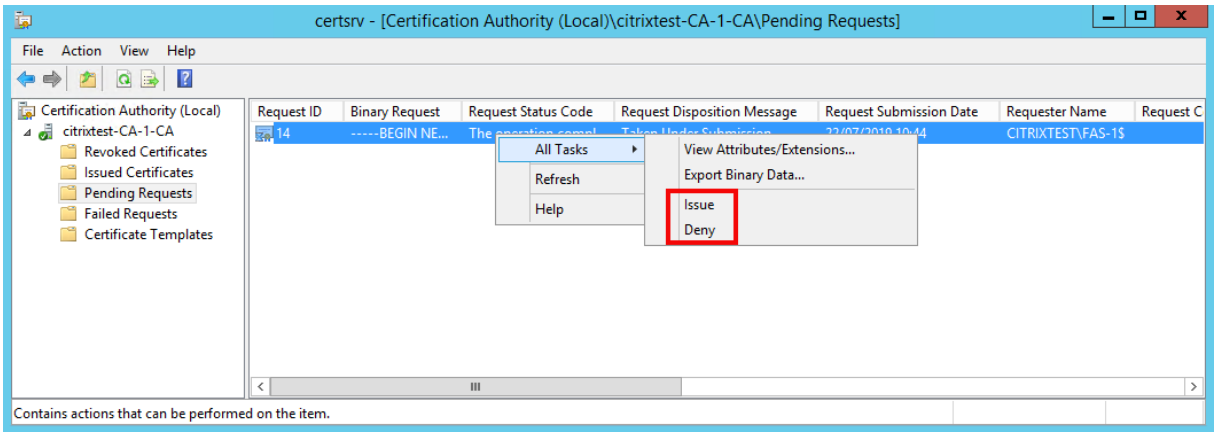
この手順により、FAS の認証が開始されます。管理コンソールは、Citrix_RegistrationAuthority_ManualAuthorization テンプレートを使用して証明書の要求生成し、この要求をテンプレートを公開する証明機関のいずれかに送信します。



要求は、送信後、FAS マシンアカウントから保留中の要求として Microsoft 証明機関コンソールの ［保留中の要求］リストに表示されます。FAS の構成を続行するには、証明機関の管理者が要求の発行または拒否を選択する必要があります。

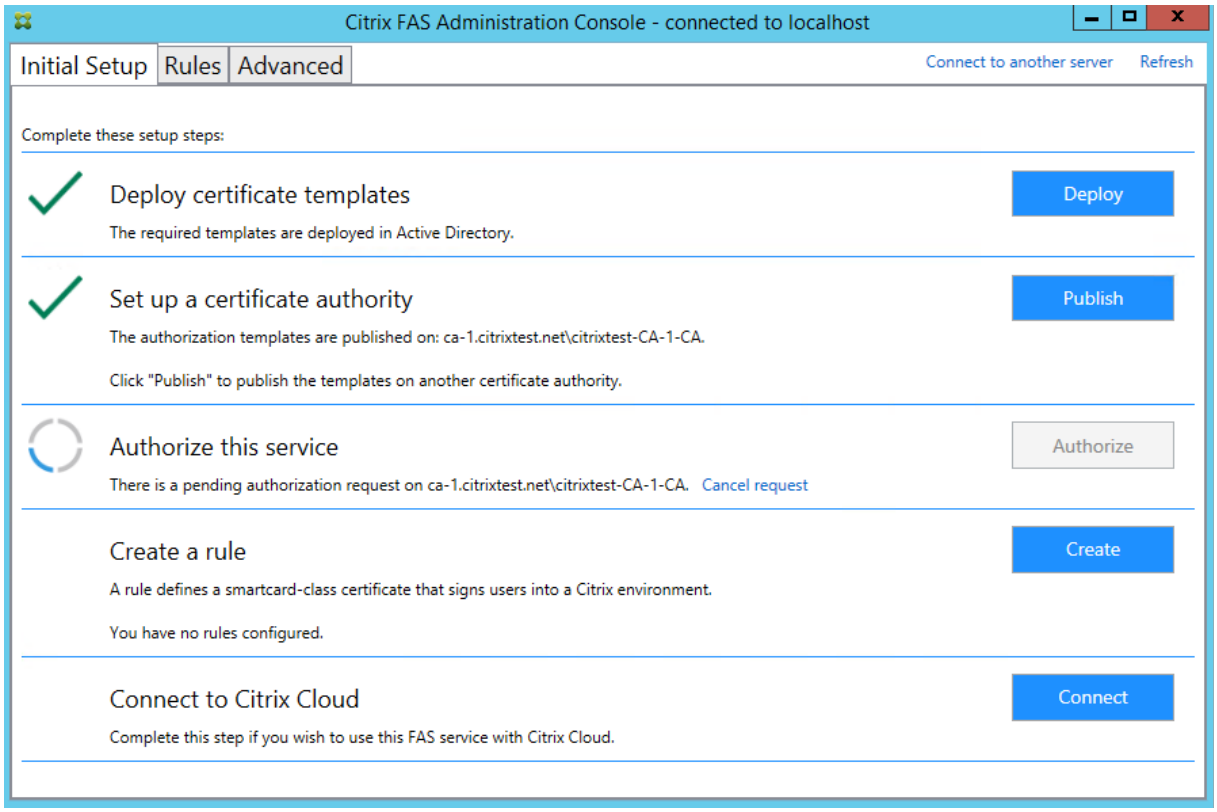
FAS 管理コンソールは、管理者が ［**Issue**］ または ［**Deny**］ を選択するまで処理中の「スピナー」アイコンを表示します。

Microsoft 証明機関コンソールで ［すべてのタスク］ を右クリックしてから、証明書要求に対して ［**Issue**］ または［**Deny**］ を選択します。［**Issue**］ を選択すると、FAS 管理コンソールが認証証明書を表示します。［**Deny**］ を選択すると、コンソールはエラーメッセージを表示します。



FAS 管理コンソールにより、このプロセスの完了が自動的に検出されます。この処理には数分かかることがありま

す。



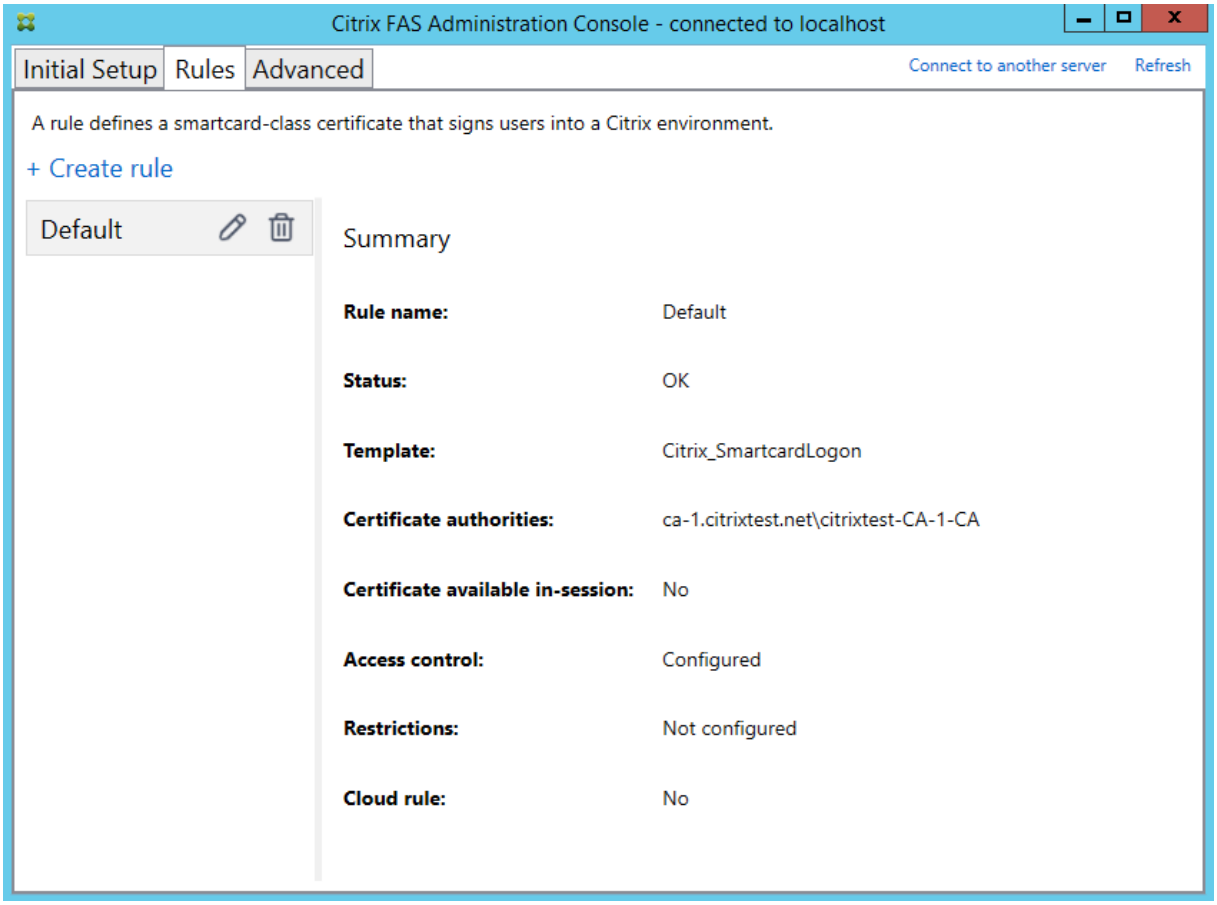
ルールの構成

FAS のルールにより、StoreFront の指示に従って、VDA ログオンおよびセッション中の使用に関する証明書発行の権限が付与されます。各ルールでは、証明書の要求を信頼する StoreFront サーバー、証明書を要求できる一連のユーザー、および証明書の使用を許可する一連の VDA マシンを指定します。

FAS では、最低 1 つのルールを作成し構成する必要があります。StoreFront は FAS にアクセスしたとき「デフォルト」という名前のルールを要求するため、「デフォルト」という名前のルールを作成することをお勧めします。

追加のカスタムルールを作成して、さまざまな証明書テンプレートおよび証明機関を参照し、各種プロパティや権限が含まれるように構成することができます。これらのルールは、さまざまな StoreFront サーバーや Workspace で使用するために構成できます。グループポリシー構成オプションを使用して、カスタムルールを名前で要求できるように StoreFront サーバーを構成します。

[**Create**]（または「Rules」タブの［**Create rule**]）をクリックしてルールを作成するための情報を収集するルール作成ウィザードを開始します。[Rules］タブは各ルールの概要を表示します。



ウィザードによって次の情報が収集されます:

テンプレート: ユーザー証明書の発行に使用される証明書テンプレート。これは Citrix_SmartcardLogon テンプレートか、その変更されたコピーである必要があります（「証明書テンプレート」を参照してください）。

証明機関: ユーザー証明書を発行する証明機関。テンプレートは証明機関によって公開される必要があります。FAS では、フェールオーバーおよび負荷分散のために、複数の証明機関の追加することができます。選択した証明機関のステータスが「Template available」であることを確認してください。「証明機関の管理」を参照してください。

セッション内使用: ［セッション内使用を許可］オプションにより、証明書を VDA へのログオン後に使用できるかどうかを制御します。

- **Allow in-session use** が選択されていない場合（デフォルトで推奨）—証明書はログオンまたは再接続にのみ使用され、認証後、ユーザーは証明書にアクセスできなくなります。
- **Allow in-session use** が選択されている場合—認証後、ユーザーは証明書にアクセスできます。通常の場合、お客様はこのオプションを選択しないでください。イントラネット Web サイトやファイル共有など、VDA セッション内からアクセスされるリソースには、Kerberos を使用したシングルサインオンでアクセスできるため、セッション内証明書は必要ありません。

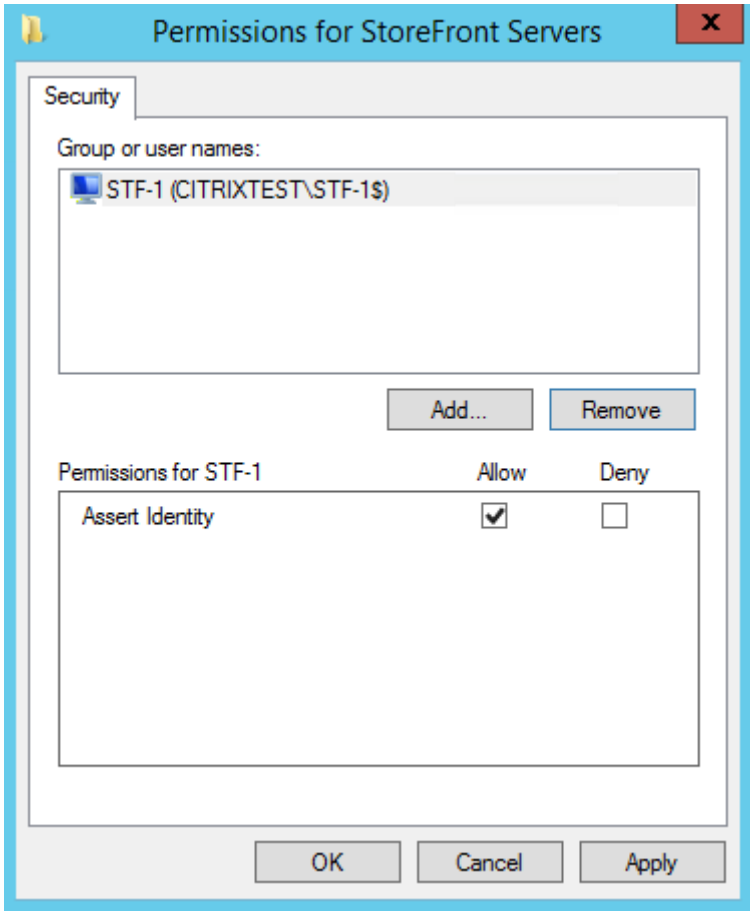
  Allow in-session use を選択した場合は、In-session Behaviorグループポリシーも有効にして VDA に適用する必要があります。これにより、ログオン後にアプリケーションが使用できるようにユーザーの個人証明

書ストアに証明書が配置されます。たとえば、VDA セッション内で Web サーバーへの TLS 認証が必要な場合、証明書は Internet Exploler によって使用されます。

アクセス制御：ユーザーのログオンまたは再接続用に証明書を要求する権限が付与された、信頼済み StoreFront サーバーの一覧。これらのすべてのアクセス許可に対して、個々の AD オブジェクトまたはグループを追加できます。

> 重要：
>
> ［アクセス制御］設定はセキュリティ上非常に重要であり、慎重に管理する必要があります。
>
> 注：
>
> FAS サーバーを Citrix Cloud でのみ使用する場合は、アクセス制御を構成する必要はありません。ただし、Citrix Cloud でルールが使用される場合、StoreFront のアクセス許可は無視されます。Citrix Cloud とオンプレミスの StoreFront 環境で、同じルールを使用できます。StoreFront のアクセス許可は、ルールがオンプレミスの StoreFront で使用される場合には適用されます。

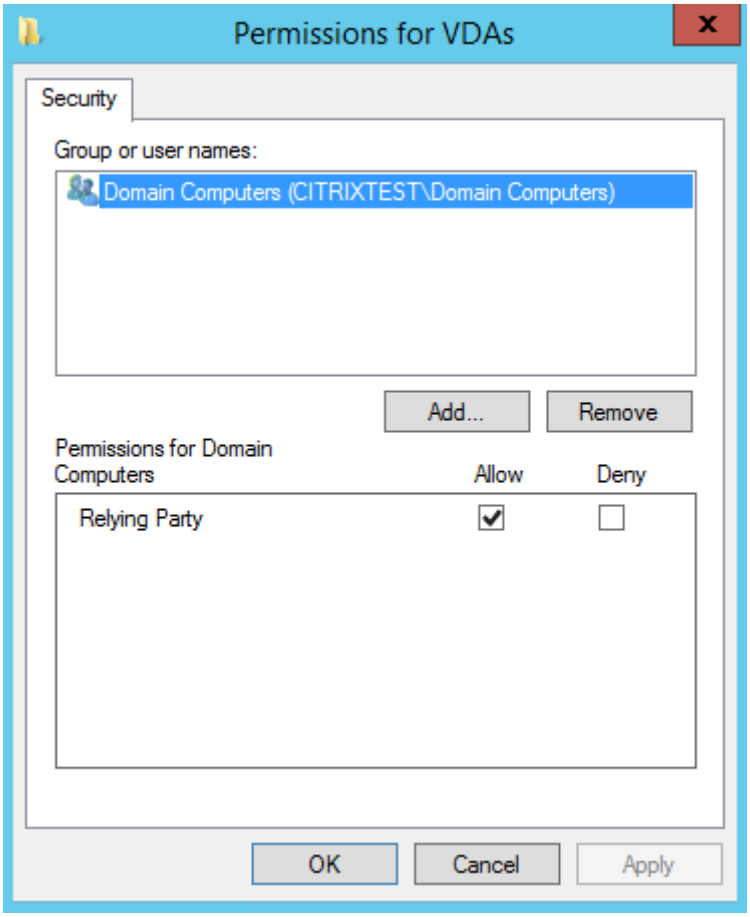
デフォルトのアクセス許可（「Assert Identity」を許可）では、すべてが拒否されます。したがって、Storefront サーバーを明示的に許可する必要があります。

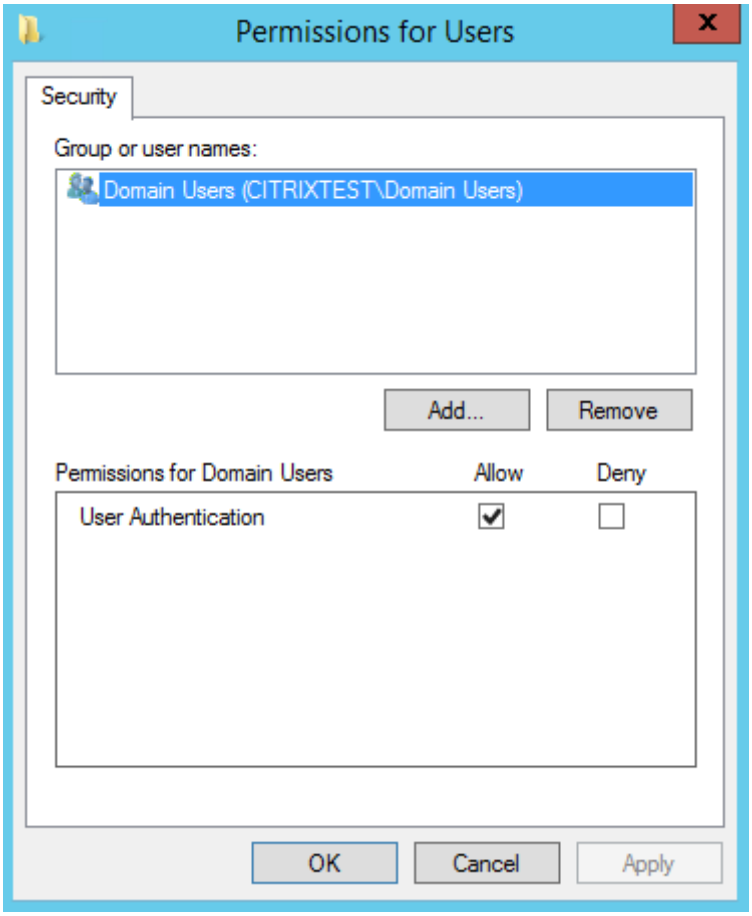


制限：ユーザーが FAS を使用してログオンできる VDA マシンのリストと、FAS を介して証明書を発行できるユーザーのリスト。

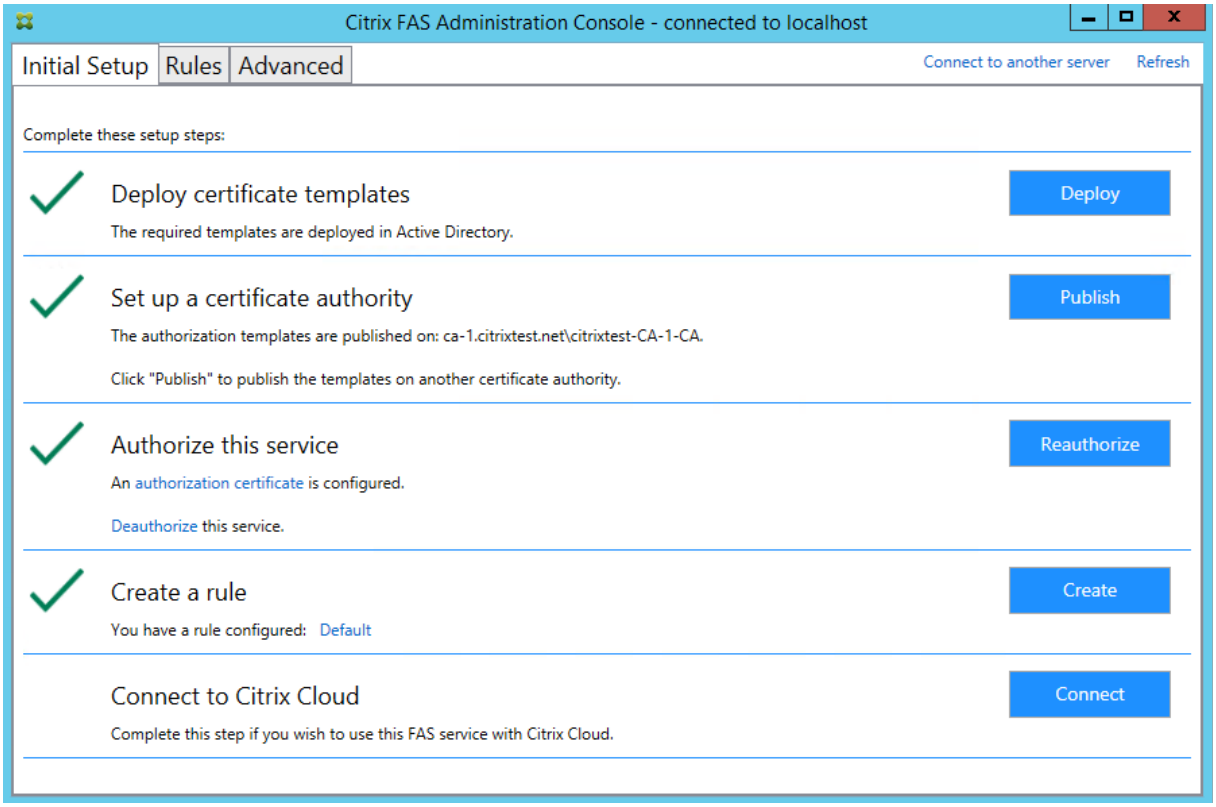
- **VDA** 権限の管理では、FAS を使用してユーザーをログオンさせる VDA を指定できます。VDA の一覧のデフォルトはドメインコンピューターになります。
- ユーザー権限の管理では、FAS を使用して VDA にサインインするユーザーを指定できます。ユーザーの一覧のデフォルトはドメインユーザーになります。

> 注:
>
> FAS サーバーが VDA およびユーザーのドメインとは異なるドメインにある場合は、デフォルトの制限を変更する必要があります。





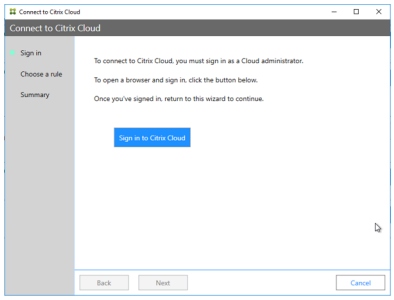
Cloud ルール：Citrix Workspace から ID アサーションを受信したときに、このルールが適用されるかを示します。Citrix Cloud に接続するときに、Citrix Cloud で使用するルールを選択します。［**Connect to Citrix Cloud**］セクションのリンクから Citrix Cloud に接続した後、ルールを変更することもできます。



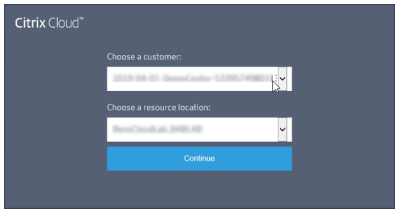
Citrix Cloud への接続

FAS サーバーを Citrix Cloud に接続して、Citrix Workspace で使用できます。このCitrix Workspace の記事を参照してください。

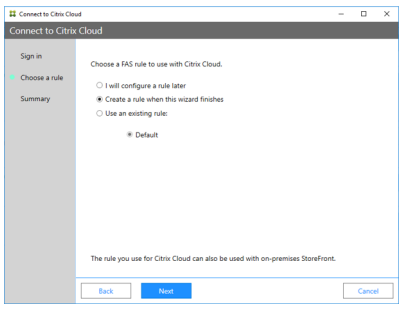
1. ［Initial Setup］タブの ［**Connect to Citrix Cloud**］で ［**Connect**］をクリックします。



2. ［**Sign in to Citrix Cloud**］をクリックし、接続先の Cloud 顧客の管理者資格情報を使用して Citrix Cloud にサインインします。



3. 必要に応じて顧客アカウントを選択して、FAS サーバーを接続するリソースの場所を選択します。[**Continue**] をクリックし、確認用のウィンドウを閉じます。



4. FAS 管理コンソールで、Citrix Workspace から ID アサーションを受信したときに適用するルールを選択するか、このウィザードの終了時に ［**Create a rule**］を選択します（[Rules］タブで、選択または作成したルールの Cloud rule の値は「Yes」です）。
5. [Summary］タブで ［**Finish**］をクリックして Citrix Cloud 接続を完了します。

Citrix Cloud で FAS サーバーが登録され、Citrix Cloud アカウントの［リソースの場所］ページに表示されます。

Citrix Cloud からの切断

このCitrix Workspace の記事の説明に従って Citrix Cloud のリソースの場所から FAS サーバーを削除した後、[**Connect to Citrix Cloud**］で ［**Disable**］を選択します。

詳細な構成

September 28, 2021

このセクションの記事では、フェデレーション認証サービス（FAS）の高度な構成および管理について説明します。

関連情報

- FAS のインストールと初期セットアップについては、「インストールと構成」を参照してください。
- 「展開アーキテクチャ」では、FAS の主要アーキテクチャの概要を説明し、より複雑なアーキテクチャに関するそのほかの記事へのリンクを掲載しています。

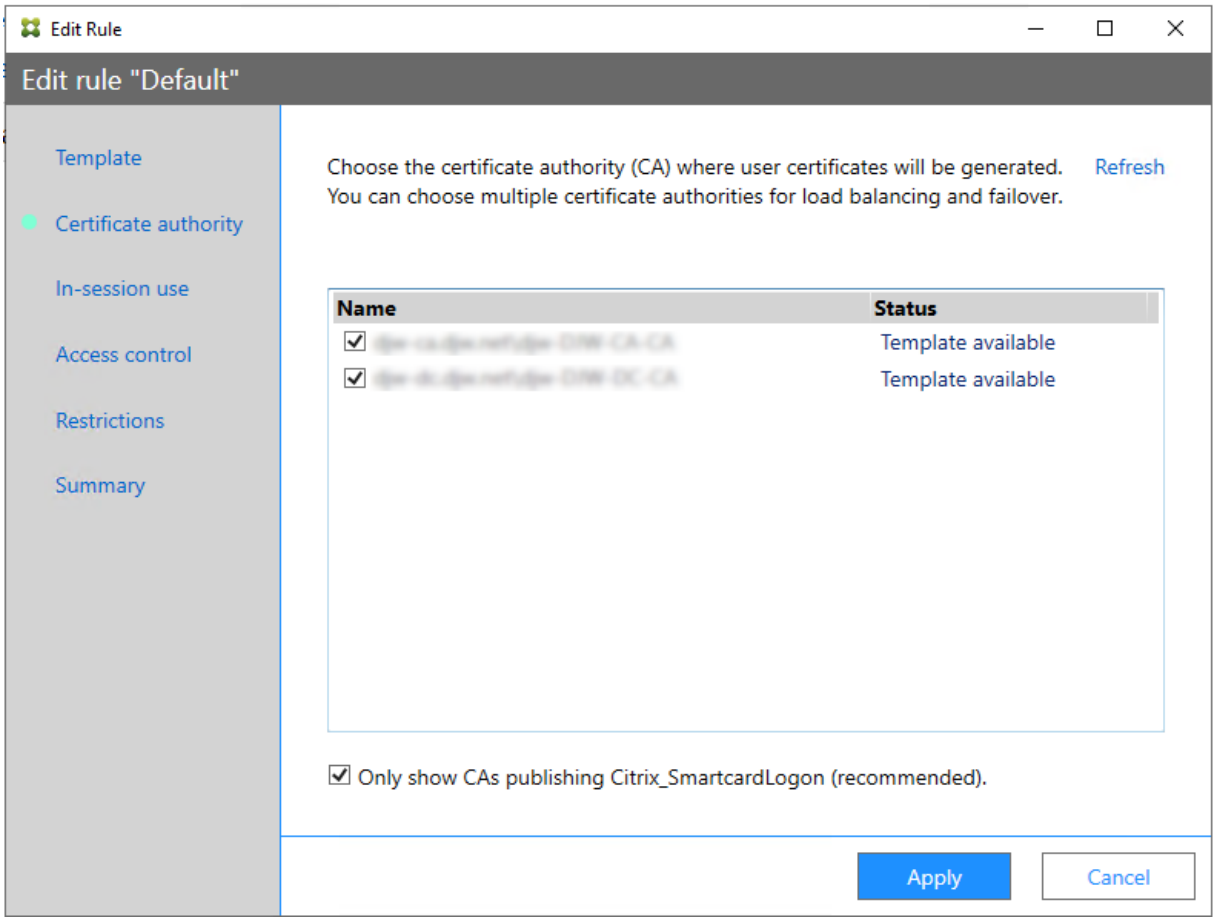
証明機関の設定

November 9, 2021

この記事では、フェデレーション認証サービス（FAS）を証明機関（CA）サーバーと統合するための詳細設定について説明します。これらの設定の大半は FAS 管理コンソールでサポートされていません。この説明では、FAS が提供する PowerShell API を使用します。この記事に記載されている説明を実行する前に、PowerShell の基礎知識を確認してください。

FAS で使用するための複数 CA サーバーのセットアップ

FAS 管理コンソールを使用して、複数の証明機関で FAS を構成し、ルールを作成または編集できます:



選択したすべての CA が Citrix_SmartcardLogon 証明書テンプレート（またはルールで選択したテンプレート）を公開する必要があります。

使用するいずれかの CA が必要なテンプレートを公開していない場合、CA の証明機関をセットアップする手順を実行します。

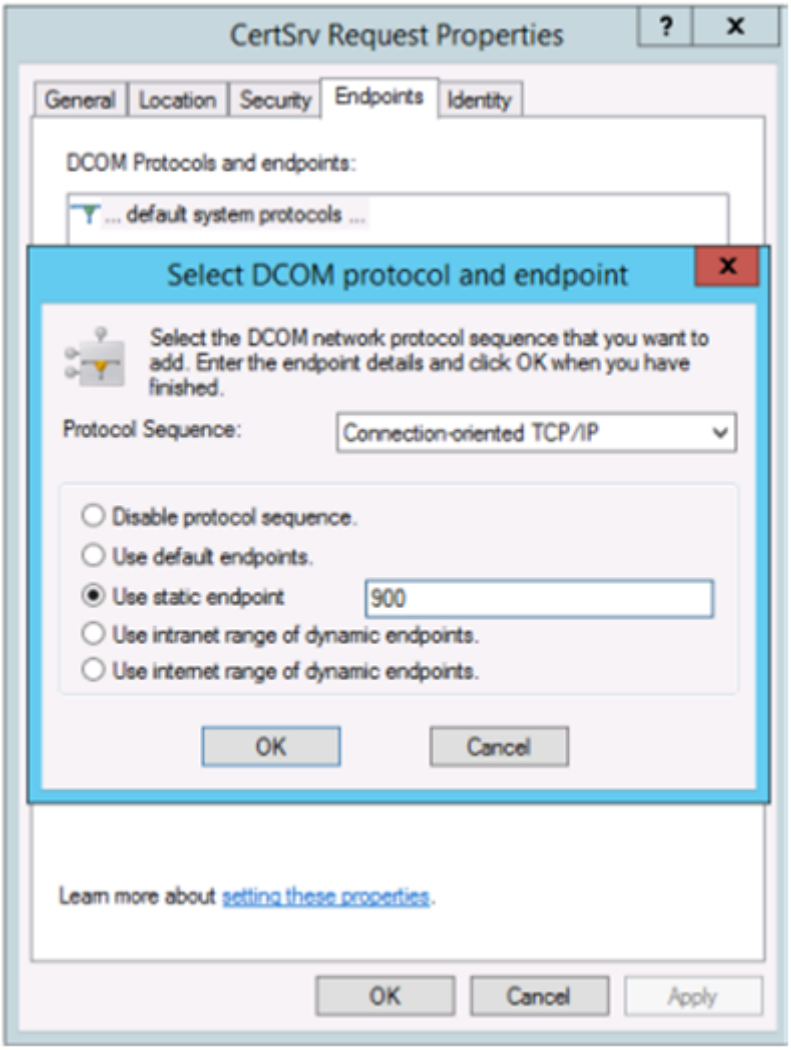
> 注:
>
> この手順で構成された認証証明書はどの CA でも使用できるため、すべての CA でこのサービスを認証する手順を実行する必要はありません。

想定される動作の変更

FAS サーバーを複数の CA サーバーで構成した後は、ユーザー証明書の生成は構成済みのすべての CA サーバー間で配信されます。さらに、構成済みの CA サーバーのうちいずれかでエラーが発生すると、FAS サーバーは別の使用可能な CA サーバーに切り替えます。

Microsoft 証明機関を **TCP** アクセス用に構成する

デフォルトでは、Microsoft 証明機関はアクセスに DCOM を使用します。この場合、ファイアウォールの実装が複雑になるため、静的 TCP ポートに切り替えることができます。Microsoft 証明機関で DCOM 構成パネルを開き、「CertSrv 要求」DCOM アプリケーションのプロパティを編集します:



[エンドポイント] を変更して静的エンドポイントを選択し、TCP ポート番号を指定します (上の図では 900 です)。

Microsoft 証明機関を再起動して、証明書要求を送信します。「`netstat -a -n -b`」を実行する場合は、certsvr がポート 900 をリスンしていることを確認する必要があります:


```
 TCP    0.0.0.0:636            dc:0                   LISTENING
[lsass.exe]
 TCP    0.0.0.0:900            dc:0                   LISTENING
[certsrv.exe]
 TCP    0.0.0.0:3268           dc:0                   LISTENING
[lsass.exe]
 TCP    0.0.0.0:3269           dc:0                   LISTENING
```

DCOM には RPC ポートを使用するネゴシエーションステージがあるため、FAS サーバー（または証明機関を使用するその他のマシン）を構成する必要はありません。クライアントが DCOM を使用する必要がある場合、クライアントは証明書サーバーの DCOM RPC Service に接続して特定の DCOM サーバーへのアクセスを要求します。これによってポート 900 が開かれ、DCOM サーバーは FAS サーバーに接続方法を指示します。

ユーザー証明書の事前生成

ユーザー証明書が FAS サーバー内で事前生成されると、ユーザーのログオンにかかる時間が大幅に短縮されます。次のセクションでは、単一または複数の FAS サーバーでユーザー証明書を事前生成する方法について説明します。

Active Directory ユーザーの一覧を取得します

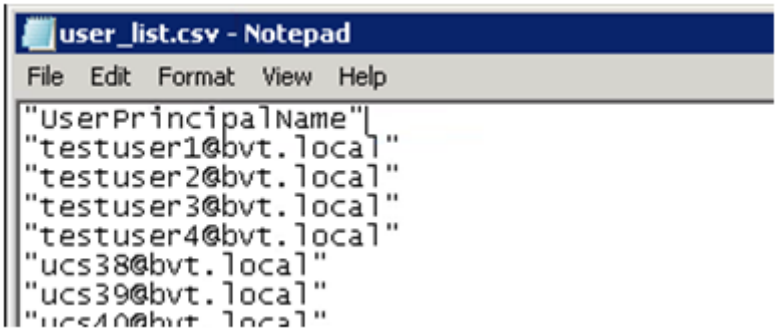
AD に対してクエリを実行し、ユーザーの一覧を次の例のようにファイル（.csv ファイルなど）に保存することにより、証明書の生成を改善することができます。

```
Import-Module ActiveDirectory

$searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for Users, leave it blank to search all
$filename = "user_list.csv" # Filename to save

if ($searchbase -ne ""){

    Get-ADUser -Filter {
 (UserPrincipalName -ne "null") -and (Enabled -eq "true") }
  -SearchBase $searchbase -Properties UserPrincipalName | Select UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -delimiter "," $filename
 }
  else {

    Get-ADUser -Filter {
 (UserPrincipalName -ne "null") -and (Enabled -eq "true") }
  -Properties UserPrincipalName | Select UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -delimiter "," $filename
 }
```

Get-ADUser は、ユーザーの一覧を要求するための標準コマンドレットです。上述の例には、UserPrincipalName を持ちステータスが「有効」のユーザーのみを一覧表示するフィルター引数が含まれています。

SearchBase 引数によって、AD のユーザー検索が制限されます。すべてのユーザーを AD に含めたい場合、これを省略できます。注：このクエリによって、多数のユーザーが返される可能性があります。

CSV の外観は、次のようになります。



FAS サーバー

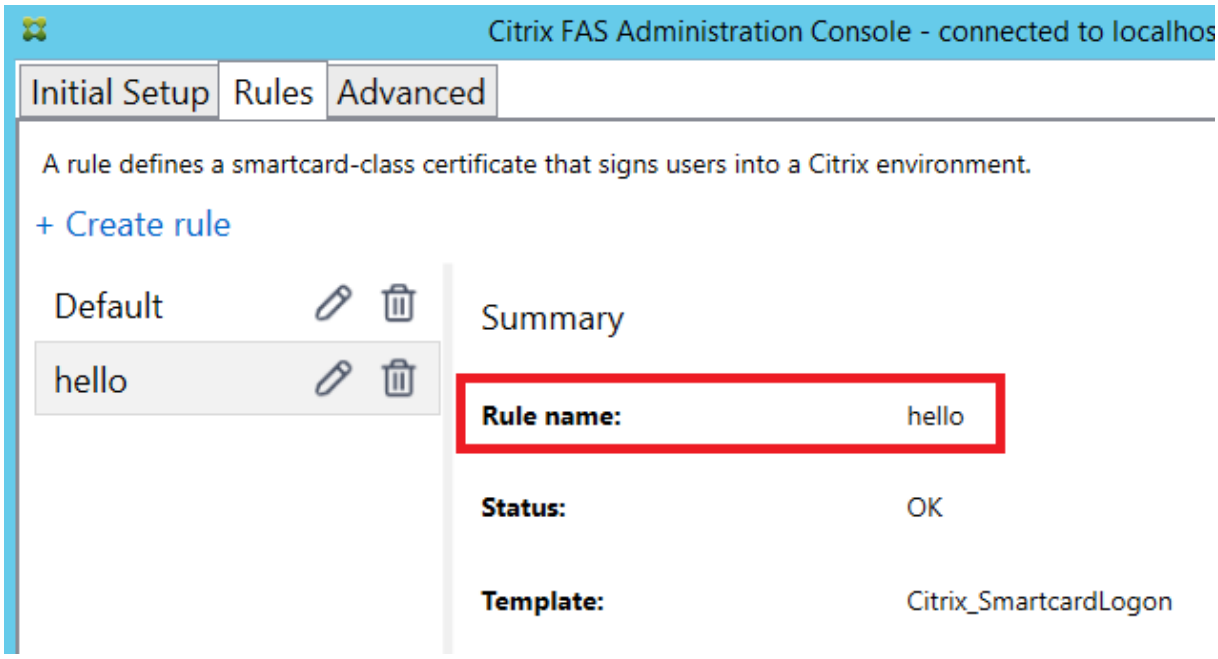
以下の PowerShell スクリプトでは、以前生成されたユーザーの一覧を使用してユーザー証明書の一覧が作成されます。

```
Add-PSSnapin Citrix.A*
$csv = "user_list.csv"
$rule = "default" # rule/role in your admin console
$users = Import-Csv -encoding utf8 $csv
foreach ( $user in $users )
{

    $server = Get-FasServerForUser -UserPrincipalNames $user.
       UserPrincipalName
    if( $server.Server -ne $NULL) {

        New-FasUserCertificate -Address $server.Server -
           UserPrincipalName $user.UserPrincipalName -
           CertificateDefinition $rule"_Definition" -Rule $rule
     }

    if( $server.Failover -ne $NULL) {

        New-FasUserCertificate -Address $server.Failover -
           UserPrincipalName $user.UserPrincipalName -
           CertificateDefinition $rule"_Definition" -Rule $rule
     }

 }
```

複数の FAS サーバーが存在する場合は、特定のユーザーの証明書がメインサーバーで 1 回、フェールオーバーサーバーで 1 回の合計 2 回生成されます。

上述のスクリプトは、「default」という名前の規則の場合のものです。規則名が異なる場合（「hello」など）は、ス

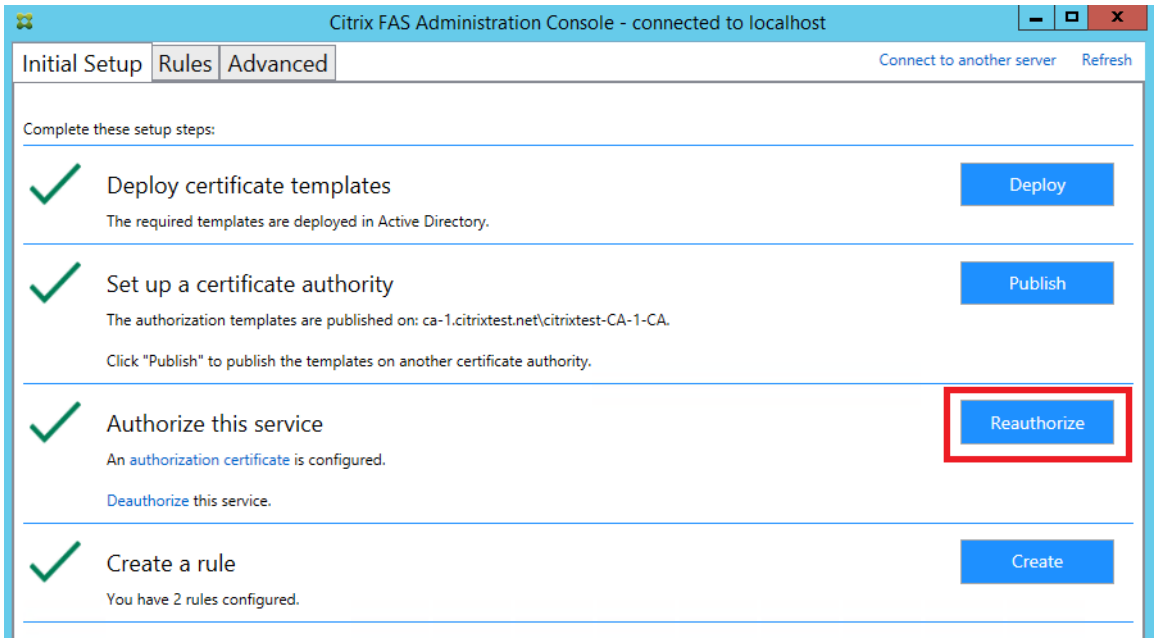
クリプトの $rule 変数を変更してください。



登録機関証明書を更新します

複数の FAS サーバーを使用中の場合は、ログオン中のユーザーに影響することなく FAS 認証証明書を更新できます。

> 注:
>
> GUI を使用して FAS を再認証することもできます:



以下の手順を実行します。

1. 新しい認証証明書を作成します。`New-FasAuthorizationCertificate`
2. 次のコマンドによって返される新しい認証証明書の GUID をメモします:`Get-FasAuthorizationCertificate`
3. FAS サーバーをメンテナンスモードにします: `Set-FasServer -Address <FAS server> -MaintenanceMode $true`
4. 新しい認証証明書を置換します。`Set-FasCertificateDefinition -AuthorizationCertificate <GUID>`
5. FAS サーバーのメンテナンスモードを解除します。`Set-FasServer -Address <FAS server> -MaintenanceMode $false`
6. 古い認証証明書を削除します。`Remove-FasAuthorizationCertificate`

関連情報

- FAS のインストールと構成については、「インストールと構成」の記事を参照してください。
- 一般的な FAS 環境については、「展開アーキテクチャ」を参照してください。
- その他の具体的な手順については、「詳細な構成」を参照してください。

秘密キー保護

November 9, 2021

はじめに

秘密キーは Network Service アカウントを使用して保存され、デフォルトでエクスポート不可としてマークされます。

秘密キーには 2 つの種類があります。

- 登録機関証明書に関連付けられている、Citrix_RegistrationAuthority 証明書テンプレートからの秘密キー
- ユーザー証明書に関連付けられている、Citrix_SmartcardLogon 証明書テンプレートからの秘密キー

登録機関証明書には Citrix_RegistrationAuthority_ManualAuthorization（デフォルトで 24 時間有効）および Citrix_RegistrationAuthority（デフォルトで 2 年間有効）の 2 つの種類があります。

フェデレーション認証サービス（FAS）管理コンソールの ［初回セットアップ］ タブの手順 3 で、管理者が ［許可する］ をクリックすると、FAS サーバーによってキーペアが生成され、証明書署名要求が Citrix_RegistrationAuthority_ManualAuthorization 証明書の証明機関に送信されます。これは一時的な証明書であり、デフォルトで 24 時間有効です。証明機関は自動的に証明書を発行しません。証明書を発行するには、管理者による証明機関での手動の権限許可が必要です。証明書が FAS サーバーに発行されると、FAS は Citrix_RegistrationAuthority_ManualAuthorization 証明書を使用して Citrix_RegistrationAuthority 証明書（デフォルトで 2 年間有効）を自動的に取得します。FAS サーバーは、Citrix_RegistrationAuthority 証明書を取得するとすぐに、Citrix_RegistrationAuthority_ManualAuthorization の証明書とキーを削除します。

登録機関証明書ポリシーは秘密キーを所有するものすべてに対して、テンプレートで構成されたユーザーセットに対する証明書要求の発行を許可するため、登録機関証明書に関連付けられた秘密キーは特に機密です。結果として、このキーを管理するものはだれでも、セット内のユーザーと同様、環境に接続できます。

次のいずれかを使用して、組織のセキュリティ要件に準拠して秘密キーが保護されるように FAS サーバーを構成できます：

- Microsoft Enhanced RSA、AES Cryptographic Provider、または Microsoft ソフトウェアキー記憶域プロバイダー（登録機関証明書およびユーザー証明書両方の秘密キー用）
- トラステッドプラットフォームモジュール（TPM）チップを使用した Microsoft プラットフォームキー記憶域プロバイダー（登録機関証明書の秘密キー用）、および Microsoft Enhanced RSA、AES Cryptographic Provider、または Microsoft ソフトウェアキー記憶域プロバイダー（ユーザー証明書の秘密キー用）
- ハードウェアセキュリティモジュール（HSM）ベンダーの HSM デバイスを使用した暗号サービスまたはキー記憶域プロバイダー（登録機関証明書およびユーザー証明書両方の秘密キー用）

