StoreFront 2203

Contents

StoreFront 2203 长期服务版本概述

February 22, 2024

StoreFront 是企业应用商店应用程序，将来自 Citrix Virtual Apps and Desktops 站点和 Citrix DaaS 的应用程序和桌面聚合到一个易于用户使用的应用商店中。

在 StoreFront 中，您可以配置一个或多个应用商店。每个应用商店都有自己的配置，包括：

- StoreFront 查询的资源源列表，用于枚举可供用户使用的应用程序和桌面。
- 用于访问应用商店的 Web 站点的外观。
- 用户使用哪些身份验证方法登录。
- 通过 NetScaler Gateway 进行外部访问。

用户可以在 Web 浏览器中使用本地安装的 Citrix Workspace 应用程序或适用于 HTML5 的 Citrix Workspace 应用程序访问 StoreFront 应用商店。有关详细信息，请参阅用户访问选项。

首先，请规划 StoreFront 部署，查看系统要求并安装 StoreFront。

新增功能

累积更新 4 (CU4) 是 StoreFront 2203 LTSR 的最新版本。请参阅新增功能。

自 CU4 版本起，当您登录 StoreFront 时，可以及时看到有关适用于 HTML5 的 Citrix Workspace 应用程序启动状态的相关信息。有关详细信息，请参阅改善了虚拟应用程序和桌面的启动体验。

早期版本

当前可用的其他版本的文档在此处提供。

有关从早期版本进行升级的步骤，请参阅升级。

支持生命周期

生命周期里程碑中介绍了 StoreFront 当前版本 (CR) 和长期服务版本 (LTSR) 的产品生命周期策略。CTX200356 中提供了 StoreFront 的其他生命周期信息。

新增功能

December 5, 2023

累积更新 **4 (CU4)**

February 22, 2024

发布日期：2023 年 11 月 16 日

适用于 **HTML5** 的 **Citrix Workspace** 应用程序

本版本包括适用于 HTML5 的 Citrix Workspace 应用程序 2307。

2203 LTSR CU4 累积更新 **4 (CU4)** 更新 **1** 中已修复的问题

- 将 StoreFront 升级到版本 2203 LTSR CU4 时，尝试启动资源或应用程序枚举可能会失败。[CVADHELP-24175]
- 此修复解决了基础组件中的一个安全漏洞。有关详细信息，请参阅 CTX583759。[CVADHELP-23724]

2203 LTSR 累积更新 **4 (CU4)** 中已修复的问题

StoreFront 2203 LTSR CU4 包含 CU3 中包含的所有修复以及以下新修复：

- 当用户的偏好的启动方法为本机 Workspace 应用程序时，新应用程序可能会使用 HTML5 而非本机 Workspace 应用程序启动。[CVADHELP-22435]
- 此修复更正了德语错误消息中出现的错字。[CVADHELP-23088]
- 当您使用本地部署启动桌面会话时，Citrix Workspace 应用程序用户界面可能会显示正面的启动状态消息。但是，用户界面很快就会显示以下错误消息：

  <Desktop name> 无法启动桌面

适用于 HTML5 的 Citrix Workspace 应用程序尝试访问处于关闭状态的桌面时会出现此问题。Citrix Workspace 应用程序会等到桌面开机，而不是显示错误对话框。[CVADHELP-23140]

- StoreFront 服务器上的应用程序枚举可能会间歇性失败。[CVADHELP-23196]
- 连接到 StoreFront 应用商店时，适用于 Mac 的 Citrix Workspace 应用程序在从“睡眠”模式中唤醒后可能会冻结。[CVADHELP-23217]
- 争用条件可能会导致 Citrix Subscriptions Store 服务在 StoreFront 服务器上意外退出并显示警告消息。[CVADHELP-23326]

累积更新 **3 (CU3)**

February 22, 2024

发布日期：2023 年 6 月 1 日

适用于 **HTML5** 的 **Citrix Workspace** 应用程序

此版本包括 适用于 HTML5 的 Citrix Workspace 应用程序 2304。

已修复的问题

StoreFront 2203 LTSR CU3 包含 CU2 中包含的所有修复以及以下新修复：

- [CVADHELP-15544] 将 Citrix Gateway 的用途或角色从仅限 **HDX** 路由选项更改为身份验证和 **HDX** 路由或仅限身份验证选项时，StoreFront MMC 控制台可能会意外退出。
- [CVADHELP-19879] 如果启用了设置了特定代理策略的站点聚合或交付组，启动应用程序或桌面会创建新会话，而非重新连接到现有会话。
- [CVADHELP-21886] 在会话中将音频和打印机设置为关时，随后打开的会话也可能将音频和打印机设置为关。
- [CVADHELP-22114] 当您将配置更改从一台 StoreFront 服务器传播到另一台服务器时，传播后可能会出现以下错误消息：

  服务器无法访问配置设置可能已过时。

累积更新 **2 (CU2)**

February 22, 2024

发布日期：2022 年 12 月 8 日

适用于 **HTML5** 的 **Citrix Workspace** 应用程序

此版本包括适用于 HTML5 的 Citrix Workspace 应用程序 2211。

浏览器扩展程序（技术预览版）

Citrix Workspace 浏览器扩展程序可用于从 Web 客户端进行无缝客户端检测和会话启动。默认情况下，此功能处于禁用状态。管理员可以在 StoreFront 服务器上使用以下 PowerShell 脚本启用此功能：

```
`Add-STFFeatureState -Name "Citrix.StoreFront.EnableBrowserExtension "
   -IsEnabled $True`
```

有关更多详细信息，请参阅基于浏览器扩展程序的客户端检测和会话启动。

已修复的问题

StoreFront 2203 LTSR CU2 包含 CU1 中包含的所有修复以及以下新修复：

- [CVADHELP-18949] SAML 身份验证不适用于 CA 服务器颁发的证书。
- [CVADHELP-21048] 升级 StoreFront 服务器后，可能无法保留配置的 **FeatureState** 值。

  > 注意：
  >
  > 此修复必须同时应用到 StoreFront 服务器的基本版本和升级版本。

- [CVADHELP-20769] 应用此修复后，您可以使用默认配置的 HTML5 抢先体验版和备份版本。无需在 StoreFront 服务器上进行其他配置。
- [CVADHELP-20780] 在 Citrix StoreFront 管理控制台中修改 Citrix Gateway 详细信息时，可能会将两个空参数 **clusternodes** 和 **silentauthenticationurls** 添加到 StoreFront 服务器上的 **Roaming\web.config** 文件中。
- [CVADHELP-21037] 从早期版本升级 StoreFront 后，设置管理 **Receiver for Web** 站点 **>** 部署 **Citrix Receiver/Workspace** 应用程序 **>** 允许用户下载 **HDX** 引擎 **> Receiver/Workspace** 应用程序的源可能会默认设置为 **Citrix Web** 站点。

累积更新 **1 (CU1)**

April 17, 2024

发布日期：2022 年 8 月 3 日

关于此版本

StoreFront（初始版本）

此版本中的已知问题

Citrix 产品专享升级服务资格日期

适用于 **HTML5** 的 **Citrix Workspace** 应用程序

此版本包括适用于 HTML5 的 Citrix Workspace 应用程序 2205。

已修复的问题

StoreFront 2203 LTSR CU1 包含以下修复：

- 尝试在 Citrix Workspace 应用程序上启动应用程序或桌面时，如果将站点聚合配置为客户端 IP 地址过滤器，则可能会显示以下错误消息：

  由于出现错误代码 **3500**，您的会话未成功启动。请与您的管理员联系，获取有关该错误的更多信息。

  [CVADHELP-19435]

- 此修复提供了一条增强的警报消息，提示如果用户在客户端检测过程中单击“已安装”链接，则可能会丢失 StoreFront 客户端检测页面上的某些功能。[CVADHELP-19714]
- 将 StoreFront 升级到版本 2203 后，Citrix 应用程序交付控制器 (ADC) 委派的用户身份验证或应用程序枚举可能会失败。在 StoreFront 升级之前，如果在 ADC 或配置了安全 XML 流量的 Delivery Controller 上禁用 TLS1.0，则会出现此问题。[CVADHELP-19774]

