自助服务密码重置 1.0

Dec 08, 2016

© 1999-2017 Citrix Systems, Inc. All rights reserved.

关于自助服务密码重置

Sep 19, 2016

通过自助服务密码重置，最终用户能够在更大程度上控制其用户帐户。 配置自助服务密码重置后，如果最终用户在登录其系统时遇到问题，可以通过正确回答多个安全问题来解锁帐户或将密码重置为新密码。

重置用户密码是一个本质上安全敏感的过程。 我们建议您参阅安全配置一文，以确保正确配置您的部署。

自助服务密码重置包含以下三个组件：

- 自助服务密码重置配置控制台
- 自助服务密码重置服务
- StoreFront 中的安全问题注册

自助服务密码重置配置控制台

- **服务配置。** 配置自助服务密码重置服务，包括中央存储地址、数据代理帐户以及自助服务密码重置帐户。
  - 中央存储地址：用于存储自助服务密码重置数据的网络共享位置。
  - 数据代理帐户：与中央存储进行通信。 该帐户需要对中央存储具有读取和写入权限。
  - 自助服务密码重置帐户：用于解锁帐户和重置密码。
- **用户配置。** 配置哪些用户/组/OU 可以使用自助服务密码重置功能，并指定许可证服务器地址和默认服务地址。
  - 命名用户配置：定义自助服务密码重置的目标用户组，其中可以包括 Active Directory 中的用户/组/OU。
  - 许可证服务器地址：只能在 XenApp 或 XenDesktop Platinum Edition 中使用自助服务密码重置。 最低许可证服务器版本必须为 11.13.1 或更高版本。
  - 选中或取消选中**解锁**和**重置**功能。
  - 默认服务地址：指定自助服务密码重置服务的 URL。
- **身份验证。** 配置用于注册以及解锁或重置密码的调查表。
  - 向从中生成调查表的问题存储中添加问题或组。
  - 从问题存储中选择要用于注册的问题列表。
  - 导出/导入安全问题或组。

自助服务密码重置服务

自助服务密码重置服务在 Web 服务器上运行，允许用户重置其 Windows 密码以及解锁其 Windows 帐户。 最终用户的申请将通过 StoreFront 发送到此服务。

StoreFront 中的安全问题注册

使用 StoreFront 可允许用户注册安全问题的答案。 注册这些答案时，用户可以重置域密码以及解锁域帐户。 有关详细信息，请参阅 StoreFront 文档中的自助服务密码重置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

已知问题

Sep 19, 2016

- 打开自助服务密码重置控制台后，可能无法将其固定到任务栏。 [#646300]

  解决方法：从**开始**菜单快捷方式将控制台固定到任务栏。

- Windows 2016 中存在的已知问题导致您无法在 Windows 2016 中搜索自助服务密码重置控制台。 [#648939]

  解决方法：使用**开始**菜单查找自助服务密码重置。

- 如果默认管理策略中的密码策略中的最短密码存在期限为默认值（1 天），并且您的用户尝试重置其密码但重置失败（例如，不满足复杂性要求），则当其关闭密码重置向导后，24 小时内将无法再次重置密码。 [#653221]

- 使用 Citrix Receiver for Mac 时，注册对应的任务按钮在用户首次登录 StoreFront 时显示。 注销 StoreFront 并重新登录后，任务按钮不显示。 [#657263]

  解决方法：
  1. 在 StoreFront 应用商店中单击右上角的用户名。
  2. 单击下拉菜单中的**刷新应用程序**按钮。
  3. 关闭 Citrix Receiver for Mac，重新打开，此时将显示任务按钮。

- 将安全问题从 Single Sign-On 身份验证迁移到自助服务密码重置时，这些问题可能不会在自助服务密码重置控制台中显示，即使在单击**刷新**后也不显示。 [#657277]

  解决方法：关闭控制台并重新打开。

- 调查表中包含特殊字符 **&** 的安全问题在注册过程中不在 StoreFront 中显示。 [#654913]

  解决方法：不在安全问题中包括 **&**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

系统要求

Dec 08, 2016

> **Important**
>
> Citrix 不支持在域控制器上安装任何自助服务密码重置组件。 请在专用服务器上部署自助服务密码重置组件。

本文介绍了您的自助服务密码重置环境的硬件和软件要求。 本文假定每台计算机都满足所安装的操作系统的最低硬件要求。

软件

您的自助服务密码重置环境中的计算机可能需要安装以下支持系统软件。

- **Windows 2016、Windows 2012 R2、Windows 2008 R2**（我们建议仅对本地文件共享以及恰当的额外锁定使用 Windows 2008 R2。 有关详细信息，请参阅创建中央存储。）- 自助服务密码重置服务器要求安装。
- **Microsoft Windows Installer 2.0 或更高版本** - 所有组件都要求安装。
- **Microsoft .NET Framework** - 自助服务密码重置服务器要求安装。
  - 4.6.x (Windows 2016)
  - 4.5.2 (Windows 2012 R2)
  - 3.5.1 (Windows 2008 R2)
- **Internet Information Services (IIS)** - 自助服务密码重置服务器要求安装。
  - IIS 10.0 (Windows 2016)
  - IIS 8.5 (Windows 2012 R2)
  - IIS 7.5 (Windows 2008 R2)

自助服务密码重置服务器

- 自助服务密码重置组件 - 中央存储
- 支持的环境 - SMB 文件共享
- 硬件要求 - 每个用户 30 KB 磁盘空间

ASP.NET 3.5/4.X 要求

适用于您的 Windows Server 计算机上安装的 .NET Framework 版本的 ASP.NET 组件。

安全性和帐户要求

安装自助服务密码重置服务之前，请确保恰当的帐户和组件可用于支持该服务。 此外，由于服务使用 HTTP (HTTPS)，因此，需要安装服务器身份验证证书，传输层安全性 (TLS) 才能与 StoreFront 进行通信。

服务器身份验证要求：

安装此服务之前，请从证书颁发机构 (CA) 或者您的内部公钥基础结构 (PKI)（如果可用）获取用于进行 TLS 通信的服务器身份验证证书。

服务模块所需的帐户：

注意：请确保两个帐户都未过期。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

自助服务密码重置服务在您的环境中运行过程中需要使用以下帐户类型来读取和写入数据：

- 数据代理帐户
- 自助服务帐户

如果不同的模块需要相同的帐户类型，可以对多个模块使用同一帐户，也可以为每个模块指定不同的自定义帐户。

- **数据代理帐户**

  需要对中央存储具有读取和写入权限。 有关详细信息，请参阅创建中央存储。

- **自助服务帐户**

  需要足够的权限才能在用户配置中解锁和重置相关用户的密码。 有关详细信息，请参阅安全配置。

StoreFront

StoreFront 3.7

Citrix Receiver

支持：

- Citrix Receiver for Web
- Citrix Receiver for Windows
- Citrix Receiver for Linux

不支持：

- Citrix Receiver for Mac
- Citrix Receiver for Chrome
- 移动设备（即使安装了 Receiver for Web 也不受支持）

在外部与 NetScaler Gateway 结合使用

不受支持

© 1999-2017 Citrix Systems, Inc. All rights reserved.

安装和配置

Sep 19, 2016

本文包含以下部分：

安装和配置清单

开始安装之前，请完成以下列表中的步骤：

✓	步骤
	选择您的环境中要在其中安装软件的计算机并将其准备好进行安装。 请参阅系统要求。
	安装服务所需的 TLS 证书和帐户。 请参阅系统要求中的*安全性和帐户要求*。
	安装许可证服务器。 请参阅许可证服务器文档。
	创建中央存储。 请参阅创建中央存储。
	安装自助服务密码重置。 请参阅安装和配置自助服务密码重置。
	使用控制台配置自助服务密码重置。 请参阅安装和配置自助服务密码重置。
	在 StoreFront 上配置自助服务密码重置。 请参阅配置 StoreFront。
	确保自助服务密码重置配置已安全配置。 请参阅安全配置一文。

安装服务所需的 SSL 证书和帐户。 请参阅"安全性和帐户要求"。

安装服务所需的 SSL 证书和帐户。 请参阅"安全性和帐户要求"。

在 StoreFront 上配置自助服务密码重置。 请参阅配置 StoreFront。

安装和配置顺序

要安装此服务并运行服务配置向导，您的登录帐户必须是域用户，并且属于服务器上的本地管理员组。

我们建议您按以下顺序安装自助服务密码重置：

1. 安装许可证服务器或将其升级到最低版本 11.13.1.2。 请从 https://www.citrix.com/downloads/licensing.html 下载许可证服务器。
2. 创建中央存储。
3. 安装自助服务密码重置。
4. 在控制台中配置自助服务密码重置。
5. 使用自助服务密码重置服务器的地址配置 StoreFront。

创建中央存储

出于安全原因，我们建议您直接在运行自助服务密码重置服务的计算机上创建中央存储。 对于需要多个自助服务密码重置服务器的部署，如果自助服务密码重置服务器和托管共享的服务器都支持 SMB 加密，则可以将中央存储托管在远程网络共享上。

此功能仅在 Windows Server 2012 R2 或 Windows Server 2016 中可用，因此，使用远程文件共享作为中央存储时不支持 Windows Server 2008 R2。