秘密キーの構成設定

3 つのオプションのうちいずれかを使用して FAS を構成します。テキストエディターを使用して、Citrix.Authentication.FederatedAuthenticationService.exe.config ファイルを編集します。ファイルのデフォルトの場所は FAS サーバーの Program Files\Citrix\Federated Authentication Service フォルダーです。


```xml
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

FAS は、サービスの起動時にのみ構成ファイルを読み込みます。いずれかの値が変更された場合、新しい設定を反映させるために FAS を再起動する必要があります。

Citrix.Authentication.FederatedAuthenticationService.exe.config ファイルの関連する値を次のとおり設定します:

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp**（CAPI と CNG API の切り替え）

値	コメント
true	CAPI API を使用
false（デフォルト）	CNG API を使用

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName**（使用するプロバイダーの名前）

値	コメント
Microsoft Enhanced RSA および AES Cryptographic Provider	デフォルトは CAPI プロバイダーです
Microsoft ソフトウェアキー記憶域プロバイダー	デフォルトは CNG プロバイダーです
Microsoft プラットフォームキー記憶域プロバイダー	デフォルトは TPM プロバイダーです。TPM はユーザーキーにはお勧めしません。TPM は登録機関キーにのみ使用します。FAS サーバーを仮想化環境で実行する予定の場合は、TPM およびハイパーバイザーのベンダーに仮想化がサポートされているかどうかを確認してください。

値	コメント
HSM_Vendor CSP/Key 記憶域プロバイダー	HSM ベンダーによって提供されます。値はベンダーによって異なります。FAS サーバーを仮想化環境で実行する予定の場合は、HSM ベンダーに仮想化がサポートされているかどうかを確認してください。

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType**（CAPI API の場合のみ必要）

値	コメント
24	Default。Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24 を参照します。CAPI で HSM を使用する場合、および HSM ベンダーで別のタイプを指定されている場合以外は、常に 24 である必要があります。

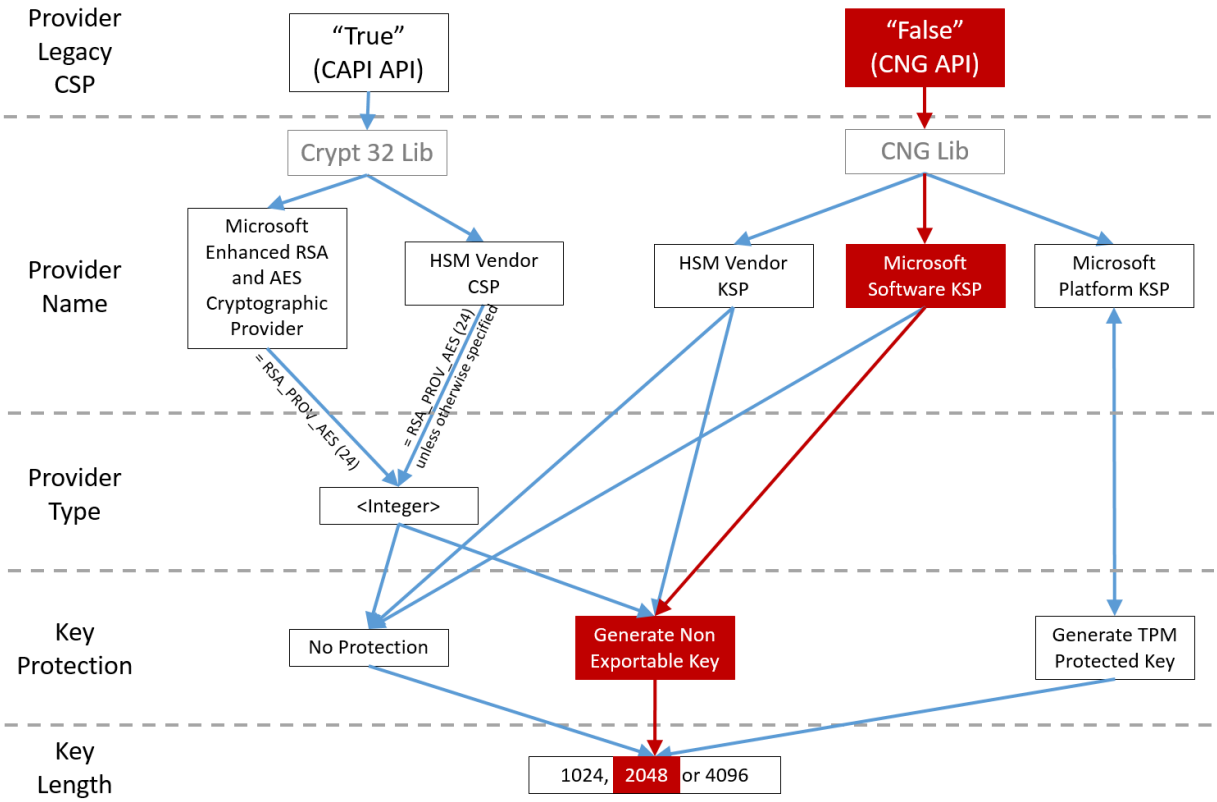
Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection**（FAS が秘密キー操作を実行する必要がある場合は、ここで使用されている値を使用します）。秘密キーの「エクスポート可能」フラグを制御します。ハードウェアでサポートされている場合は、TPM キーストレージの使用が許可されます。

値	コメント
NoProtection	秘密キーをエクスポートできます。
GenerateNonExportableKey	Default。秘密キーをエクスポートできません。
GenerateTPMProtectedKey	秘密キーは TPM を使用して管理されます。秘密キーは ProviderName で指定した ProviderName（例: Microsoft プラットフォームキー記憶域プロバイダー）を介して格納されます

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength**（秘密キーのサイズをビット単位で指定）

値	コメント
2048	デフォルト値です。1024 または 4096 を使用することもできます。

構成ファイルの設定を以下に図解します（インストール時のデフォルト設定は赤で示しています）。



構成シナリオの例

例 **1**

この例では、Microsoft ソフトウェアキー記憶域プロバイダーを使用して格納されている登録機関証明書の秘密キーおよびユーザー証明書の秘密キーについて説明します。

これはデフォルトのインストール後の構成です。追加の秘密キー構成は不要です。

例 **2**

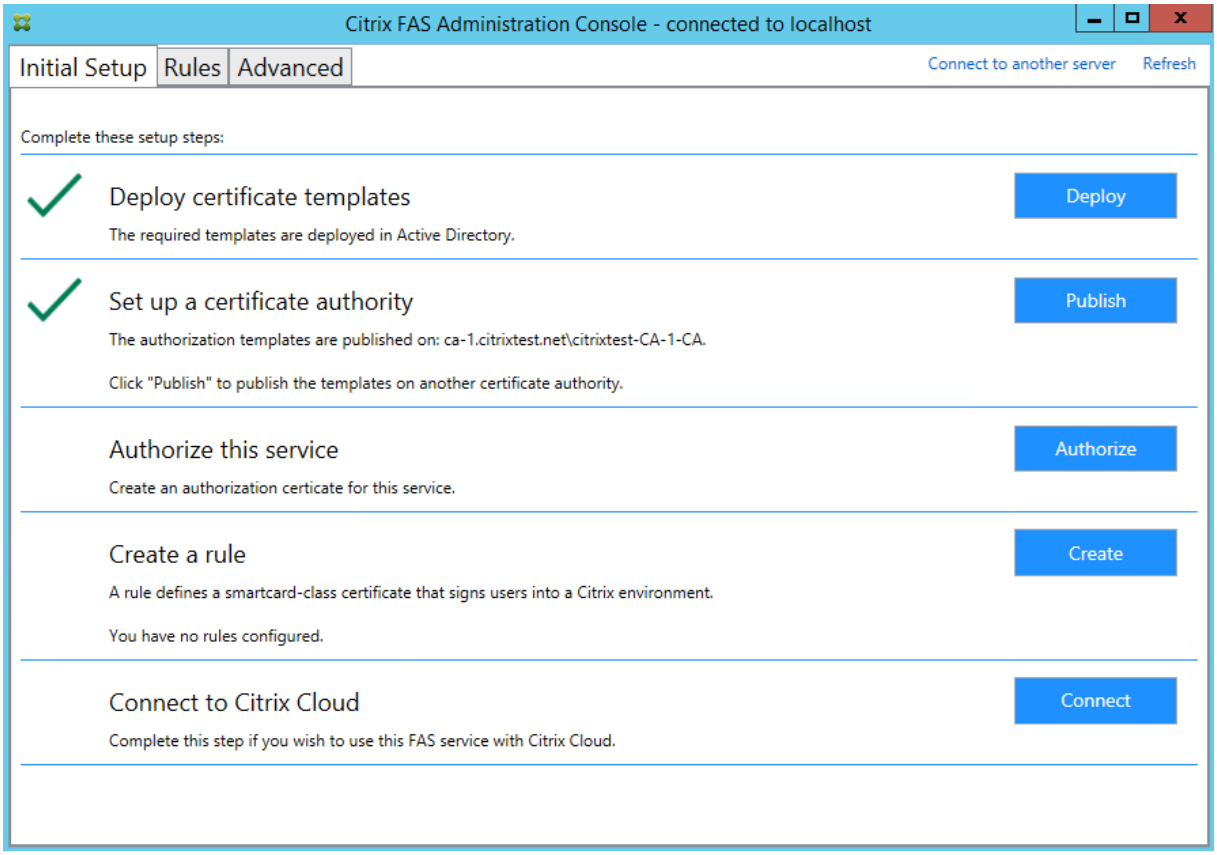
この例は、Microsoft プラットフォームキー記憶域プロバイダーを使用して FAS サーバーのマザーボードのハードウェア TPM に格納されている登録機関証明書秘密キー、および Microsoft ソフトウェアキー記憶域プロバイダーを使用して格納されているユーザー証明書秘密キーを示しています。

このシナリオでは、FAS サーバーのマザーボード上の TPM は TPM の製造元のドキュメントに基づいて BIOS で有効化され、その後 Windows で初期化されているものとみなしています。詳しくは、https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc749022(v=ws.10)を参照してください。

PowerShell の使用（推奨）　PowerShell を使用して、登録機関証明書をオフラインで要求できます。これは、証明機関がオンラインの証明書署名要求で登録機関証明書を発行しないようにする組織にお勧めです。FAS 管理コンソ

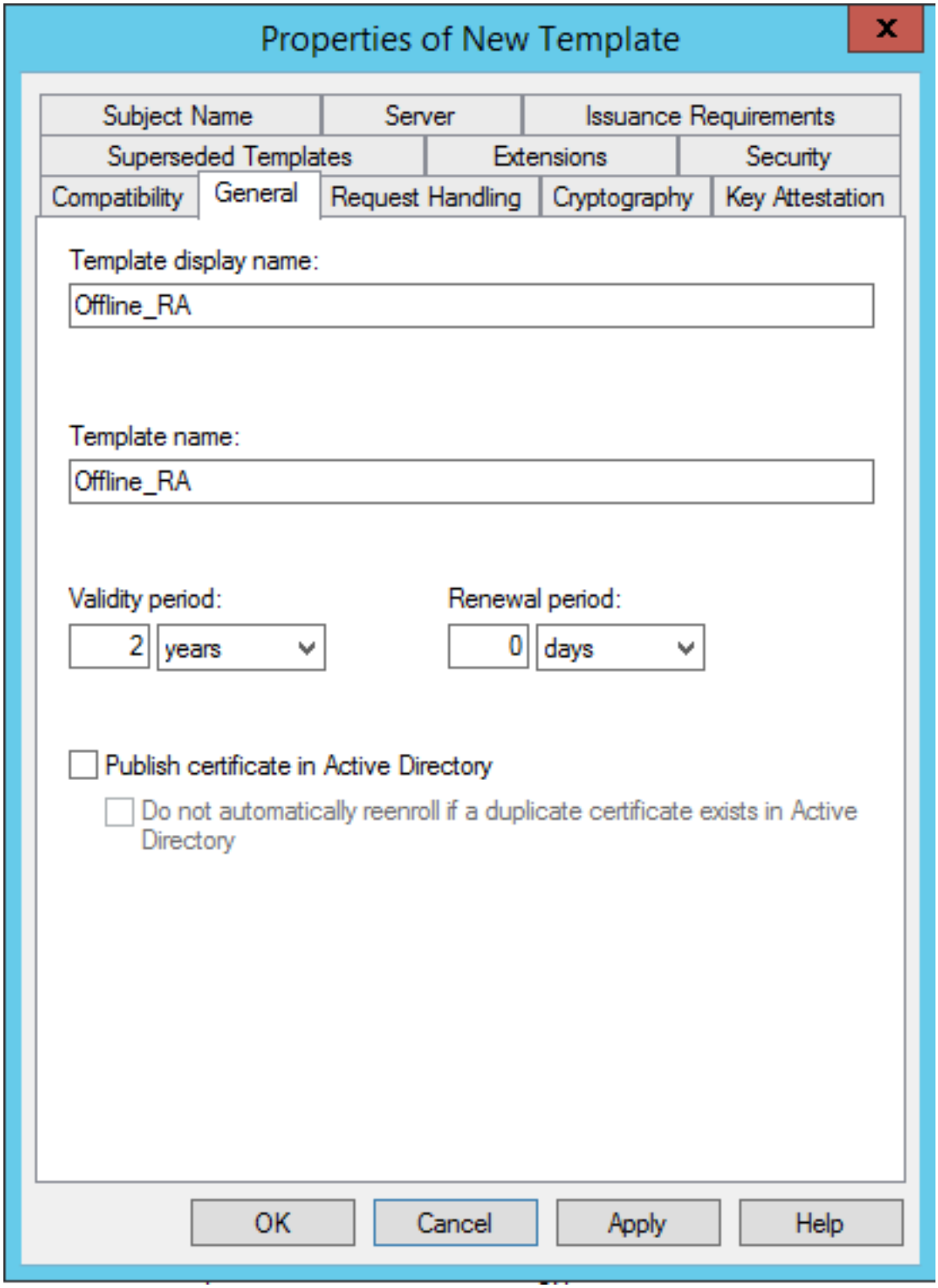
ールを使用してオフラインで登録機関証明書の署名要求を行うことはできません。

手順 **1**：管理コンソールを使用した初回 FAS 構成時には、最初の「証明書テンプレートの展開」および「証明機関のセットアップ」の 2 つの手順だけを完了します。



手順 **2**：証明機関サーバーで、証明書テンプレート MMC スナップインを追加します。**Citrix_RegistrationAuthority_ManualAu**
テンプレートを右クリックし、［テンプレートの複製］を選択します。

［一般］タブを選択します。テンプレート名と有効期間を変更します。この例では、テンプレート名は *Offline_RA*、有効期間は 2 年間です。



手順 **3**: 証明機関サーバーで、証明機関 MMC スナップインを追加します。3. ［証明書テンプレート］を右クリックします。［新規作成］を選択し、［発行する証明書テンプレート］をクリックします。作成したばかりのテンプレートを選択します。

手順 **4**: FAS サーバーで次の PowerShell コマンドレットを読み込みます。


```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

手順 **5**： RSA キーペアを FAS サーバーの TPM 内で生成し、FAS サーバーで次の PowerShell コマンドレットを入力して証明書署名要求を作成します。注：一部の TPM ではキーの長さが制限されます。デフォルトのキーの長さは、2048 ビットです。ハードウェアでサポートされているキーの長さを指定してください。

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address \<FQDN of
    FAS Server>
```

次に例を示します：

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address fashsm.
   auth.net
```

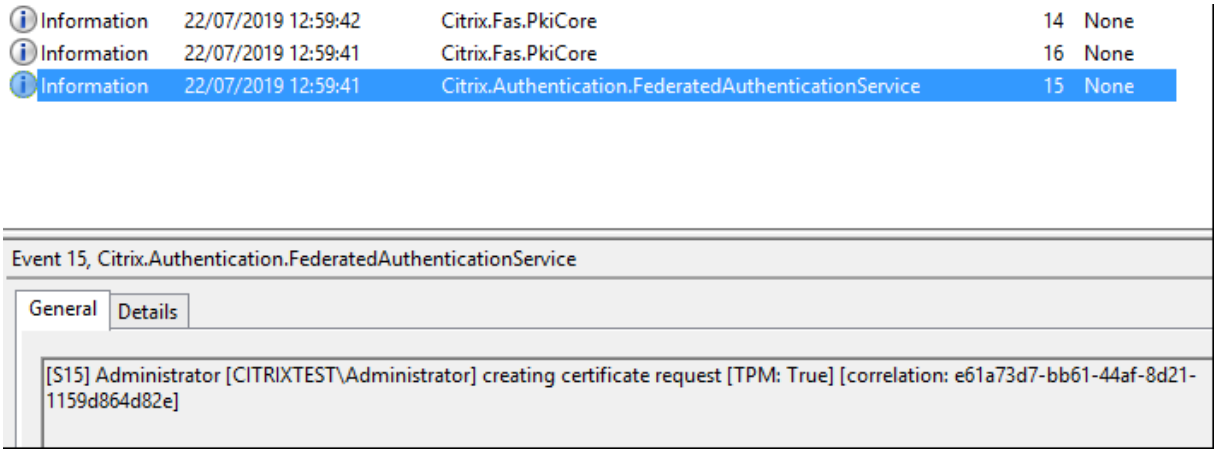
以下が表示されます。

```
PS C:\Users\Administrator.AUTH> New-UcsAuthorizationCertificateRequest -UseTPM $true -address ucshsm.auth.local


Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                      hkiG9wOBAQEFAAOCAQ8AMIIBCgKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZV3wTNfROXW
                      1hCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2BwX6JNZrLi9hAflbInFPgrz+
                      vbG3YjKuKtK35JpGqYWjUEDzKiQFaob3Dkh/pwP3V7OcEYthxB8CfbaM9MHOEFbepoSYOCAfunXW
                      snwIbXD9lc/fGyN/3f94P4fbNrjEIOHc+4Oy/WsPgPRgcq9XBwRjzpGjOgOVRoJS9g22OY5PwD77
                      7f7vZvoQkRy5NXXXATJ+xxYEPLp9JuJaE1WXrTJG+XP3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9XWHlvztpjxPeJzAVOsrLpOsCfNdvYn9u+I7J8Gsr
                      4tuLjuQ+An4Y2Rw7b6pZxEICV8rqd5Gy+wtPnVZoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c
                      YlITHOtmcHFKt4Loz5O5E+tQw39MProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsgyMgdR8F
                      3SmagQjN3C8lyqT8z1iF4l32xlmQrP/4XQvr1F+TO15PM5Fxjj6PEKWopWTYZXGzSC1ufxevcO1K
                      +tTH9tQYJM6xw3+6TIcfuWOjrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TATO3XG/AB7o=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval


PS C:\Users\Administrator.AUTH>
```

> メモ：
>
> - Id GUID（この例では「5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39」）は後続の手順で必要です。
> - この PowerShell コマンドレットは、登録機関証明書の秘密キーの生成に使用される一時的な「上書き」と認識してください。
> - このコマンドレットを実行する場合、FAS が開始されるときに構成ファイルから読み込まれる値がチェックされ、使用するキーの長さが決定されます（デフォルトは 2048 です）。
> - この手動の PowerShell によって開始される登録機関証明書秘密キー操作で-UseTPM が $true に設定されているため、ファイルからの値で TPM の使用に必要な設定に一致しないものは無視されます。
> - このコマンドレットの実行によって、構成ファイルの設定が変更されることはありません。
> - FAS で開始される後続のユーザー証明書秘密キー自動操作の実行中は、FAS が開始したときにファイルから読み込まれた値が使用されます。
> - FAS サーバーがユーザー証明書を発行するときに構成ファイルで KeyProtection 値を GenerateTPM-ProtectedKey に設定して、TPM で保護されるユーザー証明書秘密キーを生成することもできます。

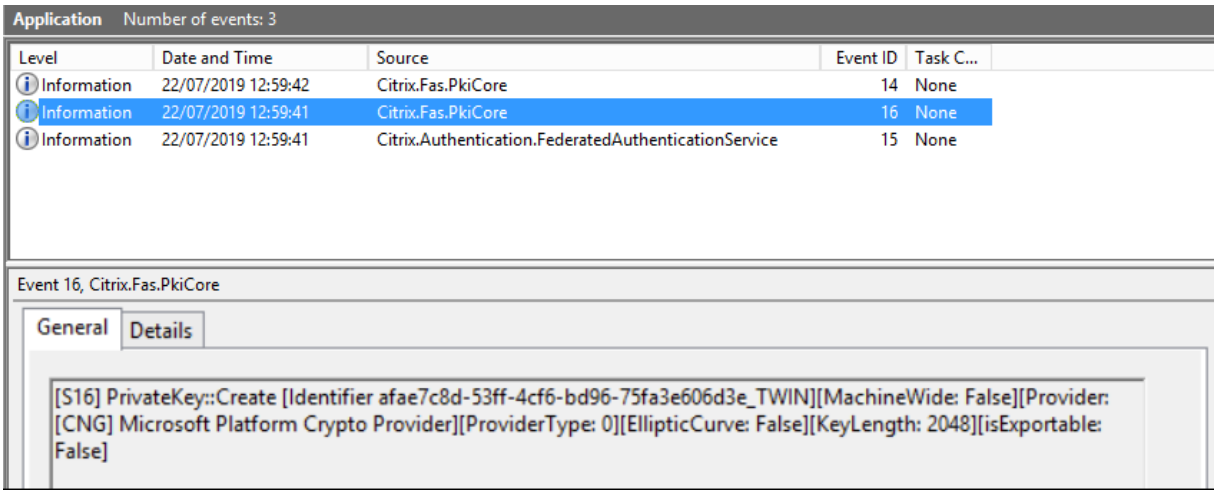
TPM がキーペアの生成に使用されたことを確認するには、FAS サーバー上でキーペアが生成された時間の Windows

イベントビューアーのアプリケーションログをチェックします。



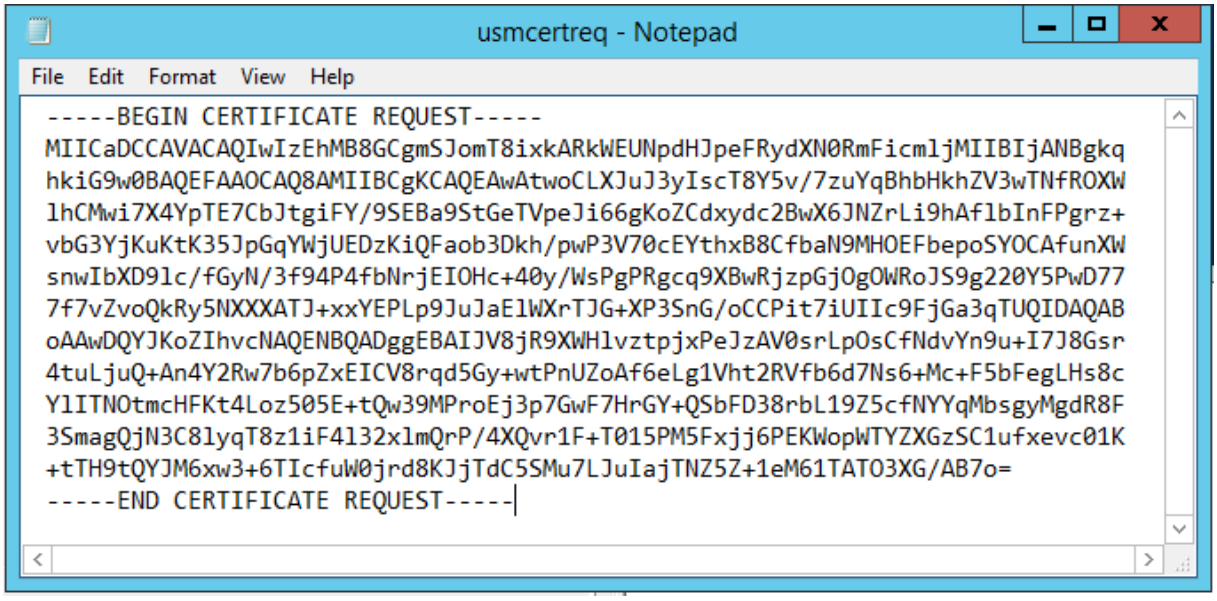
注:「[TPM: True]」となっています。

ログは以下のように続きます。



注:「Provider: CNG M[icr]osoft Platform Crypto Provider」となっています。

手順 **6**: 証明書要求セクションをテキストエディターにコピーし、テキストファイルとしてディスクに保存します。



手順 **7**: 以下のコマンドを FAS サーバーの PowerShell に入力して、証明書署名要求を証明機関に送信します:

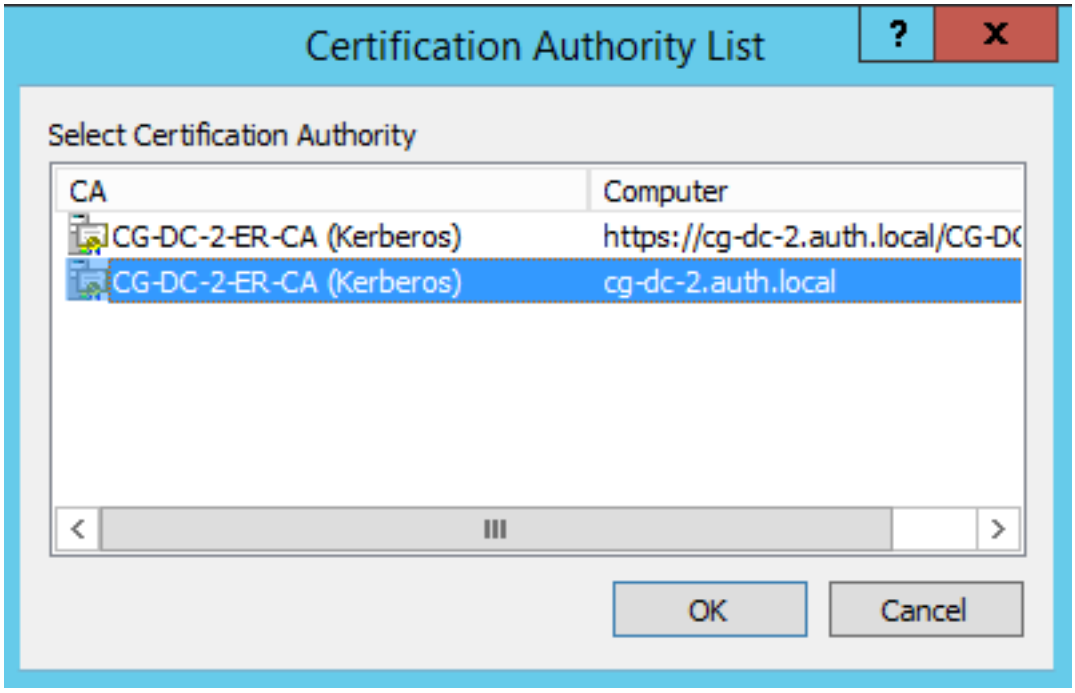
```
1  certreq -submit -attrib "certificatetemplate:\<certificate template
      from step 2>" \<certificate request file from step 6>
```

次に例を示します:

```
1  certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\
      Administrator.AUTH\Desktop\usmcertreq.txt
```

以下が表示されます。

この時点で、「証明機関の一覧」ウィンドウが表示される可能性があります。この例の証明機関では http（上部）および DCOM（下部）登録の両方が有効です。使用できる場合は DCOM オプションを選択します。

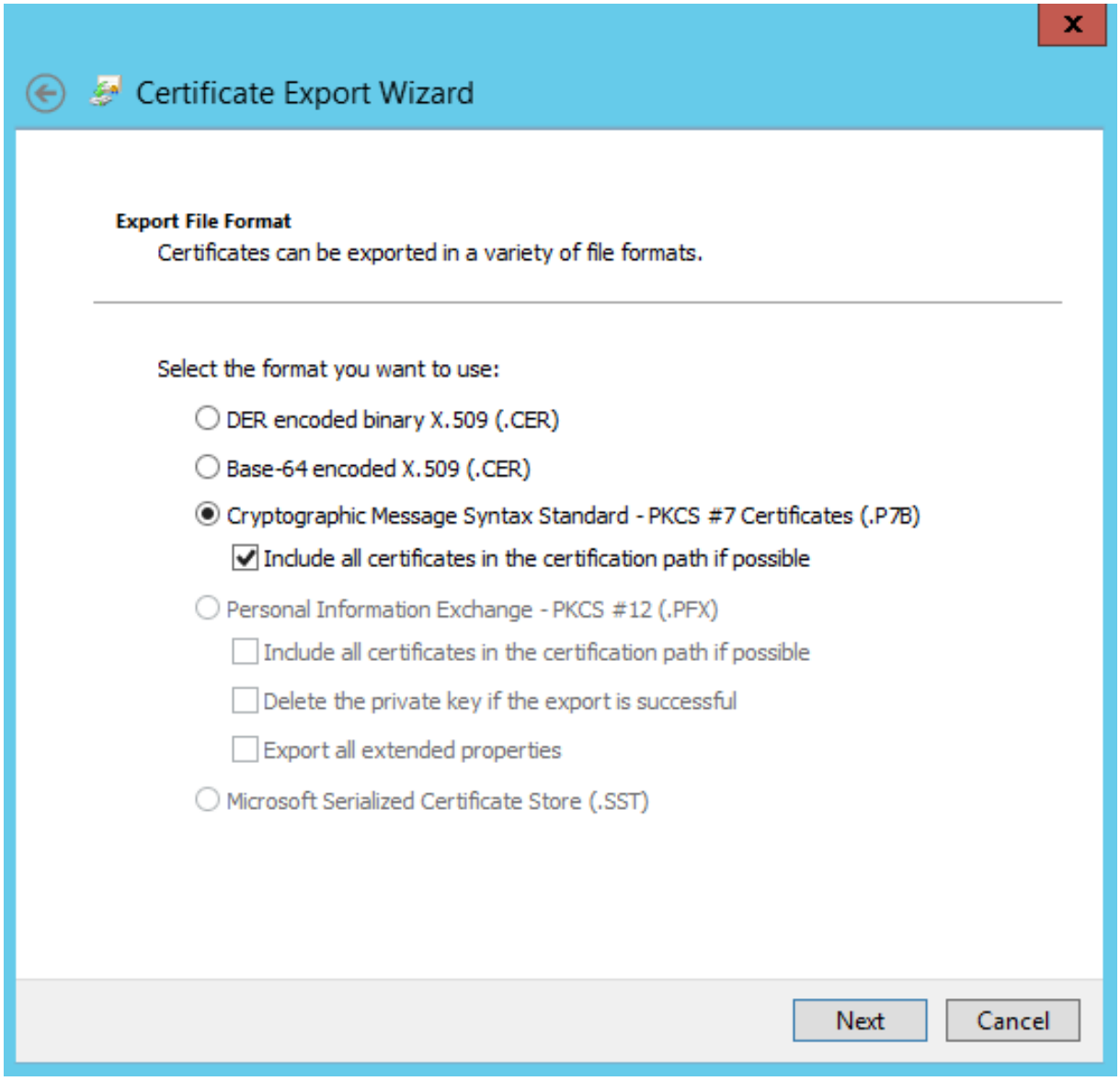


証明機関が指定されると、PowerShell によって RequestID が表示されます。

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DB0C-4D21-A4FD-2E29502177C2}
  ldap:
RequestId: 106
RequestId: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH>
```

手順 **8**：証明機関サーバーの証明機関 MMC スナップインで［**Pending Requests**］をクリックします。要求 ID を記録します。要求を右クリックし、［発行］を選択します。

手順 **9**：［発行した証明書］ノードを選択します。発行したばかりの証明書（要求 ID が一致する証明書）を見つけます。証明書をダブルクリックして開きます。［詳細］タブをクリックします。［ファイルへコピー］をクリックします。証明書のエクスポートウィザードが開きます。［次へ］をクリックします。次のファイル形式のオプションを選択します。



形式は［**Cryptographic Message Syntax Standard- PKCS #7** 証明書（**.P7B**）］を選択し、［証明のパスにある証明書を可能であればすべて含む］をオンにする必要があります。

手順 **10**：エクスポートされた証明書を FAS サーバーにコピーします。

手順 **11**： FAS サーバー上で次の PowerShell コマンドレットを入力して、登録機関証明書を FAS サーバーにインポートします：

```
Import-FasAuthorizationCertificateResponse -address <FQDN of FAS server> -Id <ID
GUID from step 5> -Pkcs7CertificateFile <Certificate file from step 10>
```

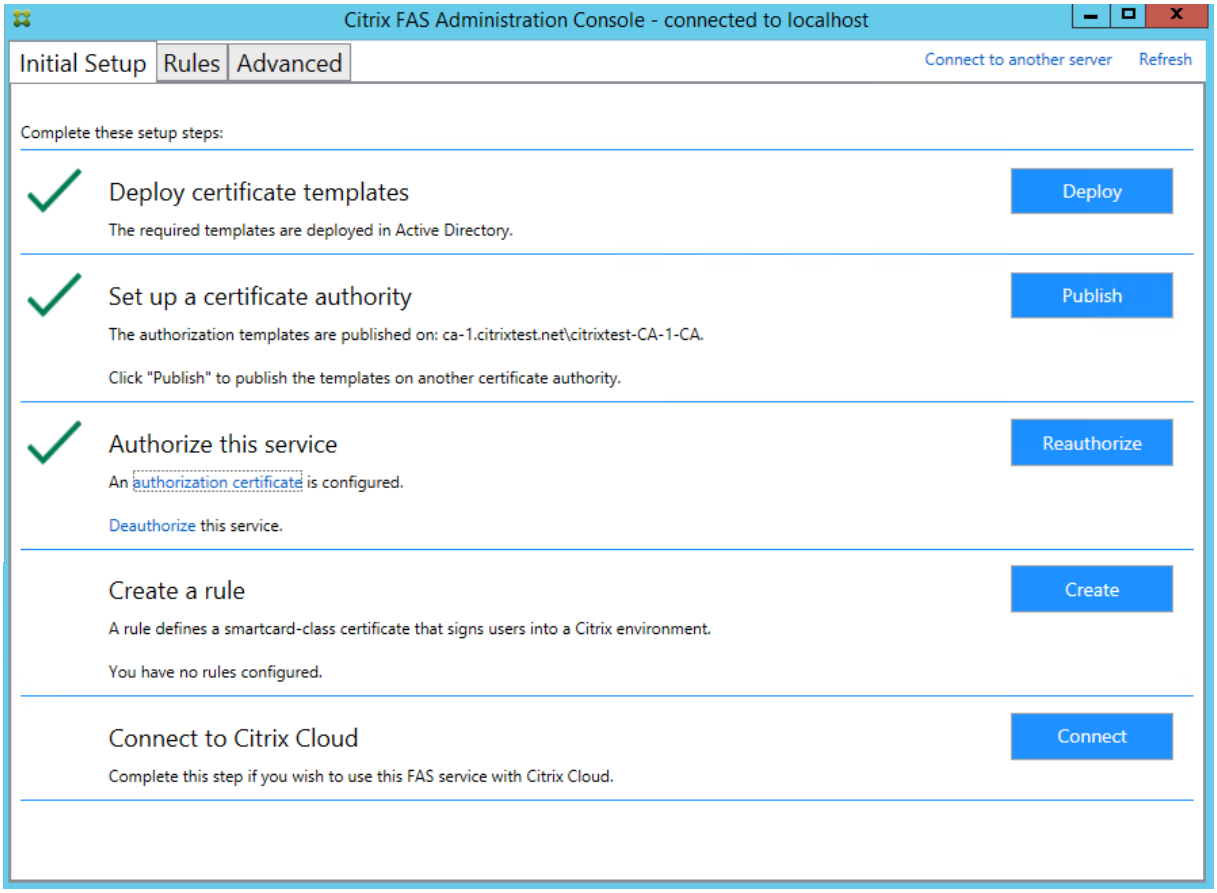
次に例を示します：

```
Import-FasAuthorizationCertificateResponse -address fashsm.auth.net -Id 5ac3d8bd-
b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile
C:\Users\Administrator.AUTH\Desktop\TPM_FAS_Cert.p7b
```


以下が表示されます。

```
PS C:\Users\Administrator.AUTH> Import-UcsAuthorizationCertificateResponse -address ucshsm.auth.local -Id 5ac3d8bd-b484-
4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile C:\Users\Administrator.AUTH\Desktop\TPM_UCS_Cert.p7b


Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           : a5c27fcc-1dd7-4c2b-8963-16ec311020fc
CertificateRequest  :
Status              : Ok
```

手順 **12**：FAS 管理コンソールを終了して再起動します。



注：［このサービスを認証する］手順には緑色のチェックマークが付いています。

手順 **13**： FAS 管理コンソールで ［ルール］タブを選択し、「インストールと構成」の記述に従って設定を編集します。

FAS 管理コンソールの使用　FAS 管理コンソールではオフラインの証明書署名要求を実行できないため、組織で登録機関証明書のオンラインの証明書署名要求が許可されない限り、FAS 管理コンソールの使用はお勧めしません。

FAS の初回のセットアップ手順の実行中、証明書テンプレートを展開して証明機関をセットアップした後、サービスを許可（構成順序の手順 3）する前に次を行います：

手順 **1**：以下の行を次のとおり変更して、構成ファイルを編集します。


```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateTPMProtectedKey"/>
```

ファイルは以下のように表示されます。

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateTPMProtectedKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

一部の TPM ではキーの長さが制限されています。デフォルトのキーの長さは、2048 ビットです。お使いのハードウェアでサポートされる長さのキーを指定してください。

手順 **2**: サービスを許可します。

手順 **3**: 証明機関サーバーから、保留中の証明書要求を手動で発行します。登録機関証明書が取得されたら、管理コンソールのセットアップ順序の手順 3 が緑色に変わります。この時点で、登録機関証明書の秘密キーは TPM で生成されています。証明書はデフォルトで 2 年間有効です。

手順 **4**: 次のように構成ファイルを編集し直します。

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateNonExportableKey"/>
```

> 注:
>
> FAS は TPM で保護されたキーでユーザー証明書を生成できますが、TPM は大規模の展開には速度が遅すぎる可能性があります。

手順 **5**: FAS を再起動します。これにより、サービスによる構成ファイルの再読み込みが強制され、変更された値が反映されます。後続の自動秘密キー操作はユーザー証明書キーに影響します。これらの操作では TPM に秘密キーが保存されませんが、Microsoft ソフトウェアキー記憶域プロバイダーが使用されます。

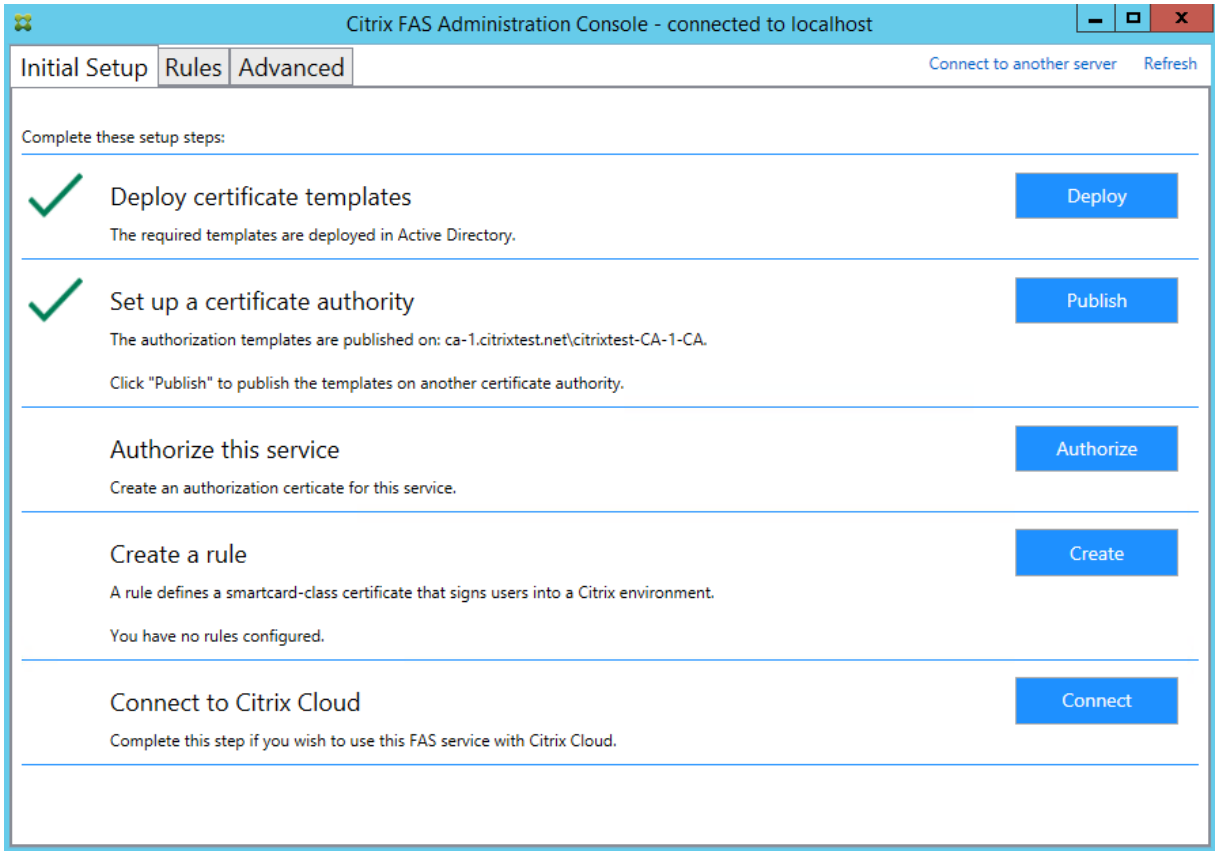
手順 **6**: FAS 管理コンソールで ［ルール］タブを選択し、「インストールと構成」の記述に従って設定を編集します。

例 **3**

この例では、HSM に格納されている登録機関証明書の秘密キーおよびユーザー証明書の秘密キーについて説明します。この例では、構成済みの HSM を想定しています。HSM にはプロバイダー名（「HSM_Vendor’s Key Storage Provider」など）が含まれます。

FAS サーバーを仮想化環境で実行する予定の場合は、HSM ベンダーにハイパーバイザーがサポートされているかどうかを確認してください。

手順 **1**：管理コンソールを使用した FAS の初期セットアップ時には、最初の「証明書テンプレートの展開」および「証明機関のセットアップ」の 2 つの手順だけを完了します。



手順 **2**： HSM ベンダーのドキュメントで、HSM の ProviderName の値を確認します。HSM が CAPI を使用している場合、プロバイダーはドキュメントで暗号化サービスプロバイダー（CSP）と記述されている可能性があります。HSM が CNG を使用している場合、プロバイダーはキー記憶域プロバイダー（KSP）と記述されている可能性があります。

手順 **3**：構成ファイルを次のように編集します。

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName"
value="HSM_Vendor’s Key Storage Provider"/>
```

ファイルは以下のように表示されます。


```xml
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="HSM_Vendor's Key Storage Provider"/>

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

このシナリオでは、HSM が CNG を使用していると想定しているため、ProviderLegacyCsp の値は false に設定されています。HSM が CAPI を使用している場合は、ProviderLegacyCsp の値は true に設定されます。HSM ベンダーのドキュメントで、HSM が CAPICN と CNG のどちらを使用しているかを確認してください。また、非対称 RSA キー生成でサポートされているキーの長さについても、HSM ベンダーのドキュメントで確認してください。この例では、キーの長さはデフォルトの 2048 ビットに設定されています。指定したキーの長さがお使いのハードウェアでサポートされていることを確認してください。

手順 **4**: Citrix フェデレーション認証サービスを再起動して、構成ファイルからの値を読み込みます。

手順 **5**: HSM 内で RSA キーペアを生成し、FAS 管理コンソールの ［**Initial Setup**］タブで ［**Authorize**］をクリックして証明書署名要求を作成します。

手順 **6**: Windows イベントログのアプリケーションエントリをチェックして、キーペアが HSM 内で生成されていることを確認します。

```
[S16] PrivateKey::Create [Identifier e1608812-6693-4c54-a937-91a2e27df75b_TWIN][MachineWide: False][Provider: [CNG]
HSM_Vendor's Key Storage Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]
```

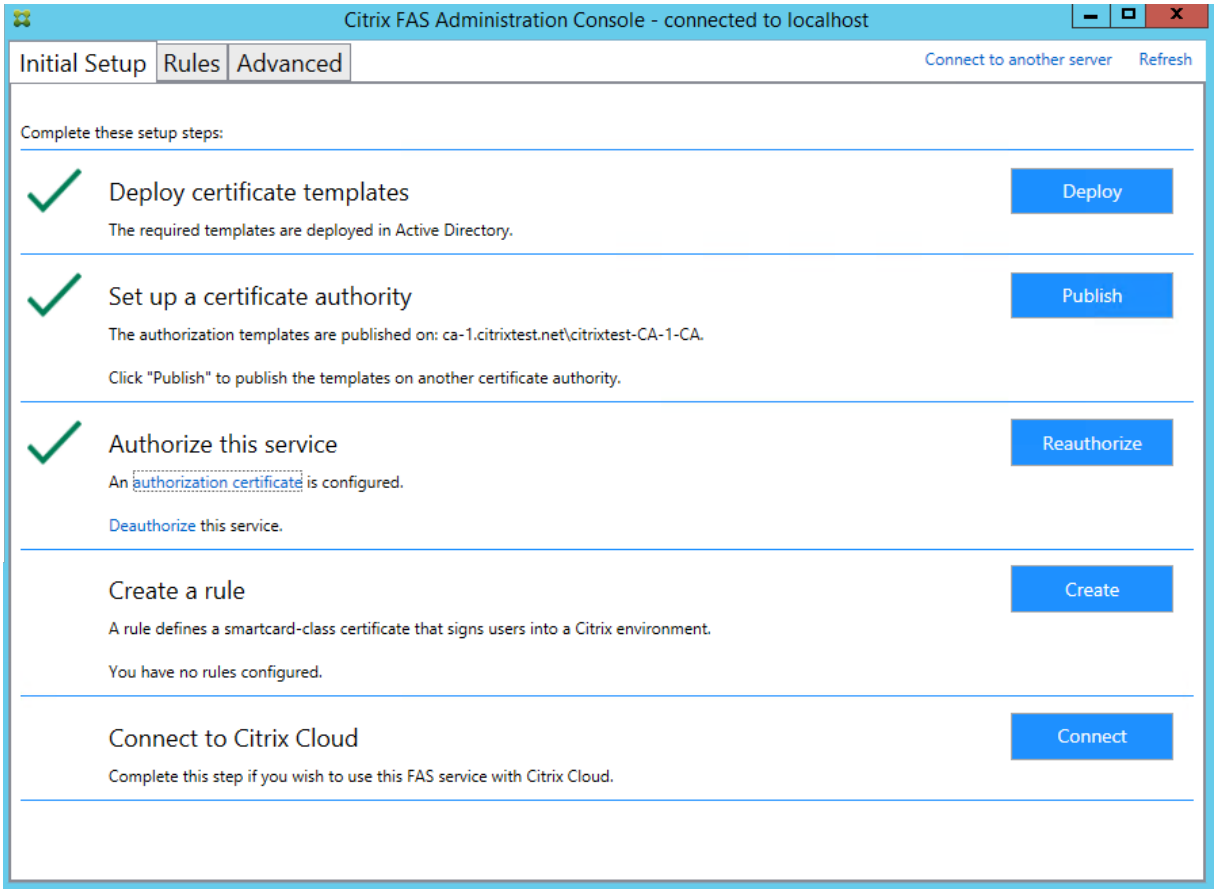
注: [Provider: [CNG] HSM_Vendor’s Key Storage Provider] となっています。

手順 **7**: 証明機関サーバーで、証明機関 MMC で ［**Pending Requests**］ノードを選択します。

Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region
107	-----BEGIN NE...	The operation compl...	Taken Under Submission	07/04/2016 14:04	AUTH\UCSHSM$	

要求を右クリックし、［発行］を選択します。

注: ［このサービスを認証する］手順には緑色のチェックマークが付いています。



手順 **8**: FAS 管理コンソールで ［ルール］タブを選択し、「インストールと構成」の記述に従って設定を編集します。

FAS 証明書ストレージ

FAS では、証明書の保存に FAS サーバー上の Microsoft 証明書ストアを使用しません。埋め込みデータベースを使用します。

登録機関証明書の GUID を特定するには、FAS サーバーで次の PowerShell コマンドレットを入力します:

```
Add-pssnapin Citrix.a\*
Get-FasAuthorizationCertificate -address \<FAS server FQDN>
```

たとえば、「**Get-FasAuthorizationCertificate –address cg-fas-2.auth.net**」と入力します:


```
PS C:\Users\Administrator.AUTH> Get-UcsAuthorizationCertificate -address cg-ucs-2.auth.local


Id                  : a3958424-b8c3-4cac-ba0d-7eb3ce24591c
Address             : cg-dc-2.auth.local\CG-DC-2-ER-CA
TrustArea           : 3df77088-00e0-4dca-a47a-28060dc16986
CertificateRequest  :
Status              : MaintenanceDue

Id                  : fcb185f9-5069-4e34-8625-a333ac126535
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXN0RmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxyNzaiWX8DhUnOZMS2YVSDhr36AV5BGeIYOGVCFKvZPe
                      Rmm/xOVM6cNKsLbew3dYlbo+vdgWg86DFRVxTORhollV86iazDZyOiYGgxe9/s8YZzCspVWN1nB1
                      zXOUJfo1qo9UsmImYr7MR/dhGAtkfsFUoPcd2+zcezmgOfq/4vmCIuerwqzRR5T/p4og7+IjR1se
                      ECz/CbXROOuiDhW+VWbjcsgklcavzvC/jR33F9dZSXNgKRiGHgfd/lBb3elZKA4OOoi9Ou64Q916
                      3ba9BnihqxIgvwWILOmyUfiJmCgbhLJV4TPBopOdKz/axZEIO5p5XYVjCcpXqhqL7Ppn1wIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAJhdvw6yrLGBMtAgo3oPL6o8/at+IqHjHKqgcJNJO/MU7/7X
                      bZB46drLPFzpzF88DkmfoCEgOxlbzFX9waaiFs9CHC/AcEzblN925y1gqljsfC3l5TCKBAeLFoMl
                      PSEkfYMQUOSBYCuLlkFn1LXLSeQ3qJTzSvptYROawFmUMQLffwLSR1vOuS8DJSrpASrwdXJk3TOa
                      Glo/xJo/NRMOwMH+AvGbBsgp3l+jnDjXED5RudqARfgVgcW714JP+XIeFrE1TZmUL2skNIXEPNHC
                      H8eAHdYD26caFigydfefbjx4fbaJDFHJs5+1tnrTZ9knCrawhUiIyOMLGZOOaiER+z8=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval
```

ユーザー証明書の一覧を取得するには、以下を入力します:

```
Get-FasUserCertificate - address \<FAS server FQDN>
```

例: **Get-FasUserCertificate –address cg-fas-2.auth.net**

```
PS C:\Users\Administrator.AUTH> Get-UcsUserCertificate -address cg-ucs-2.auth.local


ThumbPrint             : 7BA22879F40EE92125A2F96E7DD2D52C73820459
UserPrincipalName      : walter@adfs.ext
Role                   : default
CertificateDefinition  : default_Definition
ExpiryDate             : 05/04/2016 12:02:13
```