新增功能

February 22, 2024

2203 LTSR 中的新增功能

StoreFront 2203 版包括以下新增功能和增强功能：

TLS 1.0 和 **TLS 1.1** 的支持已终止

自本版本起，StoreFront 在 Citrix Virtual Apps and Desktops（以前称为 XenApp 和 XenDesktop）和 Citrix Receiver 与 Workspace Hub 之间不再支持 TLS 1.0 和 TLS 1.1 协议。

适用于 **HTML5** 的 **Citrix Workspace** 应用程序

此版本包括适用于 HTML5 的 Citrix Workspace 应用程序 2202。

已修复的问题

自版本 1912 LTSR CU4 起，以下问题已修复：

- [CVADHELP-16834] 尝试使用 Citrix StoreFront 服务 API 启动用户会话时，传递给启动请求的参数可能不正确。
- [CVADHELP-17295] 在内部连接到 StoreFront 的 Citrix Workspace 应用程序中，SAML 身份验证可能会失败。
- [CVADHELP-17385] 此修复是 StoreFront 的一项增强功能，支持 Citrix DaaS 部署中的本地主机缓存功能。此增强功能允许用户在服务未处于云中断模式时从未将连接器作为 Delivery Controller 添加到 StoreFront 的位置启动资源。
- [CVADHELP-17671] StoreFront 在一些 URL 的查询字符串中包括一个跨网站请求伪造 (Cross Site Request Forgery, CSRF) 令牌。可能会因令牌保留在浏览器历史记录中或中间设备（例如代理服务器）的日志中而引起安全问题。

  应用此修复后，可以禁用以下 URL 请求的 CSRF 令牌用法。

  ```
  Add-STFFeatureState -Name "Citrix.DeliveryServices.WebUI.CsrfValidation
  .IgnoreOnSpecificRequests"-IsEnabled $True
  ```

  > 注意：
  >
  > 如果功能开关为开，则必须在所有基于 WebAPI 的自定义设置中从 URL 中删除 CSRF 令牌。

- [CVADHELP-18083] 如果使用“部署 Citrix Receiver/Workspace 应用程序”选项选择“Receiver/Workspace 应用程序的源”作为 Citrix Web 站点，Citrix Receiver/Workspace 应用程序会从不安全的站点下载。因此，最新的 Google Chrome 浏览器更新将阻止下载。
- [CVADHELP-18221] 切换帐户以登录同一客户端上的 Citrix Workspace 应用程序时，精选应用程序组的图标可能会启动不正确的应用程序。例如，如果用户在 Citrix Workspace 应用程序上单击应用程序 **A** 的图标，应用程序 **B** 可能会启动。此外，应用程序 A 的详细信息框显示应用程序 B 的信息。
- [LCM-9536] Citrix Receiver for Web 站点中突出显示的选项卡会忽略在为“编辑 Receiver for Web 站点”对话框的自定义外观选项卡中指定的“链接颜色”值。相反，突出显示的选项卡显示为紫色。

弃用

February 22, 2024

本文中的公告旨在提前通知您正在逐渐淘汰的平台、Citrix 产品和功能，以便您能够及时制定业务决策。Citrix 将监视客户使用情况和反馈以确定其退出时间。在后续版本中公告可能会有更改，可能不会包括每个弃用的特性或功能。有关产品生命周期支持的详细信息，请参阅 Product Lifecycle Support Policy（产品生命周期支持策略）一文。有关长期服务版本 (LTSR) 服务方案的信息，请参阅https://support.citrix.com/article/CTX205549。

弃用和删除

下表显示了已弃用或删除的平台、Citrix 产品和功能。以粗体显示的日期表示此版本的变更。已弃用的项目不会立即删除。Citrix 会继续支持这些项目，直到删除了这些项目的版本为止。

项目	宣布在版本中弃用	已在版本中删除	备选
支持自助服务密码重置 (SSPR)	2203	2203	-
支持在 Citrix Virtual Apps and Desktops（以前称为 XenApp 和 XenDesktop）与 Citrix Workspace 应用程序之间使用 TLS 1.0 和 TLS 1.1 协议。	3.14	2203	请将 Citrix Receiver 升级到支持 TLS 1.2 的 Citrix Workspace 应用程序。
在 Windows Server 2012 R2 上安装 StoreFront	2203	2203	在受支持的操作系统中安装 StoreFront。
支持 4.7.2 之前的 Microsoft .NET Framework 版本。	2203	2203	升级到.NET Framework 4.7.2 或更高版本。（如果尚未安装.NET Framework 4.7.2，安装程序将自动安装。）
删除了以下生命周期已结束产品的 Delivery Controller 选项：VDI-in-a-Box 和 XenMobile（9.0 或更低版本）。	1903	1903	—
Internet Explorer 9 和 10	1903	1903	—
在 Windows Server 2012 上安装 StoreFront	1903	1903	在受支持的操作系统中安装 StoreFront。

项目	宣布在版本中弃用	已在版本中删除	备选
支持用户访问桌面设备站点上的桌面	1811	1912	将 Desktop Lock 用于未加入域的用例。
Citrix 经典体验（“绿色气泡”用户界面）	3.12	1903	使用新用户界面
在 Windows Server 2012 和 Windows Server 2008 R2 上安装 StoreFront（包括 Service Pack）。	3.12 LTSR	3.15	在受支持的操作系统中安装组件。
Citrix Online Integration（Goto 产品）集成	3.11	3.12	—
StoreFront 2.0、2.1、2.5 和 2.5.2 中的原位升级	3.9	1818	从其中一个版本升级到 3.12，然后升级到最新版本
在 32 位 (x86) 计算机上安装 StoreFront。	3.8	3.13	在受支持的 x64 操作系统中安装。

有关适用于 HTML5 的 Citrix Workspace 应用程序中的弃用的信息，请参阅弃用页面。

2203 中的已知问题

February 22, 2024

> 注意：
>
> 除非其包含在已修复的问题列表中，否则本文的 2203 初始版本中介绍的已知问题将继续存在于 CU 更新中。

StoreFront 2203 CU4 中的已知问题

- 将 StoreFront 升级到版本 2203 LTSR CU4 时，尝试启动资源或应用程序枚举可能会失败。

  > 注意：
  >
  > 该问题已在 2203 LTSR CU4 更新 1 中修复。

  [CVADHELP-24175]

- 带有特殊字符的用户名可能会显示为已损坏。[CVADHELP-24499]

StoreFront 2203 CU3 中的已知问题

累积更新 3 中没有新的已知问题。

StoreFront 2203 CU2 中的已知问题

累积更新 2 中没有新的已知问题。

StoreFront 2203 CU1 中的已知问题

累积更新 1 中没有新的已知问题。

StoreFront 2203 中的已知问题

- 当 TelemetryService.exe 文件锁定“Framework.xml”时，StoreFront 安装可能会间歇性失败。解决方法是停止 Citrix Telemetry Service 并重复安装。[LCM-12147]
- 将 StoreFront 升级到版本 2203 后，Citrix 应用程序交付控制器 (ADC) 委派的用户身份验证或应用程序枚举可能会失败。在 StoreFront 升级之前，如果在 ADC 或配置了安全 XML 流量的 Delivery Controller 上禁用 TLS1.0，则会出现此问题。有关详细信息，请参阅 https://support.citrix.com/article/CTX457757。[CVADHELP-19774]。此问题已在 2203 LTSR CU1 版本中得到修复。

