联合身份验证服务

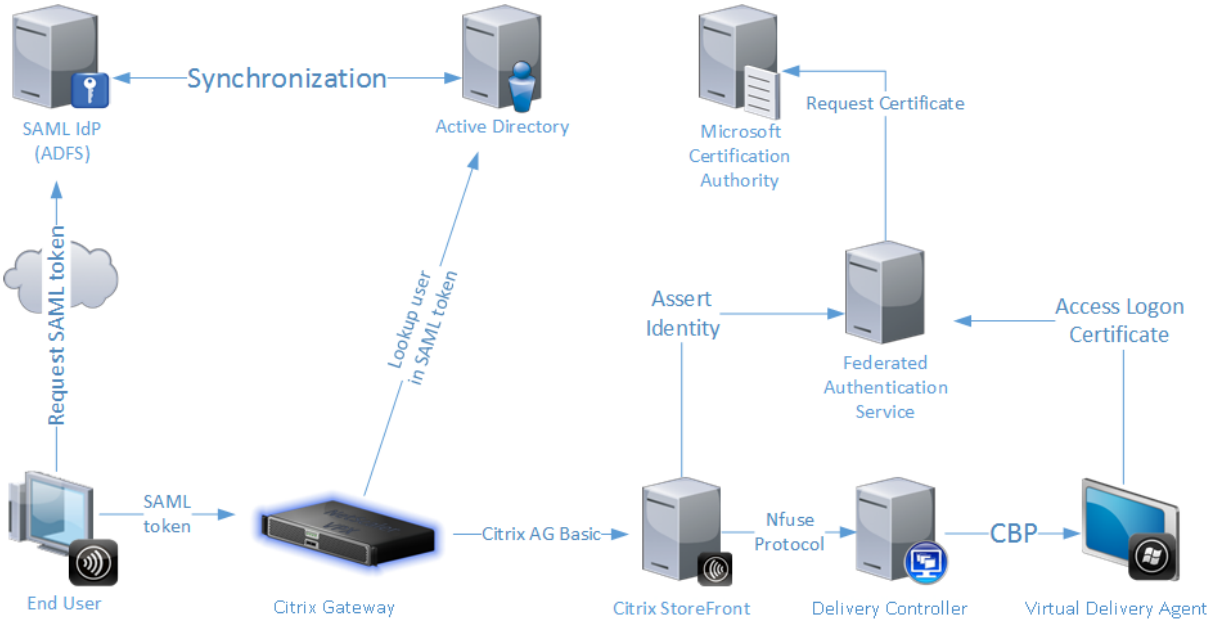
Contents

联合身份验证服务 **1909**

November 7, 2019

联合身份验证服务 (FAS) 是一个特权组件，可与 Active Directory 证书服务集成。它动态地为用户颁发证书，以便用户能够登录到 Active Directory 环境，就如同他们具有智能卡一样。这使得 StoreFront 能够使用范围更广的身份验证选项，例如 SAML（安全声明标记语言）声明。SAML 常用于替代 Internet 上的传统 Windows 用户帐户。

下图显示了 FAS 与 Microsoft 证书颁发机构集成，并向 StoreFront、Citrix Virtual Apps and Desktops Virtual Delivery Agent (VDA) 提供支持服务。



当用户请求访问 Citrix 环境时，可信 StoreFront 服务器会联系 FAS。FAS 将授予一个票据，允许单个 Citrix Virtual Apps 或 Citrix Virtual Desktops 会话使用该会话的证书进行身份验证。当 VDA 需要对用户进行身份验证时，它会连接到 FAS 并找回票据。仅 FAS 有权访问用户证书的私钥；VDA 必须发送每个签名和解密操作（它需要使用证书对 FAS 执行此操作）。

联合身份验证服务 **1909** 是 FAS 的最新当前版本。本文档介绍了此最新版本中的功能和配置。

早期版本

有关早期 FAS 版本的文档，请参阅：

- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1811

- Citrix Virtual Apps and Desktops 7 1808
- XenApp 和 XenDesktop 7.18
- XenApp 和 XenDesktop 7.17
- XenApp 和 XenDesktop 7.16
- 早期的 XenApp 和 XenDesktop 当前版本
- XenApp 和 XenDesktop 7.15 长期服务版本

生命周期里程碑中介绍了 XenServer 当前版本 (CR) 和长期服务版本 (LTSR) 产品生命周期策略。

引用

- Active Directory 证书服务 https://technet.microsoft.com/en-us/library/hh831740.aspx
- 配置 Windows 的登录证书 http://support.citrix.com/article/CTX206156

联合身份验证服务 **1909**

November 7, 2019

联合身份验证服务 1909 包括以下新增功能。有关缺陷修复的信息，请参阅已修复的问题。

FAS 管理控制台

联合身份验证服务 (FAS) 管理控制台已得到增强，其界面已焕然一新。FAS 产品文档已相应更新。管理控制台的功能改进包括以下功能：

- 从控制台内部配置多个 CA（以前此功能仅限 PowerShell），
- 从控制台内部使用新注册颁发机构证书重新授权 FAS（以前此功能仅限 PowerShell），
- 显示配置 FAS 时使用的注册机构证书，并在注册机构证书已过期或即将到期时向显示警告，
- 并行联系 CA（提高响应能力）。

以前随 FAS 安装的内置文档已删除。请改为参阅此在线文档。

FAS 错误相关 **ID**

与 FAS 有关的时间日志错误（记录在 StoreFront 或 Virtual Delivery Agent (VDA) 上）现在包含一个相关 ID。您可以使用该 ID 查找 FAS 服务器上的相应事件（可能包含更详细的错误信息），以帮助进行故障排除。

已修复的问题

November 7, 2019

以下问题自版本 1906 起已修复：

已知问题

November 7, 2019

联合身份验证服务 1909 包含以下问题。

此警告消息适用于任何建议更改注册表项的解决方法。

> 警告：
>
> 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

第三方声明

November 7, 2019

此版本的联合身份验证服务可能包含根据以下文档定义的条款获得许可的第三方软件：

- Citrix Virtual Apps and Desktops 第三方声明 （PDF 下载）
- 面向 FlexNet Publisher 2017 (11.15.0.0) 的非商用软件披露 （PDF 下载）
- FlexNet Publisher 文档补充：FlexNet Publisher 11.15.0 中使用的第三方软件和开源软件 （PDF 下载）

系统要求

September 27, 2019

当前支持的所有 Windows Server 版本都支持联合身份验证服务 (FAS)，请参阅 Citrix Virtual Apps 或 Citrix Virtual Desktops 系统要求。

- Citrix 建议在不包含其他 Citrix 组件的服务器上安装 FAS。

- Windows 服务器应受到保护。它将有权访问注册机构的证书和私钥，使其能够自动为域用户颁发证书，并将有权访问这些用户证书和私钥。

在 Citrix Virtual Apps 或 Citrix Virtual Desktops 站点中：

- Delivery Controller、Virtual Delivery Agent (VDA) 和 StoreFront 服务器都必须是当前支持的版本，请参阅 Citrix Virtual Apps 或 Citrix Virtual Desktops 系统要求。

  > 注意：
  >
  > FAS 在 XenApp 和 XenDesktop 7.6 长期服务版本 (LTSR) 中不受支持。

- 在创建计算机目录之前，必须对 VDA 正确应用联合身份验证服务组策略配置。有关详细信息，请参阅配置组策略部分。

在规划此服务的部署时，请查看安全注意事项部分。

安装和配置

November 7, 2019

安装和设置过程

1. 安装联合身份验证服务 (FAS)
2. 在 StoreFront 应用商店中启用 FAS 插件
3. 配置组策略
4. 使用 FAS 管理控制台可以执行以下操作：(a) 部署提供的模板，(b) 设置证书颁发机构，(c) 授权 FAS 使用您的证书颁发机构
5. 配置用户规则

安装联合身份验证服务

出于安全考虑，Citrix 建议将联合身份验证服务 (FAS) 安装在专用服务器上，并且此服务器应受到与域控制器或证书颁发机构类似的保护。可通过插入 ISO 时所显示的自动运行初始屏幕上的联合身份验证服务按钮安装 FAS。

这将安装以下组件：

- 联合身份验证服务
- PowerShell 管理单元 cmdlet，可远程配置 FAS
- FAS 管理控制台
- FAS 组策略模板 (CitrixFederatedAuthenticationService.admx/adml)
- 用于简单证书颁发机构配置的证书模板文件
- 性能计数器和事件日志

在 **StoreFront** 应用商店中启用 **FAS** 插件

要在 StoreFront 店上启用 FAS 集成，请使用管理员帐户运行以下 PowerShell cmdlet。如果您具有一个以上的 StoreFront，或者如果应用商店具有不同的名称，则下方的路径文本可能会有所不同。

```
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"
```

要停止使用 FAS，请使用以下 PowerShell 脚本：

```
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 ""
```

配置 **Delivery Controller**

要使用 FAS，请配置 Citrix Virtual Apps 或 Citrix Virtual Desktops Delivery Controller 以信任可与其连接的 StoreFront 服务器：运行 **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true** PowerShell cmdlet。

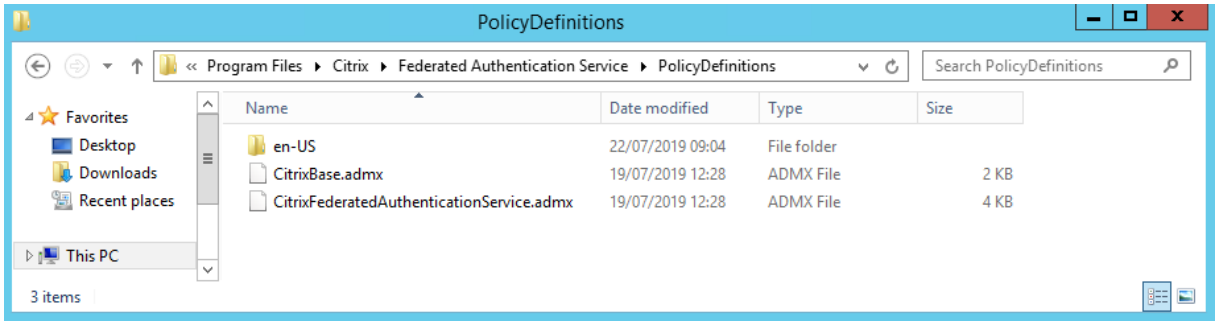
配置组策略

在安装 FAS 后，必须使用安装中提供的组策略模板指定组策略中的 FAS 服务器的完整 DNS 地址。

> 重要：
>
> 确保请求票据的 StoreFront 服务器和找回票据的 Virtual Delivery Agent (VDA) 具有相同的 DNS 地址配置，包括通过组策略对象应用的服务器自动编号。

为简单起见，以下示例在域级别配置单个策略以应用于所有计算机；但是，这并不是必需的。只要 StoreFront 服务器、VDA 以及正在运行 FAS 管理控制台的计算机查看到相同确定 DNS 地址列表，FAS 即可正常工作。请注意，组策略对象会向每一项添加一个索引号。如果使用多个对象，则索引号也必须匹配。

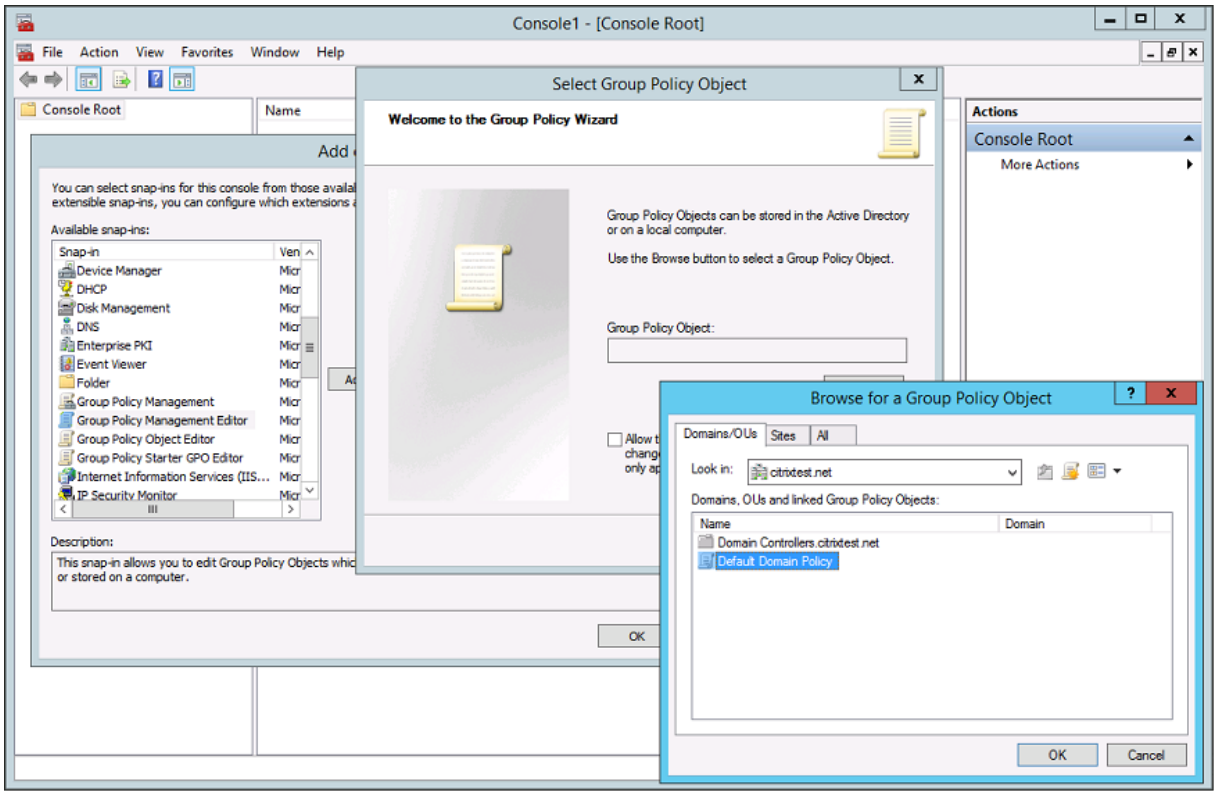
步骤 **1.** 在安装了 FAS 的服务器上，找到 C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx 和 CitrixBase.admx 文件以及 en-US 文件夹。



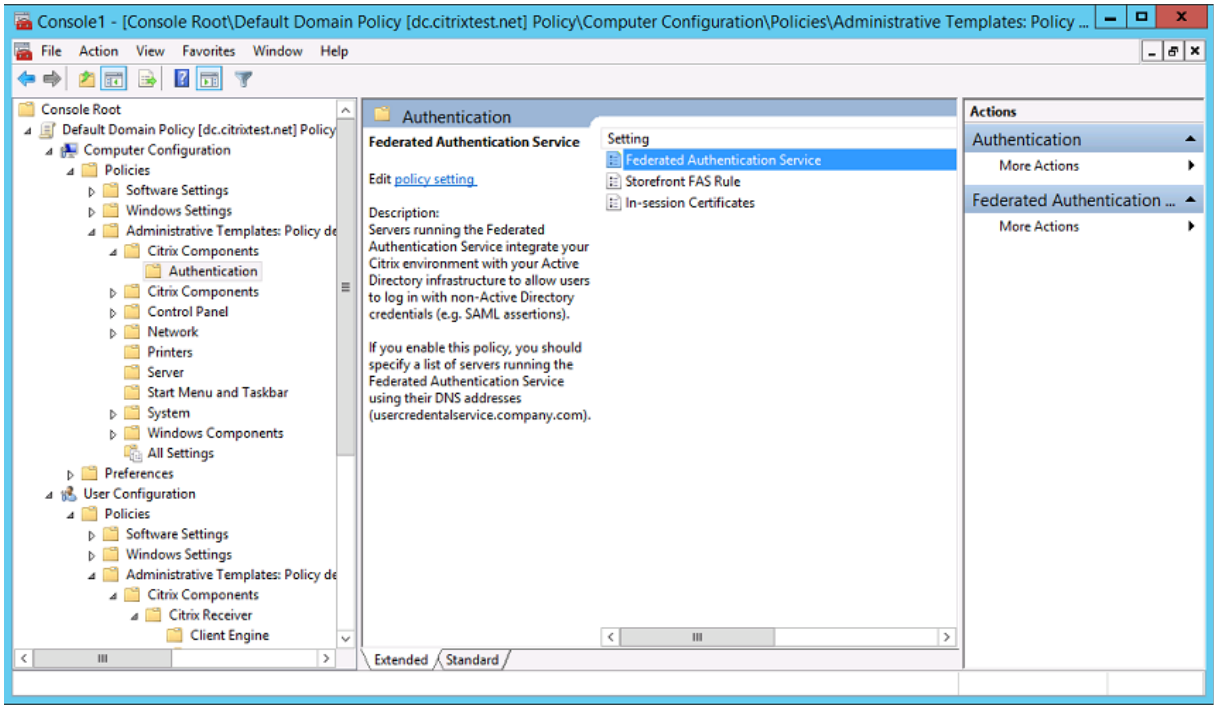
步骤 **2.** 将这些内容复制到您的域控制器，并将其放置在 C:\Windows\PolicyDefinitions 和 en-US 子文件夹中。

步骤 **3.** 运行 Microsoft 管理控制台（在命令行中运行 mmc.exe）。从菜单栏中选择文件 **>** 添加/删除管理单元。添加组策略管理编辑器。

当提示输入组策略对象时，选择浏览，然后选择默认域策略。或者，也可以使用您选择的工具为环境创建并选择相应策略对象。必须向运行相关 Citrix 软件（VDAs、StoreFront 服务器、管理工具）的所有计算机应用策略。

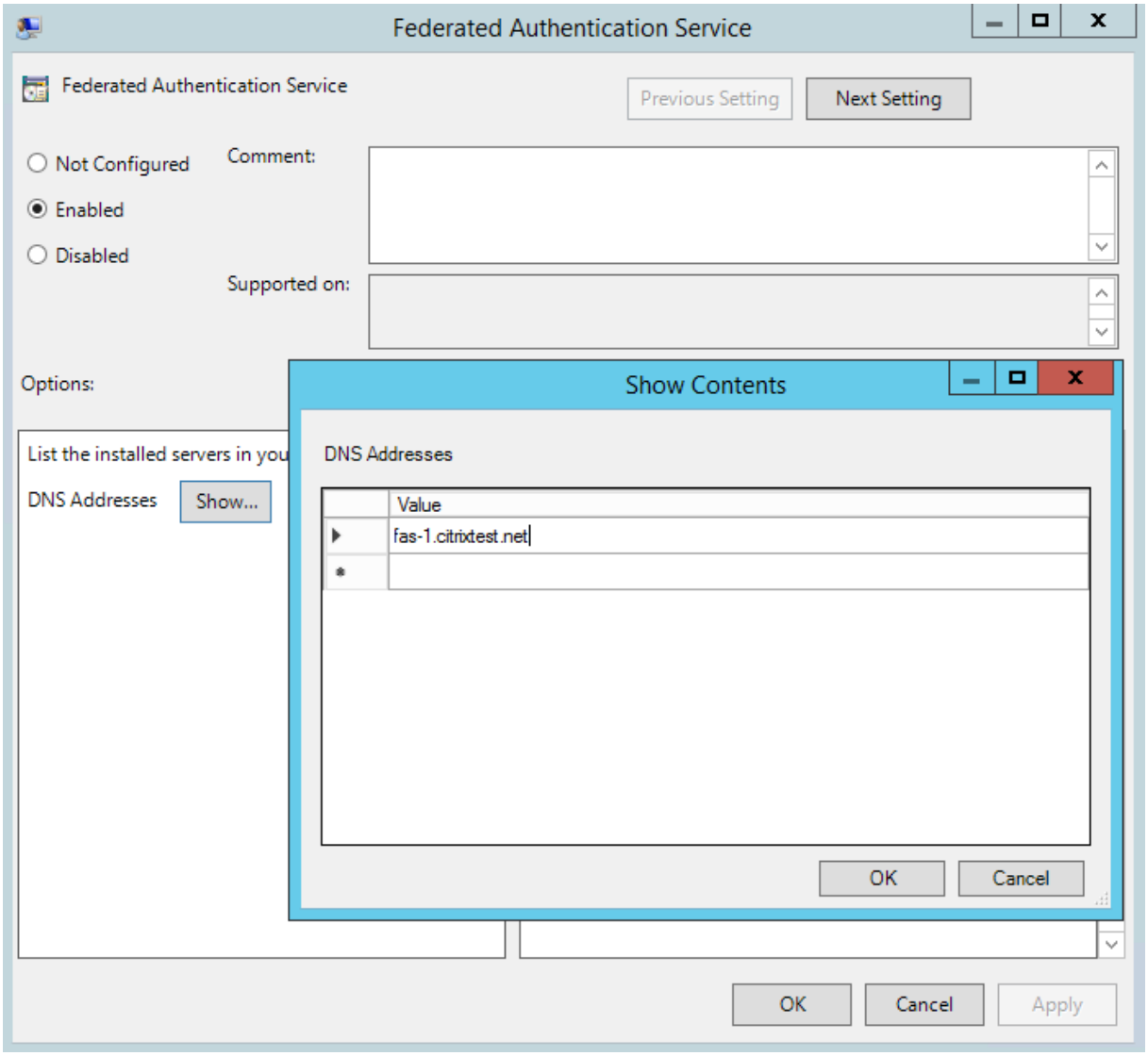


步骤 **4.** 导航到位于 Computer Configuration/Policies/Administrative Templates/Citrix Components/Authentication 的联合身份验证服务策略。



> 注意：
>
> 向 PolicyDefinitions 文件夹添加 CitrixBase.admx/CitrixBase.adml 模板文件时，“联合身份验证服务”策略设置仅在域 GPO 中可用。“联合身份验证服务”策略设置随后将在“管理模板”>“Citrix 组件”>“身份验证”文件夹中列出。

步骤 **5.** 打开“联合身份验证服务”策略，并选择启用。这将允许您选择显示按钮，然后配置 FAS 服务器的 DNS 地址。



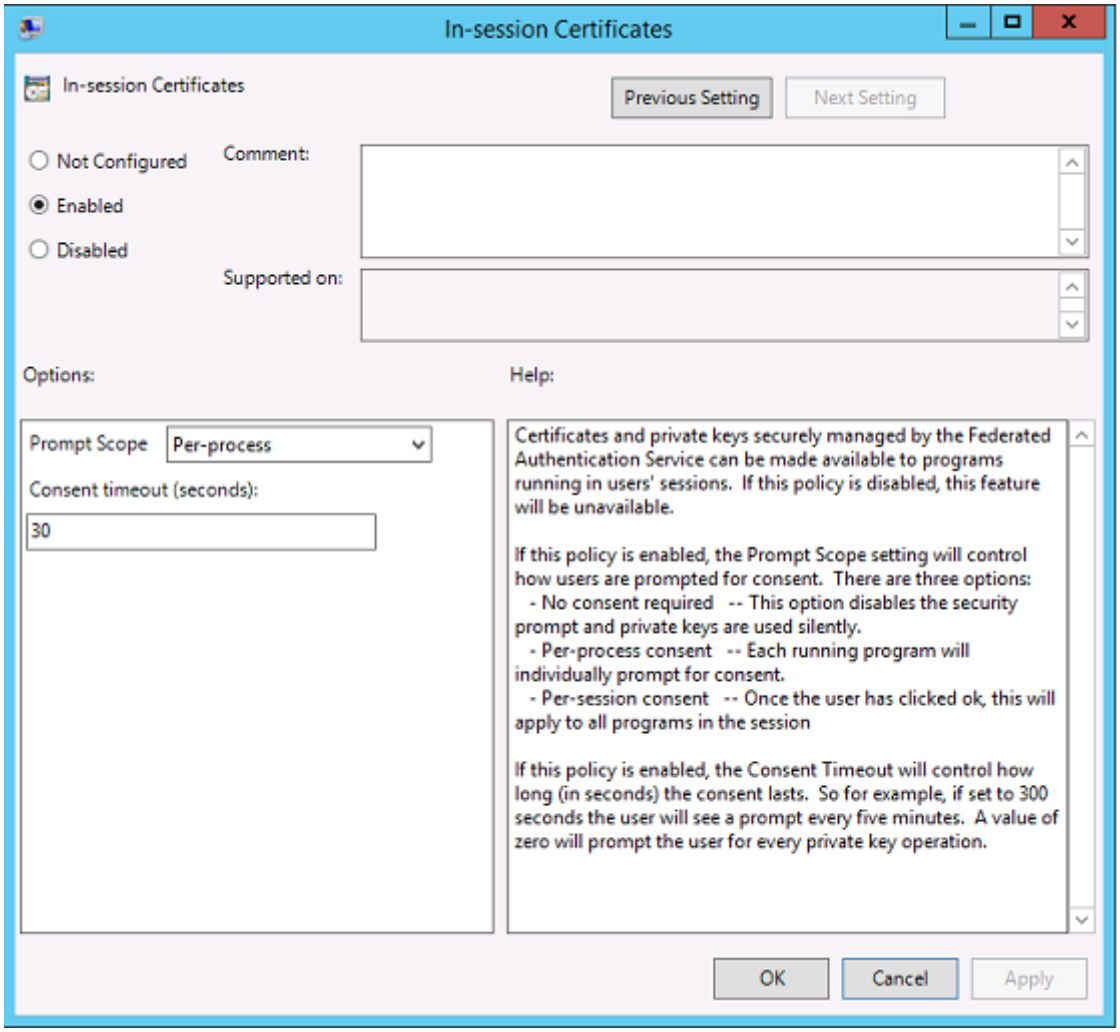
步骤 **6.** 输入托管 FAS 的服务器的完全限定域名 (FQDN)。

谨记： 如果您输入多个 FQDN，则列表的顺序必须在 StoreFront 服务器和 VDA 之间一致。这包括空白或未使用的列表条目。

步骤 **7.** 单击确定退出“组策略”向导并应用所执行的组策略更改。您可能需要重新启动计算机（或在命令行中运行 **gpupdate /force**）以使更改生效。

会话中证书支持

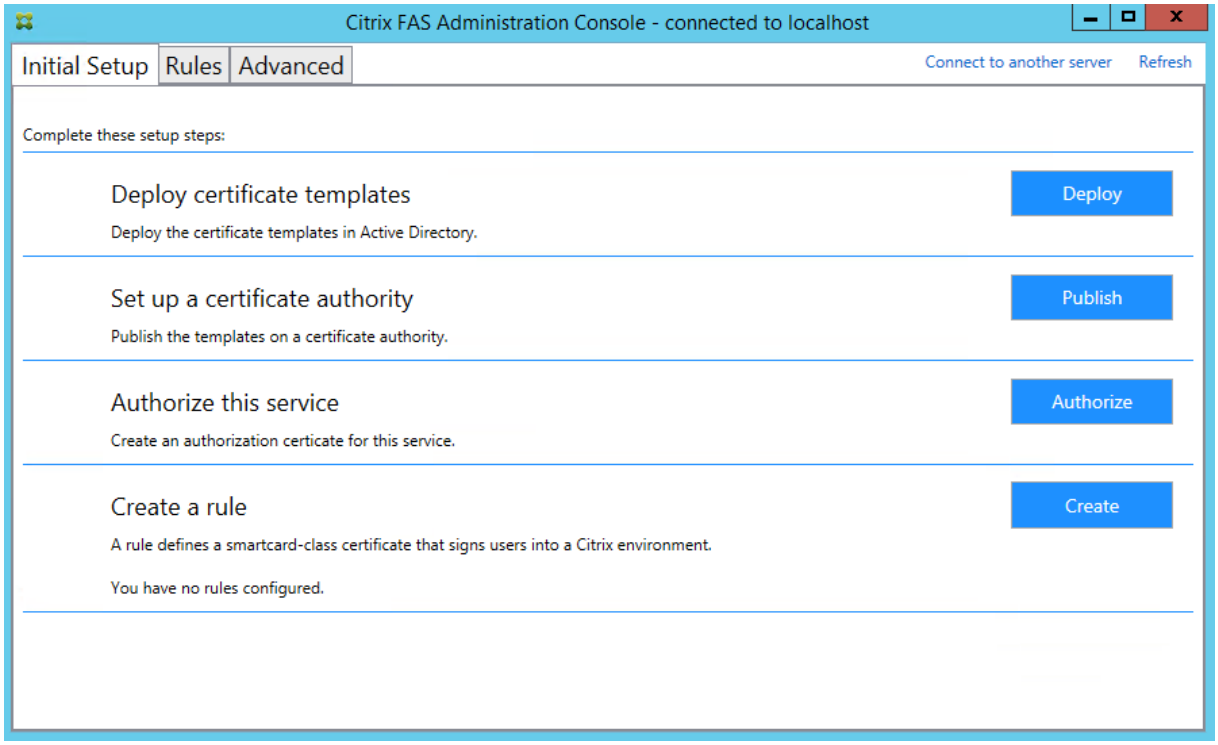
默认情况下，VDA 不允许在登录后访问证书。如有必要，可以使用组策略模板为会话中证书配置系统。这样，会在登录后将证书放置在用户的个人证书存储中，以供应用程序使用。例如，如果您需要在 VDA 会话中对 Web 服务器执行 TLS 身份验证，则可通过 Internet Explorer 使用证书。



使用联合身份验证服务管理控制台

FAS 管理控制台作为 FAS 的一部分安装。将在“开始”菜单中显示一个图标（Citrix 联合身份验证服务）。

首次使用管理控制台时，它会引导您完成部署证书模板、设置证书颁发机构以及授权 FAS 使用该证书颁发机构的过程。也可以使用操作系统配置工具手动完成其中一些步骤。

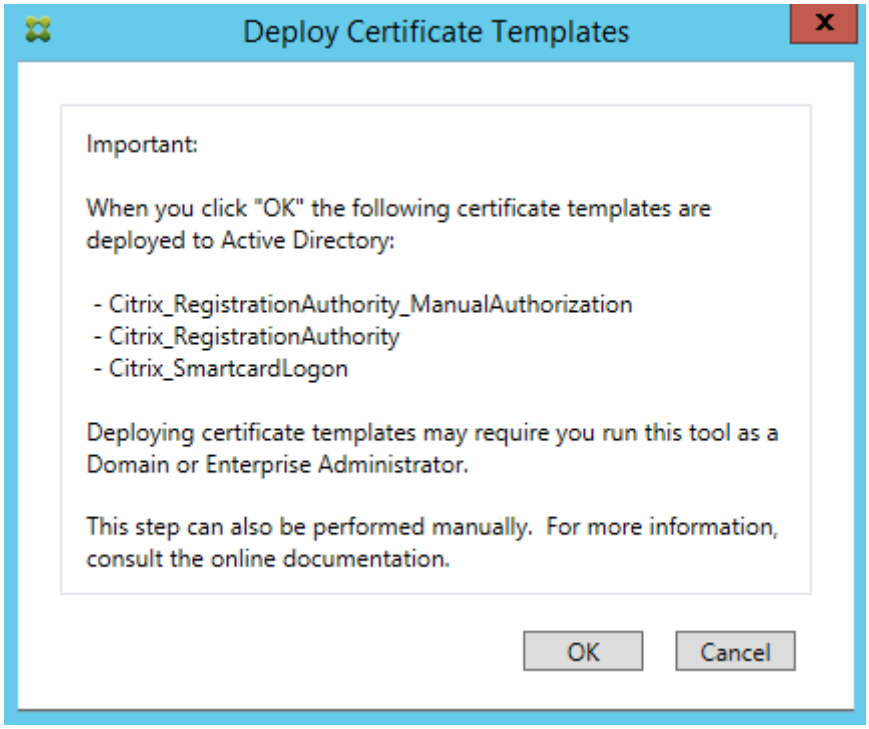


部署证书模板

为了避免发生与其他软件的互操作性问题，FAS 提供了三个 Citrix 证书模板以供其自己使用。

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

必须向 Active Directory 注册这些模板。如果控制台无法找到它们，部署证书模板工具可以安装它们。必须以有权管理您的企业林的帐户来运行此工具。



可在随 FAS 安装的 XML 文件（具有.certificatetemplate 扩展名）中找到模板配置：

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

如果无权安装这些模板文件，请将其提供给您的 Active Directory 管理员。

要手动安装这些模板，可以使用下面的 PowerShell 命令：

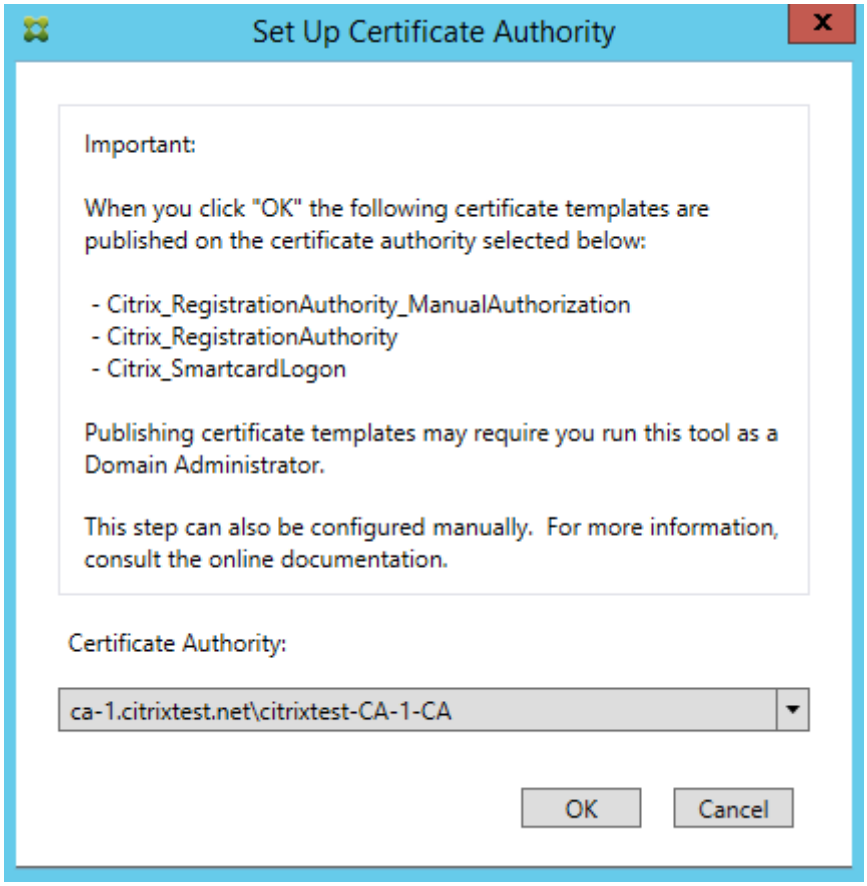
```
$template = [System.IO.File]::ReadAllBytes("$Pwd\Citrix_SmartcardLogon.certificatetemplate")
$CertEnrol = New-Object -ComObject X509Enrollment.CX509EnrollmentPolicyWebService
$CertEnrol.InitializeImport($template)
$comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)
$writabletemplate = New-Object -ComObject X509Enrollment.CX509CertificateTemplateADWritable
$writabletemplate.Initialize($comtemplate)
$writabletemplate.Commit(1, $NULL)
```

设置 **Active Directory** 证书服务

安装 Citrix 证书模板后，必须在一个或多个 Microsoft 证书颁发机构服务器中发布它们。请参阅有关如何部署 Active Directory 证书服务的 Microsoft 文档。

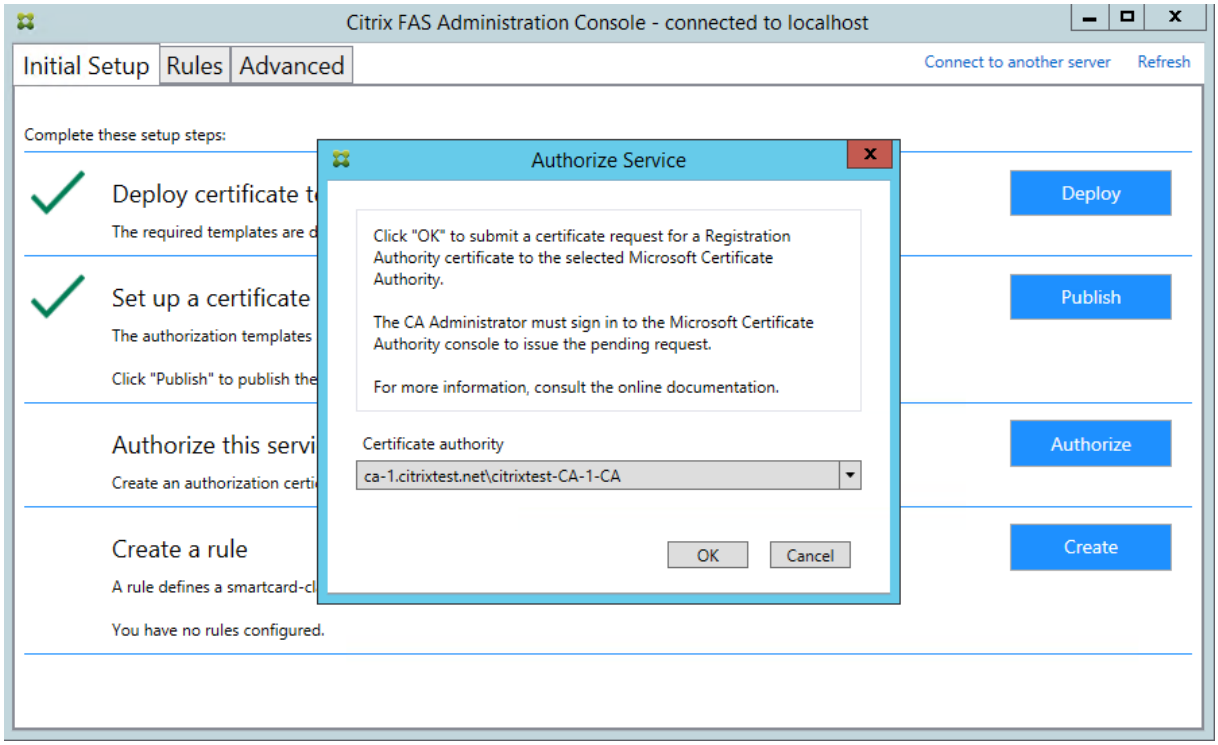
如果未至少在一台服务器上发布模板，则设置证书颁发机构工具将主动发布它们。您必须以有权管理证书颁发机构的用户身份运行此工具。

（也可以使用 Microsoft 证书颁发机构控制台发布证书模板。）

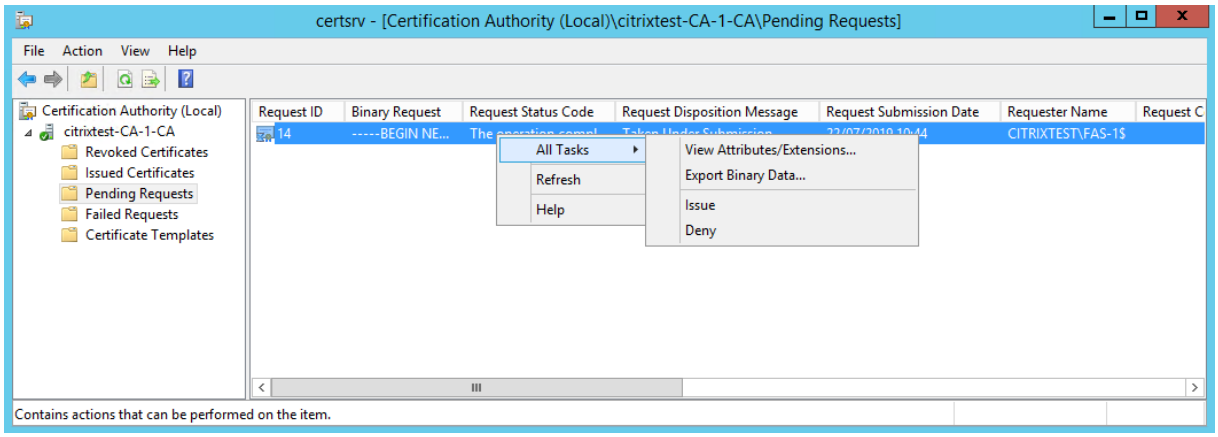


授权联合身份验证服务

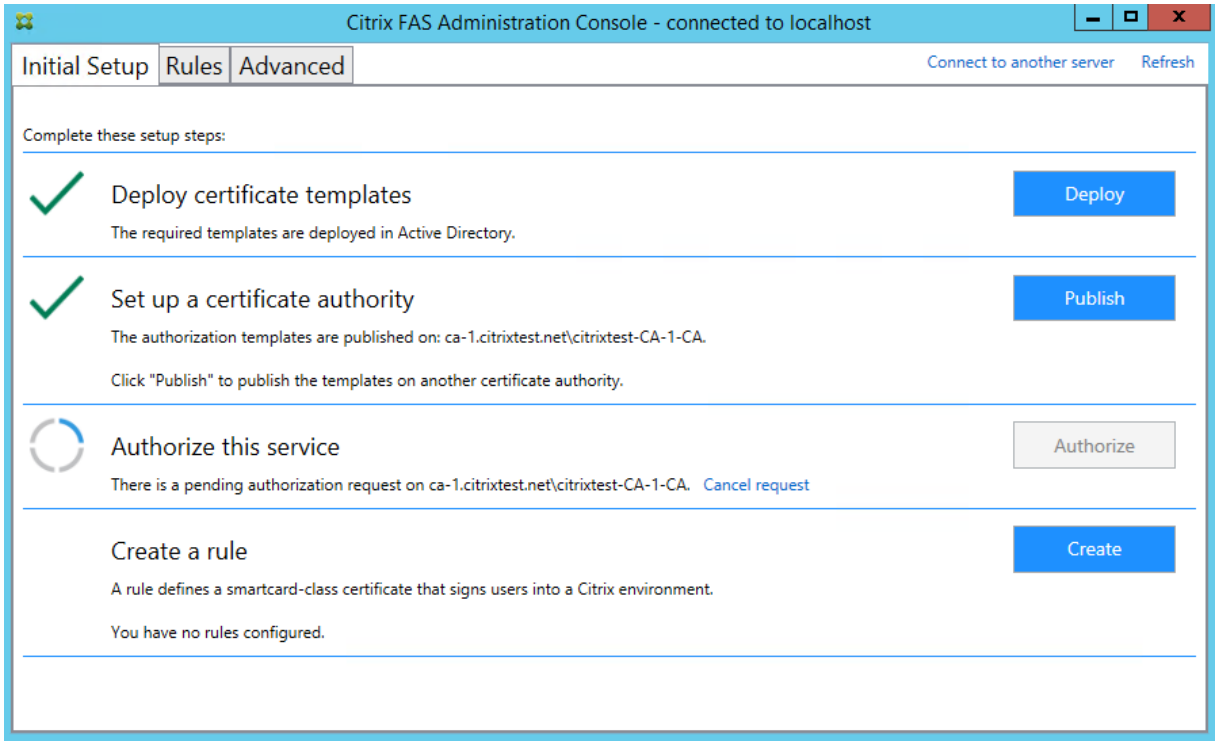
此步骤启动 FAS 的授权。管理控制台使用 Citrix_RegistrationAuthority_ManualAuthorization 模板生成一个证书请求，然后将其发送到用于发布该模板的证书颁发机构之一。



在发送请求后，该请求将出现在 Microsoft 证书颁发机构控制台的挂起的请求列表中。证书颁发机构管理员必须选择 **Issue**（颁发）或 **Deny**（拒绝）请求，然后才能继续配置 FAS。请注意，授权请求将显示为来自 FAS 计算机帐户的挂起的请求。



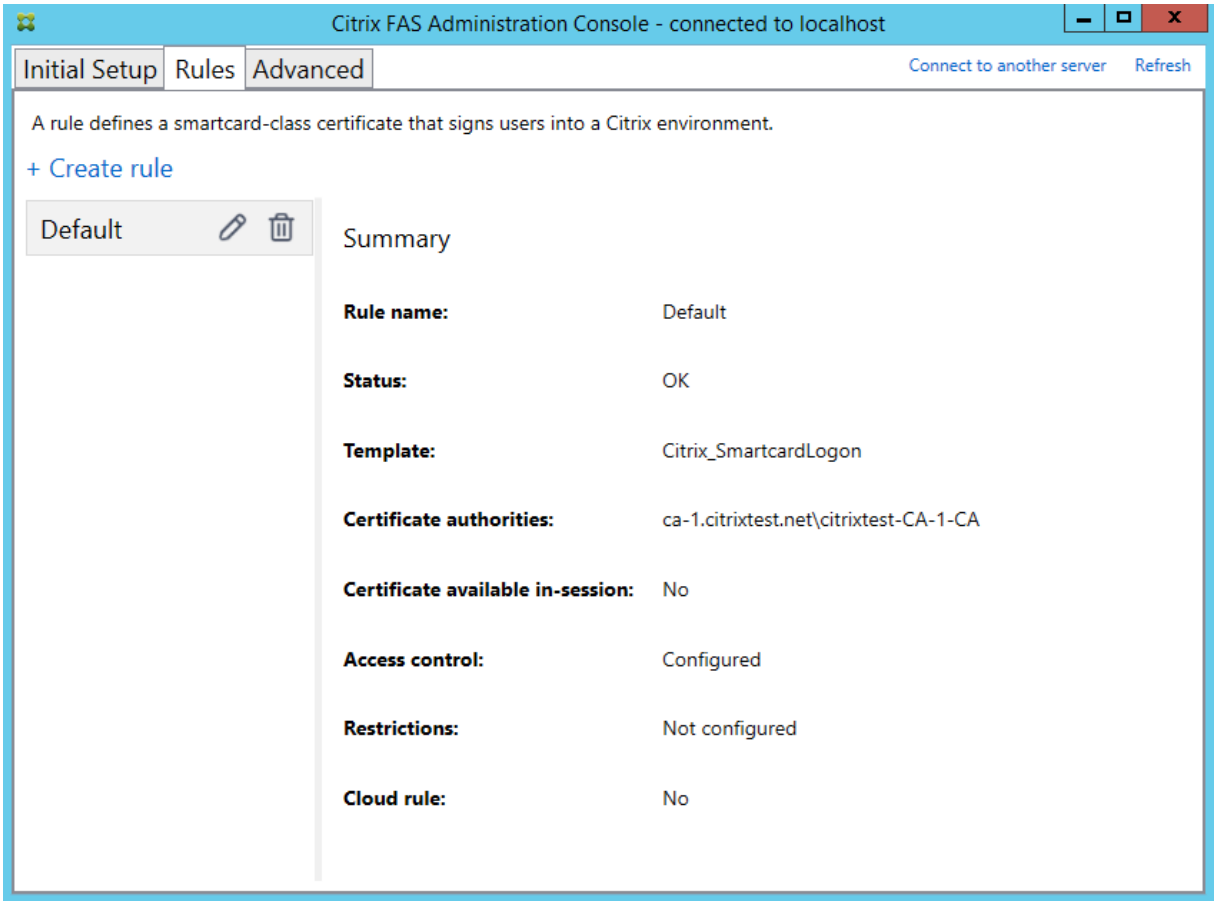
右键单击所有任务，然后选择颁发或拒绝证书请求。FAS 管理控制台会自动检测此过程的完成时间。这可能需要几分钟的时间。



配置用户规则

用户规则将按 StoreFront 的指令来授权颁发用于在登录 VDA 时及会话中使用的证书。每个规则将指定受信任请求证书的 StoreFront 服务器、这些服务器可以请求的用户集，以及可使用它们的 VDA 计算机集。

要完成 FAS 设置，您必须定义默认规则。单击 **Create**（创建）创建规则或切换到“Rules”（规则）选项卡，然后单击 **Create rule**（创建规则）。向导收集定义规则所需的信息。



向导会收集以下信息：

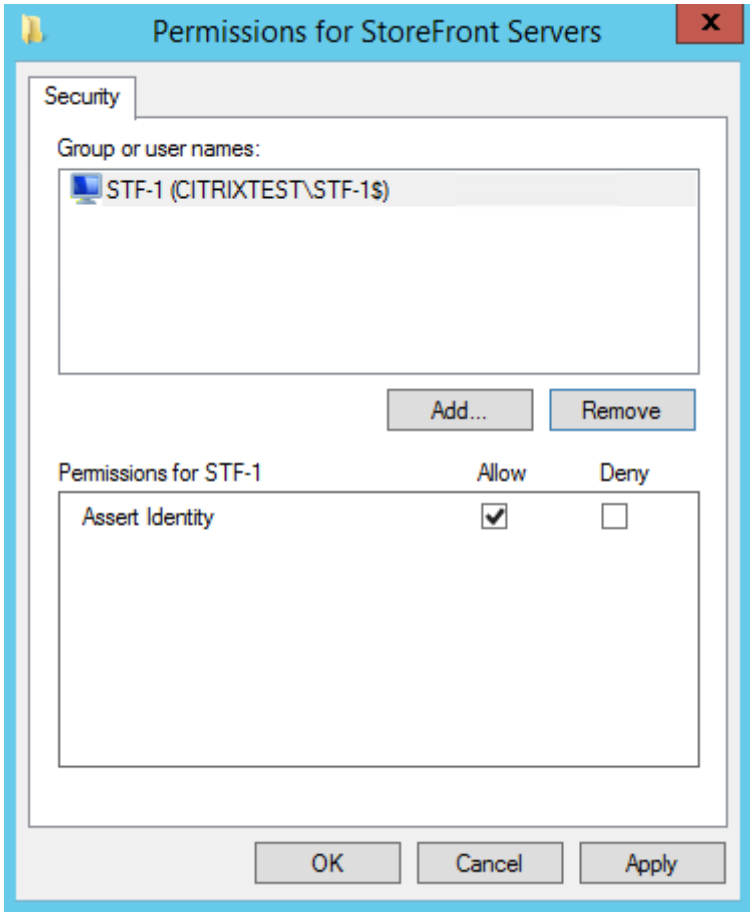
Template（模板）：用于颁发用户证书的证书模板。这应是 Citrix_SmartcardLogon 模板，或者其已修改的副本。