创建数据代理帐户

创建一个要用作数据代理帐户的常规域用户。 请勿将域管理员/本地管理员组中的用户设置为数据代理帐户。

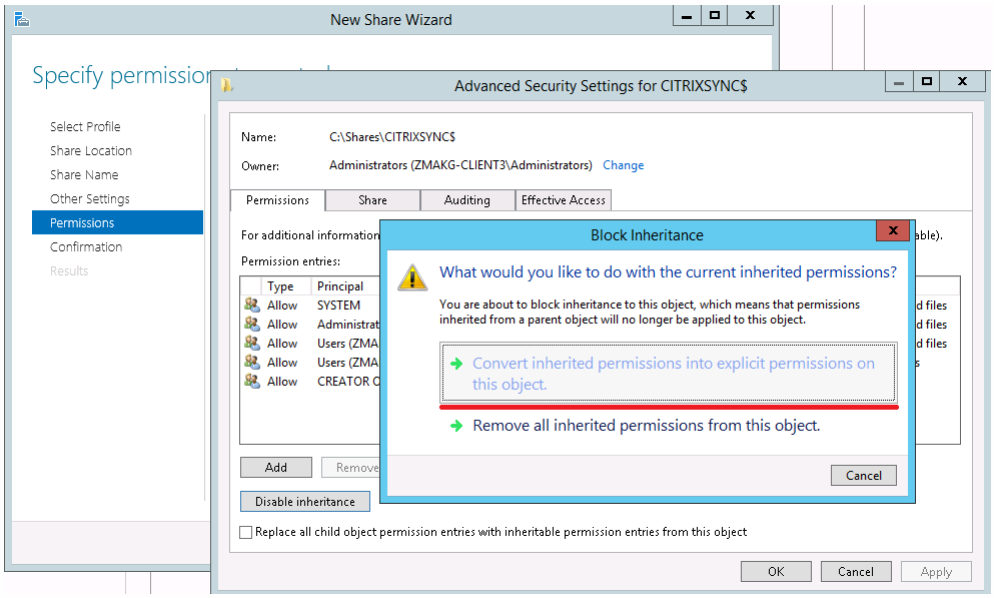
为 Windows Server 2012 R2 或 Windows Server 2016 创建中央存储

为自助服务密码重置服务器和中央存储使用 Windows Server 2012 R2 或 Windows Server 2016 时，如果按照本部分中的说明进行配置，则可以使用远程网络共享。 请务必选中 **Encrypt data access**（加密数据访问）并应用安全配置中提供的指南。

1. 要启动 **New Share**（新建共享）向导，请打开服务器管理器。 在 **File and Storage Services**（文件和存储服务）详细信息页面上，在左侧窗格中选择 **Shares**（共享），然后单击 **Tasks（任务）> New Share（新建共享）**。
2. 在左侧窗格中选择 **Select Profile**（选择配置文件），选择 **SMB Share - Quick**（SMB 共享 - 快速），然后单击 **Next**（下一步）。
3. 在左侧窗格中选择**共享位置**。 从列表中选择要在上面创建新共享的服务器以及要在上面创建新共享文件夹的卷，然后单击**下一步**。
4. 在左侧窗格中选择 **Share Name**（共享名称），键入新共享名称，例如 **CITRIXSYNC$**，然后单击 **Next**（下一步）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

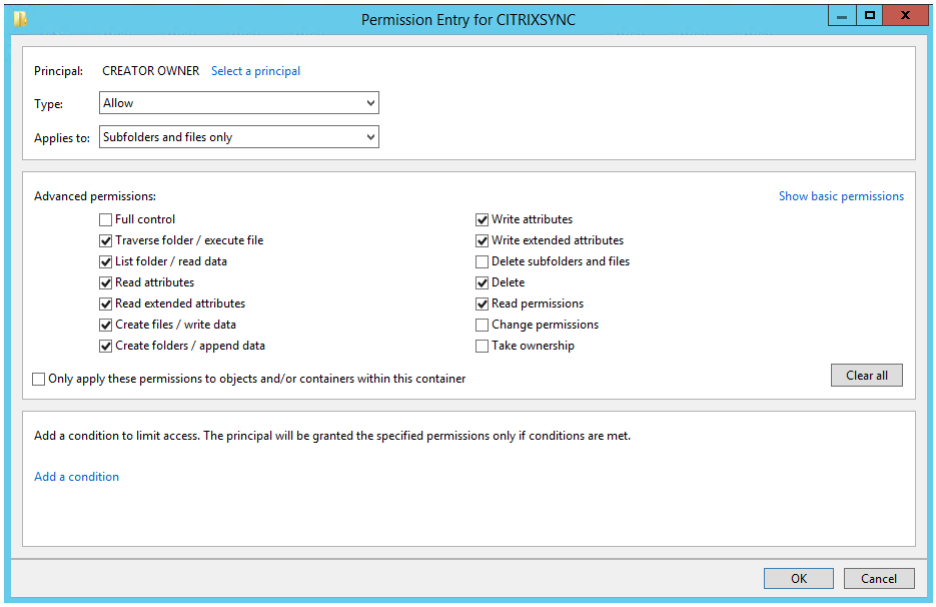
5. 在左侧窗格中选择 **Other Settings**（其他设置），选择 **Encrypt data**（加密数据），取消选中 **Allow caching of share**（允许缓存共享），然后单击 **Next**（下一步）。
6. 要自定义 **Share**（共享）权限，请在左侧窗格中选择 **Permissions**（权限），然后选择 **Customize permissions（自定义权限）> Share（共享）**。
   - o 删除**"Everyone"（所有人）**
   - o 添加具有"Full Control"（完全控制）权限的 **Data Proxy Account**（数据代理帐户）
   - o 添加具有"Full Control"（完全控制）权限的 **Local Administrators**（本地管理员）
   - o 添加具有"Full Control"（完全控制）权限的 **Domain Admins**（域管理员）
   - o 添加对本地文件共享具有"Read"（读取）权限的 **Network Service**（网络服务）
7. 要自定义 NTFS 权限，请在左侧窗格中选择 **Permissions**（权限），选择 **Customize permissions**（自定义权限），单击 **Disable inheritence**（禁用继承），然后选择 **Convert inherited permissions into explicit permissions on this object**（将已继承的权限转换为此对象的显式权限）。



8. 要删除除 **CREATOR OWNER/Local Administrators/SYSTEM**（创建者所有者/本地管理员/系统）外的所有用户，请在 **Customize permissions**（自定义权限）> **Permissions**（权限）中，单击 **Remove**（删除）。

9. 要修改 **CREATOR OWNER**（创建者所有者）> **Advanced permissions**（高级权限），请单击 **Edit**（编辑）并取消选中以下权限：

- o Full Control（完全控制）
- o Delete subfolders and files（删除子文件夹和文件）
- o Change permissions（更改权限）
- o Take ownership（获取所有权）



10. 添加具有"Full Control"（完全控制）权限的 **Data Proxy Account**（数据代理帐户）

11. 添加对本地文件共享具有"Read"（读取）权限的 **Network Service**（网络服务）

12. 在"New Share"（新建共享）向导的左侧窗格中选择 **Confirmation**（确认），检查当前选中的共享设置，单击 **Create**（创建）开始执行创建新文件夹的过程，然后单击 **Close**（关闭）。

13. 在 **CITRIXSYNC$** 共享文件夹下创建两个子文件夹 **CentralStoreRoot** 和 **People**。

重要：请确保数据代理帐户对这两个子文件夹具有 **Full Control**（完全控制）权限。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

为 Windows Server 2008 R2 创建中央存储

请务必在安装了自助服务密码重置服务的同一服务器上创建中央存储，然后继续配置 Windows 防火墙以阻止远程访问。

1. 创建一个本地文件夹 (**CITRIXSYNC1**) 作为文件共享的根目录，然后创建两个子文件夹 **CentralStoreRoot** 和 **People**。

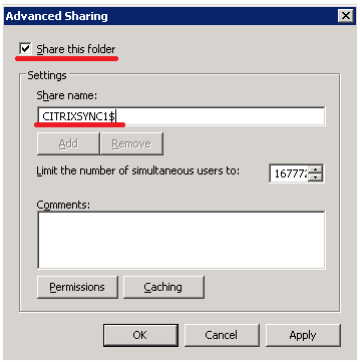
2. 设置一个文件共享并授予共享权限：

    a. 右键单击 **CITRIXSYNC1** 文件夹，选择 **Properties（属性）> Sharing（共享）> Advanced Sharing（高级设置）**。

    b. 选中 **Share this folder**（共享此文件夹）复选框，然后将 **Share name**（共享名称）设置为 **CITRIXSYNC1$**。

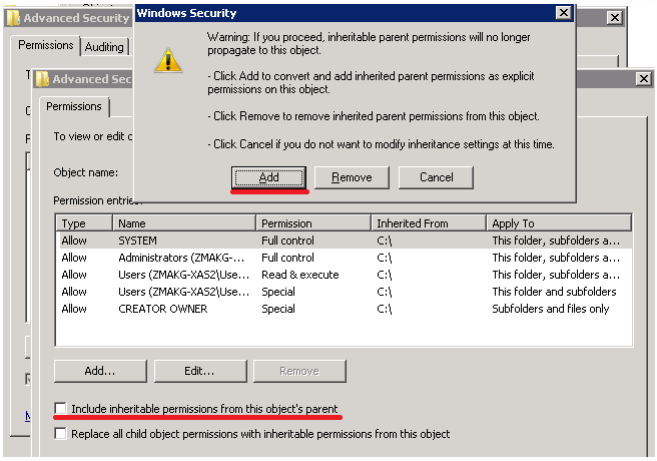
    c. 要授予共享权限，请单击 **Permissions**（权限），删除所有默认用户，然后添加具有 **Full Control**（完全控制）权限的 **Data Proxy Account**（数据代理帐户），具有 **Full Control**（完全控制）权限的 **Local Administrators Group**（本地管理员组），具有 **Full Control**（完全控制）权限的 **Domain Admin Group**（域管理员组），以及具有 **Read**（权限）的 **Network Service**（网络服务）。

    d. 单击 **Caching**（缓存）并选中 **No files or programs from the shared folder are available offline**（该共享文件夹中的文件或程序在脱机状态下不可用）。



3. 要授予安全权限，请右键单击 **CITRIXSYNC1** 文件夹，然后选择 **Properties**（属性）> **Security**（安全）。

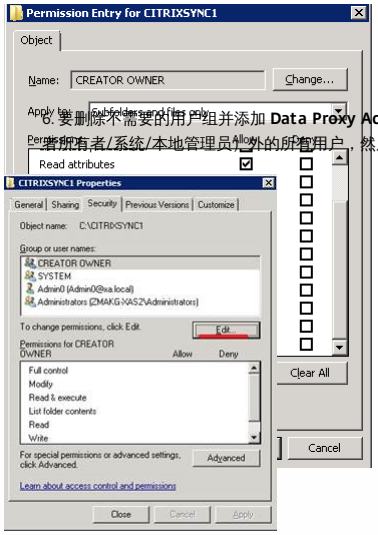
4. 要禁用可继承的权限，请单击 **Advanced**（高级）> **Change Permissions**（更改权限），取消选中 **Include inheritable permissions from the object's parent**（包括该对象的父对象中的可继承权限），然后在警告窗口中单击 **Add**（添加）。