安装、设置、升级和卸载

September 29, 2023

任务	详细信息
规划 StoreFront 部署	StoreFront 部署中所涉及的组件的概述
用户访问选项	用户可以访问您的应用商店的方式概述
系统要求	确保您具备安装 StoreFront 的必备条件
安装 StoreFront	在新服务器上安装 StoreFront
使用 HTTPS 保护 StoreFront 的安全	使用 HTTPS 加密客户端对 StoreFront 的访问
保护 StoreFront 部署的安全	配置 StoreFront 以提高安全性
创建新部署	配置一个带有新应用商店的新 StoreFront 服务器。

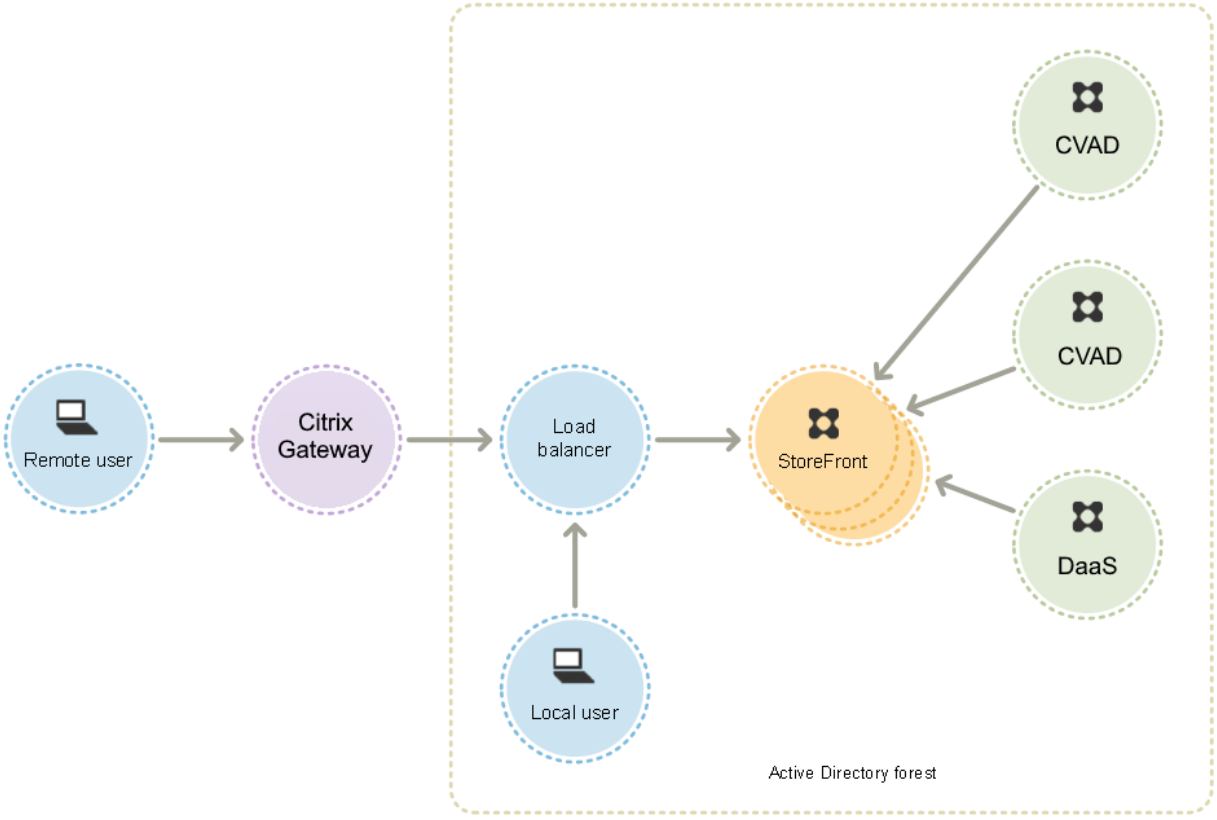
任务	详细信息
加入现有服务器组	配置一台新 StoreFront 服务器以加入现有的服务器组。
升级 StoreFront	升级运行较旧版本的 StoreFront 服务器
CEIP	参与或退出 Citrix 客户体验改善计划 (CEIP)
Citrix Analytics 服务	将 StoreFront 配置为向 Citrix Analytics Service 发送数据
卸载 StoreFront	从您的服务器中删除 StoreFront
将服务器重置为出厂默认设置	清除所有 StoreFront 设置，以便能够对其进行重新配置。

规划 **StoreFront** 部署

April 17, 2024

StoreFront 与 Citrix Virtual Apps and Desktops 部署相集成，为用户提供单一的自助访问点，以访问其桌面和应用程序。

下图显示了一个典型的 StoreFront 部署。



Active Directory

StoreFront 使用 Active Directory 对用户进行身份验证、查找组成员身份和其他详细信息，以及在 StoreFront 服务器之间同步数据。

针对单服务器部署，可以在未加入域的服务器上安装 StoreFront，但某些功能将不可用；否则，StoreFront 服务器必须驻留在包含用户帐户的 Active Directory 域中，或者驻留在与用户帐户域具有信任关系的域中，除非您启用了将身份验证委派给 Citrix Virtual Apps and Desktops 站点或场的功能。组中的所有 StoreFront 服务器必须位于同一个域中。

StoreFront 服务器组

StoreFront 可以在单个服务器上配置，也可以配置为名为 StoreFront 服务器组的多服务器部署。服务器组不但提供了额外的容量，而且还提供了更高的可用性。StoreFront 可确保将用户应用程序订阅的配置信息和详细信息存储在服务器组中的所有服务器上，并在这些服务器组之间复制。这意味着如果 StoreFront 服务器因任何原因不可用，用户可以继续使用其余的服务器访问其应用商店。同时，出现故障的服务器上的配置和订阅数据在服务器连接到服务器组时自动更新。订阅数据会在服务器重新联机时更新，但是，如果服务器在脱机期间错过任何内容，您必须传播配置更改。如果出现硬件故障，需要替换服务器，可以在新服务器上安装 StoreFront，然后将其添加到现有服务器组中。新服务器将在加入服务器组时自动配置并更新用户的应用程序订阅。

Citrix 建议一个服务器组中最多包含五台服务器。如果服务器超过五台，同步数据的开销超过了额外服务器的好处，并且性能会降低。

仅当服务器组中的服务器之间的链接延迟小于 40 毫秒（禁用订阅）或小于 3 毫秒（启用订阅）时，才支持 StoreFront 服务器组部署。理想情况下，服务器组中的所有服务器都应位于同一位置（数据中心、可用区），但服务器组可以跨同一区域内的多个位置，前提是组中的服务器之间的链接满足这些延迟条件。示例包括跨云区域内或本地区域数据中心之间的可用区的服务器组。请注意，区域间的延迟因云提供程序而异。Citrix 不建议将跨多个位置作为灾难恢复配置，但它可能适用于高可用性。

负载平衡

对于 StoreFront 服务器组中的多台服务器，必须配置外部负载平衡。请使用具有内置监视器和会话一致性的负载平衡器，例如 Citrix ADC。有关 Citrix ADC 负载平衡的详细信息，请参阅负载平衡。

用于远程访问的 Citrix Gateway

如果您计划支持从企业网络外部访问 StoreFront，则需要使用 Citrix Gateway 为远程用户提供安全连接。可以在企业网络外部部署 Citrix Gateway 并使用防火墙将 Citrix Gateway 与公用和内部网络进行分隔。请确保 Citrix Gateway 能够访问包含 StoreFront 服务器的 Active Directory 林。

全局服务器负载平衡器

在大型 Citrix 部署中，您可能会在多个数据中心中部署 StoreFront 和 NetScaler。使用全局服务器负载平衡器 (GSLB)，您可以配置单个全局 URL，GSLB 会将该 URL 重定向到其中一个区域中的网关的特定 URL。通常情况下，GSLB 会根据负载平衡算法（例如往返时间 (RTT) 或静态邻近度）选择距离最近的网关。