> 注:
>
> HSM を使用して秘密キーを保存する場合、HSM コンテナーは GUID で識別されます。HSM 内の秘密キーの GUID は、次のコマンドレットで取得できます。「FQDN of FAS Server」は、FAS サーバーの FQDN です。:
>
> ```
> Get-FasUserCertificate - address \<FAS server FQDN> -KeyInfo $true
> ```
>
> 次に例を示します:
>
> ```
> Get-FasUserCertificate - address fas3.djwfas.net -KeyInfo $true
> ```

```
PS C:\Users\administrator> Get-FasUserCertificate -Address fas3.djwfas.net -KeyInfo $true


PrivateKeyIdentifier  : 38405c4d-63af-43e4-9135-2412246b1112
PrivateKeyProvider    : Microsoft Software Key Storage Provider
PrivateKeyIsCng       : True
ThumbPrint            : AD2441F050A02966AA4DB190BA084976528DB667
UserPrincipalName     : joe@djwfas.net
Role                  : default
CertificateDefinition : default_Definition
SecurityContext       :
ExpiryDate            : 19/01/2018 09:18:48
```


関連情報

- FAS のインストールと構成については、「インストールと構成」を参照してください。
- 一般的な FAS 環境については、「Federated Authentication Service のアーキテクチャの概要」を参照してください。
- その他の具体的な手順については、「詳細な構成」を参照してください。

セキュリティとネットワークの構成

September 2, 2022

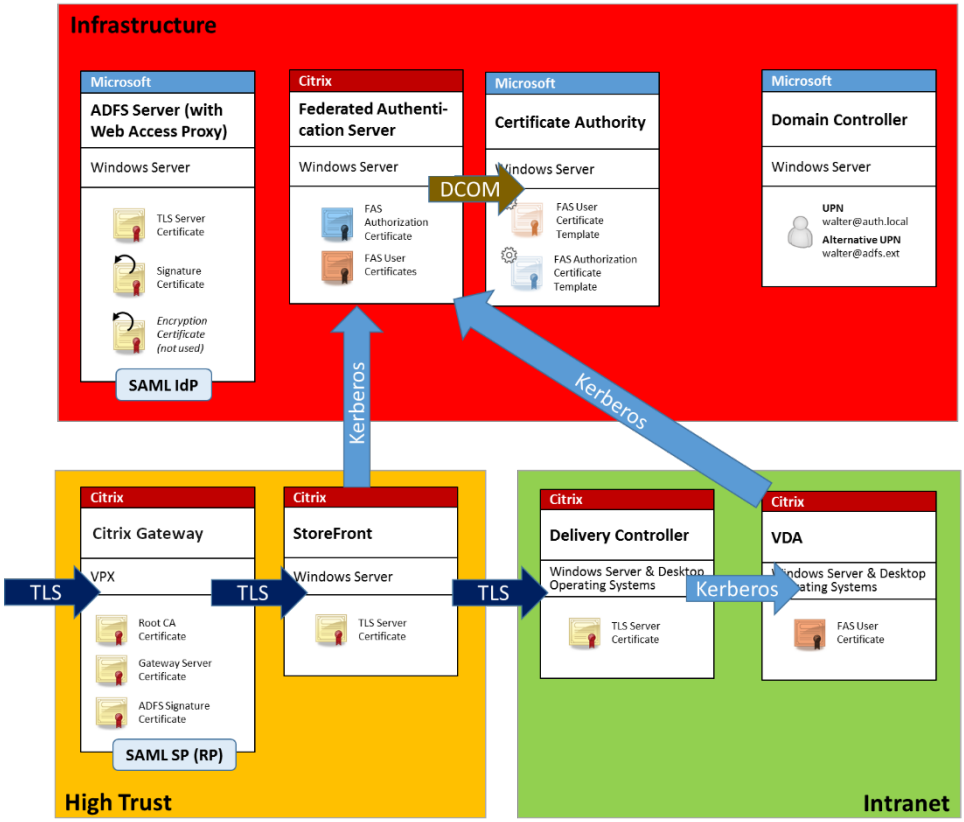
フェデレーション認証サービス（FAS）は、Microsoft Active Directory および Microsoft 証明機関と密接に統合しています。ドメインコントローラーやそのほかの重要なインフラストラクチャと同様に、セキュリティポリシーを展開することによって、システムの適切な管理と保護を行うことが重要です。

このドキュメントでは、FAS を展開する場合に考慮する、セキュリティ問題の概要について説明します。また、インフラストラクチャのセキュリティ保護に役立つ利用可能な機能の概要についても説明します。

ネットワークアーキテクチャ

次の図は、FAS 展開で使用される主要なコンポーネントとセキュリティ境界を示しています。

FAS サーバーは、証明機関やドメインコントローラーと共に、セキュリティ上重要なインフラストラクチャの一部として扱われる必要があります。フェデレーション環境では、Citrix Gateway および Citrix StoreFront が、ユーザー認証を行うことが信頼されたコンポーネントです。そのほかの Citrix Virtual Apps and Desktops コンポーネントは、FAS 導入の影響を受けません。



ファイアウォールとネットワークセキュリティ

Citrix Gateway、StoreFront、および Delivery Controller コンポーネント間の通信は、ポート 443 上で TLS によって保護される必要があります。StoreFront サーバーは発信接続のみを行い、Citrix Gateway は、HTTPS のポート 443 を使用したインターネット上の接続のみを受け入れるようにする必要があります。

StoreFront サーバーは相互認証された Kerberos を使用して、ポート 80 で FAS サーバーと通信します。認証には、FAS サーバーの Kerberos HOST/fqdn ID、および StoreFront サーバーの Kerberos マシンアカウント ID が使用されます。これにより、Citrix の Virtual Delivery Agent（VDA）がユーザーにログオンするのに必要な、1 回限り有効の「資格情報ハンドル」が生成されます。

HDX セッションが VDA に接続されると、VDA もポート 80 で FAS サーバーと通信します。認証には、FAS サーバーの Kerberos HOST/fqdn ID、および VDA の Kerberos マシン ID が使用されます。また、VDA は、証明書と秘密キーへのアクセスに「資格情報ハンドル」を提供する必要があります。

Microsoft 証明機関は、固定 TCP ポートの使用を構成できる、Kerberos 認証の DCOM を使用して、接続を受け入れます。また、証明機関は、FAS サーバーに信頼された登録エージェント証明書による署名済みの CMC パケットを提供するよう要求します。

サーバー	ファイアウォールポート
フェデレーション認証サービス	[in] StoreFront および VDA から HTTP 経由で Kerberos、[out] DCOM から Microsoft 証明機関
Citrix Gateway	[in] クライアントマシンから HTTPS、[in/out] HTTPS と StoreFront サーバー間、[out] HDX から VDA
StoreFront	[in] NetScaler から Citrix Gateway、[out] HTTPS から Delivery Controller、[out] Kerberos から HTTP 経由で FAS
Delivery Controller	[in] StoreFront サーバーから HTTPS、[in/out] VDA から HTTP 経由で Kerberos
VDA	[in/out] Delivery Controller から HTTP 経由で Kerberos、[in] Citrix Gateway から HDX、[out] Kerberos から HTTP 経由で FAS
Microsoft 証明機関	[in] DCOM と、FAS からの署名

Citrix フェデレーション認証サービスと **Citrix Cloud** の接続

コンソールと FAS は、それぞれユーザーのアカウントとネットワークサービスアカウントを使用して次のアドレスにアクセスします。

- ユーザーアカウントの下の FAS 管理コンソール
  - `*.cloud.com`
  - `*.citrixworkspacesapi.net`
  - サードパーティの ID プロバイダーが必要とするアドレス（環境で使用されている場合）
- ネットワークサービスアカウントの下の FAS サービス: `*.citrixworkspacesapi.net`

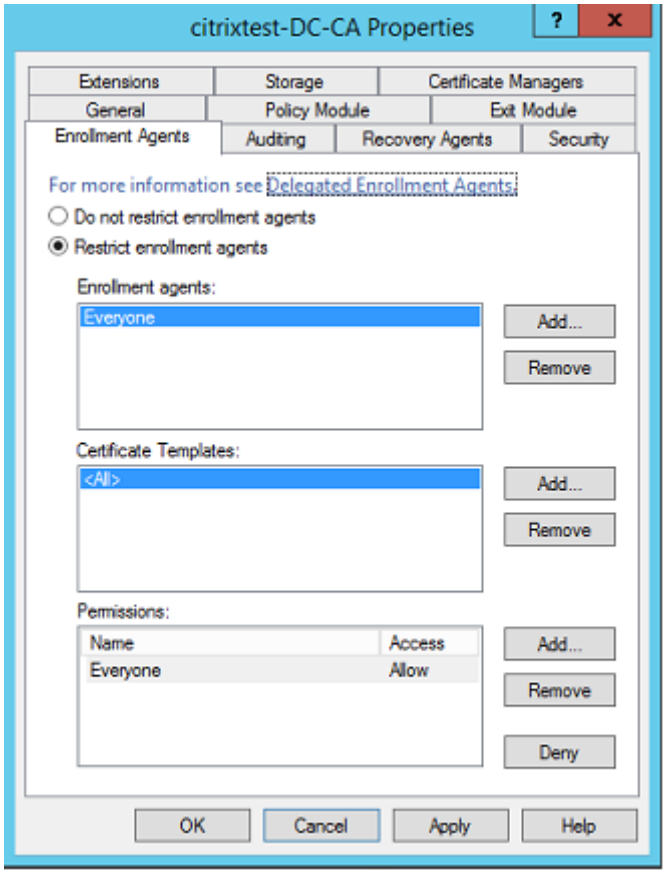
環境にプロキシサーバーが含まれている場合は、FAS 管理コンソールのアドレスを使用してユーザープロキシを構成します。また、ネットワークサービスアカウントのアドレスが netsh または同様のツールを使用して構成されていることを確認します。

セキュリティに関する注意事項

FAS には、FAS がドメインユーザーの代わりに自律的に証明書を発行できるようにする、登録機関の証明書があります。このため、セキュリティポリシーを作成および実装して FAS サーバーを保護し、権限を制限することは重要です。

委任された登録エージェント

FAS は登録エージェントとして機能することによってユーザー証明書を発行します。Microsoft 証明機関により、登録エージェント、証明書テンプレート、および登録エージェントが証明書を発行できるユーザーを制限できます。



このダイアログボックスを使用して、次のことを確認してください:

- [*Enrollment agents*] の一覧に FAS サーバーのみが含まれている。
- [*Certificate Templates*] の一覧に FAS テンプレートのみが含まれている。
- [*Permissions*] の一覧に FAS の使用が許可されているユーザーのみが含まれている。たとえば、管理グループまたは保護されたユーザーのグループに属するユーザーに FAS が証明書を発行できないようにすることをお勧めします。

アクセス制御リストの構成

「ルールの構成」セクションで説明しているように、証明書が発行された場合の FAS に対するユーザー ID の承認を信頼する StoreFront サーバーの一覧を構成する必要があります。同様に、証明書の発行対象となるユーザー、およびユーザーが認証可能な VDA マシンを制限することができます。この操作は、標準で構成を行う Active Directory または証明機関のセキュリティ機能に追加で行います。

ファイアウォールの設定

FAS サーバーへのすべての通信では、相互認証された Windows Communication Foundation（WCF）Kerberos ネットワーク接続がポート 80 で使用されます。

イベントログの監視

FAS および VDA は、Windows イベントログに情報を書き込みます。これは、情報の監視および監査に使用できます。「イベントログ」セクションに、生成される可能性のあるイベントログの一覧を示します。

ハードウェアセキュリティモジュール

FAS によって発行されたユーザー証明書の秘密キーを含むすべての秘密キーは、Network Service アカウントによってエクスポート不可の秘密キーとして保存されます。FAS は、セキュリティポリシーで暗号化ハードウェアセキュリティモジュールが必要とされる場合、このモジュールの使用をサポートします。

FederatedAuthenticationService.exe.config ファイルでは、低レベルの暗号化構成が使用可能です。これらの設定は、秘密キーが最初に作成されたときに適用されます。そのため、登録機関の秘密キー（4096 ビット、TPM 保護など）およびランタイムのユーザー証明書には異なる設定が使用されることがあります。

パラメーター	説明
ProviderLegacyCsp	true に設定した場合、FAS では Microsoft CryptoAPI（CAPI）が使用されます。false に設定した場合、FAS では Microsoft Cryptography Next Generation（CNG）API が使用されます。
ProviderName	使用する CAPI または CNG プロバイダーの名前。
ProviderType	Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24 を参照します。CAPI で HSM を使用する場合、および HSM ベンダーで別のタイプを指定されている場合以外は、常に 24 である必要があります。
KeyProtection	秘密キーの「エクスポート可能」フラグを制御します。さらに、ハードウェアでサポートされている場合は、トラステッドプラットフォームモジュール（TPM）のキーストレージの使用も許可されます。
KeyLength	RSA 秘密キーのキー長。サポートされる値は 1024、2048、および 4096 です（デフォルトは 2048 です）。

管理の責任

環境の管理は、次のグループに分かれます。

名前	責任
エンタープライズ管理者	フォレスト内の証明書テンプレートのインストールおよび保護
ドメインの管理者	グループポリシー設定の構成
証明機関の管理者	証明機関の設定
FAS 管理者	FAS サーバーのインストールと構成
StoreFront/Citrix Gateway 管理者	ユーザー認証の構成
Citrix Virtual Desktops 管理者	VDA およびコントローラーの構成

各管理者は、セキュリティモデル全体のさまざまな面を制御し、システムのセキュリティ保護のための、徹底した防御対策のアプローチを実現します。

グループポリシー設定

信頼された FAS マシンは、グループポリシーで構成済みの「index number -> FQDN」のルックアップテーブルで識別されます。FAS サーバーに接続する場合、クライアントは FAS サーバーの`HOST\<fqdn>`Kerberos ID を検証します。FAS サーバーにアクセスするすべてのサーバーは、同じインデックスに同一の FQDN を持つ必要があります。そうでない場合は、StoreFront および VDA が別の FAS サーバーに接続することがあります。

構成ミスを防ぐために、環境内のすべてのマシンに、単一のポリシーを適用することをお勧めします。FAS サーバーの一覧に変更を加える場合、特にエントリの削除や順序の変更は、注意して行ってください。

この GPO の管理は、FAS サーバーのインストールおよび運用停止を担当する FAS 管理者（またはドメイン管理者）に限定する必要があります。FAS サーバーの運用停止直後に、その FQDN を再度使用しないように注意してください。

証明書テンプレート

FAS から提供される Citrix_SmartcardLogon 証明書テンプレートを使用しない場合、証明書のコピーを変更できます。以下の変更がサポートされています。

証明書テンプレートの名前の変更

Citrix_SmartcardLogon の名前を変更する場合、所属組織のテンプレート命名標準に従って、以下を行う必要があります。

- 証明書テンプレートのコピーを作成し、所属組織のテンプレート命名標準に従ってその名前を変更します。
- 管理ユーザーインターフェイスではなく、管理 FAS への FAS PowerShell コマンドを使用します。（管理ユーザーインターフェイスは、Citrix のデフォルトのテンプレート名での使用のみを対象としています。）
  - Microsoft MMC 証明書テンプレートスナップインか Publish-FasMsTemplate コマンドを使用して、自身のテンプレートを公開し、
  - New-FasCertificateDefinition コマンドにより、自身のテンプレートの名前を使用して FAS を構成します。

全般プロパティの変更

証明書テンプレートの有効期間を変更できます。

更新期間は変更しないでください。FAS は証明書テンプレートのこの設定を無視します。FAS は有効期間の半ばで証明書を自動的に更新します。

要求処理プロパティの変更

これらのプロパティは変更しないでください。FAS は証明書テンプレートのこれらの設定を無視します。FAS では常に、［秘密キーのエクスポートを許可する］と ［同一キーで更新する］はオフにされています。

暗号プロパティの変更

これらのプロパティは変更しないでください。FAS は証明書テンプレートのこれらの設定を無視します。

FAS で提供される該当の設定については、「秘密キー保護」を参照してください。

キーの構成証明プロパティの変更

これらのプロパティは変更しないでください。FAS ではキーの構成証明はサポートされません。

優先テンプレートプロパティの変更

これらのプロパティは変更しないでください。FAS では優先テンプレートはサポートされません。

拡張プロパティの変更

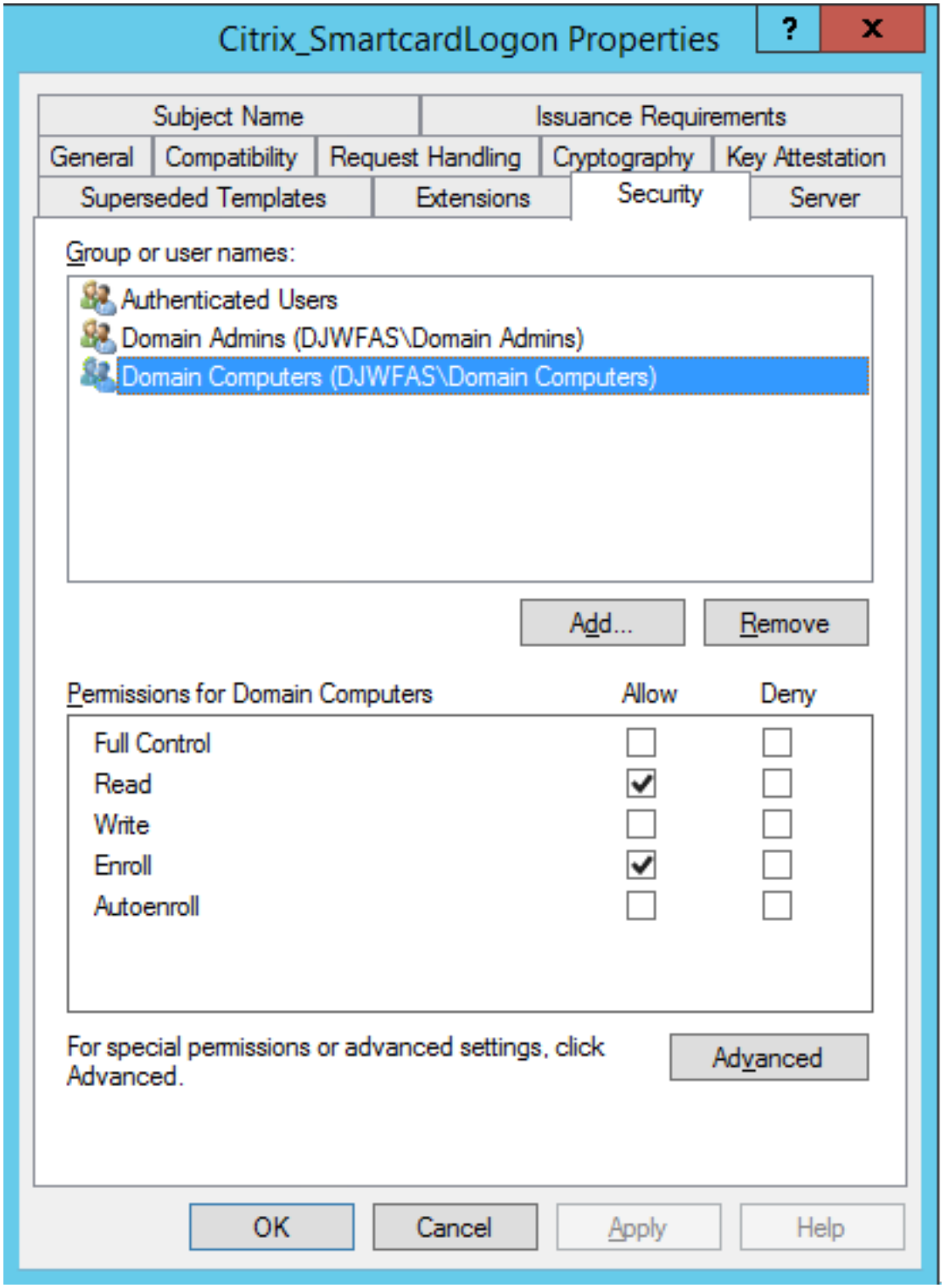
所属組織のポリシーに合わせてこれらの設定を変更できます。

注：不適切な拡張設定を行うと、セキュリティの問題が発生したり、証明書が使用できなくなる場合があります。

セキュリティプロパティの変更

FAS サーバーのマシンアカウントにのみ読み取り権限および登録権限が許可されるように、これらの設定を変更することをお勧めします。FAS サービスには、それ以外の権限は必要ありません。ただし、他の証明書テンプレートと同様、次の項目も追加できます:

- 管理者がテンプレートに対して読み取りまたは書き込みできるようにする
- 認証ユーザーがテンプレートに対して読み取りできるようにする



サブジェクト名プロパティの変更

Citrix では、これらのプロパティを変更しないことをお勧めします。

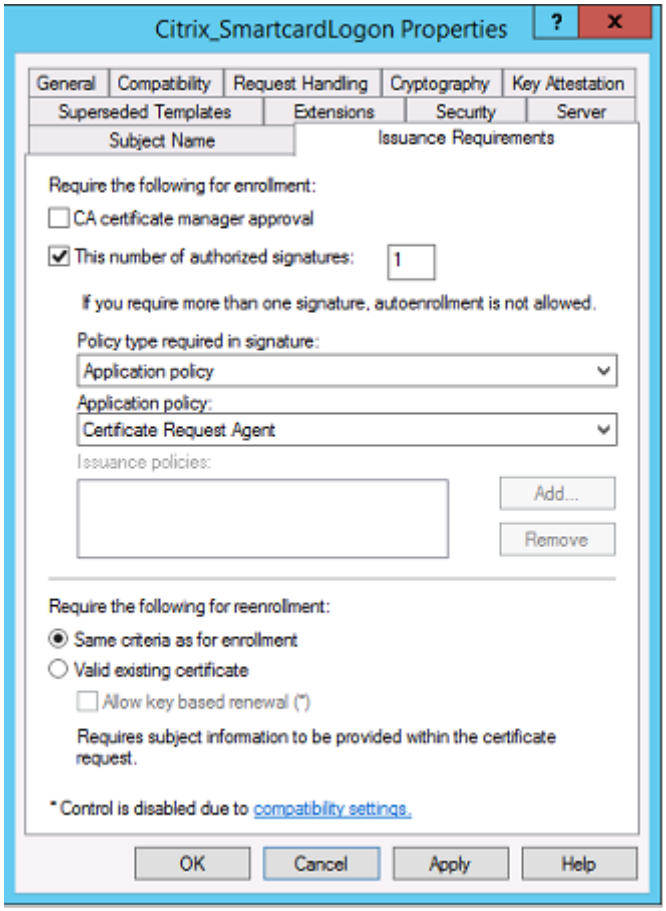
テンプレートで ［*Active Directory* の情報から構築する］が選択されているため、証明機関は証明書拡張にユーザーの SID を含めます。これにより、ユーザーの Active Directory アカウントへの強力なマッピングが提供されます。

サーバープロパティの変更

推奨はされませんが、必要に応じて、所属組織のポリシーに合わせてこれらの設定を変更できます。

発行要件プロパティの変更

これらの設定は変更しないでください。これらは以下のように設定する必要があります。



互換性プロパティの変更

これらの設定は変更できます。この設定は、**Windows Server 2003 CA**（スキーマバージョン 2）以上とする必要があります。ただし、FAS がサポートするのは Windows Server 2008 以降の CA のみです。上記の説明のとおり、**Windows Server 2008 CA**（スキーマバージョン 3）または **Windows Server 2012 CA**（スキーマバージョン 4）を選択することにより使用可能となる追加設定は、FAS では無視されます。

証明機関の管理

証明機関の管理者の任務は、証明機関サーバーの構成、および証明機関サーバーが使用する証明書用秘密キーの発行です。

テンプレートの公開

エンタープライズ管理者の提供するテンプレートに基づいた証明書を証明機関が発行するには、証明機関の管理者がテンプレートの公開を選択する必要があります。

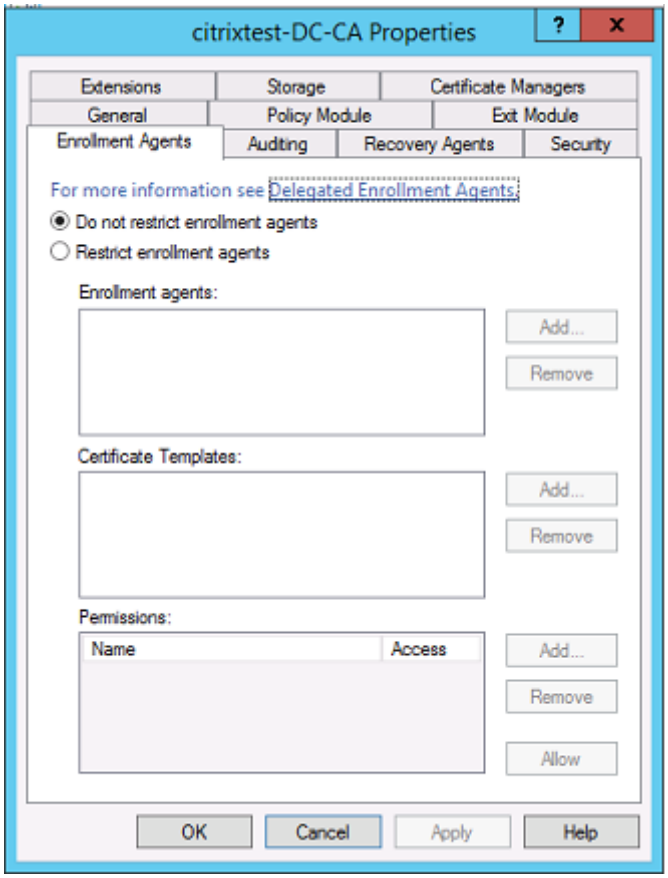
シンプルなセキュリティ対策としては、FAS サーバーのインストール時にのみ登録機関証明書テンプレートを公開するか、またはオフラインの証明書発行手続きを選択することです。いずれの場合も、証明機関の管理者は登録機関証明書の要求の承認において全面的なコントロールを維持し、FAS サーバーの承認に関するポリシーを持つ必要があります。

ファイアウォールの設定

一般的に、証明機関の管理者は、証明機関のネットワークファイアウォール設定も管理して、受信接続の制御を行います。証明機関の管理者は、DCOM TCP およびファイアウォールルールを構成し、FAS サーバーだけが証明書を要求できるようにすることができます。

登録の制限

デフォルトでは、登録機関証明書のすべての保持者が、アクセス可能な証明書テンプレートを使用して、ユーザーに証明書を発行することができます。これを、証明機関プロパティの「登録エージェントの制限」で、特権のないユーザーグループに制限する必要があります。



ポリシーモジュールと監査

高度な展開には、カスタムセキュリティモジュールを使用して、証明書の発行の追跡と拒否を行うことができます。

FAS の管理

FAS にはいくつかのセキュリティ機能があります。

アクセス制御リスト（**ACL**）による **StoreFront**、ユーザー、および **VDA** の制限

FAS セキュリティモデルの中心となるのが、機能にアクセスできる Kerberos アカウントの管理です。

アクセスベクトル	説明
StoreFront［IdP］	これらの Kerberos アカウントは、ユーザーが正しく認証されたと宣言することを信頼されています。Kerberos アカウントのいずれかが危害を受けた場合には、証明書が作成され、FAS の構成で許可されたユーザーに証明書が使用されます。
VDA［証明書利用者］	これらは、証明書および秘密キーへのアクセスが許可されたマシンです。このグループ内の危害を受けた VDA アカウントによるシステム攻撃の範囲が制限されるよう、IdP が取得した資格情報ハンドルも必要です。
ユーザー	IdP がどのユーザーをアサートするかを管理します。証明機関の「制限付き登録エージェント」構成オプションと重複していることに注意してください。一般的に、アクセス制御リストには、特権のないアカウントのみを加えることをお勧めします。これにより、危害を受けた StoreFront アカウントが、権限をより高い管理者レベルに高めることを防ぎます。特に、ドメイン管理者のアカウントは、このアクセス制御リストで許可されるべきではありません。

ルールの構成

独立した複数の Citrix Virtual Apps または Citrix Virtual Desktops の展開で同じ FAS サーバーインフラストラクチャが使用されている場合には、ルールが役立ちます。各ルールにはそれぞれの構成オプションセットがあり、特に Kerberos アクセス制御リスト（ACL）は、個別に構成することができます。

証明機関とテンプレートの設定

証明書テンプレートおよび CA は、それぞれ異なるアクセス権のために構成することができます。高度な構成は、環境に応じて、権限の度合いが異なる証明書を使用するよう選択する場合があります。たとえば、「外部」と識別されたユーザーには、「内部」ユーザーよりも権限が弱い証明書が発行されることがあります。

セッション中および認証の証明書

FAS 管理者は、認証に使用された証明書を、ユーザーのセッションで使用するかどうか管理します。たとえば、より権限のある「ログオン」証明書はログオン時にのみ使用するように、セッションでは「署名」証明書のみ使用可能にすることができます。

秘密キー保護およびキー長

FAS 管理者は、FAS が秘密キーをハードウェアセキュリティモジュール（HSM）、またはトラステッドプラットフォームモジュール（TPM）に保存するよう構成できます。少なくとも登録機関証明書の秘密キーは、TPM に保存して保護することをお勧めします。このオプションは、「オフライン」証明書要求手続きの中で提供されます。

同様に、ユーザー証明書の秘密キーも TPM または HSM に保存できます。すべてのキーは「エクスポート不可能」として生成し、キー長は 2048 ビット以上でなければなりません。

イベントログ

FAS サーバーによって、詳細な構成およびランタイムイベントのログが提供されるため、監査と侵入検出に役立てることができます。

管理アクセスと管理ツール

FAS には、リモート管理の機能（相互認証の Kerberos）およびツールが含まれています。「ローカルの Administrators グループ」のメンバーは、FAS の構成に対するフルコントロール権限を付与されています。この一覧は、注意して維持する必要があります。

Citrix Virtual Apps 管理者、**Citrix Virtual Desktops** 管理者、**VDA** 管理者

「Active Directory パスワード」は FAS の「資格情報ハンドル」にそのまま置き換えられるため、一般的には、FAS の利用によって Delivery Controller や VDA 管理者のセキュリティモデルが変更されることはありません。Controller および VDA の管理グループのメンバーは、信頼されたユーザーに限定する必要があります。監査とイベントログを維持する必要があります。

一般的な **Windows** サーバーセキュリティ

すべてのサーバーにパッチを完全に適用し、標準のファイアウォールとアンチウィルスソフトウェアを使用する必要があります。セキュリティ上重要なインフラストラクチャのサーバーは、物理的に安全な場所に設置し、ディスクの暗号化や仮想マシンのメンテナンスオプションにも十分配慮する必要があります。

監査データとイベントログは、リモートマシンに安全に保存する必要があります。

RDP アクセスは、承認された管理者のみに制限する必要があります。可能な場合は、ユーザーアカウント、特に証明機関およびドメイン管理者のアカウントでは、スマートカードを使用したログオンが要求されるようにする必要があります。

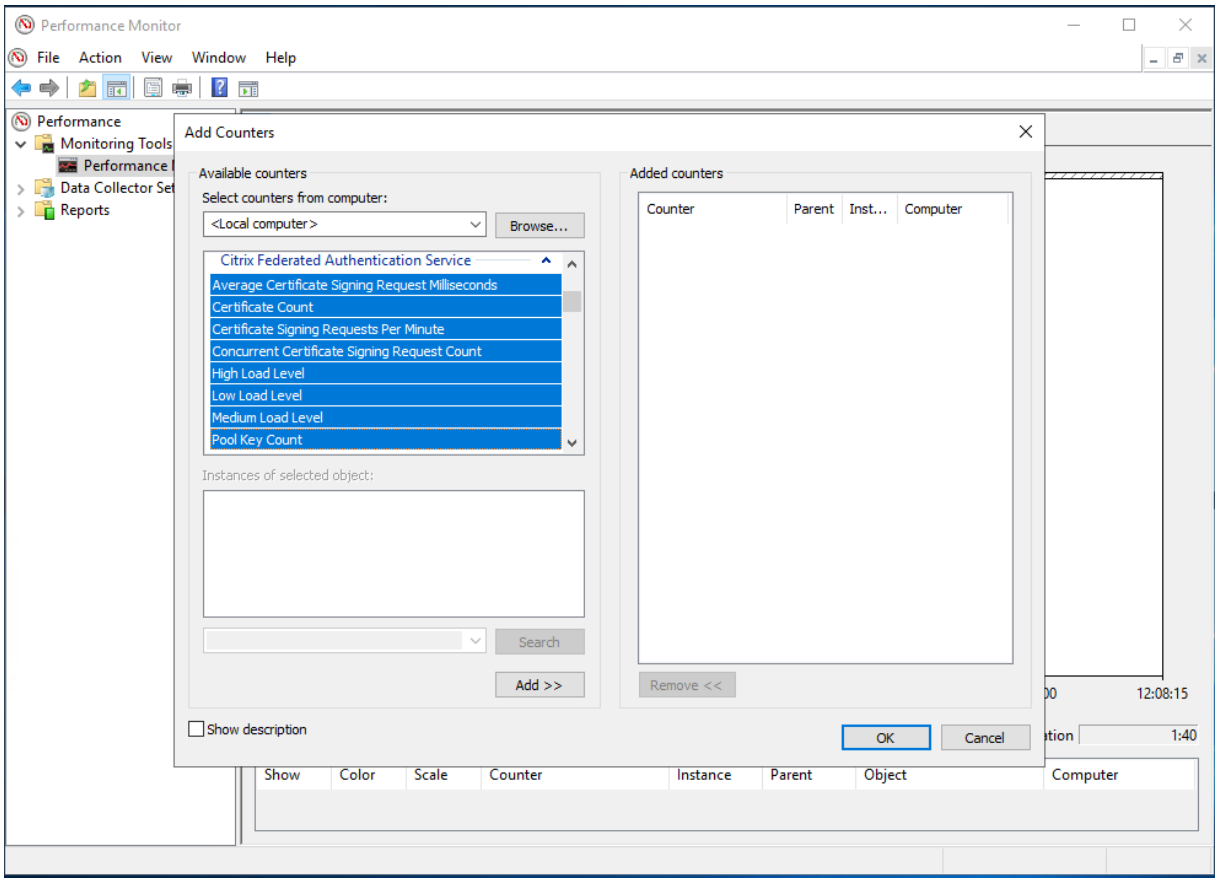
関連情報

- FAS のインストールと構成については、「インストールと構成」を参照してください。
- FAS アーキテクチャについては、「展開アーキテクチャ」を参照してください。
- その他の具体的な手順については、「詳細な構成」を参照してください。

パフォーマンスカウンター

November 9, 2021

FAS には、負荷の追跡用の一連のパフォーマンスカウンターが含まれます。



次の表は、使用可能なカウンターの一覧です。特に明記されていない限り、各カウンターは 10 秒ごとに更新されます。

名前	説明
Average Certificate Signing Request Milliseconds	直前の 1 分のデータを使用して計算された、証明書署名要求の平均期間（ミリ秒単位）。
Certificate Count	フェデレーション認証サービスで管理されている証明書の数。
Certificate Signing Requests Per Minute	直前の 1 分のデータを使用して計算された、フェデレーション認証サービスによって発行された 1 分あたりの証明書署名要求の数。
Concurrent Certificate Signing Request Count	フェデレーション認証サービスで同時に処理されている証明書署名要求の数。
Pool Key Count	事前に生成された、証明書署名要求に使用できるキープール内のキーペアの数。
Private Key Operations Per Minute	直前の 1 分のデータを使用して計算された、フェデレーション認証サービスによって実行された 1 分あたりの証明書秘密キー操作の数。
Session Count	フェデレーション認証サービスによって追跡されている VDA セッションの数。
Low/Medium/High Load Level	フェデレーション認証サービスが 1 分あたりの証明書署名要求に関して許容できる負荷の推定値。推定値は、前の 1 分のデータを使用して、毎分更新されます。「高負荷」しきい値を超過すると、公開アプリまたはデスクトップの起動に失敗することがあります。

Windows ログオンの問題のトラブルシューティング

November 9, 2021

ここでは、ユーザーが証明書やスマートカードを使用してログオンするときに、Windows が提供するログおよびエラーメッセージについて説明します。これらのログには、認証の失敗をトラブルシューティングするために使用できる情報が含まれています。

証明書と公開キー基盤

Windows Active Directory は、ユーザーのログオン用証明書を管理するいくつかの証明書ストアを保守しています。

- **NTAuth** 証明書ストア：Windows への認証のため、ユーザー証明書をすぐに発行する証明機関（つまりチェーンはサポートされません）を NTAuth ストアに配置する必要があります。これらの証明書を表示するには、certutil プログラムから次のように入力します。certutil –viewstore –enterprise NTAuth
- ルートおよび中間証明書ストア：通常、証明書ログオンシステムは単一の証明書のみを提供できるため、チェーンが使用中の場合、すべてのマシン上の中間証明書ストアがこれらの証明書を含んでいる必要があります。ルート証明書は信頼されたルートストアに、最後から 2 番目の証明書は NTAuth ストアにある必要があります。
- ログオン証明書拡張とグループポリシー：EKU や他の証明書ポリシーを強制的に検証するように Windows を構成できます。Microsoft のドキュメントサイトを参照してください：https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)。

レジストリポリシー	説明
AllowCertificatesWithNoEKU	無効にすると、証明書にスマートカードログオン拡張キー使用法（Extended Key Usage：EKU）が含まれる必要があります。
AllowSignatureOnlyKeys	デフォルトで、Windows は、RSA 復号化を許可しない証明書秘密キーを拒否します。このオプションは、そのフィルターを上書きします。
AllowTimeInvalidCertificates	デフォルトで、Windows は期限切れの証明書を拒否します。このオプションは、そのフィルターを上書きします。
EnumerateECCCerts	楕円曲線認証を有効化します。
X509HintsNeeded	証明書に一意のユーザープリンシパル名（UPN）が含まれないか、複数の解釈が可能な場合、このオプションを使用すると、ユーザーが手動で Windows ログオンアカウントを指定できます。
UseCachedCRLOnlyAnd、IgnoreRevocationUnknownErrors	失効チェックを無効にします（通常ドメインコントローラー上で設定）。

- ドメインコントローラー証明書： Kerberos 接続を認証するには、すべてのサーバーが適切な「ドメインコントローラー」証明書を持っている必要があります。これらは、［Local Computer Certificate Personal Store］MMC スナップインメニューを使用して要求できます。

UPN 名と証明書マッピング

ユーザー証明書は、一意のユーザープリンシパル名（UPN）をサブジェクトの別名拡張機能に含めることをお勧めします。

Active Directory での **UPN** 名

デフォルトで、Active Directory のすべてのユーザーは、パターン <samUsername>@<domainNetBios> および <samUsername>@<domainFQDN> に基づく暗黙的 UPN を持っています。利用できるドメインおよび FQDN は、フォレストに対応する RootDSE エントリに含まれています。RootDSE で、単一のドメインに対して複数の FQDN アドレスが登録されていることがあることに注意してください。

また、Active Directory のすべてのユーザーは明示的な UPN と altUserPrincipalNames を持っています。これらはユーザーの UPN を指定する LDAP エントリです。

UPN でユーザーを検索する場合、Windows は、まず（UPN を参照するプロセスの ID に基づいて）現在のドメインで明示的な UPN を、続けて代替 UPN を探します。一致するものがない場合、暗黙的 UPN を探しますが、これはフォレストの異なるドメインで解決されることがあります。

証明書マッピングサービス

証明書に明示的な UPN が含まれない場合、Active Directory は各使用に対して正確な公開証明書を「x509certificate」属性に保管するオプションを持っています。そのような証明書をユーザーに解決するために、コンピューターは直接この属性を問い合わせることができます（デフォルトでは単一のドメインで）。

用意されているオプションを使用すると、ユーザーがユーザーアカウントを指定してこの検索の速度を上げたり、この機能がクロスドメイン環境で使用されるようにしたりできます。

フォレストに複数のドメインがあり、ユーザーがドメインを明示的に指定しない場合、Active Directory の rootDSE が証明書マッピングサービスの場所を指定します。これは通常グローバルカタログマシンに置かれ、フォレスト内のすべての x509certificate 属性のキャッシュビューを持っています。このコンピューターは、証明書だけに基づいて任意のドメインでユーザーアカウントを効率的に検出するために使用できます。

ログオンドメインコントローラーの選択制御

ある環境に複数のドメインコントローラーが含まれる場合、認証にどのドメインコントローラーが使用されているかを把握して制限すると、ログを有効化して取得するのに便利です。

ドメインコントローラーの選択制御

Windows に対して、ログオンで特定の Windows ドメインコントローラーを強制的に使用させるために、lmhosts ファイル（\Windows\System32\drivers\etc\lmhosts）を構成することで、Windows マシンが使用するドメインコントローラーのリストを明示的に設定することができます。

通常その場所には「lmhosts.sam」という名のサンプルファイルがあります。単に次の 1 行を追加します。

1.2.3.4 dcnetbiosname #PRE #DOM:mydomai

ここで、「1.2.3.4」は、「mydomain」ドメインで「dcnetbiosname」という名前が付けられているドメインコントローラーの IP アドレスです。

再起動後に、Windows マシンはその情報を使用して mydomain にログオンします。デバッギングが完了したら、この構成を取り消す必要があることに注意してください。

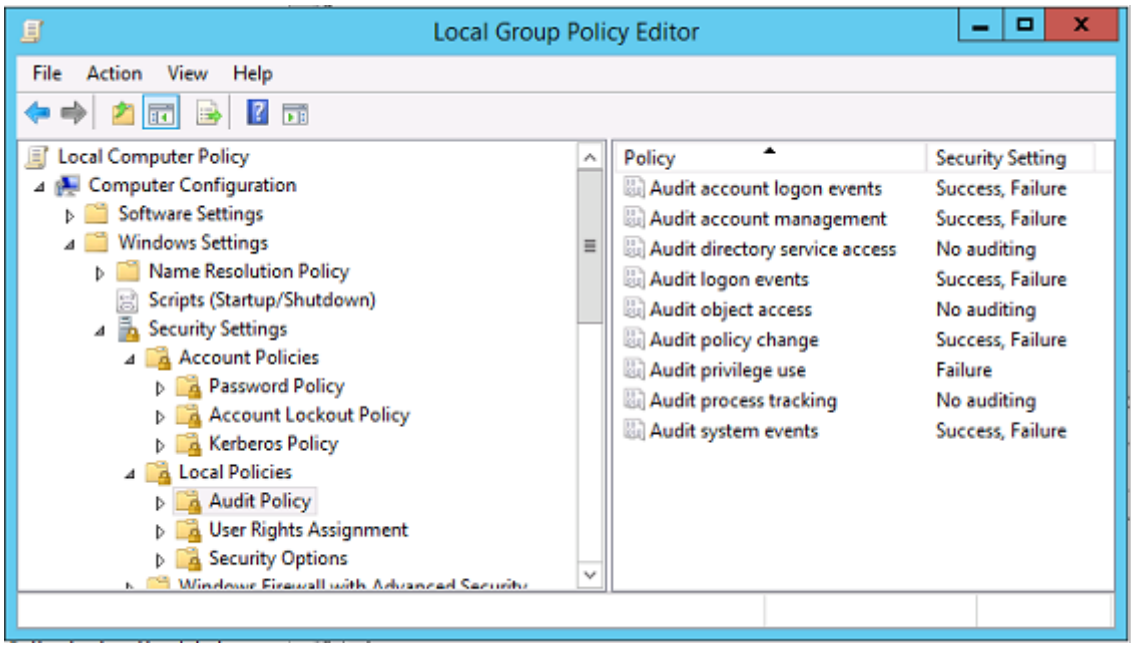
使用中のドメインコントローラーの識別

Windows はログオン時に、ユーザーをログオンさせたドメインコントローラーを MSDOS 環境変数に設定します。これを参照するには、コマンドプロンプトで「**echo %LOGONSERVER%**」を実行します。

認証に関するログは、このコマンドで返されたコンピューターに保存されます。

アカウント監査イベントの有効化

デフォルトで、Windows ドメインコントローラーは完全なアカウント監査ログを有効化していません。これは、グループポリシーエディターで、セキュリティ設定の監査ポリシーを介して制御できます。有効化すると、ドメインコントローラーはセキュリティログファイル内に追加のイベントログ情報を作成します。



証明書検証ログ

証明書の有効性チェック

スマートカード証明書が DER 証明書（秘密キー不要）としてエクスポートされた場合、次のコマンドで検証できます。certutil –verify user.cer

CAPI ログの有効化

ドメインコントローラーとユーザーマシンでは、イベントビューアーを開いて、Microsoft/Windows/-CAPI2/Operational Logs のロギングを有効化します。

CAPI ログは、次のレジストリキーで制御できます。CurrentControlSet\Services\crypt32

値	説明
DiagLevel（DWORD）	詳細度レベル（0～5）
DiagMatchAnyMask（QUADWORD）	イベントフィルター（すべてに 0xffffff を使用）
DiagProcessName（MULTI_SZ）	プロセス名（たとえば、LSASS.exe）によるフィルター

CAPI のログ

メッセージ	説明
チェーンの構築	LSA が CertGetCertificateChain をコールしました（結果含む）
失効確認	LSA が CertVerifyRevocation をコールしました（結果含む）
X509 オブジェクト	詳細モードでは、証明書と証明書失効リスト（CRL）が AppData\LocalLow\Microsoft\X509Objects にダンプされます
チェーンポリシーの検証	LSA が CertVerifyChainPolicy をコールしました（パラメーター含む）

エラーメッセージ

エラーコード	説明
信頼されていない証明書	スマートカード証明書を、証明書を使用してコンピューターの中間証明書ストアおよび信頼できるルート証明書ストアに作成できませんでした。

エラーコード	説明
証明書失効のチェックエラー	証明書 CRL 配布ポイントによって指定されたアドレスからスマートカードの CRL をダウンロードできませんでした。失効チェックが必須の場合、これが原因となってログオンが失敗します。証明書と公開キー基盤」を参照してください。
証明書使用状況エラー	証明書がログオンに適していません。たとえば、サーバー証明書または署名証明書の可能性があります。

Kerberos ログ

Kerberos ログを有効化するには、ドメインコントローラーおよびエンドユーザーマシン上で次のレジストリ値を作成します。

ハイブ	値の名前	値 [DWORD]
CurrentControlSet\Control\Lsa\Kerberos\Parameters	LogLevel	0x1
CurrentControlSet\Control\Lsa\Kerberos\Parameters	KerbDebugLevel	0xffffffff
CurrentControlSet\Services\Kdc	KdcDebugLevel	0x1
CurrentControlSet\Services\Kdc	KdcExtraLogLevel	0x1f

Kerberos ログはシステムイベントログに出力されます。

- 「信頼できない証明書」などのメッセージは診断が簡単です。
- 次の 2 つのエラーコードは情報提供目的のもので、無視しても問題ありません。
  - KDC_ERR_PREAUTH_REQUIRED（以前のドメインコントローラーとの後方互換性のために使用）
  - 不明なエラー 0x4b

イベントログメッセージ

ここでは、ユーザーが証明書を使用してログオンした場合にドメインコントローラーおよびワークステーションに出力されるログエントリの例について説明します。

- ドメインコントローラー CAPI2 ログ
- ドメインコントローラーセキュリティログ
- Virtual Delivery Agent（VDA）セキュリティログ
- VDA CAPI ログ
- VDA システムログ

ドメインコントローラー **CAPI2** ログ

ログオン時にドメインコントローラーは発信者の証明書を検証し、一連のログエントリを次の形式で作成します。

Operational Number of events: 6

Level	Date and Time	Source	Event ID	Task Category
Information	21/06/2016 15:14:54	CAPI2	30	Verify Chain Policy
Information	21/06/2016 15:14:54	CAPI2	11	Build Chain
Information	21/06/2016 15:14:54	CAPI2	90	X509 Objects
Information	21/06/2016 15:14:54	CAPI2	41	Verify Revocation
Information	21/06/2016 15:14:54	CAPI2	40	Verify Revocation
Information	21/06/2016 15:14:54	CAPI2	10	Build Chain