5. 单击 **Edit**（编辑）修改 **CREATOR OWNER**（创建者所有者）权限，并取消选中以下权限：

    o Full Control（完全控制）
    o Delete subfolders and files（删除子文件夹和文件）
    o Change permissions（更改权限）
    o Take ownership（获取所有权）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

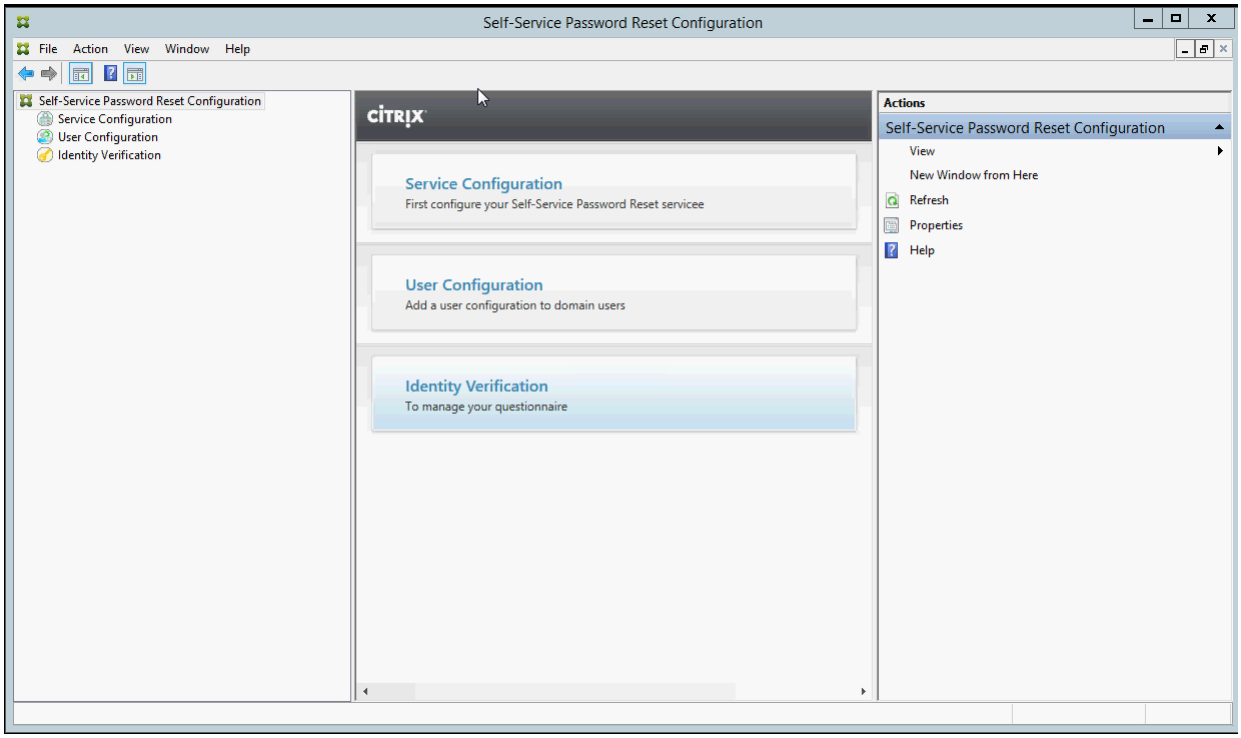


6. 要删除不需要的用户组并添加 **Data Proxy Account**（数据代理帐户），请在 **Properties**（属性）屏幕上单击 **Edit**（编辑），并删除除 **CREATOR OWNER/SYSTEM/Local Administrators**（创建者所有者/系统/本地管理员）外的所有用户，然后添加具有 **Full Control**（完全控制）权限的 **Data Proxy Account**（数据代理帐户）。
7. 添加具有 **Read**（读取）权限的 **Network Service**（网络服务）。
8. 要启用 SMB 签名功能，请单击**开始 > 管理工具 > 本地安全策略**。 在左侧窗格中，选择**安全设置 > 本地策略 > 安全选项**。
9. 启用 **Microsoft 网络客户端: 对通信进行数字签名(如果服务器允许)** 和 **Microsoft 网络服务器: 对通信进行数字签名(如果客户端允许)**。
10. 要阻止远程访问本地中央存储，请完成 Windows 防火墙配置。 有关详细信息，请参阅配置防火墙设置。

安装和配置自助服务密码重置

安装包位于 XenApp 和 XenDesktop 安装介质中。

1. 启动自助服务密码重置安装向导并按照以下步骤进行操作。
2. 依次单击**开始 > 程序 > Citrix > Citrix 自助服务密码重置配置**以配置自助服务密码重置服务。
3. 控制台打开时，请按照下面三个基本步骤配置此服务。



服务配置

配置此服务之前，请确保您已创建中央存储、数据代理帐户和自助服务帐户。

1. 在中间窗格中选择**服务配置**，然后在右侧窗格中单击**新建服务配置**。
2. 在**中央存储位置**屏幕中，指定中央存储位置，然后单击**下一步**。
3. 在**域配置**屏幕中，选择一个域，然后单击**属性**。
4. 指定**数据代理帐户**用户名和密码以及**自助服务帐户**用户名和密码，然后依次单击**确定**、**下一步**和**完成**。

用户配置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. 在左侧窗格中选择**用户配置**，然后在右侧窗格中单击**新建用户配置**。
2. 在**命名用户配置**屏幕中，定义自助服务密码服务目标用户组，从 Active Directory 中添加用户/组/OU，然后单击**下一步**。
3. 在**配置许可**屏幕上，指定许可证服务器，然后单击**下一步**。
4. 在**配置密码重置**屏幕上，使用复选框指定用户是否能够在没有管理员介入的情况下重置其 Windows 密码和解锁其域帐户，指定服务端口和地址，然后单击**创建**。

有关管理用户配置的详细信息，请参阅管理用户配置。

身份验证

1. 在左侧窗格中选择**身份验证**节点，然后在右侧窗格中单击**管理问题**。
2. 在**基于问题的身份验证**屏幕上，选择默认语言，使用复选框启用或禁用屏蔽安全问题答案的功能，然后单击**下一步**。
3. 在**安全问题**屏幕上，单击**添加问题**，在文本框中键入问题，单击**确定**，然后单击**下一步**。
4. 在**调查表**屏幕中，单击**添加**并选择一个问题。 可以使用**上移**和**下移**按钮重新整理您的问题和问题组。 完成此页面上的操作后，单击**创建**和**确定**。

有关管理身份验证问题的详细信息，请参阅管理身份验证问题。

管理用户配置

通过用户配置，您可以控制用户登录 StoreFront 时界面的行为和外观。 创建新用户配置是您在向环境中的用户分发自助服务密码重置之前执行的最后一个步骤。 请注意，您可以随时退出现有用户配置。

用户配置是您对与 Active Directory 层级结构（组织单位 [OU] 或单个用户）或 Active Directory 组相关联的用户应用的唯一设置集合。

用户配置由以下各项组成：

- 与 Active Directory 域层级结构（OU 或单个用户）或 Active Directory 组相关联的用户

重要：处于 Active Directory 混合模式的通讯组和域本地组不受支持。

- 许可证服务器
- 自助服务功能（帐户解锁和密码重置）

创建用户配置之前，请确保您已创建或定义以下各项：

- 中央存储
- 服务配置

创建用户配置

1. 依次单击**开始** > **所有程序** > **Citrix** > **Citrix 自助服务密码重置配置**。
2. 在左窗格中，选择**用户配置**节点。
3. 在**操作**菜单中，单击**添加新用户配置**。

添加用户、OU 或组

用户配置向导的**命名用户配置**页面允许您将用户配置关联到用户。

用户配置关联：

您有两种选项：根据 Active Directory 层级结构（OU 或单个用户）或 Active Directory 组关联用户。 如有需要，以后可以通过单击**操作**菜单中的**编辑用户配置**将用户配置与其他层级结构或组相关联。

将用户配置与组相关联仅在使用 Active Directory 身份验证的 Active Directory 域中受支持。

在**命名用户配置**页面上选择 OU、用户或组（从“添加新用户配置”或“编辑用户配置”向导中）。

注意：我们建议您不要将任何特权帐户（例如，本地管理员或域管理员）包括在自助服务密码重置帐户能够重置其密码的用户组中。 请使用新的专用组。

配置许可

用户配置向导的**配置许可**页面允许您配置自助服务密码重置服务使用的许可证服务器。

注意：仅当您安装了 XenApp 或 XenDesktop Platinum Edition 时才能使用解锁和重置功能。

在**配置许可**页面上输入许可证服务器名称和端口号（从“添加新用户配置”或“编辑用户配置”向导中）。

启用解锁或重置功能

自助服务密码重置允许用户在没有管理员介入的情况下重置其 Windows 密码以及解锁其域帐户。 在**启用自助服务密码重置**页面上，可以选择要启用的功能。

在**启用自助服务密码重置**页面上选择希望用户使用的功能：**解锁**或**重置**（从“添加新用户配置”或“编辑用户配置”向导中）。

管理身份验证问题

Citrix 自助服务密码重置配置控制台的身份验证向您提供了一个用于管理与身份验证、自助服务密码重置和帐户解锁相关联的所有安全问题的中央位置。 可以在默认问题列表中自定义您自己的安全问题以及创建问题组。

- 如果您在用户注册其答案后编辑现有的默认问题，请注意所编辑的问题的含义。 编辑问题不会强制用户重新进行注册，但是，如果您更改了问题的含义，最初回答该问题的用户可能无法提供正确的答案。
- 在注册用户后添加、删除和替换安全问题意味着以前使用较旧的一组问题注册的所有用户在重新注册之前将无法进行身份验证和重置密码。 用户在 Receiver 中打开“任务”时必须回答一组新问题。
- 单个安全问题可以属于多个安全问题组。 创建安全问题组时，创建的所有问题都可在任何安全问题组中使用。