例如，您可能有 3 个区域性网关：

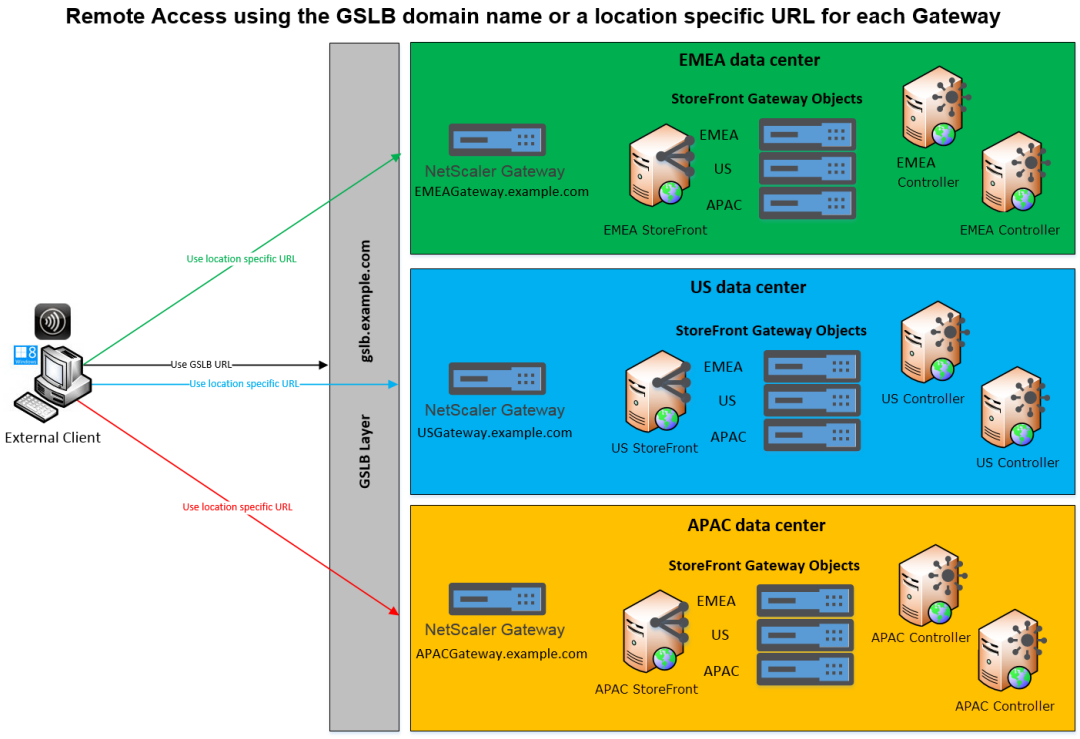
`emeagateway.example.com` - 欧洲网关

`usgateway.example.com` - 美国网关

`apacgateway.example.com` - 亚太网关

与 GSLB 一起

`gslb.example.com`



在配置 GSLB 之前，请查看您拥有哪些服务器证书以及贵组织如何执行 DNS 解析。要在您的 Citrix Gateway 和 StoreFront 部署中使用的任何 URL 都必须存在于您的服务器证书中。

StoreFront 没有任何用于在服务器组之间同步配置的内置机制；相反，管理员可以将每个 StoreFront 服务器组配置为按相同的方式进行配置，这样无论用户连接到哪个服务器组，都能获得一致的体验。

StoreFront 可以在服务器组之间定期同步订阅（收藏夹），请参阅订阅同步。

用户访问

请参阅用户访问选项。

用户访问选项

April 17, 2024

用户可以通过三种不同的方法访问 StoreFront 应用商店。

- 本地安装的 Citrix Workspace 应用程序 - 具有兼容版本的 Citrix Workspace 应用程序的用户可以通过 Citrix Workspace 应用程序用户界面访问 StoreFront 应用商店。这样可以提供最佳的用户体验和最强大的功能。
- 适用于 HTML5 的 Citrix Workspace 应用程序 - 使用兼容 Web 浏览器的用户可以通过浏览到应用商店的 Web 站点来访问 StoreFront 应用商店。默认情况下，用户还需要具有兼容版本的 Citrix Workspace 应用程序才能访问自己的桌面和应用程序，称为混合启动。但是，您可以配置自己的 Web 站点，使用户无需安装 Citrix Workspace 应用程序即可通过浏览器访问其资源。
- XenApp Services URL - 拥有无法升级的传统 Citrix 客户端的用户可以使用应用商店的 XenApp Services URL 来访问应用商店。创建新应用商店时，将默认启用 XenApp Services URL。

本地安装的 **Citrix Workspace** 应用程序

从本地安装的 Citrix Workspace 应用程序访问应用商店可提供最佳用户体验。有关可用于以这种方式访问应用商店的 Citrix Workspace 应用程序版本，请参阅系统要求 。

Citrix Workspace 应用程序使用内部和外部 URL 作为信标点。通过尝试联系这些信标点，Citrix Workspace 应用程序可以确定用户是否已连接到本地或公用网络。用户访问桌面或应用程序时，位置信息将传递给提供资源的服务器，以便能够将相应的连接详细信息返回给 Citrix Workspace 应用程序。这样可以启用 Citrix Workspace 应用程序以确保在用户访问桌面或应用程序时不会收到重新登录提示。有关详细信息，请参阅配置信标点。

向 **Workspace** 应用程序中添加应用商店

安装后，必须使用提供用户的桌面和应用程序的应用商店的连接详细信息对 Citrix Workspace 应用程序进行配置。可以通过以下方式之一向用户提供所需的信息，从而简化用户的配置过程。

> 重要提示：
>
> 默认情况下，Citrix Workspace 应用程序需要使用 HTTPS 来连接应用商店。如果 StoreFront 未配置 HTTPS，用户必须执行其他配置步骤来使用 HTTP 连接。Citrix 强烈建议不要在生产环境中启用指向 StoreFront 的不安全的用户连接。有关详细信息，请参阅适用于 Windows 的 Citrix Workspace 应用程序文档中的应用商店配置参数。

手动配置　用户可以通过在 Citrix Workspace 应用程序中输入应用商店 URL 将 Citrix Workspace 应用程序连接到自己的应用商店。有关详细信息，请参阅 Citrix Workspace 应用程序文档。

预配文件　可以为用户提供预配文件，其中包含应用商店的详细连接信息。在安装 Citrix Workspace 应用程序后，用户可以打开.cr 文件，自动为应用商店配置帐户。默认情况下，Web 站点为用户提供的预配文件仅适用于为其配置站点的单个应用商店。您可以指引用户访问其想要访问的应用商店所对应的 Web 站点，并从这些站点下载预配文件。或者，为了获得更高级别的控制，您可以使用 Citrix StoreFront 管理控制台来生成包含一个或多个应用商店的连接详细信息的预配文件。随后可以将这些文件分发给相应的用户。有关详细信息，请参阅为用户导出应用商店预配文件。

自动生成的设置 **URL**　对于运行 macOS 的用户，您可以使用适用于 Mac 的 Citrix Workspace 应用程序设置 URL 生成器创建包含应用商店详细连接信息的 URL。安装 Citrix Workspace 应用程序后，用户可以单击该 URL，以自动为应用商店配置帐户。在该工具中输入部署的详细信息，并生成可分发给用户的 URL。

基于电子邮件的帐户发现　通过基于电子邮件的帐户发现，用户无需知晓其应用商店的访问详细信息，而是在 Citrix Workspace 应用程序初始配置过程中输入其电子邮件地址即可。有关如何设置此功能的详细信息，请参阅基于电子邮件的帐户发现。

Global App Config Service

使用 Global App Config Service 可为您的 StoreFront 应用商店配置 Citrix Workspace 应用程序。请参阅为本地应用商店配置设置。

适用于 **HTML5** 的 **Citrix Workspace** 应用程序

作为使用本地安装的 Workspace 应用程序的替代方案，用户可以使用适用于 HTML5 的 Workspace 应用程序通过 Web 浏览器访问其应用商店。当用户启动自己的资源时，有两种可能性。