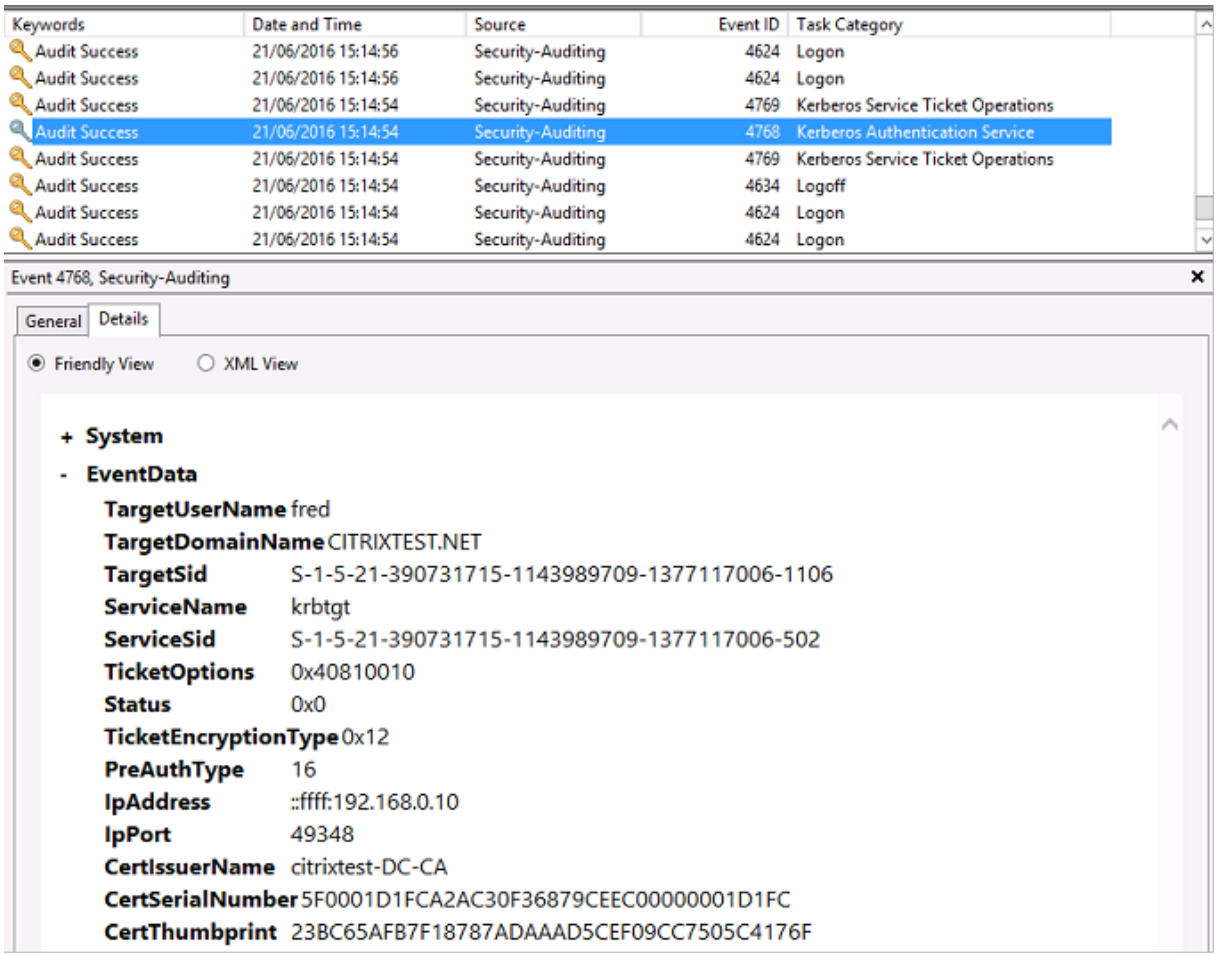
最終イベントログメッセージは、VDA によって提供される証明書に基づいてチェーンを作成するドメインコントローラー上に lsass.exe を表示し、その妥当性（失効など）を検証します。結果は「ERROR_SUCCESS」として戻されます。

- **CertVerifyCertificateChainPolicy**
  - **Policy**
    - [**type**] CERT_CHAIN_POLICY_NT_AUTH
    - [**constant**] 6
  - **Certificate**
    - [**fileRef**] 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F.cer
    - [**subjectName**] fred
  - **CertificateChain**
    - [**chainRef**] {FF03F79B-52F8-4C93-877A-5DFFE40B9574}
  - **Flags**
    - [**value**] 0
  - **Status**
    - [**chainIndex**] -1
    - [**elementIndex**] -1
  - **EventAuxInfo**
    - [**ProcessName**] lsass.exe
  - **CorrelationAuxInfo**
    - [**TaskId**] {F5E7FD3F-628F-4C76-9B1C-49FED786318F}
    - [**SeqNumber**] 1
  - **Result**
    - [**value**] 0

ドメインコントローラーセキュリティログ

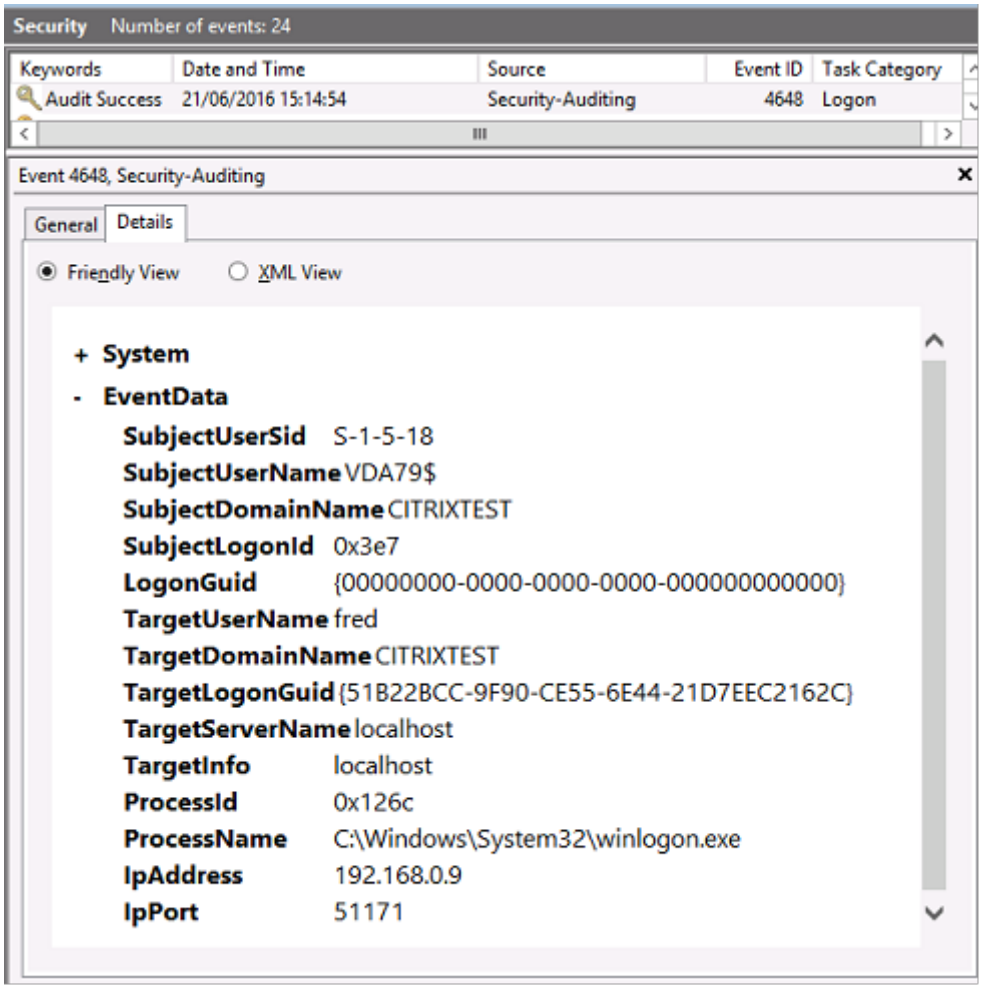
ドメインコントローラーは一連のログオンイベントを表示します。主要なイベントは 4768 で、証明書を使用して Kerberos Ticket Granting Ticket（krbtgt）を発行します。

これより前のメッセージは、ドメインコントローラーに対して認証するサーバーのマシンアカウントを表示します。これより後のメッセージは、ドメインコントローラーに対して認証するために使用される新しい krbtgt に属するユーザーアカウントを表示します。



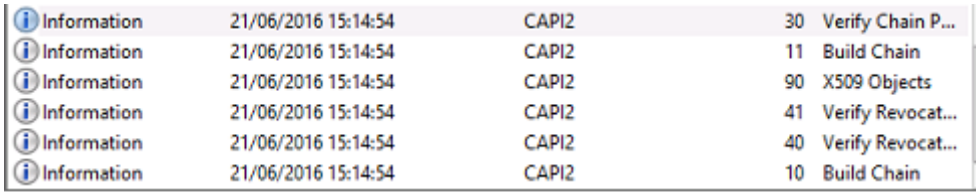
VDA セキュリティログ

ログオンイベントに対応する VDA セキュリティ監査ログはイベント ID が 4648 のエントリで、winlogon.exe により記録されます。

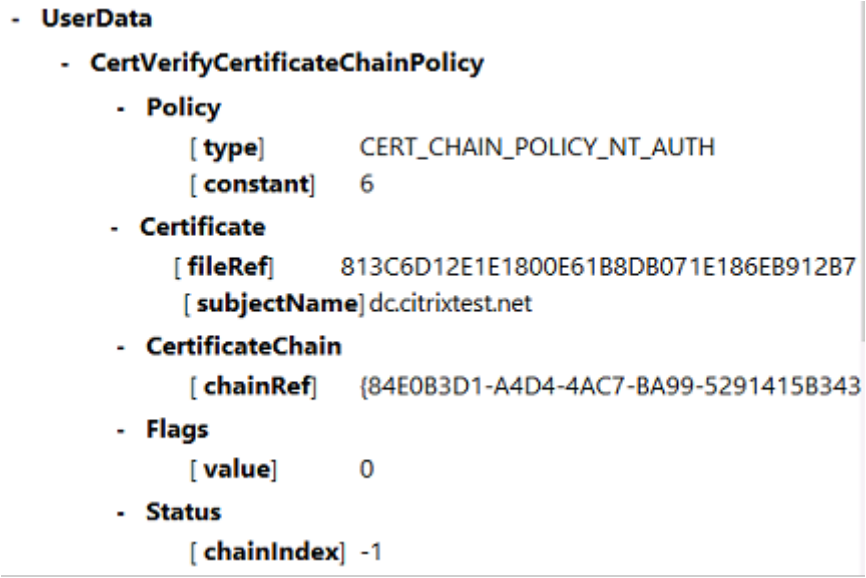


VDA CAPI ログ

このサンプルの VDA CAPI ログは、lsass.exe から単一のチェーンビルドおよび検証シーケンスを示しており、ドメインコントローラー証明書（dc.citrixtest.net）を検証しています。

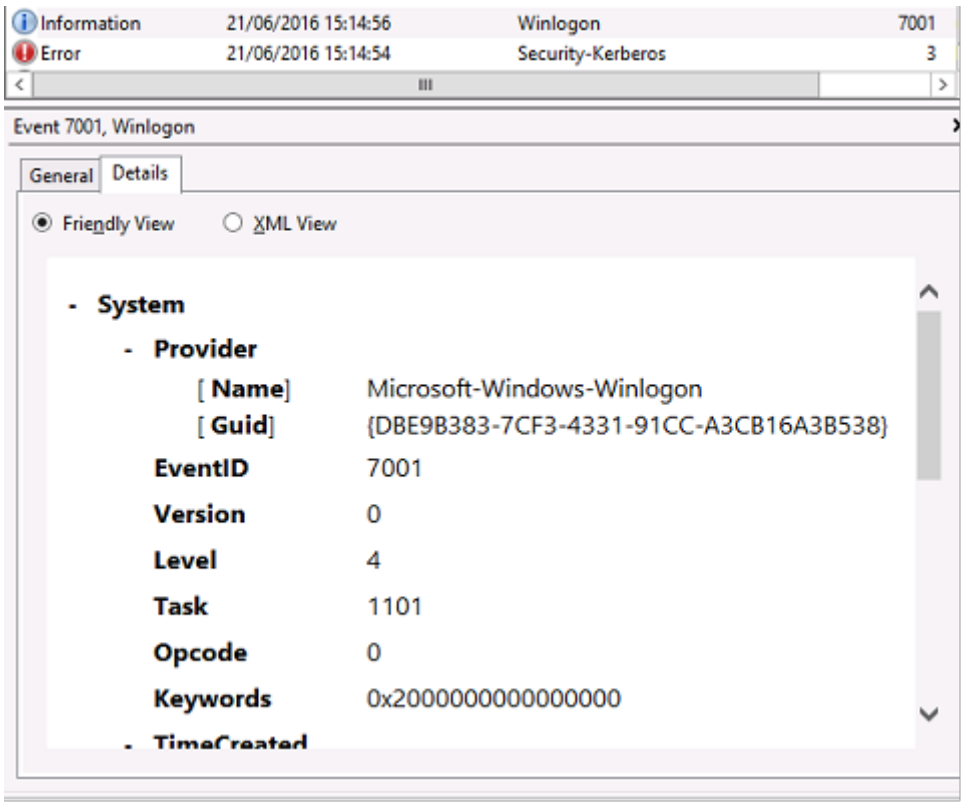


Information	21/06/2016 15:14:54	CAPI2	30	Verify Chain P...
Information	21/06/2016 15:14:54	CAPI2	11	Build Chain
Information	21/06/2016 15:14:54	CAPI2	90	X509 Objects
Information	21/06/2016 15:14:54	CAPI2	41	Verify Revocat...
Information	21/06/2016 15:14:54	CAPI2	40	Verify Revocat...
Information	21/06/2016 15:14:54	CAPI2	10	Build Chain



VDA システムログ

Kerberos ログが有効化されている場合、システムログは、エラー KDC_ERR_PREAUTH_REQUIRED（無視してかまいません）と、Kerberos ログオンが成功したことを示す Winlogon からのエントリを表示します。



イベントログ

次の表は、FAS で生成されるイベントログエントリの一覧です。

管理イベント [フェデレーション認証サービス]

[イベントソース：Citrix.Authentication.FederatedAuthenticationService]

これらのイベントは、FAS サーバーでの構成変更に応じて記録されます。

ログコード
[S001] アクセス拒否：ユーザー [{0}] は管理者グループのメンバーではありません
[S002] アクセス拒否：ユーザー [{0}] はロール [{1}] の管理者ではありません
[S003] 管理者 [{0}] は保守モードを [{1}] に設定しています
[S004] 管理者 [{0}] は CA [{1}] テンプレート [{2} および {3}] で登録しています
[S005] 管理者 [{0}] は CA [{1}] の権限を取り消しています
[S006] 管理者 [{0}] は新しい証明書定義 [{1}] を作成しています
[S007] 管理者 [{0}] は証明書定義 [{1}] を更新しています
[S008] 管理者 [{0}] は証明書定義 [{1}] を削除しています
[S009] 管理者 [{0}] は新しいロール [{1}] を作成しています
[S010] 管理者 [{0}] はロール [{1}] を更新しています
[S011] 管理者 [{0}] はロール [{1}] を削除しています
[S012] 管理者 [{0}] は証明書を作成しています [UPN：{1} sid：{2} ロール：{3}][Certificate Definition: {4}][セキュリティコンテキスト：{5}]
[S013] 管理者 [{0}] は証明書を削除しています [UPN：{1} ロール：{2} 証明書定義：{3} セキュリティコンテキスト：{4}]
[S015] 管理者 [{0}] は証明書要求を作成しています [TPM：{1}]
[S016] 管理者 [{0}] は認証証明書をインポートしています [参照：{1}]
[S050] 管理者 [{0}] は新しいクラウド構成を作成しています：[{1}]
[S051] 管理者 [{0}] はクラウド構成を更新しています：[{1}]
[S052] 管理者 [{0}] はクラウド構成を削除しています

ログコード
[S401] 構成アップグレードを実行中です–[開始バージョン {0}][to version {1}]
[S402] エラー：Citrix フェデレーション認証サービスは Network Service として実行する必要があります [現在は {0} として実行中]
[S404] Citrix フェデレーション認証サービスのデータベースを強制的に消去しています
[S405] レジストリからデータベースへのデータの移行中にエラーが発生しました：[{0}]
[S406] レジストリからデータベースへのデータ移行が完了しました（注：ユーザー証明書は移行されない）
[S407] データベースが既に存在していたため、レジストリベースのデータはデータベースに移行されませんでした
[S408] 構成をダウングレードできません–[バージョン {0} 以降][to version {1}]
[S409] ThreadPool MinThreads は [ワーカー：{0} 完了：{1}] から [ワーカー：{2} 完了：{3}] に変更されました
[S410] ThreadPool MinThreads を [ワーカー：{0} 完了：{1}] から [ワーカー：{2} 完了：{3}] に変更できませんでした
[S411] FAS サービスの開始エラー：[{0}]

ID アサーションの作成 **[**フェデレーション認証サービス**]**

[イベントソース：Citrix.Authentication.FederatedAuthenticationService]

これらのイベントは、信頼済みのサーバーがユーザーログオンをアサートすると、ランタイム時に FAS サーバーに記録されます。

ログコード
[S101] サーバー [{0}] にはロール [{1}] の ID をアサートする権限がありません
[S102] サーバー [{0}] は UPN [{1}] のアサートに失敗しました（例外：{2}{3}）
[S103] サーバー [{0}] は UPN [{1}]、SID {2} を要求しましたが、検索で SID {3} が返されました
[S104] サーバー [{0}] は UPN [{1}] のアサートに失敗しました（UPN はロール [{2}] によって許可されていません）
[S105] サーバー [{0}] は ID のアサーションを発行しました [UPN：{1}、ロール：{2}、セキュリティコンテキスト：[{3}]]
[S120] [UPN：{0}、ロール：{1}、セキュリティコンテキスト：[{2}]] に対して証明書を発行しています
[S121] 証明書が [UPN：{0} ロール：{1}] に [認証局：{2}] から発行されました
[S122] 警告：サーバー過負荷です [UPN：{0}、ロール：{1}] [1 分あたりの要求 {2}]。
[S123] [UPN：{0} ロール：{1}] の証明書の発行に失敗しました [例外：{2}]
[S124] [認証局：{2}] の [UPN：{0} ロール：{1}] の証明書の発行に失敗しました [例外：{3}]

証明書利用者の行動 **[**フェデレーション認証サービス**]**

[イベントソース：Citrix.Authentication.FederatedAuthenticationService]

これらのイベントは、VDA にユーザーがログオンすると、ランタイム時に FAS サーバーに記録されます。

ログコード
[S201] 証明書利用者 [{0}] にはパスワードへのアクセス権がありません。
[S202] 証明書利用者 [{0}] には証明書へのアクセス権がありません。
[S203] 証明書利用者 [{0}] にはログオン CSP へのアクセス権がありません
[S204] 証明書利用者 [{0}] が [{4}] によって承認されたログオン CSP にアクセスしています [UPN：{1}] 役割：[{2}] [操作：{3}]
[S205] 呼び出しアカウント [{0}] はロール [{1}] の証明書利用者ではありません
[S206] 呼び出しアカウント [{0}] は証明書利用者ではありません
[S208] 秘密キーの処理が失敗しました［操作：{0}］［UPN：{1}、ロール：{2}、証明書定義 {3}］［エラー {4} {5}］

セッション内証明書サーバー **[**フェデレーション認証サービス**]**

[イベントソース：Citrix.Authentication.FederatedAuthenticationService]

これらのイベントは、ユーザーはセッション内証明書を使用すると、FAS サーバーで記録されます。

ログコード
[S301] アクセス拒否：ユーザー [{0}] には仮想スマートカードへのアクセス権がありません
[S302] ユーザー [{0}] は不明な仮想スマートカードを要求しました [拇印：{1}]
[S303] アクセス拒否：ユーザーが [{0}] 仮想スマートカードと [UPN：{1}] 一致しません
[S304] コンピューター [{2}] でプログラム [{1}] を実行中のユーザー [{0}] は秘密キー処理 [{6}] のために仮想スマートカードを使用しています [UPN：{3}、ロール：{4}、拇印：{5}]
[S305] 秘密キーの処理が失敗しました［操作：{0}］［UPN：{1}、ロール：{2}、コンテナ名 {3}］［エラー {4} {5}］。

FAS アサーションプラグイン **[**フェデレーション認証サービス**]**

[イベントソース：Citrix.Authentication.FederatedAuthenticationService]

これらのイベントは、FAS アサーションプラグインによって記録されます。

ログコード
[S500] FAS アサーションプラグインが設定されていません
[S501] 設定された FAS アサーションプラグインをロードできませんでした [例外：{0}]
[S502FAS]FAS アサーションプラグインがロードされました [pluginId={0}] [assembly={1}] [location={2}]
[S503] サーバー [{0}] が UPN [{1}] のアサートに失敗しました（ログオン値が提供されましたがプラグイン [{2}] が対応していません）
[S504] サーバー [{0}] が UPN [{1}] のアサートに失敗しました（ログオン値が提供されましたが、FAS プラグインが構成されていません）
[S505] サーバーが [{0}]UPN の [{1}] アサートに失敗しました（プラグインに [{2}] よりログオン値が拒否されステータス [{3}] とメッセージ [{4}] が返されました）
[S506] プラグイン [{0}] がサーバー [{1}] のログオン値を UPN [{2}] として承認しメッセージ [{3}] が返されました
[S507] サーバー [{0}] は UPN [{1}] のアサートに失敗しました（プラグイン [{2}] が例外 [{3}] をスローしました）
[S507] サーバー [{0}] は UPN [{1}] のアサートに失敗しました（プラグイン [{2}] が例外 [{3}] をスローしました）
[S508] サーバー [{0}] が UPN [{1}] のアサートに失敗しました（処理へのアクセスが提供されましたがプラグイン [{2}] が対応していません）
[S509] サーバー [{0}] が UPN [{1}] のアサートに失敗しました（処理へのアクセスが提供されましたが、FAS プラグインが構成されていません）
[S510] サーバー [{0}] が UPN [{1}] のアサートに失敗しました（プラグイン [{2}] によってアクセス処理が無効と判断されました）

Workspace 対応 **FAS [**フェデレーション認証サービス**]**

[イベントソース：Citrix.Fas.Cloud]

FAS と Workspace を組み合わせて使用している場合、これらのイベントがログに記録されています。

ログコード
[S001] Citrix Cloud サービスキーを切り替えています [FAS ID={0}]
[S002] FAS クラウドサービスを開始しています。FasHub クラウドサービス URL：{0}
[S003] FAS はクラウドに登録しました [FAS ID：{0}] [トランザクション ID：{1}]
[S004] FAS はクラウドへの登録に失敗しました [FAS ID：{0}] [トランザクション ID：{1}] [例外：{2}]
[S005] FAS はクラウドに現在の構成を送信しました [FAS ID：{0}] [トランザクション ID：{1}]
[S006] FAS はクラウドに現在の構成を送信できませんでした [FAS ID：{0}] [トランザクション ID：{1}] [例外：{2}]
[S007] FAS はクラウドから登録解除しました [FAS ID：{0}] [トランザクション ID：{1}]

ログコード
[S009] FAS はクラウドからの登録解除に失敗しました [FAS ID：{0}] [トランザクション ID：{1}] [例外：{2}]
[S010] FAS サービスはクラウドメッセージング URL に接続されています：{0}
[S011] FAS サービスはクラウドに接続されていません
[S012] FAS サービスは Citrix Cloud からのシングルサインオンで利用可能です
[S013] FAS サービスは Citrix Cloud からのシングルサインオンで利用できません。[{0}] 詳しくは、管理コンソールを確認してください
[S014] クラウドサービス<service name>の呼び出しに失敗しました [FAS ID：{0}] [トランザクション ID：{1}] [例外：{2}]
[S015] Citrix Cloud からのメッセージは、呼び出し元が許可されていないためブロックされました [メッセージ ID {0}] [トランザクション ID {1}] [呼び出し元 {2}]
[S016] クラウドサービス<service name>の呼び出しに成功しました [FAS ID：{0}] [トランザクション ID：{1}]
[S019] FAS はクラウド [FAS ID：{0}] [トランザクション ID：{1}] から構成をダウンロードしました
[S020] FAS はクラウド [FAS ID：{0}] [トランザクション ID：{1}] [例外：{2}] から構成をダウンロードできませんでした
[S021] FAS クラウドサービスを開始できませんでした。例外: {0}
[S022] FAS クラウドサービスを停止しています

ログオン **[VDA]**

[イベントソース：Citrix.Authentication.IdentityAssertion]

これらのイベントは、ログオン時に VDA で記録されます。

ログコード
[S101] ID アサーションログオンに失敗しました。認識できないフェデレーション認証サービス [ID：{0}]
[S102] ID アサーションログオンに失敗しました。{0} の SID が見つかりませんでした [例外：{1}{2}]
[S103] ID アサーションログオンに失敗しました。ユーザー {0} の SID は {1} ですが、想定された SID は {2} です
[S104] ID アサーションログオンに失敗しました。フェデレーション認証サービスへの接続に失敗しました：{0} [エラー：{1} {2}]
[S105] ID アサーションログオン。[ユーザー名：{0}][Domain: {1}] にログインしています
[S106] ID アサーションログオン。[証明書：{0}] にログインしています。
[S107] ID アサーションログオンに失敗しました。[例外：{0}{1}]

ログコード
[S108] ID アサーションサブシステム。ACCESS_DENIED [呼び出し元：{0}]

セッション内証明書 **[VDA]**

[イベントソース：Citrix.Authentication.IdentityAssertion]

これらのイベントは、ユーザーがセッション内証明書を使用しようとすると、VDA に記録されます。

ログコード
[S201] 仮想スマートカードの [PID：{1} プログラム名：{2}][Certificate thumbprint: {3}] へのアクセスが [{0}] に認証されました [S203] 仮想スマートカードサブシステム。アクセスが拒否されました [呼び出し元：{0}、セッション：{1}]
[S204] 仮想スマートカードサブシステム。スマートカードのサポートが無効化されました。

証明書要求およびキーペア生成 **[**フェデレーション認証サービス**]**

[イベントソース：Citrix.Fas.PkiCore]

これらのイベントは、FAS サーバーが低レベルの暗号化操作を実行すると記録されます。

ログコード
[S001] TrustArea::TrustArea：証明書がインストールされました [TrustArea: {0}] [証明書 {1}][TrustAreaJoinParameters{2} [S014] Pkcs10Request::Create: PKCS10 要求が作成されました [識別名 {0}]
[S016] PrivateKey::Create [識別子 {0}][MachineWide: {1}][プロバイダー：{2}][ProviderType: {3}][EllipticCurve：{4}][KeyLength: {5}][isExportable：{6}] [S017] PrivateKey::Delete [CspName: {0}、識別子 {1}]

ログコード
[S104] MicrosoftCertificateAuthority::GetCredentials：{0} の使用権限が付与されました
[S105]MicrosoftCertificateAuthority::SubmitCertificateRequest エラーが応答 [{0}] を返しました
[S106] MicrosoftCertificateAuthority::SubmitCertificateRequest 証明書 [{0}] が発行されました

ログコード
[S112] MicrosoftCertificateAuthority::SubmitCertificateRequest - 承認待機中 [CR_DISP_UNDER_SUBMISSION] [参照：{0}]

エンドユーザーエラーメッセージ

ここでは、Windows ログオンページでユーザーに表示される一般的なエラーメッセージの一覧を示します。

表示されるエラーメッセージ	説明および参照先
無効なユーザー名またはパスワードです。	コンピューターはユーザーが有効な証明書および秘密キーを持っていると判断していますが、Kerberos ドメインコントローラーが接続を拒否しました。この記事の「*Kerberos* ログ」を参照してください。
システムにログオンできませんでした。資格情報を確認できませんでした。/この要求は、サポートされていません。	ドメインコントローラーに接続できないか、ドメインコントローラーにスマートカード認証をサポートする証明書が構成されていません。「Kerberos 認証」、「ドメインコントローラー認証」、または「ドメインコントローラー」証明書のドメインコントローラーを登録します。これは通常試す価値があります。既存の証明書が有効に見える場合でも同様です。
システムにログオンできませんでした。認証のために使用されたスマートカード証明書が信頼できませんでした。	中間証明書とルート証明書がローカルコンピューターにインストールされていません。「証明書と公開キー基盤」を参照してください。
不正な要求	これは通常、証明書の拡張子が正しく設定されていないか、RSA キーが短すぎることを示します（2048 ビット未満）。

関連情報

- スマートカードログオン用のドメインを構成します：http://support.citrix.com/article/CTX206156
- スマートカードログオンポリシー：https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)
- CAPI ログの有効化：http://social.technet.microsoft.com/wiki/contents/articles/242.troubleshooting-pki-problems-on-windows.aspx
- Kerberos ログの有効化：https://support.microsoft.com/en-us/kb/262177
- サードパーティの証明機関を使用してスマートカードログオンを有効化するためのガイドライン：https://support.microsoft.com/en-us/kb/281245

PowerShell コマンドレット

November 9, 2021

シンプルな展開ではフェデレーション認証サービス（FAS）管理コンソールも使用できますが、PowerShell インターフェイスにはより詳細なオプションがあります。コンソールでは使用できないオプションを使用する場合は、PowerShell のみを使用して構成を行うことをお勧めします。

次のコマンドによって FAS PowerShell コマンドレットが追加されます。

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

PowerShell ウィンドウでは、Get-Help <*cmdlet name*> を使用して、コマンドレットのヘルプを表示できます。

FAS PowerShell SDK コマンドレットについて詳しくは、https://developer-docs.citrix.com/projects/federated-authentication-service-powershell-cmdlets/en/latest/を参照してください。

展開アーキテクチャ

November 9, 2021

はじめに

フェデレーション認証サービス（FAS）は Active Directory 証明機関と統合して、Citrix 環境内でのシームレスなユーザー認証を実現する Citrix コンポーネントです。このドキュメントでは、環境に適した、さまざまな認証アーキテクチャについて説明します。

FAS が有効化されると、信頼された StoreFront サーバーにユーザー認証の判断が委任されます。StoreFront は最新の Web テクノロジを中心に構築されたビルトイン認証オプションの包括的なセットを搭載しており、StoreFront SDK やサードパーティの IIS プラグインを使用して容易に拡張できます。基本的な設計目標は、Web サイトへのユーザー認証が可能なすべての認証テクノロジを、Citrix Virtual Apps または Citrix Virtual Desktops の展開へのログインに活用することです。

このドキュメントでは、複雑さを増す上位レベルの展開アーキテクチャに関する例が記載されています。

- 内部展開
- Citrix Gateway の展開
- ADFS SAML
- B2B アカウントのマッピング
- Windows 10 Azure AD への参加

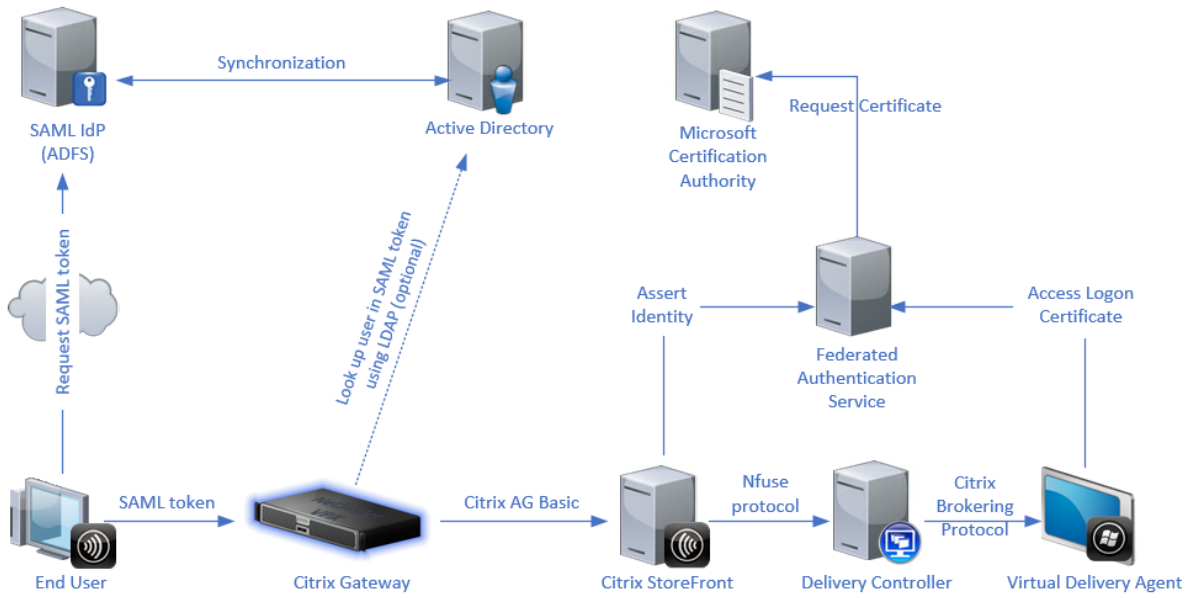
FAS 関連記事にリンクしています。すべてのアーキテクチャにおける FAS のセットアップについては「インストールと構成」を参照してください。

アーキテクチャの概要

FAS には、StoreFront の認証した Active Directory ユーザーの代わりに、スマートカードクラスの証明書を自動的に発行する権限が付与されます。これは、管理者が物理スマートカードをプロビジョニングできるツールと同様の API を使用します。ユーザーが Citrix Virtual Apps または Citrix Virtual Desktops の Virtual Delivery Agent（VDA）に仲介されると、マシンに証明書がアタッチされ、Windows ドメインはログオンを標準のスマートカード認証と見なします。

ユーザーが Citrix 環境へのアクセスを要求すると、信頼済みの StoreFront サーバーが FAS にアクセスします。FAS は、単一の Citrix Virtual Apps または Citrix Virtual Desktops セッションがそのセッションの証明書で認証できるようにするチケットを付与します。VDA でユーザーを認証する必要がある場合、VDA は FAS にアクセスしてチケットを使用します。ユーザー証明書の秘密キーにアクセスできるのは FAS だけです。VDA は、証明書を使用して実行する必要のあるすべての署名処理および暗号化解除処理を、FAS に送信しなければなりません。

以下の図に、Microsoft 証明機関と統合した FAS による、StoreFront と Citrix Virtual Apps and Desktops Virtual Delivery Agent（VDA）へのサポートサービスの提供について示します。



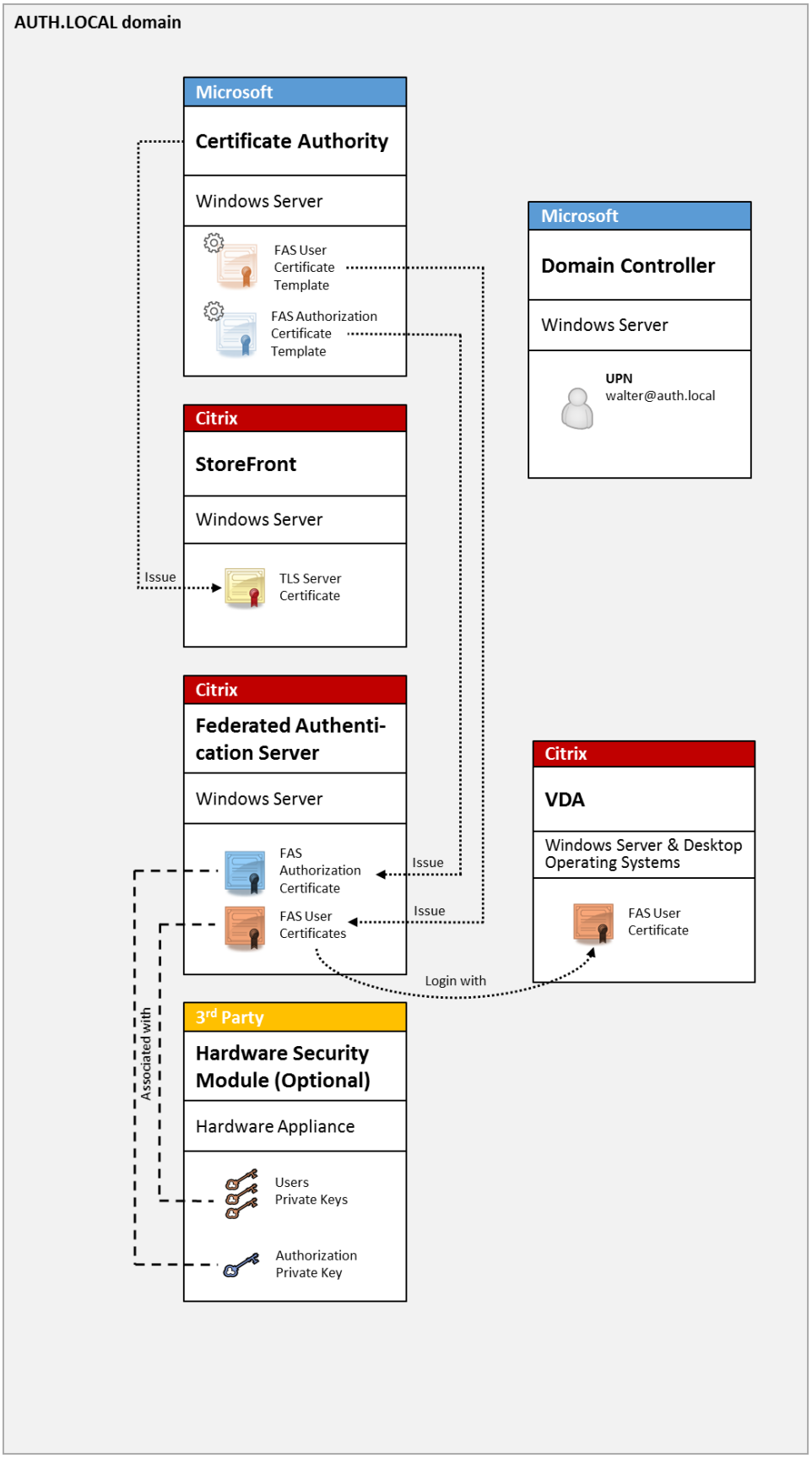
内部展開

FAS では、さまざまな認証オプション（Kerberos シングルサインオンを含む）を使用した StoreFront への安全なユーザー認証、および十分に認証された Citrix HDX セッションへの接続が可能です。

これにより、Windows 認証にユーザーの資格情報やスマートカードの PIN の入力が求められることはありません。また、シングルサインオンサービスのような「保存されたパスワードの管理」機能を使用する必要もありません。これを使用して、Citrix Virtual Apps の旧バージョンで利用可能な Kerberos 制約付き委任のログオン機能を置き換えることができます。

エンドポイントデバイスへのログオンにスマートカードを使用したかどうかにかかわらず、セッション内ではすべてのユーザーが、公開キー基盤（PKI）の証明書にアクセスできます。このため、スマートフォンやタブレットのように、スマートカードリーダーを搭載していないデバイスからも、2 要素認証モデルへの円滑な移行が可能です。

この展開では、FAS を実行する新しいサーバーが追加されますが、このサーバーにはユーザーの代わりにスマートカードクラスの証明書を発行する権限が付与されます。これらの証明書は、スマートカードによるログオンの代わりとして、Citrix HDX 環境でのユーザーセッションへのログオンに使用されます。



Citrix Virtual Apps または Citrix Virtual Desktops 環境は、CTX206156で説明するように、スマートカードによるログオンと同様の方法で構成する必要があります。

既存の展開では、通常、ドメインに参加する Microsoft 証明機関を利用可能にし、ドメインコントローラーにドメインコントローラー証明書を割り当てるだけで済みます。（CTX206156 の「Issuing Domain Controller Certificates」セクションを参照してください。）

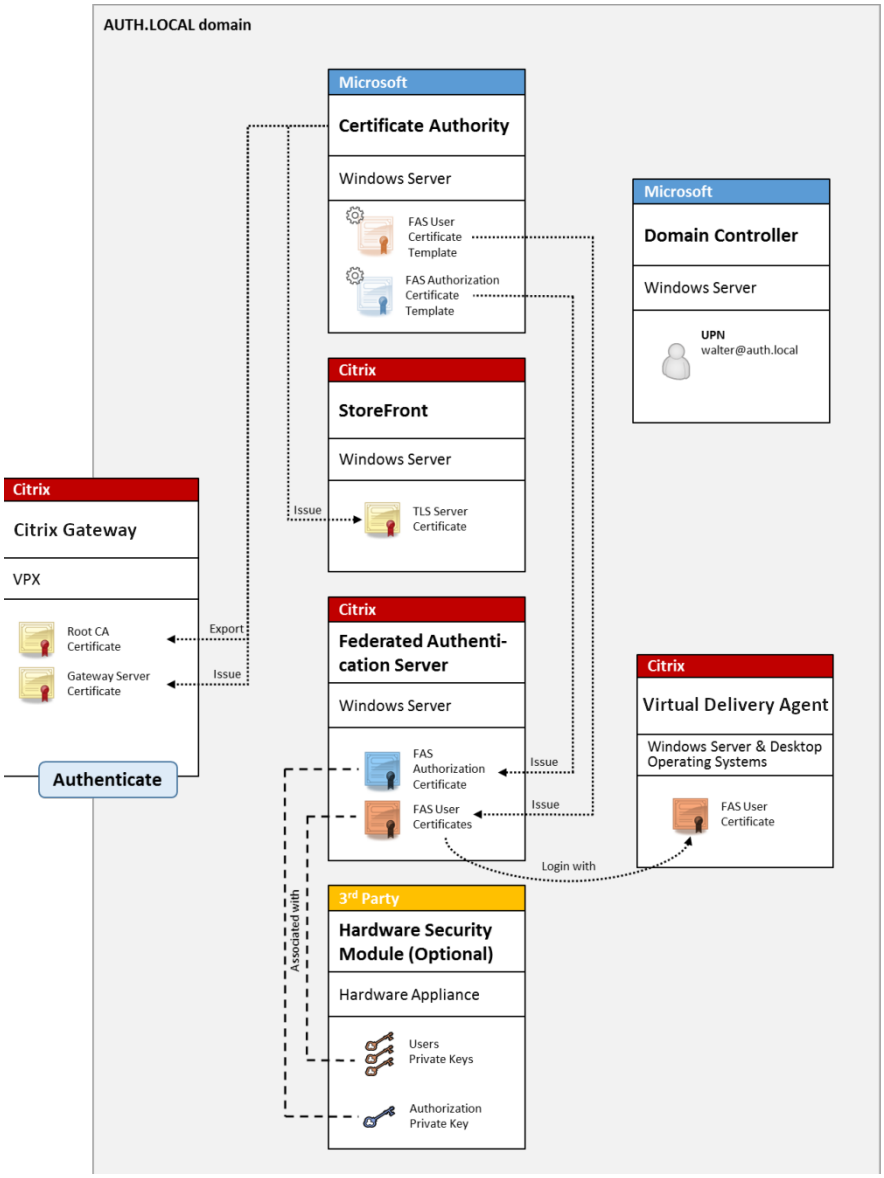
関連情報：

- キーは、ハードウェアセキュリティモジュール（HSM）やビルトインのトラステッドプラットフォームモジュール（TPM）に保存できます。詳しくは、「秘密キー保護」を参照してください。
- FAS をインストールおよび構成する方法については、「インストールと構成」を参照してください。

Citrix Gateway の展開

Citrix Gateway の展開は内部展開と似ていますが、StoreFront と組み合わせた Citrix Gateway が追加されており、認証のプライマリポイントが Citrix Gateway そのものに移動されています。Citrix Gateway には、企業 Web サイトへのリモートアクセスの保護に使用できる、認証および承認の高度なオプションが含まれています。

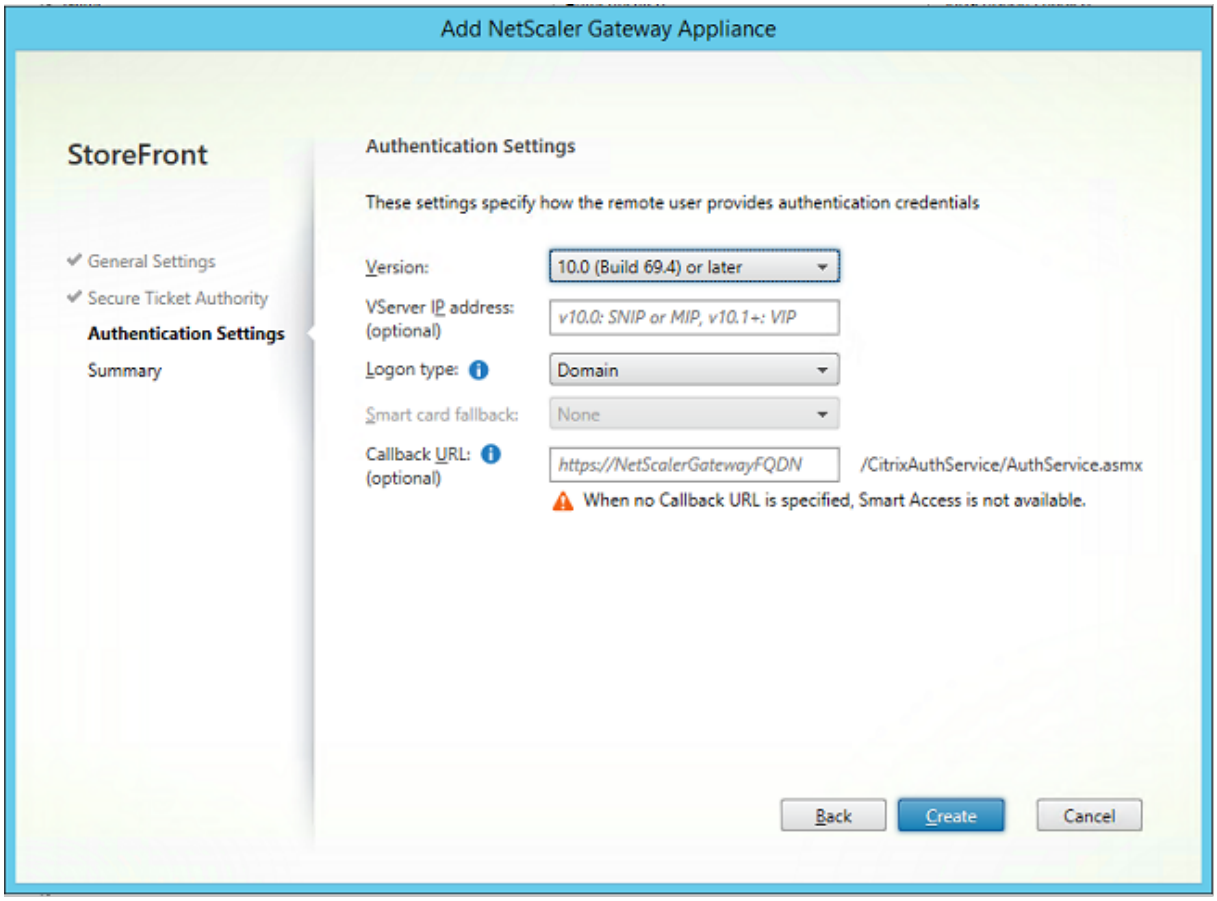
この展開を利用すれば、Citrix Gateway への初回認証時およびユーザーセッションへのログイン時に、何度も PIN の入力が求められることはありません。また、AD パスワードやスマートカードを必要とせずに、高度な Citrix Gateway 認証テクノロジを利用することができます。



Citrix Virtual Apps または Citrix Virtual Desktops 環境は、CTX206156で説明するように、スマートカードによるログオンと同様の方法で構成する必要があります。

既存の展開では、通常、ドメインに参加する Microsoft 証明機関を利用可能にし、ドメインコントローラーにドメインコントローラー証明書を割り当てるだけで済みます。(CTX206156 の「Issuing Domain Controller Certificates」セクションを参照してください。)

Citrix Gateway をプライマリ認証システムとして構成する場合は、Citrix Gateway と StoreFront 間のすべての接続を TLS で保護するようにします。特に、この展開では Citrix Gateway サーバーの認証にコールバック URL が使用されるため、コールバック URL が Citrix Gateway サーバーを指すよう正しく構成する必要があります。

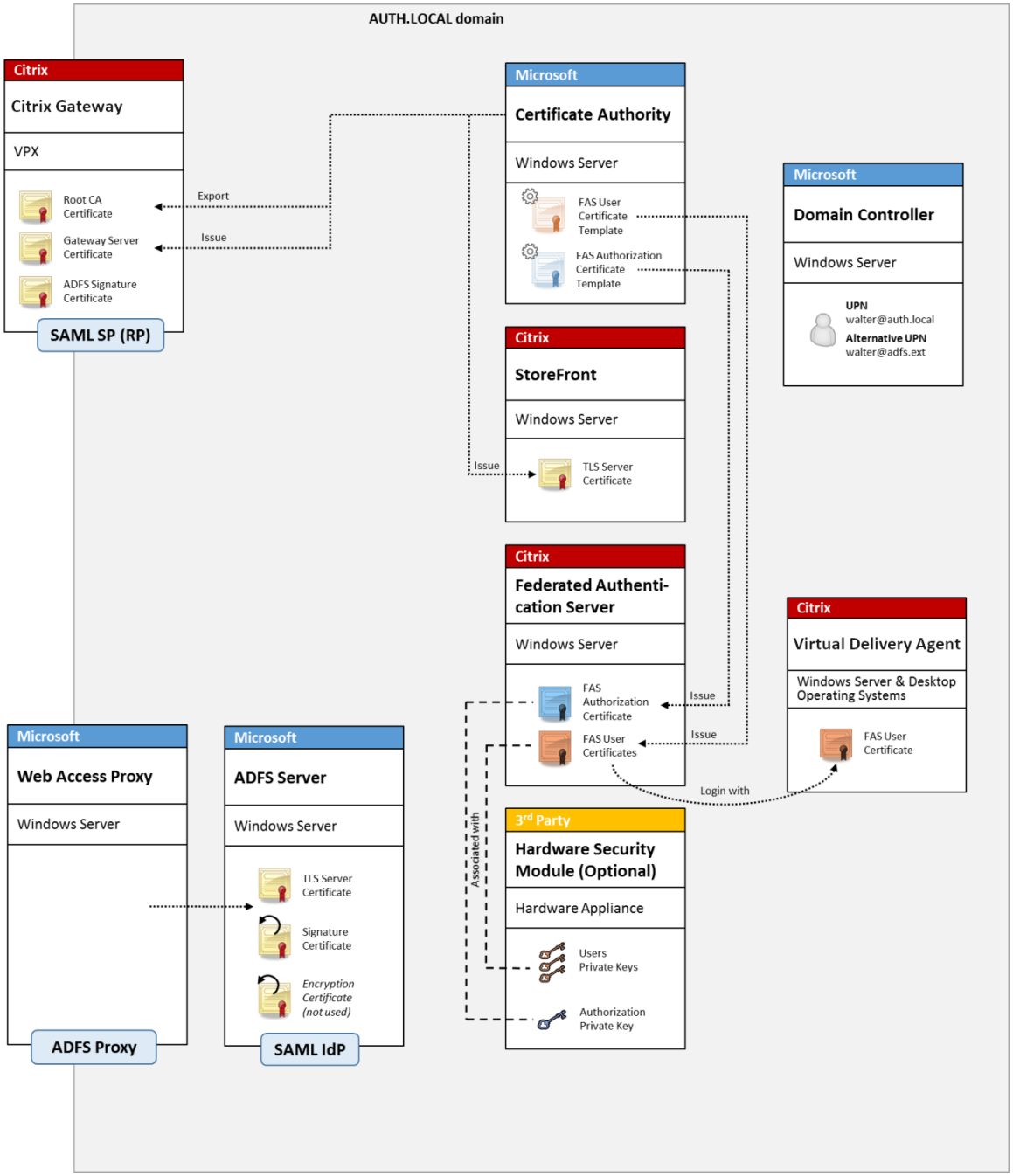


関連情報:

- Citrix Gateway を構成する方法については、『How to Configure NetScaler Gateway 10.5 to use with StoreFront 3.6 and Citrix Virtual Desktops 7.6』を参照してください。
- FAS をインストールおよび構成する方法については、「インストールと構成」を参照してください。

ADFS SAML の展開

Citrix Gateway の主要な認証テクノロジにより、SAML ID プロバイダー（IdP）として機能できる、Microsoft ADFS との統合が実現します。SAML アサーションは暗号を使用して署名された XML ブロックであり、コンピューターシステムへのユーザーのログオンを承認する、信頼された IdP によって発行されます。つまり、FAS サーバーによって、Microsoft ADFS サーバー（またはほかの SAML 対応 IdP）へのユーザー認証の委任が許可されます。



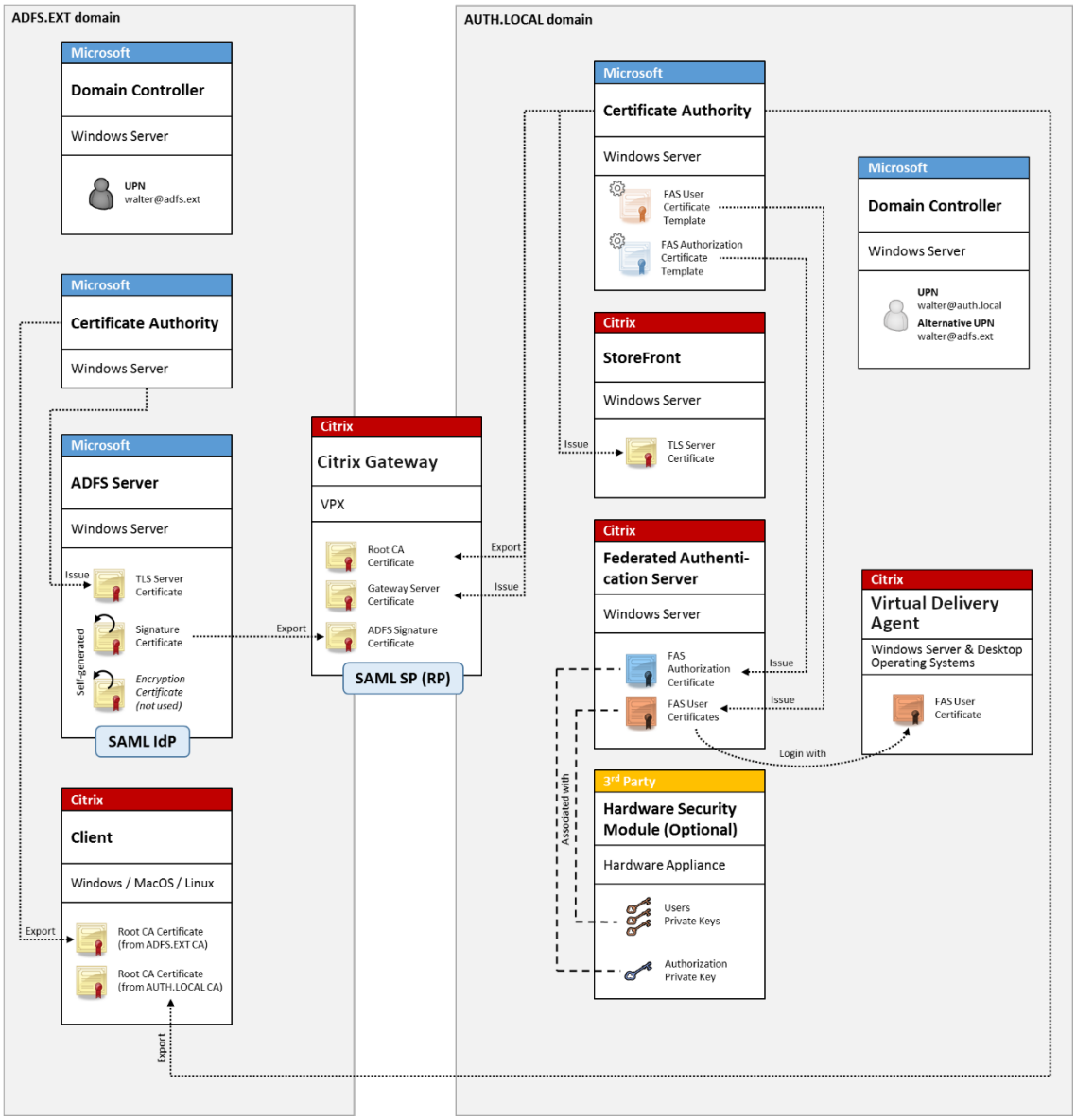
ADFS は、一般的にインターネットを利用して企業リソースにリモートでユーザーを安全に認証するために使用され、たとえば、Office 365 の統合に多く利用されます。

関連情報:

- 詳しい情報については、「ADFS の展開」を参照してください。
- FAS をインストールおよび構成する方法については、「インストールと構成」を参照してください。
- 構成に関する考慮事項については、この記事の「Citrix Gateway の展開」セクションを参照してください。

B2B アカウントのマッピング

2 つの会社が互いのコンピューターシステムを利用する場合、一般的なオプションは Active Directory フェデレーションサービス（ADFS）サーバーを信頼関係でセットアップすることです。これにより、一方の会社のユーザーが、他方の会社の Active Directory（AD）環境にシームレスに認証されるようになります。ログオン時に、各ユーザーは自社のログオン資格情報を使用します。ADFS はこれを相手の会社の AD 環境の「シャドウアカウント」に自動的にマップします。

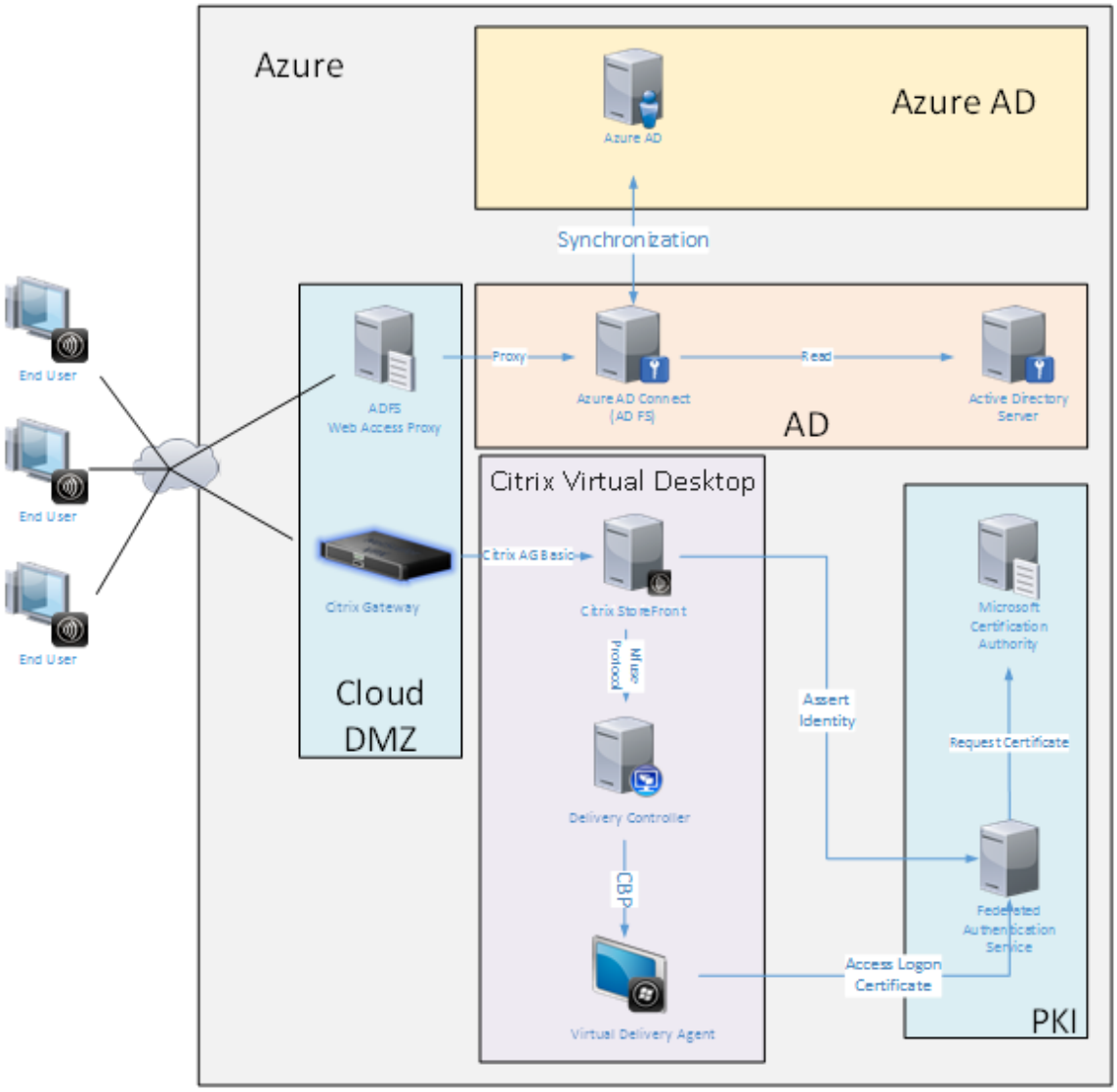


関連情報：

- FAS をインストールおよび構成する方法については、「インストールと構成」を参照してください。

Windows 10 Azure AD への参加

Windows 10 では、「Azure AD への参加」というコンセプトが導入されました。これは、従来の Windows ドメインへの参加とコンセプトが似ていますが、「インターネット上」のシナリオに焦点を当てている点が特徴です。これは、ラップトップおよびタブレットとうまく機能します。従来の Windows ドメイン参加と同様に、Azure AD には企業の Web サイトやリソースで、シングルサインオンモデルを実現する機能があります。これらはすべて「インターネットに対応」しているため、社内 LAN だけでなく、インターネットに接続したすべての場所から機能します。



この展開は、事実上「オフィスにいるエンドユーザー」という概念のない一例です。ラップトップコンピューターは最新の Azure AD 機能を使用して完全にインターネット経由で登録および認証されています。

この展開では、IP アドレスが使用可能なすべての場所、つまりオンプレミス、ホストされたプロバイダー、Azure、あるいはそのほかのクラウドプロバイダーで、インフラストラクチャが実行できる点に注意してください。Azure AD Connect の同期機能により、自動的に Azure AD に接続します。例として示した図では、簡単にするために Azure

仮想マシンを使用しています。

関連情報:

- FAS をインストールおよび構成する方法については、「インストールと構成」を参照してください。
- 詳しくは、「Azure AD の統合」を参照してください。

ADFS の展開

November 9, 2022

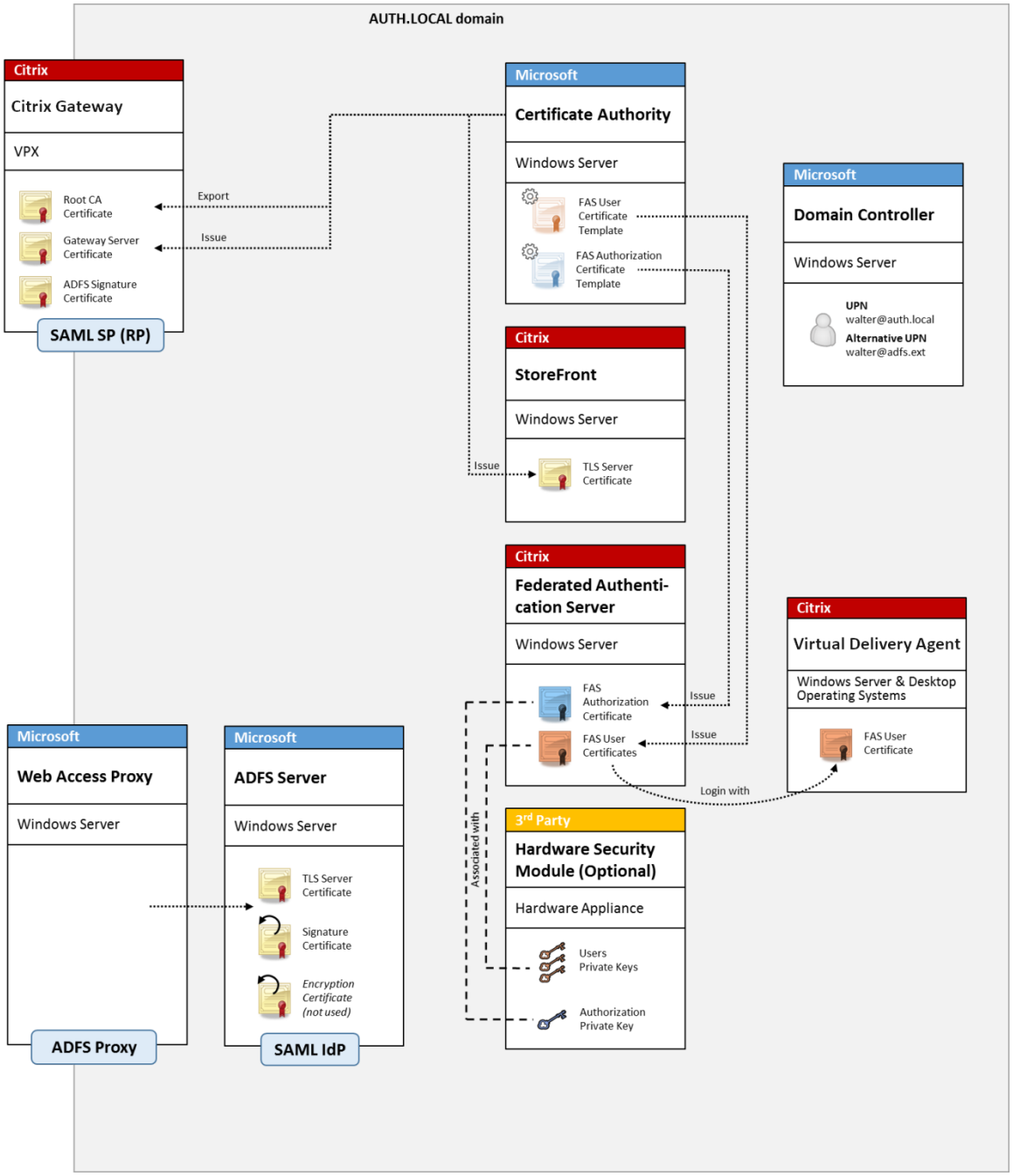
はじめに

このドキュメントでは、Citrix 環境を Microsoft ADFS と統合する方法について説明します。

ADFS は、多くの組織で単一の認証ポイントが必要な Web サイトへのセキュアなユーザーアクセスを管理するために使用されます。たとえば、従業員にとって利用可能な追加のコンテンツやダウンロードがある場合、これらの場所は、標準の Windows ログオン資格情報で保護する必要があります。

また、フェデレーション認証サービス（FAS: Federated Authentication Service）では、Citrix Gateway および Citrix StoreFront を ADFS のログオンシステムに統合できるため、企業担当者が混乱する可能性が減少します。

この展開で、Citrix Gateway は Microsoft ADFS の証明書利用者として統合されます。



> 注:
>
> バックエンドリソースが Windows VDA か Linux VDA のいずれかである場合、違いはありません。

SAML の概要

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、シンプルな「ログオンページへのリダイレクト」を実現する、Web ブラウザーのログオンシステムです。構成には次の項目が含まれます。

リダイレクト **URL**［シングルサインオンサービス **URL**］

ユーザー認証の必要があることを Citrix Gateway が検出すると、NetScaler はユーザーが使用する Web ブラウザーに、ADFS サーバー上の SAML ログオン Web ページに HTTP POST を実行するよう指示します。この URL は通常、次の形式の`https://`アドレスです: `https://adfs.mycompany.com/adfs/ls`。

この Web ページの POST には、ログオン完了時に ADFS がユーザーを返す「リターンアドレス」などの情報も含まれます。

識別子［発行者名**/EntityID**］

EntityId は、Citrix Gateway が ADFS に送信する POST データに含まれる一意の識別子です。EntityId は ADFS に、ユーザーがどのサービスにログオンしようとしているかを知らせ、必要に応じてさまざまな認証ポリシーが適用されるようにします。発行されると、SAML 認証 XML は、EntityId の識別したサービスへのログオンのみに使用されます。

通常、EntityID は Citrix Gateway サーバーのログオンページの URL ですが、一般的には、Citrix Gateway および ADFS から認められればどのような URL も使用できます（例: `https://ns.mycompany.com/application/logonpage`）。

リターンアドレス［応答 **URL**］

認証に成功すると、ADFS はユーザーの Web ブラウザーに、EntityID で構成された応答 URL の 1 つに、SAML 認証 XML を POST し返すよう指示します。この URL は、通常は元の Citrix Gateway サーバー上での次の形式の`https://`アドレスです: `https://ns.mycompany.com/cgi/samlauth`。

構成された応答 URL アドレスが複数ある場合、Citrix Gateway は ADFS への元の POST 内にある 1 つを選択できます。

署名証明書［**IDP** 証明書］

ADFS は秘密キーを使用して、SAML 認証 XML BLOB に暗号で署名します。この署名を検証するには、Citrix Gateway を構成し、証明書ファイルに含まれる公開キーを使用して、これらの署名を確認する必要があります。証明書ファイルは、通常、ADFS サーバーから取得されるテキストファイルです。

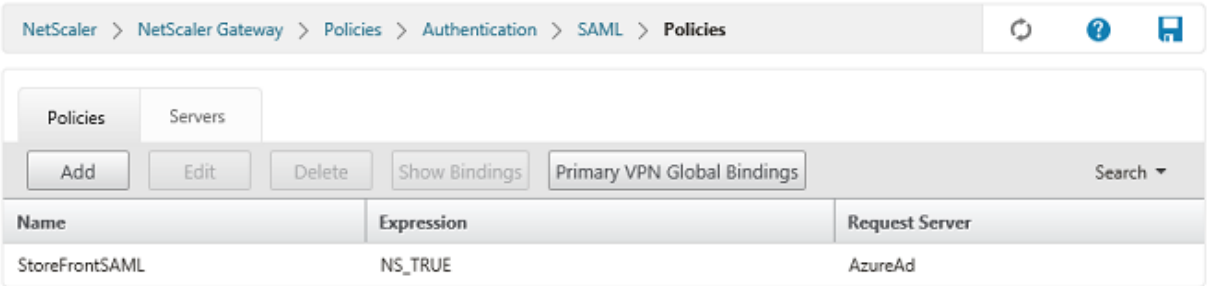
シングルサインアウト **URL**［シングルログアウト **URL**］

ADFS および Citrix Gateway は、「中央ログアウト」システムをサポートしています。これは Citrix Gateway がポーリングすることがある URL であり、SAML 認証 XML BLOB が現在ログオン中のセッションをまだ示していることを確認します。

これは、構成する必要がないオプション機能です。この URL は通常、次の形式の`https://`アドレスです: `https://adfs.mycompany.com/adfs/logout`。（シングルログオン URL と同じ場合があることに注意してください。）

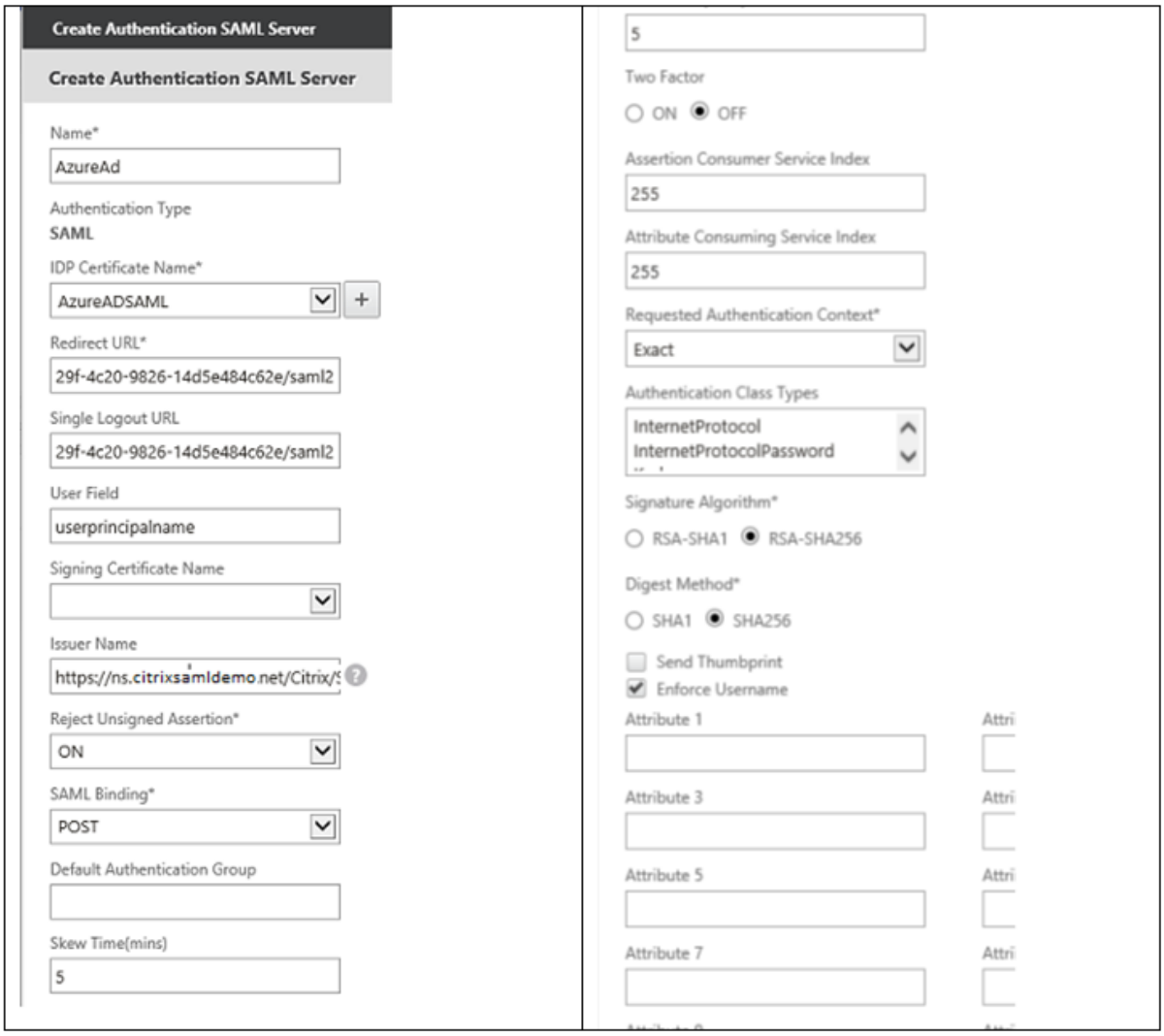
構成

セクション「Citrix Gateway の展開」では、Citrix Gateway をセットアップし、標準的な LDAP 認証オプションを処理する方法について説明します。これが正常に完了すると、SAML 認証を許可する Citrix Gateway で、新しい認証ポリシーを作成することができます。その後、Citrix Gateway ウィザードで使用されたデフォルトの LDAP ポリシーを置き換えることができます。



SAML ポリシーの記入

ADFS 管理コンソールから前に取得した情報を使用して、新しい SAML IdP サーバーを構成します。このポリシーが適用されると、Citrix Gateway はログオンのためにユーザーを ADFS-signed にリダイレクトし、ADFS の署名した SAML 認証トークンを代わりに受け取ります。



関連情報

- FAS のインストールと構成については、「インストールと構成」を参照してください。
- 一般的な FAS の展開については、「展開アーキテクチャ」を参照してください。
- 具体的な手順については、「詳細な構成」を参照してください。

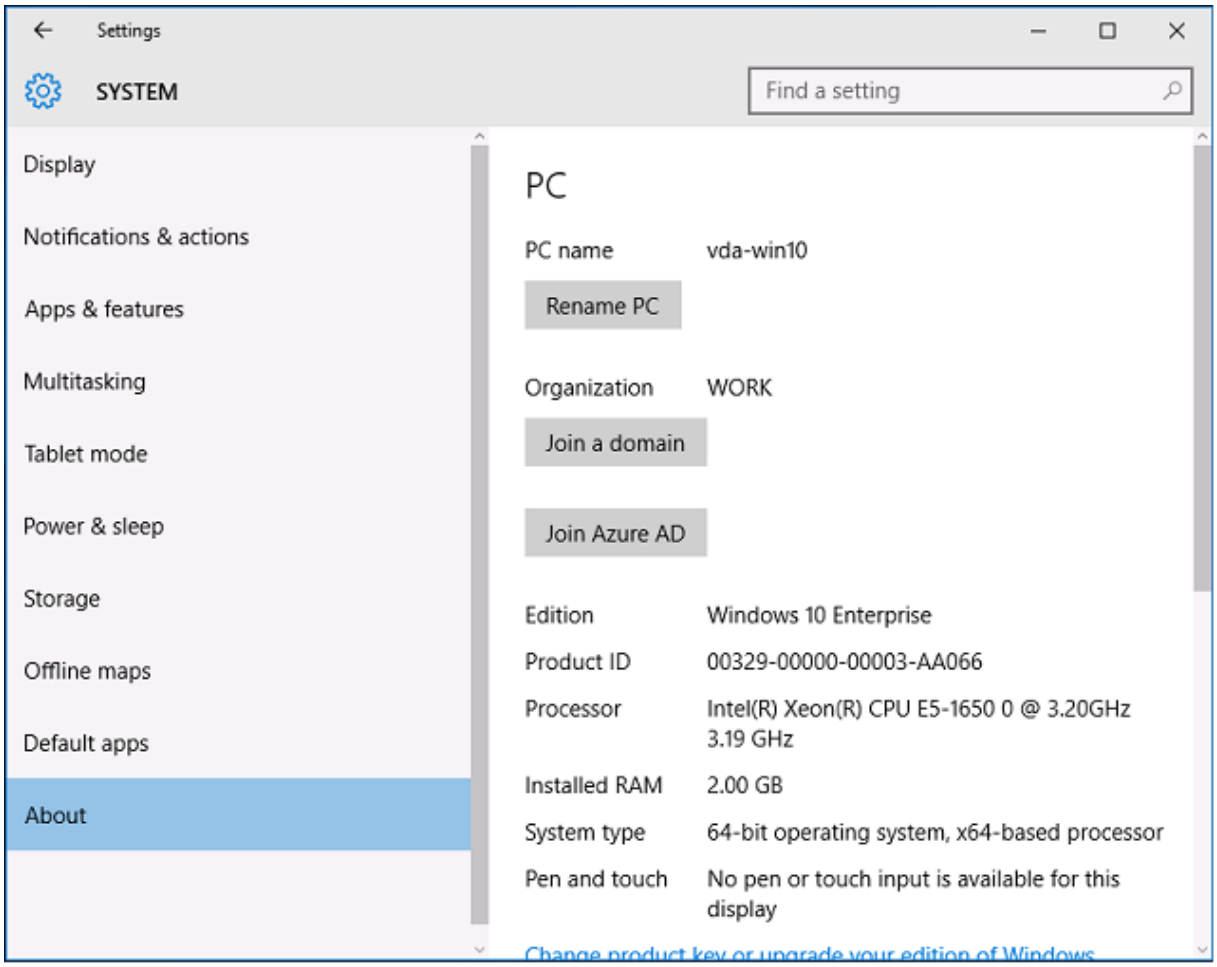
Azure AD の統合

November 9, 2021

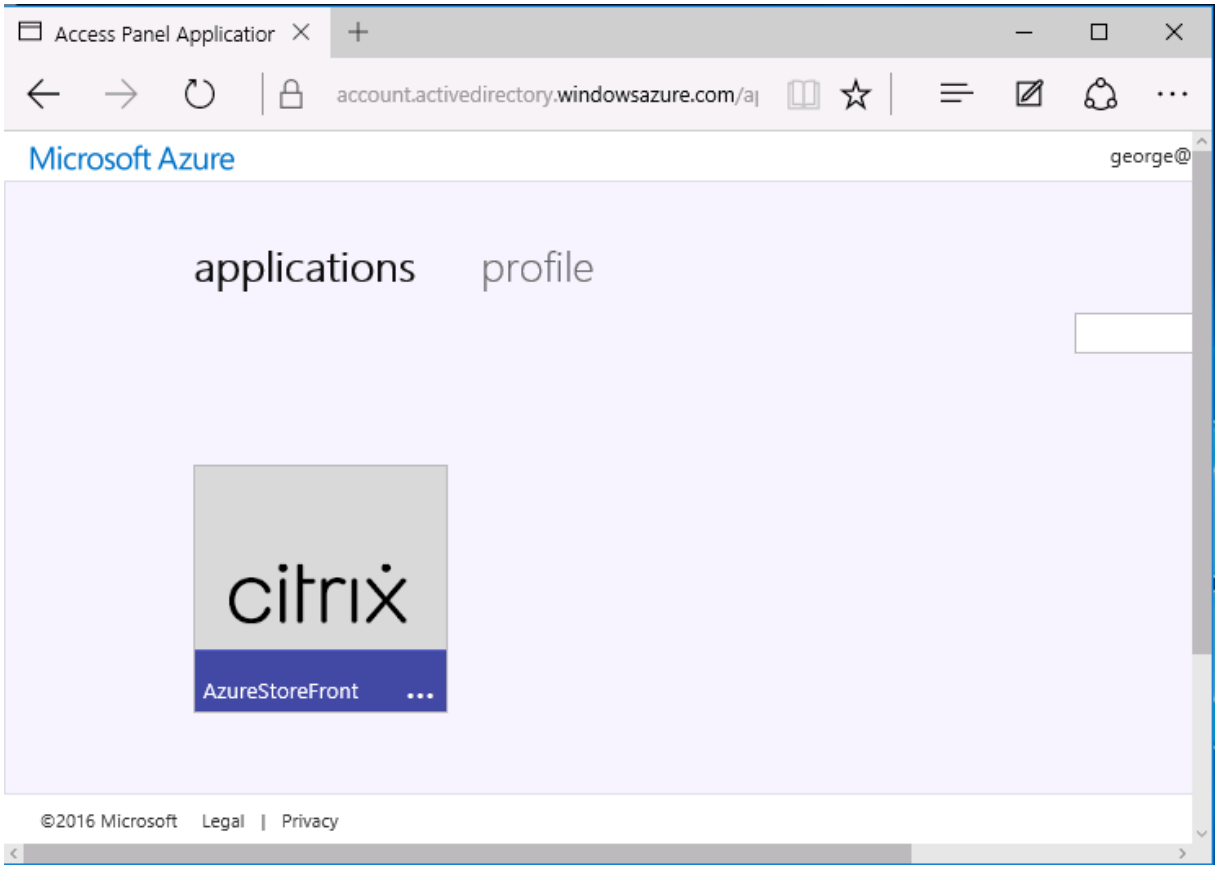
はじめに

このドキュメントでは、Citrix 環境を Windows 10 Azure AD 機能と統合する方法について説明します。Windows 10 が導入した Azure AD は、ドメイン参加の新しいモデルです。これを利用すれば、管理とシングルサインオンの目的で、ローミングラップトップを、インターネット上で企業ドメインに参加させることができます。

このドキュメントで例として示した展開では、新規ユーザーの Windows 10 ラップトップに会社のメールアドレスと登録コードが提供されるシステムを説明しています。ユーザーは ［設定］パネルの ［システム］**>**［バージョン情報］**>**［**Azure AD** に参加］から、このコードにアクセスします。



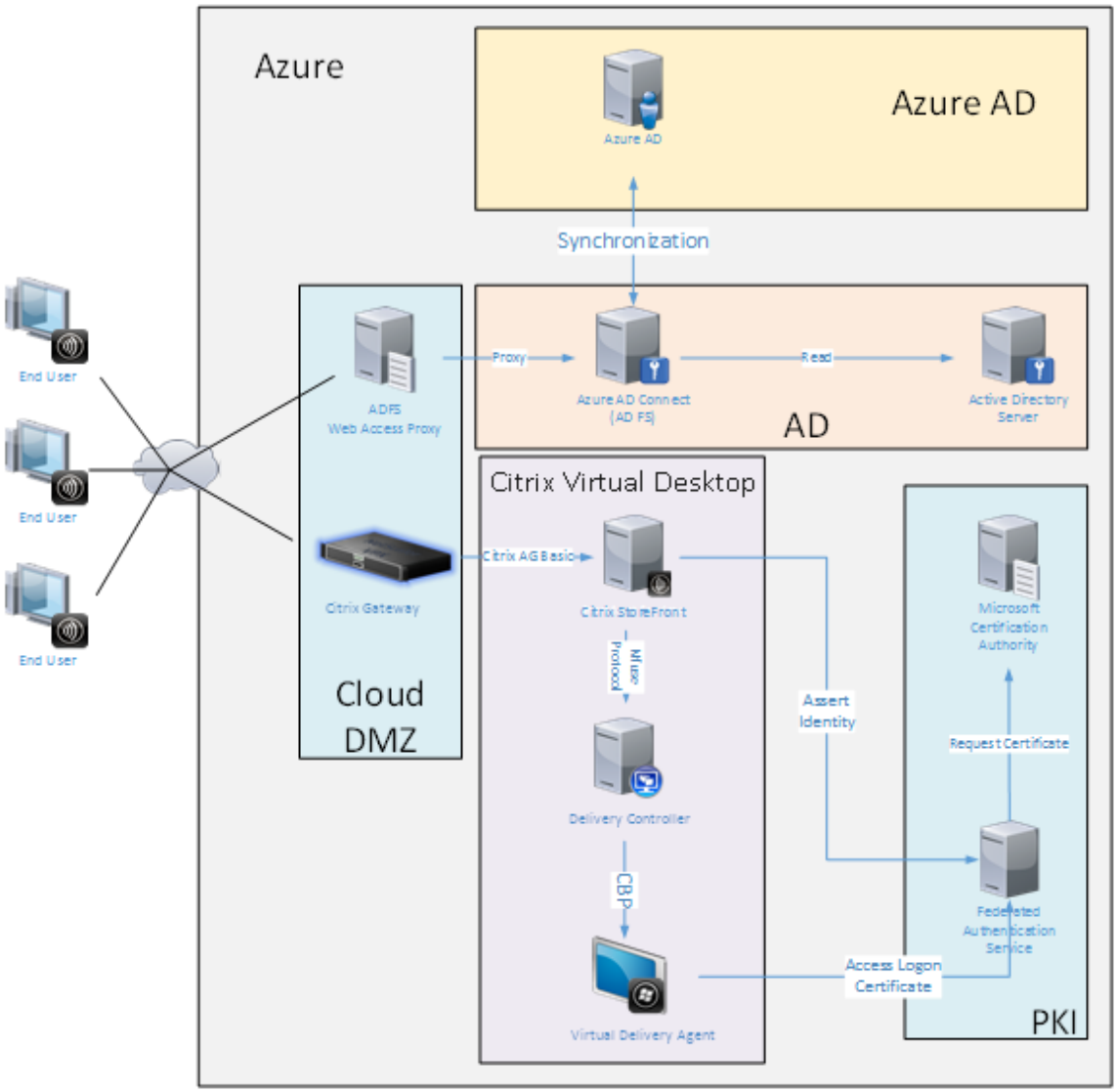
ラップトップが登録されると、Microsoft Edge の Web ブラウザーは、Azure SaaS アプリケーションの Web ページから、会社の Web サイトや Citrix の公開アプリケーション、および Office 365 などの Azure アプリケーションに自動的にサインオンします。



アーキテクチャ

このアーキテクチャでは、Azure AD や Office 365 などの最新クラウドテクノロジとの統合により、従来の企業ネットワークが Azure 内に完全に複製されます。すべてのエンドユーザーがリモートワーカーと見なされ、社内イントラネット上にはエンドユーザーが存在しないというコンセプトです。

Azure AD Connect の同期サービスが、インターネット上で Azure への橋渡しとして機能するため、既存のオンプレミスシステムを持つ企業はこのモデルを適用することができます。



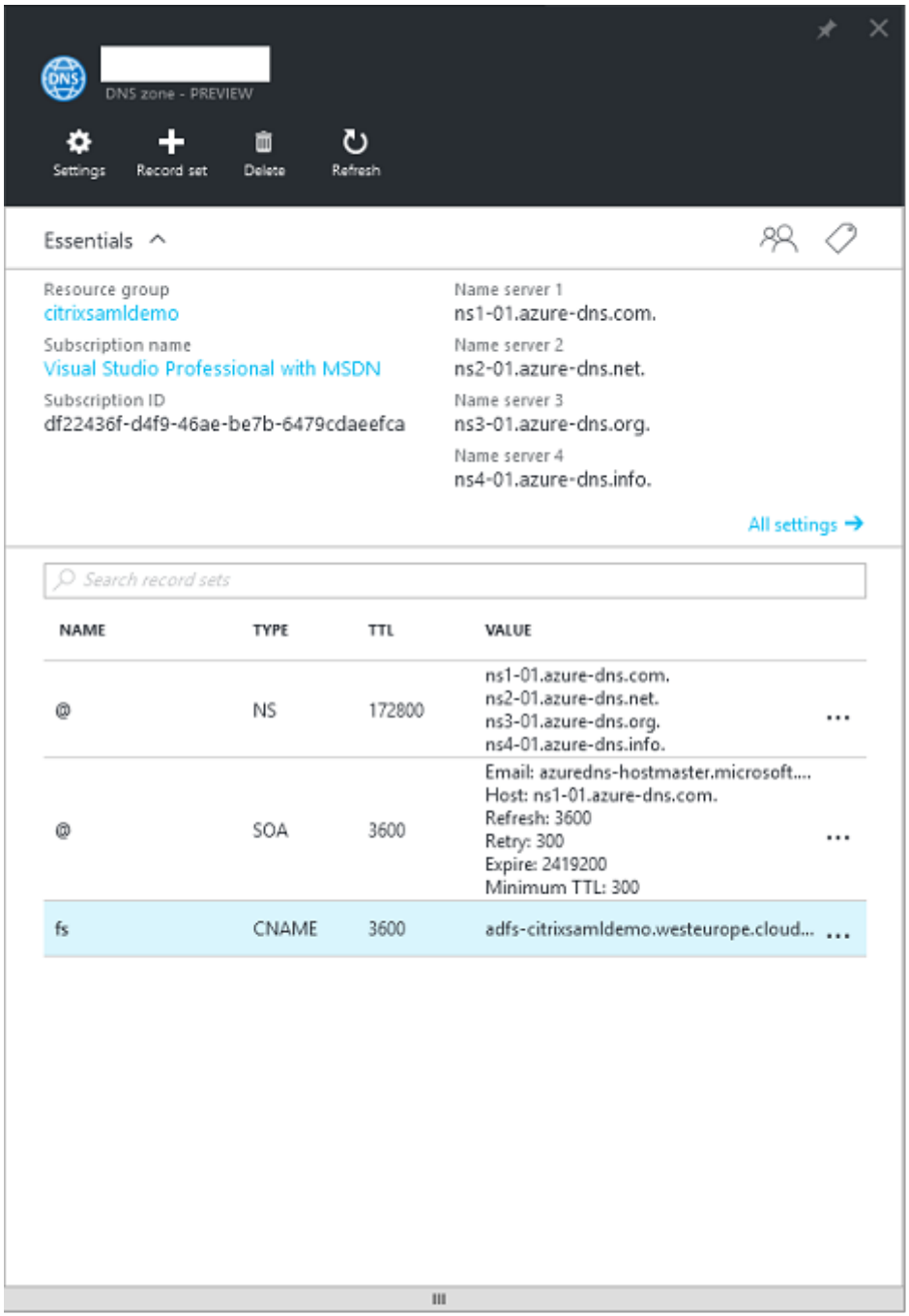
セキュアな接続やシングルサインオンといえば、従来はファイアウォールで保護された LAN や、Kerberos 認証および NTLM 認証でしたが、このアーキテクチャでは、Azure への TLS 接続および SAML がこれらに取って代わります。Azure アプリケーションの Azure AD への参加により、新しいサービスが生み出されています。Active Directory を必要とする既存のアプリケーション（SQL Server データベースなど）は、Azure クラウドサービスの IaaS 部分にある、標準的な Active Directory サーバーの仮想マシンを使用して実行できます。

ユーザーが従来のアプリケーションを起動すると、Citrix Virtual Apps and Desktops の公開アプリケーションを使用してアクセスします。Microsoft Edge のシングルサインオン機能を使用して、ユーザーの［**Azure** アプリケーション］ページからさまざまな種類のアプリケーションが照合されます。また、Microsoft は、Azure アプリケーションの一覧表示と起動ができる Android および iOS アプリを提供しています。

DNS ゾーンの作成

Azure AD では、管理者がパブリック DNS アドレスを登録し、ドメイン名サフィックスの委任ゾーンを管理する必要があります。これを実行するために、管理者は Azure DNS ゾーン機能を使用できます。

この例では、DNS ゾーン名 *citrixsamldemo.net* を使用します。



コンソールに Azure DNS ネームサーバーの名前が表示されます。これらは、ゾーンの DNS 登録の NS エントリで参照する必要があります（例: `citrixsamldemo.net. NS n1-01.azure-dns.com`）。

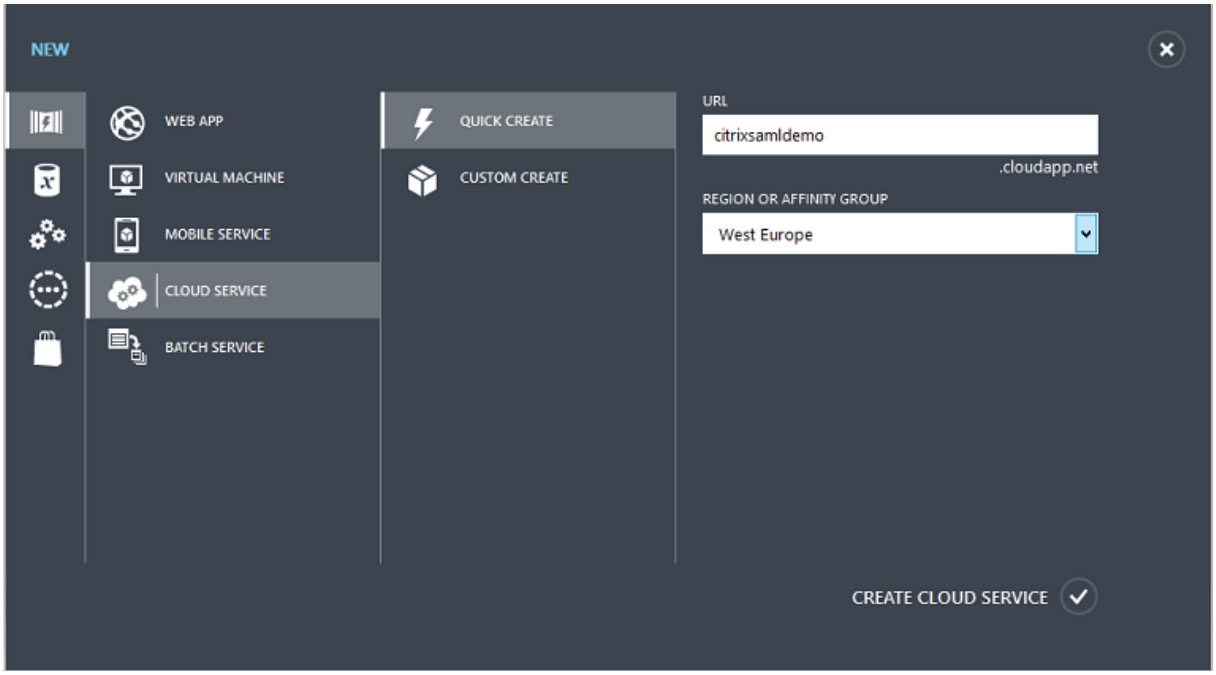
Azure で実行される仮想マシンへの参照を追加する場合は、CNAME ポインターを、Azure が管理する仮想マシンの DNS レコードに使用するのが最も簡単です。仮想マシンの IP アドレスが変更されている場合は、DNS ゾーンファイルを手動で更新する必要はありません。

内部および外部の DNS アドレスサフィックスは、この展開に一致します。ドメインは citrixsamldemo.net で、スプリット DNS（内部で 10.0.0.*）を使用します。

Web アプリケーションプロキシサーバーを参照する、「fs.citrixsamldemo.net」エントリを追加します。これがこのゾーンのフェデレーションサービスです。

クラウドサービスの作成

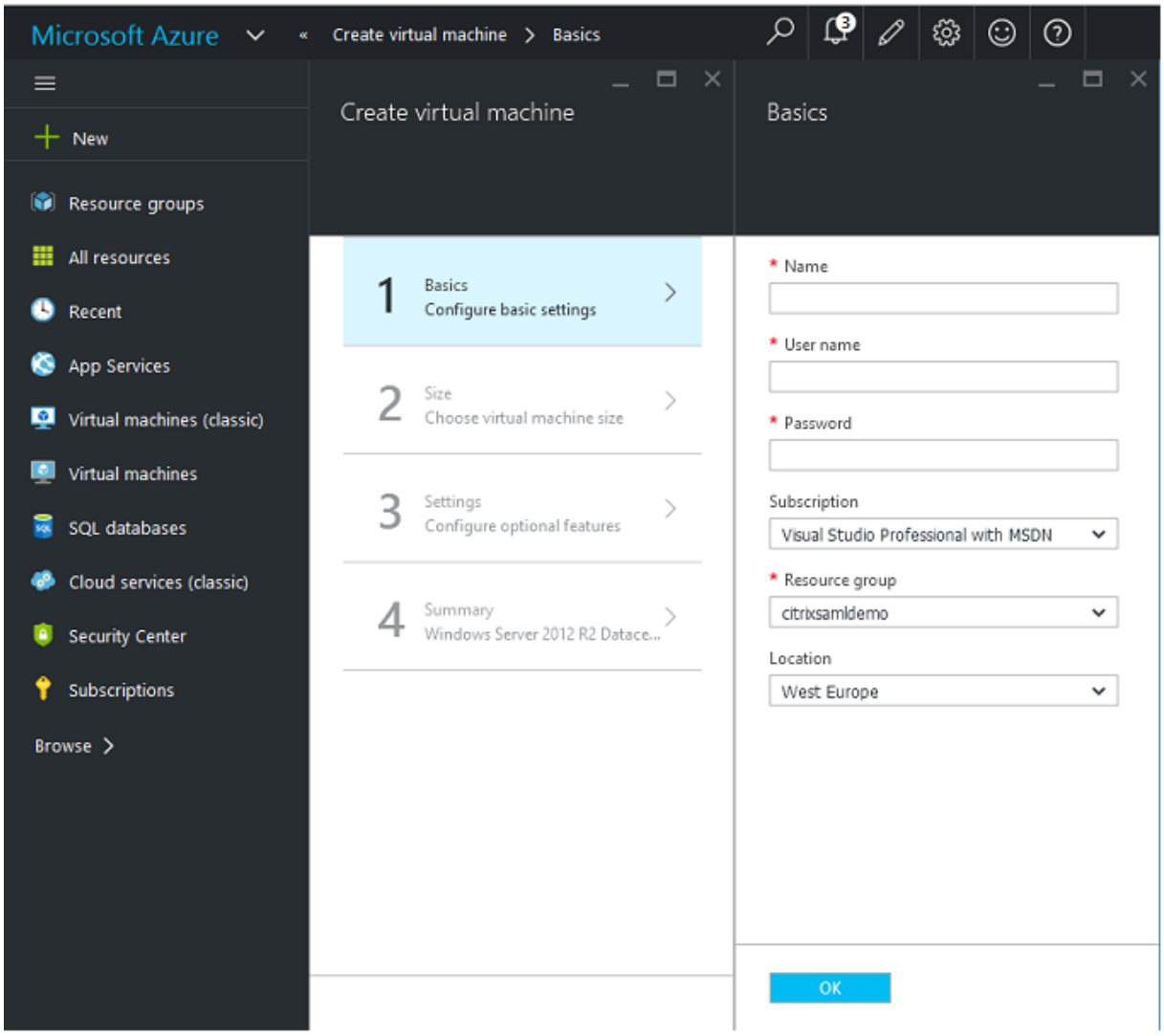
この例では、Azure で実行される ADFS サーバーが設置された AD 環境を含む、Citrix 環境を構成します。クラウドサービスを作成し、「citrixsamldemo」と名づけます。



Windows 仮想マシンの作成

クラウドサービスで実行される Windows 仮想マシンを 5 台作成します。

- ドメインコントローラー（domaincontrol）
- Azure Connect ADFS サーバー（adfs）
- ADFS Web アクセスプロキシ（ドメインに参加していない Web アプリケーションプロキシ）
- Citrix Virtual Apps and Desktops の Delivery Controller
- Citrix Virtual Apps and Desktops Virtual Delivery Agent（VDA）