请按照以下步骤进行操作，访问以下过程中引用的设置：

1. 依次单击**开始** > **所有程序** > **Citrix** > **Citrix 自助服务密码重置配置**。
2. 在左窗格中，选择**身份验证**节点。
3. 在**操作**菜单中，单击**管理问题**。

设置默认语言

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在大多数情况下，用户会看到安全问题使用与其当前用户配置文件关联的语言显示。 如果该语言不可用，自助服务密码重置将使用您指定的默认语言显示问题。

1. 依次单击**开始** > **所有程序** > **Citrix** > **Citrix 自助服务密码重置配置**。
2. 在左窗格中，选择**身份验证**节点。
3. 在**操作**菜单中，单击**管理问题**。
4. 在**基于问题的身份验证**页面上的**默认语言**下拉列表中，选择默认语言。

启用安全答案屏蔽

安全答案屏蔽功能在您的用户注册其安全问题答案或在身份验证过程中提供答案时增加了用户的安全级别。 启用此功能时，用户的答案被隐藏。 答案注册过程中，系统会要求这些用户键入其答案两次以避免出现键入和拼写错误。 身份验证过程中用户仅键入其答案一次，因为系统会在出现错误时提示其重试。

在**基于问题的身份验证**页面上选择**屏蔽安全问题的答案**。

创建新安全问题

可以创建多个不同的问题并为每个问题指定一种语言。 还可以提供一个问题的多种翻译。 Receiver 中的注册会使用与用户的配置文件的语言设置相对应的语言向用户提供调查表。 如果该语言不可用，自助服务密码重置将使用默认语言显示问题。

注意：指定安全问题的语言时，问题将向操作系统设置是针对该指定语言配置的用户显示。 如果选定的操作系统设置与任何可用的问题不匹配，则向用户显示您所选择的默认语言。

1. 在**安全问题**页面上的**语言**下拉列表中，选择一种语言并单击**添加问题**。 此时将显示“安全问题”对话框。
2. 在**安全问题**对话框中创建新问题。

重要：必须使用**编辑**按钮将所翻译的现有问题的文本包括在内。 如果选择**添加问题**，您将创建与原始问题不关联的新问题。

添加或编辑现有问题的文本

在注册用户后添加、删除和替换安全问题意味着以前使用较旧的一组问题注册的所有用户在重新注册之前将无法进行身份验证和重置密码。 用户在 Receiver 中打开“任务”时必须回答一组新问题。 编辑问题不会强制用户重新注册。

重要：如果要编辑现有问题，请务必不要改变问题的含义。 这可能会导致重新身份验证过程中用户答案中出现不一致。 即，用户可能会提供与存储的答案不匹配的其他答案。

1. 从**安全问题**页面上的**语言**下拉框中选择一种语言。
2. 选择问题并单击**编辑**。
3. 编辑**安全问题**对话框中的问题。

创建安全问题组

可以创建多个用户在确认其身份时需要回答的安全问题。 添加到调查表中的每个问题必须由您的用户回答。 但是，您还可以将这些问题编组到一个安全问题组中。

例如，将问题放置到组中可使您能够向调查表中添加一组六个问题，并且允许您的用户从该问题组中选择回答其中的三个问题（举例说明）。 这使您的用户能够灵活地选择问题和提供用于身份验证的答案。

1. 在**安全问题**页面上单击**添加组**。
2. 在**安全问题组**对话框中，命名该组，选择问题，然后设置用户必须回答的问题数量。

编辑安全问题组

选择要编辑的安全组，然后单击**安全问题**页面上的**编辑**。 此时将显示“安全问题组”对话框，其中包含可作为安全问题组的一部分的安全问题列表。 当前在组中的问题通过复选标记指示。 您可以在此编辑组的名称、向组中添加问题以及选择此组中用户必须回答的问题数量。

添加或删除现有调查表

在调查表中添加或删除安全问题和问题组。 按照要向用户显示的顺序上下移动问题。 如果更改了调查表，需要通知用户在登录 StoreFront 后执行重新注册任务。

1. 单击**调查表**页面上的**添加**可向调查表中添加问题或组。
2. 单击**删除**可从调查表中删除问题。
3. 单击**上移**或**下移**可管理向用户提供的问题。

管理身份验证

通过自助服务密码重置，您可以执行以下操作：

- 导入或导出安全问题。
- 吊销对用户的安全问题注册。

导入或导出安全问题

可以导入或导出安全问题和组的数据。

1. 依次单击**开始** > **所有程序** > **Citrix** > **Citrix 自助服务密码重置配置**。
2. 在左窗格中，选择**身份验证**节点。
3. 在**操作**菜单中，单击以下操作之一：

导入安全问题
指定文件位置以导入安全问题和组的数据。

导出安全问题
指定文件位置以导出安全问题和组的数据。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

安全

Sep 19, 2016

本文包含确保安全部署和配置自助服务密码重置组件需要执行的过程。

- 配置 Internet Information Services (IIS) 设置
- 创建具有重置用户密码和解锁用户帐户权限的域用户帐户
- 配置防火墙设置

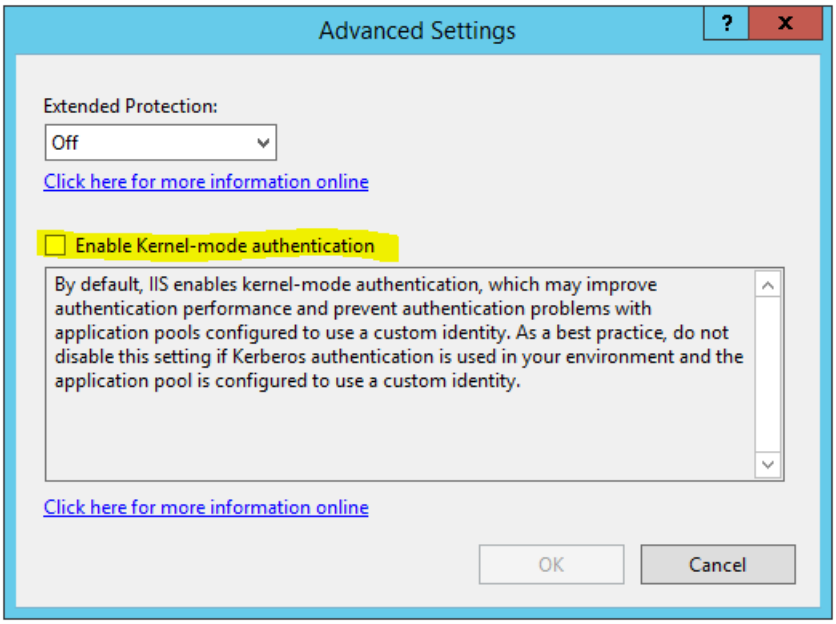
配置 Internet Information Services (IIS) 设置

请应用以下过程，以确保安全配置 IIS MPMService 站点。

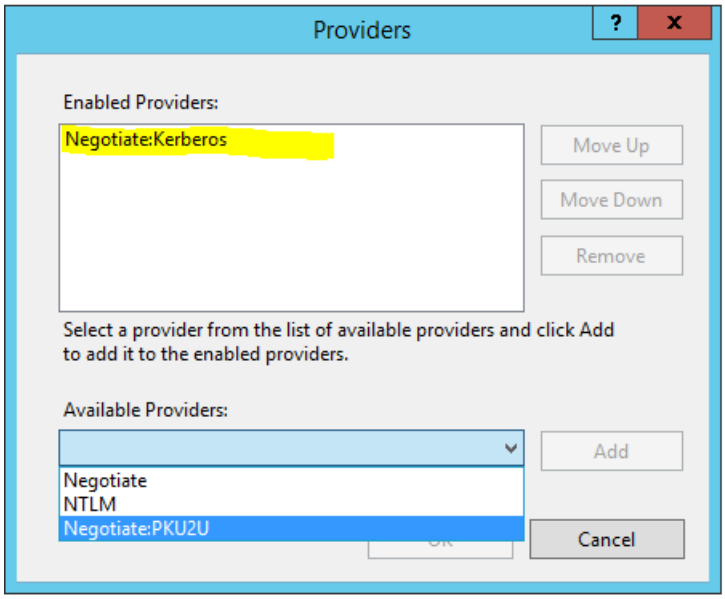
1. 安装自助服务密码重置服务后，在 IIS 管理器中单击 Web 站点 **MPMService**。 在**身份验证**中，依次选择 **Windows 身份验证**、**高级设置**和**提供程序**。

    a. 如果启用了内核模式身份验证，Kerberos 服务票证解密将失败。 要为站点设置 Kerberos，请不要在“高级设置”屏幕中选中“启用内核模式身份验证”以支持 Kerberos。

    b. 在“提供程序”屏幕中，从“可用提供程序”部分中添加 Negotiate:Kerberos。 请从“已启用提供程序”列表中删除所有其他提供程序。



© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 在 IIS 管理器的左侧窗格中，单击 Web 站点 **MPMService**。 在 **SSL 设置**中，启用**要求 SSL**。

创建自助服务帐户

如果要使用自助服务密码重置的密码重置或帐户解锁功能，请在服务配置过程中指定自助服务模块用于执行密码重置和帐户解锁操作的自助服务帐户。 请确保该帐户具有足够的权限，但我们不建议您使用域管理员组中的帐户进行生产部署。 建议授予的帐户权限如下：

- 域成员
- 相关域用户的密码重置和帐户解锁权限

在 **Active Directory 用户和计算机**中，创建要具有重置用户密码和解锁用户帐户权限的组或用户帐户。

1. 在 **Active Directory 用户和计算机**中，右键单击域，然后在菜单中单击**委派控制**。
2. 此时将显示**控制委派**向导。 在**欢迎**对话框中，单击**下一步**。
3. 在**用户和组**对话框中，单击**添加**。 在列表中选择要向其授予解锁帐户权限的组，然后单击**确定**。 在**用户和组**对话框中，单击**下一步**。
4. 在**要委派的任务**对话框中，单击**创建自定义任务去委派**，然后单击**下一步**。
5. 在 **Active Directory 对象类型**对话框中，单击“只是在这个文件夹中的下列对象”>“用户对象”，然后单击**下一步**。
6. 在**权限**对话框中，选中**常规**和**特定属性**对话框。 在**权限**列表中，选中**读取 lockoutTime**、**写入 lockoutTime**、**重置密码**、**更改密码**、**读取 userAccountControl**、**写入 userAccountControl**、**读取 pwdLastSet** 和**写入 pwdLastSet** 复选框，然后单击**下一步**。
7. 在**完成控制委派**向导对话框中，单击**完成**。