1. 资源将在本地安装的 Citrix Workspace 应用程序中启动。这称为混合启动。这为用户提供了最佳体验，因为它可以利用完整的操作系统集成。有关更多详细信息，请参阅混合启动
2. 资源在浏览器中启动。这使用户无需在本地安装任何软件即可访问资源。

默认配置是要求在本地安装 Citrix Workspace 应用程序才能进行混合启动。您可以将配置更改为始终在浏览器中启动资源或者让用户做出选择。请参阅部署 Workspace 应用程序。

如果管理员选择了如果本地 **Receiver** 不可用，则使用 **Receiver for HTML5**，则当用户首次在浏览器中打开应用商店 Web 站点时，用户可以选择单击使用简易版本在其 Web 浏览器中启动资源。

在浏览器中打开资源的要求

对于内部网络中的用户，默认情况下禁止通过适用于 HTML5 的 Citrix Workspace 应用程序访问 Citrix Virtual Apps and Desktops 提供的资源。要允许使用适用于 HTML5 的 Citrix Workspace 应用程序本地访问桌面和应用程序，请在您的 Citrix Virtual Apps and Desktops 服务器上启用“ICA WebSockets 连接”策略。Citrix Virtual Apps and Desktops 对适用于 HTML5 的 Citrix Workspace 应用程序使用端口 8008。确保防火墙和其他网络设备允许访问此端口。有关详细信息，请参阅 WebSockets 策略设置。

要成功启动 Citrix Virtual Apps and Desktops 资源，请配置与托管应用程序和桌面的 VDA 的 TLS 连接。通过 Citrix Gateway 建立的远程连接可以使用适用于 HTML5 的 Citrix Workspace 应用程序启动资源，而无需配置到 VDA 的 TLS 连接。

混合启动

当用户首次通过浏览器打开 Citrix Workspace for HTML5 但在本地安装的 Citrix Workspace 应用程序中启动应用程序时，这称为“混合启动”。Web 站点可以通过多种方式与本地安装的 Workspace 应用程序进行通信以启动资源。

Citrix Workspace Launcher

当用户首次访问安装了受支持的操作系统和浏览器的 StoreFront Web 站点时，适用于 HTML5 的 Citrix Workspace 应用程序将尝试调用 Citrix Workspace Launcher。如果安装了受支持的 Citrix Workspace 应用程序版本，该应用程序会通知 StoreFront。适用于 HTML5 的 Citrix Workspace 应用程序会记住这一点，当它启动应用程序时会使用 Citrix Workspace Launcher。

使用以下浏览器时，应用商店 Web 站点会在 Windows、Mac 和 Linux 中调用 Citrix Workspace Launcher：

- Firefox 52 或更高版本
- Chrome 42 或更高版本
- Safari 12 或更高版本
- Edge 25 或更高版本

Citrix Workspace Launcher 需要下列最低版本的 Citrix Receiver 或 Citrix Workspace 应用程序。

- Receiver for Windows 4.3 或更高版本
- Receiver for Mac 12.0 或更高版本
- 适用于 Linux 的 Workspace 应用程序 2003 或更高版本

如果 Workspace 应用程序启动器不可用，或者用户不允许其打开，它将检测不到本地安装的 Citrix Workspace 应用程序。用户可以选择重试，也可以单击已安装，在这种情况下，它会回退到使用.ica 文件启动应用程序。用户稍后可以转到“设置”屏幕并单击更改 **Citrix Workspace** 应用程序重试。

如果您在全局服务器负载平衡器后面使用多个处于活动状态的 StoreFront 服务器组，Citrix Workspace Launcher 可能会间歇性出现故障。为了避免出现这种情况，您必须配置全局服务器负载平衡器，以强制用户 Web 会话在客户端检

测过程的整个生命周期内持续在一个 StoreFront 服务器组中进行，请参阅 CTX460312。或者部署 Citrix Workspace Web 扩展程序。

Citrix Workspace Web 扩展（技术预览版）

Citrix Workspace Web 扩展是适用于常用 Web 浏览器的扩展，可以改善用户检测本地安装的 Citrix Workspace 应用程序以及启动虚拟应用程序和桌面的体验。与 Citrix Workspace Launcher 相比，它可以提供更加出色的用户体验，并且避免了全局服务器负载平衡器出现问题。

要启用基于浏览器扩展程序的客户端检测，请执行以下操作：

- 在 StoreFront 服务器上启用该功能。
- 在客户端设备上部署浏览器扩展程序。
- 部署适用于 Windows 的 Citrix Workspace 应用程序 2303、适用于 Mac 的 Citrix Workspace 应用程序 2304 或适用于 Linux 的 Citrix Workspace 应用程序 2302 或更高版本。

用户首次在受支持的平台上访问应用商店 Web 站点时，它会提示用户检测本地安装的 Workspace 应用程序。它首先尝试使用 Web 扩展程序，如果失败，则尝试使用 Citrix Workspace Launcher。已完成 Workspace 应用程序检测的现有用户可以转至帐户设置，单击更改 **Citrix Workspace** 应用程序以重新检测 Workspace 应用程序。

默认情况下，此功能处于关闭状态。管理员可以在 StoreFront 服务器上使用以下 PowerShell 脚本启用此功能：`Add-STFFeatureState -Name "Citrix.StoreFront.EnableBrowserExtension"-IsEnabled $True`。

Internet Explorer

用户首次在 Internet Explorer 中打开应用商店 Web 站点时，它会提示用户安装包含适用于 Internet Explorer 的 Citrix ICA 客户端加载项在内的 Citrix Workspace 应用程序。安装该插件后，它将用于通过本地安装的 Citrix Workspace 应用程序启动应用程序和桌面。

ICA 文件下载

如果 HTML5 版 Citrix Workspace 应用程序无法通过任何其他方式检测到本地安装的 Citrix Workspace 应用程序，则当用户启动应用程序或桌面时，它会下载.ica 文件。用户可以使用本地安装的 Citrix Workspace 应用程序打开此文件。

资源快捷方式

您可以生成 URL，利用这些 URL 可以访问您的应用商店中提供的桌面和应用程序。将这些链接嵌入托管在内部网络上的 Web 站点中，可以方便用户快速访问资源。用户单击某个链接时会重定向到应用商店的 Web 站点，如果用户尚未登

录，可以在该站点登录。该应用商店 Web 站点会自动启动资源。有关生成资源快捷方式的详细信息，请参阅 Web 站点快捷方式。

在创建应用程序快捷方式时，请确保应用商店中没有与其同名的其他应用程序。快捷方式无法区分具有相同名称的多个应用程序实例。同样，如果您通过应用商店提供单个桌面组中的某个桌面的多个实例，则不能单独为每个实例都创建一个快捷方式。快捷方式不能将命令行参数传递给应用程序。

要创建应用程序快捷方式，您可以使用将用于托管快捷方式的内部 Web 站点的 URL 来配置 StoreFront。用户单击 Web 站点上的应用程序快捷方式时，StoreFront 会对照您输入的 URL 列表来检查该 Web 站点，以确保请求来自可信 Web 站点。但是，对于通过 Citrix Gateway 连接的用户，不会对托管快捷方式的 Web 站点进行验证，因为不会将 URL 传递给 StoreFront。要确保远程用户只能访问可信内部 Web 站点上的应用程序快捷方式，请将 Citrix Gateway 配置为限定用户只能访问这类特定站点。

自定义用户界面

Citrix StoreFront 提供了一种用于自定义用户界面的机制。无论是通过 Citrix Workspace 应用程序还是通过 Web 浏览器访问应用商店，这些都适用。您可以自定义字符串、层叠样式表，以及 JavaScript 文件。还可以添加自定义的登录前和登录后屏幕，并添加语言包。有关详细信息，请参阅自定义外观。

XenApp Services URL

具有无法升级的旧版 Citrix 客户端的用户可以通过为客户端配置应用商店的 XenApp Services URL 来访问应用商店。您也可以启用从已加入域的桌面设备和运行 Citrix Desktop Lock 的重用 PC 通过 XenApp Services URL 访问应用商店。在本上下文中，已加入域表示设备已加入包含 StoreFront 服务器的 Microsoft Active Directory 林中的一个域。