Certificate Authority（证书颁发机构）：颁发用户证书的证书颁发机构。模板必须由证书颁发机构发布。FAS 支持添加多个证书颁发机构以用于故障转移和负载平衡。

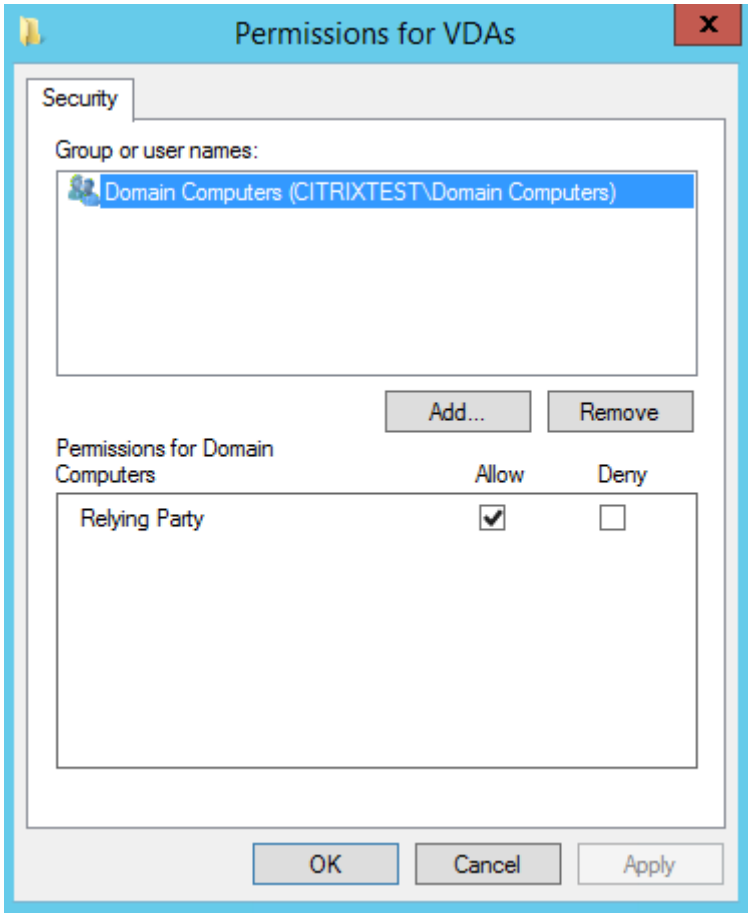
In-Session Use（会话中使用）：**Allow in-session use**（允许会话中使用）选项控制在登录到 VDA 后是否可以使用证书。仅当您希望用户在进行身份验证后对证书具有访问权限时才选择此选项。如果未选择此选项，则只会将证书用于登录或重新连接，并且用户在进行身份验证后对证书没有访问权限。

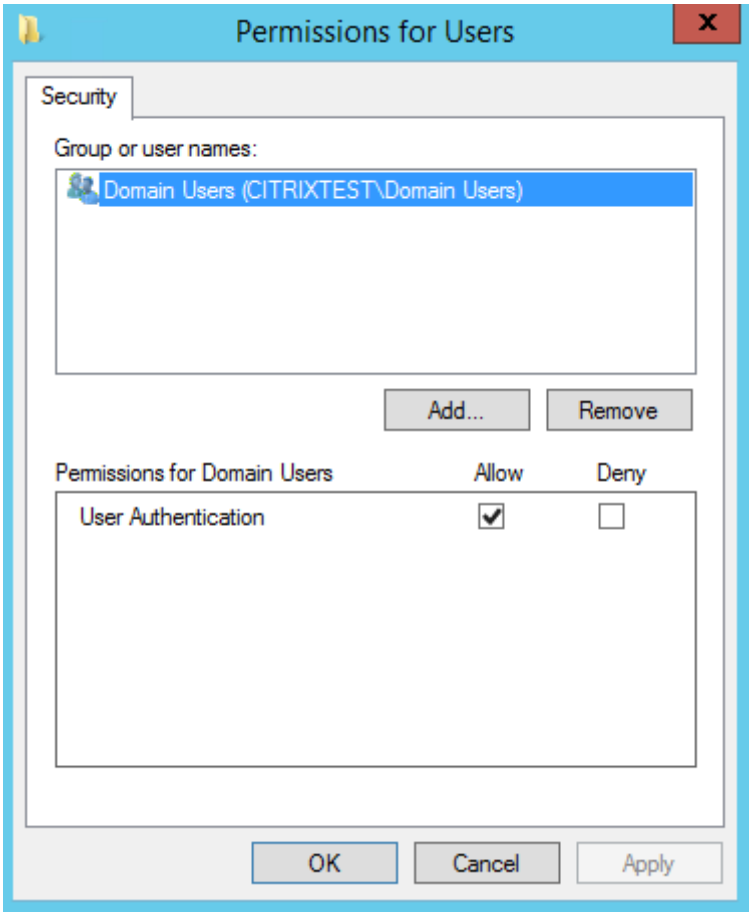
Access control（访问控制）：被授权请求用于用户登录或重新连接过程的证书的可信 StoreFront 服务器计算机的列表。

> 重要：
>
> **Access control**（访问控制）设置对于安全性至关重要，因此必须谨慎地加以管理。



Restrictions（限制）：可以记录用户使用 FAS 的 VDA 计算机的列表以及可以通过 FAS 颁发证书的用户列表。VDA 列表默认为“域计算机”，用户列表默认为“域用户”列表；如果默认值不适当，可以更改这些值。





Cloud rule（云规则）：当前不支持。

高级用法

可以创建其他规则来引用不同的证书模板和颁发机构。可为它们配置不同的属性和权限。这些规则可配置为由不同的 StoreFront 服务器（将需要对其进行配置以便按名称请求新规则）使用。默认情况下，在联系 FAS 时，StoreFront 会请求默认设置。可以通过使用“组策略配置”选项对其进行更改。

要创建新证书模板，请在 Microsoft 证书颁发机构控制台中复制 Citrix_SmartcardLogon 模板，将其重命名（例如 Citrix_SmartcardLogon2），并根据需要进行修改。通过单击添加引用新证书模板来创建新用户规则。

升级注意事项

- 执行原位升级时，将保留所有 FAS 服务器设置。
- 请通过运行 Virtual Apps and Desktops 的完整产品安装程序来升级 FAS。
- 在升级 FAS 之前，请将 Controller 和 VDA（以及其他核心组件）升级到所需版本。
- 请务必在升级 FAS 之前关闭 FAS 管理控制台。

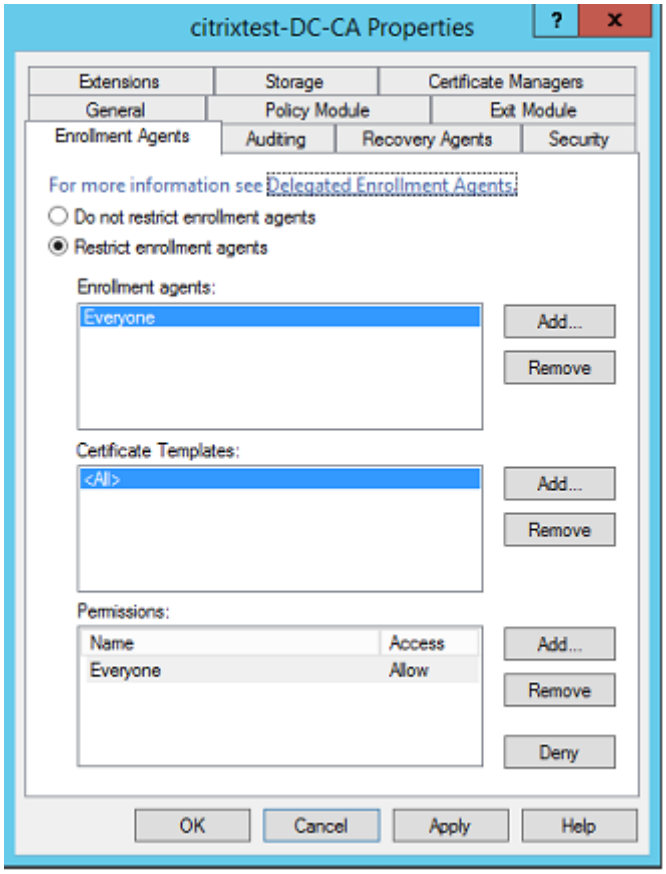
- 请确保至少一个 FAS 服务器始终可用。如果启用了联合身份验证服务的 StoreFront 服务器无法访问任何服务器，用户将无法登录或启动应用程序。

安全注意事项

FAS 具有注册机构证书，允许它代表您的域用户自主颁发证书。因此，必须制定并实施安全策略来保护 FAS 服务器，并限制其权限。

委派注册代理

FAS 充当注册代理来颁发用户证书。Microsoft 证书颁发机构可以控制可由 FAS 服务器使用的模板，以及限制 FAS 服务器可为其颁发证书的用户。



Citrix 强烈建议配置这些选项，以便 FAS 只能为目标用户颁发证书。例如，建议阻止 FAS 向“管理”或“受保护的用户”组中的用户颁发证书。

访问控制列表配置

如配置用户规则部分中所述，您必须配置可信 StoreFront 服务器的列表证书，以便在颁发证书时向 FAS 声明用户身份。同样，您可以限制将为其颁发证书的用户，以及用户可向其进行身份验证的 VDA 计算机。这是对您配置的任何标准 Active Directory 或证书颁发机构安全功能的补充。

防火墙设置

与 FAS 服务器的所有通信均通过端口 80 以相互身份验证的 Windows Communication Foundation (WCF) Kerberos 网络连接。

事件日志监视

FAS 和 VDA 会将信息写入 Windows 事件日志。此信息可以用于监视和审核信息。事件日志部分列出了可生成的事件日志条目。

硬件安全模块

所有私钥，包括由 FAS 颁发的用户证书的私钥，均通过网络服务帐户存储为不可导出的私钥。FAS 支持使用加密硬件安全模块（如果您的安全策略需要此模块）。

在 FederatedAuthenticationService.exe.config 文件中提供了低级别的加密配置。当首次创建私钥时，将应用这些设置。因此，可将不同的设置用于注册机构私钥（例如，4096 位，受 TPM 保护）和运行时用户证书。

参数	说明
ProviderLegacyCsp	当设置为 true 时，FAS 使用 Microsoft CryptoAPI (CAPI)。否则，FAS 将使用 Microsoft Cryptography Next Generation API (CNG)。
ProviderName	要使用的 CAPI 或 CNG 提供程序的名称。
ProviderType	请参阅 Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24。应该始终为 24，除非您使用 CAPI 与 HSM 并且 HSM 提供商另有规定。
KeyProtection	控制私钥的“可导出”标志。如果硬件支持，还允许使用受信任的平台模块 (TPM) 密钥存储。
KeyLength	RSA 私钥的密钥长度。支持的值包括 1024、2048 和 4096（默认值：2048）。

PowerShell SDK

虽然 FAS 管理控制台适用于简单部署，但是 PowerShell 界面提供了更高级选项。当您要使用在控制台中不可用的选项时，Citrix 建议仅使用 PowerShell 执行配置。

以下命令将添加 PowerShell cmdlet：

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

使用 **Get-Help** <*cmdlet name*> 显示 cmdlet 帮助信息。下表列出了几个命令，其中 * 表示标准 PowerShell 谓词（例如新建、获取、设置、删除）。

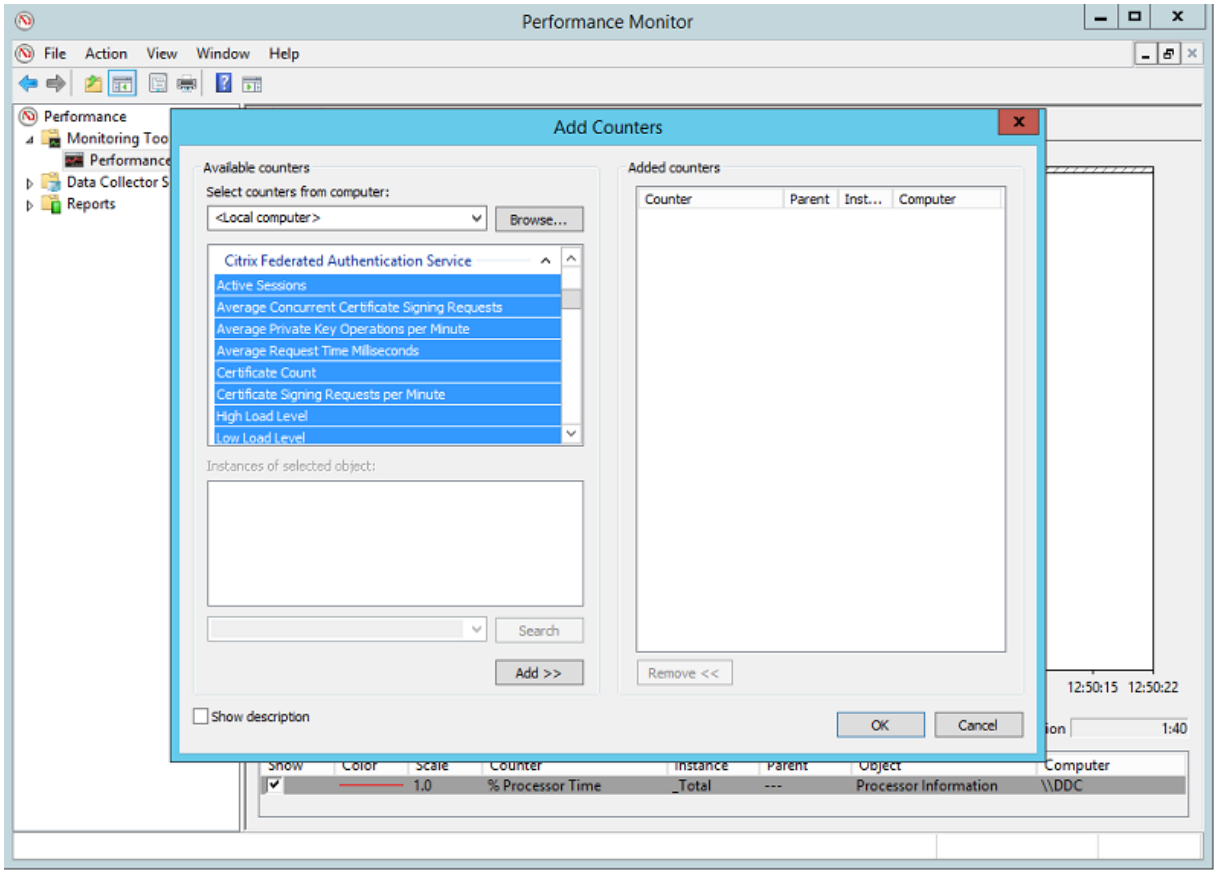
命令	概述
*-FasServer	列出并重新配置当前环境中的 FAS 服务器。
*-FasAuthorizationCertificate	管理“注册机构”证书。
*-FasCertificateDefinition	控制由 FAS 用于生成证书的参数。
*-FasRule	管理在 FAS 上配置的用户规则。
*-FasUserCertificate	列出并管理 FAS 缓存的证书。

可通过指定 FAS 服务器地址来远程使用 PowerShell cmdlet。

有关 FAS PowerShell cmdlet 的信息，请参阅 PowerShell cmdlet。

性能计数器

FAS 包括一组用于跟踪负载的性能计数器。



下表列出了可用的计数器。大多数计数器会在五分钟后滚动平均值。

名称	说明
活动会话	FAS 跟踪的连接数。
并发 CSR	在同一时间处理的证书申请数。
私钥 OPS	每分钟执行的私钥操作数。
请求时间	生成并签署证书所用的时间长度。
证书计数	在 FAS 中缓存的证书数。
每分钟的 CSR	每分钟处理的证书签名请求数量。
低/中/高	以“每分钟 CSR 数”为依据估算 FAS 可接受的负载。如果超过“高负载”阈值，可能会导致会话启动失败。

事件日志

以下各表列出了由 FAS 生成的事件日志条目。

管理事件

[事件来源：Citrix.Authentication.FederatedAuthenticationService]

将记录这些事件，以响应 FAS 服务器的配置变化。

日志代码
[S001] ACCESS DENIED: User [{0}] is not a member of Administrators group
[S002] ACCESS DENIED: User [{0}] is not an Administrator of Role [{1}]
[S003] Administrator [{0}] setting Maintenance Mode to [{1}]
[S004] Administrator [{0}] enrolling with CA [{1}] templates [{2} and {3}]
[S005] Administrator [{0}] de-authorizing CA [{1}]
[S006] Administrator [{0}] creating new Certificate Definition [{1}]
[S007] Administrator [{0}] updating Certificate Definition [{1}]
[S008] Administrator [{0}] deleting Certificate Definition [{1}]
[S009] Administrator [{0}] creating new Role [{1}]
[S010] Administrator [{0}] updating Role [{1}]
[S011] Administrator [{0}] deleting Role [{1}]
[S012] Administrator [{0}] creating certificate [upn: {1} sid: {2} role: {3}][Certificate Definition: {4}][Security Context: {5}]
[S013] Administrator [{0}] deleting certificates [upn: {1} role: {2} Certificate Definition: {3} Security Context: {4}]
[S015] Administrator [{0}] creating certificate request [TPM: {1}]
[S016] Administrator [{0}] importing Authorization certificate [Reference: {1}]

日志代码
[S401] Performing configuration upgrade – [From version {0}][to version {1}]
[S402] ERROR: The Citrix Federated Authentication Service must be run as Network Service [currently running as: {0}]
[S404] Forcefully erasing the Citrix Federated Authentication Service database
[S405] An error occured while migrating data from the registry to the database: [{0}]
[S406] Migration of data from registry to database is complete (note: user certificates are not migrated)

日志代码
[S407] Registry-based data was not migrated to a database since a database already existed
[S408] Cannot downgrade the configuration – [From version {0}][to version {1}]
[S409] ThreadPool MinThreads adjusted from [workers: {0} completion: {1}] to: [workers: {2} completion: {3}]
[S410] Failed to adjust ThreadPool MinThreads from [workers: {0} completion: {1}] to: [workers: {2} completion: {3}]

Creating identity assertions [Federated Authentication Service]

在运行期间，当可信服务器声明用户登录时，将在 FAS 服务器上记录这些事件。

日志代码
[S101] Server [{0}] is not authorized to assert identities in role [{1}]
[S102] Server [{0}] failed to assert UPN [{1}] (Exception: {2}{3})
[S103] Server [{0}] requested UPN [{1}] SID {2}, but lookup returned SID {3}
[S104] Server [{0}] failed to assert UPN [{1}] (UPN not allowed by role [{2}])
[S105] Server [{0}] issued identity assertion [upn: {1}, role {2}, Security Context: [{3}]]
[S120] Issuing certificate to [upn: {0} role: {1} Security Context: [{2}]]
[S121] Certificate issued to [upn: {0} role: {1}] by [certifcate authority: {2}]
[S122] Warning: Server is overloaded [upn: {0} role: {1}][Requests per minute {2}].
[S123] Failed to issue a certificate for [upn: {0} role: {1}] [exception: {2}]
[S124] Failed to issue a certificate for [upn: {0} role: {1}] at [certifcate authority: {2}] [exception: {3}]

Acting as a relying party [Federated Authentication Service]

VDA 将用户登录时，这些事件将在运行时记录在 FAS 服务器上。

日志代码
[S201] Relying party [{0}] does not have access to a password.
[S202] Relying party [{0}] does not have access to a certificate.
[S203] Relying party [{0}] does not have access to the Logon CSP

日志代码
[S204] Relying party [{0}] accessing the Logon CSP for [upn: {1}] in role: [{2}] [Operation: {3}] as authorized by [{4}]
[S205] Calling account [{0}] is not a relying party in role [{1}]
[S206] Calling account [{0}] is not a relying party
[S208] Private Key operation failed [Operation: {0}][upn: {1} role: {2} certificateDefinition {3}][Error {4} {5}].

In-session certificate server [Federated Authentication Service]

当用户使用会话中证书时，会在 FAS 服务器上记录这些事件。

日志代码
[S301] Access Denied: User [{0}] does not have access to a Virtual Smart Card
[S302] User [{0}] requested unknown Virtual Smart Card [thumbprint: {1}]
[S303] Access Denied: User [{0}] does not match Virtual Smart Card [upn: {1}]
[S304] User [{0}] running program [{1}] on computer [{2}] using Virtual Smart Card [upn: {3} role: {4} thumbprint: {5}] for private key operation [{6}]
[S305] Private Key operation failed [Operation: {0}][upn: {1} role: {2} containerName {3}][Error {4} {5}].

FAS assertion plugin [Federated Authentication Service]

日志代码
[S500] No FAS assertion plugin is configured
[S501] The configured FAS assertion plugin could not be loaded [exception:{0}]
[S502] FAS assertion plugin loaded [pluginId={0}] [assembly={1}] [location={2}]
[S503] Server [{0}] failed to assert UPN [{1}] (logon evidence was supplied but the plugin [{2}] does not support it)
[S504] Server [{0}] failed to assert UPN [{1}] (logon evidence was supplied but there is no configured FAS plugin)

日志代码
[S505] Server [{0}] failed to assert UPN [{1}] (the plugin [{2}] rejected the logon evidence with status [{3}] and message [{4}])
[S506] The plugin [{0}] accepted logon evidence from server [{1}] for UPN [{2}] with message [{3}]
[S507] Server [{0}] failed to assert UPN [{1}] (the plugin [{2}] threw exception [{3}])
[S507] Server [{0}] failed to assert UPN [{1}] (the plugin [{2}] threw exception [{3}])
[S508] Server [{0}] failed to assert UPN [{1}] (access disposition was supplied but the plugin [{2}] does not support it)
[S509] Server [{0}] failed to assert UPN [{1}] (access disposition was supplied but there is no configured FAS plugin)
[S510] Server [{0}] failed to assert UPN [{1}] (the access disposition was deemed invalid by plugin [{2}]

Log on [VDA]

[事件来源：Citrix.Authentication.IdentityAssertion]

在登录阶段会在 VDA 上记录这些事件。

日志代码
[S101] Identity Assertion Logon failed. Unrecognised Federated Authentication Service [id: {0}]
[S102] Identity Assertion Logon failed. Could not lookup SID for {0} [Exception: {1}{2}]
[S103] Identity Assertion Logon failed. User {0} has SID {1}, expected SID {2}
[S104] Identity Assertion Logon failed. Failed to connect to Federated Authentication Service: {0} [Error: {1} {2}]
[S105] Identity Assertion Logon. Logging in [Username: {0}][Domain: {1}]
[S106] Identity Assertion Logon. Logging in [Certificate: {0}]
[S107] Identity Assertion Logon failed. [Exception: {0}{1}]
[S108] Identity Assertion Subsystem. ACCESS_DENIED [Caller: {0}]

In-session certificates [VDA]

当用户尝试使用会话中证书时，会在 VDA 上记录这些事件。

日志代码
[S201] Virtual smart card access authorized by [{0}] for [PID: {1} Program Name: {2}][Certificate thumbprint: {3}]
[S203] Virtual Smart Card Subsystem. Access Denied [caller: {0}, session {1}]
[S204] Virtual Smart Card Subsystem. Smart card support disabled

Certificate request and generation codes [Federated Authentication Service]

[事件来源：Citrix.Fas.PkiCore]

当 FAS 服务器执行日志级别的加密操作时，会记录这些低级别事件。

日志代码
[S001] TrustArea::TrustArea: Installed certificate [TrustArea: {0}] [Certificate {1}][TrustAreaJoinParameters{2}
[S014] Pkcs10Request::Create: Created PKCS10 request [Distinguished Name {0}]
[S016] PrivateKey::Create [Identifier {0}][MachineWide: {1}][Provider: {2}][ProviderType: {3}][EllipticCurve: {4}][KeyLength: {5}][isExportable: {6}]
[S017] PrivateKey::Delete [CspName: {0}, Identifier {1}]

日志代码
[S104] MicrosoftCertificateAuthority::GetCredentials: Authorized to use {0}
[S105] MicrosoftCertificateAuthority::SubmitCertificateRequest Error submit response [{0}]
[S106] MicrosoftCertificateAuthority::SubmitCertificateRequest Issued certificate [{0}]
[S112] MicrosoftCertificateAuthority::SubmitCertificateRequest - Waiting for approval [CR_DISP_UNDER_SUBMISSION] [Reference: {0}]

相关信息

- 部署体系结构总结了常见的 FAS 部署。
- 高级配置中介绍了“操作方法”文章。

部署体系结构

November 7, 2019

简介

联合身份验证服务 (FAS) 是一个 Citrix 组件，与 Active Directory 证书颁发机构相集成，允许用户在 Citrix 环境中无缝执行身份验证。本文档介绍了可能适合于您的部署的各种身份验证体系结构。

启用后，FAS 将用户身份验证决策任务委派给可信 StoreFront 服务器。StoreFront 内置一组全面的身份验证选项，这些选项根据新型 Web 技术构建，可以很方便地通过 StoreFront SDK 或第三方 IIS 插件进行扩展。基本设计目标是，任何可在 Web 站点中对用户进行身份验证的身份验证技术现在都可以用于登录 Citrix Virtual Apps 或 Citrix Virtual Desktops 部署。

本文档介绍了顶级部署体系结构示例（按复杂性升序排列）。

- 内部部署
- Citrix Gateway 部署
- ADFS SAML
- B2B 帐户映射
- Windows 10 Azure AD 联接

提供了指向相关 FAS 文章的链接。对于所有体系结构，都可以将安装和配置一文用作设置 FAS 时所参考的主要信息源。

工作原理

FAS 已获授权，能够代表经 StoreFront 身份验证的 Active Directory 用户自动颁发智能卡类证书。这将对工具使用类似的 API，以便管理员能够预配物理智能卡。

当用户中转到 Citrix Virtual Apps 或 Citrix Virtual Desktops Virtual Delivery Agent (VDA) 时，证书将附加到计算机，并且 Windows 域会将登录视为标准智能卡身份验证。

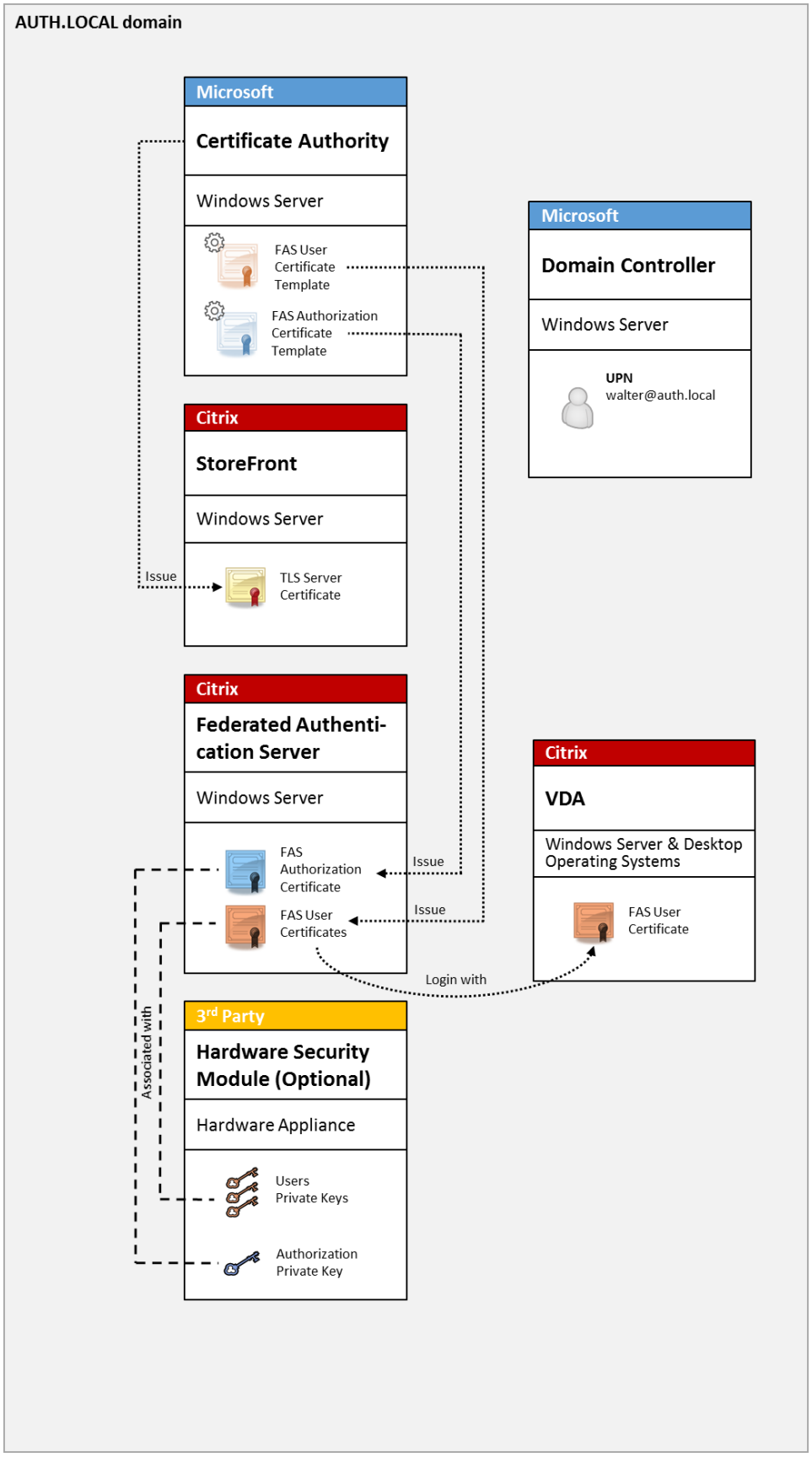
内部部署

FAS 允许用户使用多种身份验证选项（包括 Kerberos 单点登录）安全地向 StoreFront 进行身份验证，并连接到已经过完全身份验证的 Citrix HDX 会话。

这允许在不提示输入用户凭据或智能卡 PIN 码且不使用“已保存密码管理”功能（例如 Single Sign-On Service）的情况下执行 Windows 身份验证。这可用于取代 Citrix Virtual Apps 早期版本中提供的“Kerberos 约束委派”登录功能。

所有用户都有权在自己的会话中访问公钥基础结构 (PKI) 证书，而无论其是否使用智能卡登录到端点设备。这样就能够平滑迁移到双重身份验证模型，即使是从智能手机和平板电脑等不具备智能卡读卡器的设备迁移也是如此。

此部署中增加了一个用于运行 FAS 的新服务器，该服务器已获得代表用户颁发智能卡类证书的授权。这些证书之后在 Citrix HDX 环境中用于登录用户会话，就如同已使用智能卡登录一样。



必须以类似于智能卡登录的方式配置 Citrix Virtual Apps 或 Citrix Virtual Desktops 环境，CTX206156 对此进行了说明。

在现有部署中，此过程通常只需确保已加入域的 Microsoft 证书颁发机构可用，并且已为域控制器分配域控制器证书。（请参阅 CTX206156 中的 “颁发域控制器证书” 部分。）

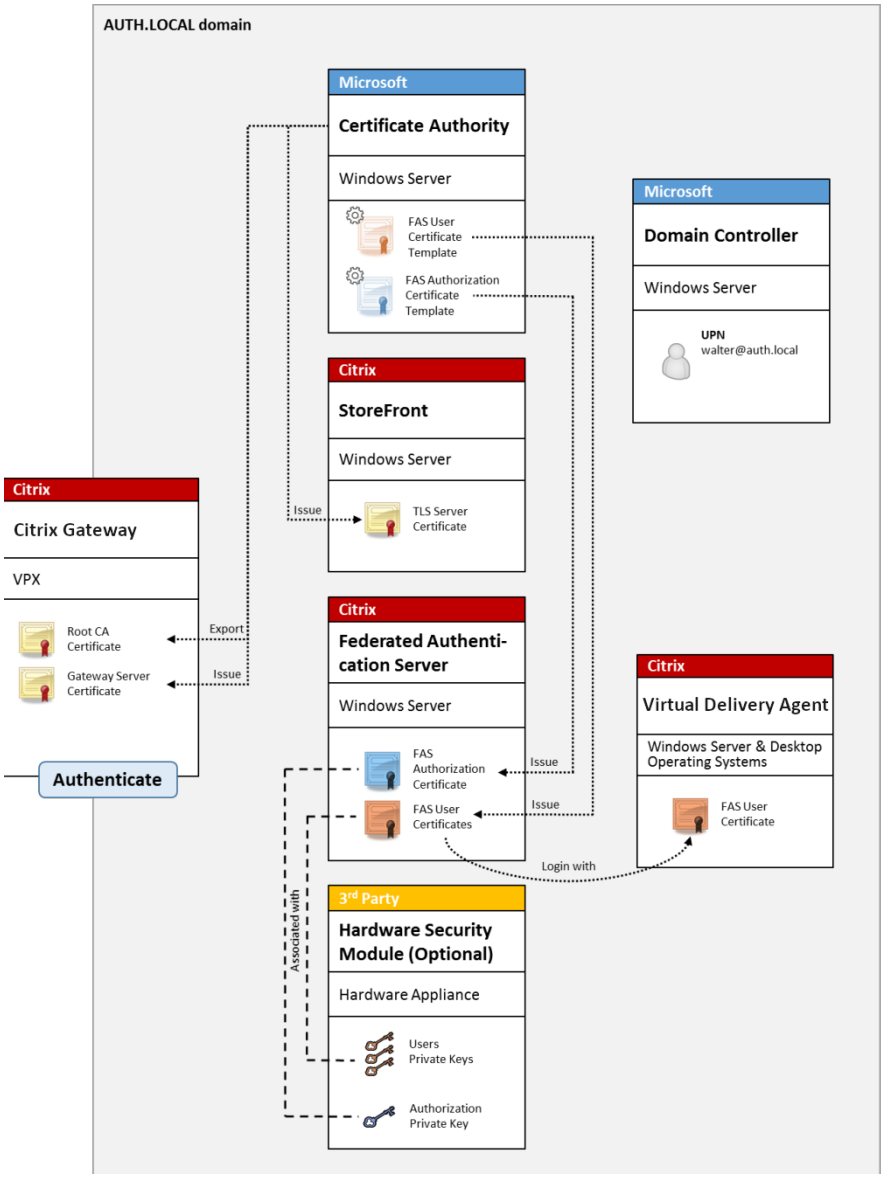
相关信息：

- 密钥可存储在硬件安全模块 (HSM) 或内置的受信任的平台模块 (TPM) 中。有关详细信息，请参阅私钥保护一文。
- 安装和配置一文介绍了如何安装和配置 FAS。

Citrix Gateway 部署

Citrix Gateway 部署与内部部署类似，但增加了与 StoreFront 配对的 Citrix Gateway，从而将主身份验证点移动到 Citrix Gateway 本身。Citrix Gateway 包括多个复杂的身份验证和授权选项，这些选项可用于确保安全地远程访问公司的 Web 站点。

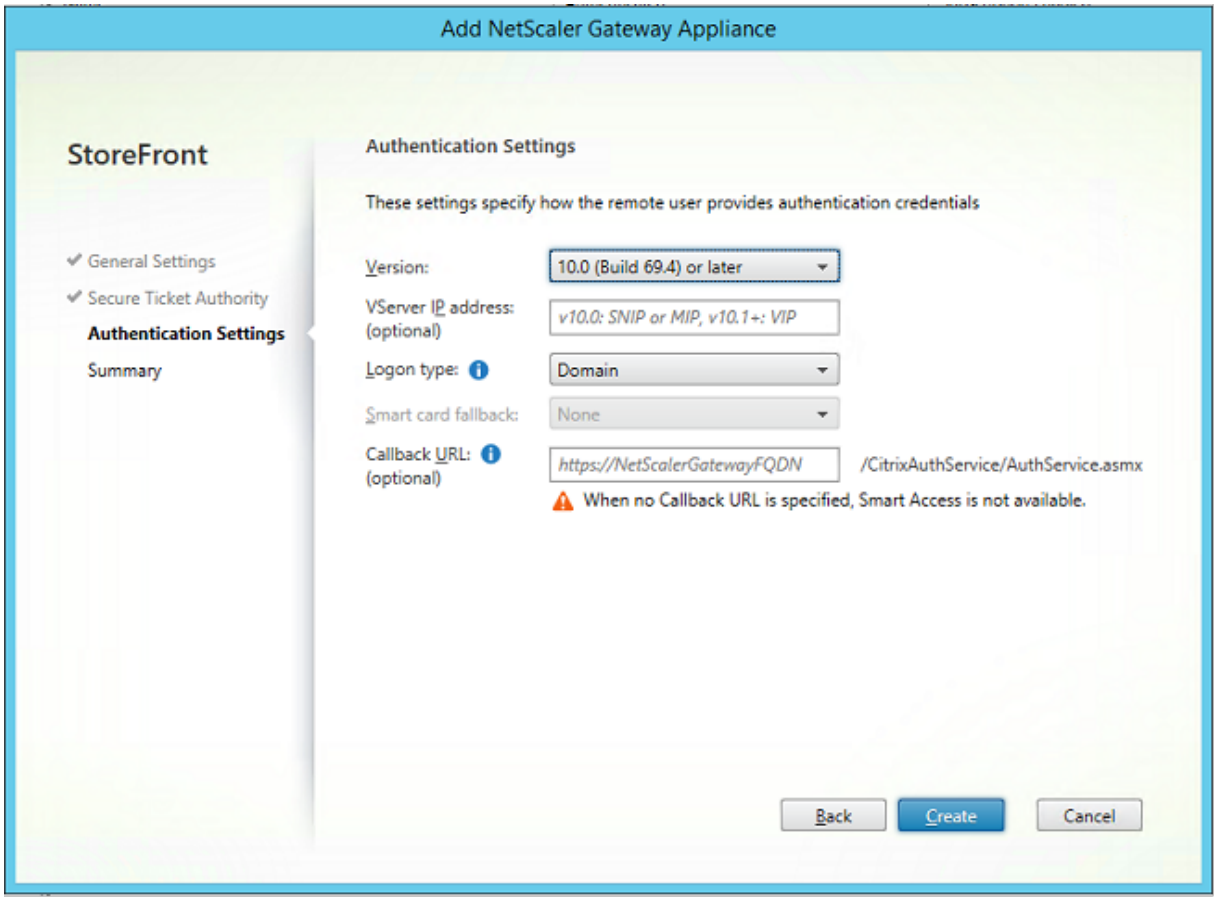
此部署可用于避免在首次对 Citrix Gateway 进行身份验证后登录用户会话时多次提示输入 PIN 码。此外，还允许使用高级 Citrix Gateway 身份验证技术，不再需要 AD 密码或智能卡。



必须以类似于智能卡登录的方式配置 Citrix Virtual Apps 或 Citrix Virtual Desktops 环境，CTX206156 对此进行了说明。

在现有部署中，此过程通常只需确保已加入域的 Microsoft 证书颁发机构可用，并且已为域控制器分配域控制器证书。（请参阅 CTX206156 中的“颁发域控制器证书”部分）。

将 Citrix Gateway 配置为主身份验证系统时，请确保 Citrix Gateway 与 StoreFront 之间的所有连接都通过 TLS 确保安全。具体而言，请务必将回调 URL 正确配置为指向 Citrix Gateway 服务器，因为这可用于对此部署中的 Citrix Gateway 服务器进行身份验证。

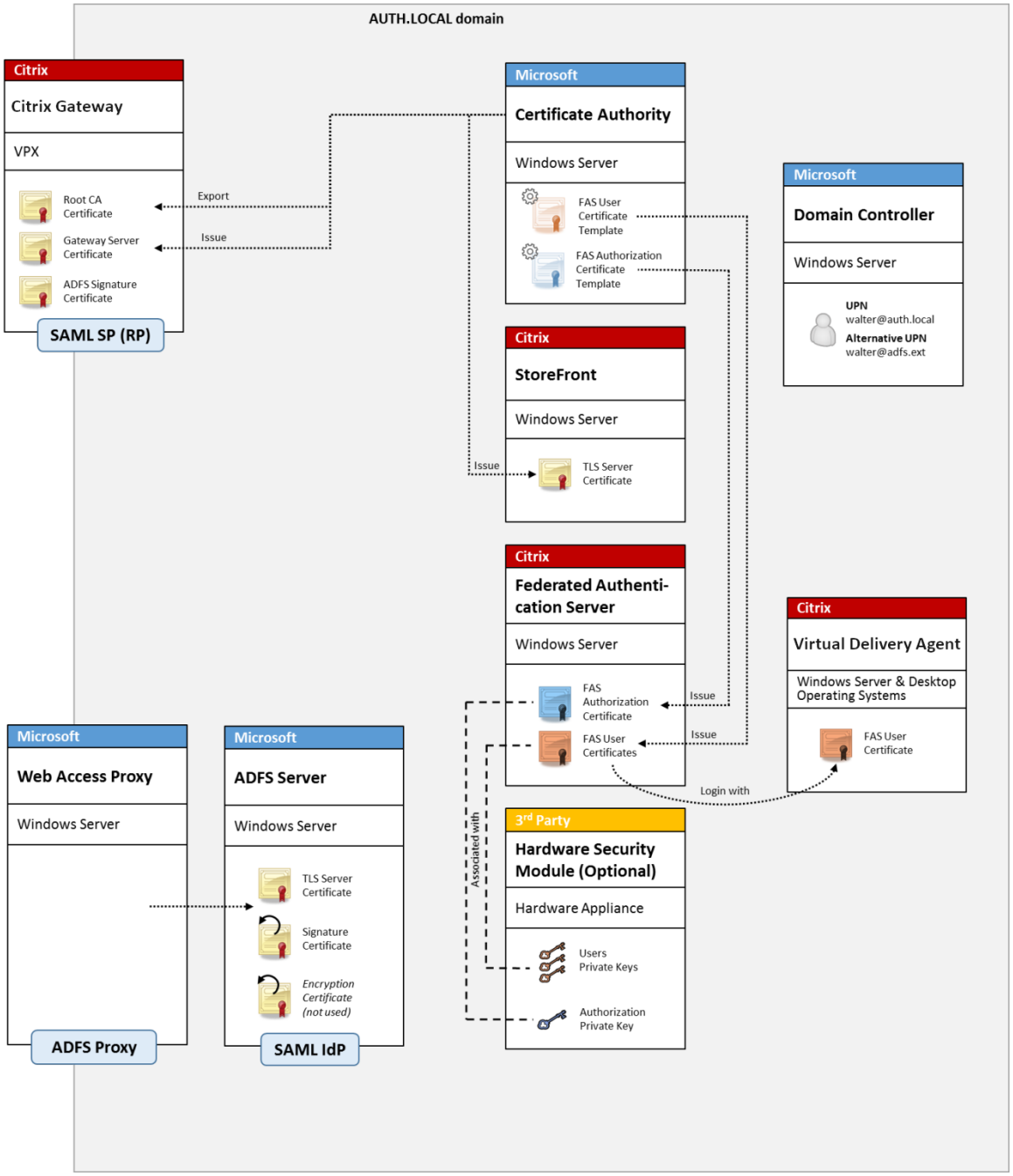


相关信息：

- 要配置 Citrix Gateway，请参阅 如何配置 NetScaler Gateway 10.5 以与 StoreFront 3.6 和 Citrix Virtual Desktops 7.6 配合使用。
- 安装和配置介绍了如何安装和配置 FAS。

ADFS SAML 部署

关键 Citrix Gateway 身份验证技术允许与 Microsoft ADFS 相集成，这样可用作 SAML 身份提供程序 (IdP)。SAML 断言是一个通过密码签名的 XML 块，由授权用户登录计算机系统的可信 IdP 颁发。这表示 FAS 服务器允许将用户的身份验证委派给 Microsoft ADFS 服务器（或其他能够识别 SAML 的 IdP）。



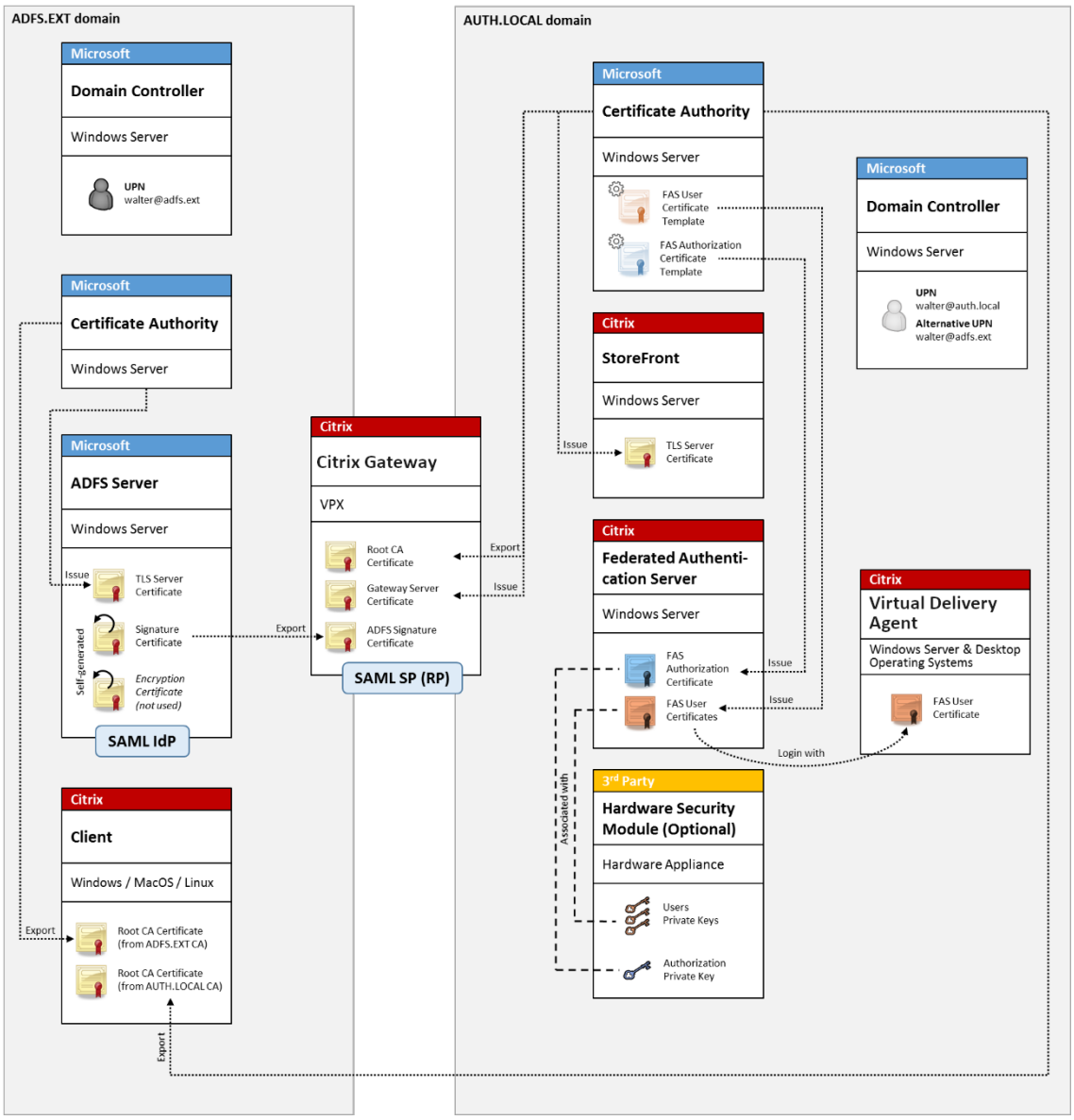
ADFS 通常用于安全地验证用户的身份以通过 Internet 远程访问公司资源；例如，通常用于 Office 365 集成。

相关信息：

- ADFS 部署一文介绍了详细信息。
- 安装和配置一文介绍了如何安装和配置 FAS。
- 本文中的 Citrix Gateway 部署部分介绍了配置注意事项。

B2B 帐户映射

如果有两家公司希望使用对方的计算机系统，常见方案为设置一个具有信任关系的 Active Directory 联合身份验证服务 (ADFS) 服务器。这样将允许一家公司的用户无缝进行身份验证以登录另一家公司的 Active Directory (AD) 环境。登录时，每个用户都将使用自己的公司登录凭据；ADFS 会自动将其映射到同行公司的 AD 环境中的“影子帐户”。