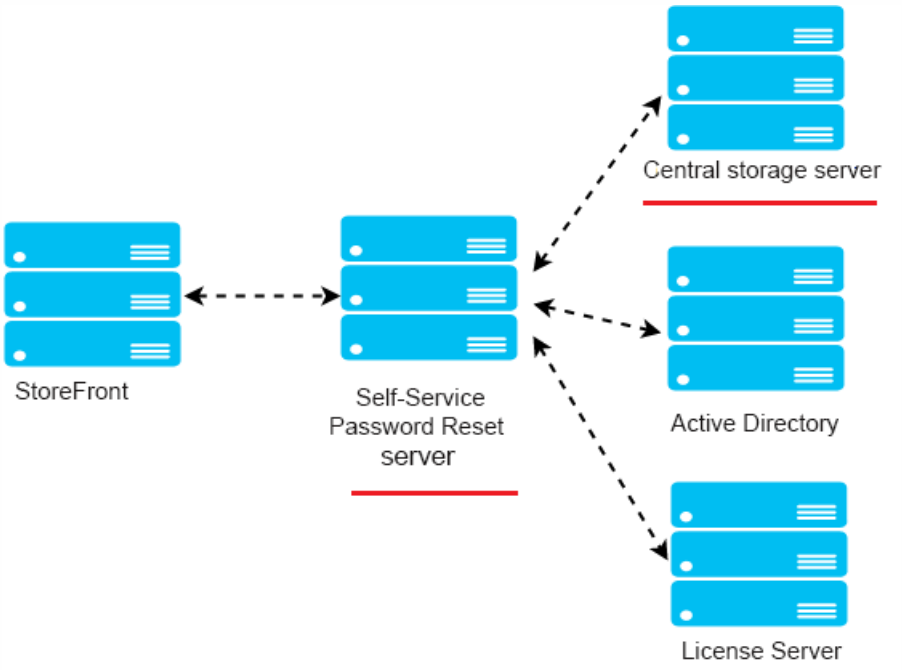
配置防火墙设置

由于自助服务密码重置服务器和中央存储服务器组件负责管理用户密码，因此，我们强烈建议您在可信网络中部署这些组件，并且这些组件只能由特定的可信组件进行访问。 本部分内容介绍了确保您为这些服务器正确配置 Windows 防火墙需要执行的步骤。 我们还建议您配置现有网络基础结构，以确保将这些服务器与不可信网络流量隔离开来。

在部署中完成这些配置后，只能使用服务器消息块 (SMB) 从自助服务密码重置服务器访问自助服务密码重置中央存储服务器，并且只能通过 HTTPS 连接从 StoreFront 服务器访问自助服务密码重置服务器。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

面向 Windows 2012 R2 的远程文件共享部署



环境

- 请在专用服务器上部署自助服务密码重置组件。 请勿将这些组件与现有 StoreFront 或 Delivery Controller 组件部署在相同的服务器上，否则，下面显示的防火墙配置可能会阻止 StoreFront 或 Controller 流量。
- StoreFront 与自助服务密码重置服务器之间不存在非透明 HTTP/HTTPS 代理。

  如果 StoreFront 与自助服务密码重置服务器之间存在任何非透明代理，请在防火墙规则中将自助服务密码重置服务器配置为只能从代理服务器访问。

- 这些过程中的配置建立在 Windows 默认防火墙规则的基础之上。

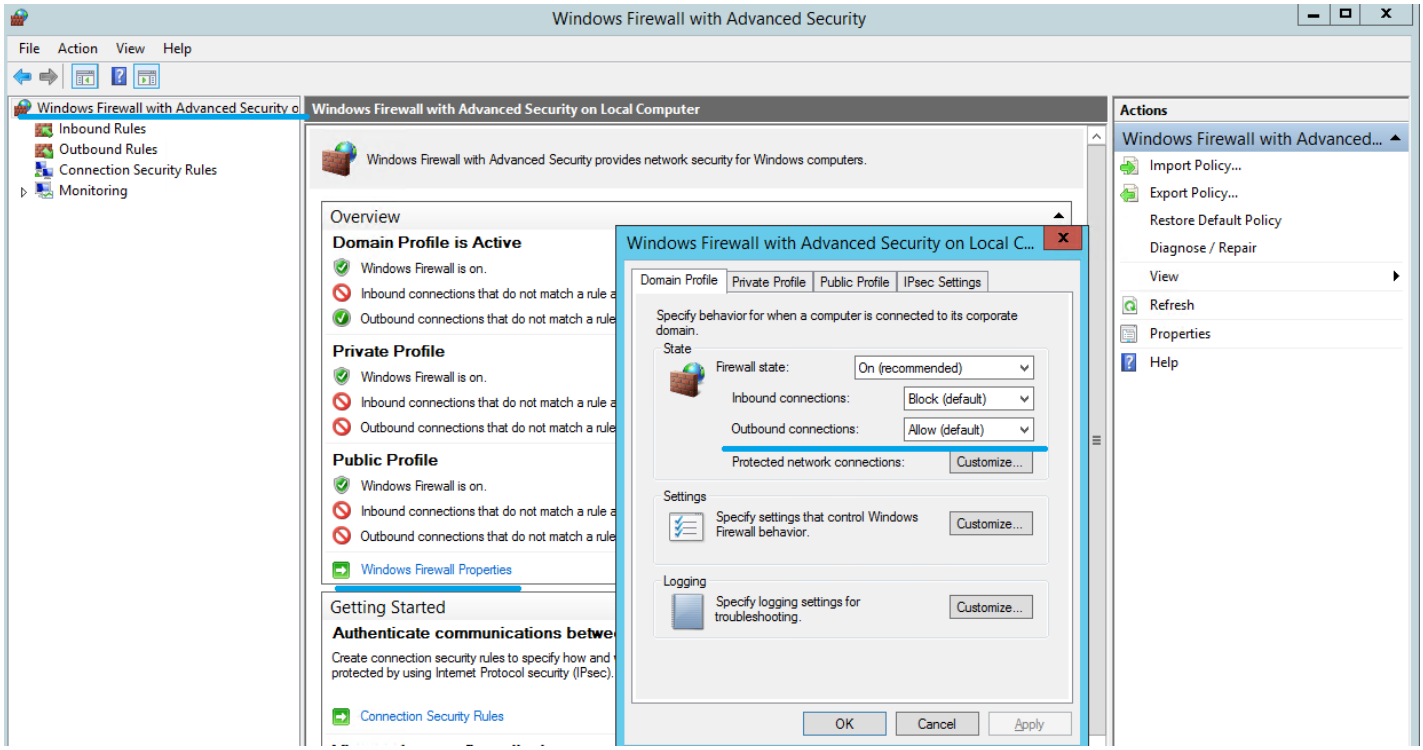
为自助服务密码重置中央存储配置防火墙

完成配置后，自助服务密码重置中央存储提供的 SMB 服务在入站上只能从自助服务密码重置服务器访问，并且自助服务密码重置中央存储服务器在出站上只能访问企业网络上的服务。

1. 打开服务器管理器，并从顶部导航栏上的**工具**菜单中选择**高级安全 Windows 防火墙**。

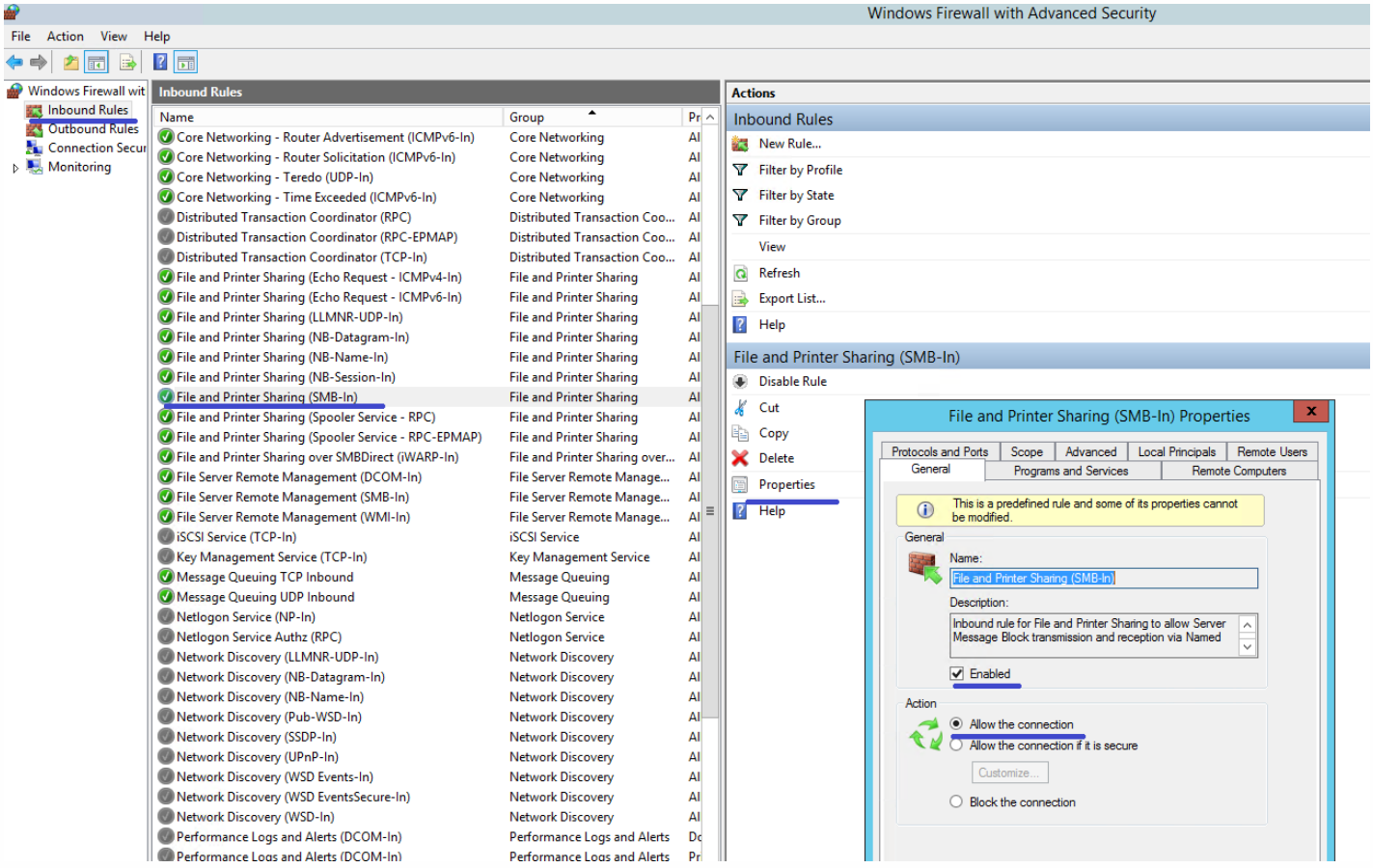
2. 在**高级安全 Windows 防火墙**中，选择中央窗格中的 **Windows 防火墙属性**。 有三个防火墙配置文件，即域配置文件、专用配置文件和公用配置文件。 选择**域配置文件**选项卡。 请务必将**防火墙状态**设置为**开**，将**入站连接**设置为**阻止**，将**出站连接**设置为**允许**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 选择**专用配置文件**和**公用配置文件**选项卡，并且务必将**防火墙状态**设置为**开**，将**入站连接**和**出站连接**设置为**阻止**。 应用并保存所做的更改。