StoreFront 支持从 Citrix Workspace 应用程序到 XenApp Services URL 的感应卡直通身份验证。Citrix Ready 合作伙伴产品使用 Citrix Fast Connect API 来简化用户通过 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序登录以使用 XenApp Services URL 连接到应用商店的过程。用户使用感应卡向工作站验证身份后，即可快速连接到 Citrix Virtual Apps and Desktops 提供的桌面和应用程序。有关详细信息，请参阅最新的适用于 Windows 的 Citrix Workspace 文档。

创建新应用商店时，将默认启用应用商店的 XenApp Services URL。应用商店的 XenApp Services URL 的格式为 http[s]://serveraddress/Citrix/storename/PNAgent/config.xml，其中 serveraddress 为 StoreFront 部署的服务器或负载平衡环境的完全限定域名，storename 为创建应用商店时为其指定的名称。这样可允许只能使用 PNAgent 协议的 Citrix Workspace 应用程序连接到 StoreFront。有关可用于通过 XenApp Services URL 访问应用商店的客户端，请参阅用户设备要求。

重要注意事项

XenApp Services URL 用于支持无法升级到 Citrix Workspace 应用程序的用户，适用于没有备选访问方法的情况。决定是否使用 XenApp Services URL 向用户提供对应用商店的访问时，请考虑以下限制。

- 不能修改应用商店的 XenApp Services URL。
- 不能通过编辑配置文件 config.xml 来修改 XenApp Services URL 设置。
- XenApp Services URL 支持显式身份验证、域直通、智能卡身份验证和使用智能卡的直通身份验证。默认情况下会启用显式身份验证。只能为每个 XenApp Services URL 配置一种身份验证方法，而且每个应用商店只能使用一个 URL。如果需要启用多个身份验证方法，则必须为每种身份验证方法创建单独的应用商店，每个应用商店都具有一个 XenApp Services URL。然后，用户必须连接到与其身份验证方法所对应的应用商店。有关详细信息，请参阅基于 XML 的身份验证。
- 默认情况下，对 XenApp Services URL 启用工作区控制功能，并且不能配置或禁用工作区控制功能。
- 用户的更改密码请求将绕过 StoreFront 身份验证服务，直接通过为应用商店提供桌面和应用程序的 Citrix Virtual Apps and Desktops 服务器路由到域控制器。

系统要求

April 17, 2024

在安装 StoreFront 之前，请查看规划 StoreFront 部署。

StoreFront 服务器要求

Citrix 已测试过，可以支持在以下平台上安装 StoreFront：

- Windows Server 2022 Datacenter Edition 和 Standard Edition
- Windows Server 2019 Datacenter Edition 和 Standard Edition
- Windows Server 2016 Datacenter Edition 和 Standard Edition

> 注意：
>
> StoreFront 需要 Windows 桌面体验，因此无法安装在 Windows Server Core 中。

服务器组中的所有 StoreFront 服务器必须使用相同的操作系统版本、语言和区域设置。

不支持在运行 StoreFront 的服务器上升级操作系统版本。Citrix 建议您在新安装的操作系统中安装 StoreFront。

除了操作系统的要求外，Storefront 服务器还必须满足以下最低要求：

- 处理器：2 个虚拟 CPU
- RAM：每位用户 4 GB，外加每个可用资源 700 字节。
- 存储：
  - StoreFront 本身为 250 MB。
  - 每个应用商店 30 MB，假定每个应用商店有一个 Web 站点。

  - 对于每个启用了收藏夹的应用商店，每 1000 个收藏夹 5 MB，再加上 8 MB。
  - 根据您的要求有足够的空间存放 IIS 日志文件，请参阅有关管理 IIS 日志文件存储的 Microsoft 文档。
  - 有足够的空间存放 StoreFront 诊断日志。默认情况下，StoreFront 仅保留 15 MB 的日志，但您可能希望增加此值。请参阅 Storefront 故障排除。

必须先在 Web 服务器上启用以下 Windows 功能，才能安装 StoreFront。这些组件在新的 Windows 安装中默认处于启用状态，因此除非已明确卸载这些组件，否则无需执行任何操作。

- NET-Framework-45-Features
  - NET-Framework-45-Core
- PowerShellRoot
  - PowerShell

如果安装的.NET Framework 版本低于 4.7.2，安装程序会自动安装.NET Framework 4.7.2。请注意，这要求已安装 NET-Framework-45-Core Windows 功能。

如果 StoreFront 安装程序检测到缺少以下任何 Windows 功能，则会自动安装这些功能：

- Web-Server
  - Web-WebServer
    - Web-Common-Http
      - Web-Default-Doc
      - Web-Http-Errors
      - Web-Static-Content
      - Web-Http-Redirect
    - Web-Health
      - Web-Http-Logging
    - Web-Security
      - Web-Filtering
      - Web-Basic-Auth
      - Web-Windows-Auth
    - Web-App-Dev
      - Web-Net-Ext45
      - Web-AppInit
      - Web-Asp-Net45
      - Web-ISAPI-Ext
      - Web-ISAPI-Filter
    - Web-Mgmt-Tools
      - Web-Mgmt-Console

        - Web-Scripting-Tools
- NET-Framework-45-Features
    - NET-Framework-45-ASPNET
    - NET-WCF-Services45
        - NET-WCF-TCP-PortSharing45

在安装 StoreFront 之前，可以将 IIS Web 站点移至其他目录或驱动器。IIS 中 StoreFront 的相对路径在服务器组中的所有服务器上必须相同。

StoreFront 使用以下端口进行通信。请确保您的防火墙及其他网络设备允许访问这些端口。

- TCP 端口 80 和 443 分别用于 HTTP 和 HTTPS 通信，必须可同时从企业网络内部和外部进行访问。
- TCP 端口 808 用于 StoreFront 服务器之间的通信，因此必须可进行访问。
- 从所有未预留的端口中随机选择的 TCP 端口用于服务器组中 StoreFront 服务器之间的通信。安装 StoreFront 时，将配置 Windows 防火墙规则，以允许访问 StoreFront 可执行文件。但是，由于端口是随机分配的，必须确保内部网络中的任何防火墙或其他设备不会阻止流向任何未分配的 TCP 端口的流量。
- 启用后，TCP 端口 8008 由适用于 HTML5 的 Citrix Workspace 应用程序或者受支持的 Citrix Workspace 应用程序版本使用，可供内部网络中的本地用户用来与向其提供桌面和应用程序的服务器进行通信。

StoreFront 支持纯 IPv6 网络和双协议栈 IPv4/IPv6 两种环境。

使用 **Microsoft SQL Server** 存储订阅数据

可以选择性使用 Microsoft SQL Server 存储订阅数据。StoreFront 支持对此功能使用与 Citrix Virtual Apps and Desktops 对数据库使用的相同 Microsoft SQL Server 版本。在 Citrix Virtual Apps and Desktops 系统要求中，请参阅数据库。

基础结构要求

Citrix 已测试过，在与以下 Citrix 产品版本一起使用时可提供对 StoreFront 的支持。

Citrix Virtual Apps and Desktops

StoreFront 支持以下版本的 Citrix Virtual Apps and Desktops：

- Citrix Virtual Apps and Desktops 7 2203 LTSR
- Citrix Virtual Apps and Desktops 7 2112
- Citrix Virtual Apps and Desktops 7 2109
- Citrix Virtual Apps and Desktops 7 2106
- Citrix Virtual Apps and Desktops 7 2103

- Citrix Virtual Apps and Desktops 7 2012
- Citrix Virtual Apps and Desktops 7 1912 LTSR
- XenApp 和 XenDesktop 7.15 LTSR