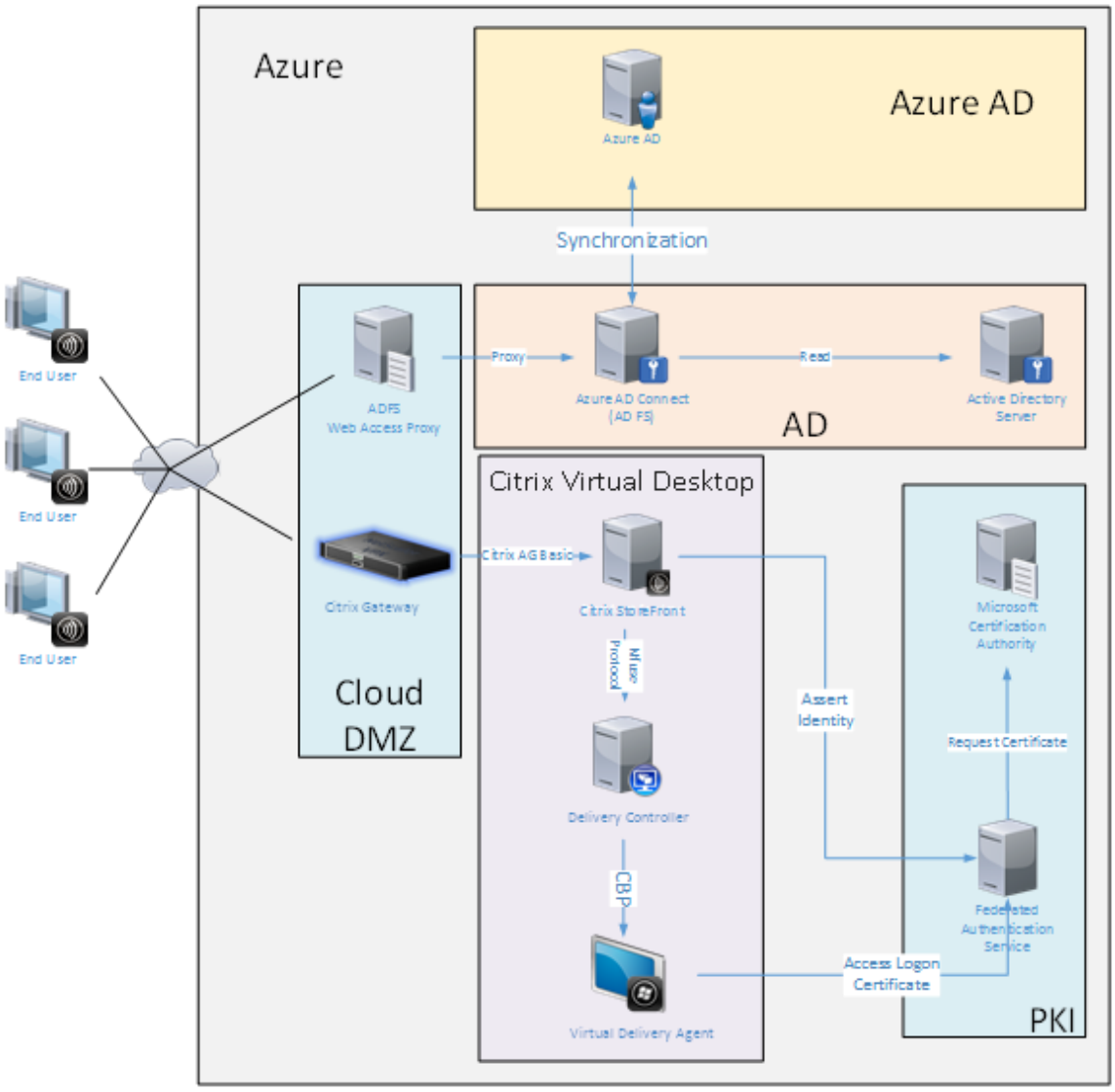


相关信息：

- 安装和配置一文介绍了如何安装和配置 FAS。

Windows 10 Azure AD 联接

Windows 10 中引入了“Azure AD 联接”的概念，其概念与传统的 Windows 域加入类似，但主要针对“通过 Internet”的场景。此功能特别适用于便携式计算机和平板电脑。与传统的 Windows 域加入相同，Azure AD 具有允许对公司 Web 站点和资源使用单点登录模块的功能。这些都能“识别 Internet”，因此，将从任何连接了 Internet 的位置进行工作，而非仅从办公室局域网进行工作。



此部署是实际上没有“办公室中的最终用户”概念的示例。便携式计算机完全通过 Internet 使用最新的 Azure AD 功能进行注册和身份验证。

请注意，此部署中的基础结构能够在提供了 IP 地址的任意位置运行：本地、托管提供程序、Azure 或其他云提供程序。Azure AD Connect 同步器将自动连接到 Azure AD。为便于说明，示例图形使用 Azure VM。

相关信息：

- 安装和配置一文介绍了如何安装和配置 FAS。

- Azure AD 集成一文介绍了详细信息。

ADFS 部署

November 7, 2019

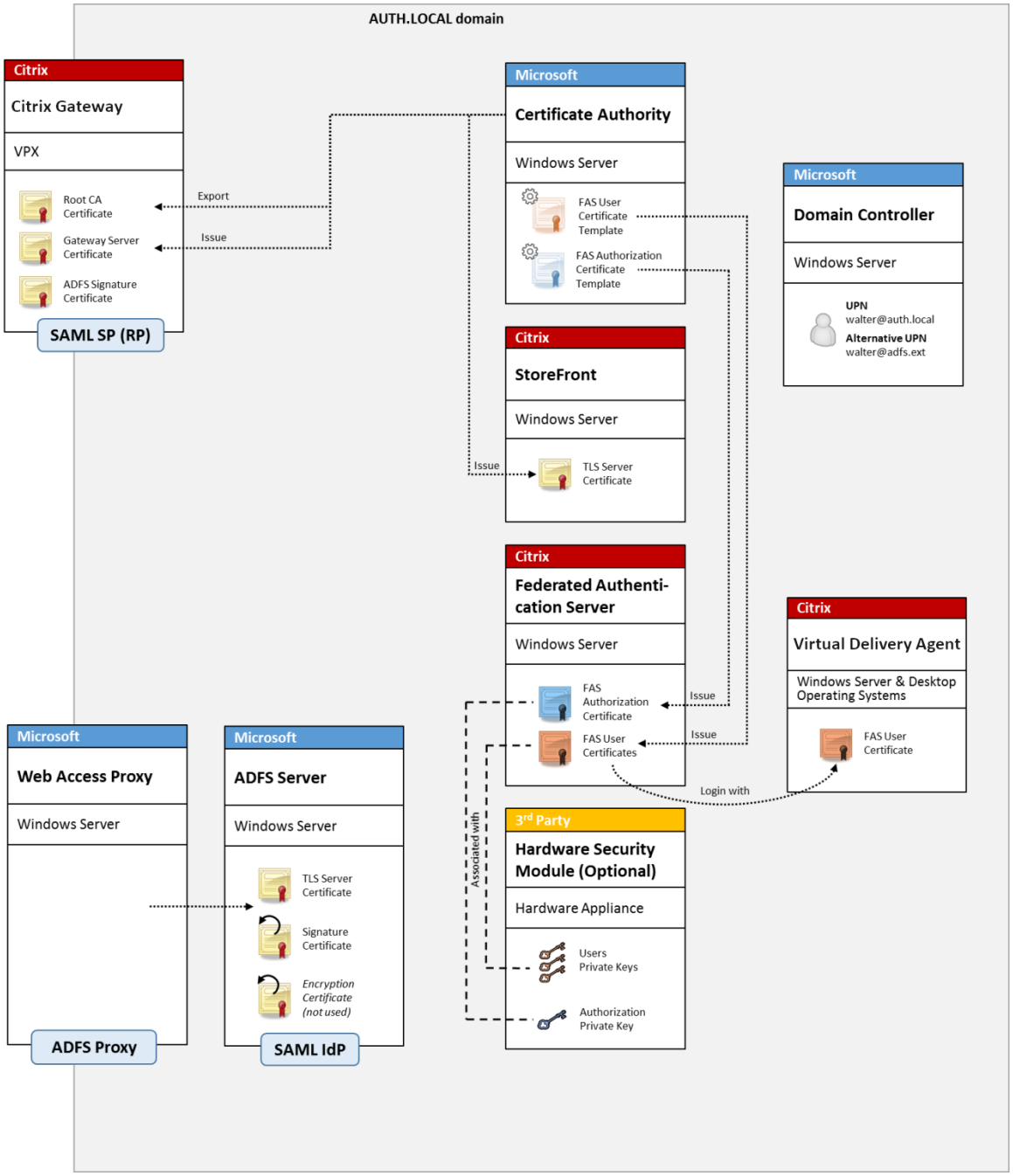
简介

本文介绍了如何将 Citrix 环境与 Microsoft ADFS 相集成。

许多组织都使用 ADFS 管理用户对需要进行单点身份验证的 Web 站点的安全访问。例如，公司可能会向员工提供额外的内容和下载对象；需要使用标准 Windows 登录凭据保护这些位置。

联合身份验证服务 (FAS) 还允许 Citrix Gateway 和 Citrix StoreFront 与 ADFS 登录系统相集成，缓解了可能会对公司员工造成的困扰。

此部署集成 Citrix Gateway 作为 Microsoft ADFS 的信赖方。



SAML 概述

安全声明标记语言 (SAML) 是一个简单的“重定向到登录页面”的 Web 浏览器登录系统。配置包括以下各项：

重定向 **URL [Single Sign-On Service URL]**

Citrix Gateway 发现用户需要进行身份验证时，会指示用户的 Web 浏览器在 ADFS 服务器上对 SAML 登录 Web 页面执行 HTTP POST。这通常是 `https://` 地址，格式为：`https://adfs.mycompany.com/adfs/ls`。

此 Web 页面 POST 包含其他信息，包括 ADFS 在登录完成时在其中返回用户的“返回地址”。

标识符 **[**颁发者名称**/**实体 **ID]**

实体 ID 是指 Citrix Gateway 在向 ADFS 发送的 POST 数据中包含的唯一标识符。这将通知 ADFS 用户正在尝试登录的服务，并通知 ADFS 根据需要应用不同的身份验证策略。如果已颁发，SAML 身份验证 XML 将仅适用于登录通过实体 ID 标识的服务。

一般情况下，实体 ID 是指 Citrix Gateway 服务器登录页面的 URL，但通常可以指任何内容，前提是 Citrix Gateway 与 ADFS 达成共识：`https://ns.mycompany.com/application/logonpage`。

返回地址 **[**答复 **URL]**

如果身份验证成功，ADFS 将指示用户的 Web 浏览器将 SAML 身份验证 XML POST 回为实体 ID 配置的答复 URL 之一。这通常是原始 Citrix Gateway 服务器上的 `https://` 地址，格式为 `https://ns.mycompany.com/cgi/samlauth`。

如果配置了多个答复 URL 地址，Citrix Gateway 可以在向 ADFS 发送的原始 POST 中选择一个 URL。

签名证书 **[IDP** 证书**]**

ADFS 使用私钥通过密码对 SAML 身份验证 XML blob 进行签名。要验证此签名，必须将 Citrix Gateway 配置为使用证书文件中包含的公钥检查这些签名。证书文件通常是从 ADFS 服务器获取的一个文本文件。

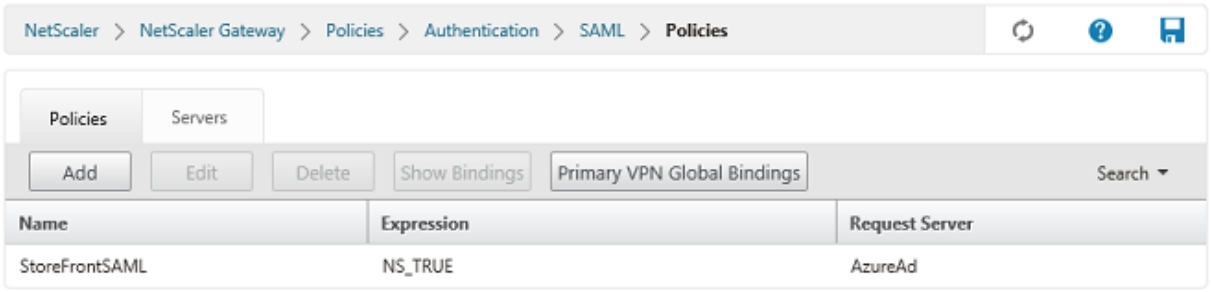
单点注销 **URL [**单点注销 **URL]**

ADFS 和 Citrix Gateway 支持“中央注销”系统。Citrix Gateway 会偶尔轮询此 URL 以检查 SAML 身份验证 XML blob 是否仍表示当前登录的会话。

这是一项可选功能，不需要配置。这通常是 `https://` 地址，格式为：`https://adfs.mycompany.com/adfs/logout`。（请注意，此地址可以与单点登录 URL 相同。）

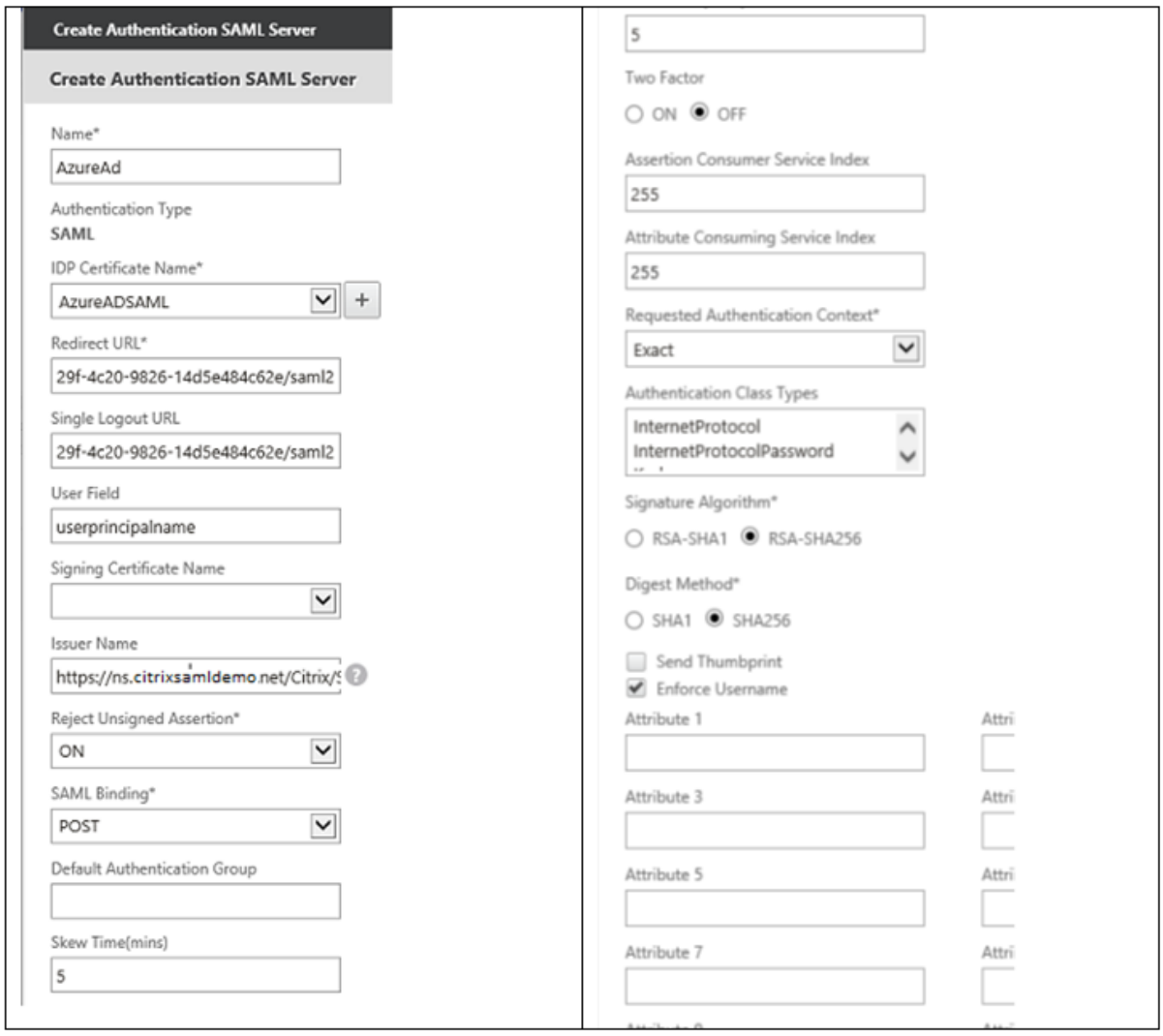
配置

Citrix Gateway 部署部分介绍了如何设置 Citrix Gateway 以处理标准 LDAP 身份验证选项。成功完成设置后，可以在 Citrix Gateway 上创建一条允许进行 SAML 身份验证的新身份验证策略。此策略以后可以替换 Citrix Gateway 向导使用的默认 LDAP 策略。



填充 **SAML** 策略

可以使用之前从 ADFS 管理控制台获取的信息配置新 SAML IdP 服务器。应用此策略时，Citrix Gateway 会将用户重定向到 ADFS 进行登录，并反过来接受 ADFS 签名的 SAML 身份验证令牌。



相关信息

- 安装和配置是 FAS 安装和配置的主要参考资料。
- 部署体系结构一文总结了常见的 FAS 部署。
- 高级配置一文中介绍了“操作方法”文章。

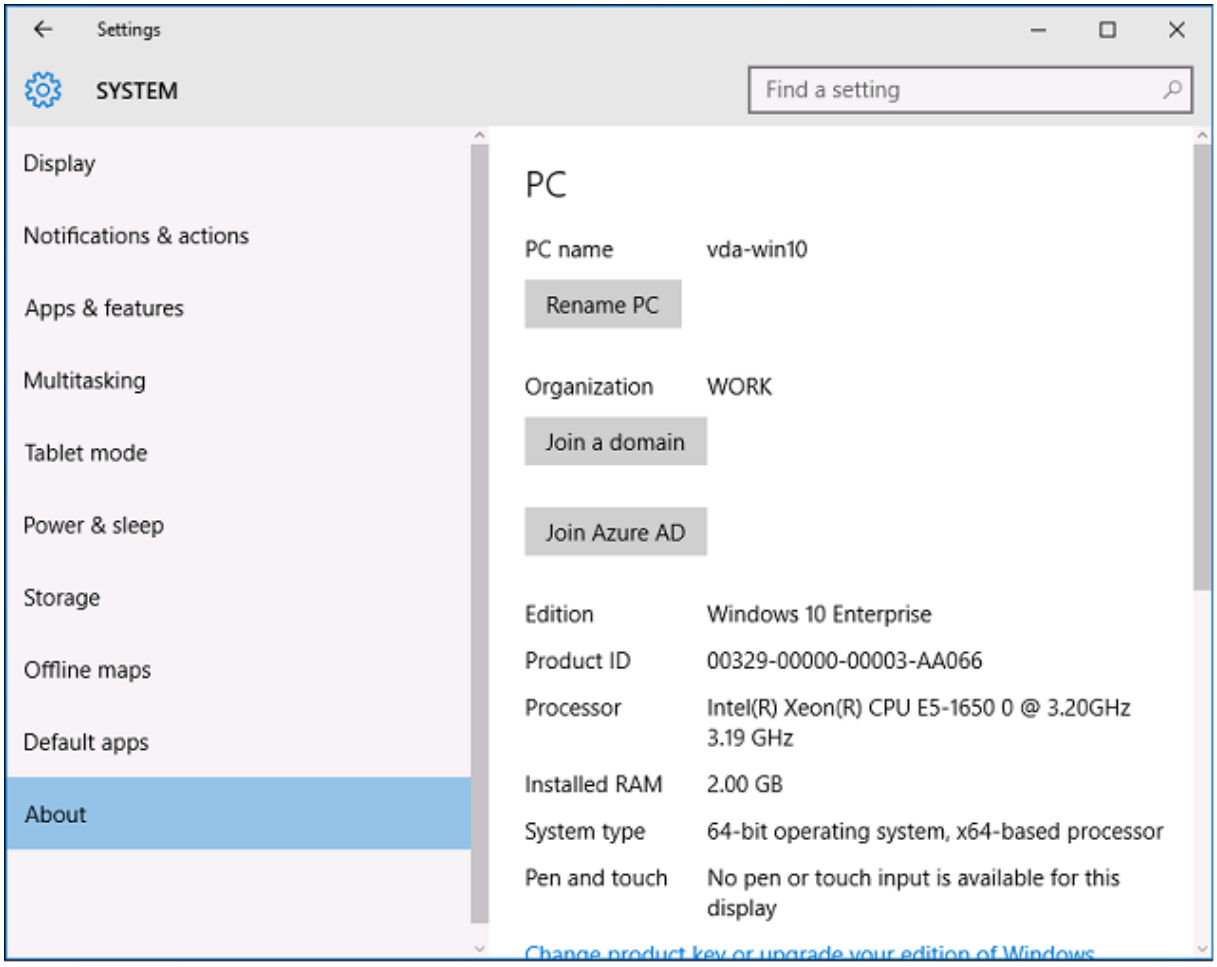
Azure AD 集成

November 7, 2019

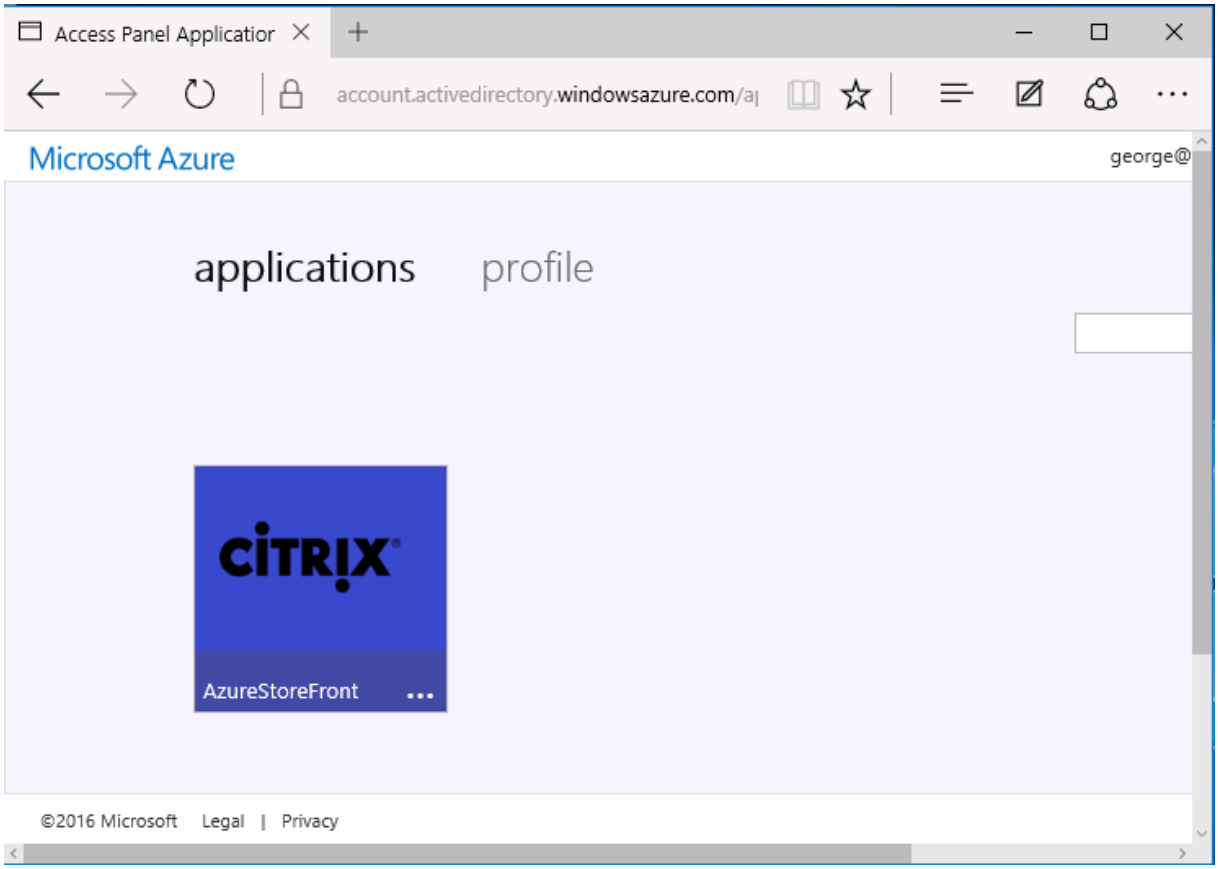
简介

本文档介绍如何将 Citrix 环境与 Windows 10 Azure AD 功能相集成。Windows 10 中引入了 Azure AD，这是一个新的域加入模块，可以在此模块中通过 Internet 将漫游便携式计算机加入企业域，以便进行管理和单点登录。

本文档中的示例部署描述了一个具有以下特点的系统：IT 人员向新用户提供其私人 Windows 10 便携式计算机的企业电子邮件地址和注册代码。用户通过设置面板中的系统 **>** 关于 **>** 加入 **Azure AD** 选项访问此代码。



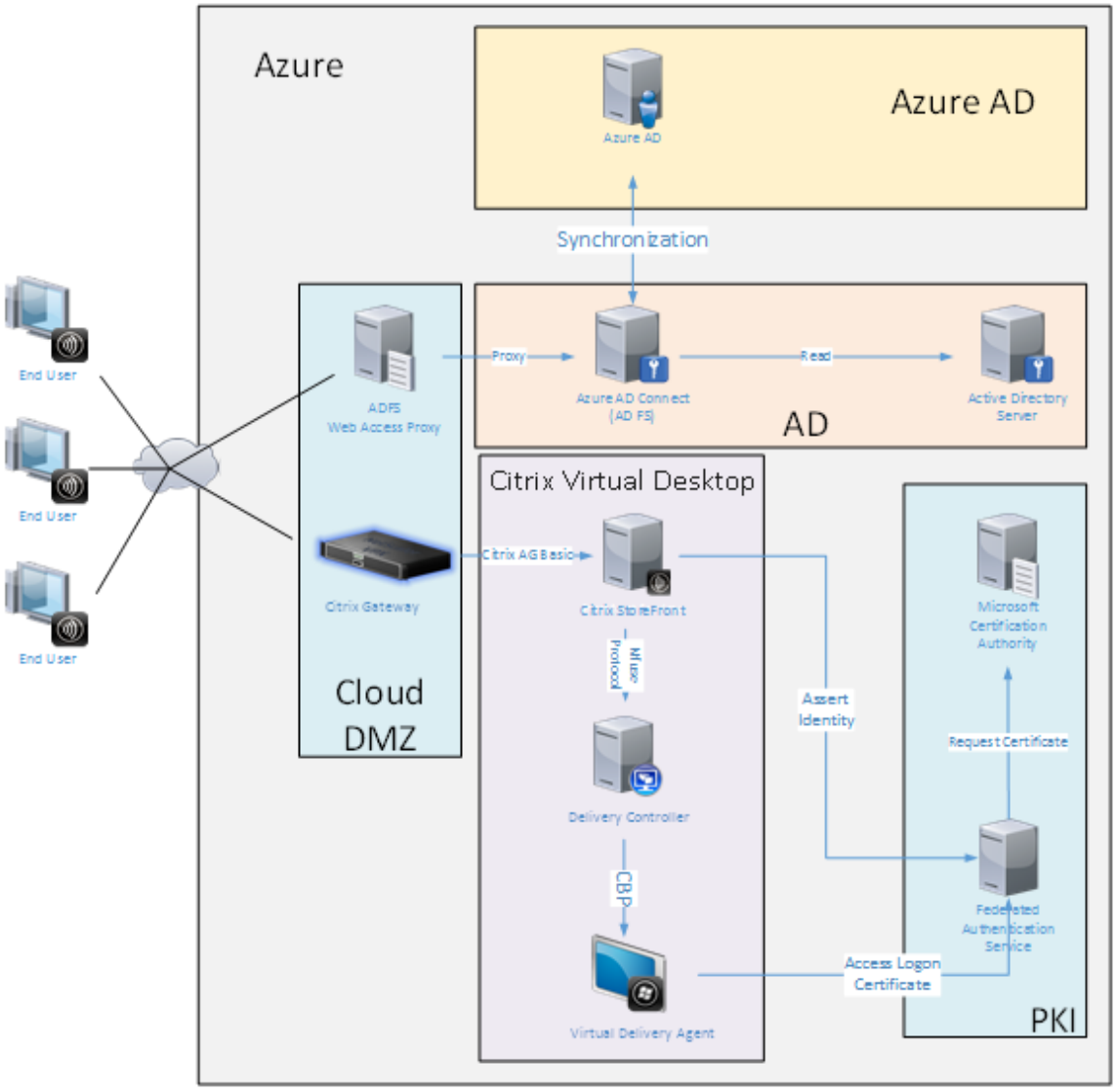
注册便携式计算机后，Microsoft Edge Web 浏览器将通过 Azure SaaS 应用程序 Web 页面自动登录到公司的 Web 站点和 Citrix 的已发布应用程序，以及其他 Azure 应用程序（例如 Office 365）。



体系结构

此体系结构完全复制 Azure 中的传统公司网络，从而与最新的云技术（例如 Azure AD 和 Office 365）相集成。最终用户都被视为远程工作人员，没有位于办公室 Intranet 上的概念。

可以将该模型应用到使用现有本地系统的公司，因为 Azure AD Connect 同步服务可以通过 Internet 桥接到 Azure。



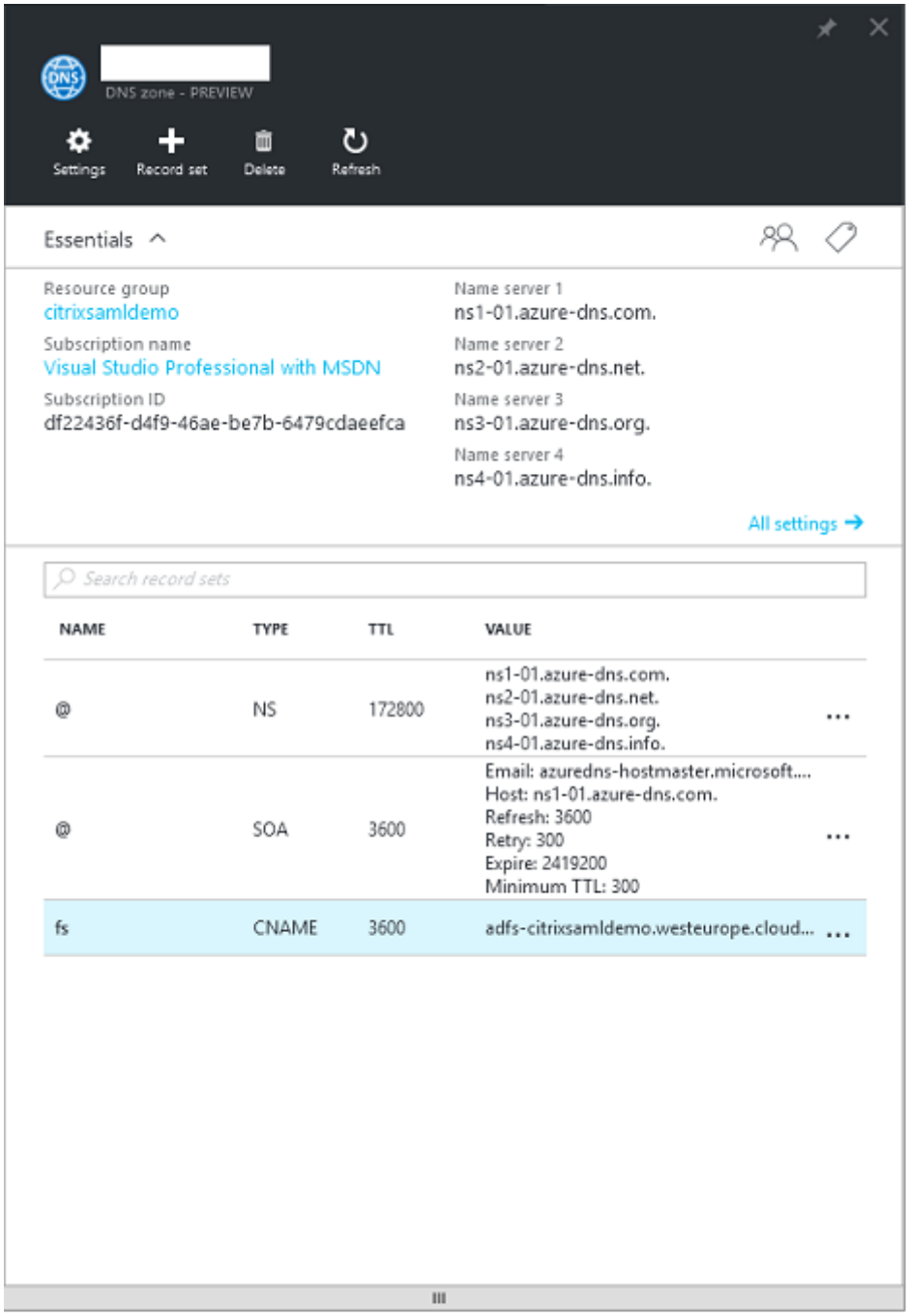
安全连接和单点登录（传统上已通过有防火墙的局域网和 Kerberos/NTLM 身份验证）在此体系结构中将替换为与 Azure 和 SAML 之间的 TLS 连接。新服务内置为加入到 Azure AD 的 Azure 应用程序。可以使用 Azure 云服务的 IAAS 部分中的标准 Active Directory 服务器 VM 运行需要 Active Directory 的现有应用程序（例如 SQL Server 数据库）。

用户启动传统应用程序时，将使用 Citrix Virtual Apps and Desktops 发布的应用程序进行访问。不同类型的应用程序使用 Microsoft Edge 的单点登录功能通过用户的 **Azure** 应用程序页面进行整理。Microsoft 还提供能够枚举和启动 Azure 应用程序的 Android 和 iOS 应用程序。

创建 **DNS** 区域

Azure AD 要求管理员已注册公用 DNS 地址，并控制域名后缀的委派区域。为此，管理员可以使用 Azure DNS 的区域功能。

此示例使用 DNS 区域名称 *citrixsamldemo.net*。



控制台显示 Azure DNS 名称服务器的名称。这些名称应在区域对应的 DNS 注册器的 NS 条目中引用（例如 `citrixsamldemo.net. NS n1-01.azure-dns.com`）

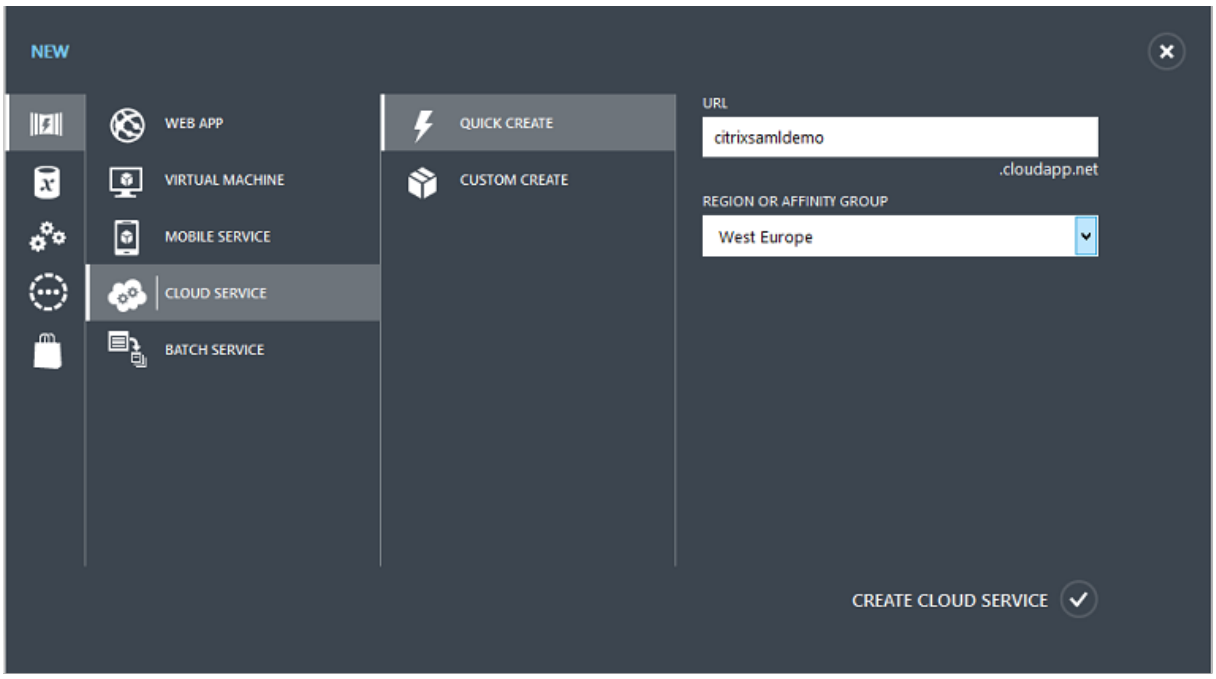
添加对 Azure 中运行的 VM 的引用时，最简单的方法是对 VM 使用指向 Azure 托管的 DNS 记录的 CNAME 指针。如果 VM 的 IP 地址发生变化，不需要手动更新 DNS 区域文件。

此部署的内部和外部 DNS 地址前缀都保持一致。域为 citrixsamldemo.net，使用拆分 DNS（在内部为 10.0.0.*）。

添加一个引用 Web 应用程序代理服务器的 “fs.citrixsamldemo.net” 条目。这是此区域的联合身份验证服务。

创建云服务

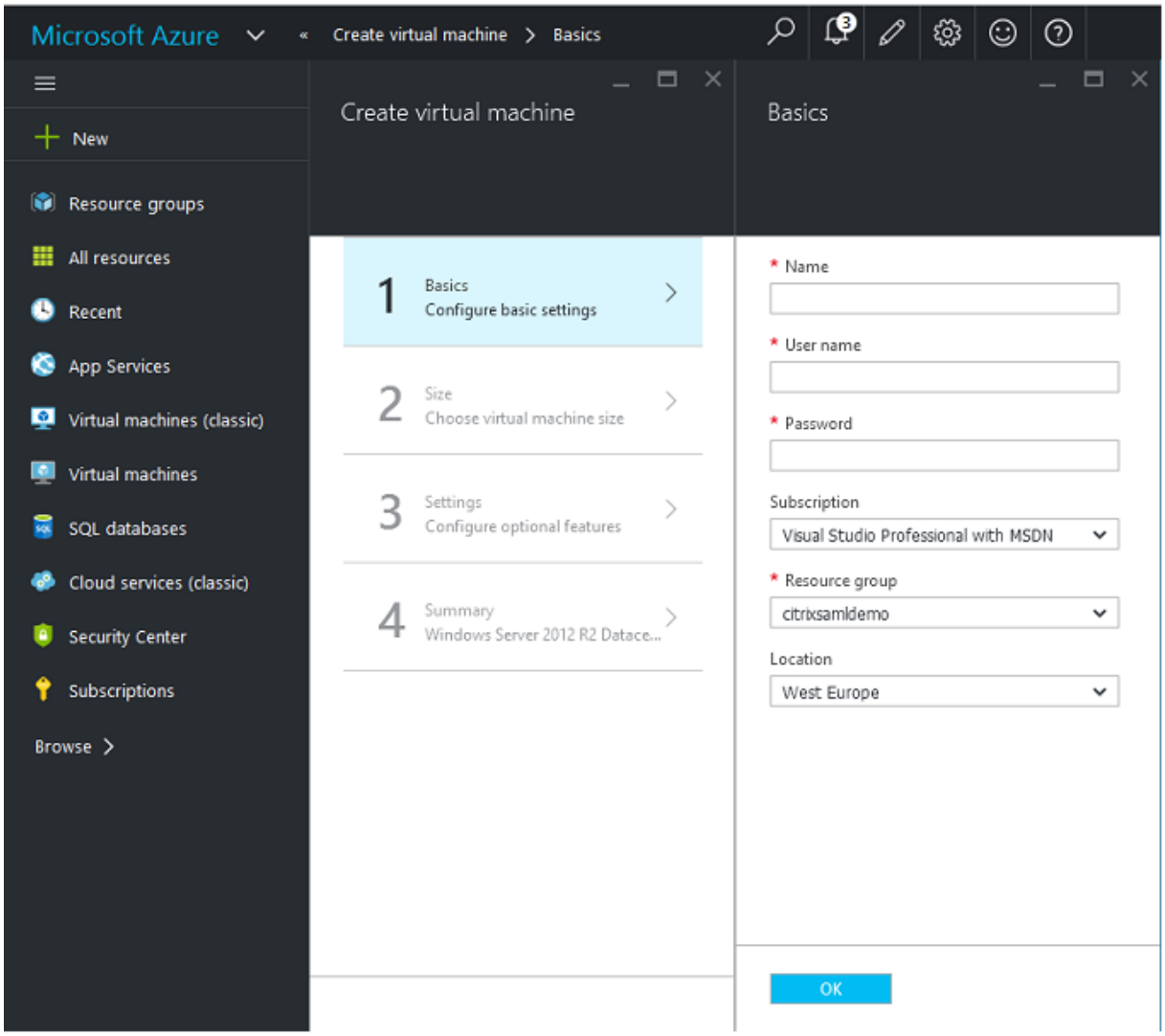
下例配置了一个 Citrix 环境，其中包括一个 ADFS 服务器在 Azure 中运行的 AD 环境。创建了一个云服务，名为“citrixsamldemo”。



创建 **Windows** 虚拟机

创建五个在云服务中运行的 Windows VM：

- 域控制器 (domaincontrol)
- Azure Connect ADFS 服务器 (adfs)
- ADFS Web 访问代理（Web 应用程序代理，未加入域）
- Citrix Virtual Apps and Desktops Delivery Controller
- Citrix Virtual Apps and Desktops Virtual Delivery Agent (VDA)



域控制器

- 添加 **DNS** 服务器和 **Active Directory** 域服务角色以创建一个标准 Active Directory 部署（在此示例中为 citrixsamldemo.net）。域提升完成后，请添加 **Active Directory** 证书服务角色。
- 创建一个普通用户帐户用于测试（例如，George@citrixsamldemo.net）。
- 由于此服务器将运行内部 DNS，因此，所有服务器都应引用此服务器以便进行 DNS 解析。此操作可通过 **Azure DNS** 设置页面完成。（有关详细信息，请参阅本文档中的“附录”。）

ADFS 控制器和 **Web** 应用程序代理服务器

- 将 ADFS 服务器加入到 citrixsamldemo domain 中。Web 应用程序代理服务器应始终保留在独立的工作组中，因此，请在 AD DNS 中手动注册 DNS 地址。

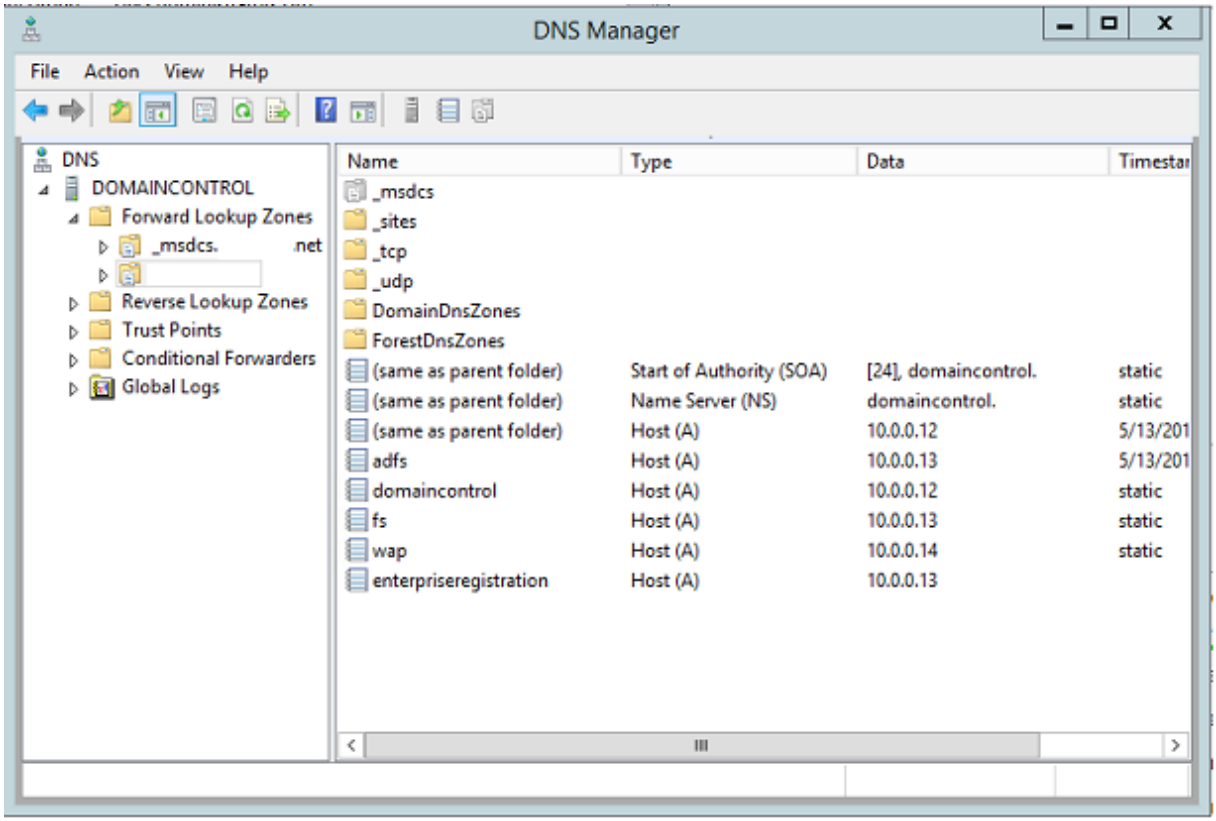
- 在这些服务器上运行 **Enable-PSRemoting –Force** cmdlet，以允许 PS 通过防火墙从 AzureAD Connect 工具远程连接。

Citrix Virtual Desktops Delivery Controller 和 VDA

- 请在加入到 citrixsamldemo 的其余两个 Windows Server 上安装 Citrix Virtual Apps 或 Citrix Virtual Desktops Delivery Controller 和 VDA。

配置内部 DNS

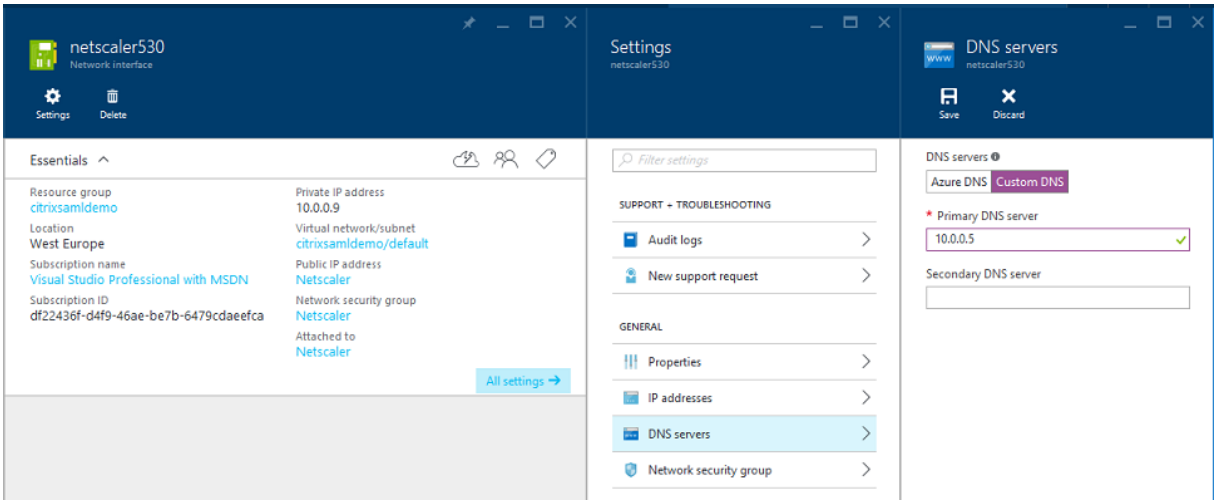
安装域控制器后，请将 DNS 服务器配置为处理 citrixsamldemo.net 的内部查看，并用作指向外部 DNS 服务器（例如 8.8.8.8）的转发器。



添加以下各项的静态记录：

- wap.citrixsamldemo.net [Web 应用程序代理 VM 将不加入域]
- fs.citrixsamldemo.net [内部联合身份验证服务器地址]
- enterpriseregistration.citrixsaml.net [与 fs.citrixsamldemo.net 相同]

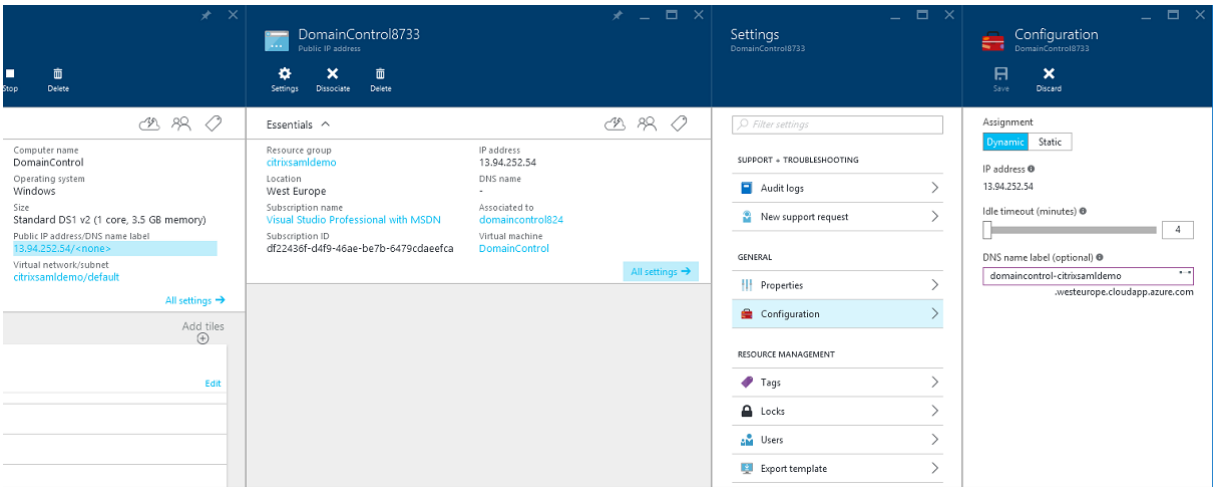
应将 Azure 中运行的所有 VM 配置为仅使用此 DNS 服务器。可以通过网络接口 GUI 执行此操作。