ドメインコントローラー

- **DNS** サーバーおよび **Active Directory** ドメインサービスの役割を追加し、標準的な Active Directory 展開を作成します（この例では、citrixsamldemo.net）。ドメインの昇格が完了したら、**Active Directory** 証明書サービスの役割を追加します。
- テスト用に通常のユーザーアカウントを作成します（例：George@citrixsamldemo.net）。
- このサーバーでは内部 DNS が実行されるため、すべてのサーバーは DNS 解決にこのサーバーを参照する必要があります。これは、［**Azure DNS** 設定］ページで行います。（詳しくは、このドキュメントの付録を参照してください。）

ADFS コントローラーと **Web** アプリケーションプロキシサーバー

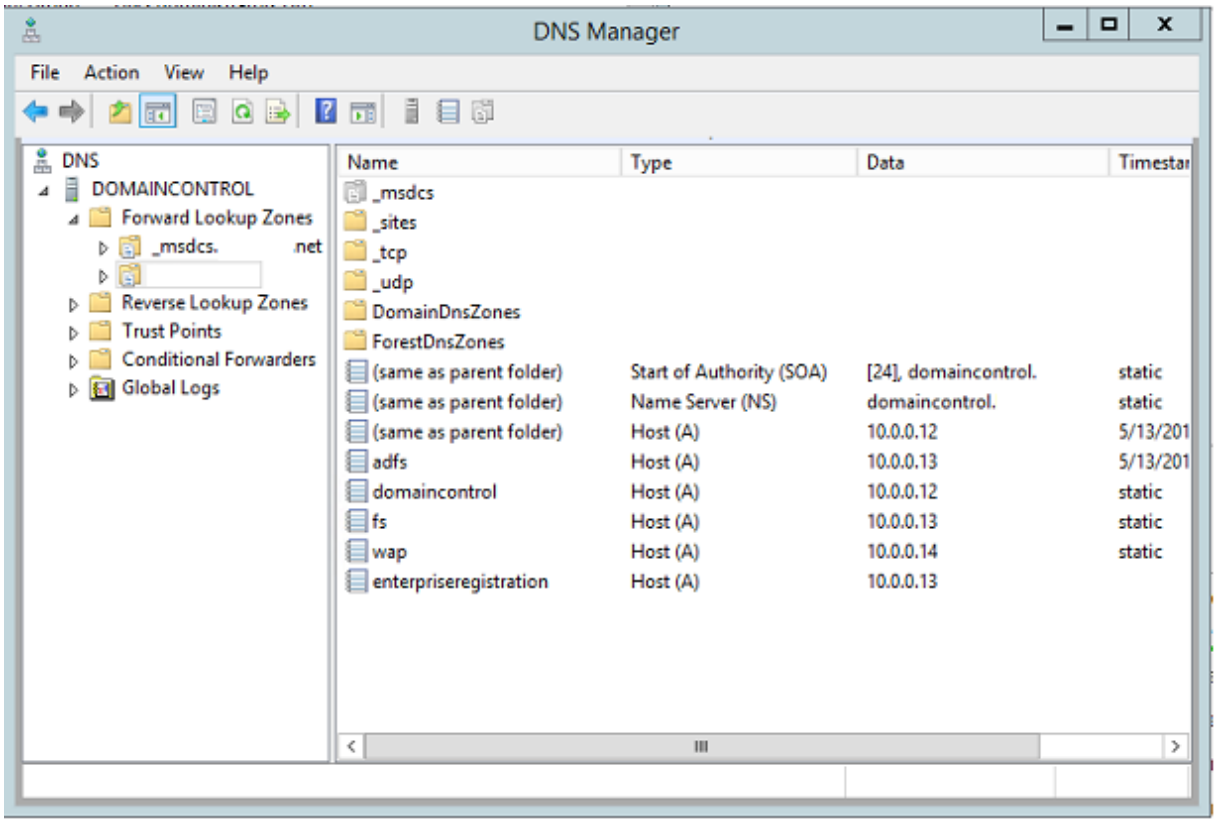
- ADFS サーバーを citrixsamldemo ドメインに参加させます。Web アプリケーションプロキシサーバーは、分離されたワークグループにとどまる必要があるため、AD DNS で DNS アドレスを手動で登録します。
- これらのサーバーで **Enable-PSRemoting –Force** コマンドレットを実行して、Azure AD Connect ツールからファイアウォール経由の PS リモーティングを有効にします。

Citrix Virtual Desktops の **Delivery Controller** と **VDA**

- Citrix Virtual Apps または Citrix Virtual Desktops の Delivery Controller と VDA を、citrixsamldemo に参加した残り 2 台の Windows サーバーにインストールします。

内部 **DNS** の構成

ドメインコントローラーのインストール後に DNS サーバーを構成し、citrixsamldemo.net の内部ビューを処理し、外部 DNS サーバーに対してフォワーダーとして機能するように設定します（例：8.8.8.8）。

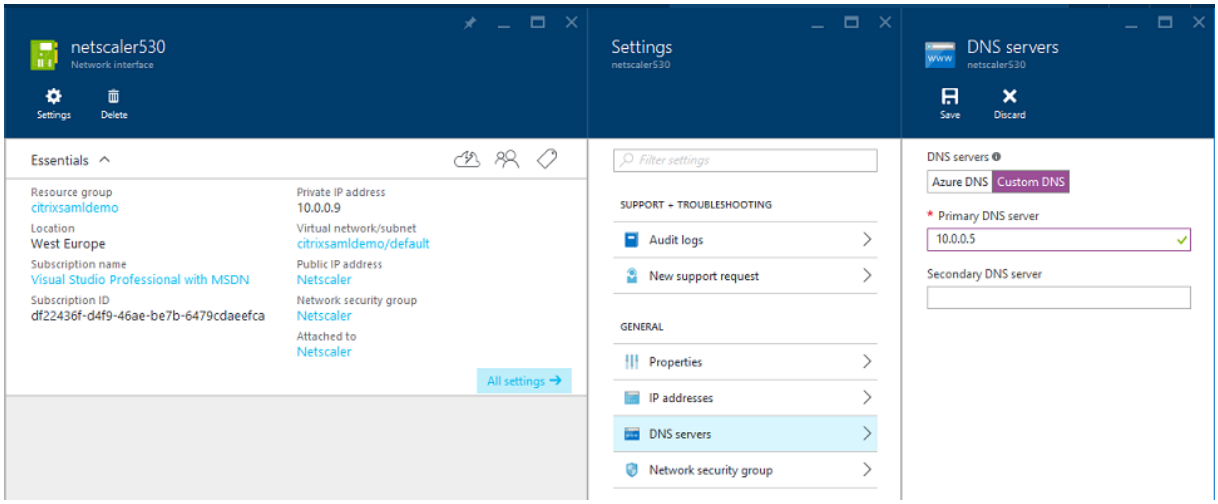


静的なレコードを追加します。

- wap.citrixsamldemo.net [Web アプリケーションプロキシの仮想マシンはドメインに参加しません]
- fs.citrixsamldemo.net [内部フェデレーションサーバーのアドレス]

- enterpriseregistration.citrixsaml.net [fs.citrixsamldemo.net と同じ]

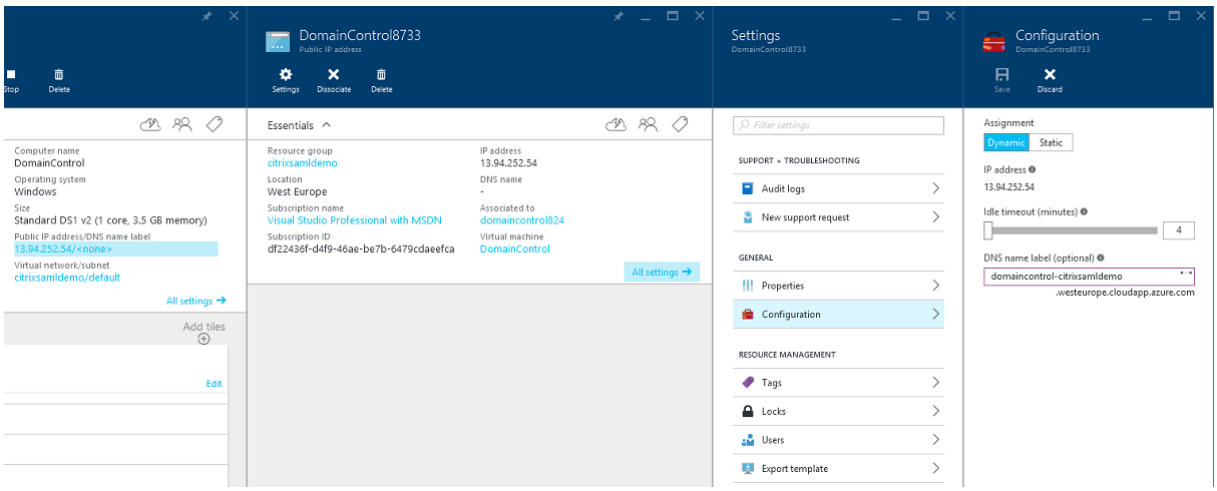
Azure で実行されるすべての仮想マシンは、この DNS サーバーのみを使用するように構成する必要があります。これは、ネットワークインターフェイス GUI から実行できます。



デフォルトでは、内部 IP（10.0.0.9）アドレスは動的に割り当てられます。IP アドレスの設定を使用して、IP アドレスを永続的に割り当てることができます。これは、Web アプリケーションプロキシサーバーとドメインコントローラーで実行する必要があります。

外部 **DNS** アドレスの構成

仮想マシン実行時に、Azure は、仮想マシンに割り当てられた現在のパブリック IP アドレスを指す自身の DNS ゾーンサーバーを維持します。Azure はデフォルトで各仮想マシンの起動時に IP アドレスを割り当てるため、この便利な機能を有効にします。

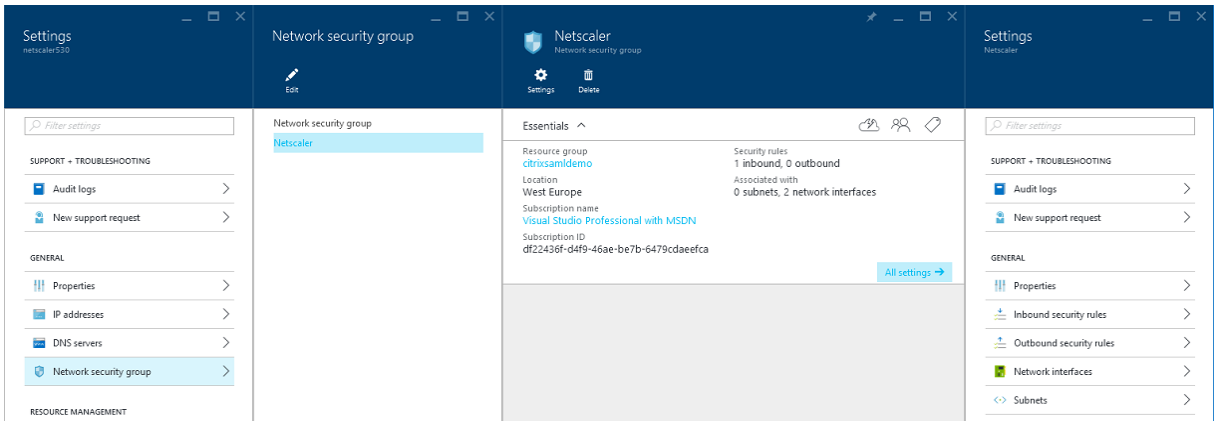


この例では、DNS アドレス domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com を、ドメインコントローラーに割り当てています。

リモート構成の完了時にパブリック IP アドレスを有効にする必要があるのは、Web アプリケーションプロキシと Citrix Gateway 仮想マシンだけである点に注意してください。（構成では、環境への RDP アクセスにパブリック IP アドレスが使用されます）。

セキュリティグループの構成

Azure クラウドは、セキュリティグループを使用して、インターネットから仮想マシンへの TCP および UDP アクセスのファイアウォールルールを管理します。デフォルトでは、すべての仮想マシンで RDP アクセスが許可されます。また、Citrix Gateway および Web アプリケーションプロキシサーバーでは、ポート 443 で TLS を許可する必要があります。

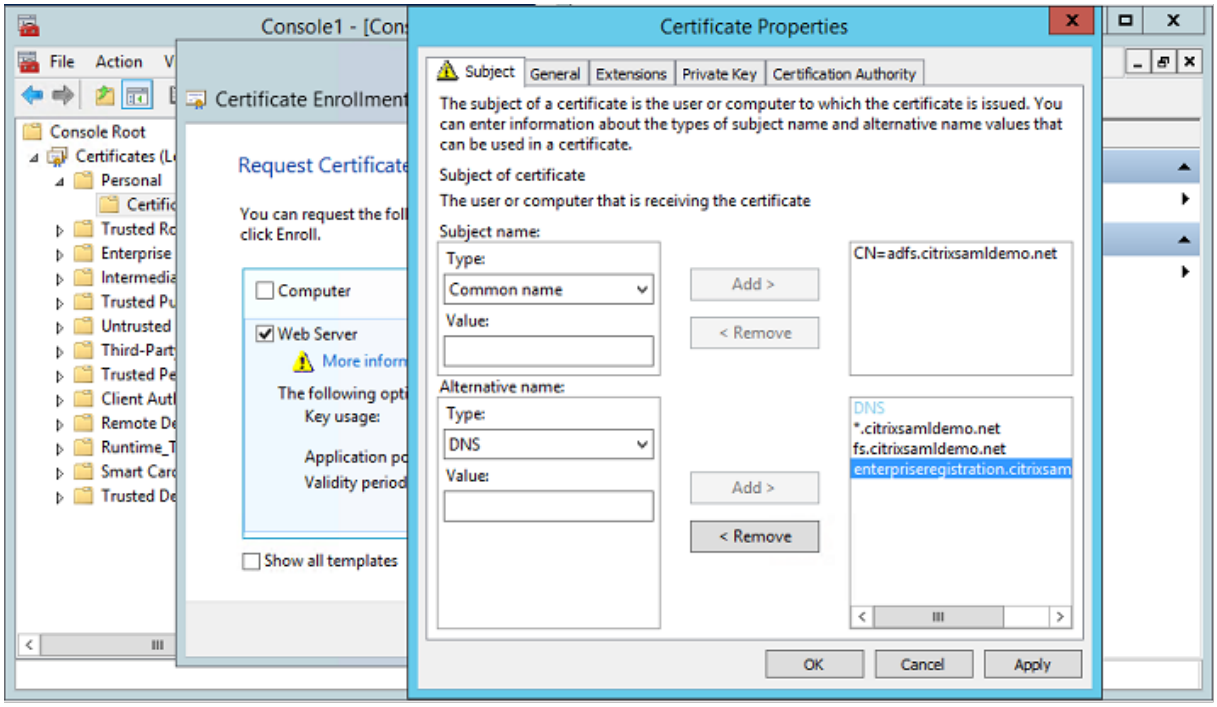


ADFS 証明書の作成

Microsoft 証明機関で **Web** サーバー証明書テンプレートを有効にします。これにより、PFX ファイルにエクスポート（秘密キーも含む）できる、カスタム DNS アドレスを持つ証明書を作成できます。PFX ファイルを優先オプションにするには、この証明書を ADFS と Web アプリケーションプロキシサーバーの両方にインストールする必要があります。

次のサブジェクト名を使用して、Web サーバー証明書を発行します。

- Commonname:
  - adfs.citrixsamldemo.net [コンピューター名]
- SubjectAltname:
  - *.citrixsamldemo.net [ゾーン名]
  - fs.citrixsamldemo. net [DNS のエントリ]
  - enterpriseregistration.citrixsamldemo.net



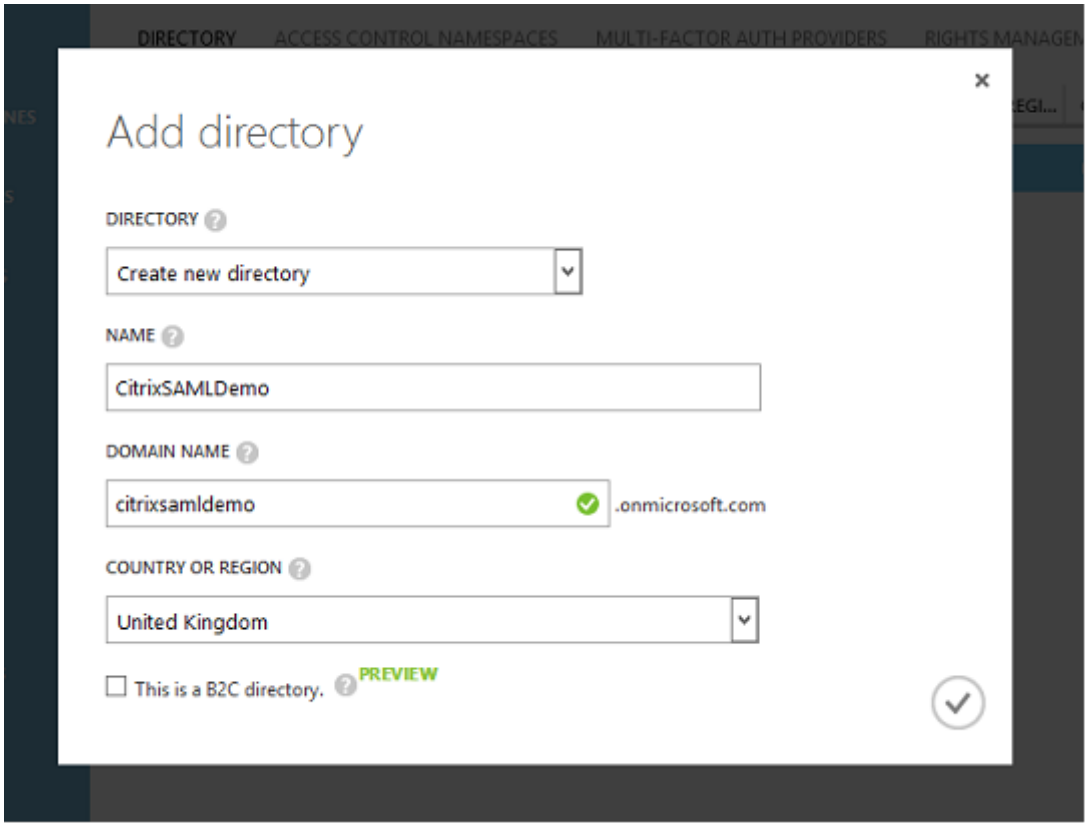
パスワードで保護された秘密キーを含め、証明書を PFX ファイルにエクスポートします。

Azure AD のセットアップ

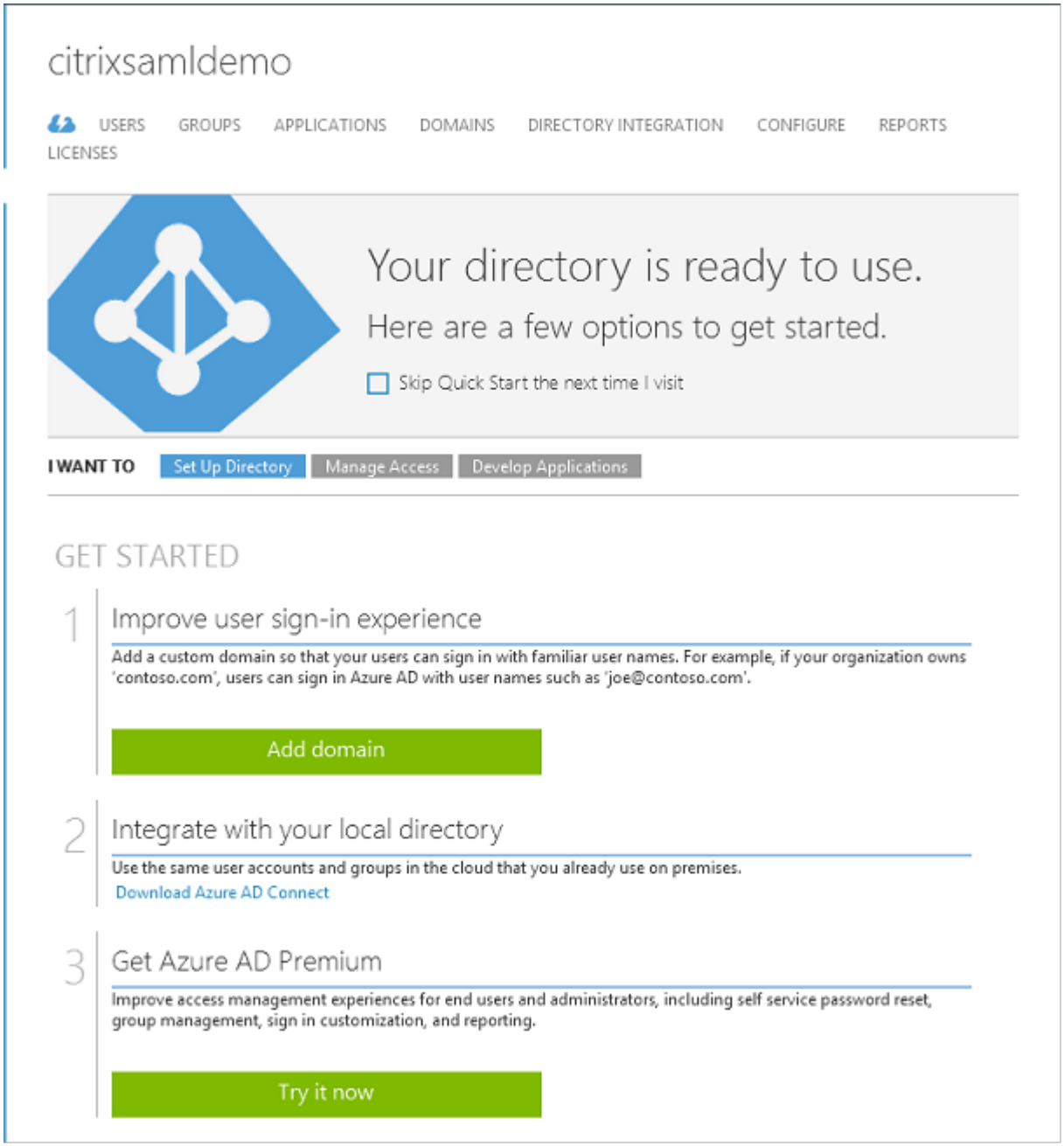
このセクションでは、新しい Azure AD インスタンスをセットアップして、Windows 10 を Azure AD に参加させるために使用できるユーザー ID を作成する方法について説明します。

新しいディレクトリの作成

Azure クラシックポータルにログオンして、新しいディレクトリを作成します。

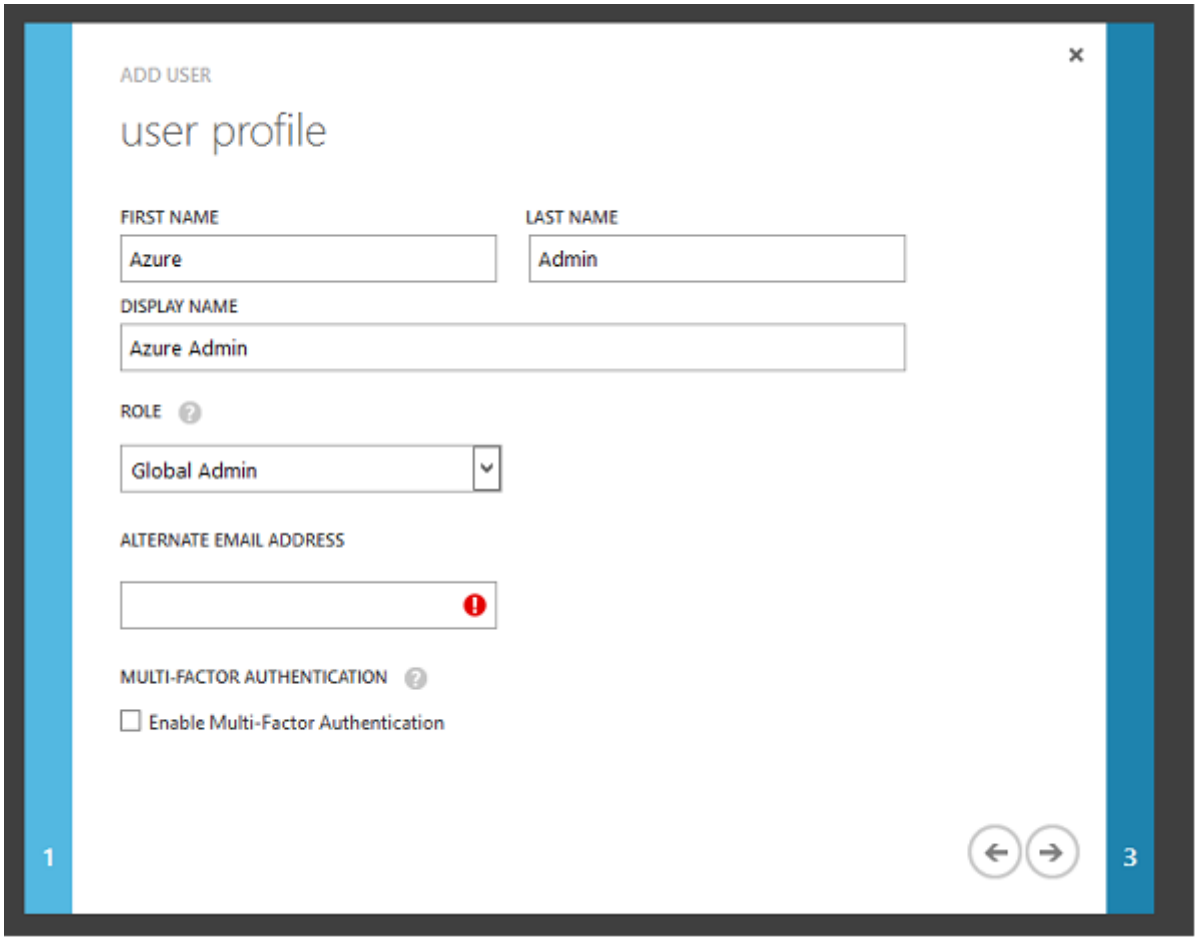


完了すると、概要ページが表示されます。



グローバル管理者ユーザー（**AzureAdmin**）の作成

Azure でグローバル管理者を作成し（この例では`AzureAdmin@citrixsamldemo.onmicrosoft.com`）、この新しいアカウントでログオンしてパスワードを設定します。



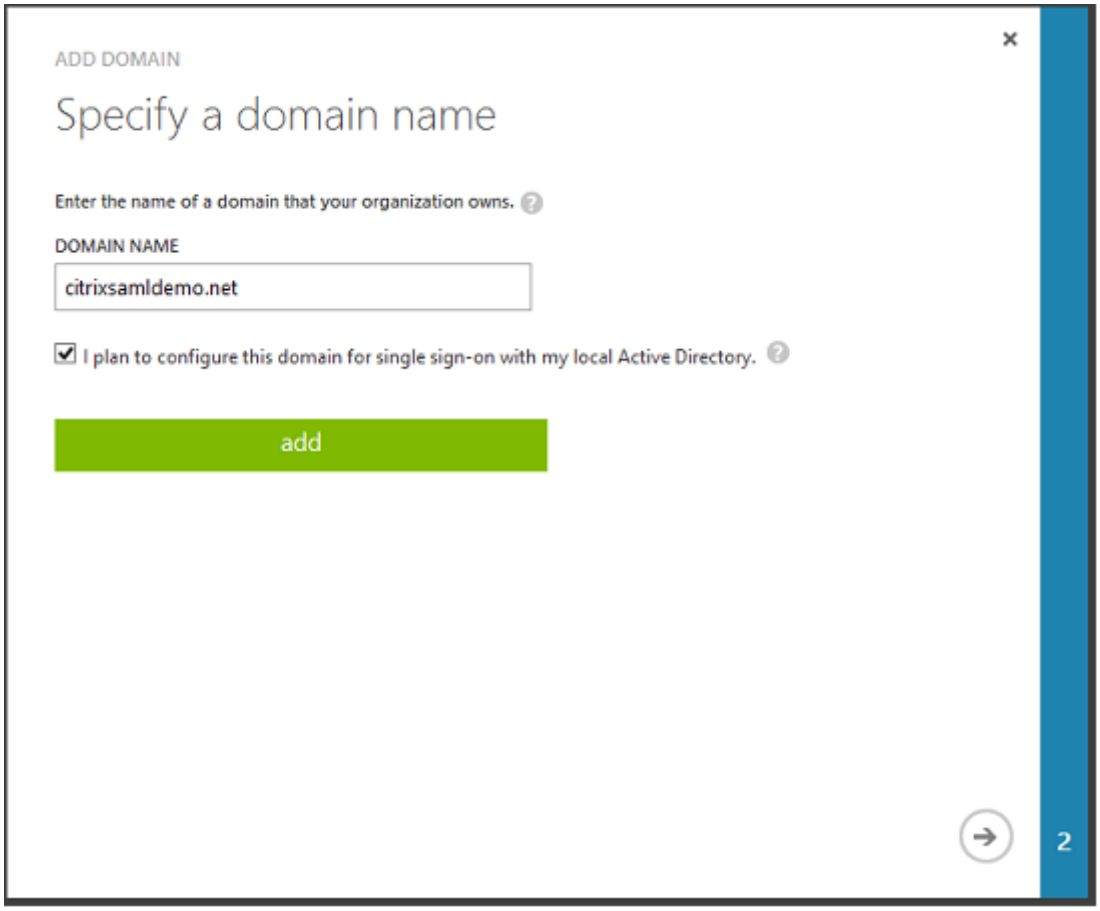
Azure AD を使用したドメインの登録

デフォルトでは、ユーザーは次の形式のメールアドレスで識別されます: `<user.name>@<company>.onmicrosoft.com`。

このアドレスは追加の構成なしで機能しますが、エンドユーザーのメールアカウントと一致する、次の標準形式のメールアドレスをお勧めします: `<user.name>@<company>.com`。

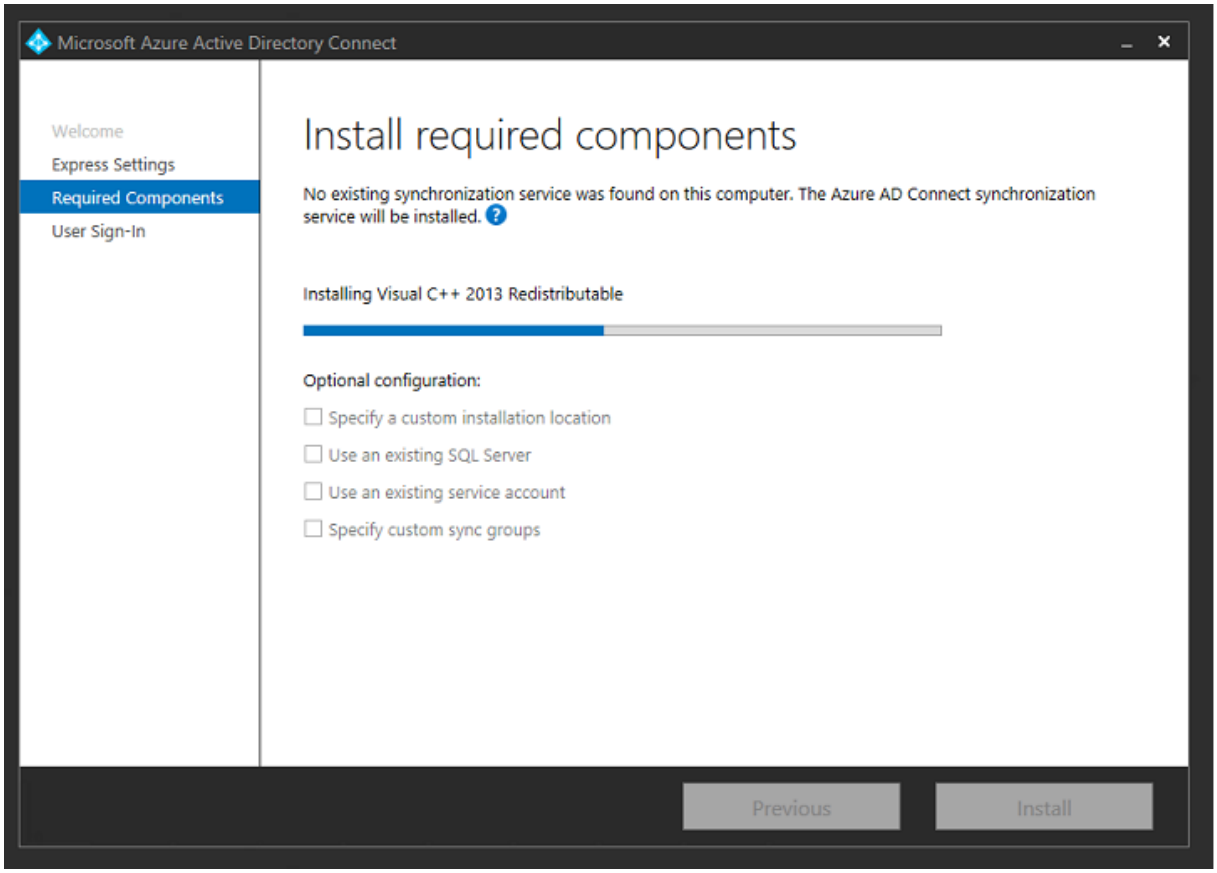
[ドメインの追加]で、ユーザーの会社のドメインからのリダイレクトを構成します。この例では、`citrixsamldemo.net`を使用します。

ADFS をシングルサインオンにセットアップしている場合は、チェックボックスにチェックマークを入れます。

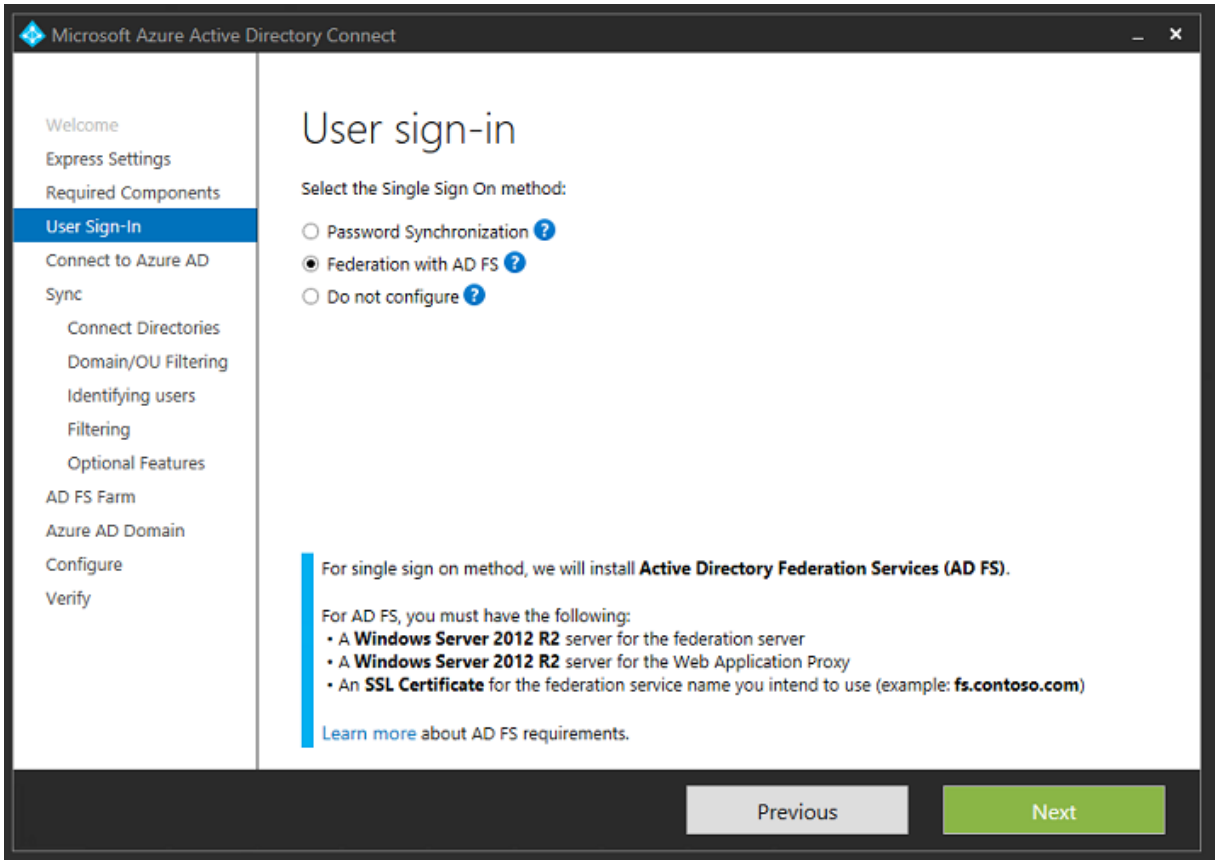


Azure AD Connect のインストール

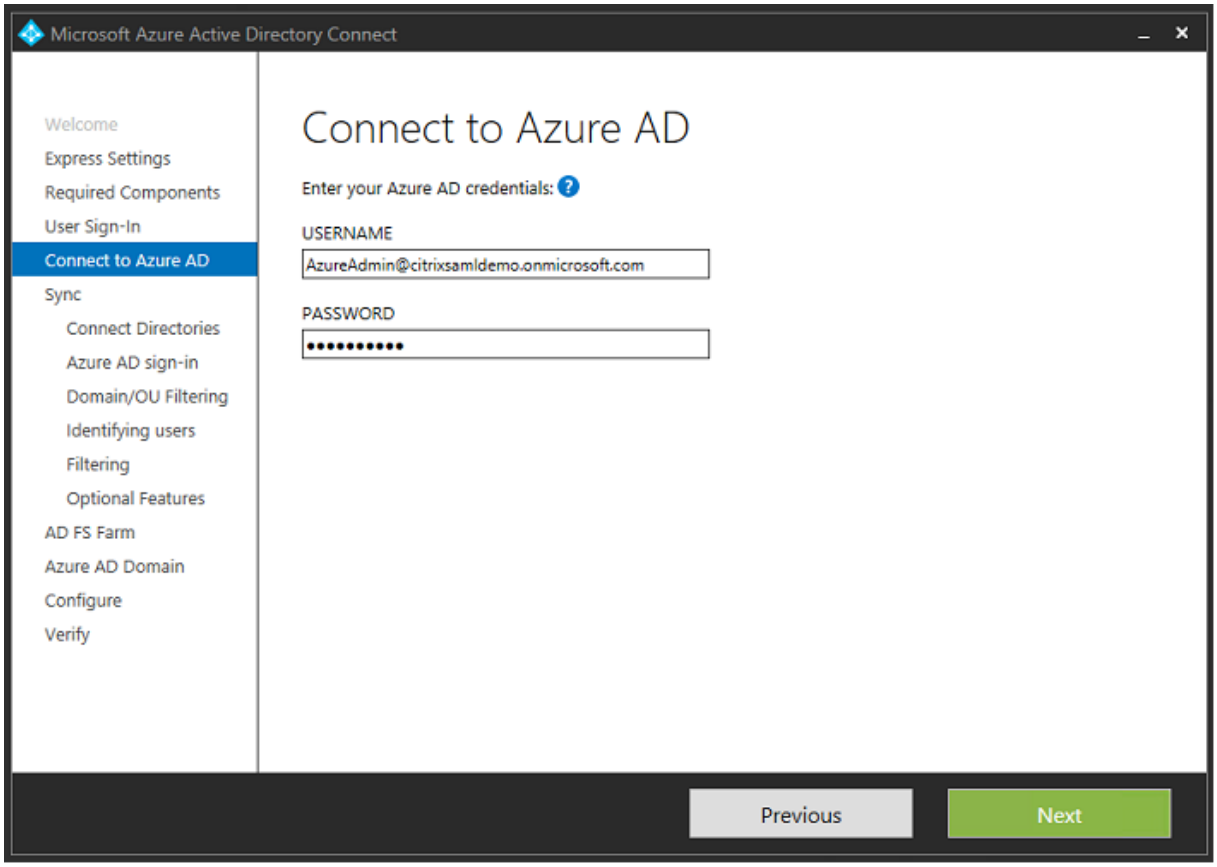
Azure AD 構成 GUI の手順 2 により、Azure AD Connect の Microsoft ダウンロードページにリダイレクトされます。これを ADFS 仮想マシンにインストールします。［簡単設定］ではなく ［カスタムインストール］を使用し、ADFS のオプションが利用できるようにします。



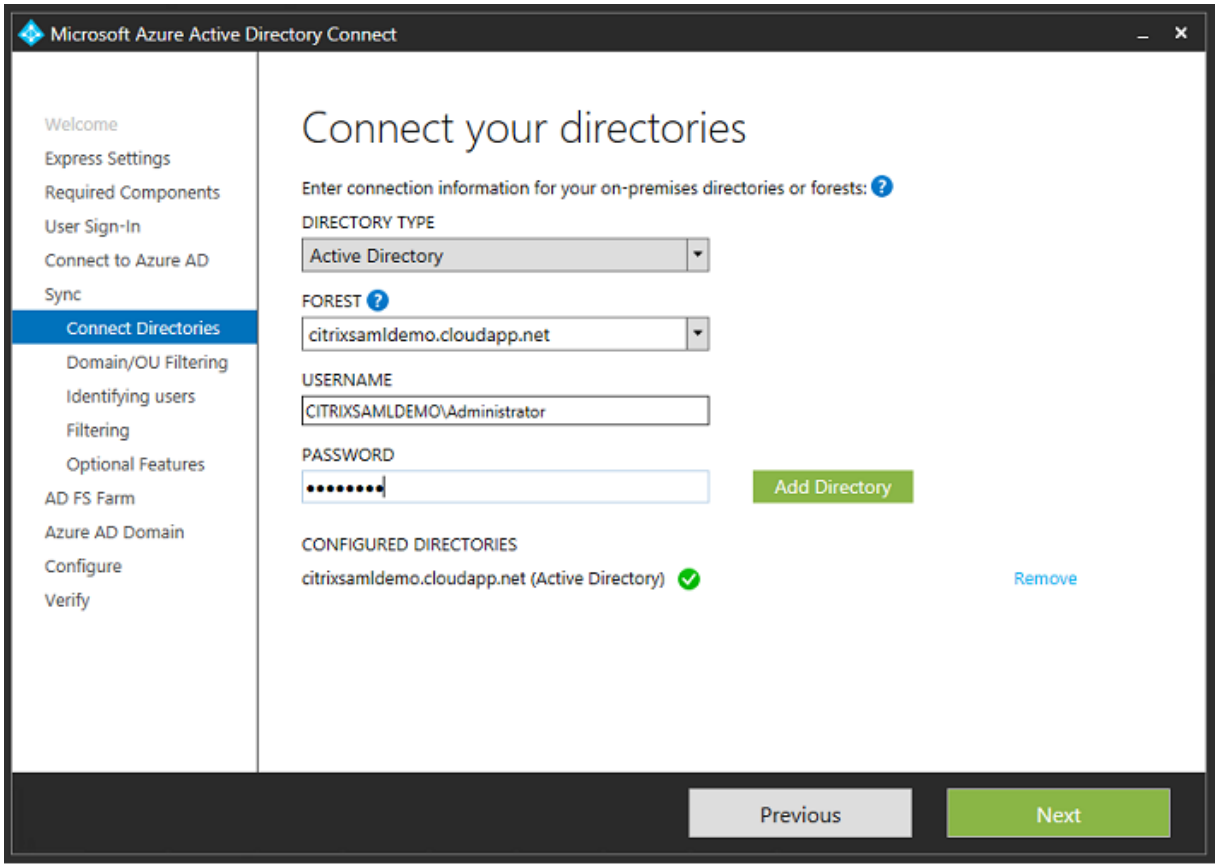
[**AD FS** とのフェデレーション］シングルサインオンオプションを選択します。



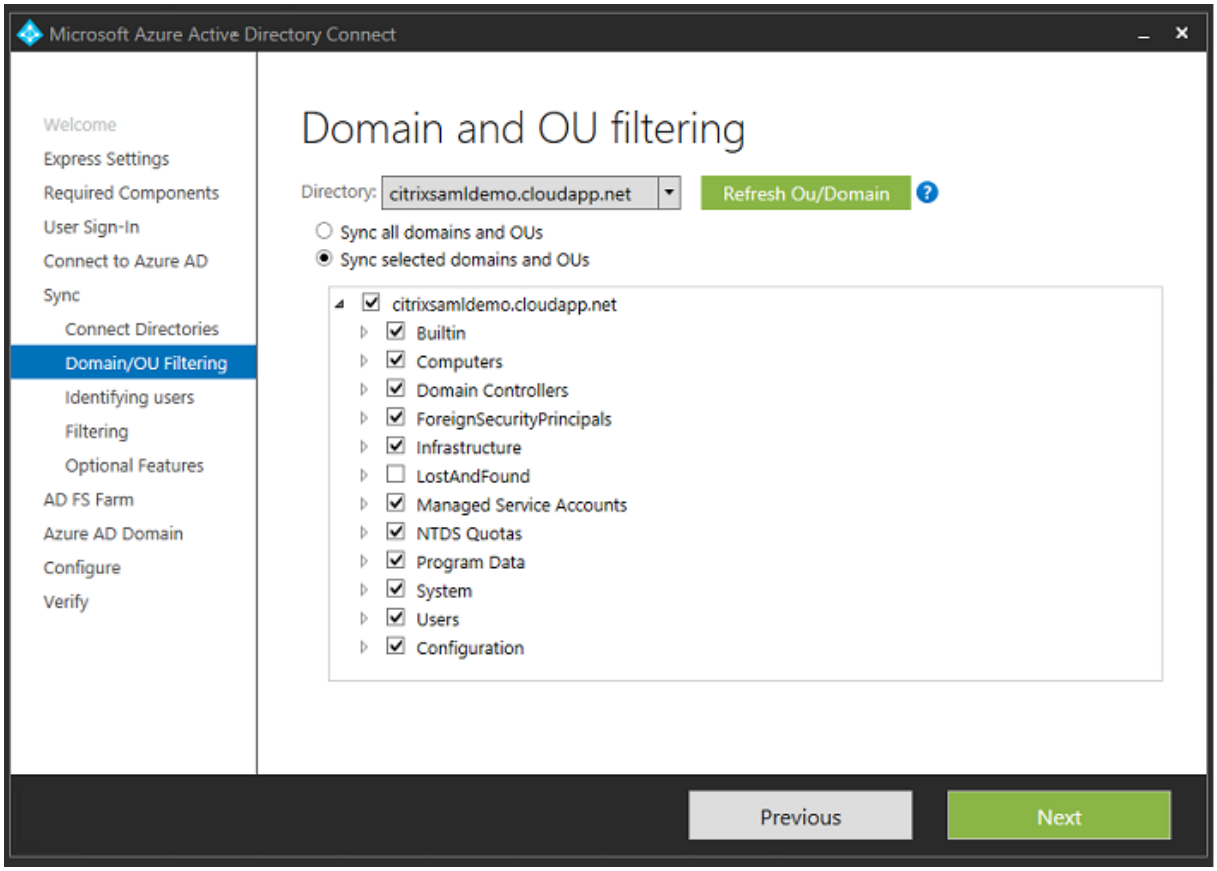
あらかじめ作成した管理アカウントで Azure に接続します。



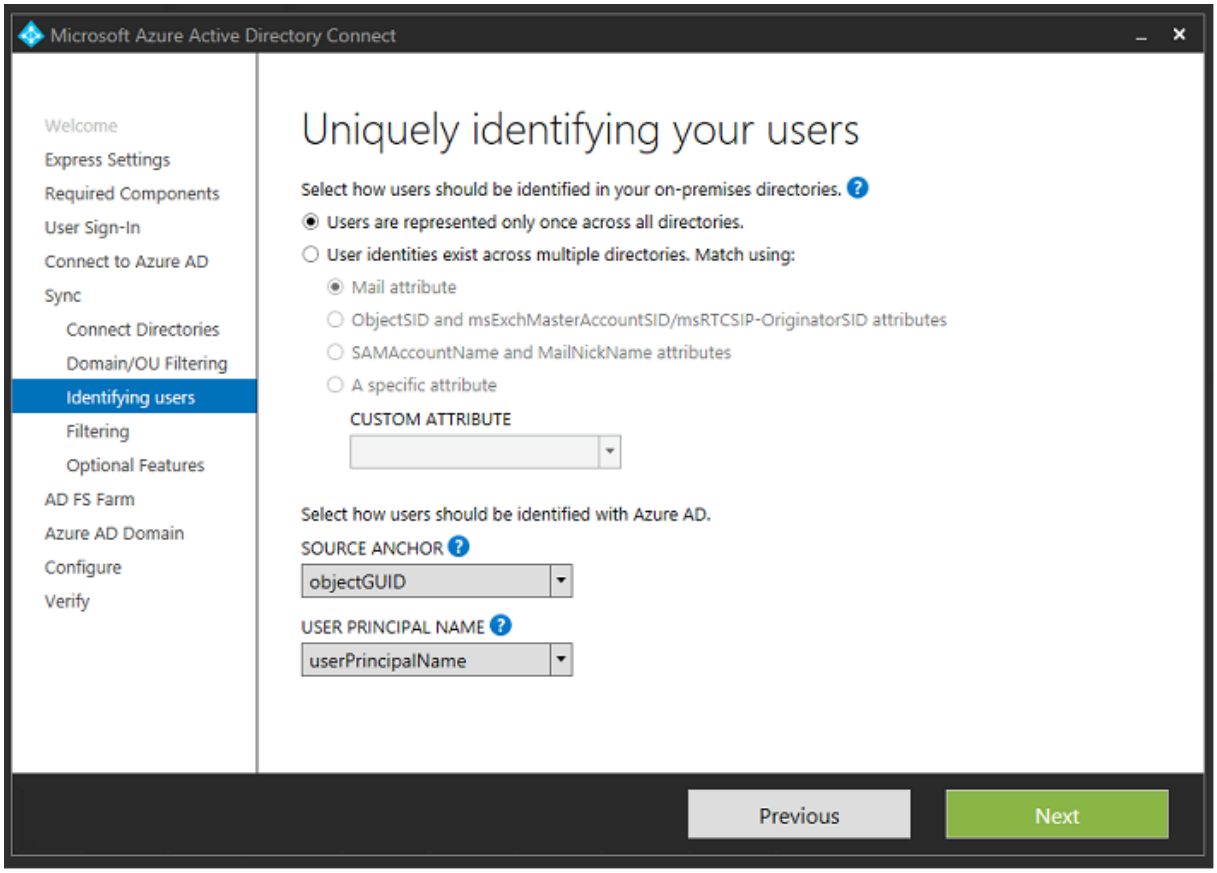
内部 AD フォレストを選択します。



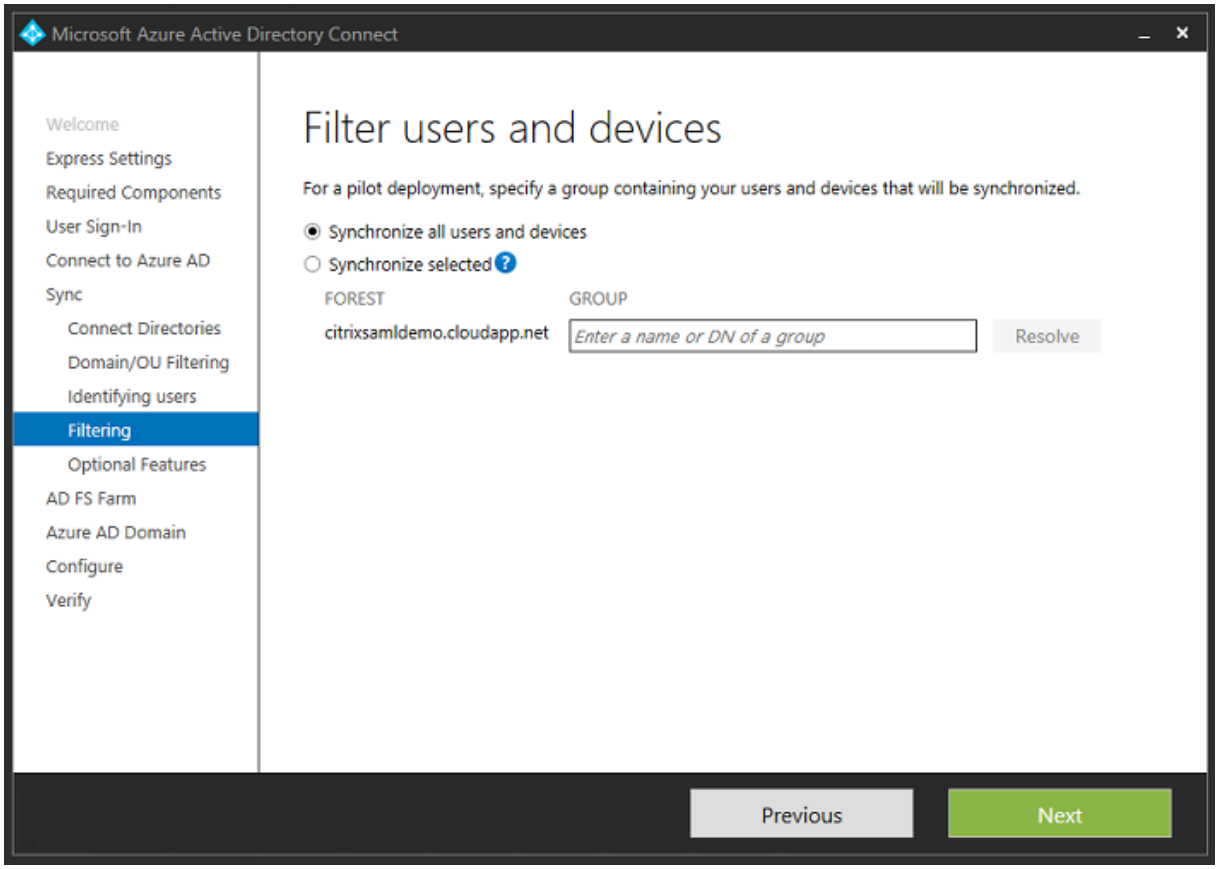
Active Directory の従来のオブジェクトをすべて Azure AD と同期します。