4. 在**入站规则**中，选择**文件和打印机共享(SMB-In)**，并且务必将此规则设置为**已启用**，将**操作**设置为**允许连接**。



5. 在**文件和打印机共享(SMB-In)属性**中，更改到**范围**选项卡，选择**这些 IP 地址**，并将所有自助服务密码重置服务器 IP 地

© 1999-2017 Citrix Systems, Inc. All rights reserved.

址添加到列表中。 例如，自助服务密码重置服务器 A (192.168.1.10) 和自助服务密码重置服务器 B (192.168.1.11)。

6. 在**文件和打印机共享(SMB-In)属性**中，更改到**高级**选项卡，选择配置文件**域**、**专用**和**公用**，并保存对此规则所做的更改。

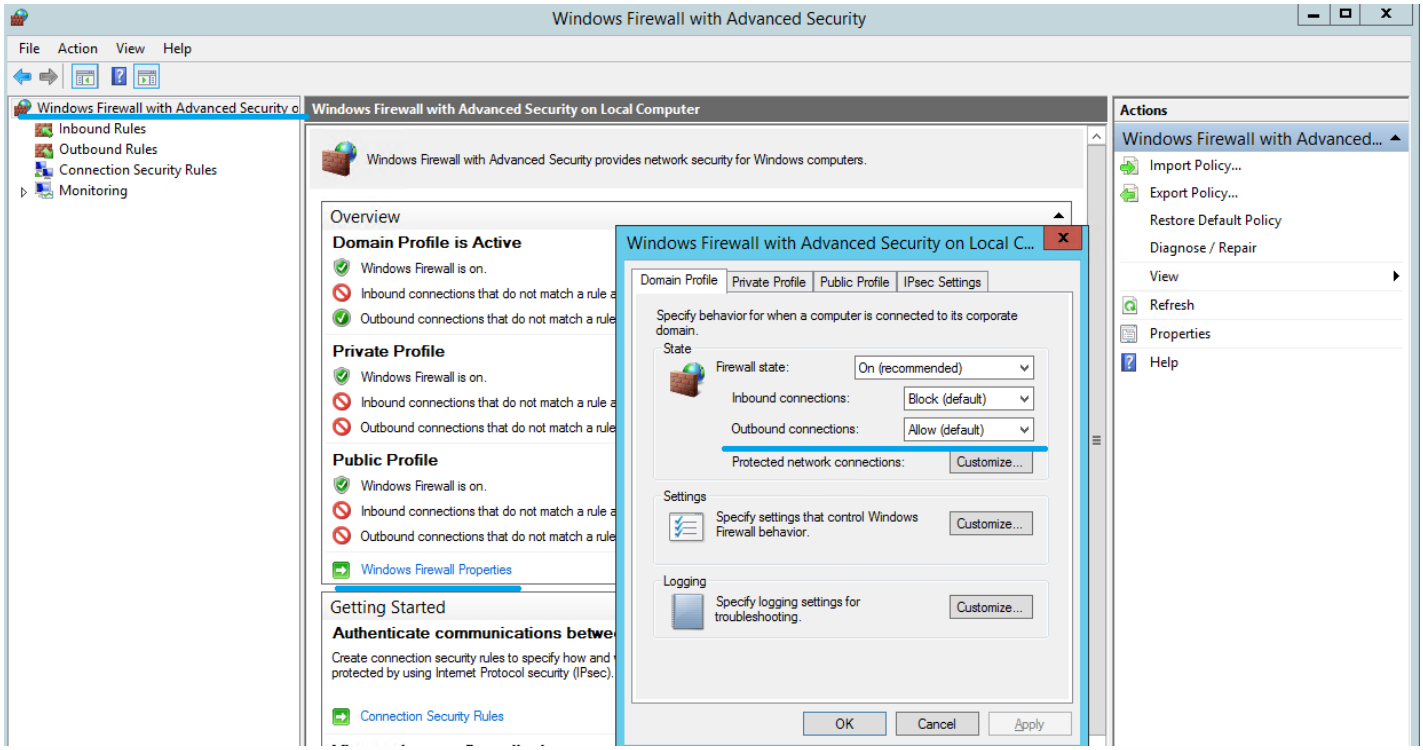
7. 在**文件服务器远程管理(SMB-In)** 和**文件和打印机共享 (NB-Session-In)** 的**入站**规则上重复此步骤。

为自助服务密码重置服务器配置防火墙

完成配置后，自助服务密码重置服务器提供的 Web 服务将只能使用 HTTPS 通过 StoreFront 服务器访问，并且自助服务密码重置服务器只能访问企业网络中的服务。

1. 打开服务器管理器，并从顶部导航栏上的**工具**菜单中选择**高级安全 Windows 防火墙**。

2. 在**高级安全 Windows 防火墙**中，选择中央窗格中的 **Windows 防火墙属性**。 有三个防火墙配置文件，即域配置文件、专用配置文件和公用配置文件。 选择**域配置文件**选项卡。 请务必将**防火墙状态**设置为**开**，将**入站连接**设置为**阻止**，将**出站连接**设置为**允许**。



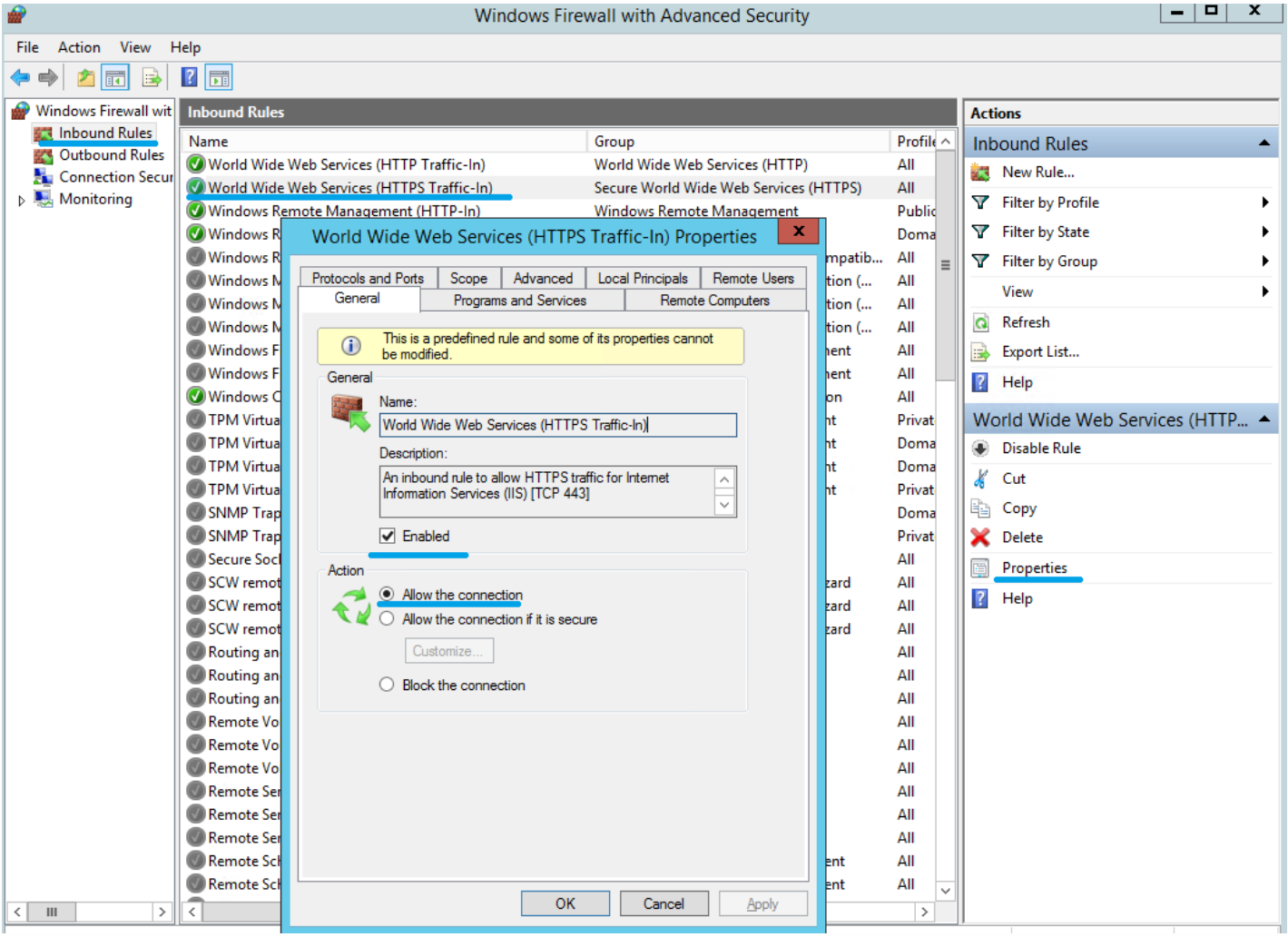
3. 选择**专用配置文件**和**公用配置文件**选项卡，并且务必将**防火墙状态**设置为**开**，将**入站连接**和**出站连接**设置为**阻止**。 应用并保存所做的更改。