有关在长期服务 (LTSR) 环境中使用版本以及其他常见问题解答的详细信息，请参阅知识中心文章。

Citrix Gateway

公用网络中的用户可以使用以下版本的 Citrix Gateway 访问 StoreFront。

- Citrix Gateway 14.1（自 2203 LTSR CU4 起开始支持）
- Citrix Gateway 13.1
- Citrix Gateway 13.0
- Citrix Gateway 12.1

可以使用 ICA 代理、Citrix Gateway 插件或无客户端 VPN (cVPN) 通过 Citrix Gateway 建立连接。

用户设备要求

StoreFront 提供了各种选项供用户用于访问自己的桌面和应用程序。Citrix 用户可以通过本地安装的 Citrix Workspace 应用程序访问应用商店，也可以在其浏览器中使用适用于 HTML5 的 Citrix Workspace 应用程序。

本地安装的 **Citrix Workspace** 应用程序

您可以使用 Citrix Workspace 应用程序当前受支持的所有版本通过内部网络连接和 Citrix Gateway 来访问 StoreFront 应用商店。有关 Citrix Workspace 应用程序生命周期日期，请参阅 https://www.citrix.com/support/product-lifecycle/workspace-app.html。

Web 浏览器中适用于 **HTML5** 的 **Citrix Workspace** 应用程序

可以使用适用于 HTML5 的 Citrix Workspace 应用程序通过 Web 浏览器访问您的应用商店。应用程序和桌面可以通过本机安装的 Citrix Workspace 应用程序（称为“混合启动”）启动，也可以在 Web 浏览器中启动。根据 Web 站点配置，最终用户可以在这两种启动方法之间切换。

请使用以下浏览器的最新版本。

在 Windows 中：

- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Internet Explorer 11 - 自 CU2 起，此设置只能用于浏览应用商店，不能用于连接到资源。

在 Mac 上：

- Safari
- Google Chrome
- Mozilla Firefox

在 Linux 上：

- Google Chrome
- Mozilla Firefox

有关使用适用于 HTML5 的 Citrix Workspace 应用程序通过 Web 浏览器连接到资源的要求的更多信息，请参阅适用于 HTML5 的 Citrix Workspace 应用程序文档。

传统设备

传统 Citrix 客户端可以使用 XenApp Services URL 访问功能减少的 StoreFront 应用商店。XenApp Services URL 为通过 Citrix Receiver 3.4 Enterprise 和较旧的客户端建立的连接提供向后兼容的旧版支持，这些客户端仅支持通过 PNAgent 建立的连接。

智能卡要求

使用带有智能卡的 **Citrix Workspace** 应用程序

Citrix 针对与美国国防部通用访问卡 (CAC)、国家标准和技术研究所个人身份验证 (NIST PIV) 卡及某些 USB 智能卡令牌的兼容性进行了测试。可以使用符合 USB 芯片/智能卡接口设备 (CCID) 规范并由德国 Zentraler Kreditausschuss (ZKA) 归类为“1 类”智能卡读卡器的接触式读卡器。ZKA“1 类”接触式读卡器需要用户将智能卡插入读卡器中。不支持其他类型的智能卡读卡器，包括“2 类”读卡器（具有输入 PIN 的键盘）、非接触式读卡器及基于受信任的平台模块 (TPM) 芯片的虚拟智能卡。

对于 Windows 设备，对智能卡的支持基于 Microsoft 个人计算机/智能卡 (Microsoft Personal Computer/Smart Card, PC/SC) 标准规范。智能卡和智能卡读卡器必须受操作系统支持且已收到 Windows 硬件认证，此为最低要求。

有关与 Citrix 兼容的智能卡和中间件的详细信息，请参阅 Citrix Virtual Apps and Desktops 文档中的智能卡以及 http://www.citrix.com/ready。

Citrix Analytics 服务要求

可以对 Citrix StoreFront 进行配置，以允许 Citrix Workspace 应用程序将数据发送到 Citrix Analytics 服务。Citrix Analytics 服务中将介绍配置详细信息。以下场景支持此功能：

- 可以通过 Web 浏览器访问的应用商店。
- 可以从适用于 Windows 的 Citrix Workspace 应用程序 1903 或更高版本访问的应用商店。

- 从适用于 Linux 的 Citrix Workspace 应用程序 1901 或更高版本访问的应用商店。

安装 **StoreFront**

April 17, 2024

安装和配置之前

要安装和配置 StoreFront，请按顺序完成以下步骤：

1. 检查系统要求。
2. 如果要使用 StoreFront 来向用户交付 Citrix Virtual Apps and Desktops 资源，请确保 StoreFront 服务器已加入包含相应用户帐户的 Microsoft Active Directory 域或与用户帐户域之间存在信任关系的域。

   > 重要提示：
   >
   > - 对于单服务器部署，可以在未加入域的服务器上安装 StoreFront。
   > - StoreFront 可以安装在域控制器上。

3. （可选）如果要配置多服务器 StoreFront 部署，请为 StoreFront 服务器设置一个负载平衡环境。

   要使用 Citrix ADC 进行负载平衡，应定义一个虚拟服务器作为 StoreFront 服务器的代理。有关通过配置 Citrix ADC 实现负载平衡的详细信息，请参阅使用 Citrix ADC 进行负载平衡。

4. 确保防火墙和其他网络设备允许从企业网络内部和外部访问 TCP 端口 80 或 443（如果适用）。此外，确保内部网络的任何防火墙或其他设备均不阻止通信流向任何未分配的 TCP 端口。

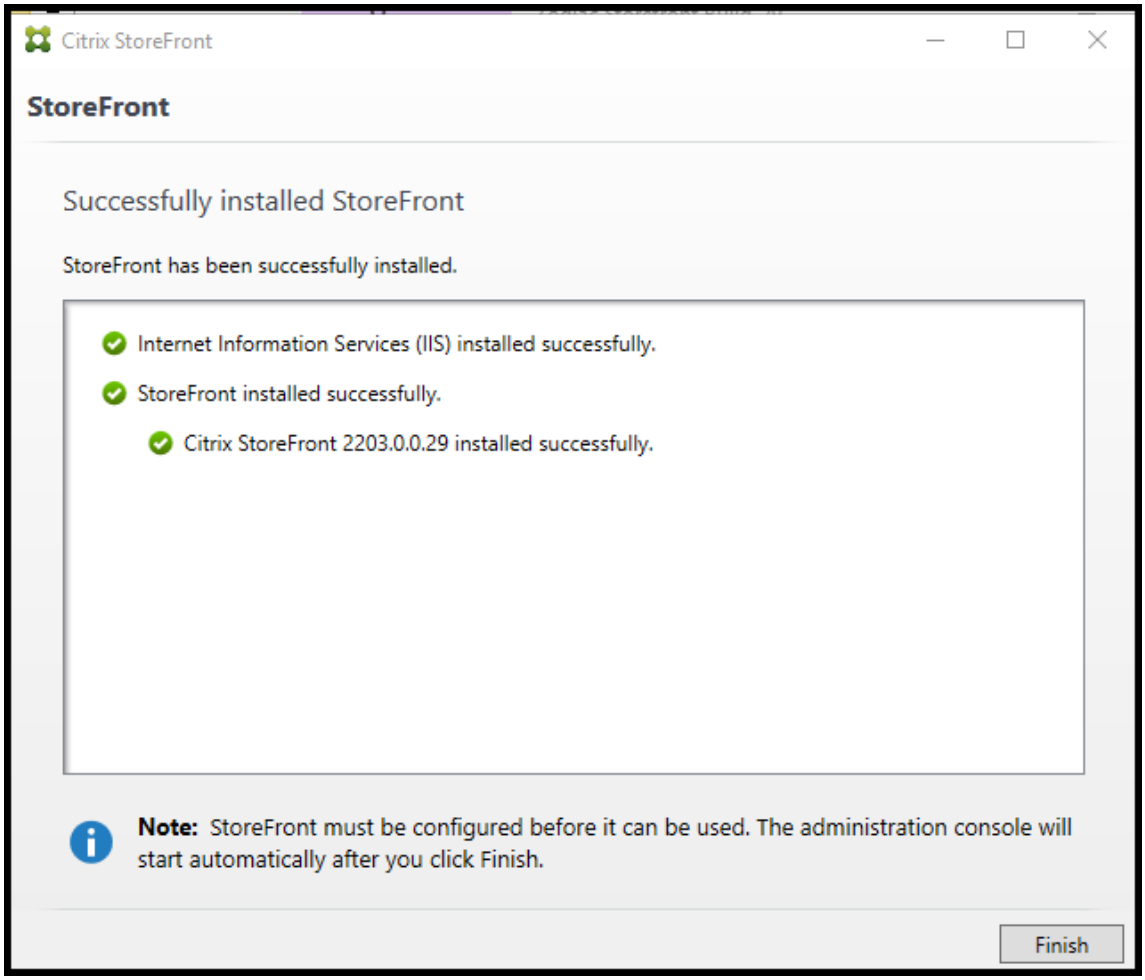
   安装 StoreFront 时，配置一个 Windows 防火墙规则，允许通过从所有非保留端口中随机选择的 TCP 端口访问 StoreFront 可执行文件。此端口用于在服务器组的各 StoreFront 服务器之间实现通信。