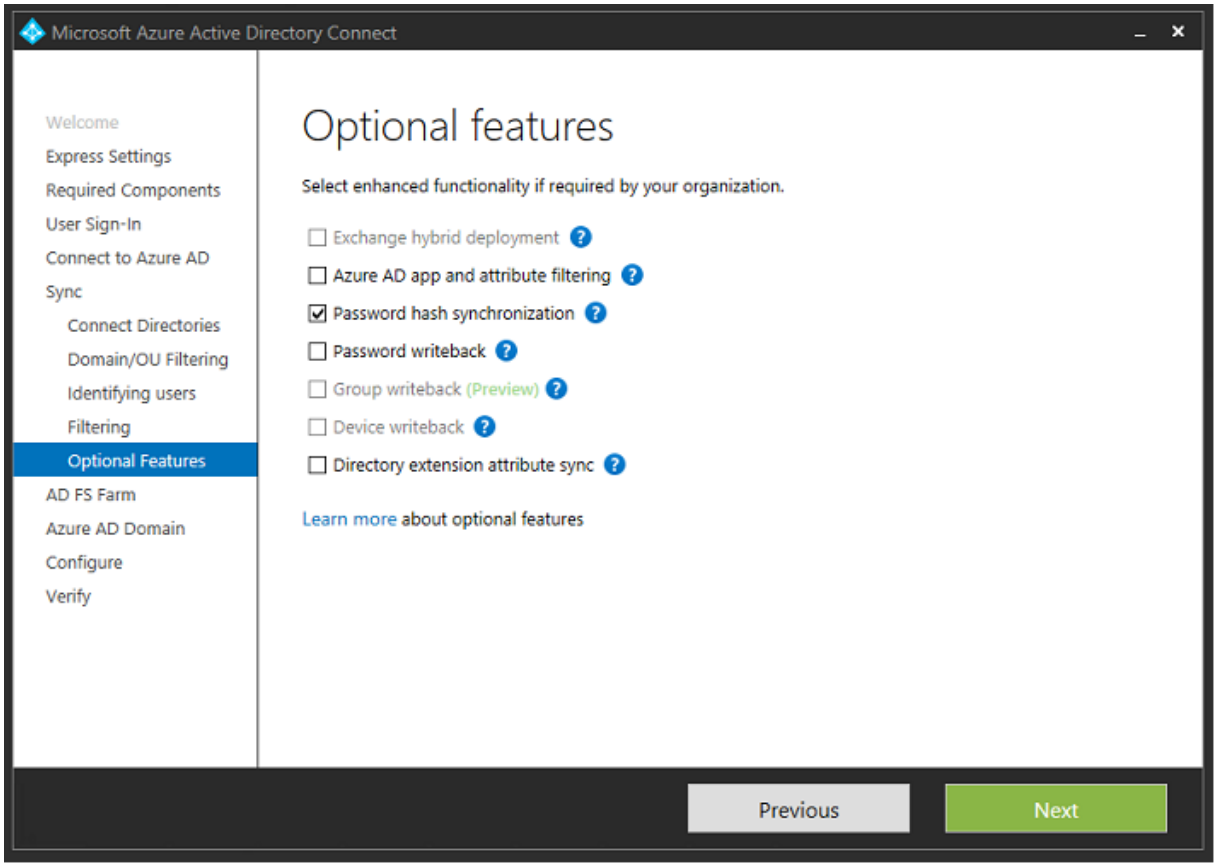
ディレクトリ構造がシンプルな場合は、ユーザー名の一意性に依存して、ログオンするユーザーを識別することができます。



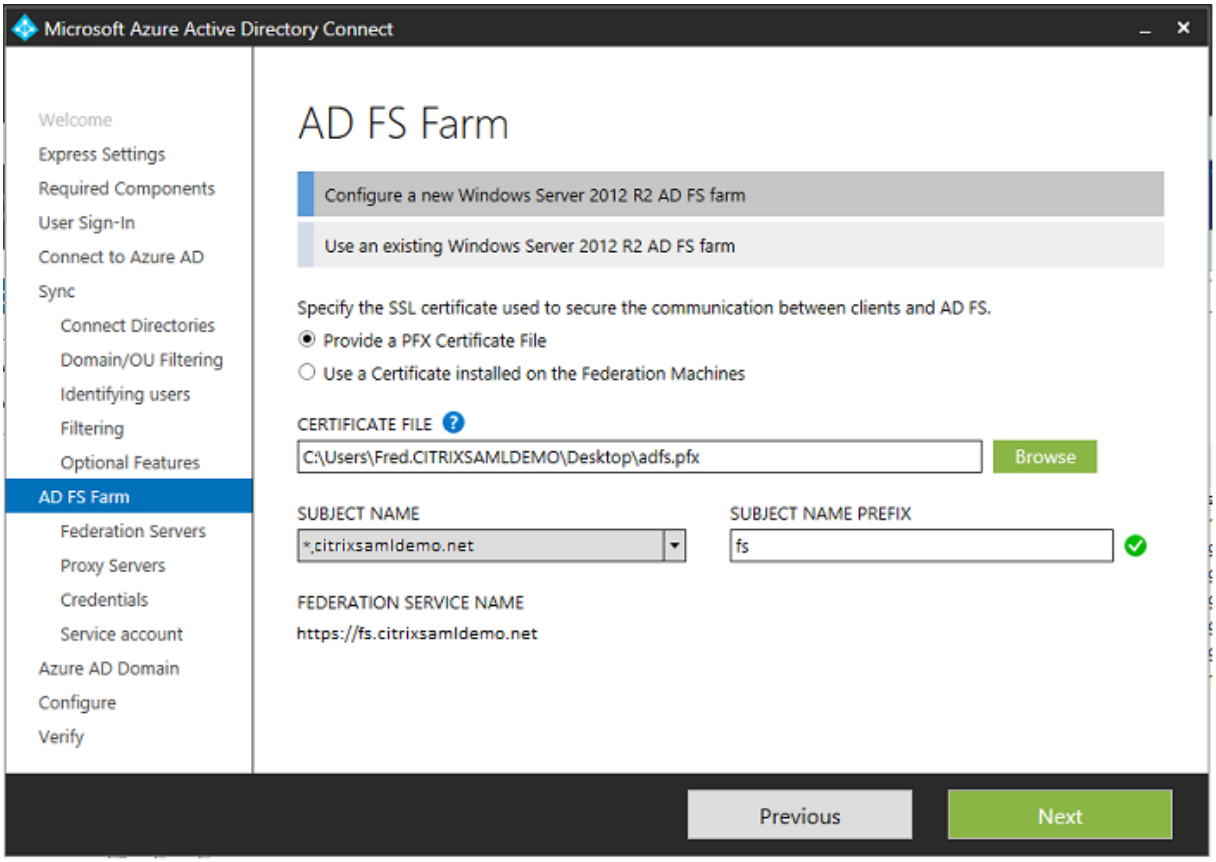
デフォルトのフィルタリングオプションを使用するか、あるいはユーザーとデバイスを特定のグループセットに制限します。



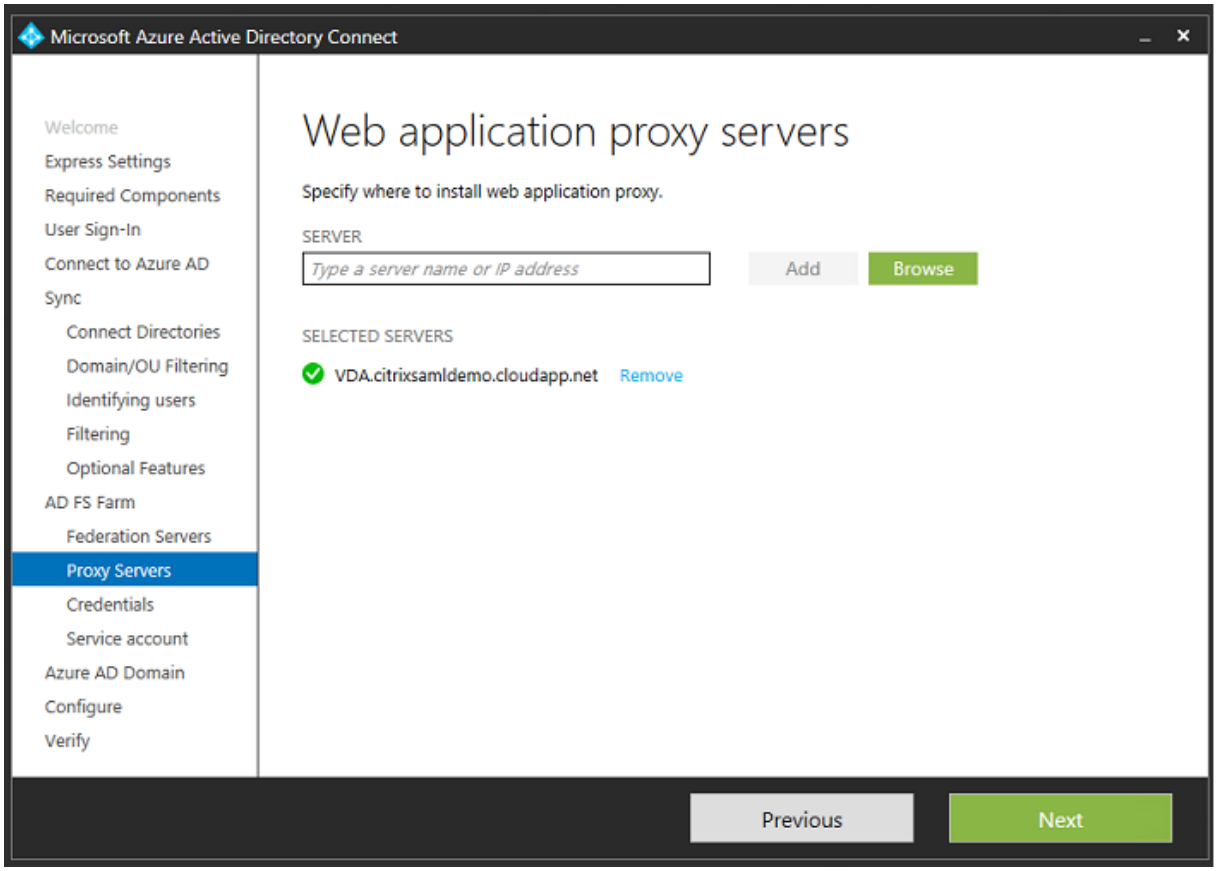
必要に応じて、Azure AD パスワードを Active Directory と同期することができます。これは、通常、ADFS ベースの認証では必要ありません。



証明書の PFX ファイルを AD FS で使用するように選択します。DNS 名として fs.citrixsamldemo.net を指定します。

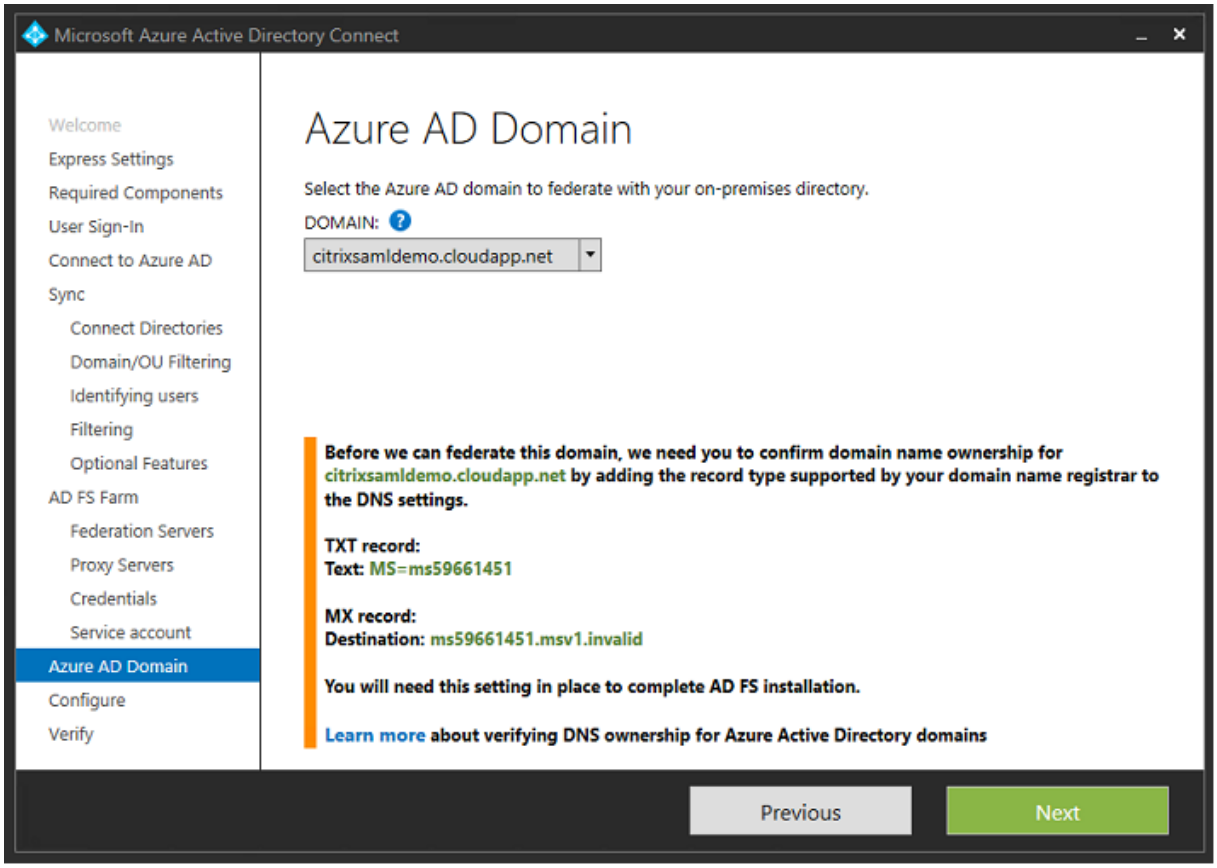


プロキシサーバーの選択を求める画面が表示されたら、wap.citrixsamldemo.net サーバーのアドレスを入力します。Azure AD Connect が構成できるよう、Web アプリケーションプロキシサーバーの管理者として **Enable-PSRemoting –Force** コマンドレットを実行する必要がある場合があります。

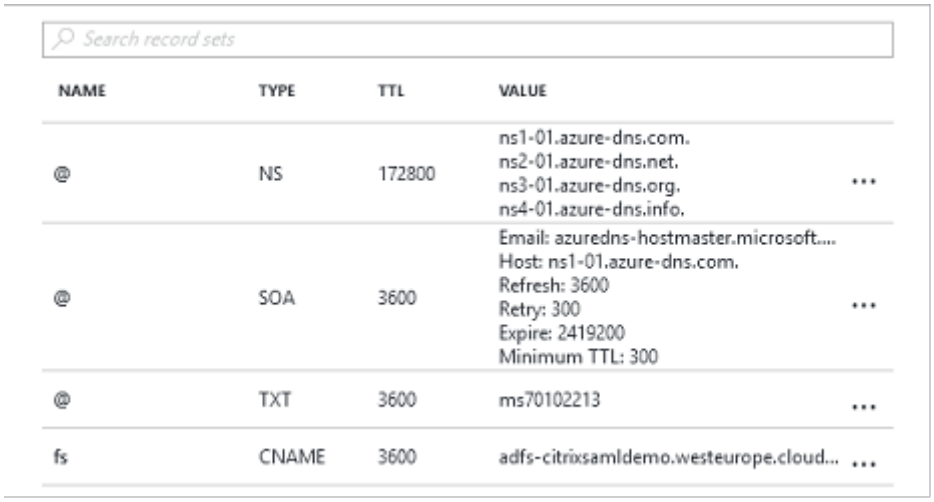


> 注:
>
> Remote PowerShell の信頼性の問題でこの手順に失敗した場合は、Web アプリケーションプロキシサーバーをドメインに参加させてみてください。

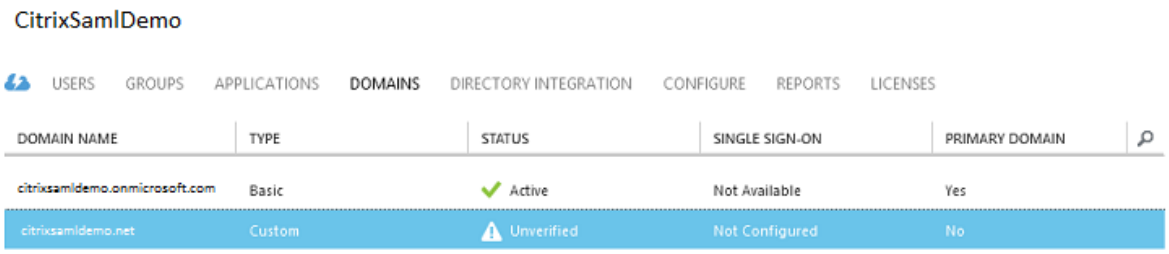
ウィザードの残りの手順については、標準の管理者パスワードを使用して、ADFS のサービスアカウントを作成します。Azure AD Connect により、DNS ゾーンの所有権の検証が求められます。



TXT レコードと MX レコードを Azure の DNS アドレスレコードに追加します。

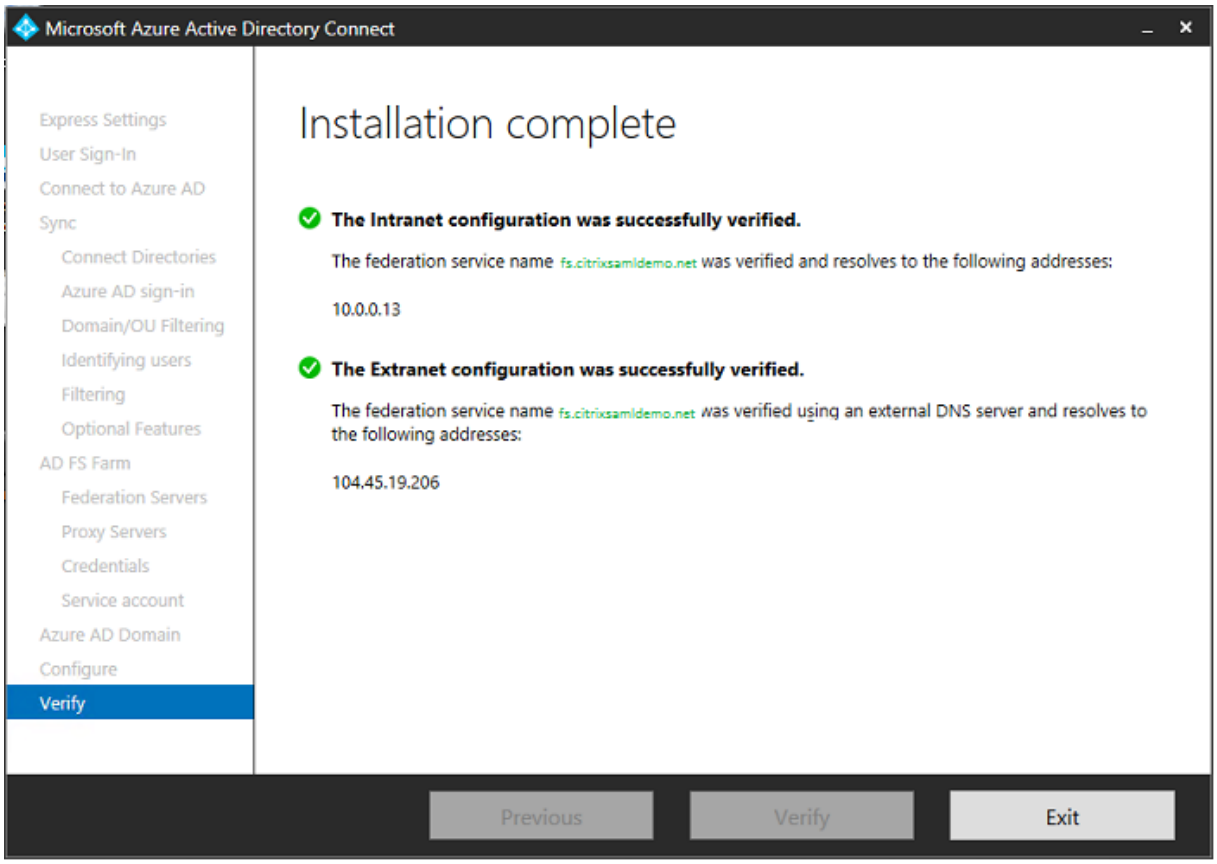


Azure 管理コンソールで［検証］をクリックします。



> 注:
>
> この手順に失敗した場合は、Azure AD Connect を実行する前にドメインを検証します。

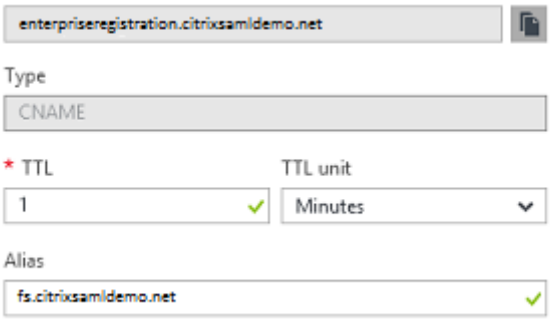
完了すると、外部アドレス fs.citrixsamldemo.net がポート 443 で接続されます。



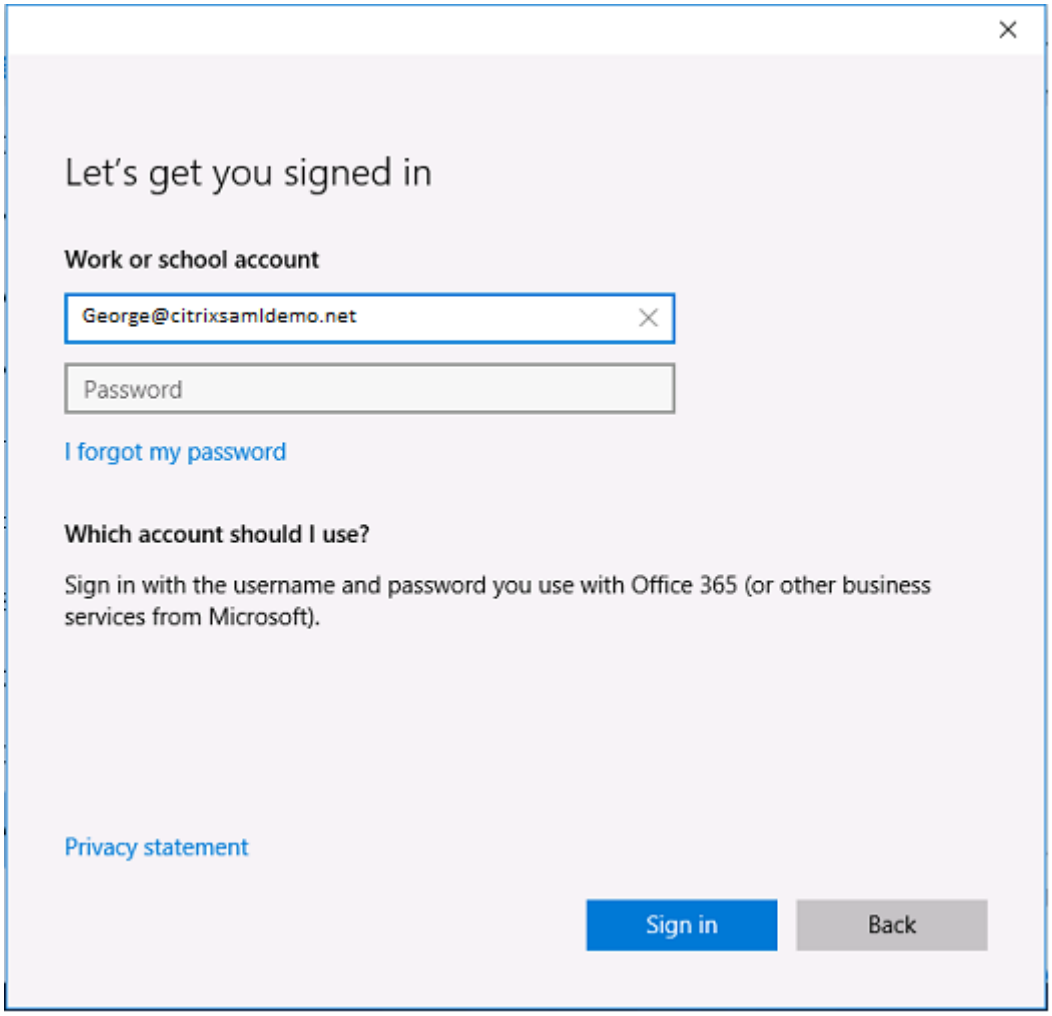
Azure AD への参加の有効化

Windows 10 が Azure AD への参加を実行するよう、メールアドレスを入力すると、ADFS を指す必要がある CNAME DNS レコードの作成に DNS サフィックスが使用されます（enterpriseregistration.<*upnsuffix*>）。

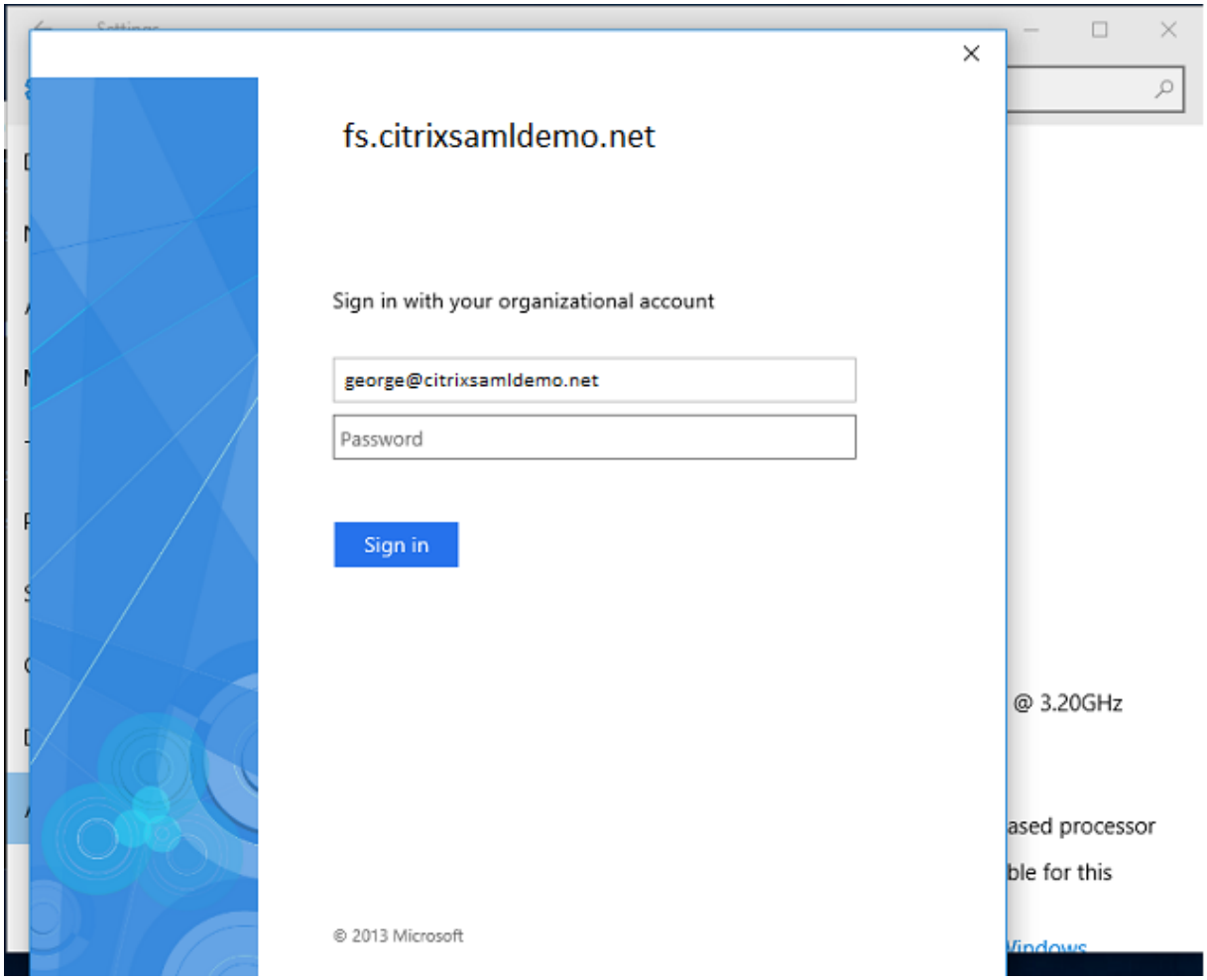
この例では、`fs.citrixsamldemo.net`となります。

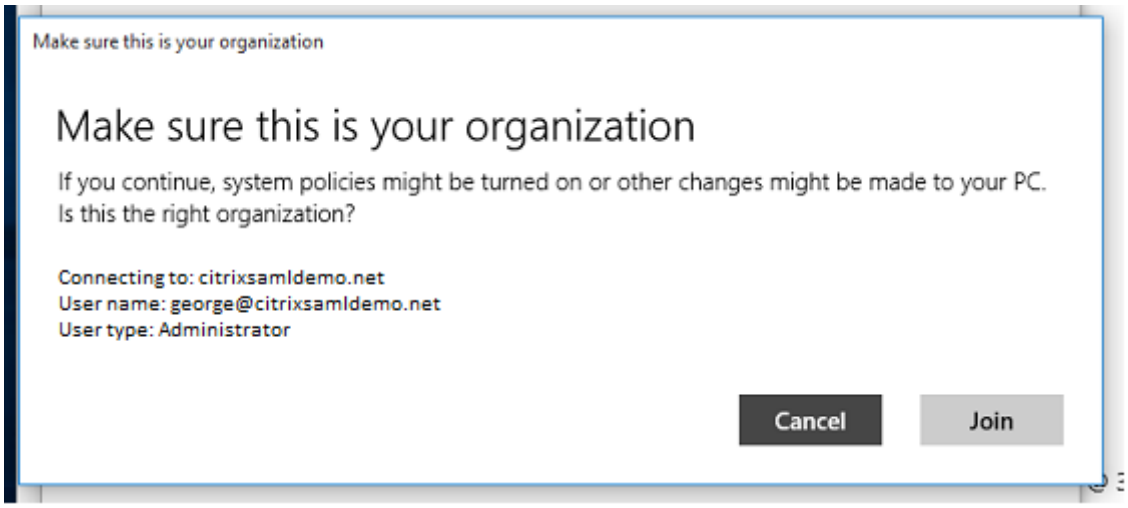


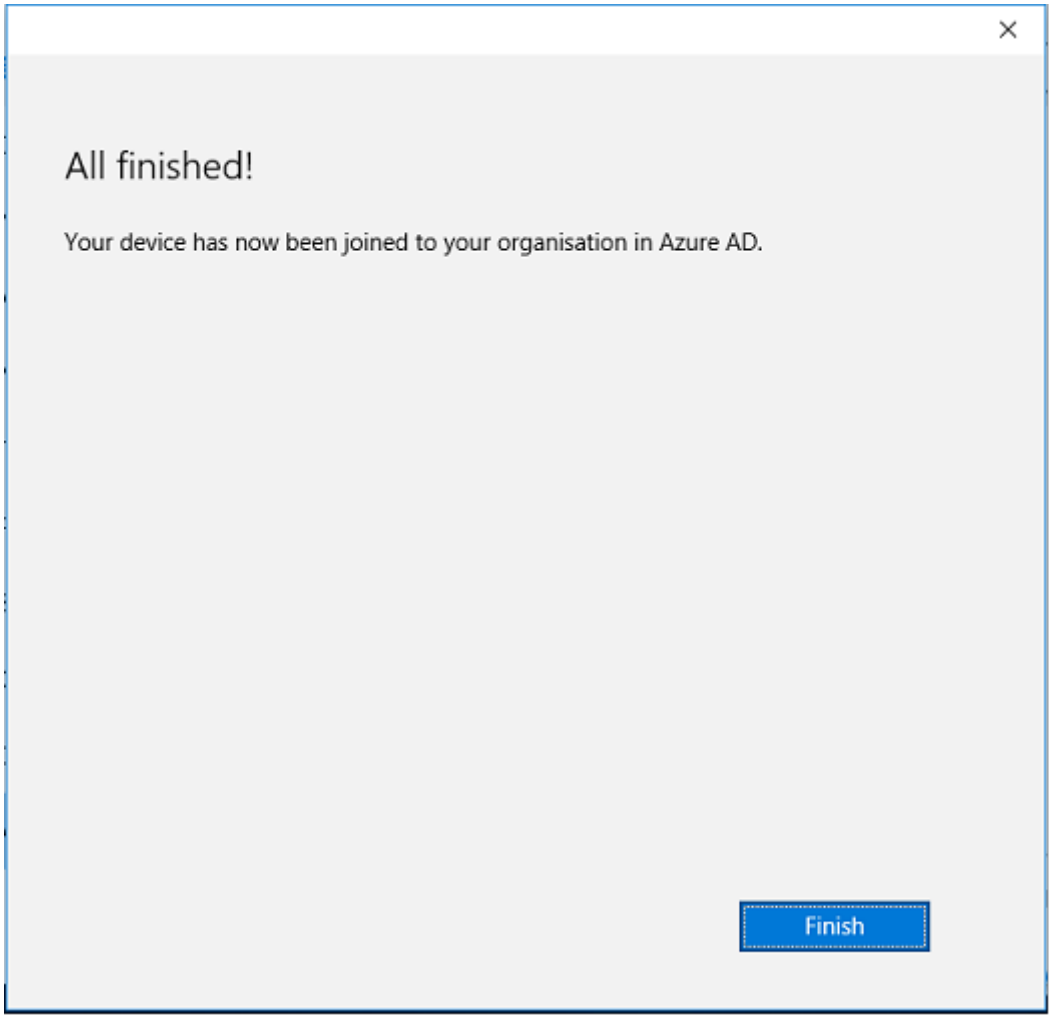
パブリック証明機関を使用していない場合は、Windows が ADFS サーバーを信頼するよう、ADFS のルート証明書を Windows 10 コンピューターにインストールします。あらかじめ生成された標準のユーザーアカウントを使用して、Azure AD ドメインに参加します。



UPN は、ADFS ドメインコントローラーで認識される UPN と一致する必要があることに注意してください。





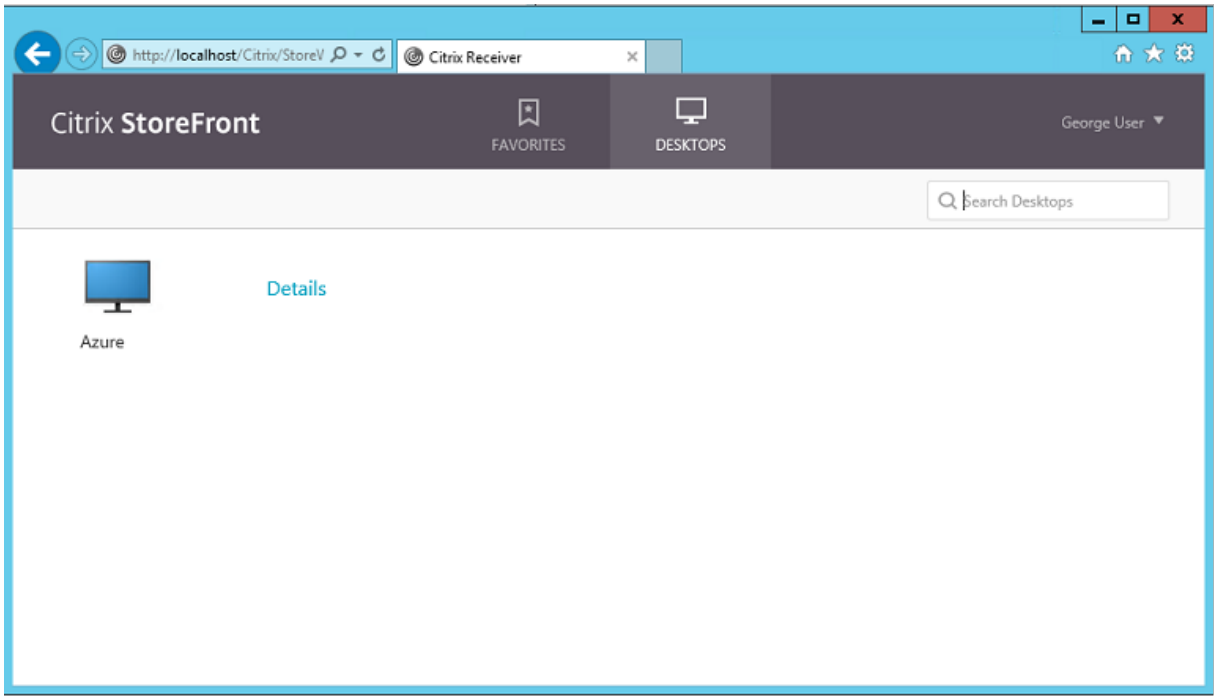


メールアドレスを使用してマシンの再起動とログオンを行い、Azure AD への参加が正常に行われたことを検証します。ログオンすると Microsoft Edge が起動してhttp://myapps.microsoft.comに接続します。この Web サイトでは、シングルサインオンが自動的に使用されます。

Citrix Virtual Apps または **Citrix Virtual Desktops** のインストール

通常の方法で、Citrix Virtual Apps または Citrix Virtual Desktops の ISO から、Delivery Controller および VDA 仮想マシンを Azure に直接インストールすることができます。

この例では、StoreFront は Delivery Controller と同じサーバーにインストールされています。VDA はスタンドアロンの Windows 2012 R2 用 RDS ワーカーとしてインストールされ、Machine Creation Services とは統合していません（ただしオプションで構成することができます）。作業を続行する前に、ユーザー George@citrixsamldemo.net がパスワードで認証できることを確認します。



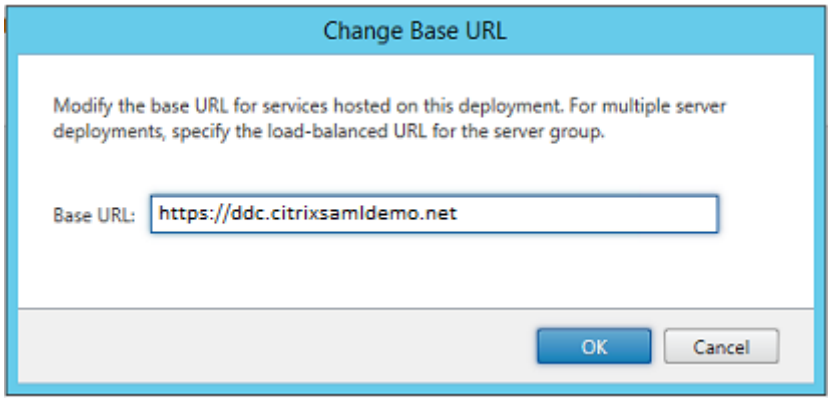
StoreFront がユーザー資格情報なしに認証できるよう、**Set-BrokerSite –TrustRequestsSent-ToTheXmlServicePort $true** PowerShell コマンドレットを Controller で実行します。

フェデレーション認証サービスのインストール

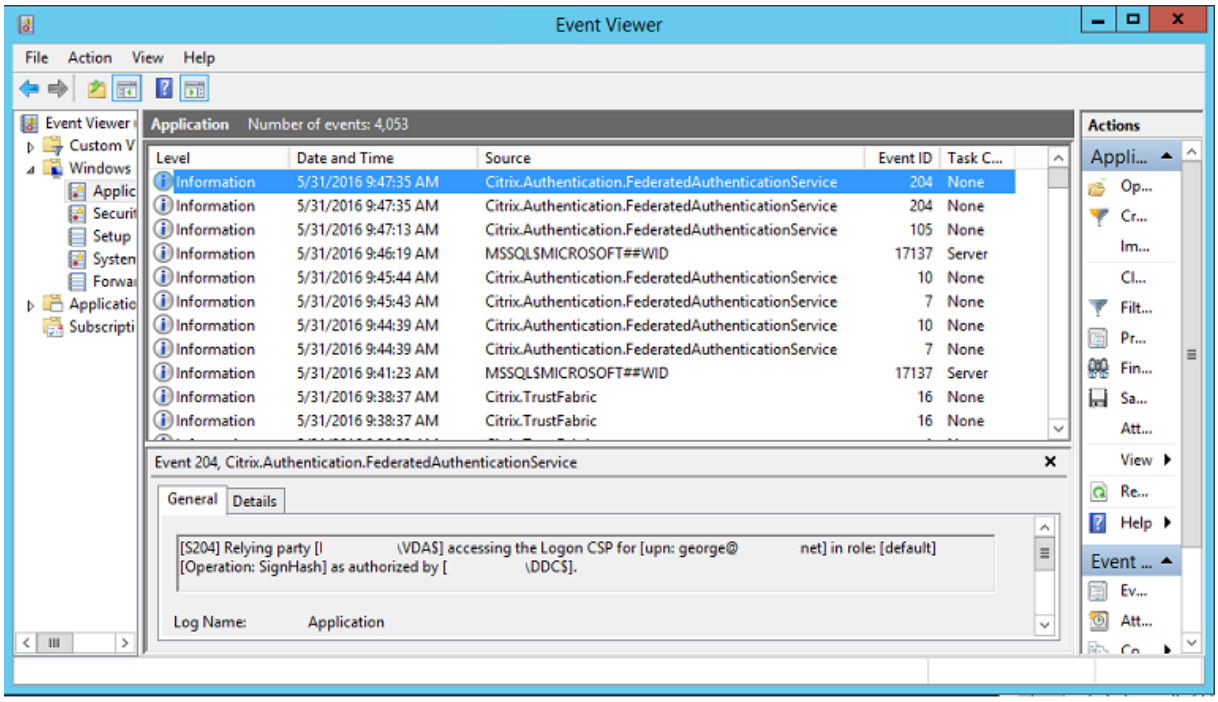
ADFS サーバーに FAS をインストールし、Delivery Controller が信頼できる StoreFront として機能するためのルールを構成します（この例では、StoreFront が Delivery Controller と同じ仮想マシンにインストールされているため）。「インストールと構成」を参照してください。

StoreFront の構成

Delivery Controller のコンピューター証明書を要求します。また、ポート 443 に IIS バインドを設定し、StoreFront のベースアドレスを https: に変更して、IIS および StoreFront で HTTPS が使用されるように構成します。

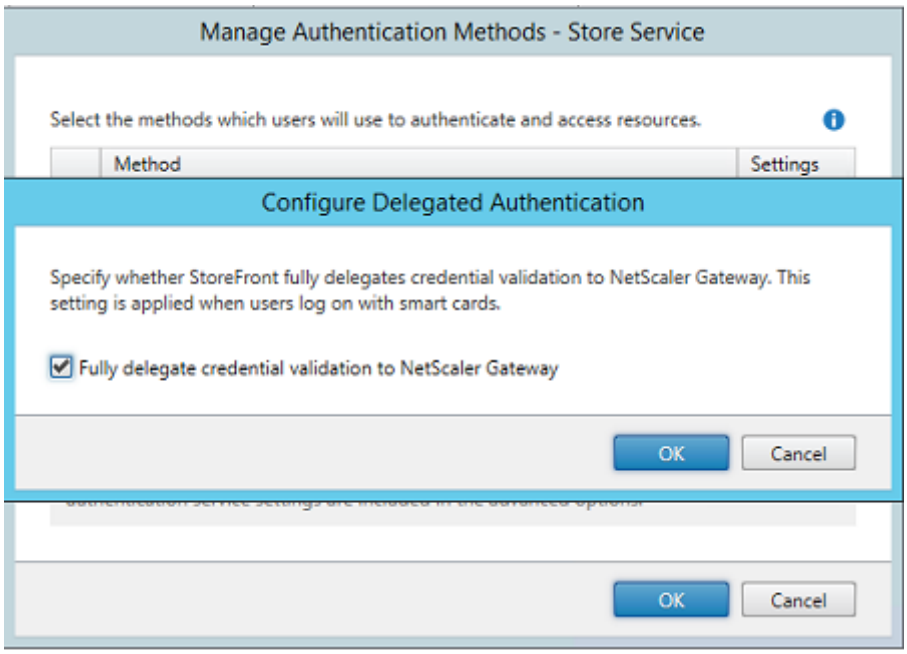


StoreFront で FAS サーバーが使用されるように構成し（「インストールと構成」の PowerShell スクリプトを使用します）、Azure 内で内部テストを行います。FAS サーバーのイベントビューアーをチェックして、ログオンに FAS が使用されることを確認します。