默认情况下，内部 IP (10.0.0.9) 地址动态分配。可以使用 IP 地址设置永久分配 IP 地址。应对 Web 应用程序代理服务器和域控制器执行此操作。

配置外部 **DNS** 地址

VM 运行过程中，Azure 保留自己的指向当前已分配给 VM 的公用 IP 地址的 DNS 区域服务器。这是一项可启用的有用功能，因为 Azure 默认在每个 VM 启动时分配 IP 地址。

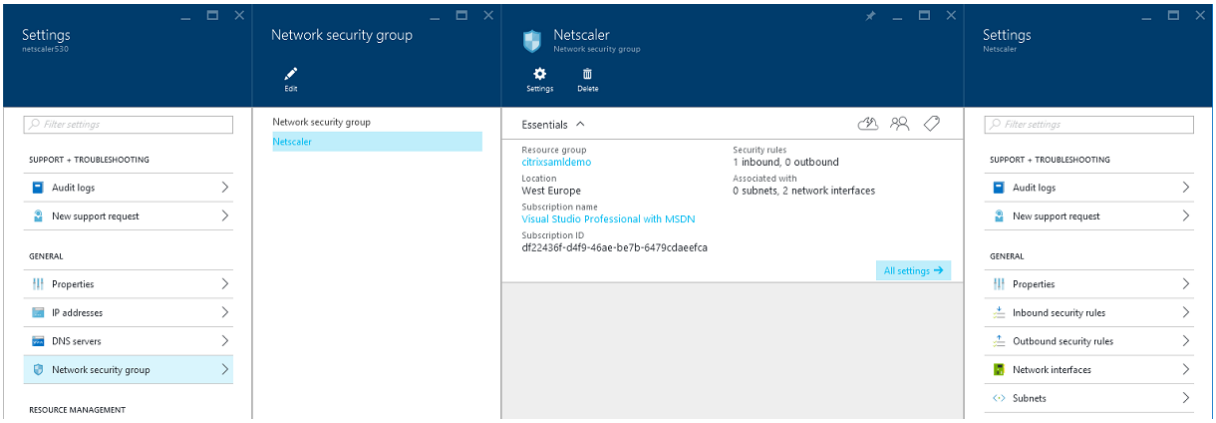


下例将 domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com 的 DNS 地址分配给域控制器。

请注意，远程配置完成后，只有 Web 应用程序代理和 Citrix Gateway VM 应启用公用 IP 地址。（配置过程中，公用 IP 地址用于对环境进行 RDP 访问。）

配置安全组

Azure 云使用安全组从 Internet 管理对 VM 进行 TCP/UDP 访问时使用的防火墙规则。默认情况下，所有 VM 都允许进行 RDP 访问。Citrix Gateway 和 Web 应用程序代理服务器还应允许在端口 443 上启用 TLS。

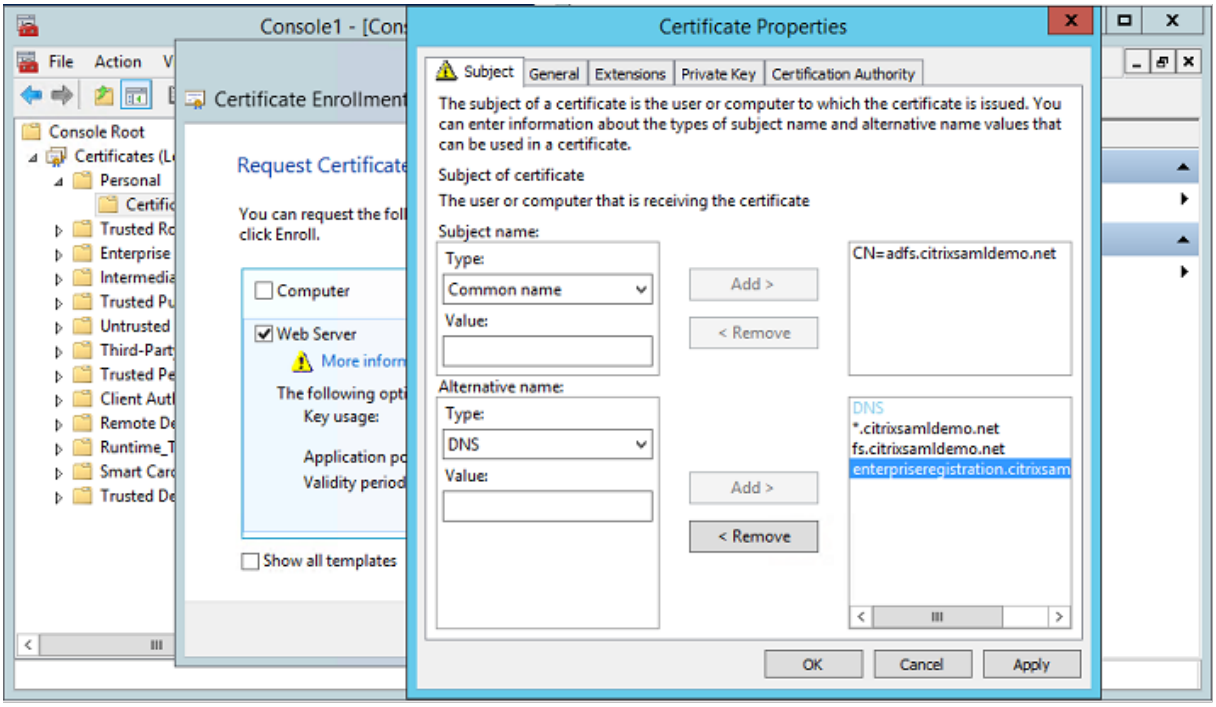


创建 **ADFS** 证书

请在 Microsoft 证书颁发机构上启用 **Web** 服务器证书模板。这允许创建能够导出（包括私钥）为 pfx 文件且使用自定义 DNS 地址的证书。必须同时在 ADFS 和 Web 应用程序代理服务器上安装此证书，PFX 文件才能成为首选项。

颁发使用以下使用者名称的 Web 服务器证书：

- 公用名：
  - adfs.citrixsamldemo.net [计算机名称]
- 使用者备用名称：
  - *.citrixsamldemo.net [区域的名称]
  - fs.citrixsamldemo. net [DNS 中的条目]
  - enterpriseregistration.citrixsamldemo.net



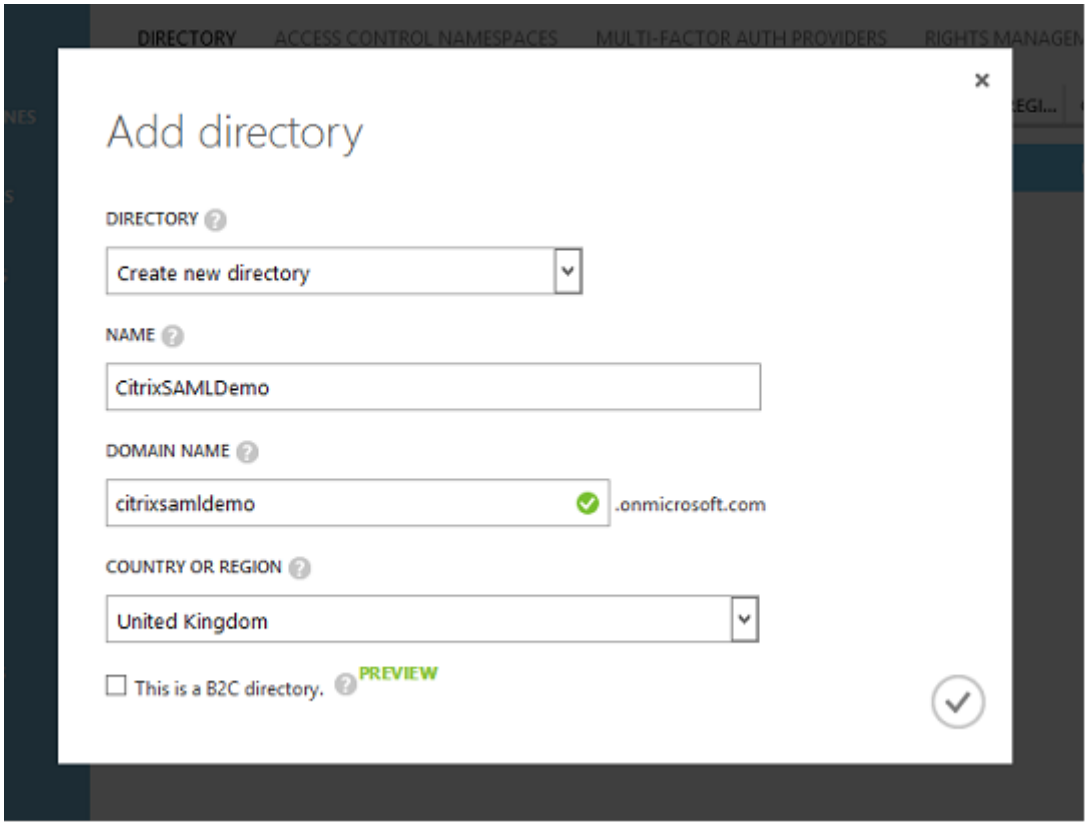
将证书导出为 pfx 文件，包括受密码保护的私钥。

设置 **Azure AD**

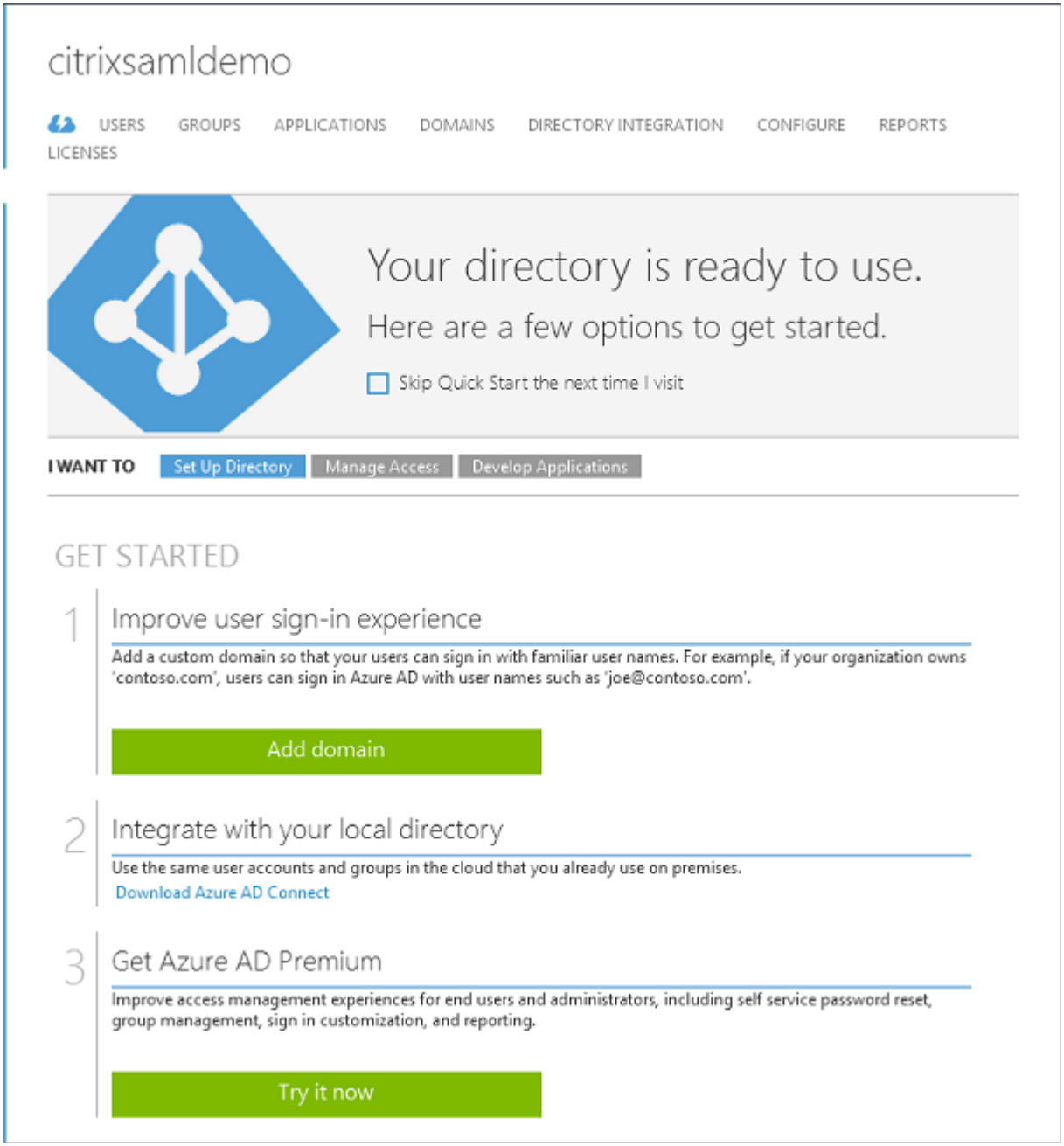
本节详细介绍了设置新 Azure AD 实例以及创建能够用于将 Windows 10 加入 Azure AD 的用户标识的过程。

创建新目录

登录经典 Azure 门户并创建一个新目录。

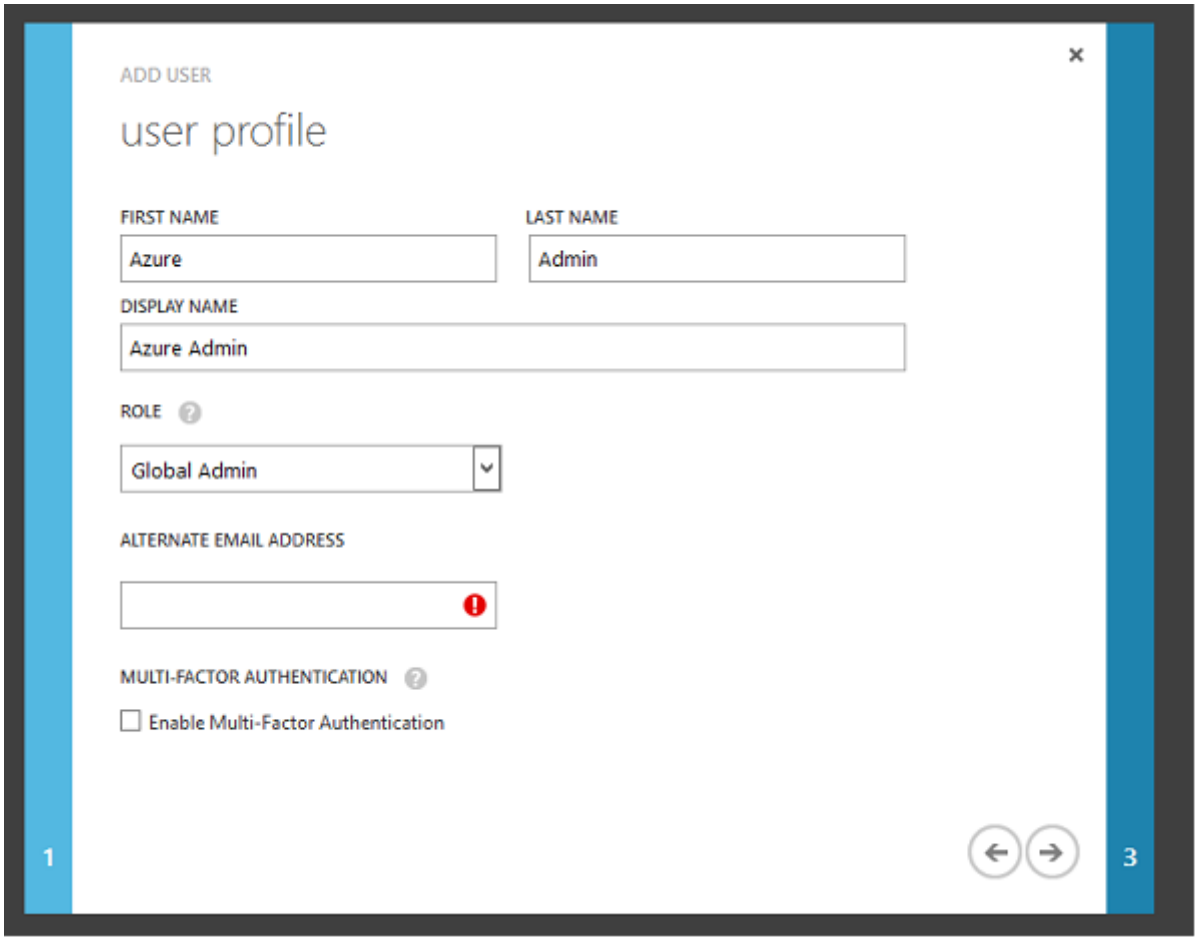


完成时，将显示一个摘要页面。



创建全局管理员用户 **(AzureAdmin)**

在 Azure 中创建一个全局管理员（在此示例中为 `AzureAdmin@citrixsamldemo.onmicrosoft.com`）并使用新帐户登录以设置密码。



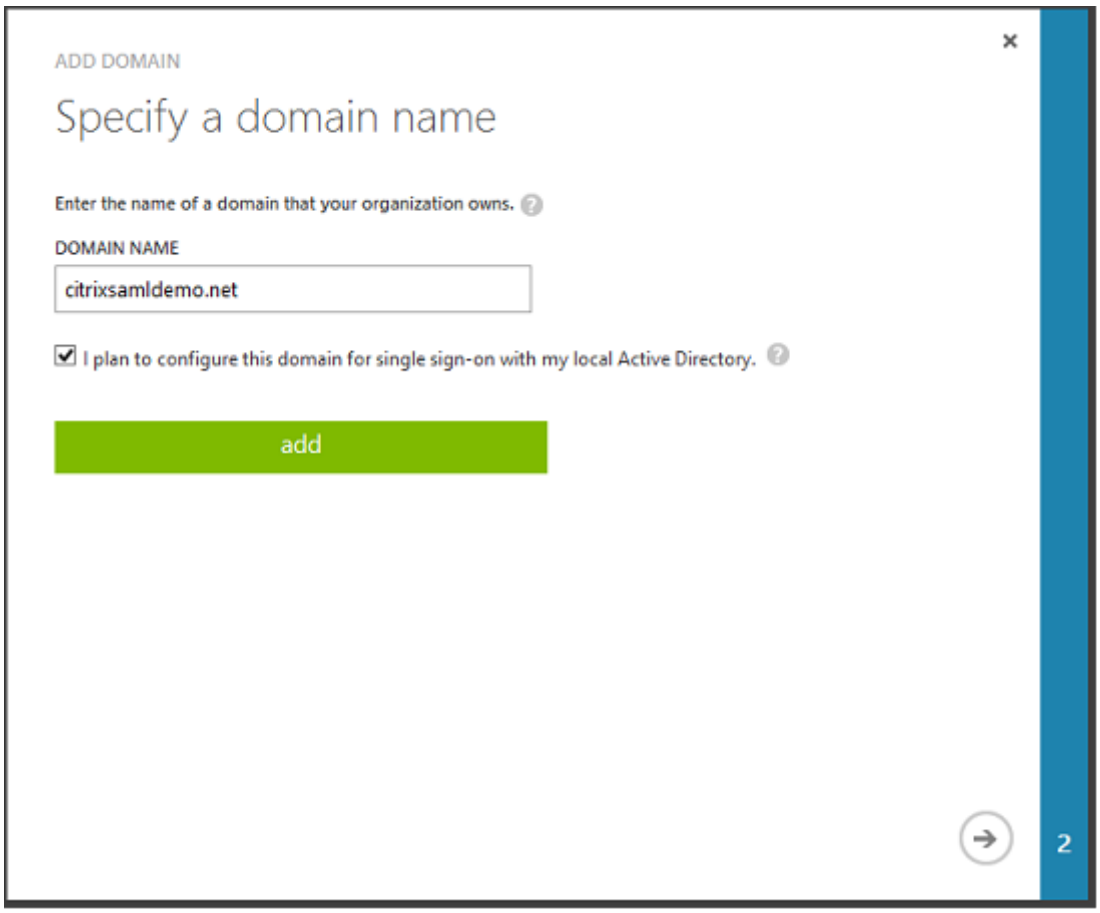
在 **Azure AD** 中注册您的域

默认情况下，用户通过格式为 `<user.name>@<company>.onmicrosoft.com` 的电子邮件地址进行标识。

虽然这在未进一步配置的情况下有效，但最好使用标准格式的电子邮件地址，首选地址为与最终用户的电子邮件帐户匹配的地址：`<user.name>@<company>.com`

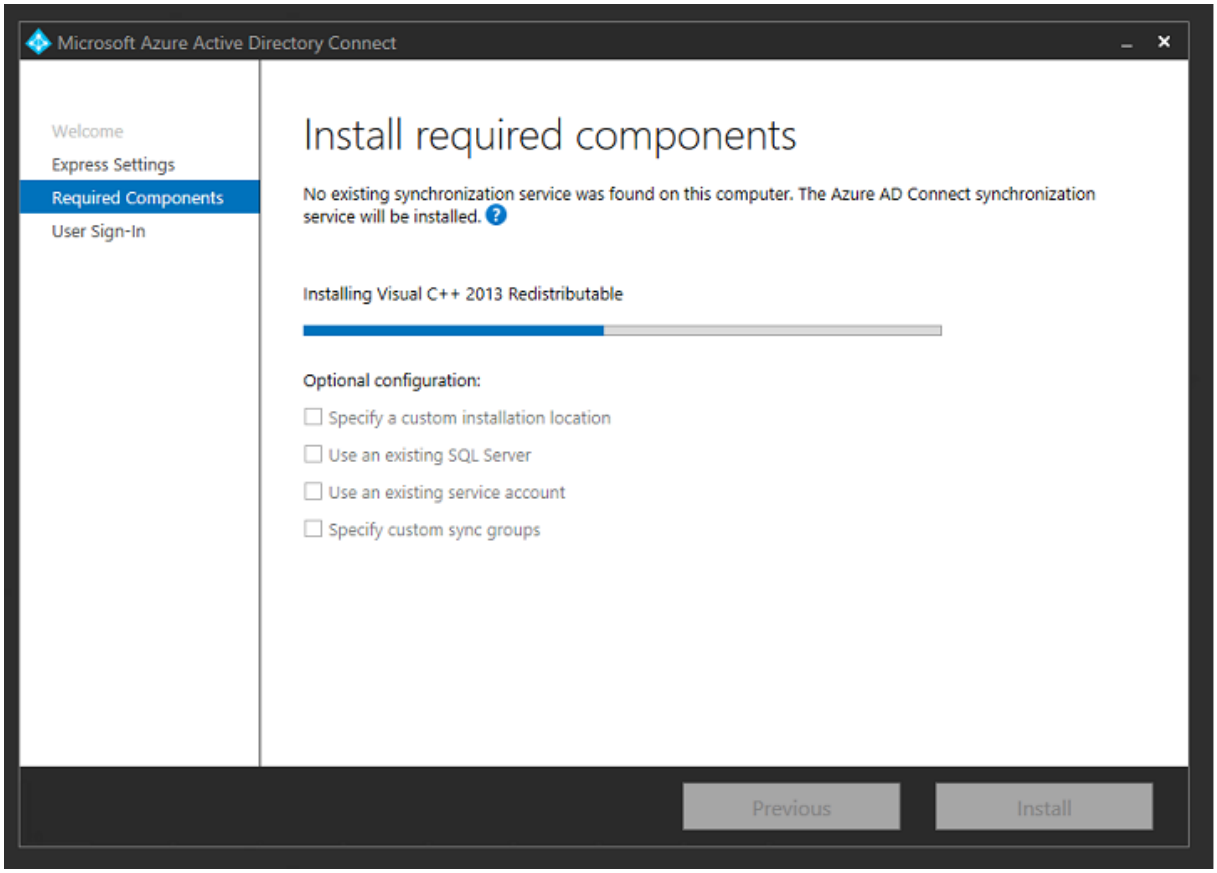
添加域操作配置从您的真实公司域的重定向。此示例使用 `citrixsamldemo.net`。

如果要设置 ADFS 以便进行单点登录，请启用该复选框。

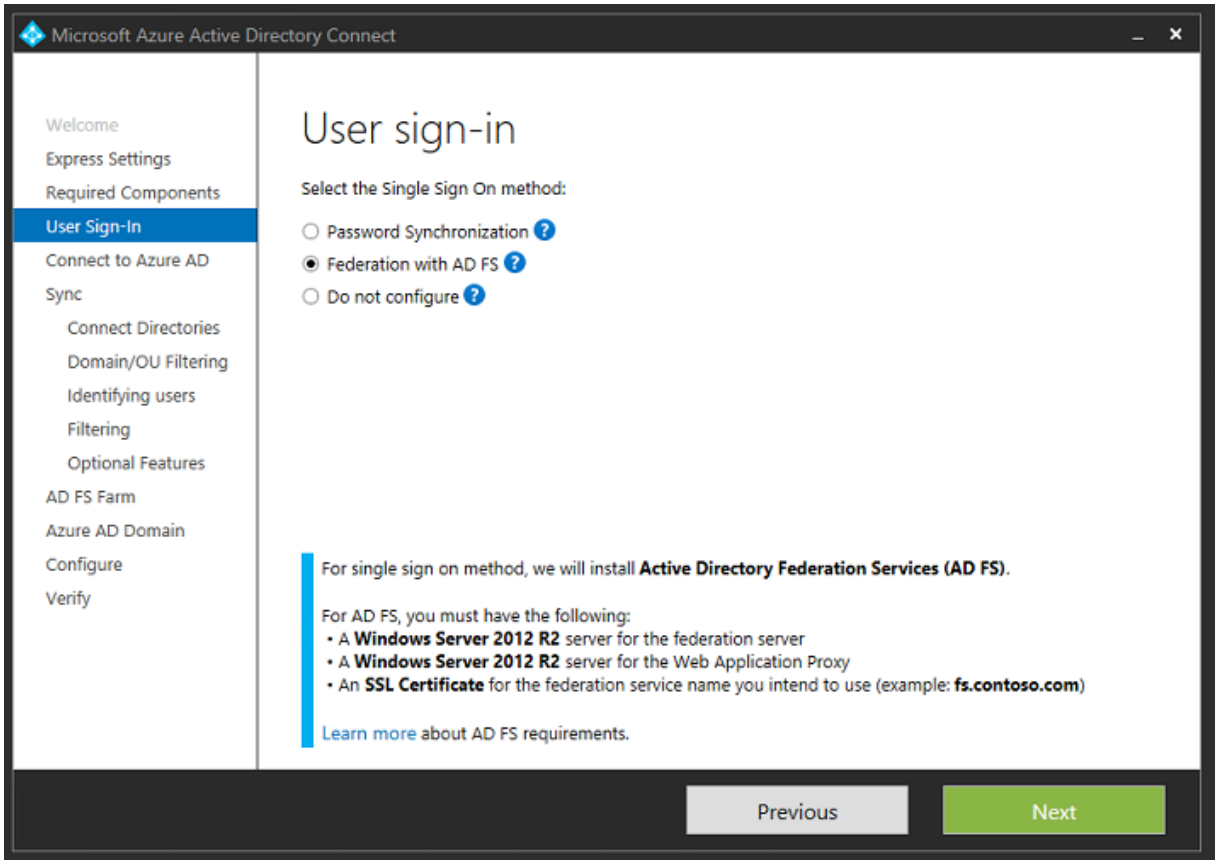


安装 **Azure AD Connect**

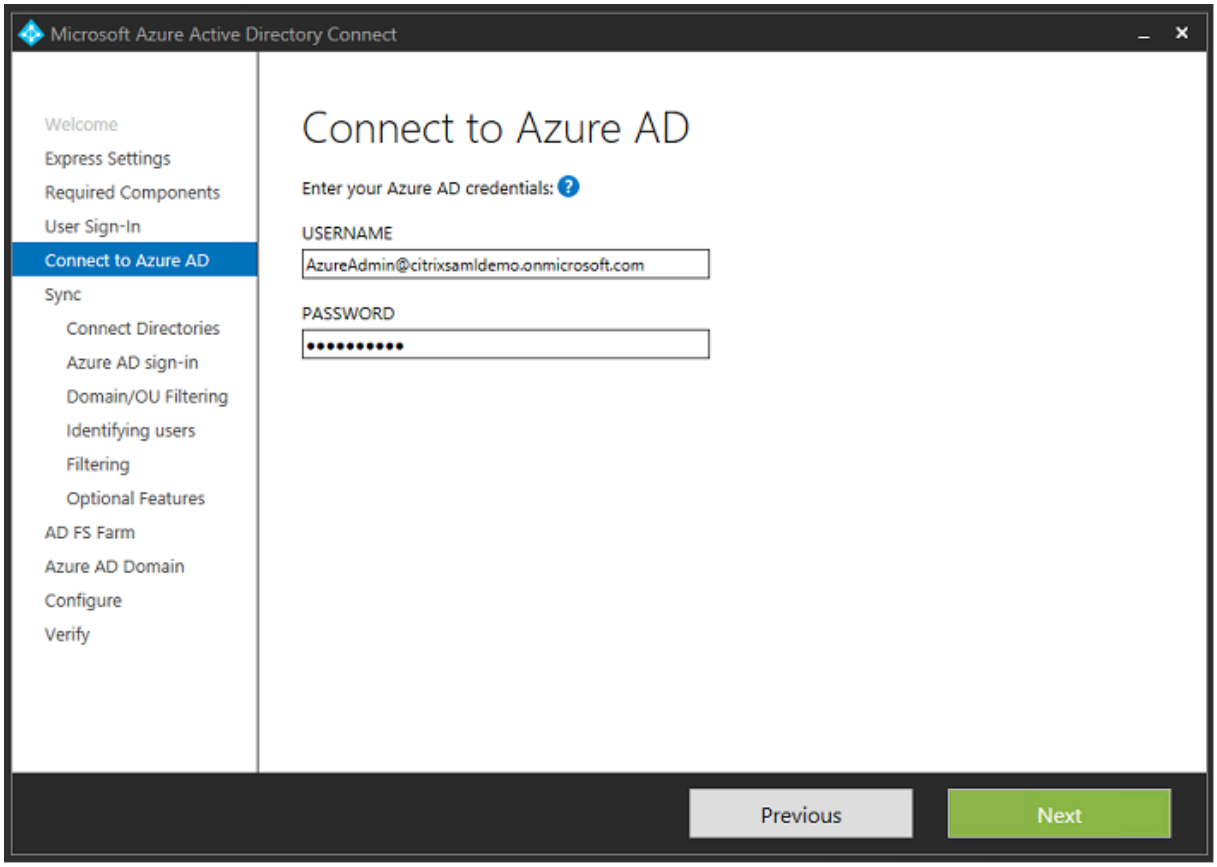
Azure AD 配置 GUI 的步骤 2 重定向到 Azure AD Connect 的 Microsoft 下载页面。在 ADFS VM 上安装此工具。请使用自定义安装（而非快速设置），以使 ADFS 选项可用。



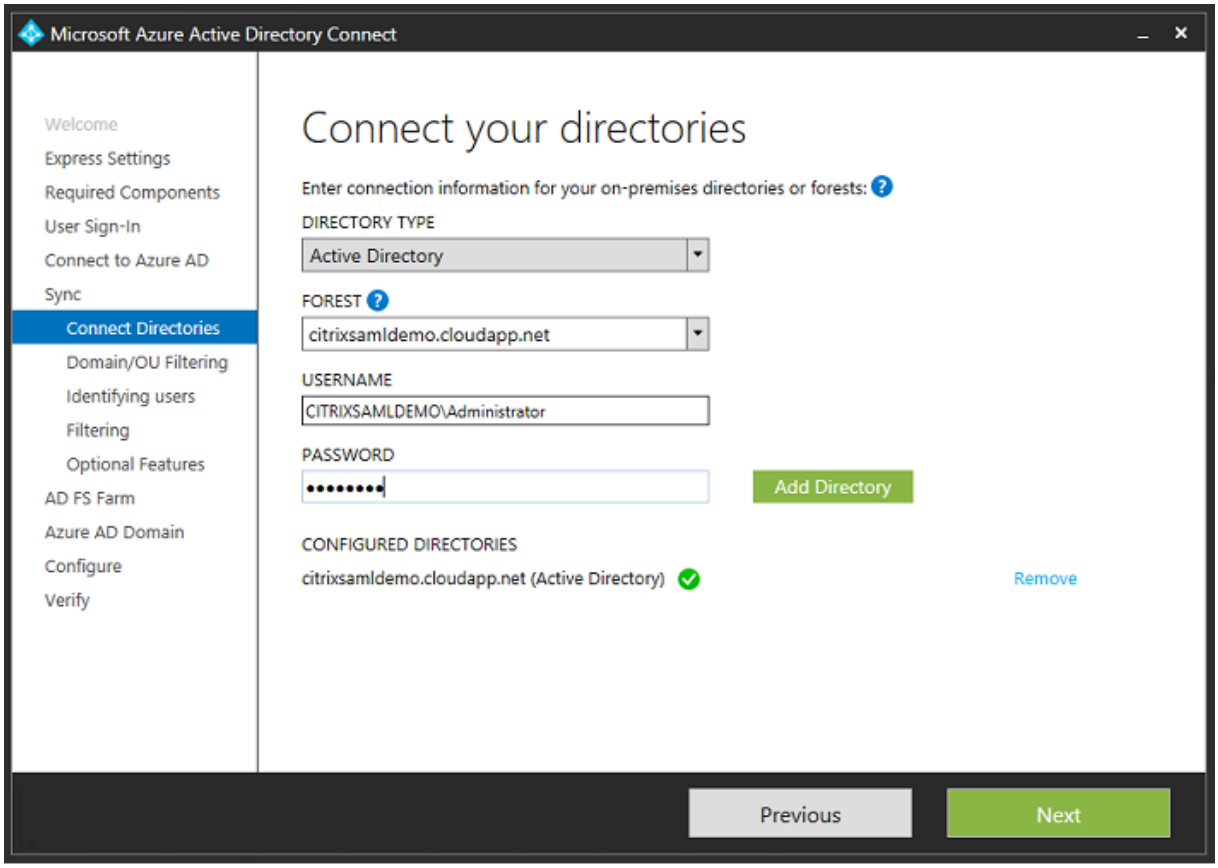
选择使用 **AD FS** 进行联合身份验证单点登录选项。



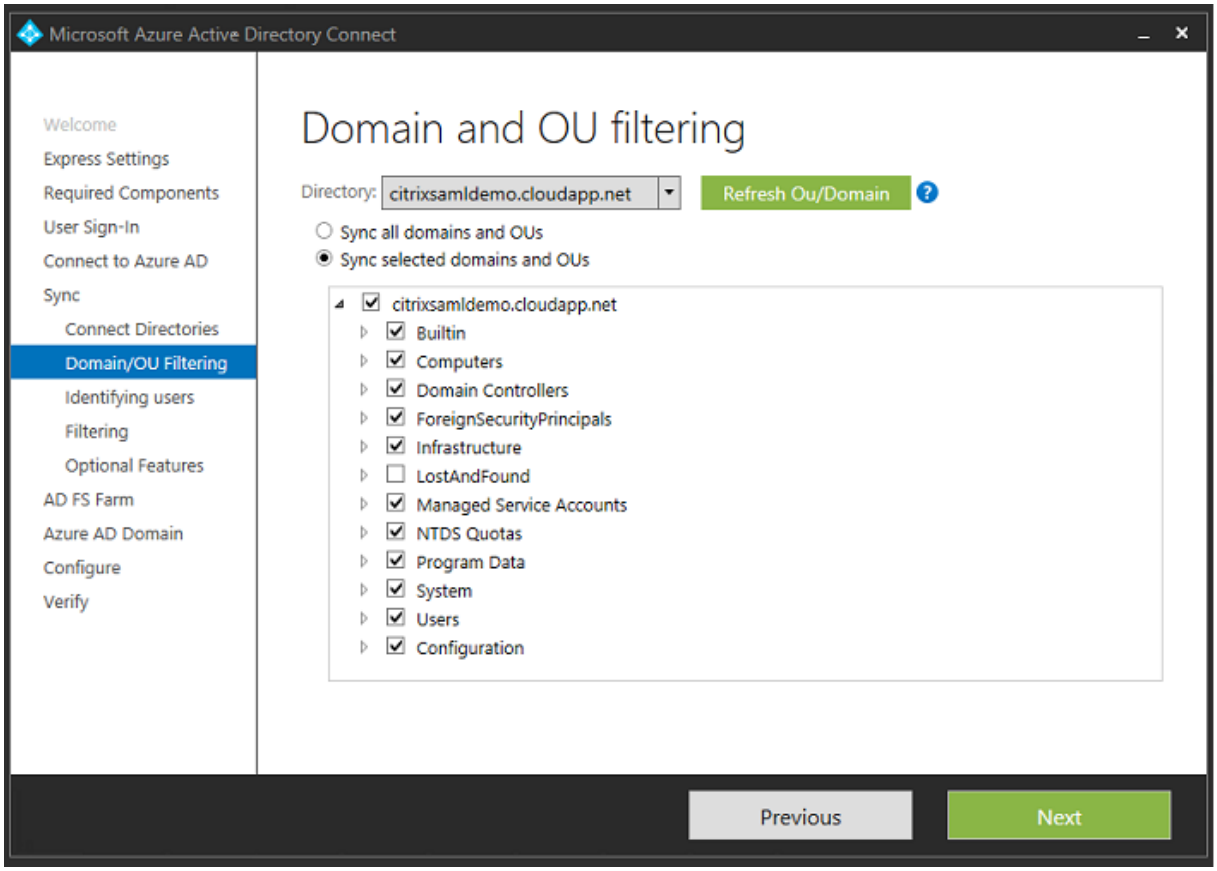
使用之前创建的管理员帐户连接到 Azure。



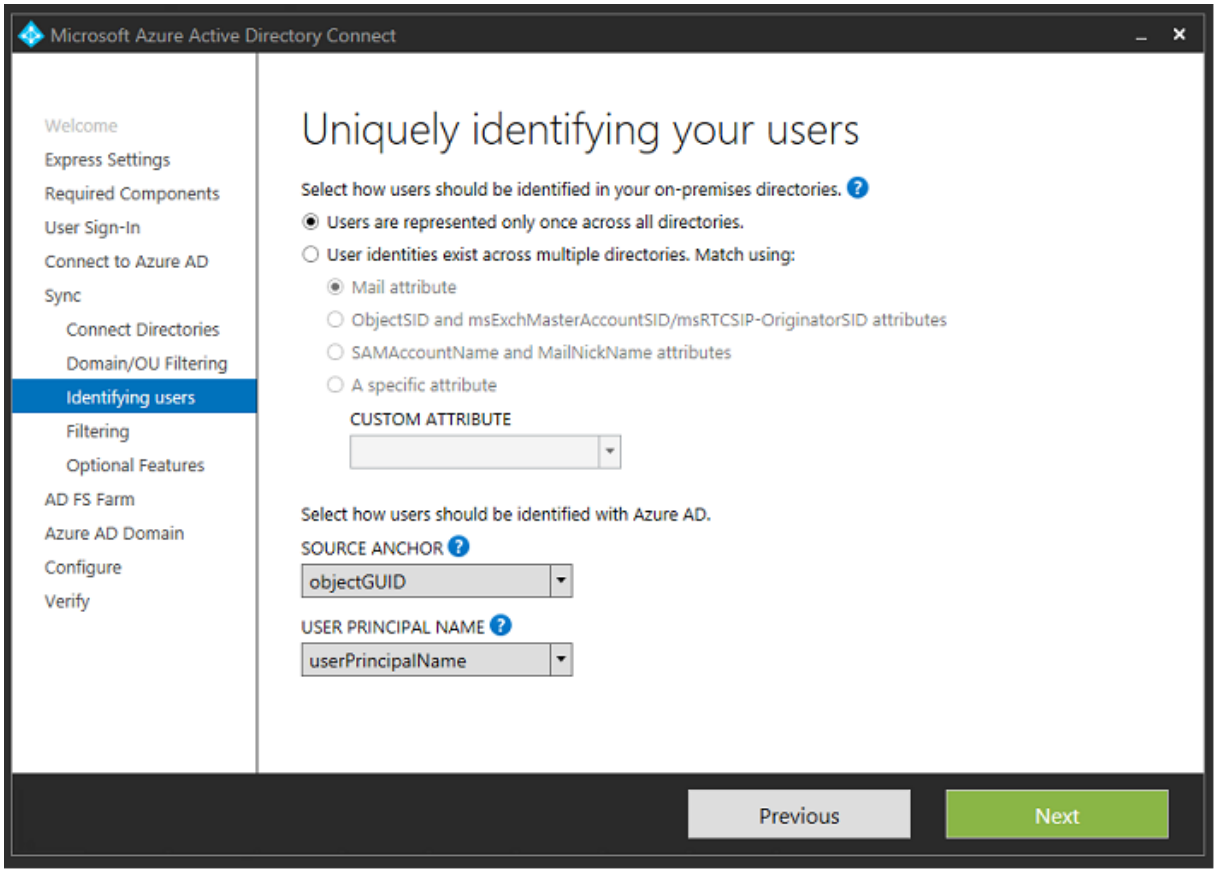
选择内部 AD 林。



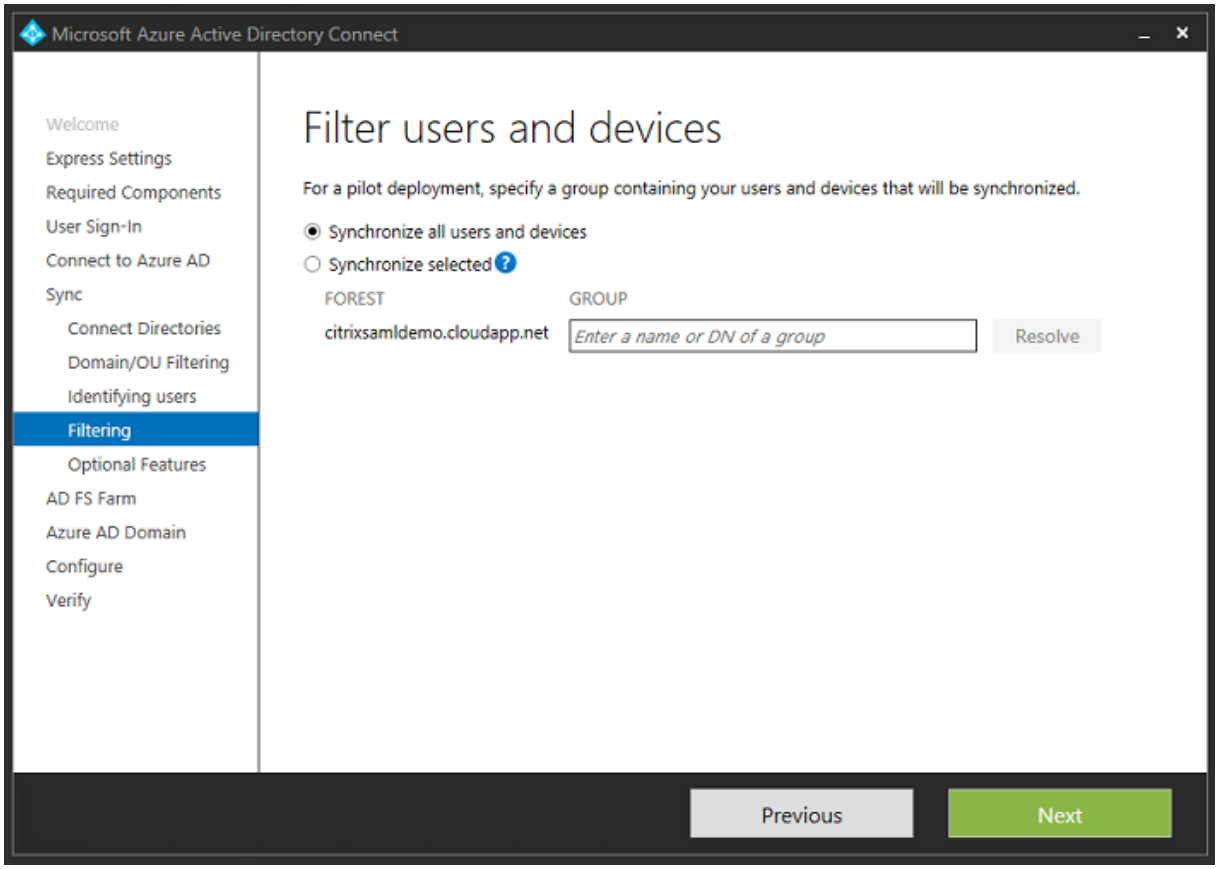
将所有旧 Active Directory 对象与 Azure AD 同步。



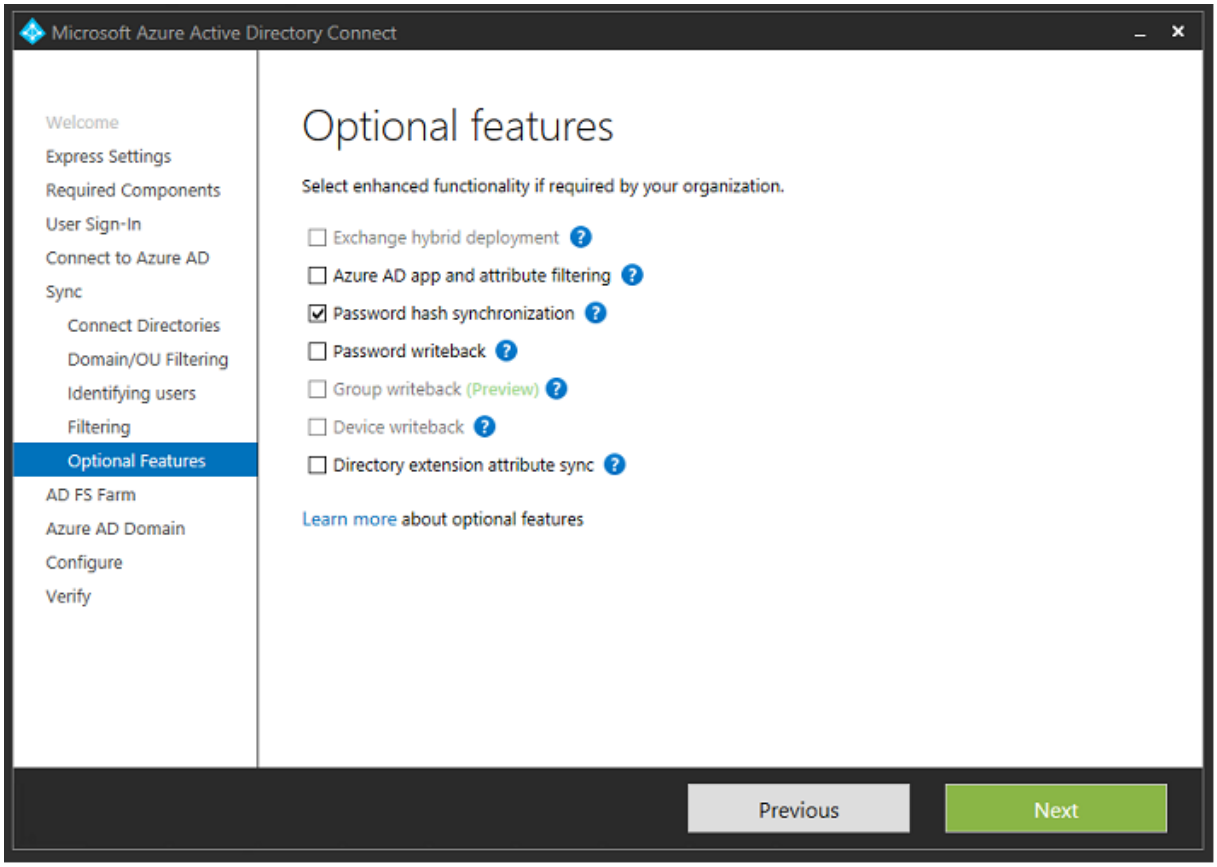
如果目录结构非常简单，可以依靠足够独特的用户名来识别登录的用户。



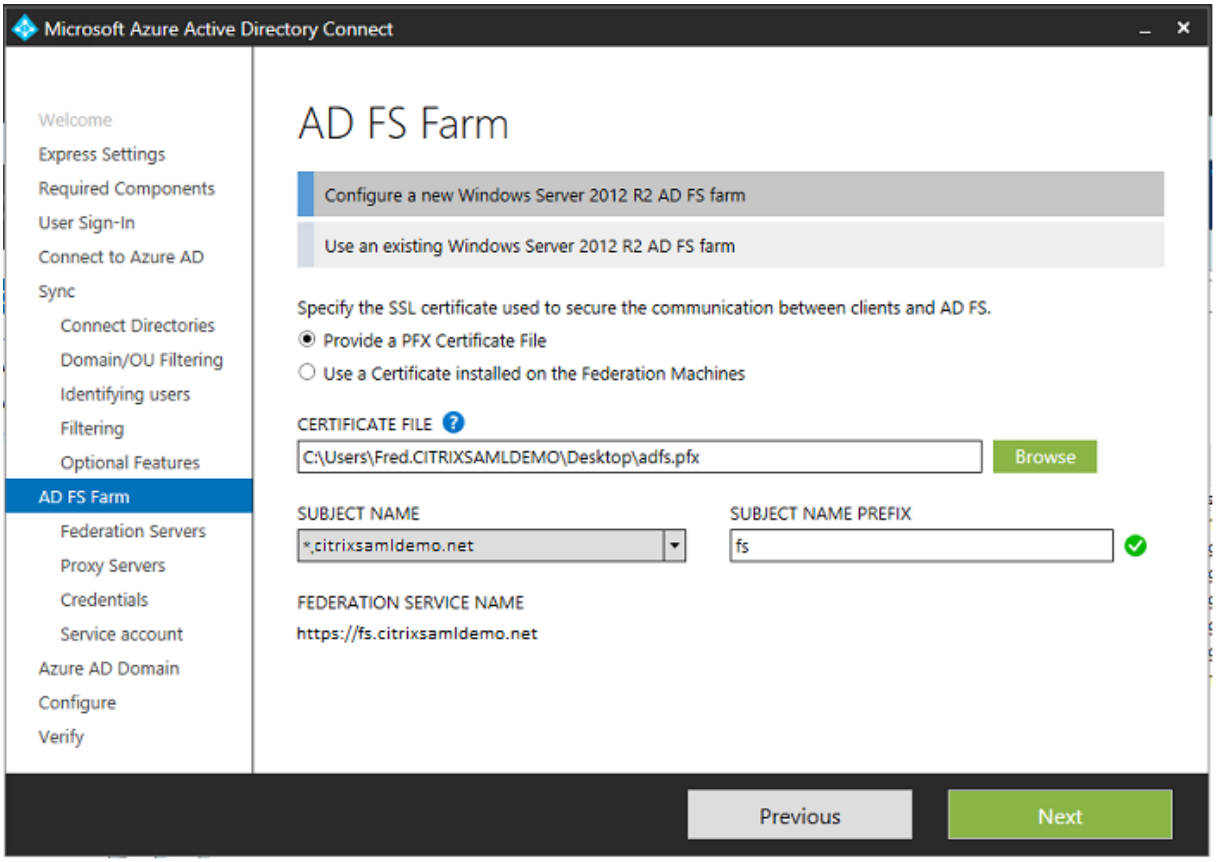
接受默认过滤选项，或者将用户和设备限制为一组特定的用户和设备。



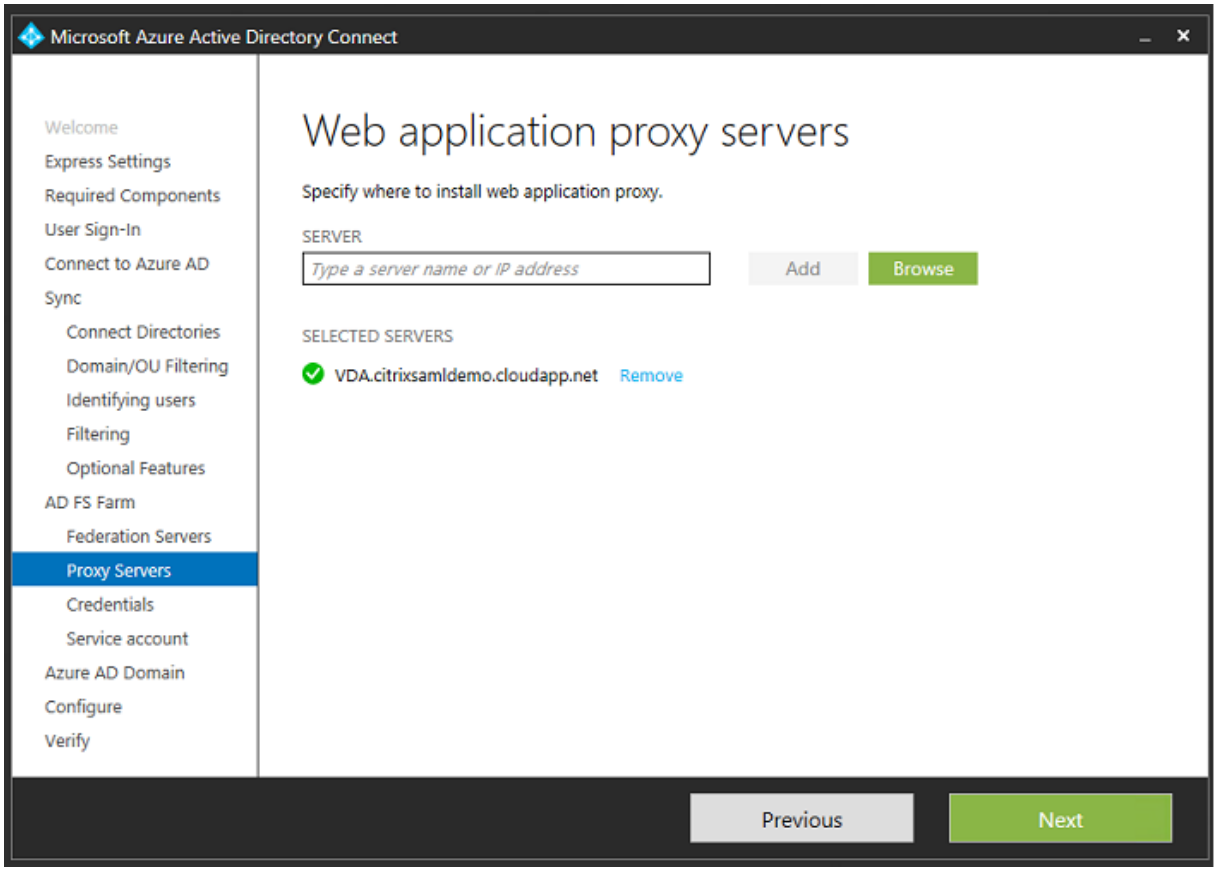
如果需要，可以将 Azure AD 密码与 Active Directory 同步。基于 ADFS 的身份验证通常不需要同步。