4. 在**入站规则**中，选择**万维网服务(HTTP 流入量)**，并且务必将此规则设置为**已启用**，将**操作**设置为**阻止连接**。

5. 在**万维网服务(HTTP 流入量)属性**中，更改到**高级**选项卡，选择配置文件**域**、**专用**和**公用**，并保存对此规则所做的更改。

6. 在**入站规则**中，选择**万维网服务(HTTPS 流入量)**，并且务必将此规则设置为**已启用**，将**操作**设置为**允许连接**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



7. 在**万维网服务(HTTPS 流入量)属性**中，更改到**范围**选项卡，选择**这些 IP 地址**，并将所有 StoreFront 服务器 IP 地址添加到列表中。 例如，StoreFront A (192.168.1.50) 和 StoreFront B (192.158.1.51)。

8. 在**万维网服务(HTTPS 流入量)属性**中，更改到**高级**选项卡，选择配置文件**域**、专用和**公用**，并保存对此规则所做的更改。

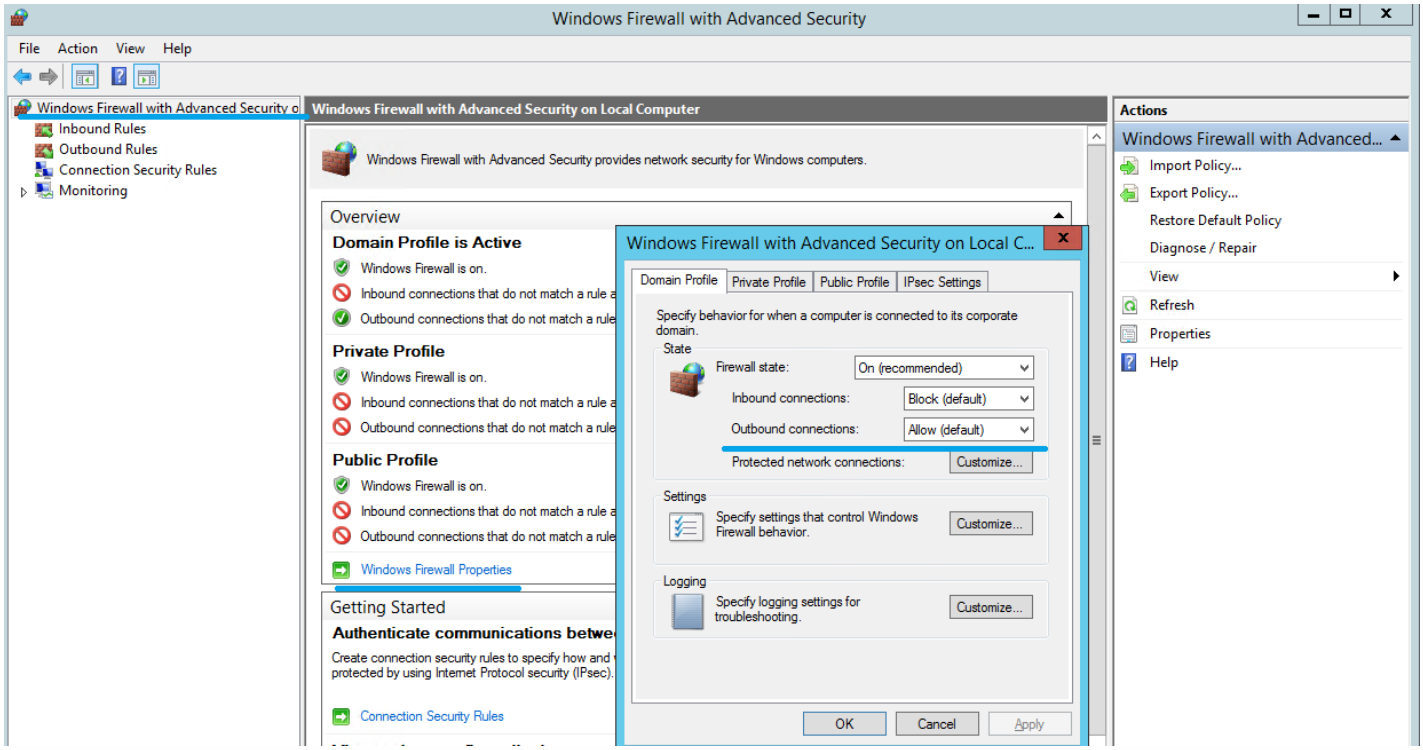
面向 Windows 2008 R2 的本地文件共享部署

完成配置后，将阻止来自远程客户端的任何 SMB 访问。 只能从本地访问 SMB 文件共享，并且只能使用 HTTPS 连接从 StoreFront 服务器访问自助服务密码重置服务。

1. 打开服务器管理器，并从顶部导航栏上的**工具**菜单中选择**高级安全 Windows 防火墙**。

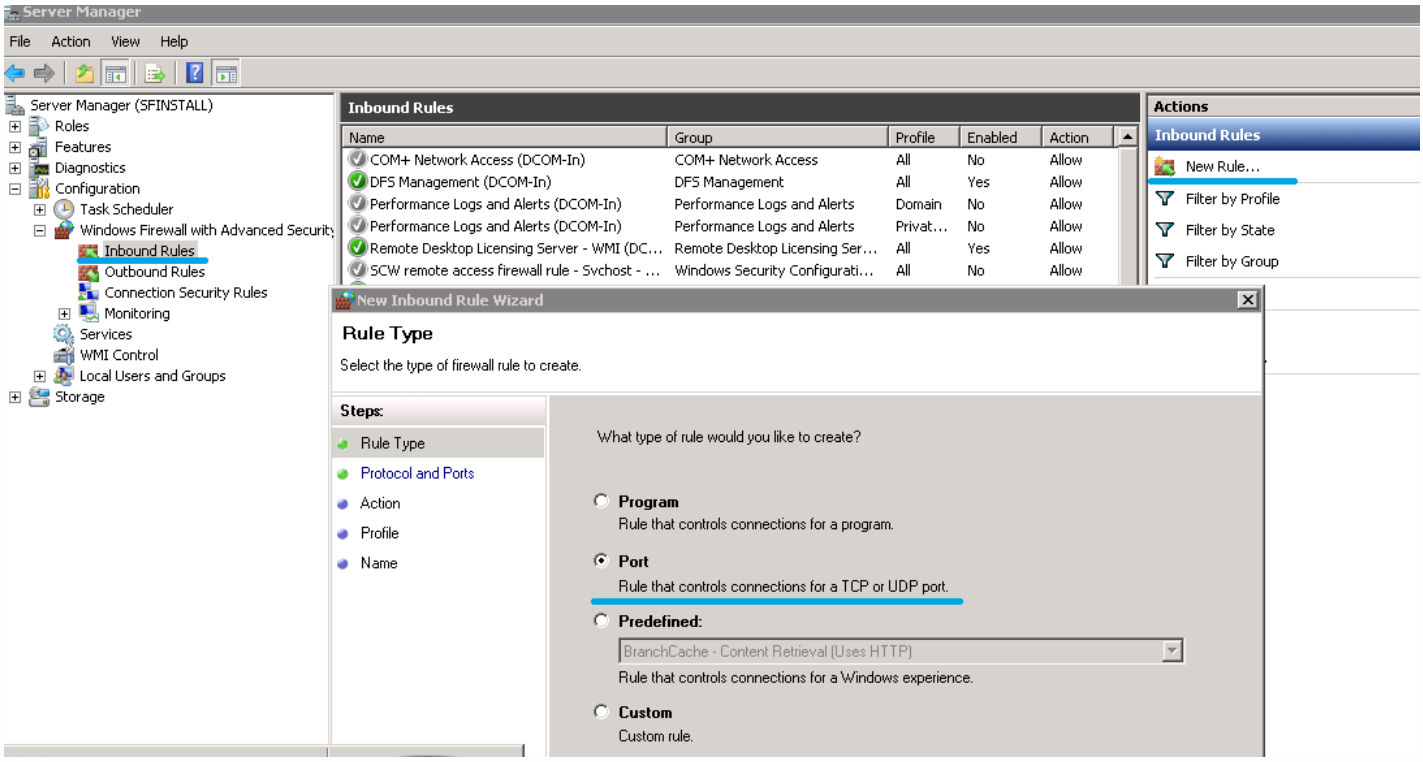
2. 在**高级安全 Windows 防火墙**中，选择中央窗格中的 **Windows 防火墙属性**。 有三个防火墙配置文件，即域配置文件、专用配置文件和公用配置文件。 选择**域配置文件**选项卡。 请务必将**防火墙状态**设置为**开**，将**入站连接**设置为**阻止**，将**出站连接**设置为**允许**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 选择**专用配置文件**和**公用配置文件**选项卡，并且务必将**防火墙状态**设置为**开**，将**入站连接**和**出站连接**设置为**阻止**。 应用并保存所做的更改。

4. 在**入站规则**中，选择**新建规则**以创建新入站规则。 在**新建入站规则向导**中，选择**规则类型**，选择**端口**作为新规则的类型，然后单击**下一步**。