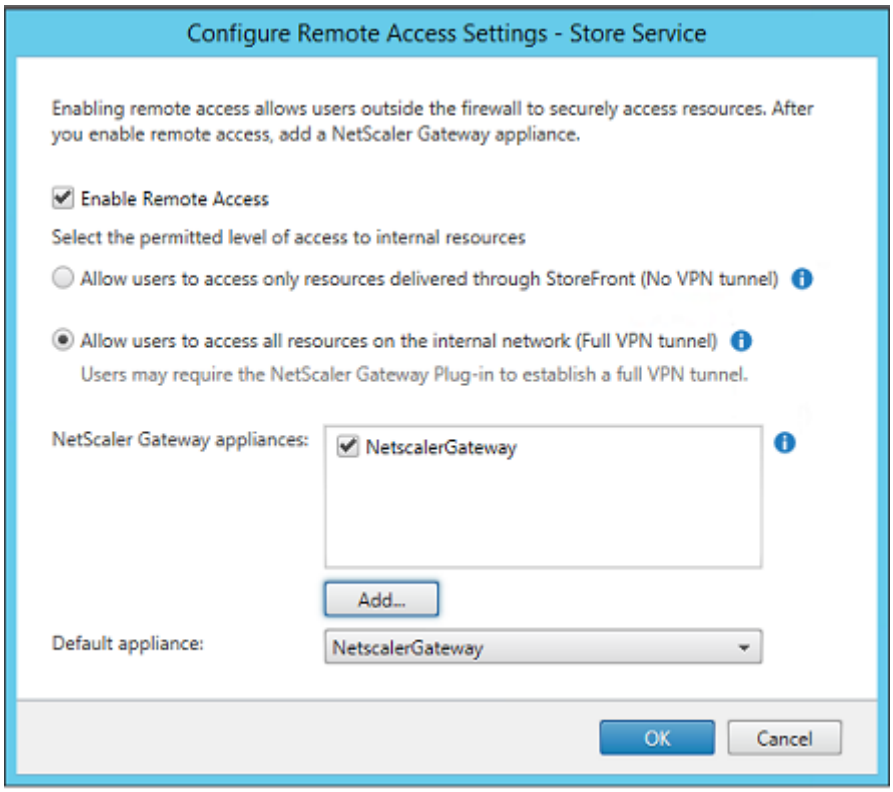


Citrix Gateway を使用するための **StoreFront** の構成

StoreFront 管理コンソールの ［認証方法の管理］ GUI を使用して、StoreFront が認証に Citrix Gateway を使用するよう構成します。

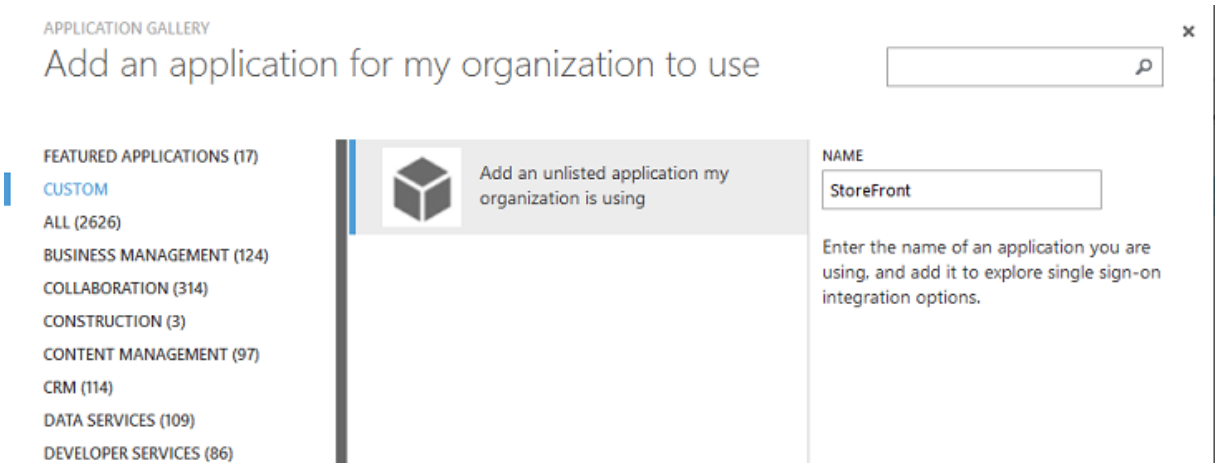


Citrix Gateway 認証オプションを統合するには、Secure Ticket Authority（STA）の構成および Citrix Gateway アドレスの構成を行います。



新しい **Azure AD** アプリケーションを **StoreFront** へのシングルサインオンに構成

このセクションでは、Azure AD SAML 2.0 シングルサインオン機能を使用します。現在は、Azure Active Directory プレミアムサブスクリプションが必要です。Azure AD 管理ツールで ［新しいアプリケーション］を選択し、［ギャラリーからアプリケーションを追加します］を選択します。



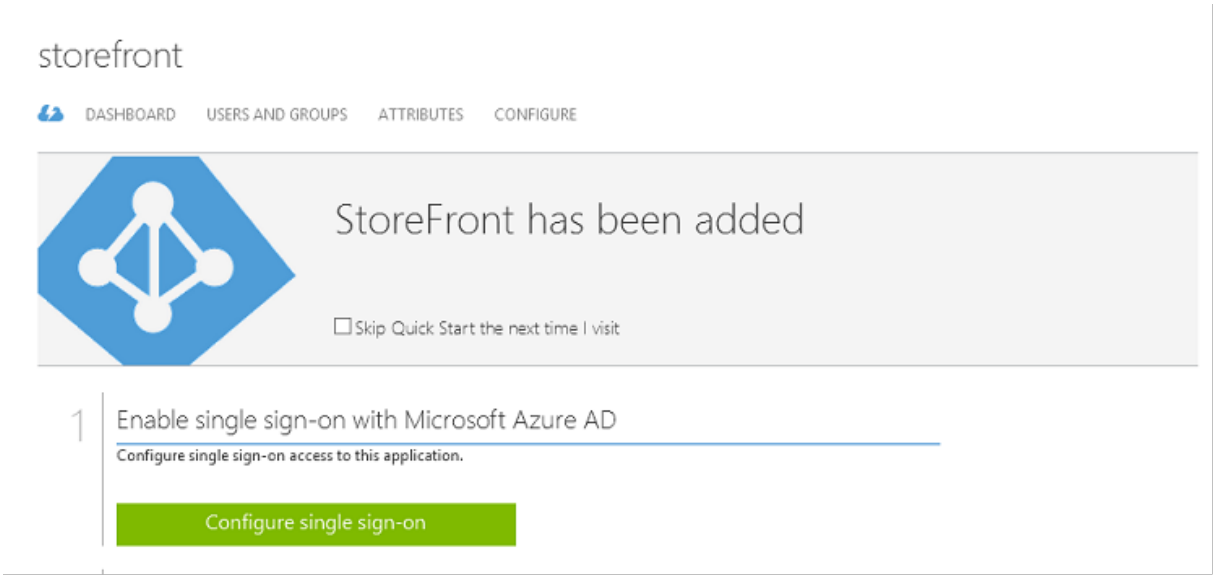
［カスタム］カテゴリの［私の組織で使用している、一覧にないアプリケーションを追加］を選択して、ユーザーが使用する新しいカスタムアプリケーションを作成します。

アイコンの構成

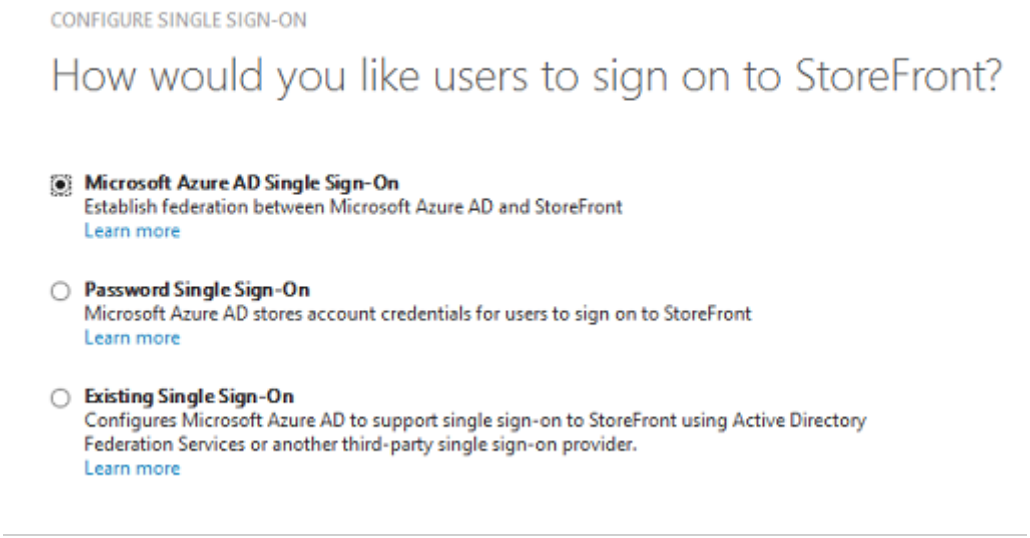
縦横 215 ピクセルの画像を作成して［構成］ページにアップロードし、アプリケーションのアイコンとして使用します。

SAML 認証の構成

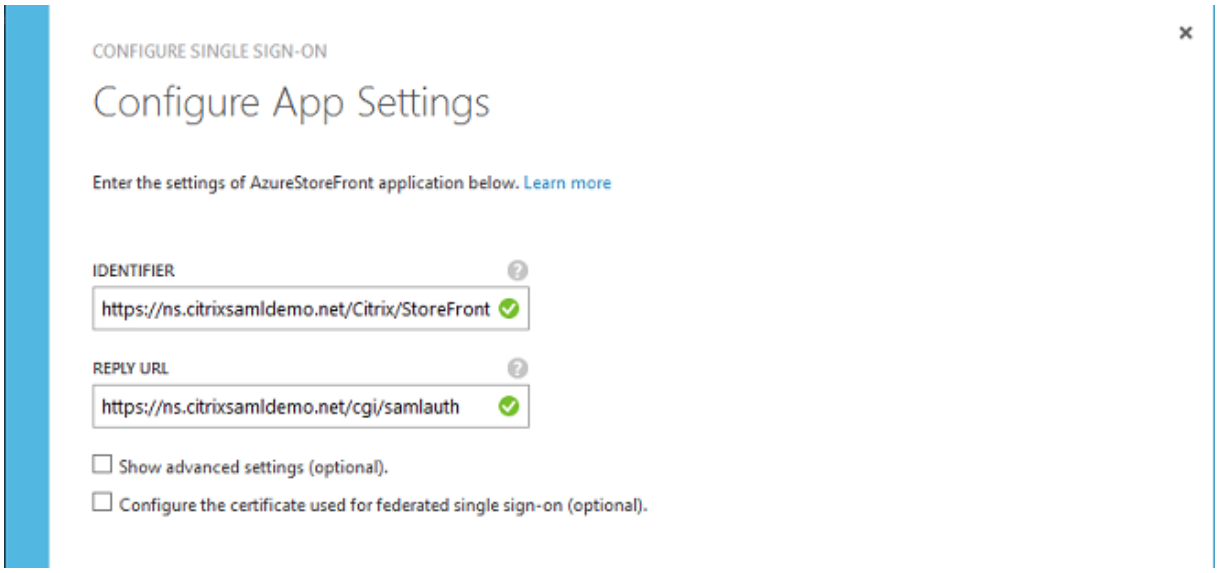
アプリケーションダッシュボードの概要ページに戻り、［シングルサインオンの構成］を選択します。



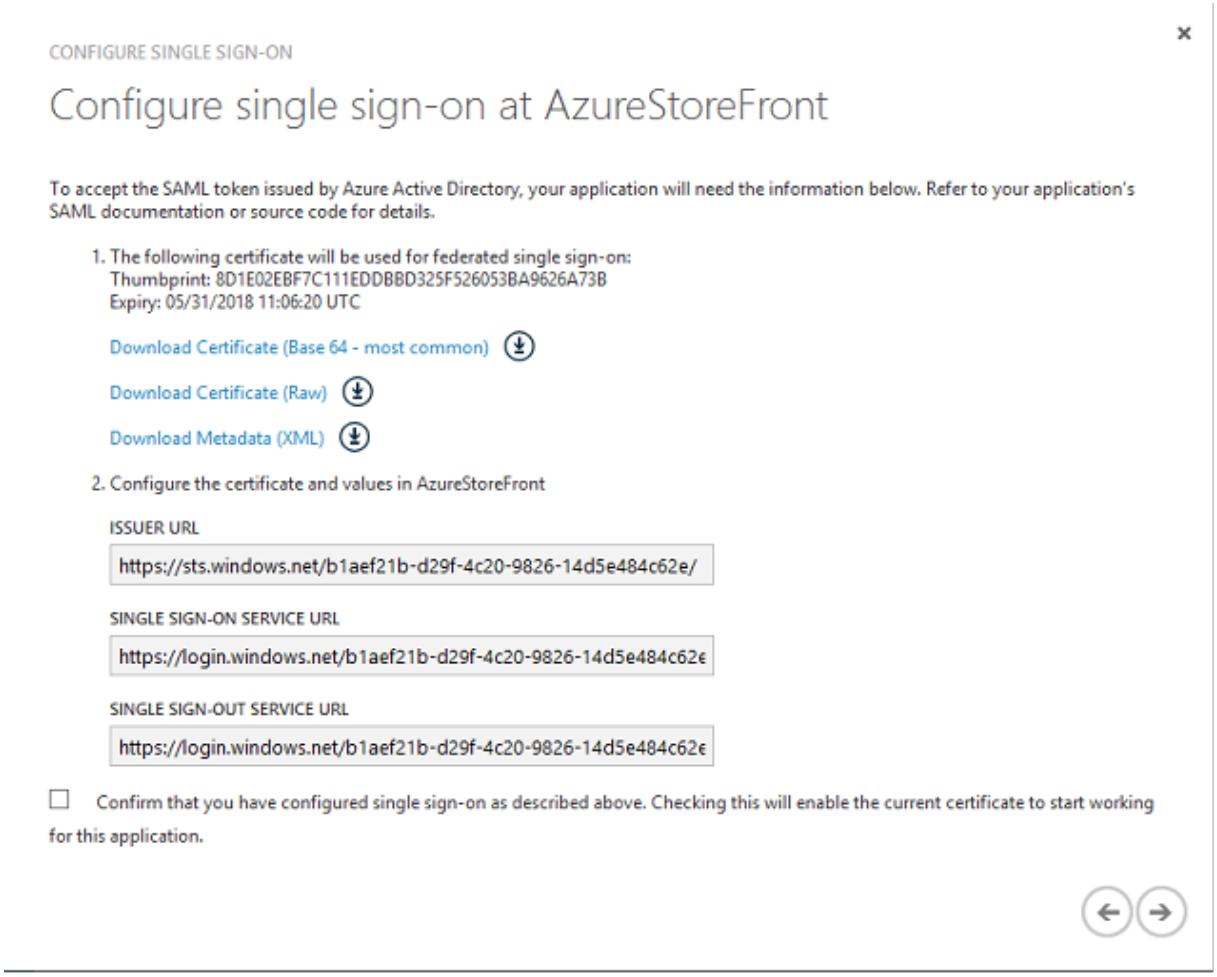
この展開では、［**Microsoft Azure AD** のシングルサインオン］に対応する SAML 2.0 認証を使用します。



［識別子］には任意の文字列を指定できます（Citrix Gateway に提供された構成と一致する必要があります）。この例では、［応答 **URL**］が Citrix Gateway サーバーの */cgi/samlauth* になっています。



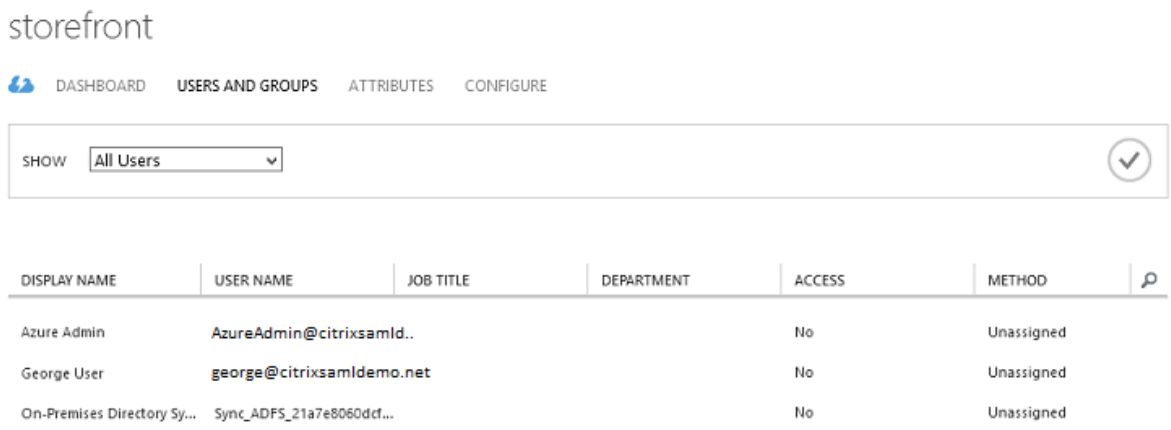
次のページには、Citrix Gateway を Azure AD の証明書利用者として構成するために使用される情報が含まれています。



Base 64 の信頼された署名証明書をダウンロードして、サインオン URL とサインアウト URL をコピーします。これらを Citrix Gateway の［構成］画面にペーストします。

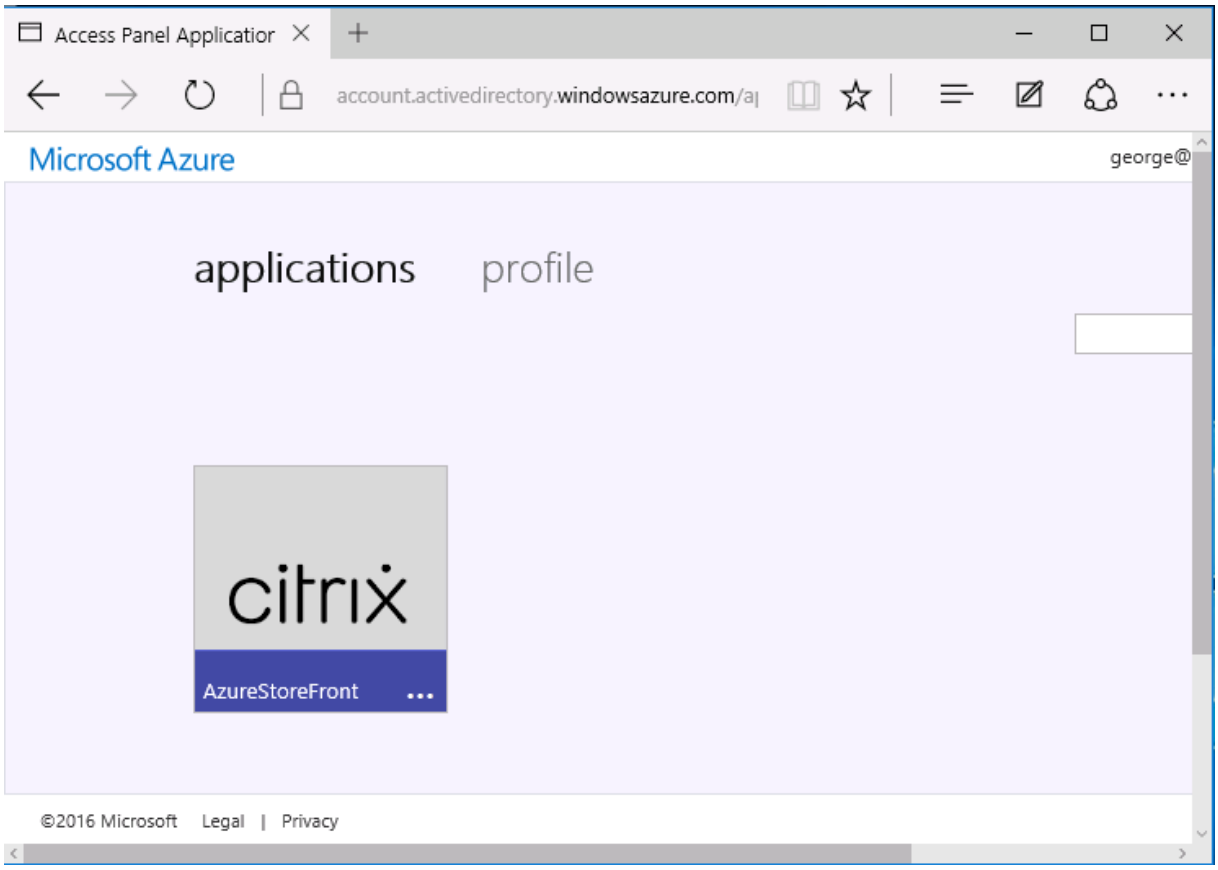
ユーザーへのアプリケーションの割り当て

最後の手順では、アプリケーションを有効にして、ユーザーの「myapps.microsoft.com」コントロールページにアプリケーションが表示されるようにします。これは［ユーザーとグループ］ページで行います。Azure AD Connect が同期したドメインユーザーアカウントへのアクセスを割り当てます。ほかのアカウントも使用できますが、<user>@<domain> パターンに従っていないため、明示的にマップする必要があります。



MyApps ページ

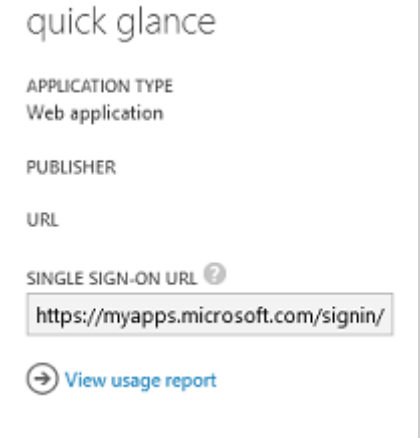
アプリケーションが構成されると、https://myapps.microsoft.comで、Azure アプリケーションのユーザー一覧に表示されます。



Azure AD に参加している場合、ログオンしたユーザーは、Windows 10 により、Azure アプリケーションへのシングルサインオンがサポートされます。アイコンをクリックすると、ブラウザーは前に構成した SAML cgi/samlauth Web ページに移動します。

シングルサインオン **URL**

Azure AD ダッシュボードのアプリケーションに戻ります。アプリケーションに利用できるシングルサインオン URL があることを確認します。この URL は、Web ブラウザーリンクの提供や、StoreFront に直接移動するための、スタートメニューのショートカットの作成に使用されます。



この URL を Web ブラウザーにペーストして、前に構成した Citrix Gateway cgi/samlauth Web ページに、Azure AD がリダイレクトするようにします。これが機能するのは、割り当てられたユーザーだけです。また、シングルサインオンが利用できるのは、Windows 10 の Azure AD に参加しているログオンセッションだけです。（そのほかのユーザーには、Azure AD の資格情報の入力が求められます。）

Citrix Gateway のインストールと構成

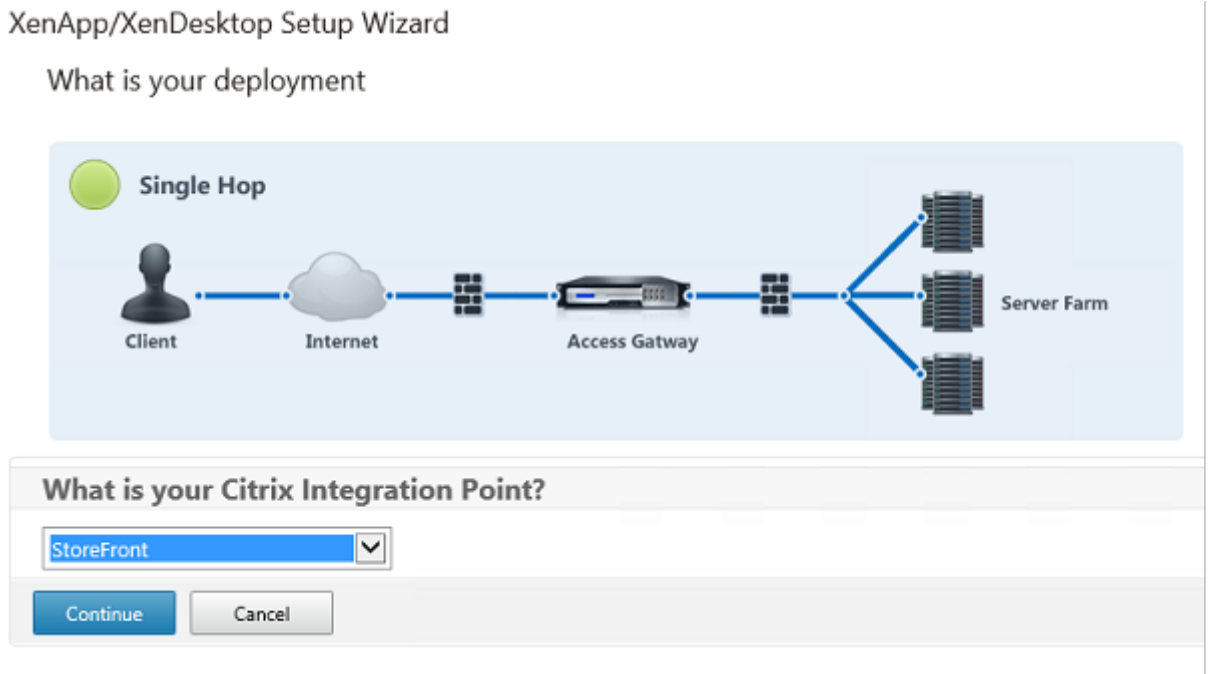
この例では、展開へのリモートアクセスに、NetScaler（現 Citrix Gateway）を実行する独立した仮想マシンを使用します。仮想マシンは Azure ストアで購入できます。この例では、NetScaler 11.0 の「Bring your own License」バージョンを使用しています。

Web ブラウザーのアドレスバーに内部 IP アドレスを入力し、ユーザー認証の際に指定された資格情報を使用して、NetScaler 仮想マシンにログオンします。Azure AD 仮想マシンの nsroot ユーザーのパスワードを変更する必要があることに注意してください。

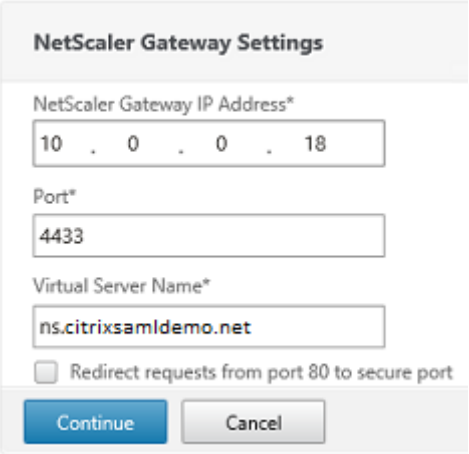
ライセンスを追加し、各ライセンスファイルが追加されたら ［再起動］を選択して、DNS リゾルバーが Microsoft ドメインコントローラーをポイントするようにします。

Citrix Virtual Apps and Desktops のインストールウィザードを実行する

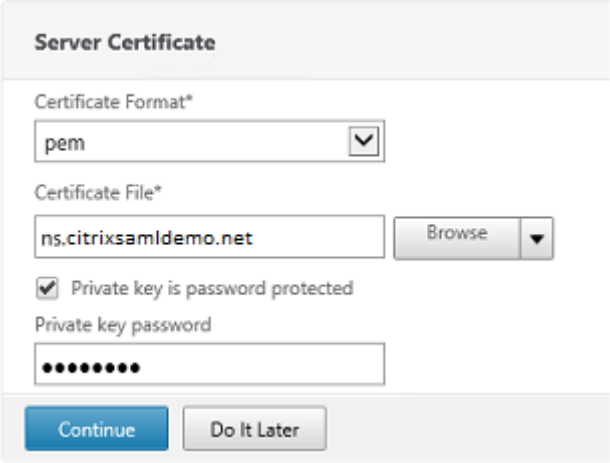
この例では、SAML を使用しない、シンプルな StoreFront 統合を構成することから始めます。この展開が機能するようになってから、SAML のログオンポリシーが追加されます。



Citrix Gateway および StoreFront の標準設定を選択します。Microsoft Azure での使用のため、この例ではポート 443 ではなく、ポート 4433 を構成します。あるいは、ポート転送したり、Citrix Gateway 管理 Web サイトを再マップしたりすることもできます。

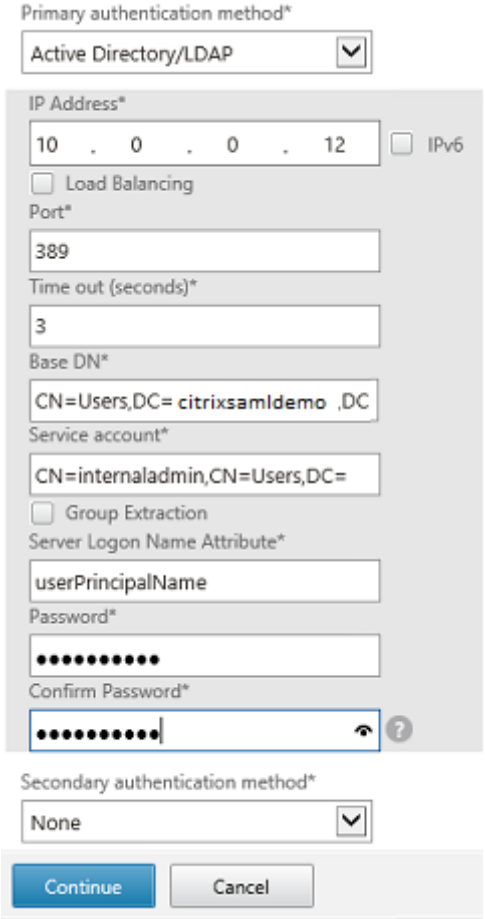


この例では、簡単にするために、ファイルに保存された既存のサーバー証明書と秘密キーをアップロードします。



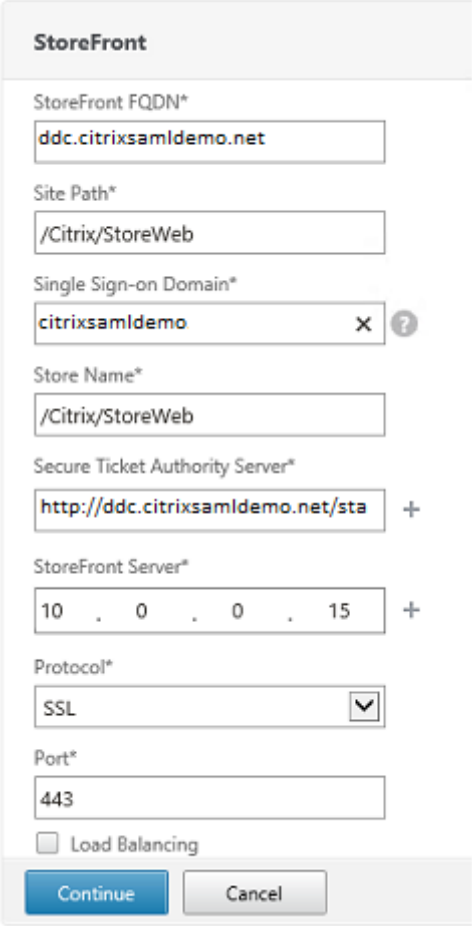
AD アカウント管理のためのドメインコントローラーの構成

ドメインコントローラーはアカウント解決に使用されるため、その IP アドレスをプライマリ認証方法に追加します。ダイアログボックスの各フィールドで求められる形式に注意してください。



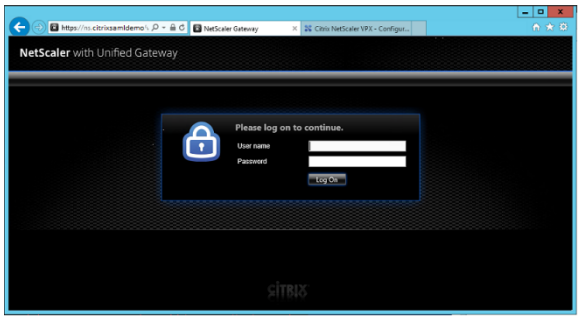
StoreFront アドレスの構成

この例では、HTTPS を使用して StoreFront が構成されているため、SSL プロトコルのオプションを選択します。



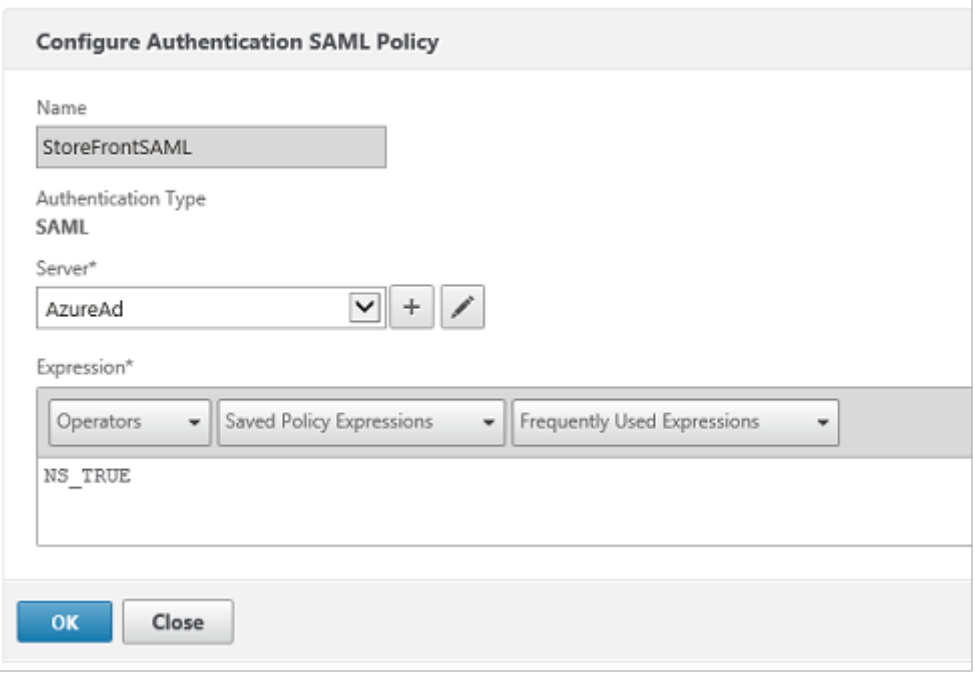
Citrix Gateway 展開の検証

Citrix Gateway に接続し、ユーザー名とパスワードを使用して、認証と起動が正常に行われることを確認します。

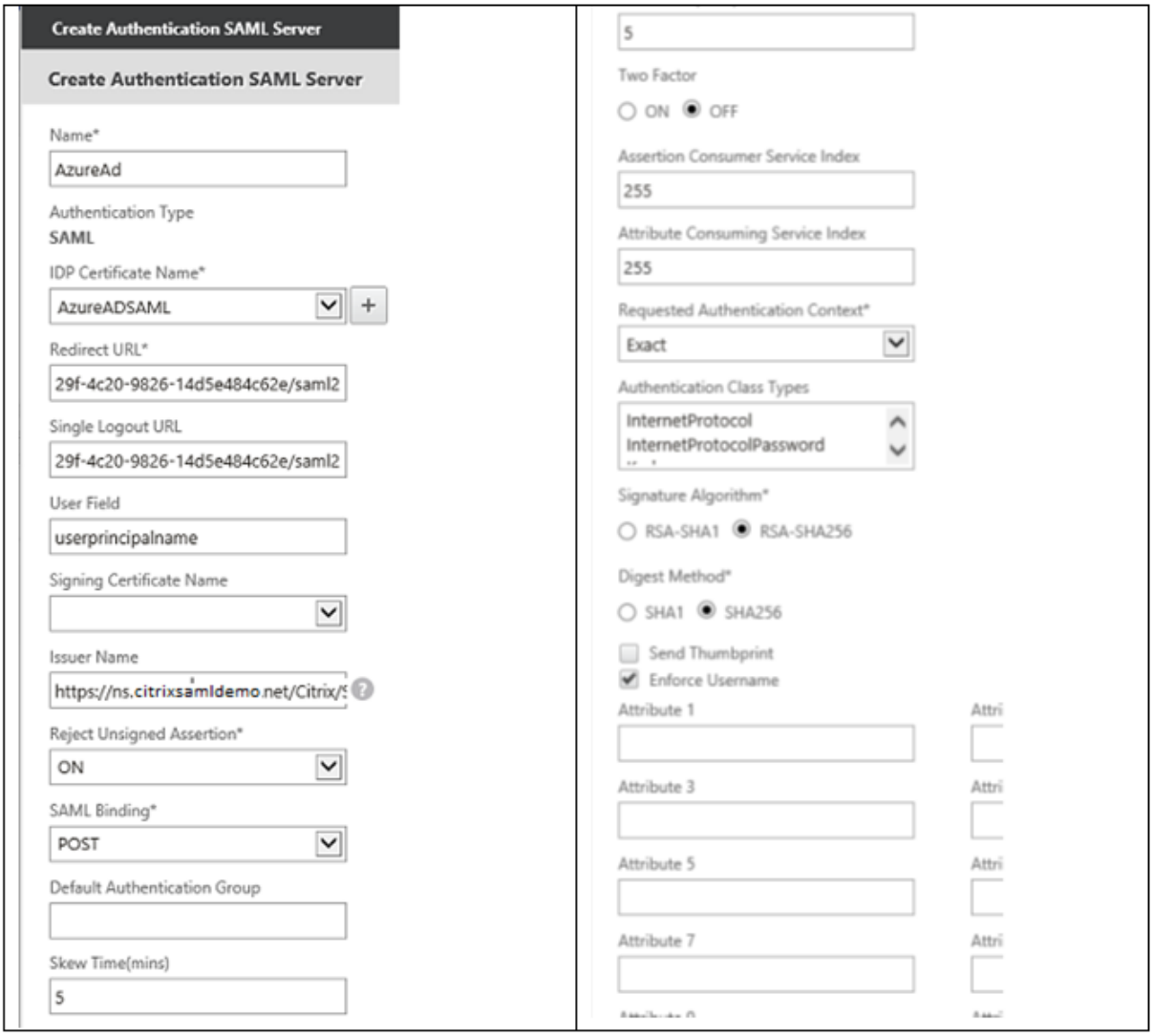


Citrix Gateway SAML 認証サポートの有効化

StoreFront での SAML の使用は、ほかの Web サイトで SAMl を使用するのと同様です。**NS_TRUE** の式を使用して、新しい SAML ポリシーを追加します。



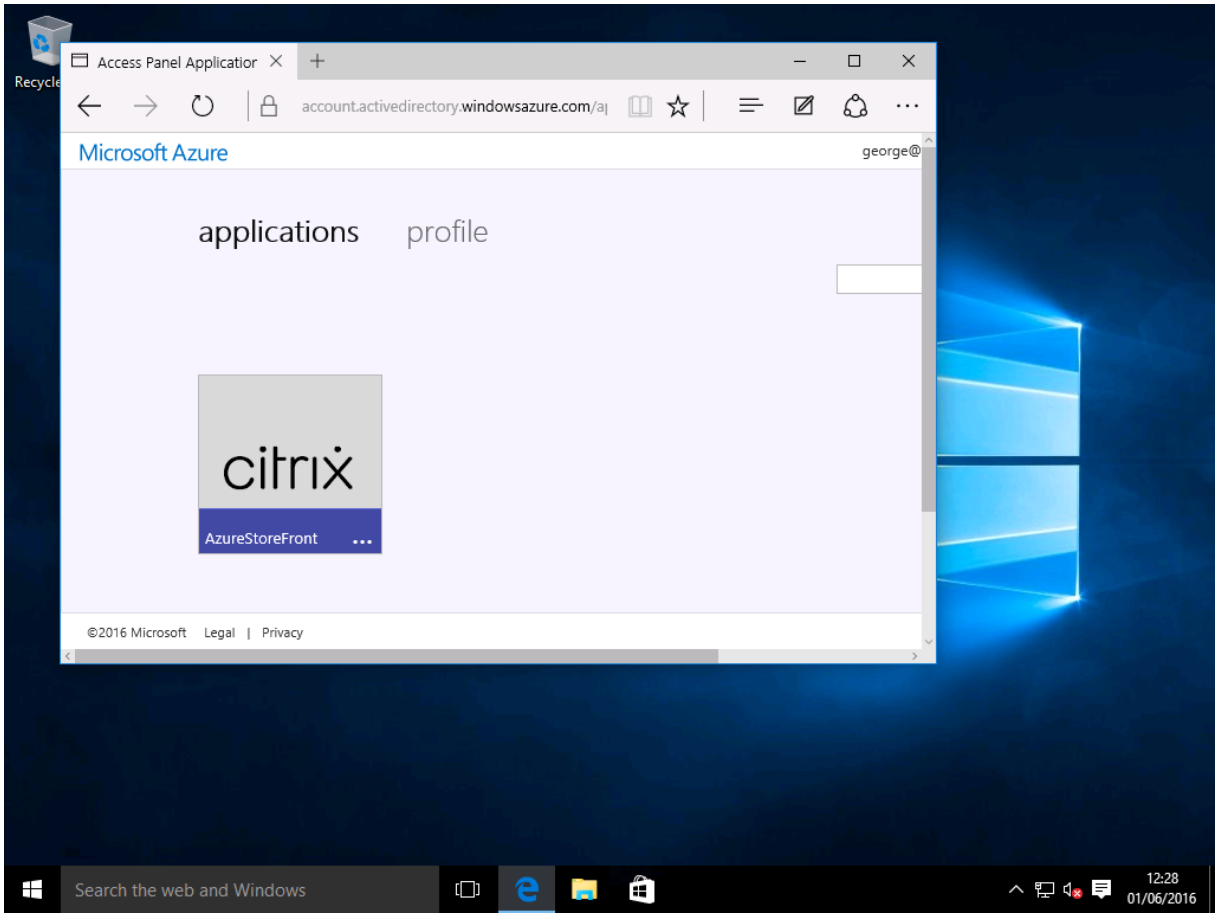
Azure AD から前に取得した情報を使用して、新しい SAML IdP サーバーを構成します。



エンドツーエンドシステムの検証

Azure AD に登録したアカウントを使用して、Azure AD に参加している Windows 10 デスクトップにログオンします。Microsoft Edge を起動してhttps://myapps.microsoft.comに接続します。

Web ブラウザーには、ユーザーの Azure AD アプリケーションが表示されます。



アイコンをクリックすると認証された StoreFront サーバーにリダイレクトされることを確認します。

同様に、シングルサインオン URL を使用した直接接続、および Citrix Gateway のサイトへの直接接続により、Microsoft Azure との間でリダイレクトされることを確認します。

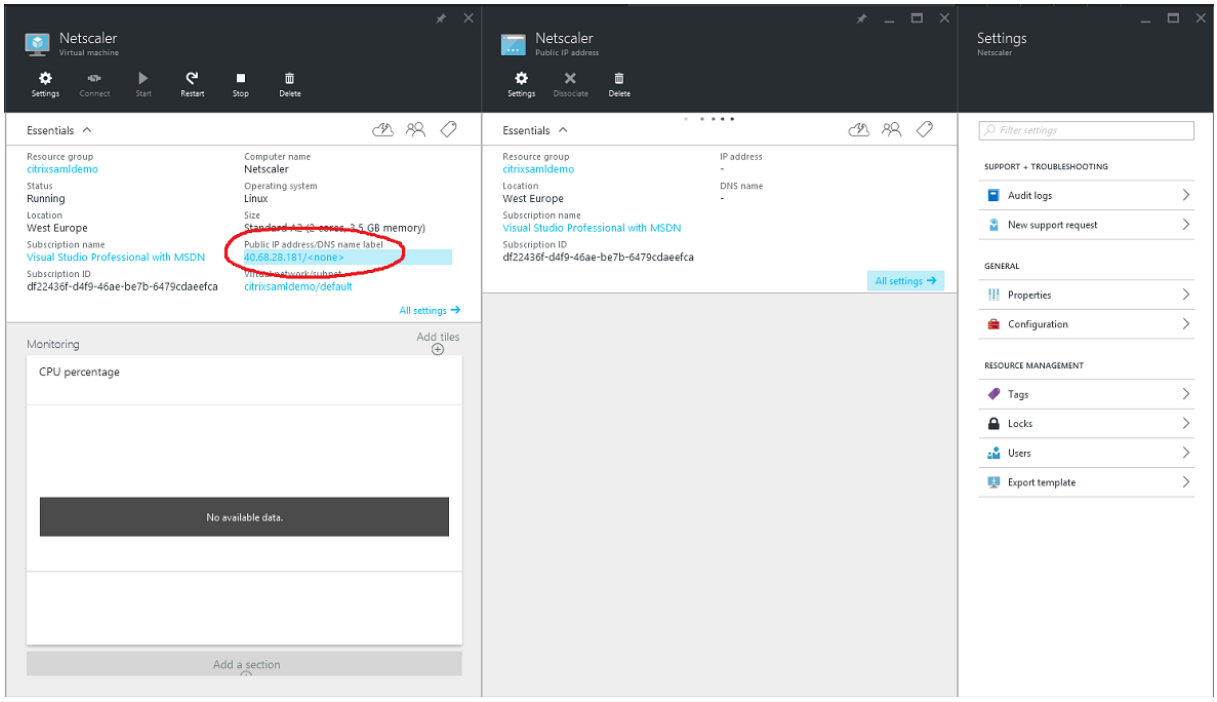
最後に、Azure AD に参加していないマシンも同じ URL で動作することを確認します（ただし、最初の接続時に、Azure AD への明示的なサインオンが 1 回行われます）。

付録

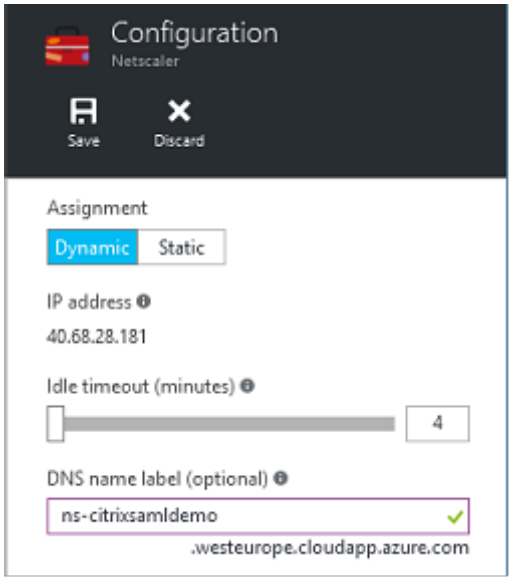
Azure で仮想マシンをセットアップするときには、次の標準オプションを構成してください。

パブリック **IP** アドレスと **DNS** アドレスの入力

Azure は内部サブネット上で、すべての仮想マシンに IP アドレスを提供します（この例では 10.*.*.*）。デフォルトでは、動的に更新された DNS ラベルで参照できる、パブリック IP アドレスも提供されます。



［パブリック **IP** アドレス**/DNS** 名］ラベルの［構成］を選択します。仮想マシンのパブリック DNS アドレスを選択します。これは、ほかの DNS ゾーンファイルでの CNAME 参照に使用でき、IP アドレスが再割り当てされた場合も、すべての DNS レコードが正しく仮想マシンをポイントするようにします。

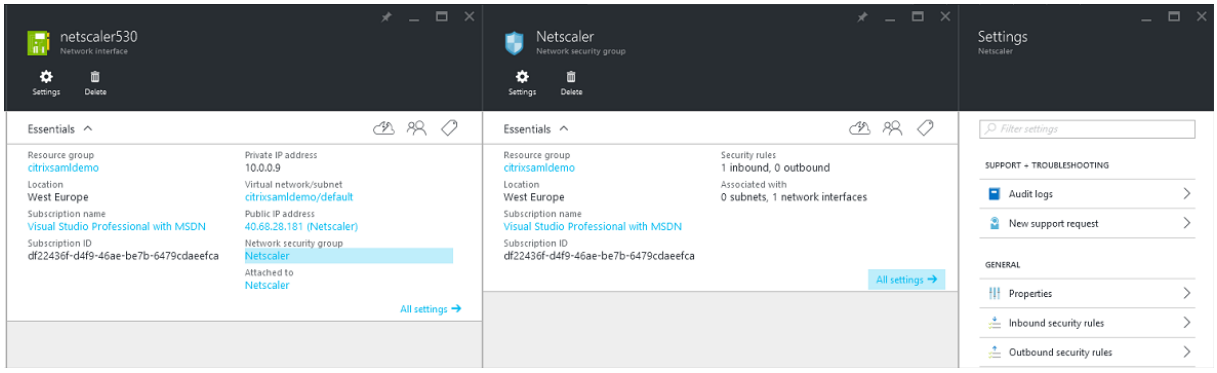


ファイアウォールルールのセットアップ（セキュリティグループ）

クラウド上の各仮想マシンには、自動的に適用されたファイアウォールルールのセットがあり、このセットはセキュリティグループとして知られています。セキュリティグループはパブリック IP アドレスからプライベート IP アドレスに転送されるトラフィックを制御します。デフォルトでは、Azure はすべての仮想マシンへの RDP の転送を許可

します。また、Citrix Gateway サーバーおよび ADFS サーバーは、TLS トラフィック（443）を転送する必要があります。

仮想マシンの［ネットワークインターフェイス］を開いて［ネットワークセキュリティグループ］ラベルをクリックします。［受信セキュリティ規則］を構成し、適切なネットワークトラフィックを許可します。



関連情報

- FAS のインストールと構成については、「インストールと構成」を参照してください。
- 一般的な FAS の展開については、「展開アーキテクチャ」を参照してください。
- 具体的な手順については、「詳細な構成」を参照してください。