选择要在 AD FS 中使用的证书 PFX 文件，指定 fs.citrixsamldemo.net 作为 DNS 名称。

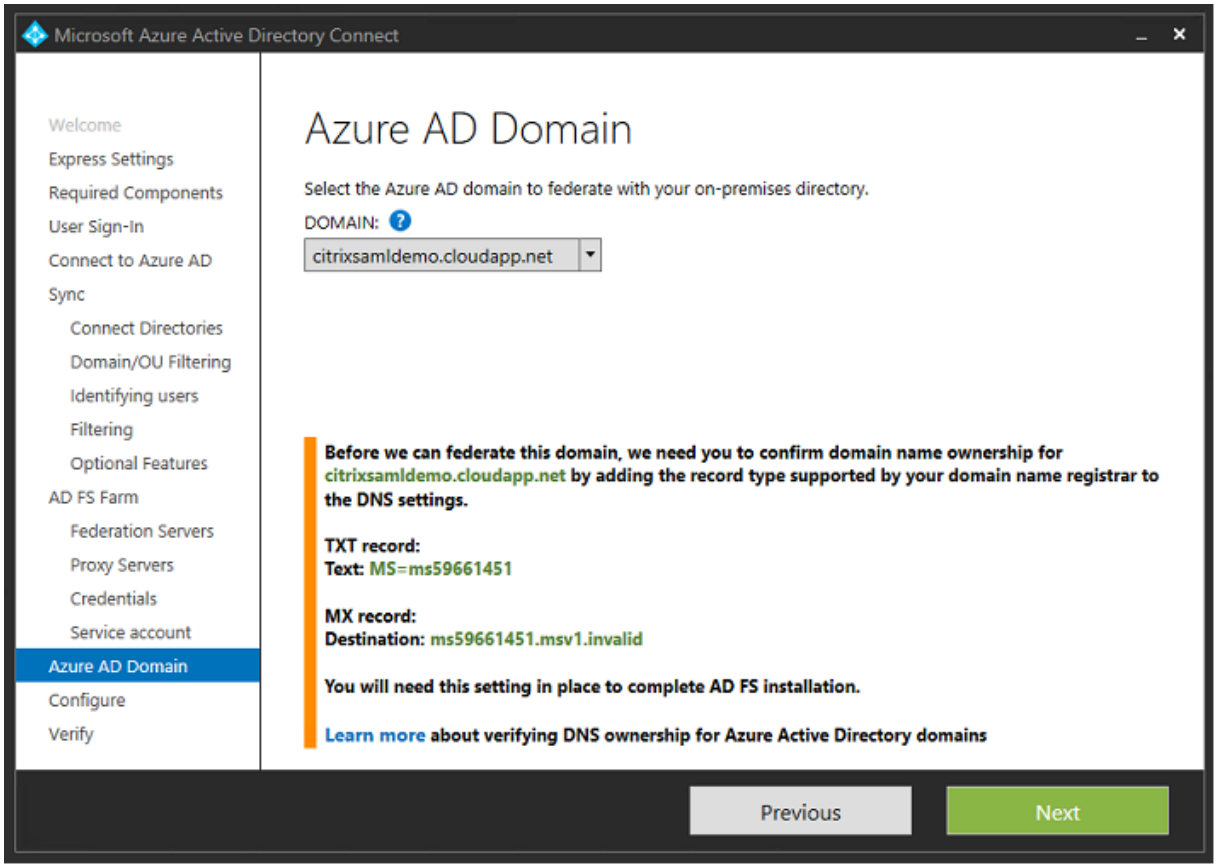


提示选择代理服务器时，输入 wap.citrixsamldemo.net 服务器的地址。您可能需要在 Web 应用程序代理服务器上以管理员身份运行 **Enable-PSRemoting -Force** cmdlet，以便 Azure AD Connect 能够对其进行配置。

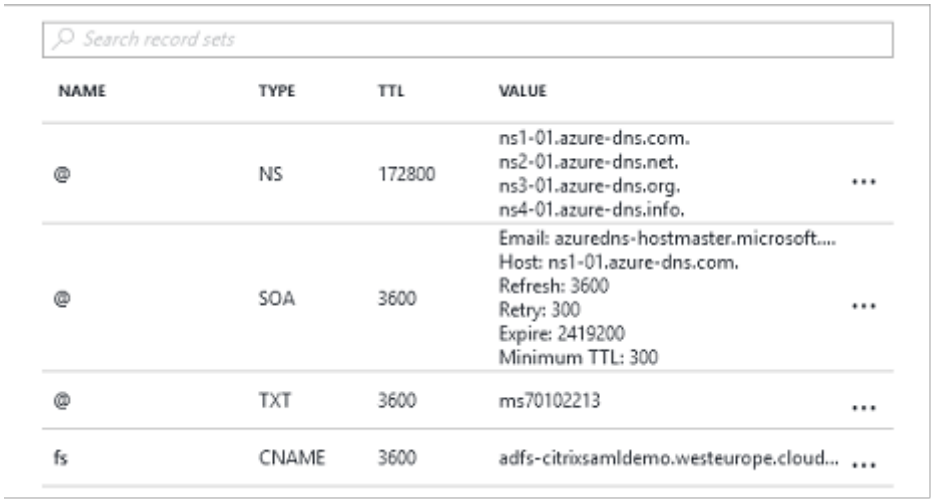


> 注意：
>
> 如果此步骤由于远程 PowerShell 信任问题失败，请尝试将 Web 应用程序代理服务器加入域中。

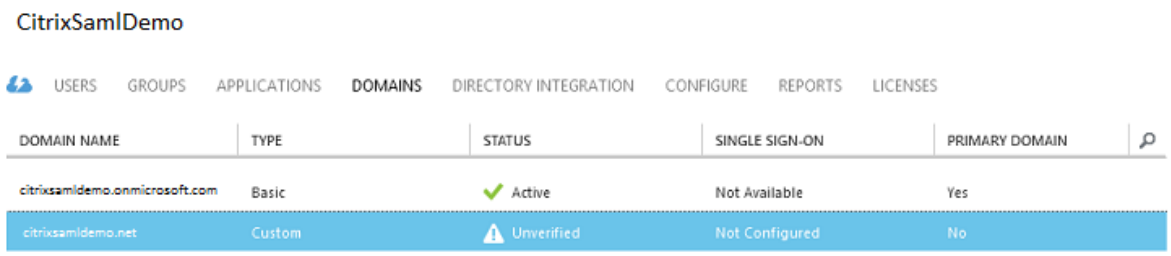
对于向导的其余步骤，请使用标准的管理员密码，并为 ADFS 创建一个服务帐户。Azure AD Connect 之后将提示您验证 DNS 区域的所有权。



将 TXT 和 MX 记录添加到 Azure 中的 DNS 地址记录。

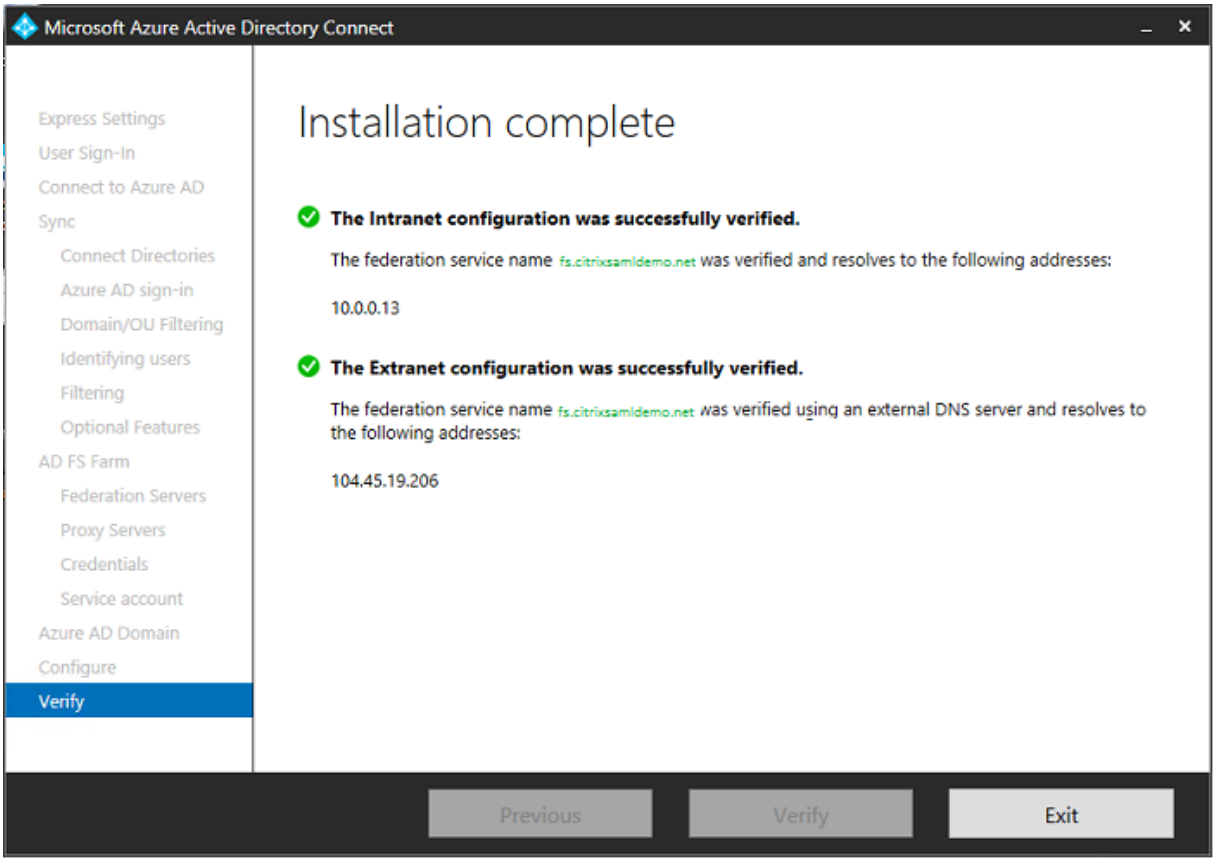


在 Azure 管理控制台中单击验证。



> 注意：
>
> 如果此步骤失败，可以在运行 Azure AD Connect 之前验证域。

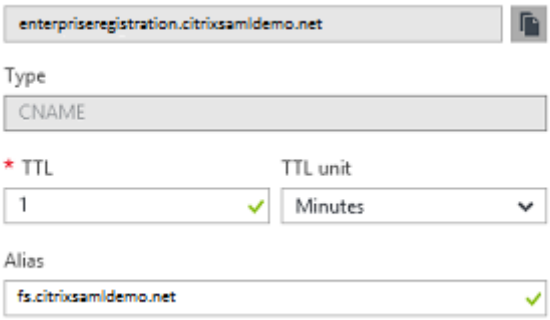
完成后，外部地址 fs.citrixsamldemo.net 将通过端口 443 进行访问。



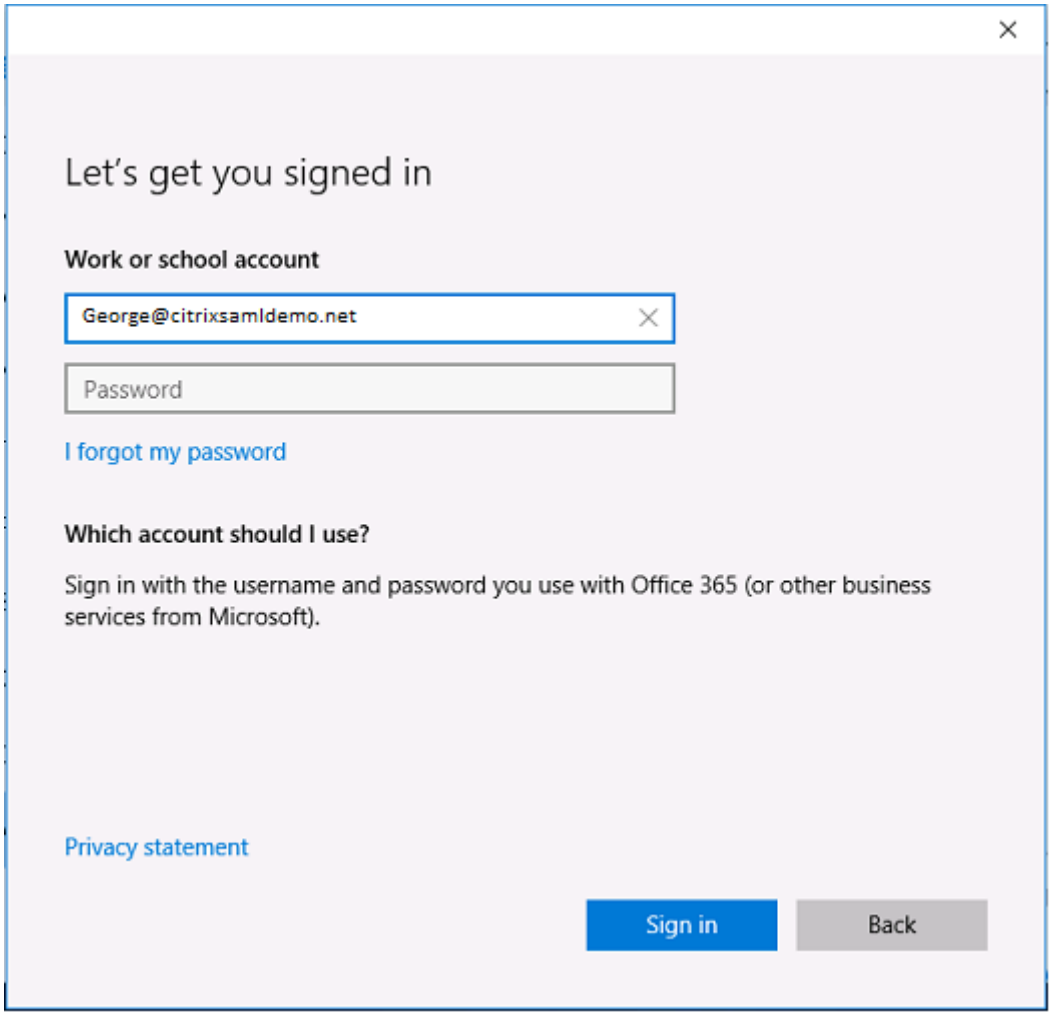
启用 **Azure AD** 联接

用户输入电子邮件地址以便 Windows 10 能够执行 Azure AD 加入操作时，将使用 DNS 后缀构建应指向 ADFS 的 CNAME DNS 记录：enterpriseregistration.<*upnsuffix*>。

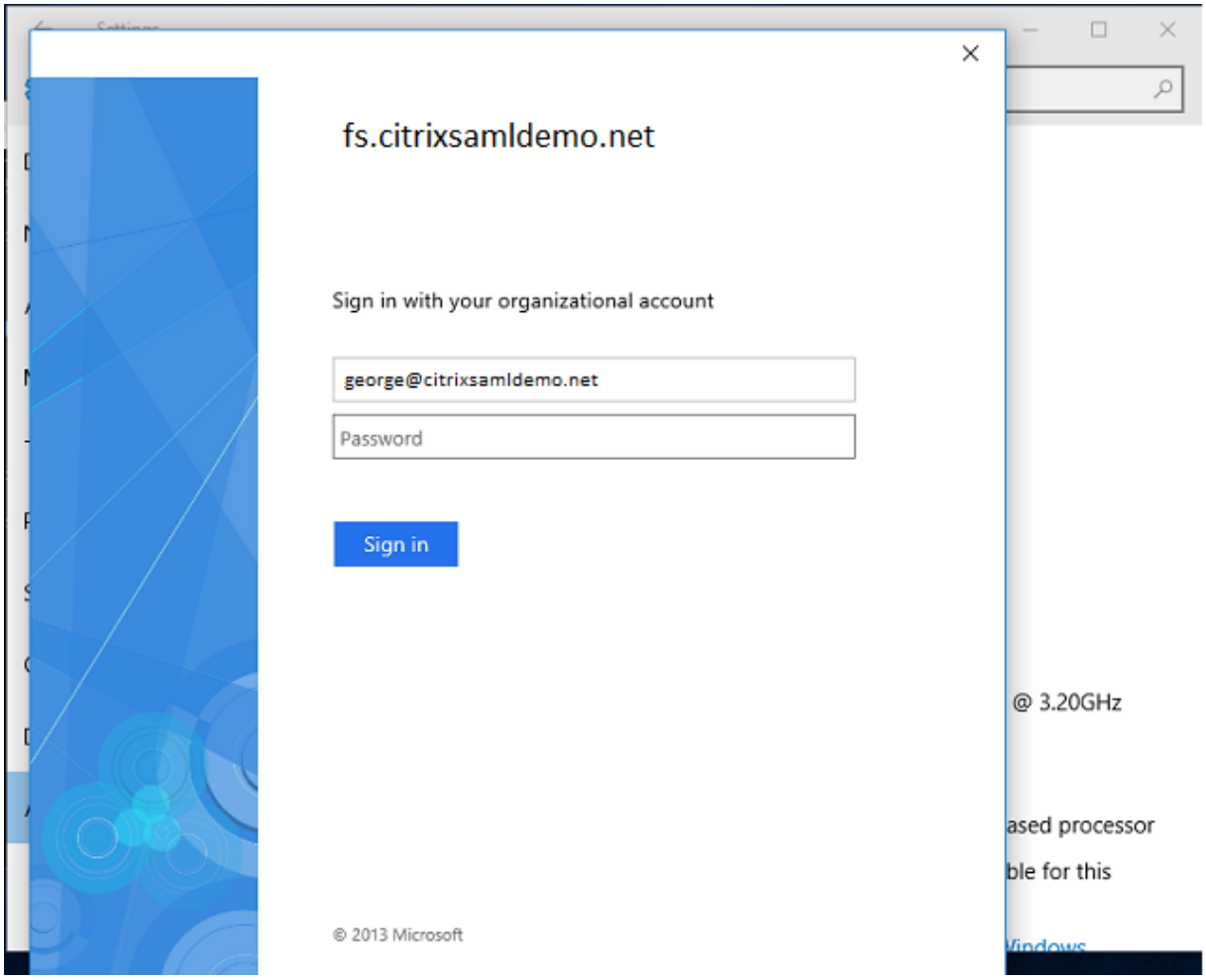
在此示例中，这是 `fs.citrixsamldemo.net`。

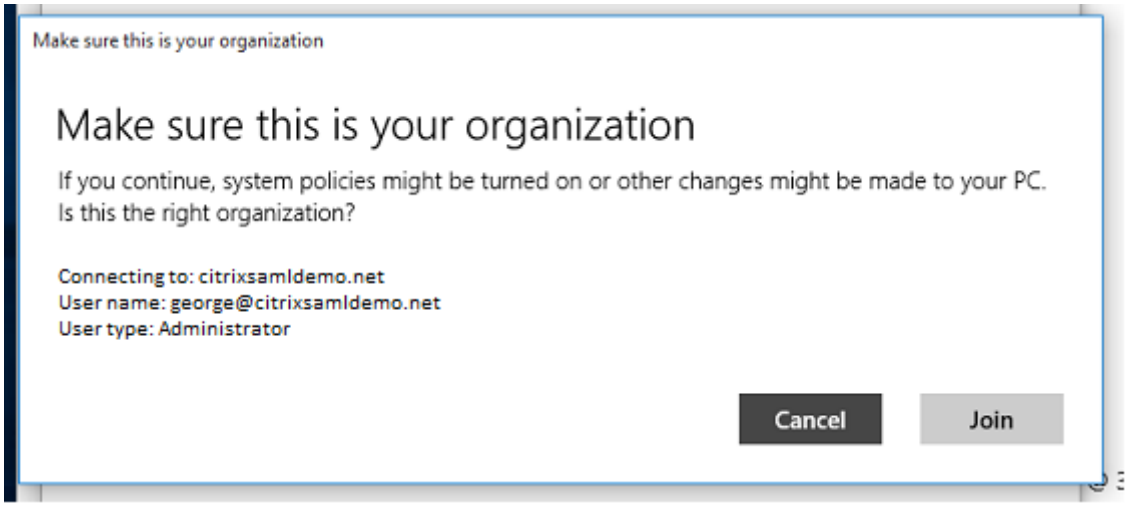


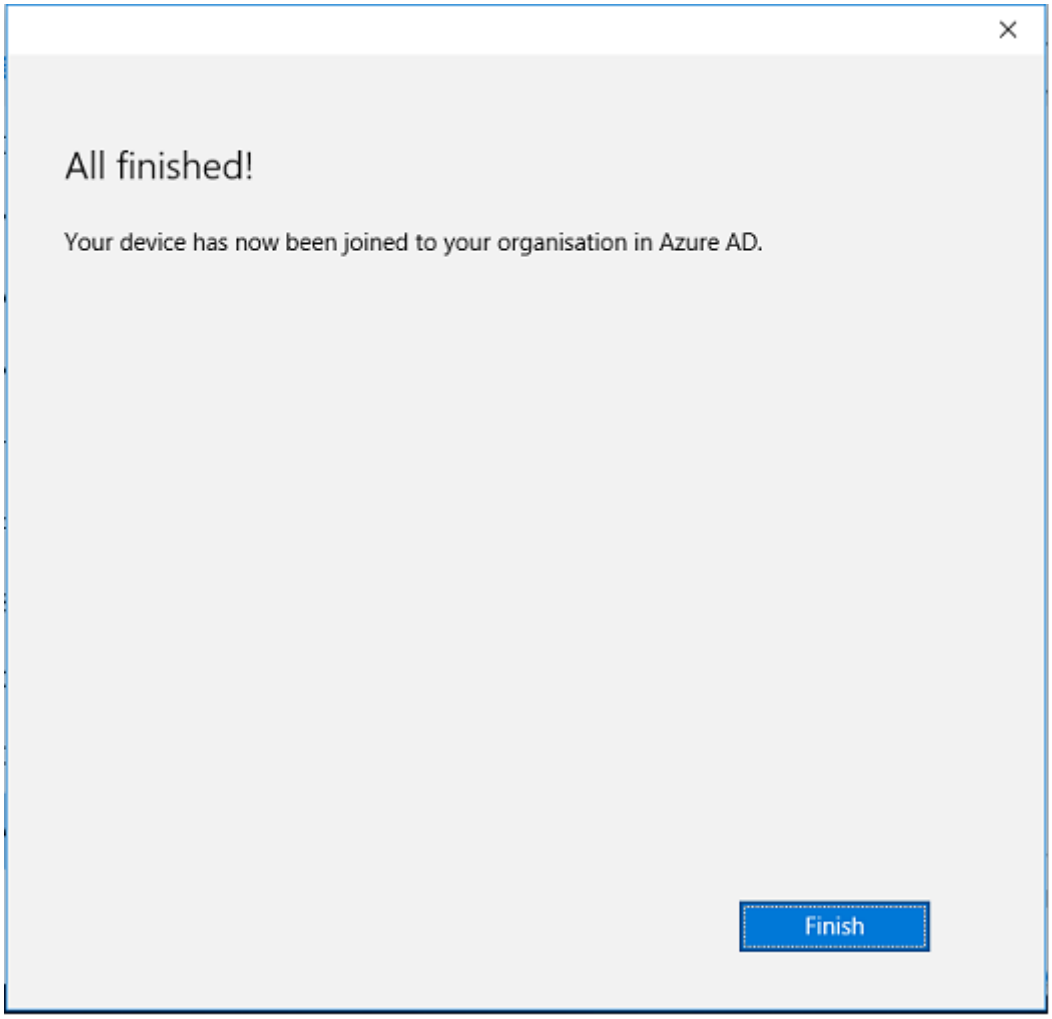
如果未使用公用证书颁发机构，请务必在 Windows 10 计算机上安装 ADFS 根证书，这样 Windows 将信任 ADFS 服务器。使用之前生成的标准用户帐户执行 Azure AD 域联接操作。



请注意：UPN 必须与 ADFS 域控制器能够识别的 UPN 匹配。





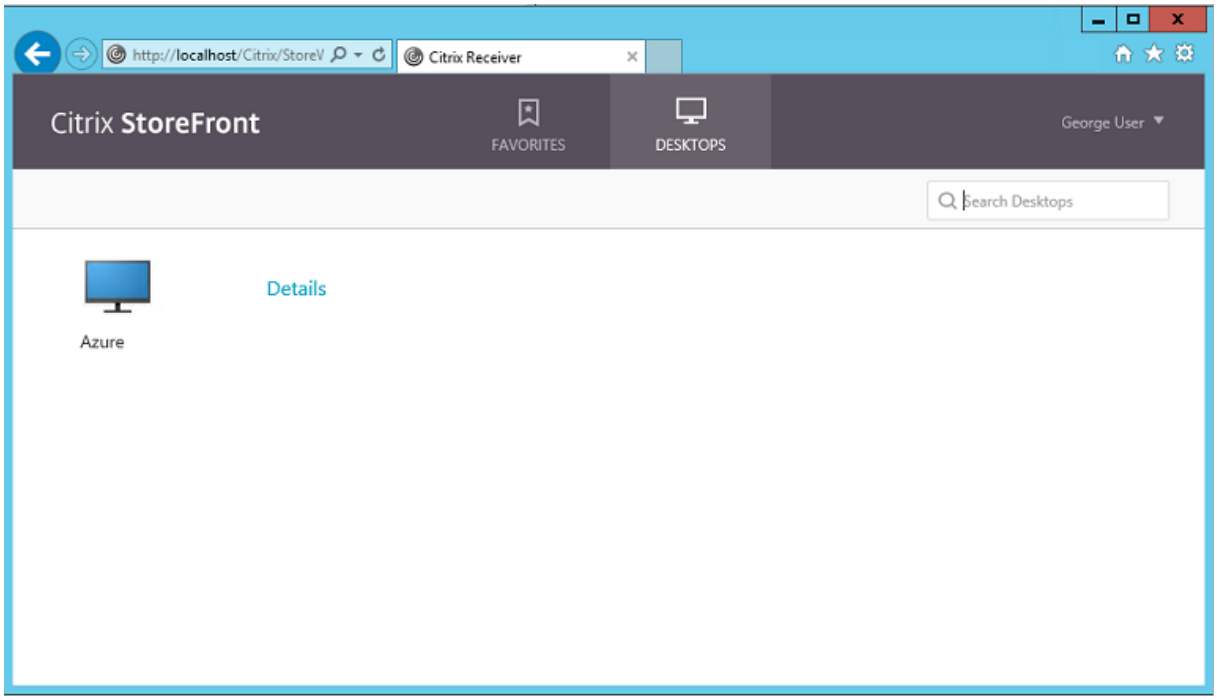


使用用户的电子邮件地址通过重新启动计算机并登录来验证 Azure AD 联接操作是否成功。登录后，请启动 Microsoft Edge 并连接到 http://myapps.microsoft.com。该 Web 站点应自动使用单点登录功能。

安装 Citrix Virtual Apps 或 Citrix Virtual Desktops

可以按常规方式在 Azure 中直接从 Citrix Virtual Apps 或 Citrix Virtual Desktops ISO 安装 Delivery Controller 和 VDA 虚拟机。

在此示例中，StoreFront 与 Delivery Controller 安装在相同的服务器上。VDA 作为独立的 Windows 2012 R2 RDS 工作进程安装，不与 Machine Creation Services 集成（尽管能够选择性配置）。继续操作之前，请检查用户 George@citrixsamldemo.net 是否能够使用密码进行身份验证。



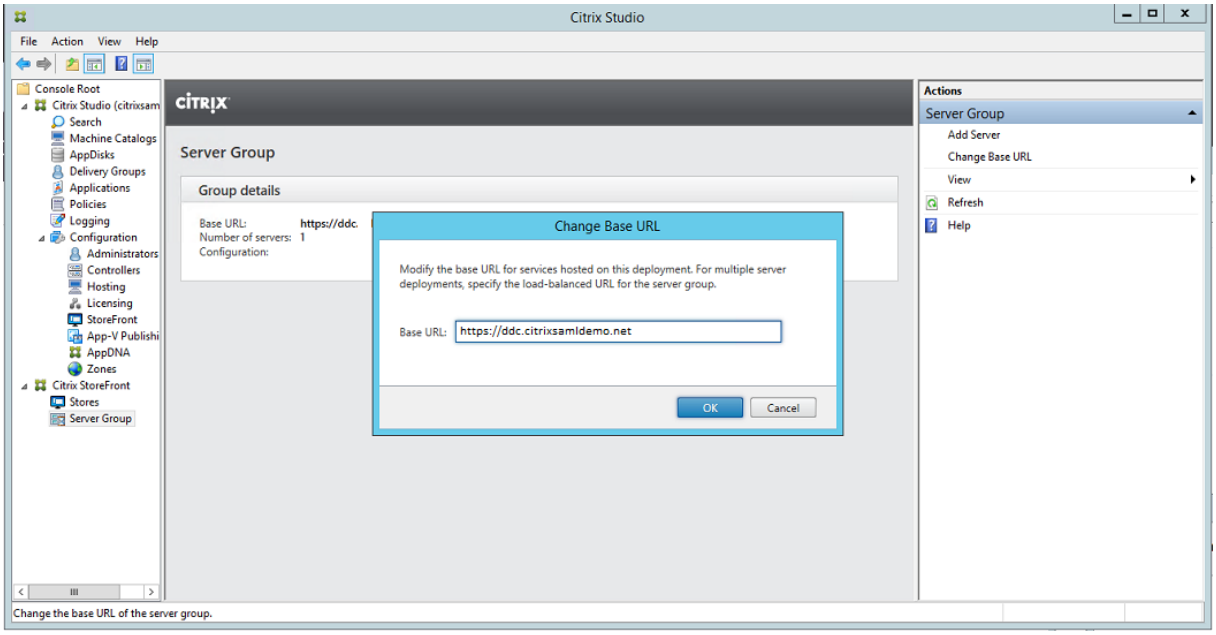
在 Controller 上运行 **Set-BrokerSite –TrustRequestsSentToTheXmlServicePort $true** PowerShell cmdlet 以允许 StoreFront 不使用用户的凭据进行身份验证。

安装联合身份验证服务

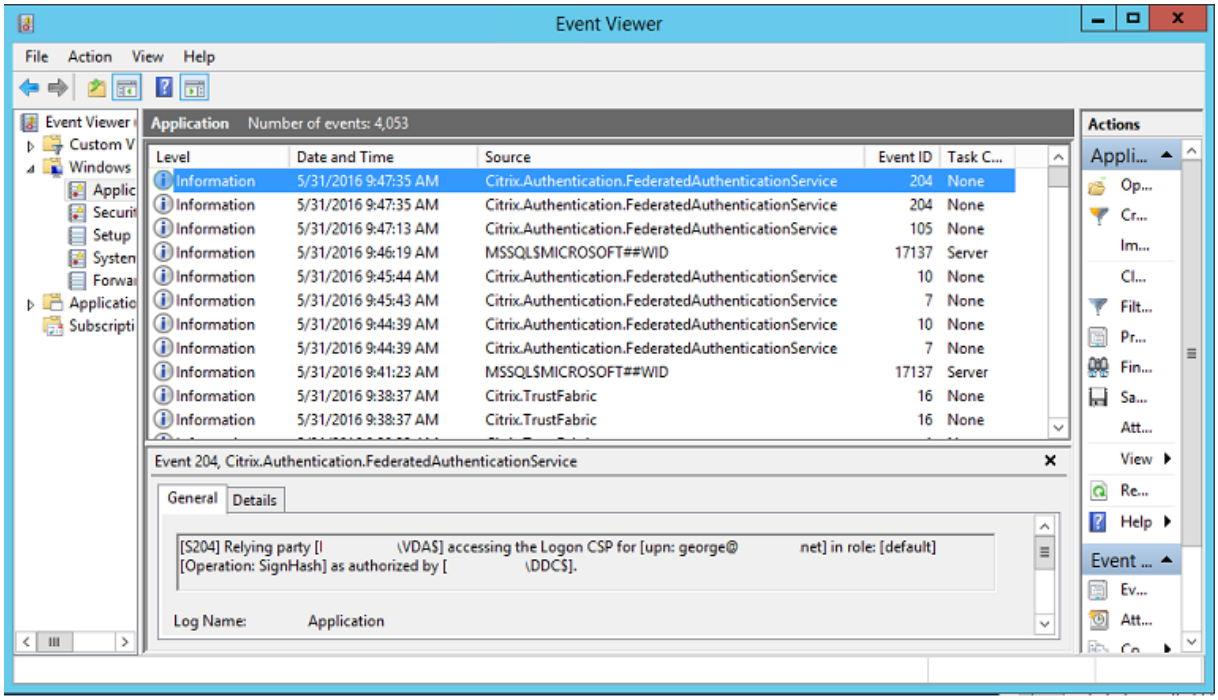
在 ADFS 服务器上安装 FAS，并为 Delivery Controller 配置规则以充当可信 StoreFront（因为在本示例中，StoreFront 安装在与 Delivery Controller 相同的 VM 上）。请参阅安装和配置。

配置 **StoreFront**

为 Delivery Controller 申请一个计算机证书，然后将 IIS 和 StoreFront 配置为使用 HTTPS，方法是为端口 443 设置 IIS 绑定，并将 StoreFront 基址更改为 https:。

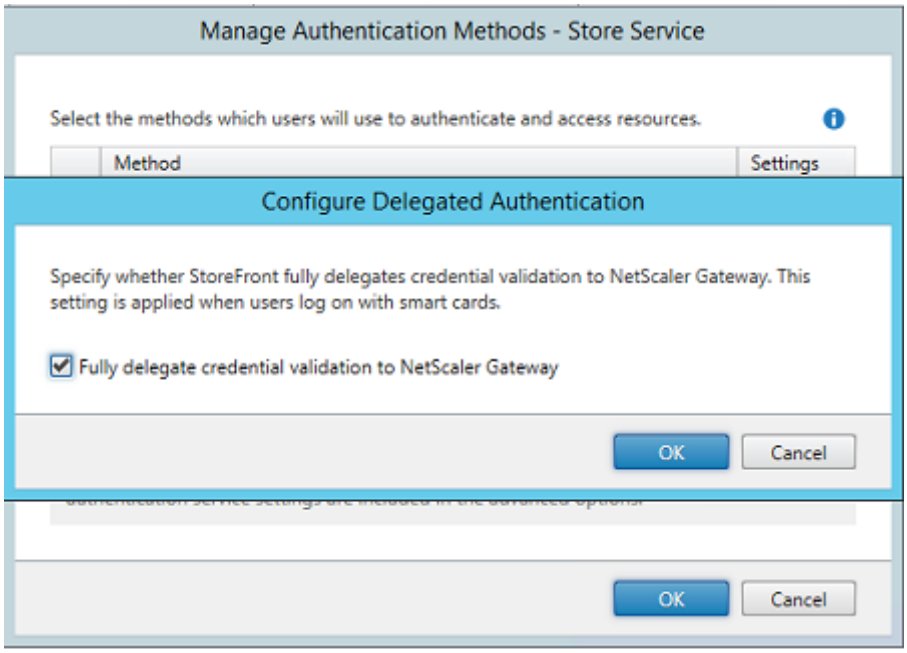


将 StoreFront 配置为使用 FAS 服务器（使用安装和配置中的 PowerShell 脚本），然后在 Azure 中进行内部测试，通过查看 FAS 服务器上的事件查看器来确保登录使用 FAS。

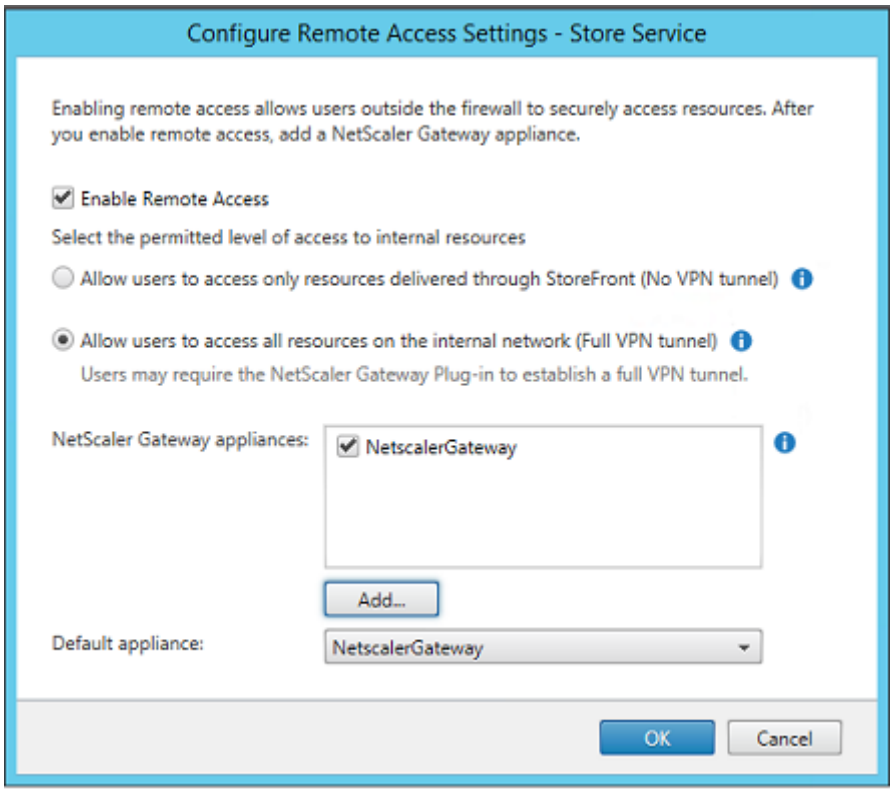


将 **StoreFront** 配置为使用 **Citrix Gateway**

在 StoreFront 管理控制台中使用管理身份验证方法 GUI 将 StoreFront 配置为使用 Citrix Gateway 执行身份验证。

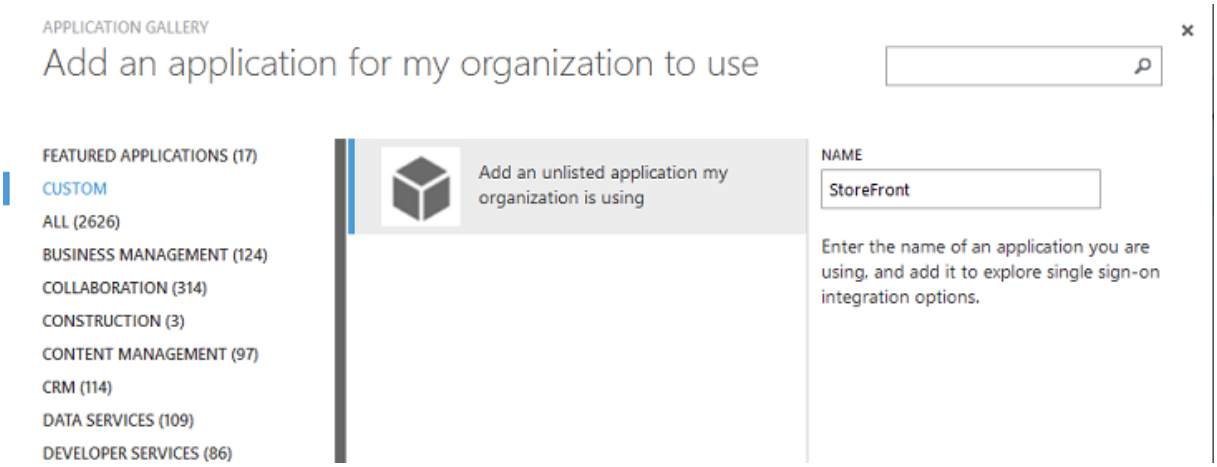


要集成 Citrix Gateway 身份验证选项，请配置一个 Secure Ticket Authority (STA) 并配置 Citrix Gateway 地址。



配置新 **Azure AD** 应用程序以单点登录到 **StoreFront**

本节使用 Azure AD SAML 2.0 单点登录功能，该功能当前要求订阅 Azure Active Directory Premium。在 Azure AD 管理工具中，选择新建应用程序和从库中添加一个应用程序。



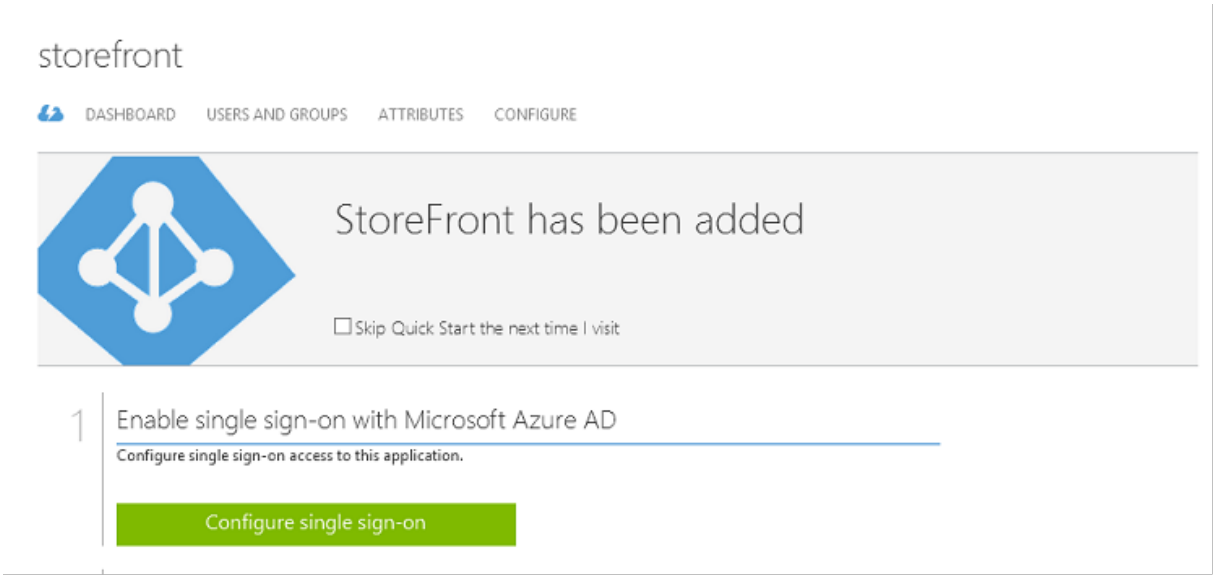
选择自定义 **>** 添加我的组织在使用的未列出应用程序为您的用户创建一个新自定义应用程序。

配置图标

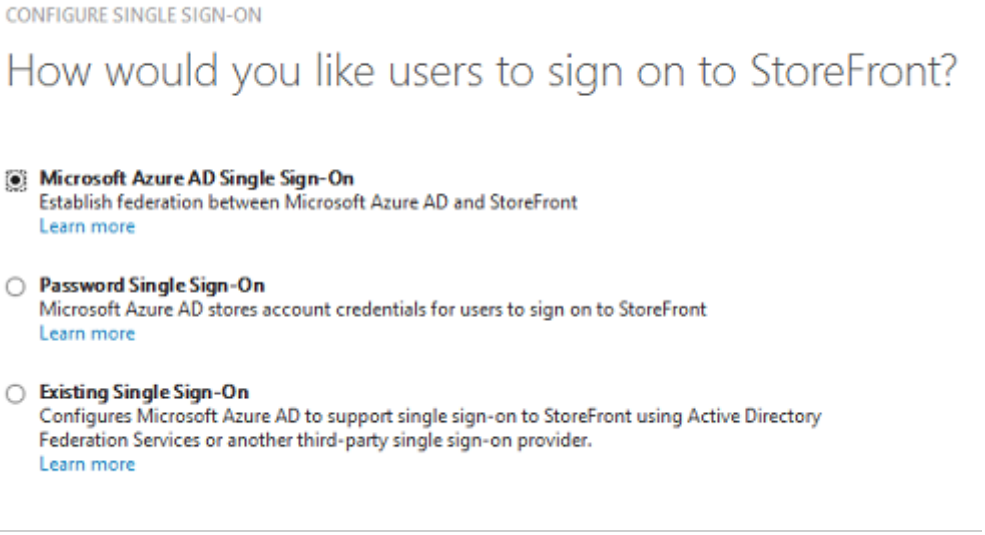
创建一个大小为 215 x 215 像素的图片并在“配置”页面上上载该图片以用作应用程序的图标。