5. 在**新建入站规则向导**中，选择**协议和端口**、**TCP**、**特定本地端口**，在文本框中键入 **445**，然后单击**下一步**。

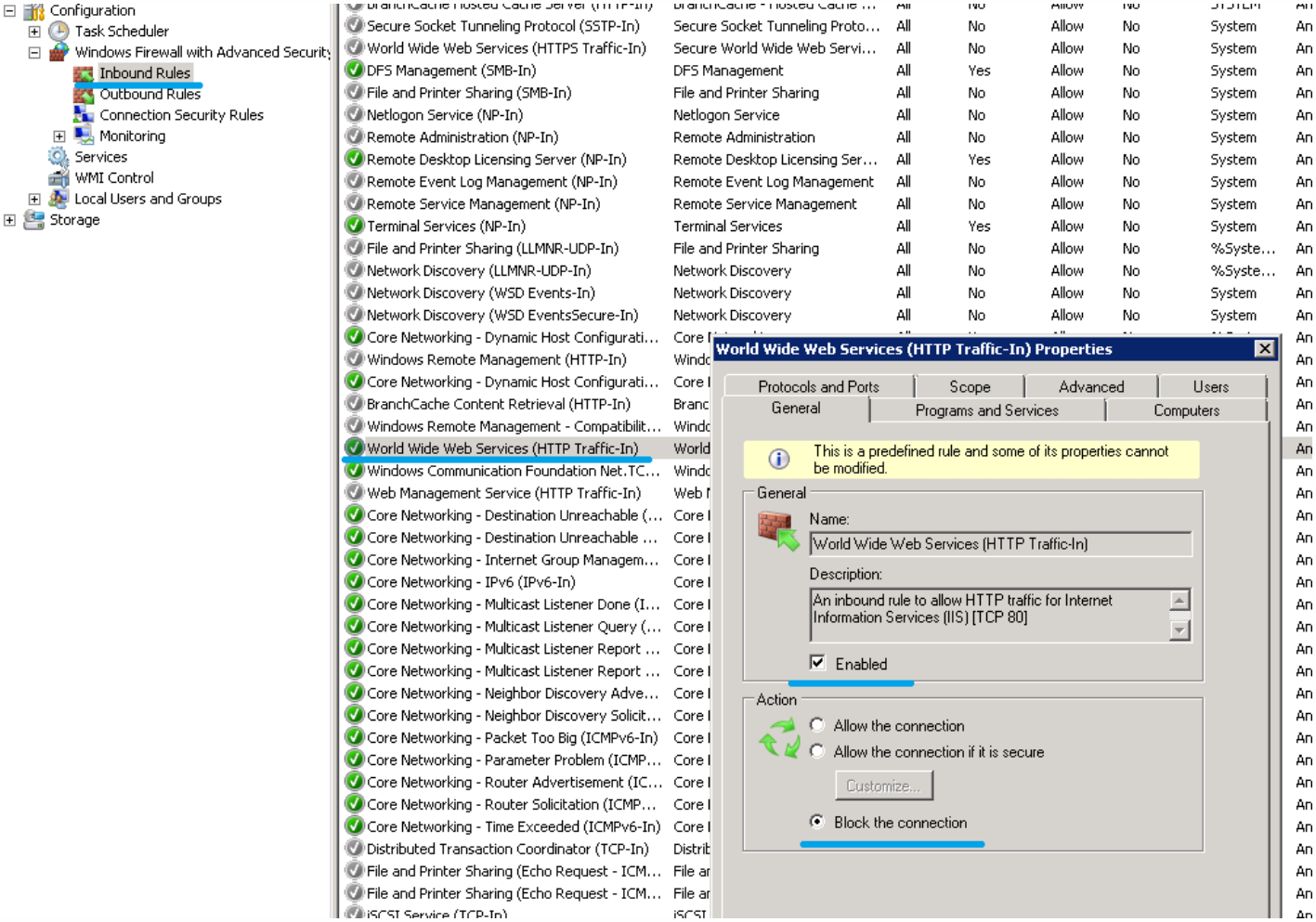
6. 在**新建入站规则向导**中，选择**操作**、**阻止连接**，然后单击**下一步**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7. 在**新建入站规则向导**中，选择**配置文件**、**域**、**专用**和**公用**，然后单击**下一步**。

8. 在**新建入站规则向导**中，选择**名称**，输入名称和说明，然后单击**下一步**。

9. 在**入站规则**中，选择**万维网服务(HTTP 流入量)**，并且务必将此规则设置为**已启用**，将**操作**设置为**阻止连接**。



10. 在**万维网服务(HTTP 流入量)属性**中，更改到**高级**选项卡，选择配置文件**域**、**专用**和**公用**，并保存对此规则所做的更改。

11. 在**入站规则**中，选择**万维网服务(HTTPS 流入量)**，并且务必将此规则设置为**已启用**，将**操作**设置为**允许连接**。

12. 在**万维网服务(HTTPS 流入量)属性**中，更改到**作用域**选项卡。 在**远程 IP 地址**部分中，选择**这些 IP 地址**，然后将所有 StoreFront 服务器 IP 地址添加到列表中。 例如，StoreFront A (192.168.1.13) 和 StoreFront B (192.158.1.14)。

13. 在**万维网服务(HTTP 流入量)属性**中，更改到**高级**选项卡，选择配置文件**域**、**专用**和**公用**，并保存对此规则所做的更改。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

从 Single Sign-On 中央存储迁移数据

Sep 19, 2016

Single Sign-On 中央存储是一个由 Single Sign-On 用于存储和管理用户及管理数据的集中存储库。 用户数据包括用户凭据、安全问题答案以及其他用户关注的数据。 管理数据包括密码策略、应用程序定义、安全问题以及其他范围较广的数据。

不能将所有数据从 Single Sign-On 中央存储迁移到自助服务密码重置中央存储。 下表说明了能够迁移和不能迁移的数据。

无法迁移	能够迁移
密码策略 - 不受支持	包含注册数据的 People 文件夹
应用程序模板 - 不受支持	客户使用的调查表
应用程序定义 - 不受支持	
用户配置 - 在自助服务密码重置控制台上创建	
应用程序组 - 不受支持	
Single Sign-On 服务数据 - 在自助服务密码重置控制台上创建	

Important

- 自助服务密码重置不支持将 Active Directory 作为中央存储，仅支持网络共享。
- 自助服务密码重置仅支持来自 Single Sign-On 4.8 或 5.0 的数据。

从 Single Sign-On 中央存储迁移数据

迁移您的数据之前，请熟悉如何安装和配置自助服务密码重置。 有关详细信息，请参阅“安装和配置”。

1. 创建新中央存储。
2. 安装自助服务密码重置服务和控制台。
3. 在控制台中，指定新中央存储的位置。
4. 创建新用户配置并将在 Single Sign-On 上启用了自助服务密码重置的用户包括在内。
5. 将 Single Sign-On 注册数据和安全问题复制到新中央存储中。

    注意：请确保数据代理帐户对所有复制的文件具有完全控制权限。

    仅需要两个文件夹/文件。

    示例

    将所有用户的注册数据

    \\SSO-SERVER\citrixsync$\People

© 1999-2017 Citrix Systems, Inc. All rights reserved.

复制到

\\SSPR-SVC\citrixsync$\People

请使用以下命令：
Robocopy \\SSO-SERVER\citrixsync$\People\ \\SSPR-SVC\citrixsync$\People /e /xd QBA /Log+:copylog.txt /tee

将客户使用的安全问题

\\SSOSERVERcitrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\QuestionBasedAuthentication2

复制到

\\SSPRSVCcitrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\

请使用以下命令：
Robocopy \\SSO-SERVER\citrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\ \\SSPR-SVC\citrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2 /e /Log+:copylog.txt /tee

现在，所有用户都能使用其 Single Sign-On 注册问题和答案解锁和重置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

将 StoreFront 配置为允许用户记录安全问题的答案。

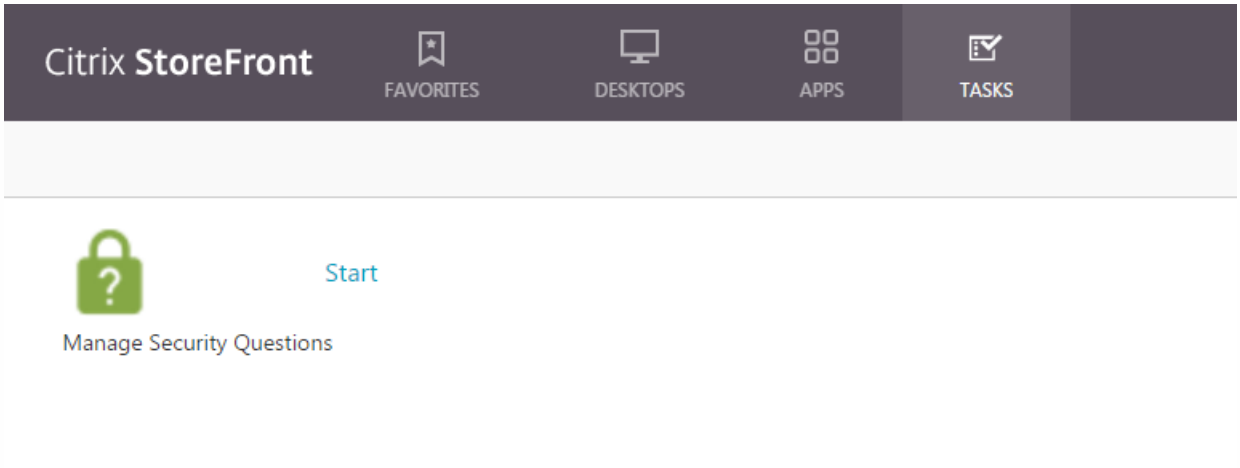
Dec 08, 2016

将 StoreFront 配置为允许用户注册安全问题的答案。 注册这些答案时，用户可以重置域密码以及解锁域帐户。 有关详细信息，请参阅 StoreFront 文档。

1. 将 StoreFront Internet Information Services (IIS) 配置为 HTTPS。
2. 在 StoreFront 中创建一个新部署。
3. 在 StoreFront 管理控制台的右侧窗格中，选择**管理身份验证方法 > 用户名和密码**。 从下拉菜单中选择**管理密码选项**。
4. 选择希望用户更改密码的时间，然后单击**确定**。
5. 从**用户名和密码**下拉菜单中选择**配置帐户自助服务**，选择 **Citrix SSPR**，然后单击**配置**。
6. 指定用户是否能够通过自助服务密码重置重置密码和解锁帐户，添加密码服务帐户服务 URL，然后单击**确定**。

注意：必须将站点配置为使用统一体验。

用户下次登录 Citrix Receiver 或 Citrix Receiver for Web 时，安全注册将可用。 单击**启动**后，将显示用户必须指定回答的问题。



© 1999-2017 Citrix Systems, Inc. All rights reserved.