配置 **SAML** 身份验证

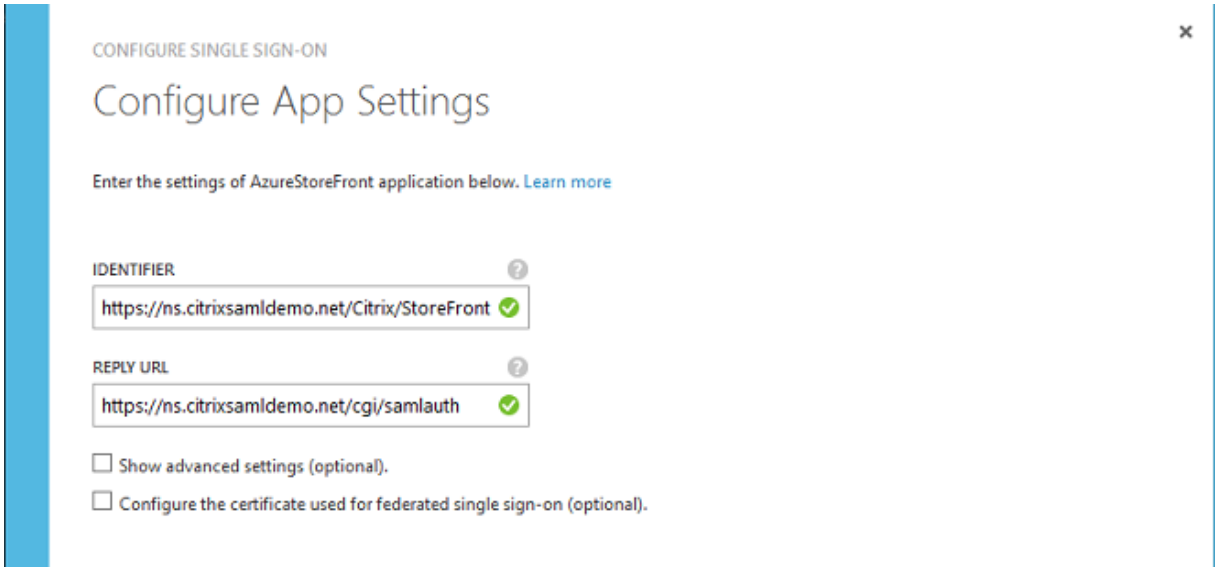
返回到“应用程序”控制板概览页面并选择配置单点登录。



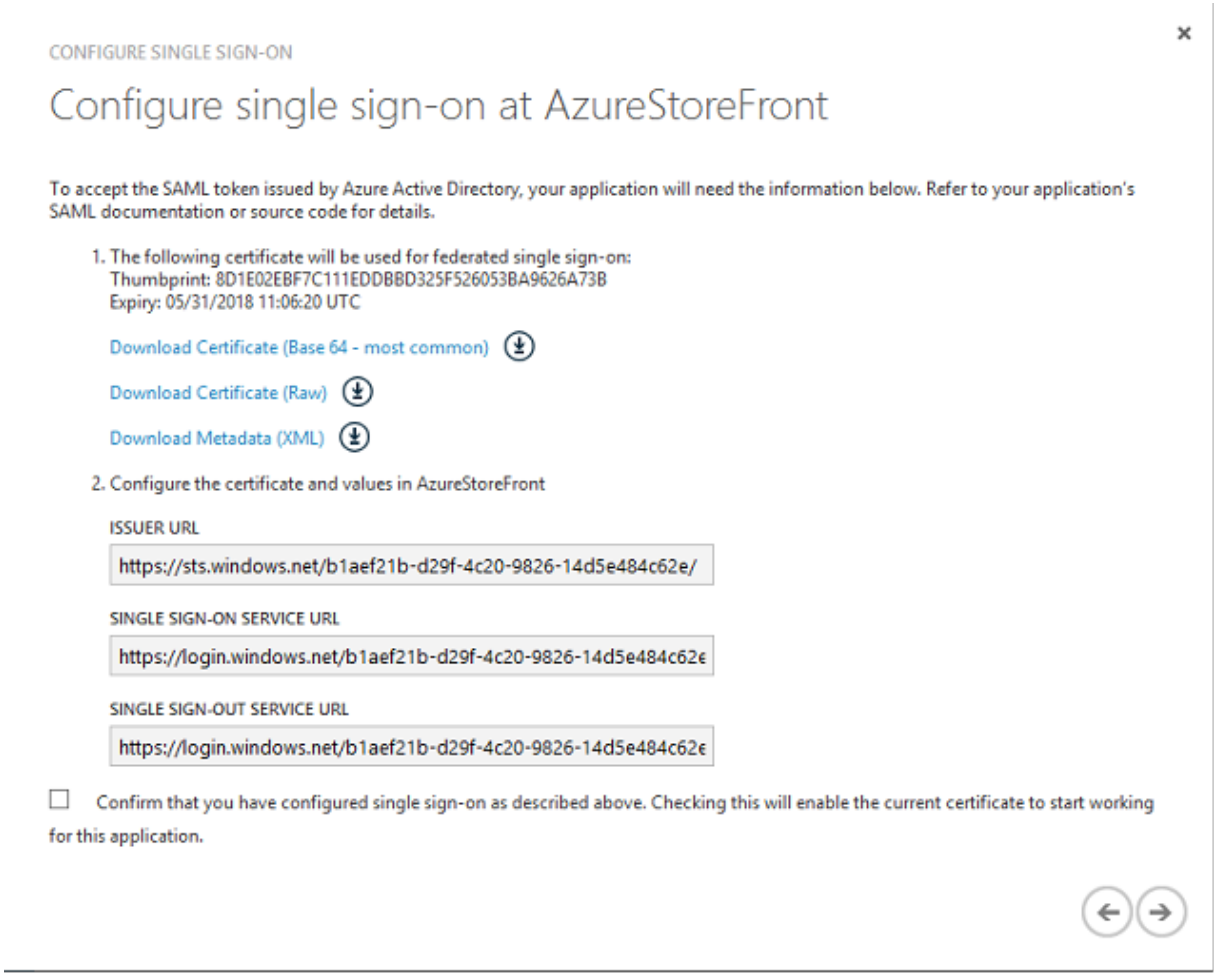
此部署将使用 SAML 2.0 身份验证，这与 **Microsoft Azure AD** 单点登录相对应。



标识符可以是任意字符串（必须与向 Citrix Gateway 提供的配置匹配）；在此示例中，答复 **URL** 在 Citrix Gateway 服务器上为 */cgi/samlauth*。



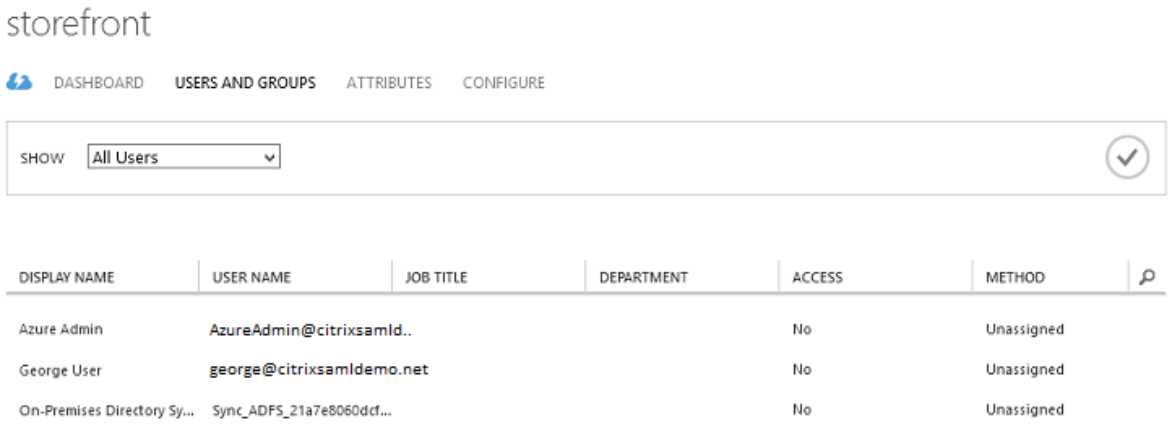
下一页中包含用于将 Citrix Gateway 配置为 Azure AD 信赖方的信息。



下载 Base 64 可信签名证书并复制登录和注销 URL。您稍后将在 Citrix Gateway 的配置屏幕中粘贴这些 URL。

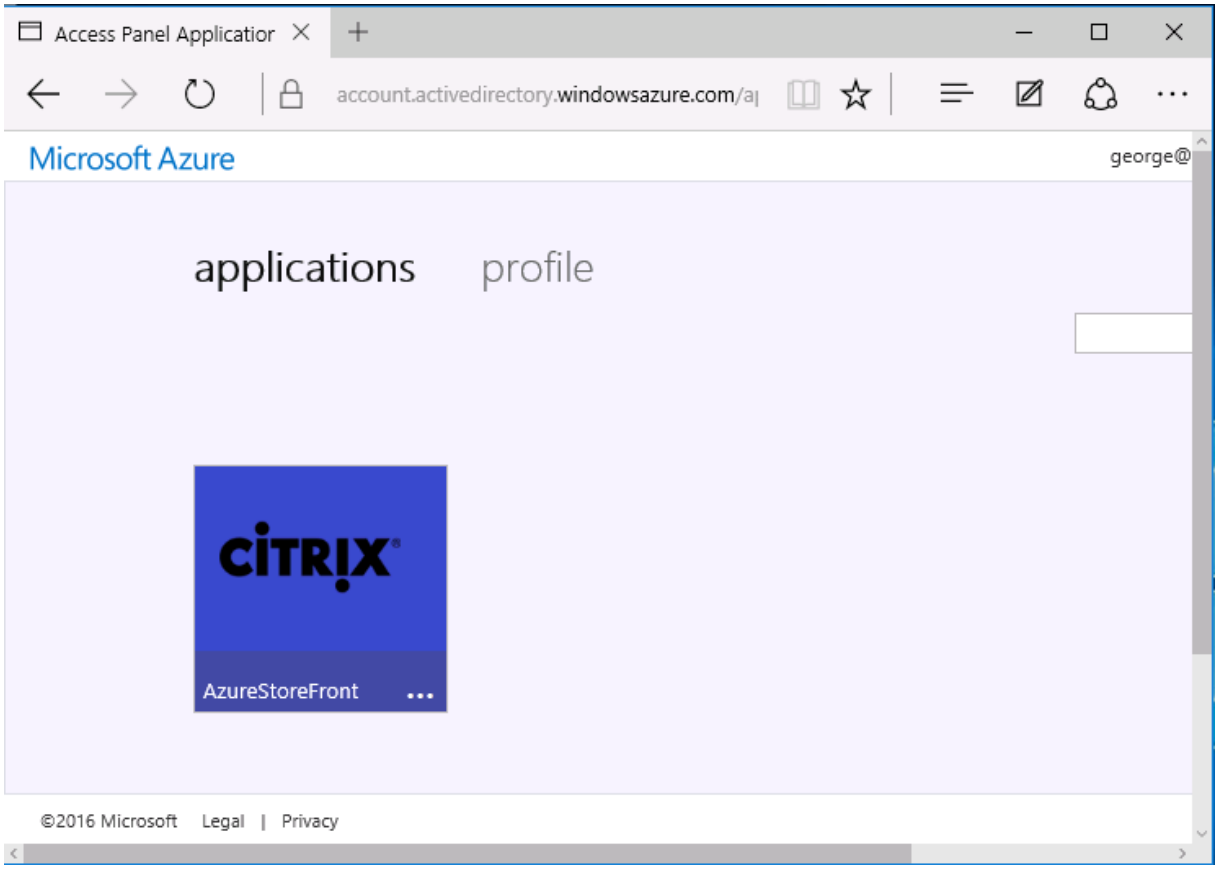
向用户分配应用程序

最后一个步骤为启用应用程序以使其在用户的 “myapps.microsoft.com” 控制页面上显示。此步骤在 “用户和组” 页面上完成。分配通过 Azure AD Connect 同步的域用户帐户的访问权限。也可以使用其他帐户，但必须明确映射这些帐户，因为它们不使用 <user>@<domain> 模式。



MyApps 页面

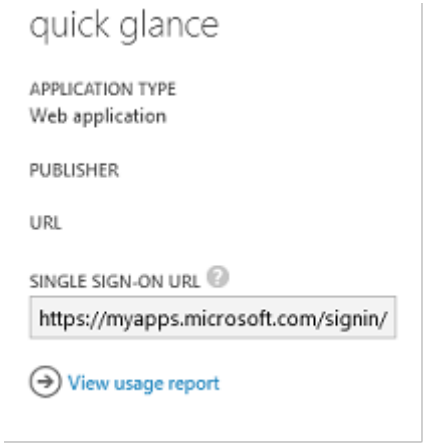
配置应用程序后，该应用程序将在用户访问 https://myapps.microsoft.com 时在用户的 Azure 应用程序列表中显示。



与 Azure AD 联接后，Windows 10 将支持登录用户单点登录到 Azure 应用程序。单击图标会将浏览器定向到之前配置的 SAML cgi/samlauth Web 页面。

单点登录 **URL**

返回到 Azure AD 控制板中的应用程序。现在有对应用程序可用的单点登录 URL。此 URL 用于提供 Web 浏览器链接或创建直接将用户定向到 StoreFront 的“开始”菜单快捷方式。



将此 URL 粘贴到 Web 浏览器中以确保 Azure AD 能够将您重定向到之前配置的 Citrix Gateway cgi/samlauth

Web 页面。这仅适用于已分配的用户，并且仅对联接了 Windows 10 Azure AD 的登录会话提供单点登录。（系统将提示其他用户输入 Azure AD 凭据。）

安装并配置 **Citrix Gateway**

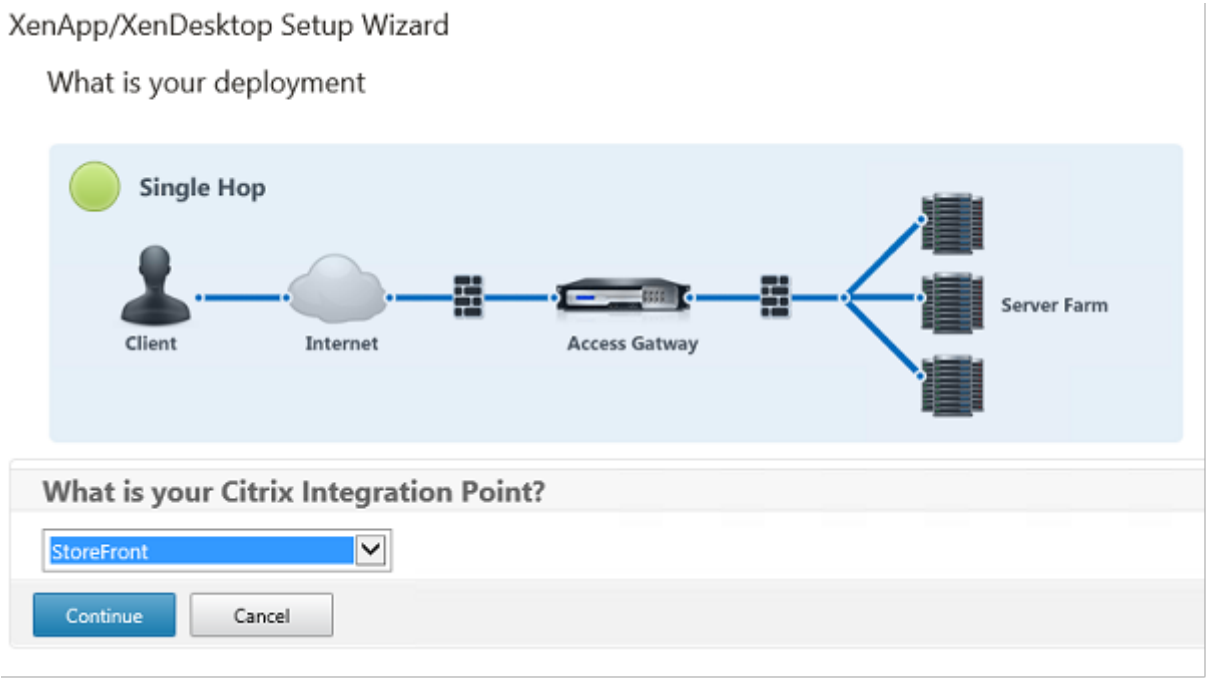
为远程访问部署，此示例使用运行 NetScaler（现在称为 Citrix Gateway）的独立 VM。可以从 Azure 应用商店购买。此示例使用 NetScaler 11.0 的“自带许可证”版本。

使用对用户进行身份验证时指定的凭据登录 NetScaler VM，从而将 Web 浏览器指向内部 IP 地址。请注意，必须在 Azure AD VM 中更改用户 nsroot 的密码。

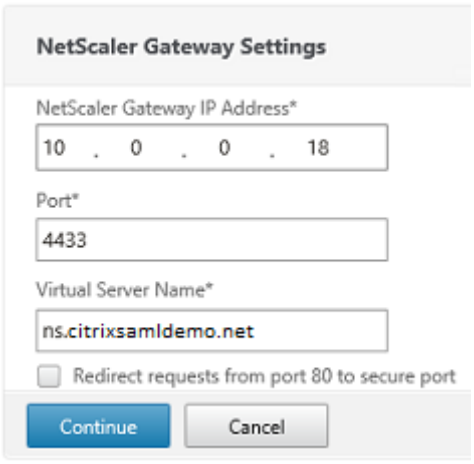
添加许可证，在添加每个许可证文件后选择重新启动，然后将 DNS 解析器指向 Microsoft 域控制器。

运行 **Citrix Virtual Apps and Desktops** 设置向导

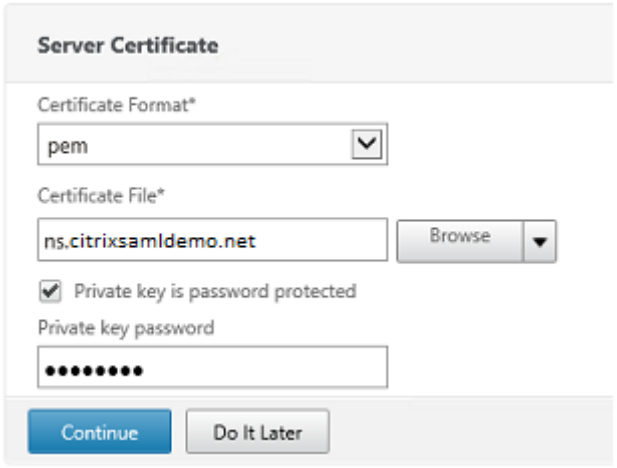
下例首先配置一个不带 SAML 的简单 StoreFront 集成。该部署运行后，将添加 SAML 登录策略。



选择标准 Citrix Gateway StoreFront 设置。此示例将配置端口 4433（而非端口 443），以在 Microsoft Azure 中使用。或者，您可以对 Citrix Gateway 管理 Web 站点进行端口转发或重新映射。

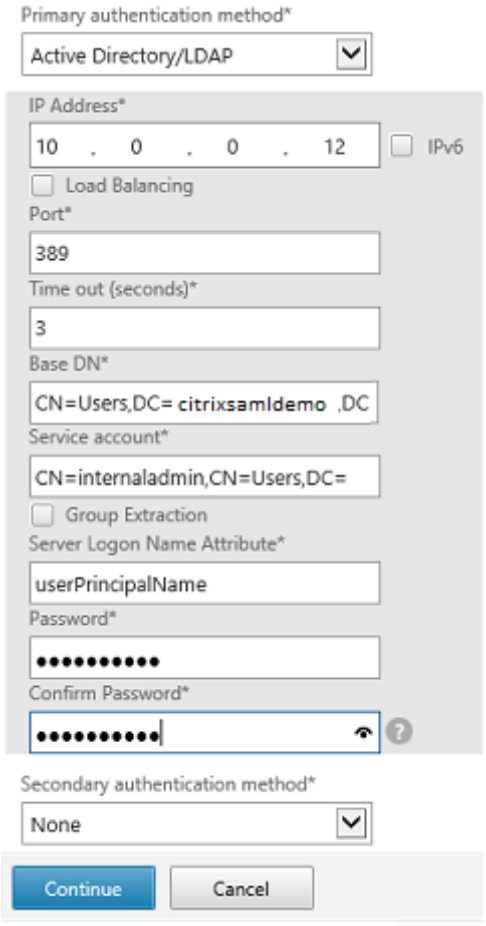


为简单起见，此示例将上载现有服务器证书以及存储在文件中的私钥。



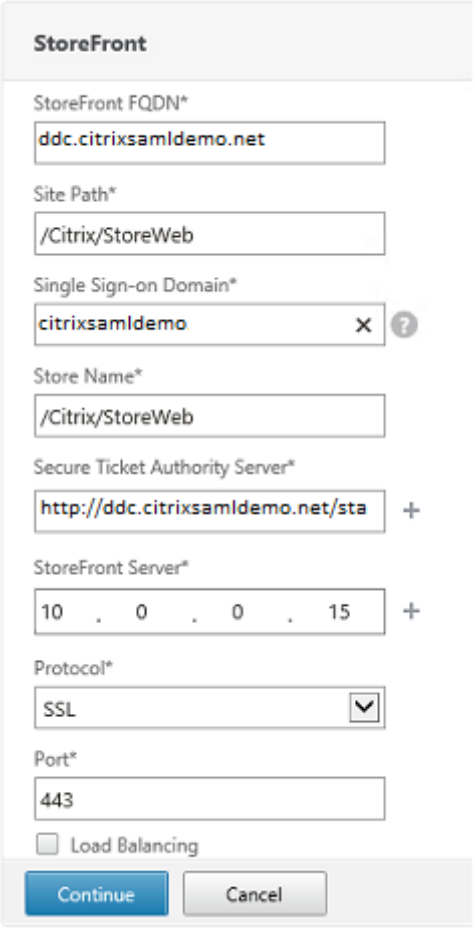
配置域控制器以便管理 **AD** 帐户

域控制器将用于帐户解析，因此，请将其 IP 地址添加到主身份验证方法中。记录对话框中每个字段要求的格式。



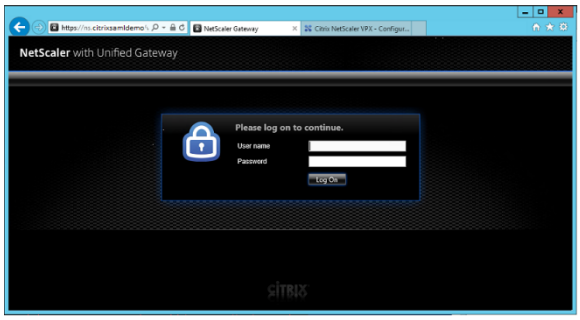
配置 **StoreFront** 地址

在此示例中，已使用 HTTPS 配置 StoreFront，因此，请选择 SSL 协议选项。



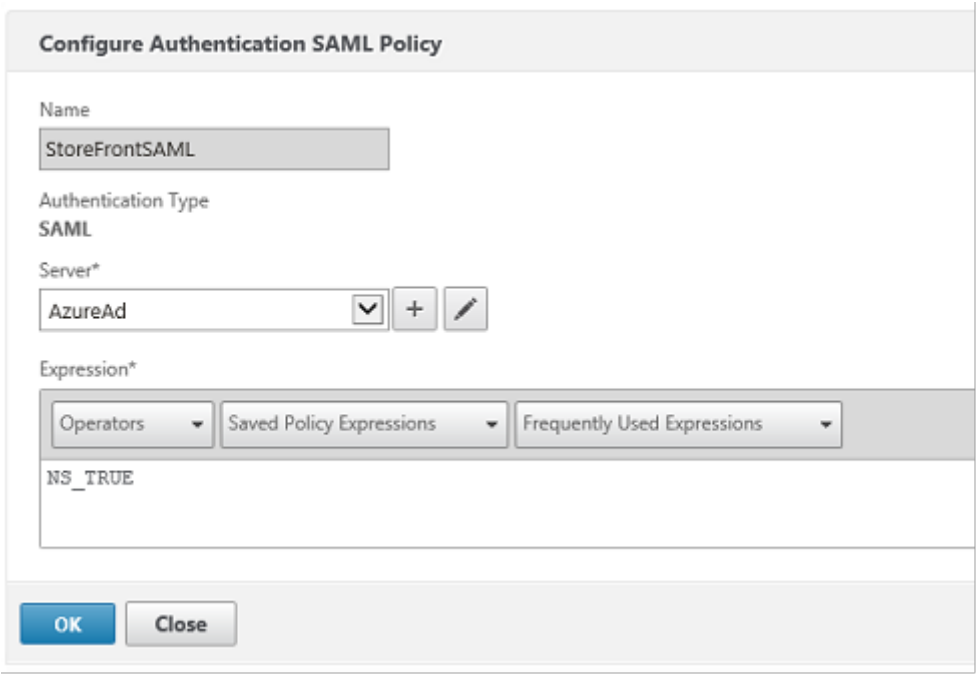
验证 **Citrix Gateway** 部署

使用用户名和密码连接到 Citrix Gateway 并检查身份验证和启动是否成功。

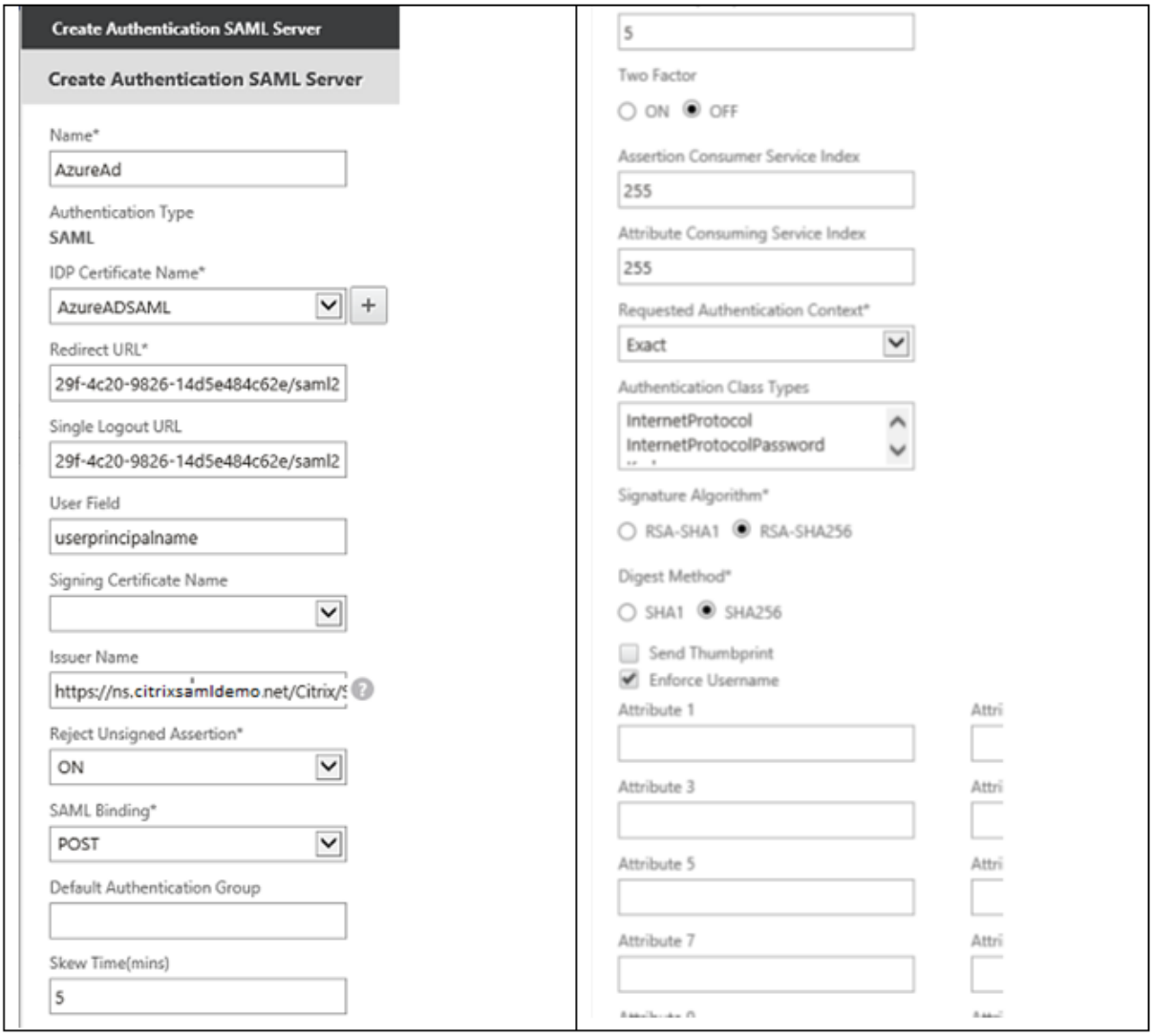


启用 **Citrix Gateway SAML** 身份验证支持

在 StoreFront 中使用 SAML 与在其他 Web 站点中使用 SAMl 类似。添加新的 SAML 策略，表达式为 **NS_TRUE**。



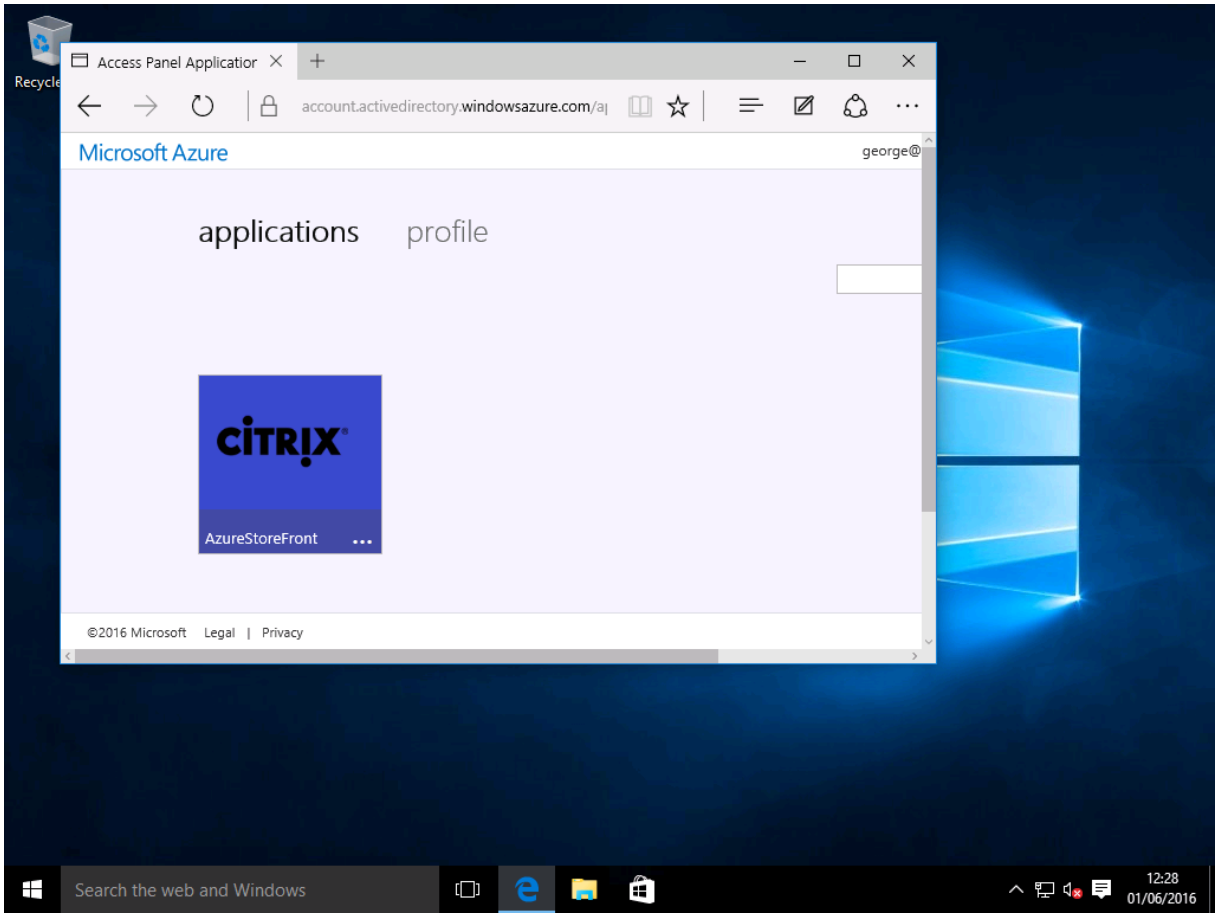
使用之前从 Azure AD 获取的信息配置新 SAML IdP 服务器。



验证端到端系统

使用在 Azure AD 中注册的帐户登录到加入了 Azure AD 的 Windows 10 桌面。启动 Microsoft Edge 并连接到：https://myapps.microsoft.com。

Web 浏览器应为用户显示 Azure AD 应用程序。



验证单击图标是否会将您重定向到通过身份验证的 StoreFront 服务器。

同样，请验证使用单点登录 URL 的直接连接以及与 Citrix Gateway 站点的直接连接是否会将您重定向到 Microsoft Azure 并返回。

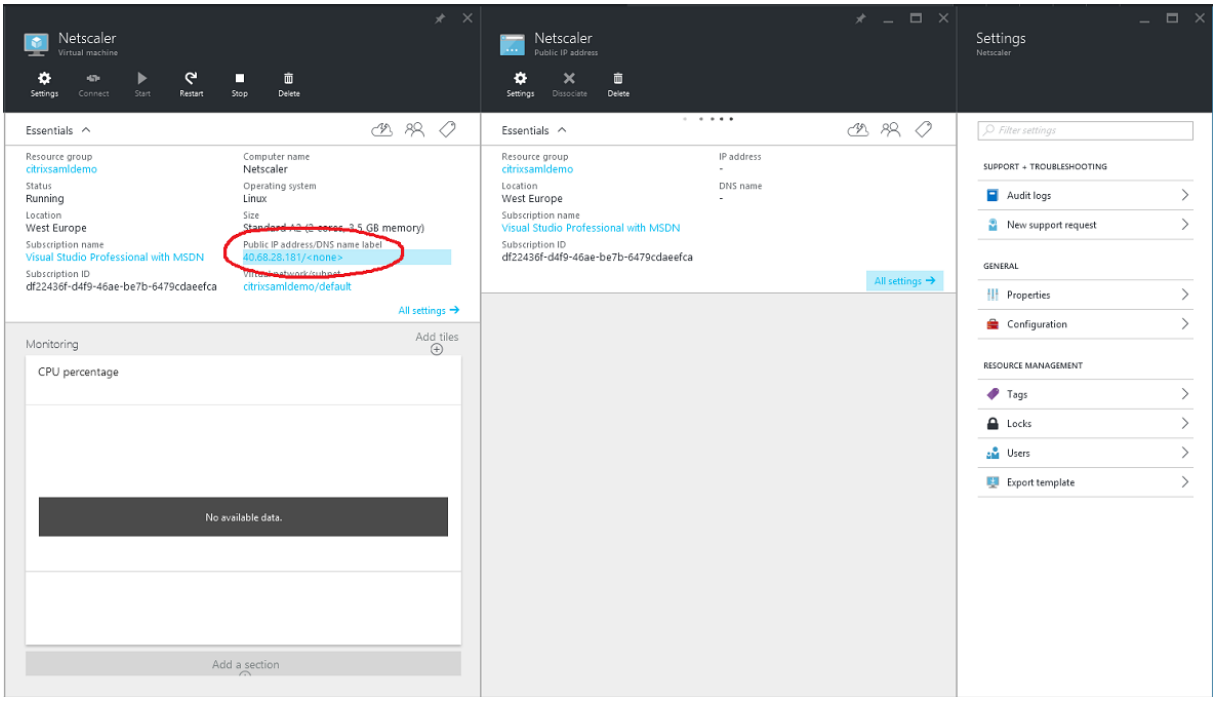
最后，验证未加入 Azure AD 的计算机是否也能通过相同的 URL 运行（尽管会有一次显式登录到 Azure AD 以建立初始连接）。

附录

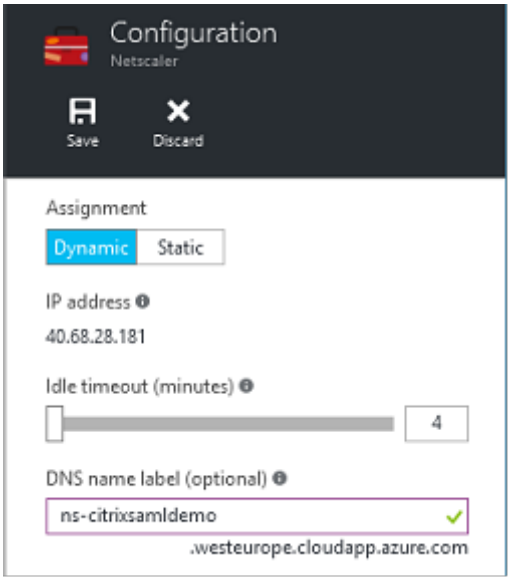
在 Azure 中设置 VM 时，应该配置以下标准选项。

提供公用 **IP** 地址和 **DNS** 地址

Azure 在内部子网中向所有 VM 提供 IP 地址（在此示例中为 10.*.*.*）。默认情况下，还会提供公用 IP 地址，该地址可以被动态更新的 DNS 标签引用。



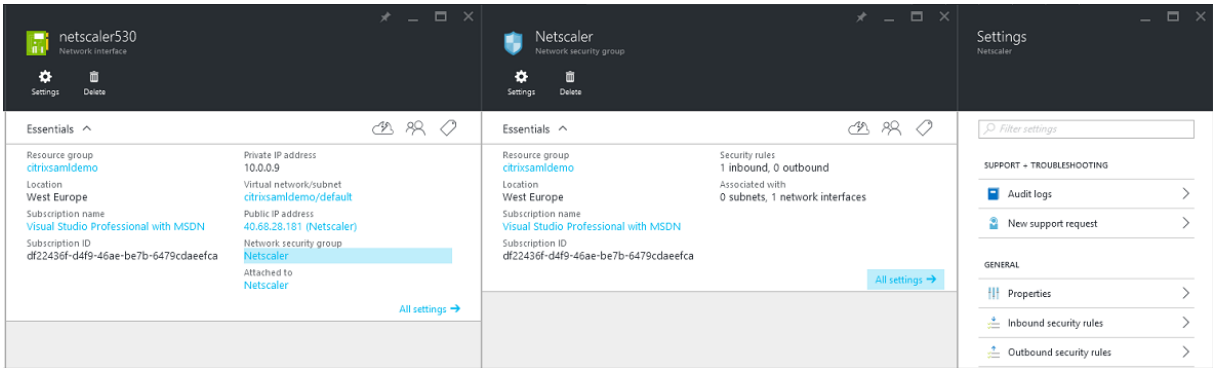
选择公用 **IP** 地址/**DNS** 名称标签的配置。为 VM 选择一个公用 DNS 地址。此地址可用于其他 DNS 区域文件中的 CNAME 引用，以确保即使重新分配了 IP 地址，所有 DNS 记录仍始终正确地指向该 VM。



设置防火墙规则（安全组）

云中的每个 VM 都将自动应用一组防火墙规则，称为安全组。安全组控制从公用 IP 地址转发到专用 IP 地址的流量。默认情况下，Azure 允许将 RDP 转发到所有 VM。Citrix Gateway 和 ADFS 服务器还需要转发 TLS 流量 (443)。

打开 VM 的网络接口，然后单击网络安全组标签。配置入站安全规则以允许传输相应的网络流量。



相关信息

- 安装和配置是 FAS 安装和配置的主要参考资料。
- 部署体系结构一文总结了常见的 FAS 部署。
- 高级配置一文中介绍了“操作方法”文章。

高级配置

September 27, 2019

本部分中的“操作方法”文章提供了联合身份验证服务 (FAS) 的高级配置和管理指导。

相关信息

- FAS 的安装和初始设置的主要参考资料为安装和配置一文。
- 部署体系结构一文总结了主要的 FAS 体系结构，并提供了指向与更复杂的体系结构有关的其他文章的链接。

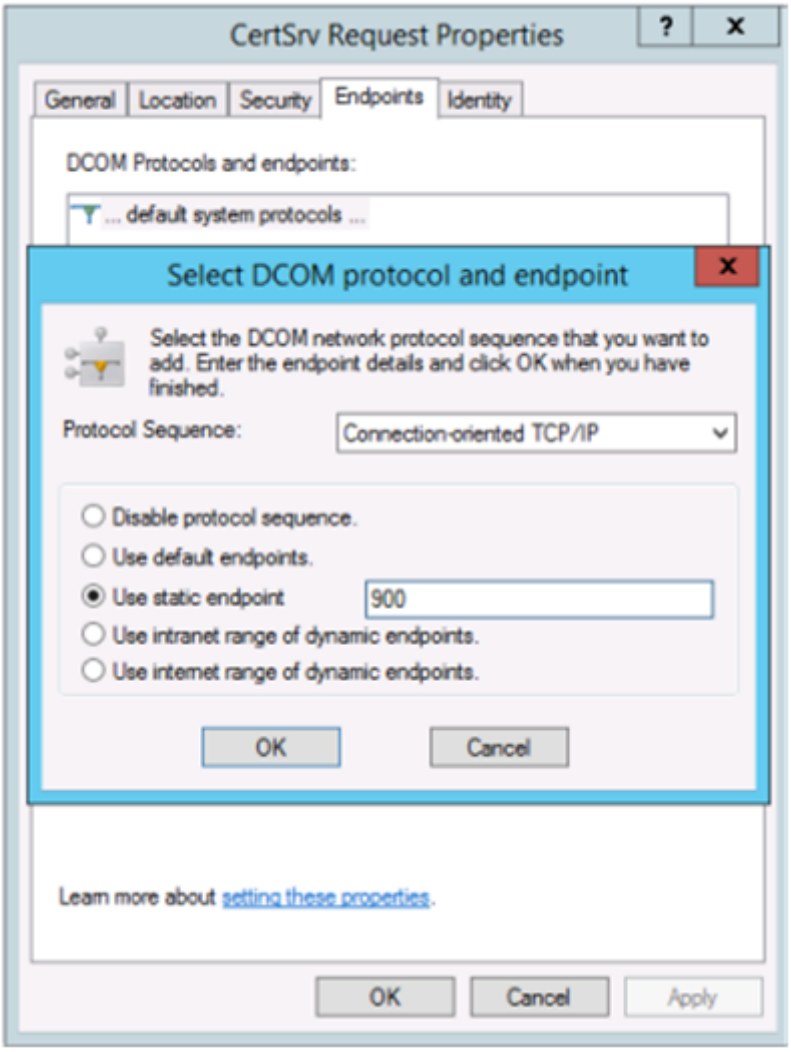
证书颁发机构配置

November 7, 2019

本文介绍联合身份验证服务 (FAS) 的高级配置，以便与不受 FAS 管理控制台支持的证书颁发机构服务器集成。这些说明信息将采用 FAS 所提供的 PowerShell API。在执行本文中的任何说明之前，您应具有 PowerShell 基础知识。

配置 **Microsoft** 证书颁发机构以进行 **TCP** 访问

默认情况下，Microsoft 证书颁发机构使用 DCOM 进行访问。这会导致需在实现防火墙安全功能时执行复杂的操作，因此，Microsoft 提供了一个预配项，可用于切换到静态 TCP 端口。在 Microsoft 证书颁发机构中，打开 DCOM 配置面板并编辑 “CertSrv Request”DCOM 应用程序的属性：



更改 “端点” 以选择静态端点，并指定 TCP 端口号（在上图中为 900）。

重新启动 Microsoft 证书颁发机构并提交证书申请。如果您运行 `netstat -a -n -b`，应该会看到 certsvr 在侦听端口 900：

```
 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
```


无需配置 FAS 服务器（或任何其他正在使用证书颁发机构的计算机），因为 DCOM 具有一个将通过 RPC 端口进行的协商阶段。当客户端需要使用 DCOM 时，它连接到证书服务器上的 DCOM RPC Service，并请求访问特定的 DCOM 服务器。这会导致打开端口 900，并且 DCOM 服务器会指示 FAS 服务器如何进行连接。

预生成用户证书

当在 FAS 服务器中预生成用户证书时，将显著缩短用户的登录时间。以下各节描述如何为单个或多个 FAS 服务器完成此操作。

获取 **Active Directory** 用户的列表

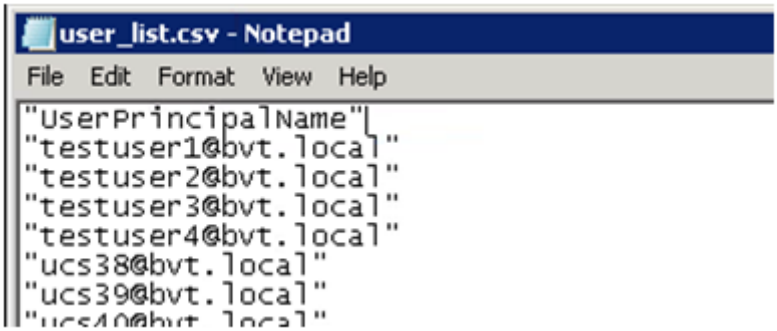
可以通过查询 AD 并将用户列表存储到文件（例如.csv 文件）来改进证书生成过程，如下面的示例所示。

```
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 是一个用于查询用户列表的标准 cmdlet。以上示例中包含一个 filter 参数以便只列出名称为 UserPrincipalName 且帐户状态为 “已启用” 的用户。

SearchBase 参数将缩小在其中搜索用户的 AD 部分。如果要包括 AD 中的所有用户，可省略此项。注意：此查询可能会返回大量用户。

CSV 类似于如下所示：



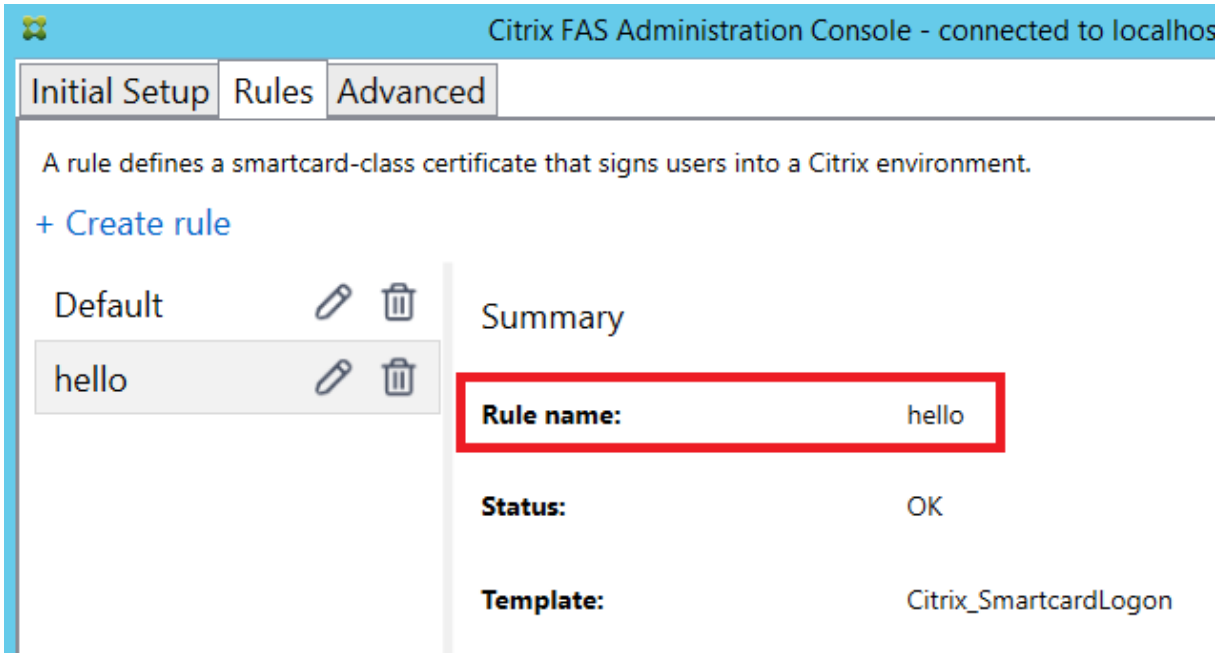
FAS 服务器

下面的 PowerShell 脚本采用以前生成的用户列表，并创建用户证书的列表。

```
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
     }

 }
```

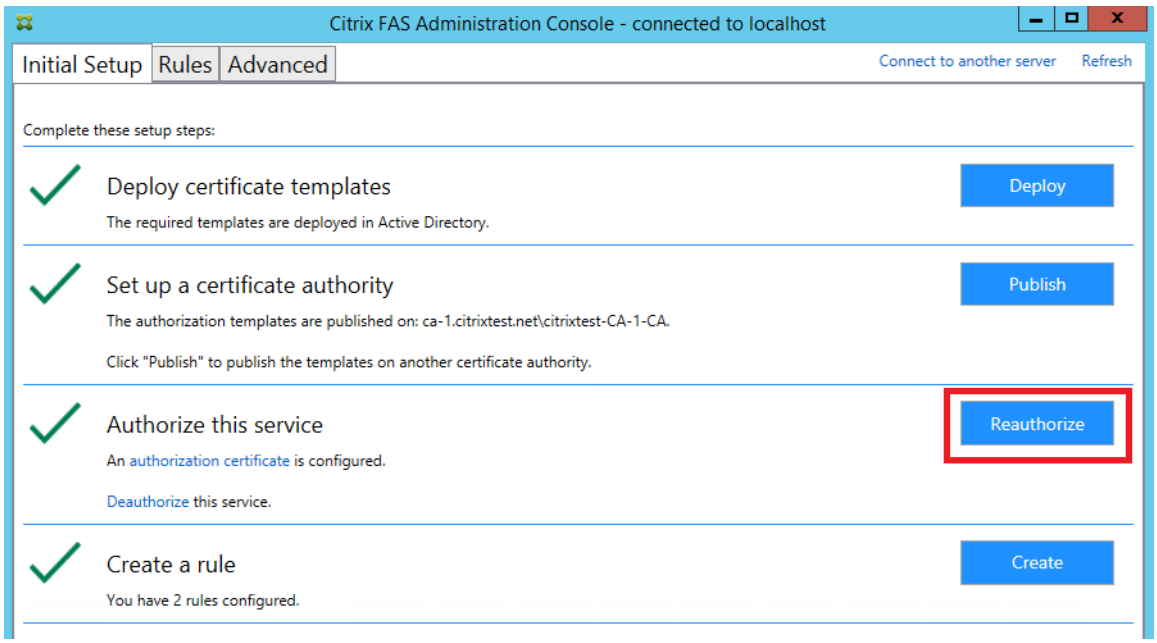
如果您具有多个 FAS 服务器，则将生成特定用户证书两次：一次在主服务器上生成，一次在故障转移服务器上生成。

以上脚本针对一个名为 “default” 的规则。如果您具有不同的规则名称（例如 “hello”），则只需更改脚本中的 $rule 变量。



更新注册机构证书

如果正在使用多个 FAS 服务器，则可以续订 FAS 授权证书而不会影响已登录的用户。

> 注意：
>
> 也可以使用 GUI 重新授权 FAS：
>
> 
>

请完成以下操作过程：

1. 创建新授权证书：`New-FasAuthorizationCertificate`

2. 记录由以下命令返回的新授权证书的 GUID：`Get-FasAuthorizationCertificate`
3. 使 FAS 服务器进入维护模式：`Set-FasServer -Address <FAS server> -MaintenanceMode $true`
4. 更换新授权证书：`Set-FasCertificateDefinition -AuthorizationCertificate <GUID>`
5. 使 FAS 服务器退出维护模式：`Set-FasServer -Address <FAS server> -MaintenanceMode $false`
6. 删除旧授权证书：`Remove-FasAuthorizationCertificate`

相关信息

- 安装和配置一文是 FAS 安装和配置的主要参考资料。
- 通用联合身份验证服务部署在部署体系结构一文中加以概述。
- 高级配置一文中介绍了其他“操作方法”文章。

私钥保护

November 7, 2019

简介

默认情况下，将通过网络服务帐户方式存储私钥并将其标记为不可导出。

有两种类型的私钥：

- 与注册机构证书关联的私钥（来自 Citrix_RegistrationAuthority 证书模板）。
- 与用户证书关联的私钥（来自 Citrix_SmartcardLogon 证书模板）。

实际上有两个注册机构证书：Citrix_RegistrationAuthority_ManualAuthorization（默认有效期为 24 小时）及 Citrix_RegistrationAuthority（默认有效期为两年）。

在联合身份验证服务 (FAS) 管理控制台中的初始设置选项卡的步骤 3 中，单击授权时，FAS 服务器会生成一个密钥对，并向证书颁发机构发送针对 Citrix_RegistrationAuthority_ManualAuthorization 证书的证书签名请求。这是一个临时证书，默认有效期为 24 小时。证书颁发机构不会自动颁发此证书；必须在证书颁发机构上由管理员手动授权颁发此证书。一旦向 FAS 服务器颁发证书，FAS 将使用 Citrix_RegistrationAuthority_ManualAuthorization 证书自动获取 Citrix_RegistrationAuthority 证书（默认有效期为两年）。一旦 Citrix_RegistrationAuthority_ManualAuthorization 获得 Citrix_RegistrationAuthority 证书，FAS 服务器将删除它的证书和密钥。

与注册机构证书关联的私钥特别敏感，因为注册机构证书策略允许任何拥有私钥的人员为在模板中配置的用户集颁发证书请求。因此，控制了此密钥的任何人都可作为用户集中的任何用户连接到环境。

可以通过使用下列项之一配置 FAS 服务器，以便按符合您所在组织的安全要求的方法保护私钥：

- 同时针对注册机构证书和用户证书私钥的 Microsoft 增强 RSA 和 AES 加密提供程序或 Microsoft 软件密钥存储提供程序。
- 针对注册机构证书的私钥的含受信任的平台模块 (TPM) 芯片的 Microsoft 平台密钥存储提供程序，以及针对用户证书私钥的 Microsoft 增强 RSA 和 AES 加密提供程序或 Microsoft 软件密钥存储提供程序。
- 同时针对注册机构证书和用户证书私钥的硬件安全模块 (HSM) 供应商的加密服务或密钥存储提供程序与 HSM 设备。

私钥配置设置

配置 FAS 以使用下列三个选项之一。使用文本编辑器编辑 Citrix.Authentication.FederatedAuthenticationService.exe.config 文件。该文件默认情况下位于 FAS 服务器上的 Files\Citrix\Federated Authentication Service 文件夹中。

```
<?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>
```

仅当服务启动时，FAS 才会读取此配置文件。如果更改了任何值，必须重新启动 FAS 才能反映新的设置。

按如下所示设置 Citrix.Authentication.FederatedAuthenticationService.exe.config 文件中的相关值：

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp**（在 CAPI 与 CNG API 之间切换）

值	备注
true	使用 CAPI API
false（默认）	使用 CNG API

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName**（要使用的提供程序的名称）

值	备注
Microsoft 增强 RSA 和 AES 加密提供程序	默认 CAPI 提供程序
Microsoft 软件密钥存储提供程序	默认 CNG 提供程序
Microsoft 平台密钥存储提供程序	默认 TPM 提供程序。请注意，建议不要将 TPM 用于用户密钥。仅将 TPM 用于注册机构密钥。如果计划在虚拟化环境中运行 FAS 服务器，请咨询您的 TPM 和虚拟机管理程序供应商以确认是否支持虚拟化。
HSM_Vendor CSP/密钥存储提供程序	由 HSM 供应商提供。对于不同的供应商，该值有所不同。如果您计划在虚拟化环境中运行 FAS 服务器，请咨询您的 HSM 供应商以确认是否支持虚拟化。

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType**（仅在使用 CAPI API 时需要）

值	备注
24	默认。请参阅 Microsoft KeyContainerPermission-AccessEntry.ProviderType Property PROV_RSA_AES 24。应该始终为 24，除非您使用 CAPI 与 HSM 并且 HSM 提供商另有规定。

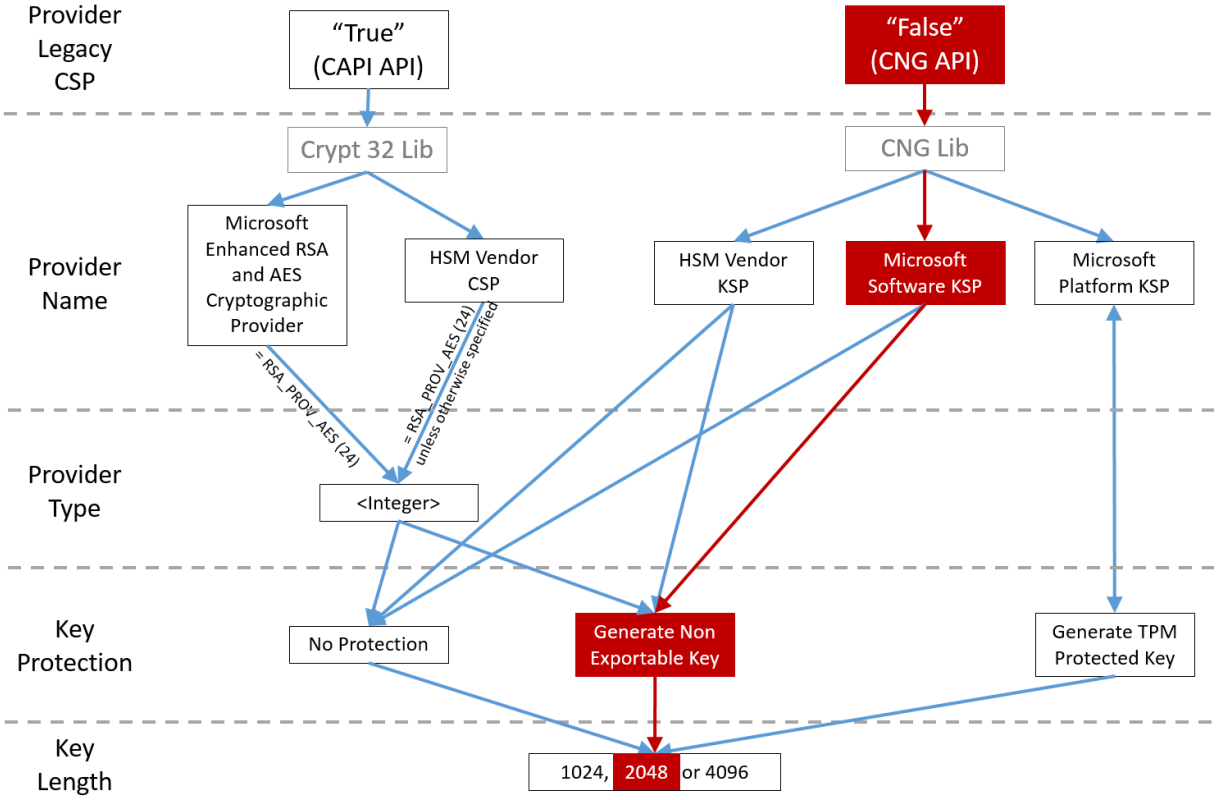
Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection**（当 FAS 需要执行私钥操作时，将使用在此处指定的值）控制私钥的 “exportable” 标志。允许使用 TPM 密钥存储（如果硬件支持）。

值	备注
NoProtection	可以导出私钥。
GenerateNonExportableKey	默认。无法导出私钥。
GenerateTPMProtectedKey	将使用 TPM 管理私钥。通过您在 ProviderName 中指定的 ProviderName（例如 Microsoft 平台密钥存储提供程序）存储私钥

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength**（指定私钥的大小，单位为位）

值	备注
2048	默认值。也可以使用 1024 或 4096。

下方以图形方式显示了该配置文件的设置（默认安装设置显示为红色）：



配置方案示例

示例 **1**

此示例介绍通过使用 Microsoft 软件密钥存储提供程序存储的注册机构证书私钥和用户证书私钥

这是默认的安装后配置。无需进行其他私钥配置。

示例 **2**

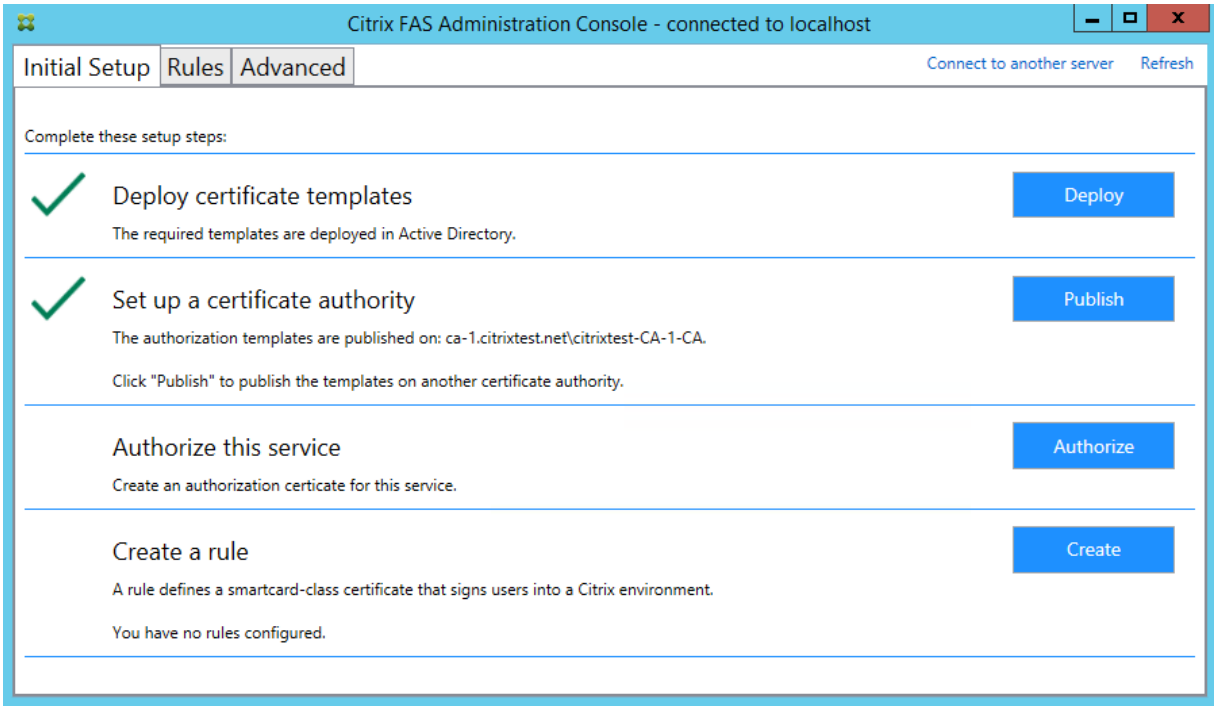
此示例介绍通过 Microsoft 平台密钥存储提供程序存储在 FAS 服务器主板的硬件 TPM 中的注册机构证书私钥，以及通过 Microsoft 软件密钥存储提供程序存储的用户证书私钥。

此方案假设您已根据 TPM 制造商文档在 BIOS 中启用 FAS 服务器主板上的 TPM，并已在 Windows 中初始化 TPM；请参阅 https://technet.microsoft.com/en-gb/library/cc749022(v=ws.10).aspx。

使用 **PowerShell**（建议）

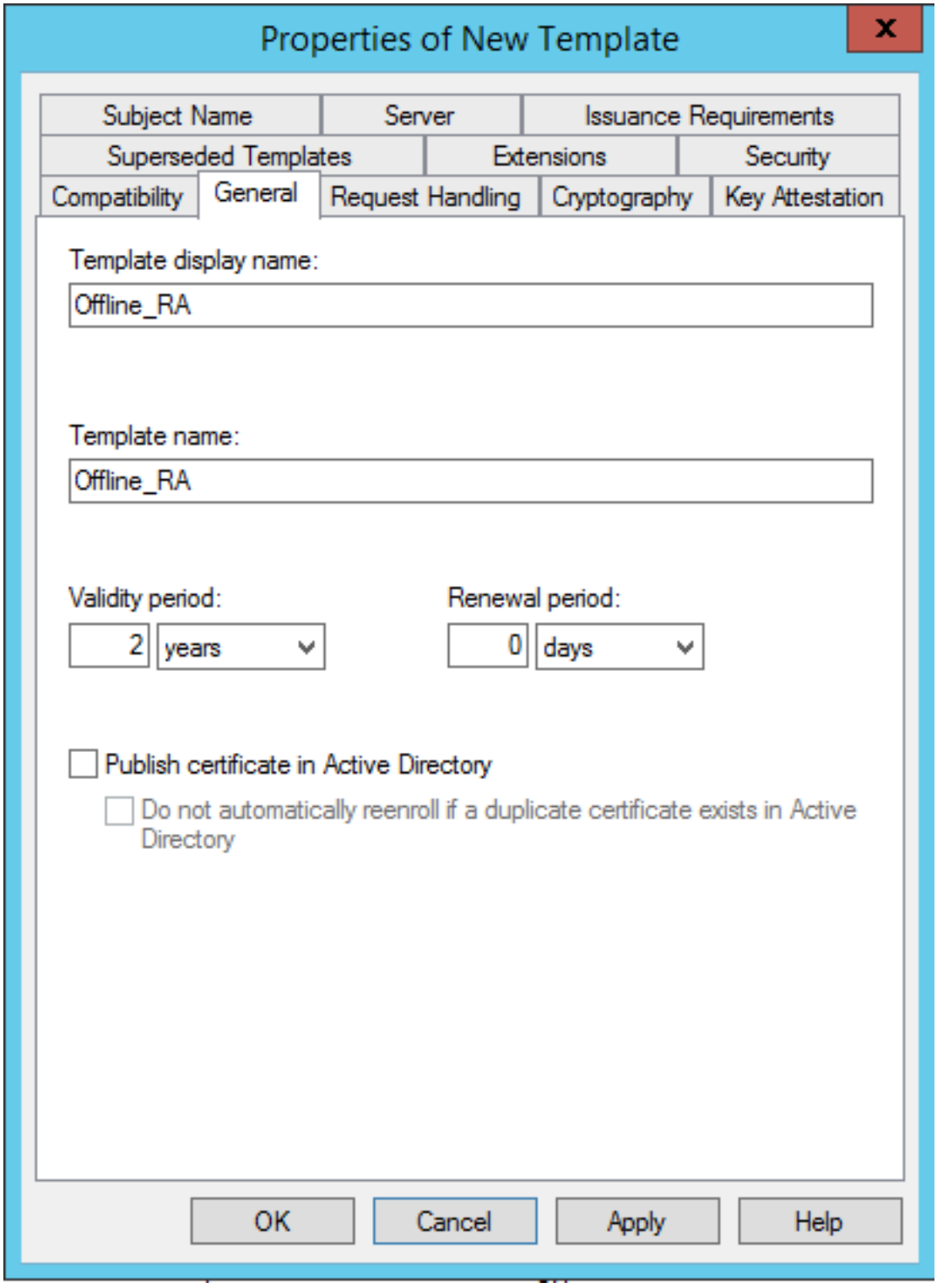
可使用 PowerShell 以脱机方式请求注册机构证书。对于不希望其证书颁发机构通过联机证书签名请求颁发注册机构证书的组织，建议执行此操作。无法使用 FAS 管理控制台发出脱机注册机构证书签名请求。

步骤 **1**：在使用管理控制台执行初始 FAS 配置期间，请仅完成前两个步骤：“部署证书模板”和“设置证书颁发机构”。



步骤 **2**：在证书颁发机构服务器中，添加证书模板 MMC 管理单元。右键单击 **Citrix_RegistrationAuthority_ManualAuthorizati** 模板并选择复制模板。

选择 **General**（常规）选项卡。更改名称和有效期。在此示例中，名称是 *Offline_RA*，有效期为 2 年：



步骤 **3**：在证书颁发机构服务器上，添加证书颁发机构 MMC 管理单元。右键单击 **Certificate Templates**（证书模板）。选择 **New**（新建），然后单击 **Certificate Template to Issue**（要颁发证书模板）。选择刚才创建的模板。

步骤 **4**：在 FAS 服务器中加载以下 PowerShell cmdlet：


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

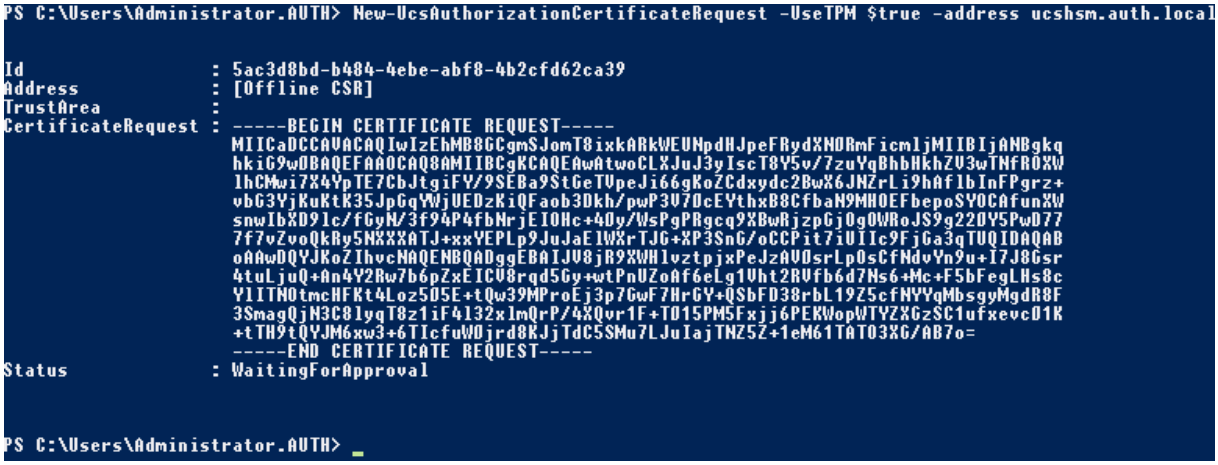
步骤 **5**：在 FAS 服务器的 TPM 内部生成 RSA 密钥，并通过在 FAS 服务器上输入以下 PowerShell cmdlet 来创建证书签名请求。注意：有些 TPM 会限制密钥长度。默认密钥长度为 2048 位。请务必指定受硬件支持的密钥长度。

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address \<FAS 服务器的 FQDN>
```

例如：

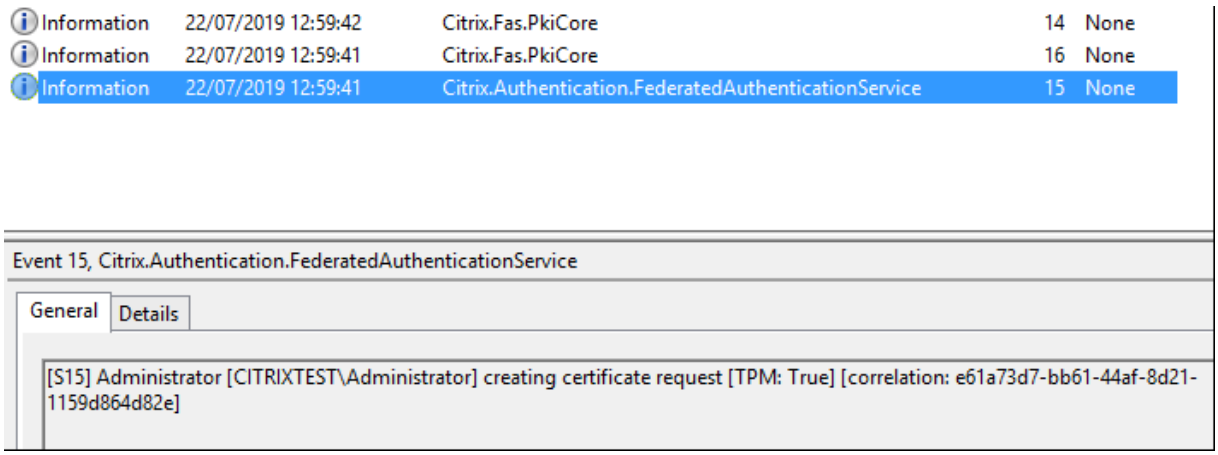
```
New-FasAuthorizationCertificateRequest -UseTPM $true -address fashsm.auth.net
```

将显示以下内容：



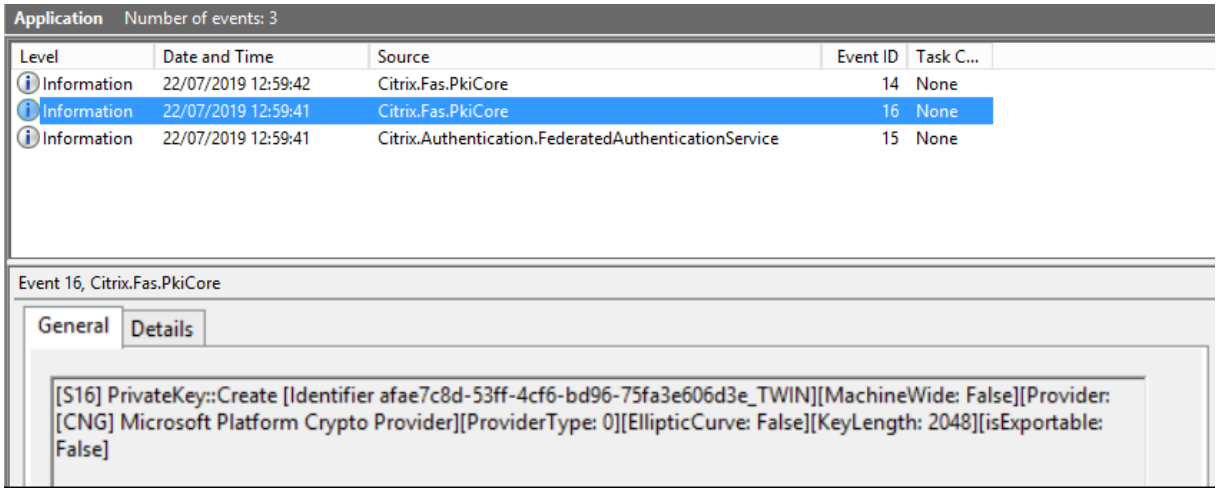
> 注意：
>
> - 在后续步骤中，必须使用 Id GUID（在此示例中为 “5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39”）。
> - 将此 PowerShell cmdlet 视为一次性的 “覆盖”，用于生成注册机构证书的私钥。
> - 当运行此 cmdlet 时，将检查在 FAS 启动时从配置文件读取的值，以确定要使用的密钥长度（默认为 2048）。
> - 由于在此手动 PowerShell 发起的注册机构证书私钥操作时会将 -UseTPM 设置为 $true，因此系统将忽略文件中与使用 TPM 时所需设置不匹配的值。
> - 运行此 cmdlet 不会更改配置文件中的任何设置。
> - 在随后的自动 FAS 发起的用户证书私钥操作中，将使用在启动 FAS 时从此文件读取的值。
> - 此外，当 FAS 服务器颁发用户证书以生成受 TPM 保护的用户证书私钥时，也可以在此配置文件中将 KeyProtection 值设置为 GenerateTPMProtectedKey。

要验证用于生成密钥对的 TPM，请在生成密钥对时，在 FAS 服务器上的 Windows 事件查看器中查看应用程序日志。



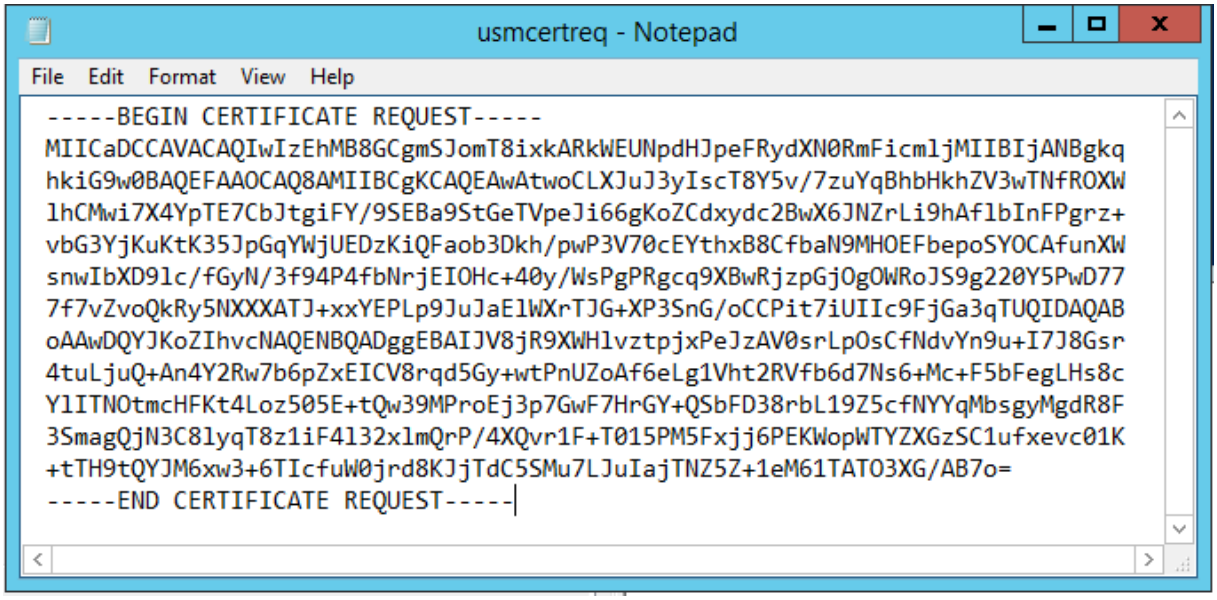
注意： [TPM：True]

后跟：



注意： 提供程序：[CNG] Microsoft 平台加密提供程序

步骤 **6**：将证书请求部分复制到文本编辑器，并将其保存为磁盘上的文本文件。



步骤 **7**：通过在 FAS 服务器上的 PowerShell 中键入以下命令将证书签名请求提交到证书颁发机构：

```
certreq -submit -attrib "certificatetemplate:\<步骤 2 中的证书模板>" \<
    步骤 6 中的证书请求文件>
```

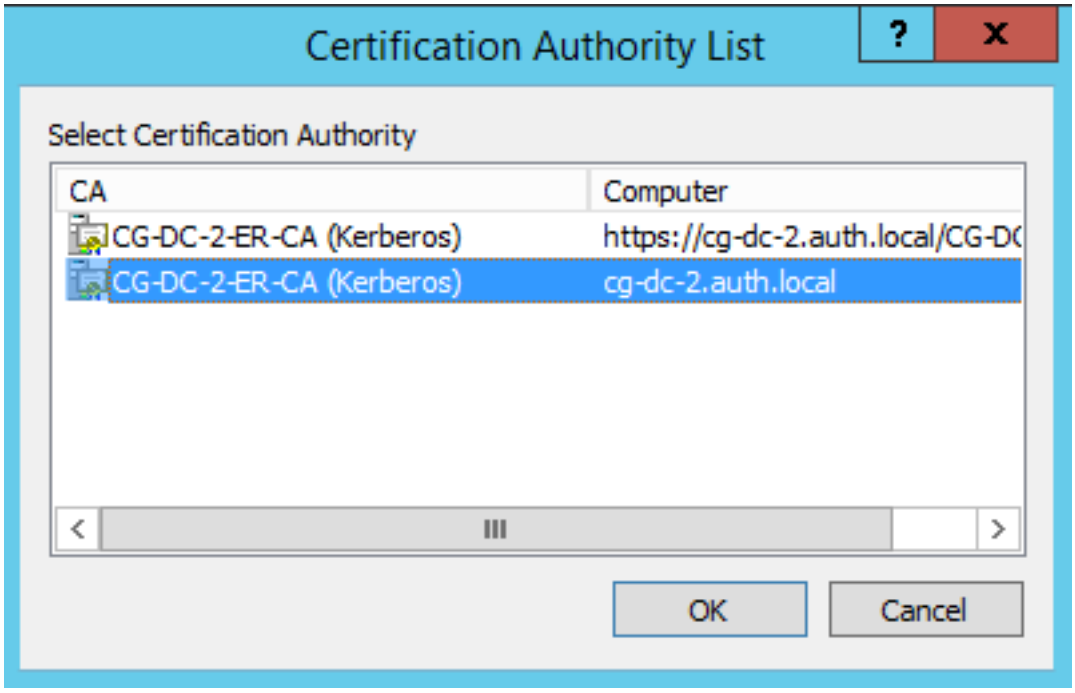
例如：

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

将显示以下内容：

```
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:
```

此时，可能会出现“Certification Authority List”（证书颁发机构列表）窗口。此示例中的证书颁发机构已同时启用 HTTP（顶部）和 DCOM（底部）注册。选择 DCOM 选项（如果有）：

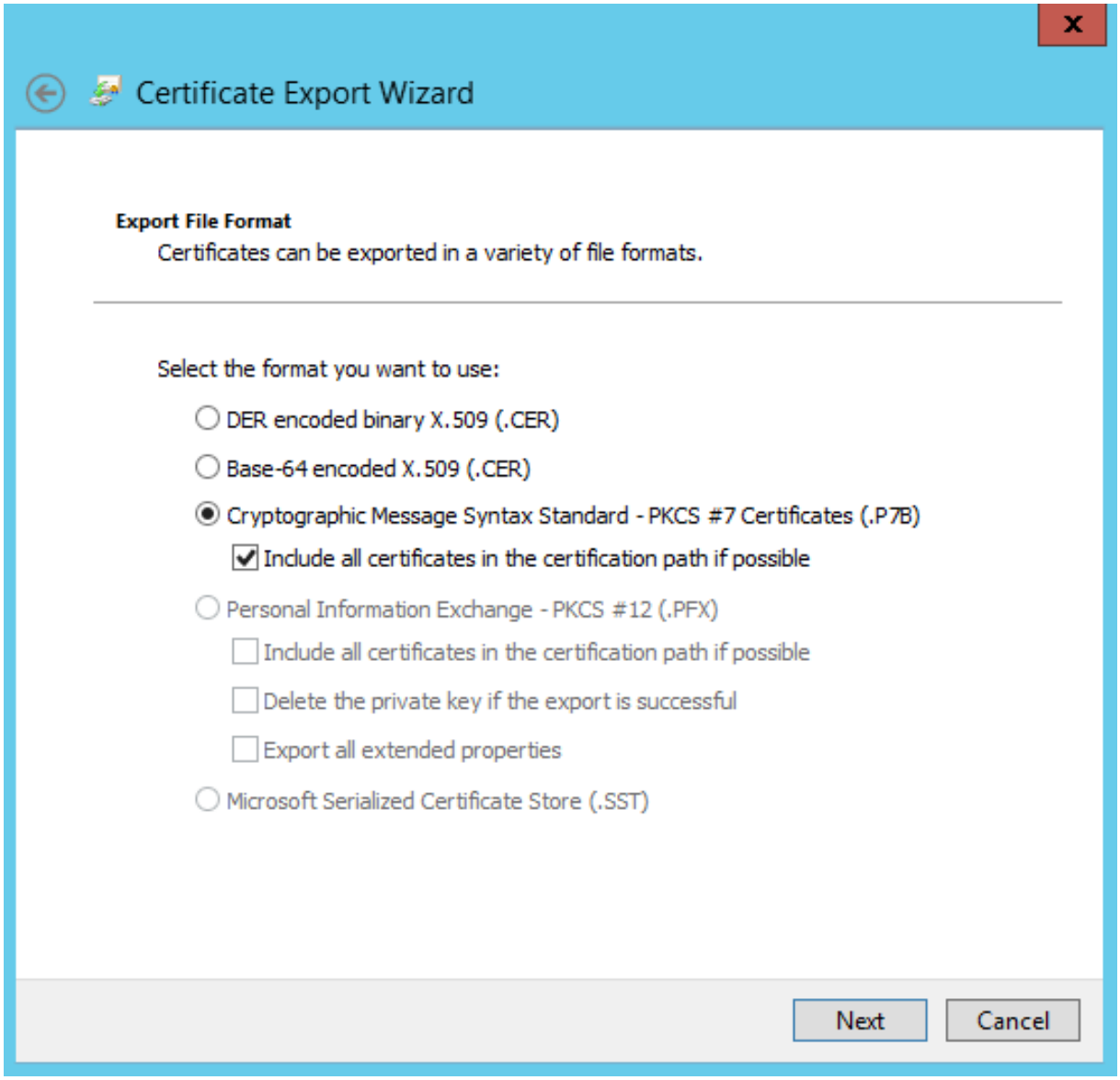


在指定证书颁发机构后，PowerShell 将显示 RequestID：

```
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>
```

步骤 **8**：在证书颁发机构服务器上的证书颁发机构 MMC 管理单元中，单击待处理的请求。记录请求 ID。然后右键单击该请求，并选择 **Issue**（颁发）。

步骤 **9**：选择 **Issued Certificates**（已颁发的证书节点）。找到刚颁发的证书（请求 ID 应匹配）。双击以打开证书。选择 **Details**（详细信息）选项卡。单击 **Copy to File**（复制到文件）。将启动“证书导出向导”。单击下一步。为文件格式选择下列选项：



格式必须是 “**Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)**”，并且必须选中 “**Include all certificates in the certification path if possible**”（如果可能则包括证书路径中的所有证书）。

步骤 **10**：将导出的证书文件复制到 FAS 服务器。

步骤 **11**：通过在 FAS 服务器中输入以下 PowerShell cmdlet 将注册机构证书导入 FAS 服务器：

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

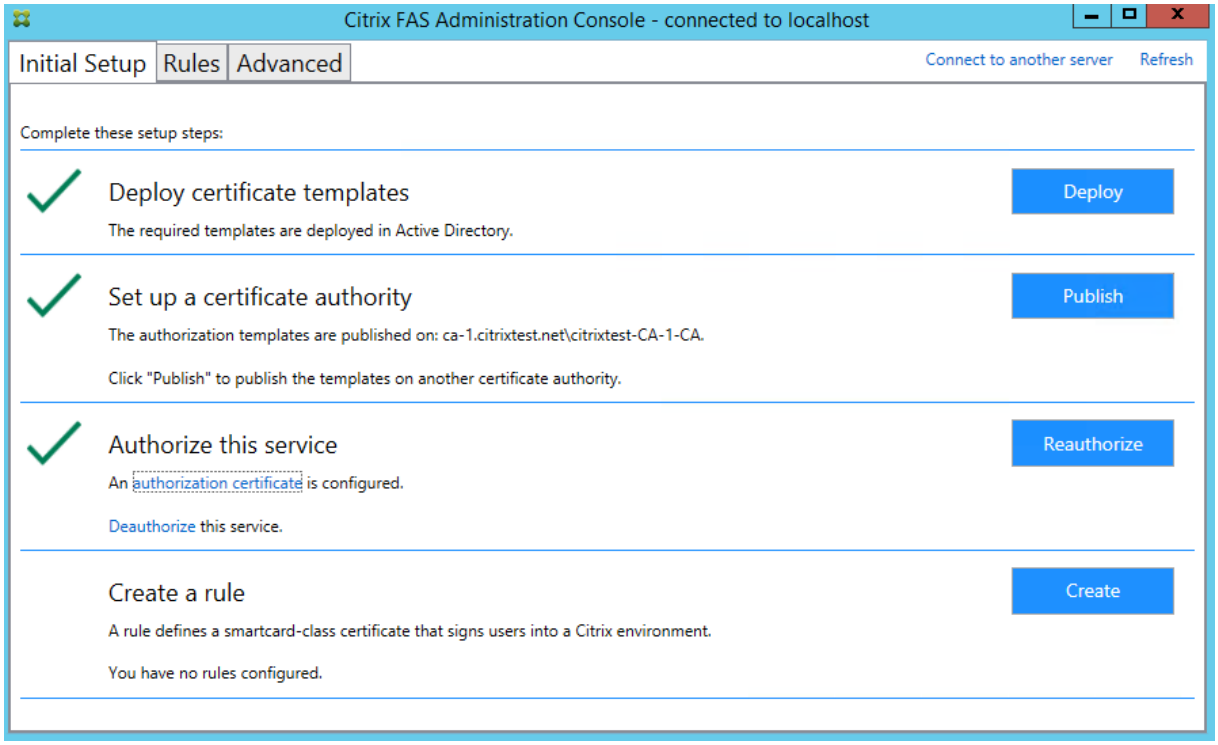
例如：

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

将显示以下内容：


```
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-8963-16ec31102dfc
CertificateRequest  :
Status              : Ok
```

步骤 **12**：关闭然后重新启动 FAS 管理控制台。



注意：“授权此服务”步骤带有绿色对勾。

步骤 **13**： 在 FAS 管理控制台中选择 **Rules**（规则）选项卡，并编辑安装和配置中所述的设置。

使用 **FAS** 管理控制台

FAS 管理控制台无法执行脱机证书签名请求，因此不建议使用，除非贵组织允许为注册机构证书执行联机证书签名请求。

执行初始 FAS 设置时，在部署证书模板和设置证书颁发机构之后、授权服务（配置程序中的步骤 3）之前：

步骤 **1**：通过更改下列行来编辑配置文件，如下所示：

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

该文件现在应显示如下：


```
<?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>
```

一些 TPM 会限制密钥长度。默认密钥长度为 2048 位。请务必指定受硬件支持的密钥长度。

步骤 **2**：授权服务。

步骤 **3**： 从证书颁发机构服务器手动发出挂起证书请求。获得注册机构证书后，安装过程中的步骤 3 将在管理控制台中显示为绿色。此时，将在 TPM 中生成注册机构证书的私钥。默认情况下该证书的有效期为 2 年。

步骤 **4**：将配置文件恢复为如下所示：

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

> 注意：
>
> 虽然 FAS 可使用 TPM 保护的密钥来生成用户证书，但是 TPM 硬件对于大型部署可能速度太慢。

步骤 **5**： 重新启动 FAS。这将强制此服务重新读取配置文件，并反映更改后的值。随后的自动私钥操作会影响用户证书密钥；这些操作不会在 TPM 中存储私钥，而会使用 Microsoft Software Key Storage Provider。

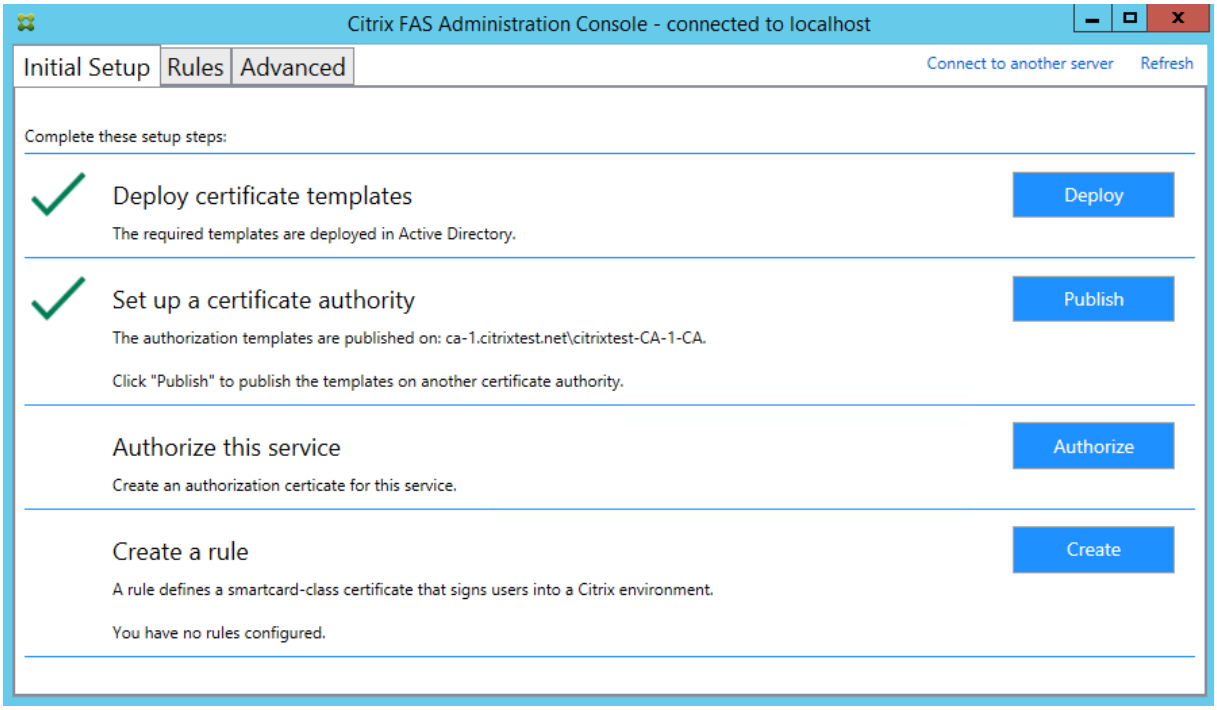
步骤 **6**： 在 FAS 管理控制台中选择 **Rules**（规则）选项卡，并编辑安装和配置中所述的设置。

示例 **3**

此示例介绍 HSM 中存储的注册机构证书私钥和用户证书私钥。此示例假设已配置 HSM。您的 HSM 将具有一个提供程序名称，例如 “HSM_Vendor’s Key Storage Provider”。

如果计划在虚拟化环境中运行 FAS 服务器，请向您的 HSM 供应商咨询有关虚拟机管理程序支持的信息。

步骤 **1.** 在使用管理控制台对 FAS 进行初始设置期间，请仅完成前两个步骤：“部署证书模板” 和 “设置证书颁发机构”。



步骤 **2**：请阅读您的 HSM 供应商文档，以确定 HSM ProviderName 值应是什么。如果 HSM 使用的是 CAPI，则文档中的提供程序可能称为加密服务提供程序 (CSP)。如果 HSM 使用的是 CNG，则文提供程序可能称为 Key Storage Provider (KSP)。

步骤 **3**：编辑配置文件，如下所示：

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

该文件现在应显示如下：

```
<?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>
```


此方案假设 HSM 使用是的 CNG，因此 ProviderLegacyCsp 值设置为 false。如果 HSM 使用是的 CAPI，则 ProviderLegacyCsp 值应设置为 true。请阅读您的 HSM 供应商文档，以确定 HSM 使用的是 CAPI 还是 CNG。此外，请阅读 HSM 供应商文档了解在生成非对称 RSA 密钥时受支持的密钥长度。在此示例中，密钥长度设置为默认值 2048 位。确保指定的密钥长度受硬件支持。

步骤 **4**：重新启动 Citrix 联合身份验证服务，以从配置文件中读取值。

步骤 **5**：在 HSM 内生成 RSA 密钥对，并通过在 FAS 管理控制台的 **Initial Setup**（初始设置）选项卡上单击 **Authorize**（授权）来创建证书签名请求。

步骤 **6**：要验证是否已在 HSM 中生成密钥对，请检查 Windows 事件日志中的应用程序条目：

```
[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]
```

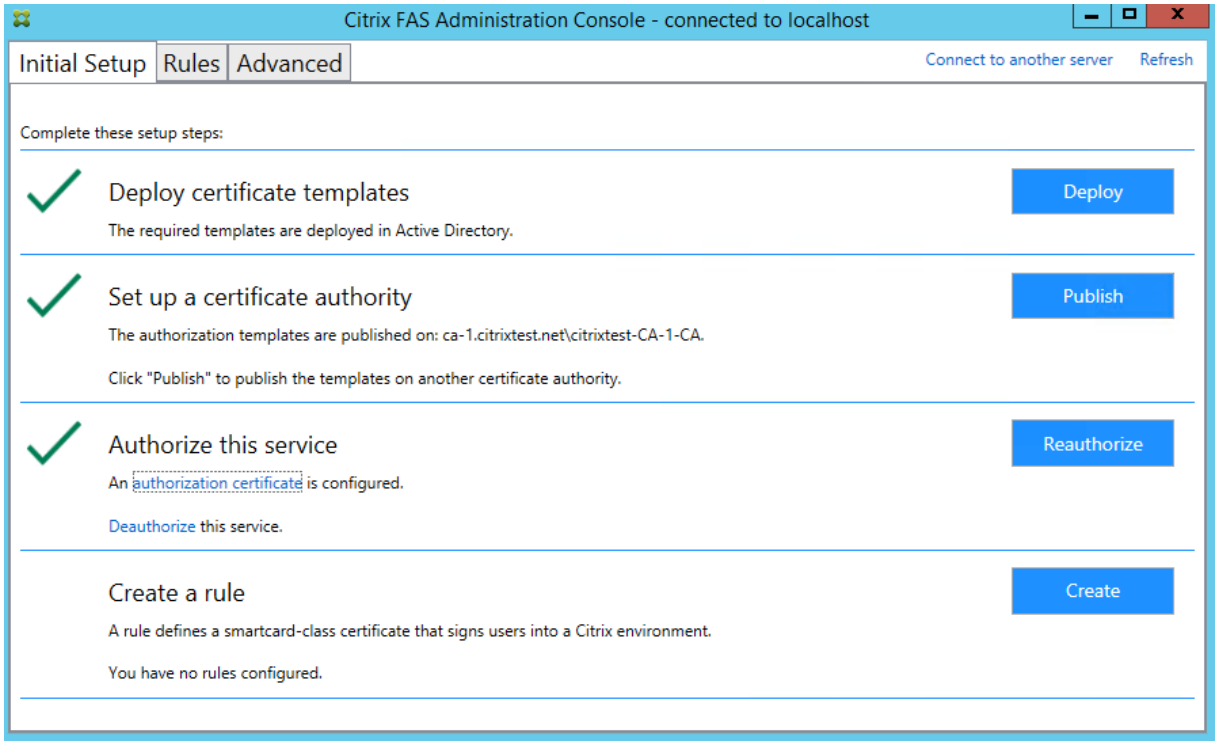
注意：[提供程序：[CNG] HSM_Vendor 的密钥存储提供程序]

步骤 **7**：在证书颁发机构服务器上的证书颁发机构 MMC 中，选择待处理的请求节点。

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$	

右键单击该请求，并选择 **Issue**（颁发）。

注意：“授权此服务”步骤带有绿色对勾。



步骤 **8**：在 FAS 管理控制台中选择 **Rules**（规则）选项卡，并编辑安装和配置中所述的设置。

FAS 存储证书

FAS 不使用 FAS 服务器上的 Microsoft 证书存储来存储证书。使用嵌入式数据库。

要确定注册机构证书的 GUID，请在 FAS 服务器中输入以下 PowerShell cmdlet：

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

例如 **Get-FasAuthorizationCertificate –address cg-fas-2.auth.net**：

```
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-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxyNzaiWX8DhUnOZMS2YVSDhr36AV5BGeIYOGVCFKvZPe
                      Rmm/xOVM6cNKsLbew3dYlbo+vdgWg86DFRVxTORhollV86iazDZyOiYGgxe9/s8YZzCspVWN1nB1
                      zX0UJfo1qo9UsmImYr7MR/dhGAtkfsFUoPcd2+zcezmgOfq/4vmCIuerwqzRR5T/p4og7+IjR1se
                      ECz/CbXROOuiDhW+VWbjcsgklcavzvC/jR33F9dZSXNgKRiGHgfd/lBb3elZKA4OOoi90u64Q916
                      3ba9BnihqxIgvwWILOmyUfiJmCgbhLJV4TPBopOdKz/axZEIO5p5XYVjCcpXqhqL7Ppn1wIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAJhdvw6yrLGBMtAgo3oPL6o8/at+IqHjHKqgcJNJO/MU7/7X
                      bZB46drLPFzpzF88DkmfoCEg0xlbzFX9waaiFs9CHC/AcEzblN925y1gqljsfC3l5TCKBAeLFoMl
                      PSEkfYMQUOSBYCuLlkFn1LXLSeQ3qJTzSvptYROawFmUMQLffwLSR1vOuS8DJSrpASrwdXJk3TOa
                      Glo/xJo/NRMOwMH+AvGbBsgp3l+jnDjXED5RudqARfgVgcW714JP+XIeFrE1TZmUL2skNIXEPNHC
                      H8eAHdYD26caFigydfefbjx4fbaJDFHJs5+1tnrTZ9knCrawhUiIyOMLGZOOaiER+z8=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval
```

要获得用户证书列表，请输入：

```
Get-FasUserCertificate -address \<FAS 服务器的 FQDN>
```

例如 **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
```

> 注意：
>
> 使用 HSM 存储私钥时，HSM 容器通过 GUID 进行标识。可以通过使用以下命令获取 HSM 中的私钥的 GUID：
>
> ```
> Get-FasUserCertificate -address \<FAS 服务器的 FQDN> -KeyInfo
>     $true
> ```
>
> 例如：


```
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
```

相关信息

- 安装和配置是 FAS 安装和配置的主要参考资料。
- 联合身份验证服务体系结构概述一文总结了常见的 FAS 部署。
- 高级配置一文中介绍了其他“操作方法”文章。

安全性和网络配置

November 7, 2019

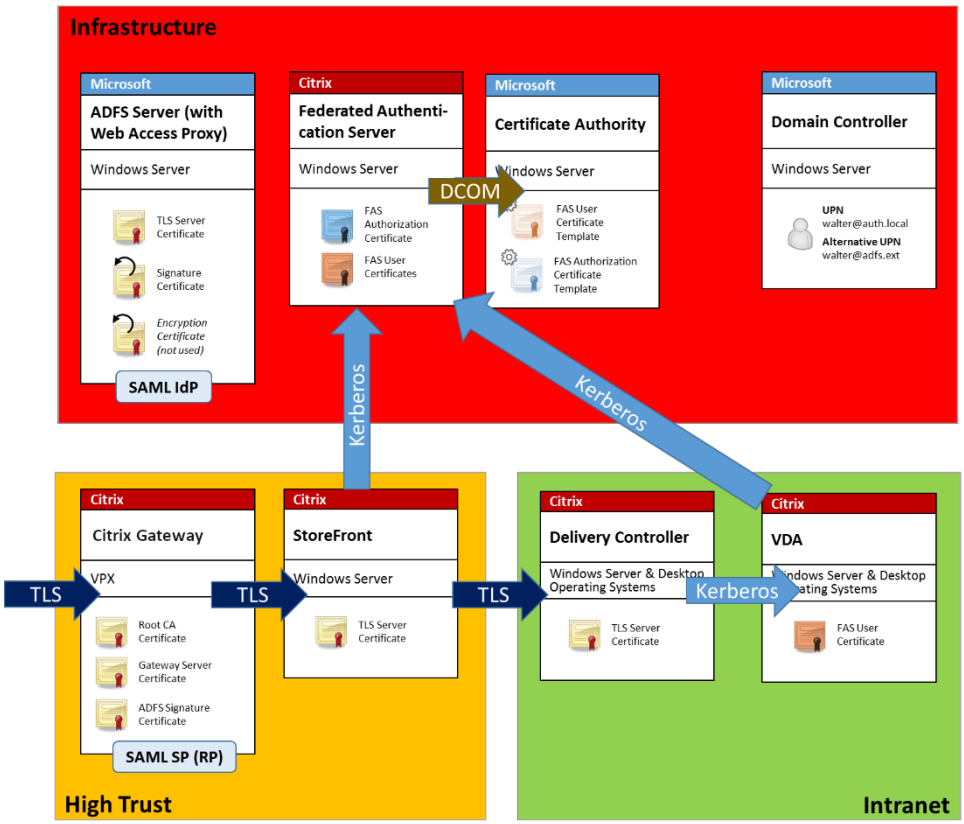
联合身份验证服务 (FAS) 与 Microsoft Active Directory 和 Microsoft 证书颁发结构紧密集成。确保恰当管理系统和确保系统安全非常重要，因此，请像对域控制器或其他关键性基础结构一样制定安全策略。

本文档概述了部署 FAS 时需要注意的安全问题。此外，还概述了可以帮助确保您的基础结构安全的可用功能。

网络体系结构

下图显示了 FAS 部署中使用的主要组件和安全范围。

应将 FAS 服务器以及证书颁发机构和域控制器视为安全关键型基础结构的一部分。在联合环境中，Citrix Gateway 和 Citrix StoreFront 是可信的用于执行用户身份验证的组件；其他 Citrix Virtual Apps and Desktops 组件不受引入 FAS 影响。



防火墙和网络安全性

Citrix Gateway、StoreFront 与 Delivery Controller 组件之间的通信应通过端口 443 受 TLS 保护。StoreFront 服务器仅执行传出连接，而 Citrix Gateway 仅应接受使用 HTTPS 端口 443 通过 Internet 建立的连接。

StoreFront 服务器使用相互身份验证的 Kerberos 通过端口 80 访问 FAS 服务器。身份验证使用 FAS 服务器的 Kerberos HOST/fqdn 标识以及 StoreFront 服务器的 Kerberos 计算机帐户标识。这将生成 Citrix Virtual Delivery Agent (VDA) 登录用户时所需的一次性使用的“凭据句柄”。

HDX 会话连接到 VDA 时，VDA 还将通过端口 80 访问 FAS 服务器。身份验证使用 FAS 服务器的 Kerberos HOST/fqdn 标识以及 VDA 的 Kerberos 计算机标识。此外，VDA 必须提供“凭据句柄”才能访问证书和私钥。

Microsoft 证书颁发机构接受使用通过 Kerberos 验证的 DCOM 的通信，可以将其配置为使用固定 TCP 端口。此外，证书颁发机构还要求 FAS 服务器提供通过可信注册代理证书签名的 CMC 数据包。

服务器	防火墙端口
联合身份验证服务	[输入] 从 StoreFront 和 VDA 至基于 HTTP 的 Kerberos，[输出] DCOM 至 Microsoft 证书颁发机构

服务器	防火墙端口
Citrix Gateway	[输入] 从客户端计算机至 HTTPS，[输入/输出] 从 HTTPS 至 StoreFront 服务器/从 StoreFront 服务器至 HTTPS，[输出] HDX 至 VDA
StoreFront	[输入] 从 Citrix Gateway 至 HTTPS，[输出] HTTPS 至 Delivery Controller，[输出] Kerberos HTTP 至 FAS
Delivery Controller	[输入] 从 StoreFront 服务器至 HTTPS，[输入/输出] 从 VDA 至基于 HTTP 的 Kerberos
VDA	[输入/输出] 从 Delivery Controller 至基于 HTTP 的 Kerberos，[输入] 从 Citrix Gateway 至 HDX [输出] Kerberos HTTP 至 FAS
Microsoft 证书颁发机构	[输入] FAS 至 DCOM 且已签名

管理职责

可以将对环境的管理职责分为以下几组：

名称	职责
企业管理员	在林中安装证书模板并确保其安全
域管理员	配置组策略设置
证书颁发机构管理员	配置证书颁发机构
FAS 管理员	安装并配置 FAS 服务器
StoreFront/Citrix Gateway 管理员	配置用户身份验证
Citrix Virtual Desktops 管理员	配置 VDA 和 Controller

每个管理员分别控制整体安全模型的不同部分，从而允许采用深度防御措施来确保系统安全。

组策略设置

可信 FAS 计算机借助通过组策略配置的“索引号 -> FQDN”查询表进行标识。访问 FAS 服务器时，客户端将验证 FAS 服务器的 `HOST\<fqdn>` Kerberos 标识。访问 FAS 服务器的所有服务器都必须具有相同的 FQDN 配置以使索引相同，否则，StoreFront 和 VDA 可能会访问不同的 FAS 服务器。

为避免配置不正确，Citrix 建议您对环境中的所有计算机应用一条策略。修改 FAS 服务器的列表时应谨慎，特别是删除条目或对条目重新排序时。

应将此 GPO 限制为只能被安装 FAS 服务器以及解除其授权的 FAS 管理员（和/或域管理员）控制。请小心操作，以免在解除 FAS 服务器授权后立即重复使用计算机 FQDN 名称。

证书模板

如果您不希望使用与 FAS 一起提供的 Citrix_SmartcardLogon 证书模板，您可以修改它的副本。支持以下修改。

重命名证书模板

如果您希望重命名 Citrix_SmartcardLogon 以符合您的组织模板命名标准，您必须：

- 创建证书模板的一个副本，然后对其重命名以符合您的组织模板命名标准。
- 使用 FAS PowerShell 命令管理 FAS，而不是管理用户界面。（管理用户界面仅适用于 Citrix 默认模板名称。）
  - 使用 Microsoft MMC 证书模板管理单元或 Publish-FasMsTemplate 命令发布您的模板，以及
  - 使用 New-FasCertificateDefinition 命令在 FAS 中配置您的模板的名称。

修改常规属性

您可以修改证书模板中的有效期。

请勿修改续订期。FAS 会忽略证书模板中的此设置。FAS 会自动在证书的有效期中间续订证书。

修改请求处理属性

请勿修改这些属性。FAS 会忽略证书模板中的这些设置。FAS 会始终取消选中 **Allow private key to be exported**（允许导出私钥）及取消选中 **Renew with same key**（使用相同密钥续订）。

修改加密属性

请勿修改这些属性。FAS 会忽略证书模板中的这些设置。

请参阅 私钥保护，了解 FAS 提供的等效设置。

修改密钥证明属性

请勿修改这些属性。FAS 不支持密钥证明。

修改被取代的模板属性

请勿修改这些属性。FAS 不支持取代模板。

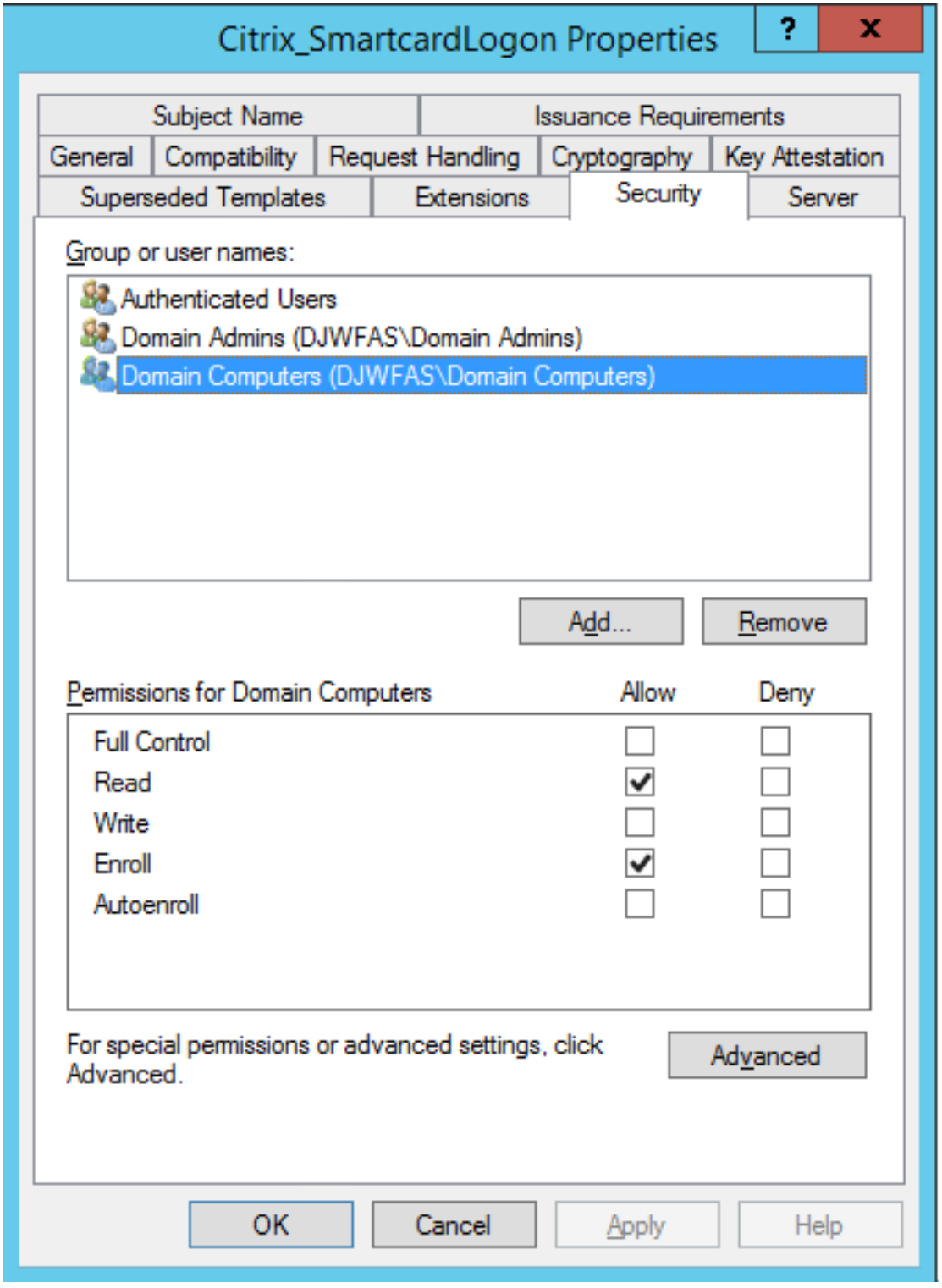
修改扩展属性

您可以修改这些设置以符合您的组织策略。

注意：不合适的扩展设置可能会导致出现安全问题，或导致证书无法使用。

修改安全属性

Citrix 建议修改这些设置以仅允许 FAS 服务的计算机帐户具有注册权限。对于其他服务，还允许对系统具有完全控制权限。不需要任何其他权限。您可能希望允许其他权限，例如，允许 FAS 管理员查看修改后的模板以便进行故障排除。



修改使用者名称属性

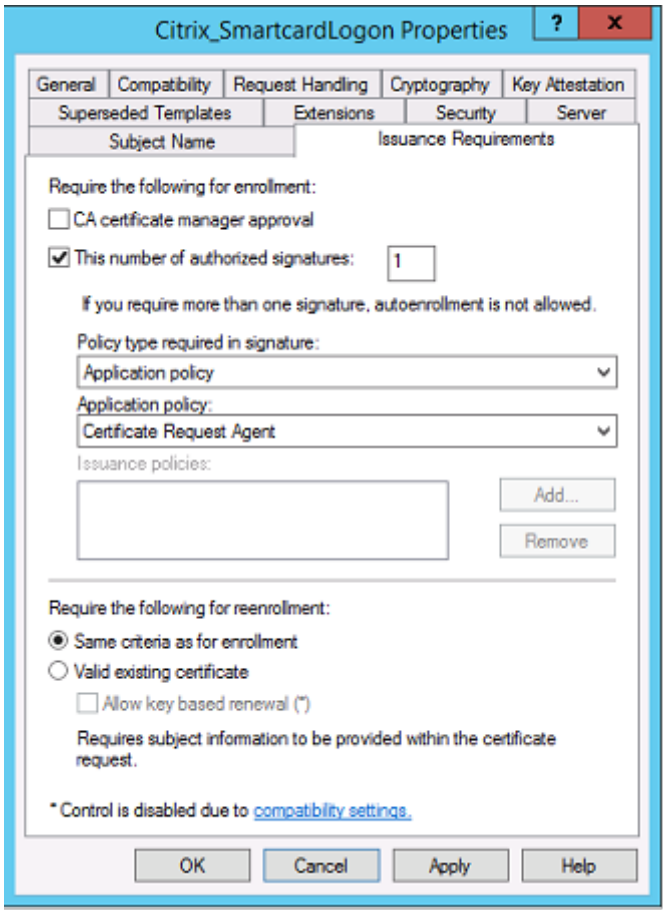
您可以修改这些设置以符合您的组织策略（如果需要）。

修改服务器属性

尽管 Citrix 不建议，但您仍可以修改这些设置以符合您的组织策略（如果需要）。

修改颁发要求属性

请勿修改这些设置。这些设置应该如下所示：



修改兼容性属性

您可以修改这些设置。该设置必须至少为 **Windows Server 2003 CA**（架构版本 2）。但是，FAS 仅支持 Windows Server 2008 及更高版本的 CA。此外，如上文所述，FAS 会忽略通过选择 **Windows Server 2008 CA**（架构版本 3）或 **Windows Server 2012 CA**（架构版本 4）可用的其他设置。

证书颁发机构管理

证书颁发机构管理员负责配置证书颁发机构服务器以及颁发证书颁发机构服务器使用的证书私钥。

发布模板

要使证书颁发机构能够颁发基于企业管理员提供的模板创建的证书，证书颁发机构管理员必须选择发布该模板。

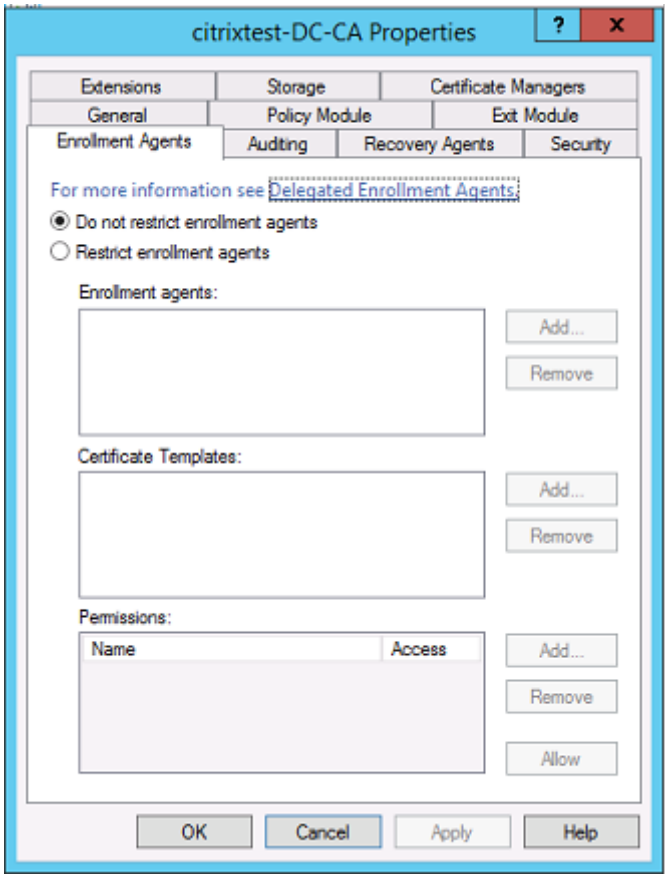
简单的安全做法是在安装 FAS 服务器时仅发布注册机构证书模板，或者坚持执行完全脱机的颁发过程。在任何一种情况下，证书颁发机构管理员都应通过授权注册机构证书申请来保持完全控制能力，并配置用于向 FAS 服务器授权的策略。

防火墙设置

一般情况下，证书颁发机构管理员还能够控制证书颁发机构的网络防火墙设置，进而允许控制传入连接。证书颁发机构管理员可以配置 DCOM TCP 和防火墙规则，以便只有 FAS 服务器能够申请证书。

限制注册

默认情况下，任何注册机构证书的持有者都能使用允许访问的任何证书模板为任何用户颁发证书。应使用“限制注册代理”证书颁发机构属性将其限制为一组非特权用户。



策略模块和审核

对于高级部署，可以使用自定义安全模块来跟踪和否决证书颁发。

FAS 管理

FAS 具有多项安全功能。

通过 ACL 限制 StoreFront、用户和 VDA

FAS 安全模型的核心是控制哪些 Kerberos 帐户能够访问功能：

访问矢量	说明
StoreFront [IdP]	信任这些 Kerberos 帐户以声明已正确验证某个用户的身份。如果这些帐户中的某个帐户已损坏，可以创建证书并将其用于 FAS 配置所允许的用户。
VDA [信赖方]	这些是有权访问证书和私钥的计算机。此外，还需要使用通过 IdP 检索的凭据句柄，使该组中已损坏的 VDA 帐户具有受限的系统攻击范围。
用户	这将控制可通过 IdP 声明的用户。请注意，这与证书颁发机构中的“受限注册代理”配置选项存在重叠。一般来说，建议仅在此列表中包含非特权帐户。这样可以阻止已损坏的 StoreFront 帐户将权限提升到更高管理级别。具体而言，此 ACL 不应允许域管理员帐户。

配置规则

如果有多个独立 Citrix Virtual Apps 或 Citrix Virtual Desktops 部署采用相同的 FAS 服务器基础结构，规则将很有用。每条规则都带有一组独立的配置选项；具体而言，可以单独配置 ACL。

配置证书颁发机构和模板

可以为不同的访问权限配置不同的证书模板和 CA。高级配置可以选择使用功能较弱或较强的证书，具体取决于环境。例如，标识为“外部”的用户拥有证书的权限可能会低于标识为“内部”的用户拥有的证书。

会话中证书和身份验证证书

FAS 管理员可以控制用于身份验证的证书是否在用户的会话中可用。例如，此控制功能可用于仅使“签名”证书在会话中可用，使具有更高功能的“登录”证书只在登录时使用。

私钥保护和密钥长度

FAS 管理员可以将 FAS 配置为在硬件安全模块 (HSM) 或受信任的平台模块 (TPM) 中存储私钥。Citrix 建议您应至少通过将注册机构证书私钥存储在 TPM 中来保护私钥；此选项在“脱机”证书请求过程中提供。

同样，可以将用户证书私钥存储在 TPM 或 HSM 中。所有密钥都应以“不可导出”格式生成，长度应至少为 2048 位。

事件日志

FAS 服务器提供详细的配置和运行时事件日志，这些日志可用于审核和入侵检测目的。

管理访问权限和管理工具

FAS 中包括一些远程管理功能（相互验证 Kerberos）和工具。“本地管理员组”成员对 FAS 配置具有完全控制权限。应仔细维护此列表。

Citrix Virtual Apps、Citrix Virtual Desktops 和 VDA 管理员

一般而言，在使用 FAS 时不会更改 Delivery Controller 和 VDA 管理员的安全模型，因为 FAS“凭据句柄”只会替换“Active Directory 密码”。Controller 和 VDA 管理组中应仅包含可信用户。应保留审核日志和事件日志。

常规 Windows 服务器安全性

所有服务器都应安装所有修补程序，并安装标准防火墙和防病毒软件。应将安全关键型基础结构服务器放置在安全的物理位置，并仔细管理磁盘加密选项和虚拟机维护选项。

应将审核日志和事件日志安全地存储在远程计算机上。

应仅允许授权管理员访问 RDP。如有可能，应要求用户帐户进行智能卡登录，尤其对于证书颁发机构和域管理员帐户更是如此。

相关信息

- 安装和配置是 FAS 安装和配置的主要参考资料。
- 部署体系结构一文中介绍了 FAS 体系结构。
- 高级配置一文中介绍了其他“操作方法”文章。

解决了 **Windows** 登录问题

November 7, 2019

本文介绍了用户使用证书和/或智能卡登录时 Windows 提供的日志和错误消息。可以使用这些日志提供的信息对身份验证失败问题进行故障排除。

证书和公钥基础结构

Windows Active Directory 维护负责管理用户登录时使用的证书的多个证书存储。

- **NTAuth** 证书存储：要针对 Windows 进行身份验证，必须将即时颁发用户证书（即，不支持任何证书链）的证书颁发机构放置在 NTAuth 存储中。要查看这些证书，请在 certutil 程序中输入以下命令：certutil –viewstore –enterprise NTAuth。
- 根证书和中间证书存储：一般而言，证书登录系统只能提供单个证书，因此，如果正在使用证书链，所有计算机上的中间证书存储都必须包括这些证书。根证书必须位于可信证书存储中，而倒数第二个证书必须位于 NTAuth 存储中。
- 登录证书扩展名和组策略：可以将 Windows 配置为强制验证 EKU 以及其他证书策略。请参阅 Microsoft 文档：https://technet.microsoft.com/en-us/library/ff404287%28v=ws.10%29.aspx。

注册表策略	说明
AllowCertificatesWithNoEKU	禁用时，证书必须包括智能卡登录扩展密钥用法 (EKU)。
AllowSignatureOnlyKeys	默认情况下，Windows 会过滤掉不允许进行 RSA 解密的证书私钥。此选项将覆盖该过滤器。
AllowTimeInvalidCertificates	默认情况下，Windows 会过滤掉过期的证书。此选项将覆盖该过滤器。
EnumerateECCCerts	启用椭圆曲线身份验证。
X509HintsNeeded	如果某个证书不包含唯一的用户主体名称 (UPN)，或者可以不确定，此选项将允许用户手动指定其 Windows 登录帐户。
UseCachedCRLOnlyAnd、IgnoreRevocationUnknownErrors	禁用吊销检查（通常在域控制器上设置）。

- 域控制器证书：所有服务器必须具有恰当的“域控制器”证书，才能对 Kerberos 连接进行身份验证。可以使用“本地计算机证书个人存储”MMC 管理单元菜单申请这些证书。

UPN 名称和证书映射

建议用户证书在使用者替代名称扩展名中包括一个唯一的用户主体名称 (UPN)。

Active Directory 中的 UPN 名称

默认情况下，Active Directory 中的每个用户都具有建立在模式 <samUsername>@<domainNetBios> 和 <samUsername>@<domainFQDN> 的基础之上的隐式 UPN。可用域和 FQDN 都包括在林的 RootDSE 条目中。请注意，单个域可以具有多个在 RootDSE 中注册的 FQDN 地址。

此外，Active Directory 中的每个用户都具有显式 UPN 和 altUserPrincipalNames。这些是用于指定该用户的 UPN 的 LDAP 条目。

按 UPN 搜索用户时，Windows 首先在当前域（取决于对查找 UPN 的过程的识别）中查找显式 UPN，然后查找替代 UPN。如果没有匹配项，则将查找隐式 UPN，这样可以解析到林中的其他域。

证书映射服务

如果某个证书不包括显式 UPN，Active Directory 将具有用于存储完全匹配的公用证书以供在 x509certificate 属性中使用的选项。计算机可以直接查询此属性（默认情况下，在单个域中查询），以便为用户解析此类证书。

系统将向用户提供一个选项以指定可加快此搜索速度并且还允许在跨域环境中使用此功能的用户帐户。

如果林中存在多个域，并且用户未明确指定域，Active Directory rootDSE 将指定证书映射服务的位置。该服务通常位于全局目录计算机上，并且在林中具有所有 x509certificate 属性的缓存视图。可以使用此计算机仅基于证书来有效地查找任意域中的用户帐户。

控制登录域控制器选择

当环境中包含多个域控制器时，查看并显示用于身份验证的域控制器将非常有用，这样可以启用并检索日志。

控制域控制器选择

要强制 Windows 使用特定的 Windows 域控制器进行登录，可以通过配置 lmhosts 文件(\Windows\System32\drivers\etc\lmh
来显式设置 Windows 计算机使用的域控制器列表。

该位置通常存在一个名为 lmhosts.sam 的示例文件。其内容只有一行：

1.2.3.4 dcnetbiosname #PRE #DOM:mydomai

其中，1.2.3.4 为 mydomain 域中名为 dcnetbiosname 的域控制器的 IP 地址。

重新启动后，Windows 计算机将使用该信息登录 mydomain。请注意，完成调试后，必须还原此配置。

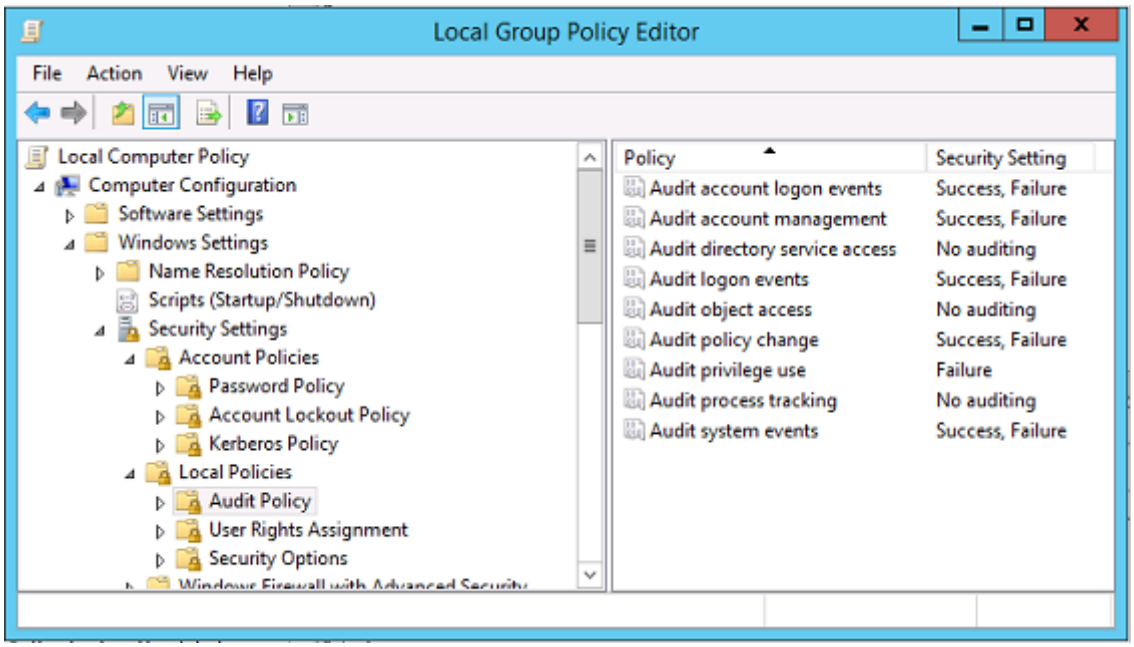
识别正在使用的域控制器

登录时，Windows 将使用让该用户登录的域控制器设置一个 MSDOS 环境变量。要查看该变量，请启动命令提示窗口并输入以下命令：**echo %LOGONSERVER%**。

与身份验证有关的日志存储在此命令返回的计算机中。

启用帐户审核事件

默认情况下，Windows 域控制器不启用完全帐户审核日志。可以在组策略编辑器中通过安全设置中的审核策略对其进行控制。启用后，域控制器将在安全日志文件中生成额外的事件日志信息。



证书验证日志

检查证书有效性

如果将智能卡证书导出为 DER 证书（不需要任何私钥），则可以通过以下命令验证其有效性：certutil –verify user.cer

启用 **CAPI** 日志记录

在域控制器和用户计算机上，打开事件查看器并启用 Microsoft/Windows/CAPI2/Operational Logs 的日志记录功能。

可以通过 CurrentControlSet\Services\crypt32 下的注册表项控制 CAPI 日志记录功能。

值	说明
DiagLevel (DWORD)	详细级别（0 到 5）
DiagMatchAnyMask (QUADWORD)	事件过滤器（对所有事件使用 0xffffff）
DiagProcessName (MULTI_SZ)	按进程名称过滤（例如，LSASS.exe）

CAPI 日志

消息	说明
构建链	名为 CertGetCertificateChain 的 LSA（包括结果）
验证吊销	名为 CertVerifyRevocation 的 LSA（包括结果）
X509 对象	在详细模式下，证书和证书吊销列表 (CRL) 转储到 AppData\LocalLow\Microsoft\X509Objects
验证证书链策略	名为 CertVerifyChainPolicy 的 LSA（包括参数）

错误消息

错误代码：	说明
证书不可信	无法使用计算机的中间证书存储和可信根证书存储中的证书构建智能卡证书。
证书吊销检查错误	无法从证书 CRL 分发点指定的地址下载智能卡的 CRL。如果强制执行吊销检查，则会阻止成功登录。请参阅证书和公钥基础结构部分。
证书用途错误	证书不适用于登录。例如，证书可能是服务器证书或签名证书。

Kerberos 日志

要启用 Kerberos 日志记录，请在域控制器和最终用户计算机上创建以下注册表值：

配置单元	Value name（值名称）	值 [DWORD]
CurrentControlSet\Control\Lsa	日志级别	0x1
CurrentControlSet\Control\Lsa\Kerberos\Parameters	KerbDebugLevel	0xffffffff

配置单元	Value name（值名称）	值 [DWORD]
CurrentControlSet\Services\Kd	KdcDebugLevel	0x1
CurrentControlSet\Services\Kdc	KdcExtraLogLevel	0x1f

Kerberos 日志记录输出到系统事件日志中。

- “不可信证书”等消息应能够轻松诊断。
- 下面两个错误代码为信息性代码，可以安全地忽略：
  - KDC_ERR_PREAUTH_REQUIRED（用于向后兼容域控制器较旧的域控制器）
  - 未知错误 0x4b

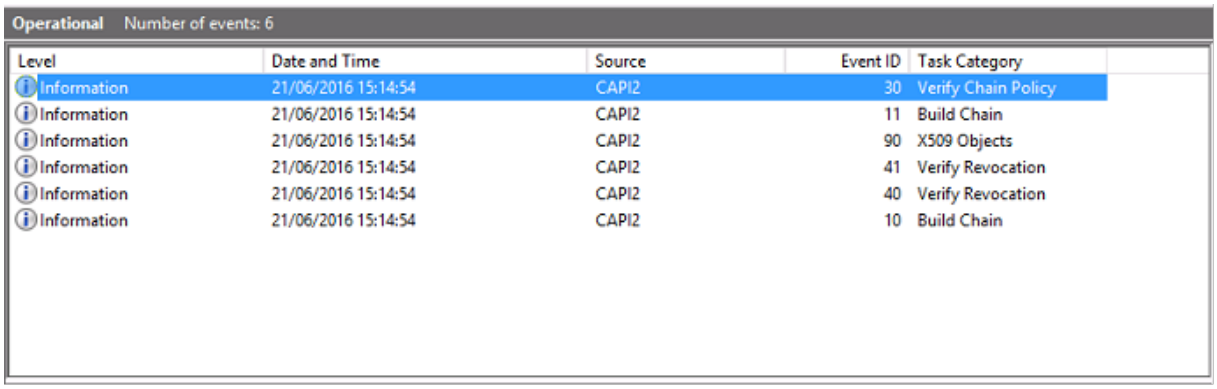
事件日志消息

本节介绍了用户使用证书登录时域控制器和工作站上的预期日志条目。

- 域控制器 CAPI2 日志
- 域控制器安全日志
- Virtual Delivery Agent (VDA) 安全日志
- VDA CAPI 日志
- VDA 系统日志

域控制器 **CAPI2** 日志

登录过程中，域控制器将验证调用者的证书，从而生成以下格式的一系列日志条目。



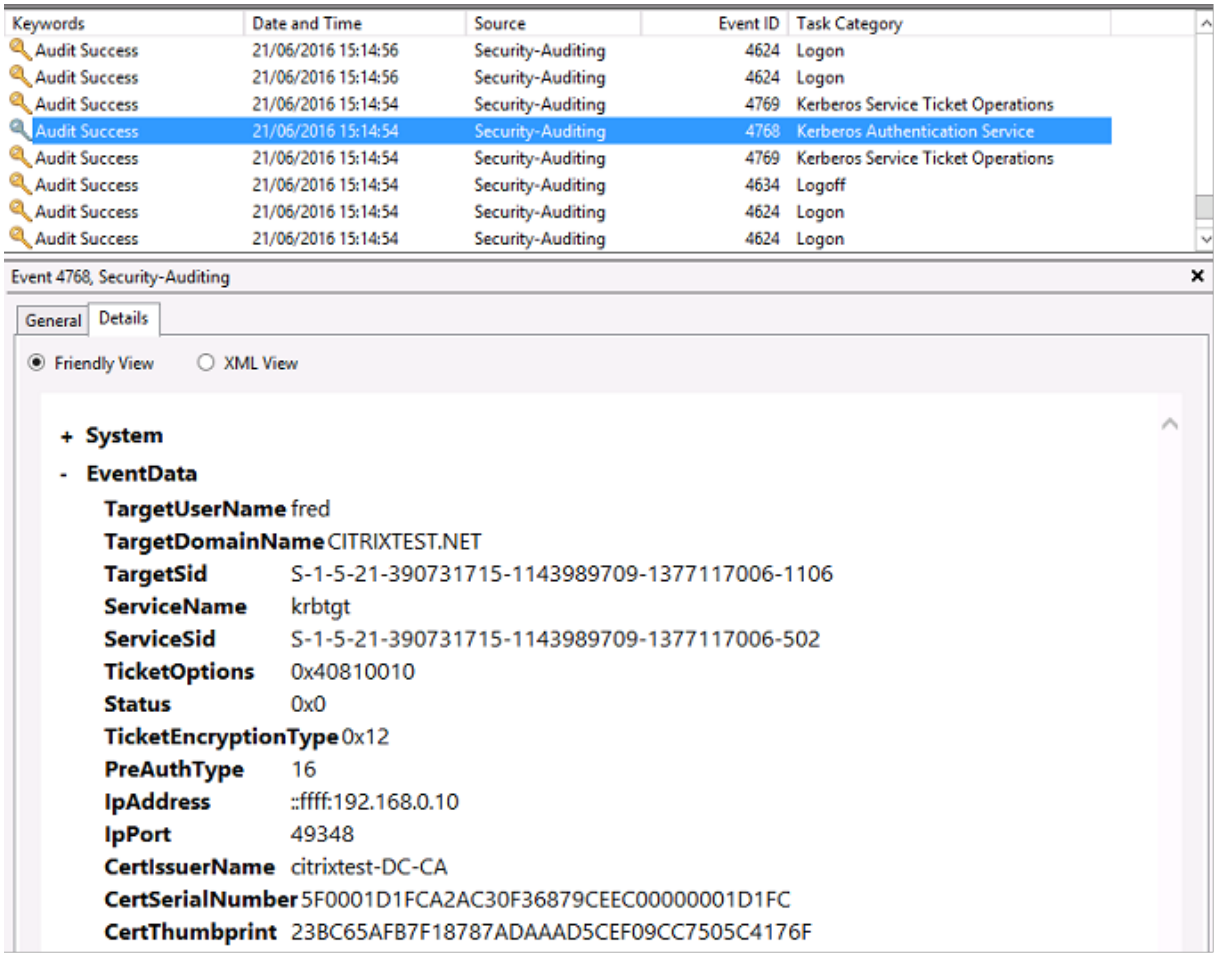
最终事件日志消息在域控制器上显示 lsass.exe，从而根据 VDA 提供的证书构建一个链，并验证其有效性（包括吊销）。结果返回为“ERROR_SUCCESS”。

- **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

域控制器安全日志

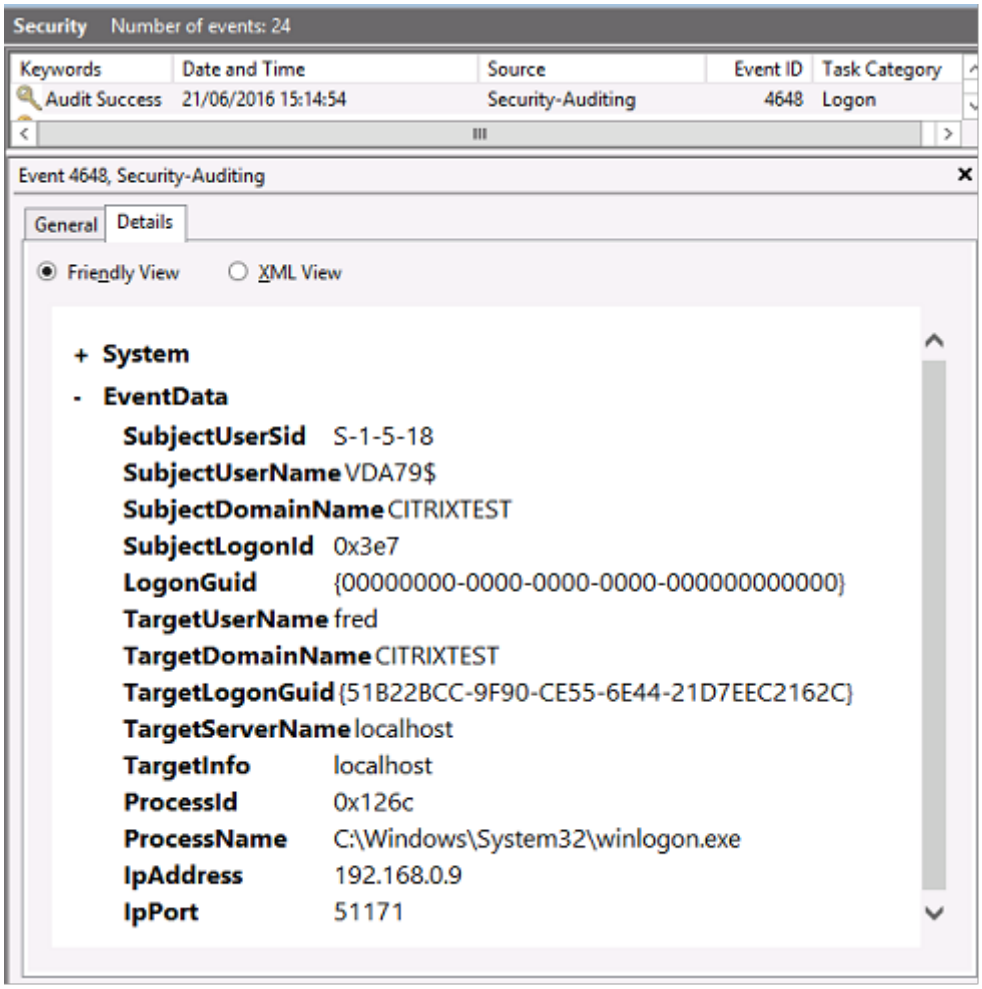
域控制器显示一系列登录事件，关键事件为 4768，其中，证书用于发出 Kerberos Ticket Granting Ticket (krbtgt)。

在此消息之前显示的消息将显示用于进行身份验证以登录域控制器的服务器的计算机帐户。在此消息之后显示的消息将显示属于正在用于针对域控制器进行身份验证的新 krbtgt 的用户帐户。



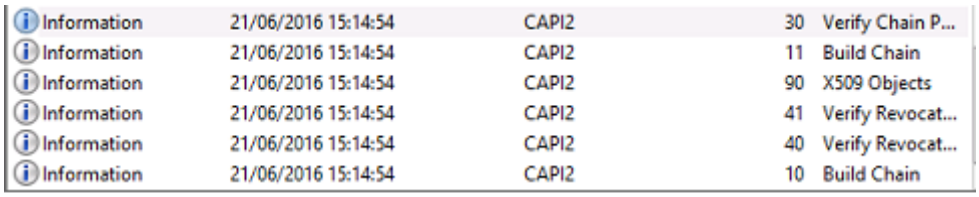
VDA 安全日志

与登录事件相对应的 VDA 安全审核日志是指 winlogon.exe 中事件 ID 为 4648 的条目。



VDA CAPI 日志

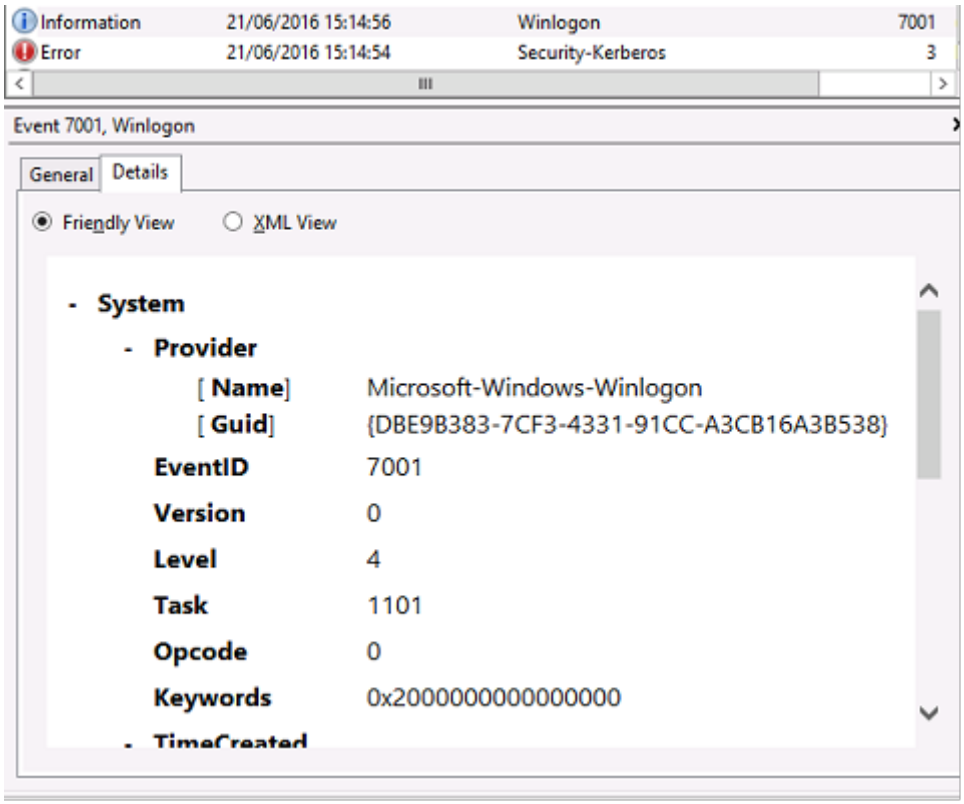
此示例 VDA CAPI 日志显示 lsass.exe 中的单个链构建和验证顺序，用于验证域控制器证书 (dc.citrixtest.net)。



- **UserData**
  - **CertVerifyCertificateChainPolicy**
    - **Policy**
      - [**type**] CERT_CHAIN_POLICY_NT_AUTH
      - [**constant**] 6
    - **Certificate**
      - [**fileRef**] 813C6D12E1E1800E61B8DB071E186EB912B7
      - [**subjectName**] dc.citrixtest.net
    - **CertificateChain**
      - [**chainRef**] {84E0B3D1-A4D4-4AC7-BA99-5291415B343
    - **Flags**
      - [**value**] 0
    - **Status**
      - [**chainIndex**] -1

VDA 系统日志

启用了 Kerberos 日志记录时，系统日志将显示错误 KDC_ERR_PREAUTH_REQUIRED（可以忽略）以及 Winlogon 中显示 Kerberos 登录成功的条目。



最终用户错误消息

本节列出了在 Windows 登录页面上向用户显示的常见错误消息。

显示的错误消息	说明和参考
无效用户名或密码	计算机相信您拥有有效的证书和私钥，但 Kerberos 域控制器拒绝了连接。参阅本文的 *Kerberos* 登录部分。
系统无法让您登录。无法验证您的凭据。/不支持该请求	无法访问域控制器，或者域控制器未安装恰当的证书。在域控制器上重新注册“域控制器”和“域控制器身份验证”证书，如 CTX206156 中所述。此操作通常值得一试，即使在现有证书可能有效时也是如此。
系统无法让您登录。用于身份验证的智能卡证书不可信。	未在本地计算机上安装中间证书和根证书。有关在未加入域的计算机上安装智能卡证书的说明，请参阅 CTX206156。另请参阅证书和公钥基础结构。
无法登录的原因是您的帐户不支持智能卡登录。	未将工作组用户帐户完全配置为执行智能卡登录。
请求的密钥不存在	证书引用不可访问的私钥。PIV 卡未完全配置并且缺少 CHUID 或 CCC 文件时会出现此问题。
尝试使用智能卡时出错	未正确安装智能卡中间件。有关智能卡的安装说明，请参阅 CTX206156。
Insert a smart card（插入智能卡）	未检测到智能卡或读卡器。如果插入了智能卡，则此消息指示存在硬件或中间件问题。有关智能卡的安装说明，请参阅 CTX206156。
PIN 不正确	智能卡拒绝了用户输入的 PIN。
找不到有效的智能卡证书。	可能未正确设置证书上的扩展名，或者 RSA 密钥太短（小于 2048 位）。有关生成有效的智能卡证书的信息，请参阅 CTX206901。
智能卡被阻止	智能卡已被锁定（例如，用户多次输入了错误的 PIN）。管理员可能对智能卡的 PIN 解锁 (puk) 代码具有访问权限，并且可以使用智能卡供应商提供的工具重置用户的 PIN。如果 puk 代码不可用，或者被锁定，则必须将智能卡重置为出厂设置。
请求错误	智能卡私钥不支持域控制器要求的加密。例如，域控制器可能已申请“私钥解密”，但智能卡仅支持签名。这通常指示未正确设置证书上的扩展名，或者 RSA 密钥太短（小于 2048 位）。有关生成有效的智能卡证书的信息，请参阅 CTX206901。

相关信息

- 配置域以进行智能卡登录：http://support.citrix.com/article/CTX206156
- 智能卡登录策略：https://technet.microsoft.com/en-us/library/ff404287%28v=ws.10%29.aspx
- 启用 CAPI 日志记录：http://social.technet.microsoft.com/wiki/contents/articles/242.troubleshooting-pki-problems-on-windows.aspx
- 启用 Kerberos 日志记录：https://support.microsoft.com/en-us/kb/262177
- 有关通过第三方证书颁发机构启用智能卡登录的指导原则：https://support.microsoft.com/en-us/kb/281245

PowerShell cmdlet

November 7, 2019

可使用联合身份验证服务 (FAS) 管理控制台执行简单的部署。不过，PowerShell 界面中提供了更多的高级选项。When you are using options that are not available in the console, Citrix recommends using only PowerShell for configuration.

以下命令将添加 FAS PowerShell cmdlet：

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

在 PowerShell 窗口中，可以使用 Get-Help <*cmdlet name*> 显示 cmdlet 帮助信息。

有关 FAS PowerShell SDK cmdlet 的详细信息，请参阅 https://developer-docs.citrix.com/。