安装 **StoreFront**

> 重要
>
> 为避免安装 StoreFront 过程中可能会出现的错误和数据丢失情况，请务必关闭所有应用程序，并且不要在目标系统中运行任何其他任务或操作。

1. 从下载页面下载安装程序。
2. 使用具有本地管理员权限的帐户登录 StoreFront 服务器。
3. 如果使用 Windows 2016，请安装.NET Framework 4.7.2 或更高版本。在 Windows Server 2019 及更高版本中，这是一项 Windows 功能，默认情况下处于启用状态。

4. 找到 CitrixStoreFront-x64.exe，然后以管理员身份运行此文件。
5. 阅读并接受许可协议，然后单击下一步。
6. 如果显示检查必备项页面，请单击下一步。
7. 在已做好安装准备页面上，检查所列的安装必备项和 StoreFront 组件，然后单击安装。
8. 安装完成后，单击完成。



9. StoreFront 可能会要求重新启动以完成安装。单击是立即重新启动。
10. 为 HTTPS 配置 Microsoft Internet Information Services (IIS)。有关步骤，请参阅使用 HTTPS 保护 StoreFront 的安全。

从命令提示窗口安装 **StoreFront**

1. 使用具有本地管理员权限的帐户登录 StoreFront 服务器。
2. 安装 StoreFront 之前，请务必满足 StoreFront 安装的要求。有关详细信息，请参阅安装和配置之前。

3. 浏览您的安装介质或下载软件包，找到 CitrixStoreFront-x64.exe，然后将该文件复制到服务器上的一个临时位置。

4. 从命令提示窗口中，导航到包含安装文件的文件夹并键入以下命令。

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

使用 **-silent** 参数可无提示安装 StoreFront 及其必备项。默认情况下，StoreFront 安装在 C:\Program Files\Citrix\Receiver StoreFront 下。但是，可以使用 **-INSTALLDIR** 参数指定其他安装位置，其中 *installationlocation* 为 StoreFront 的安装目录。如果计划将服务器作为服务器组的一部分，则这些服务器之间的 StoreFront 安装位置和 IIS Web 站点设置、物理路径和站点 ID 必须一致。

默认情况下，当用户在 Windows 或 macOS 上使用 Web 浏览器打开应用商店时，如果检测不到 Citrix Workspace 应用程序，系统会提示用户从 Citrix Web 站点下载并安装恰当的适用于其平台的 Citrix Workspace 应用程序。您可以修改此行为，以使用户从 StoreFront 服务器下载 Citrix Workspace 应用程序安装文件。有关详细信息，请参阅配置资源对用户的显示方式。

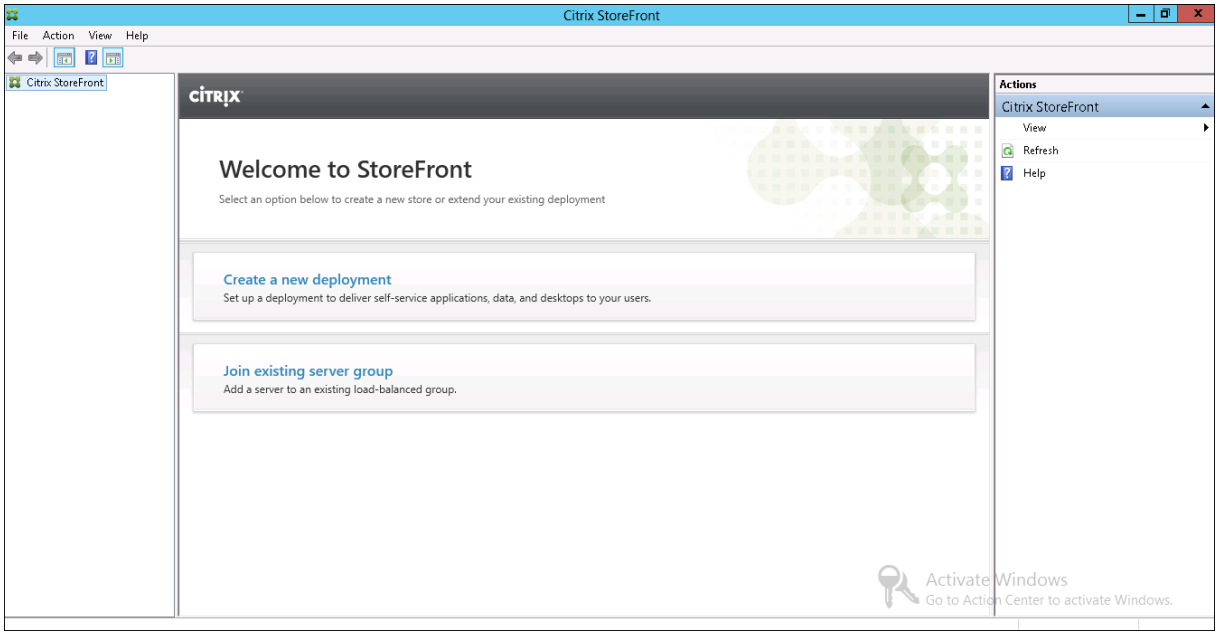
如果要更改此配置，请指定 **-WINDOWS_CLIENT** 和 **-MAC_CLIENT** 参数，以将 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序以及 Citrix Receiver for Mac 或适用于 Mac 的 Citrix Workspace 应用程序安装文件分别复制到 StoreFront 部署中的适当位置。请将 *filelocation* 替换为包含要复制的安装文件的目录，将 *filename* 替换为安装文件的名称。适用于 Windows 的 Citrix Workspace 应用程序和 Citrix Receiver for Mac 或适用于 Mac 的 Citrix Workspace 应用程序安装文件包含在 Citrix Virtual Apps and Desktops 安装介质中。

安装日志

有关日志文件的更多详细信息，请参阅安装日志。

配置 StoreFront

完成安装后，Citrix StoreFront 管理控制台将自动启动。您还可以从 “开始” 菜单打开 StoreFront。Citrix StoreFront 管理控制台首次启动时，会提供两个选项。



- 创建部署。在新 StoreFront 部署中配置第一台服务器。单服务器部署适用于评估 StoreFront 或小型生产部署。配置第一台 StoreFront 服务器后，可以随时向组中添加更多服务器，以提高部署的容量。
- 加入现有服务器组。将其他服务器添加到现有 StoreFront 部署中。选择此选项可快速提高 StoreFront 部署的容量。多服务器部署需要实现外部负载平衡。要添加服务器，需要访问部署中的现有服务器。

现在，用户可以通过浏览器或 Citrix Workspace 应用程序访问您的应用商店。请参阅用户指南。

Citrix 客户体验改善计划

September 29, 2023

如果您参与 Citrix 客户体验改善计划 (CEIP) 时，系统会向 Citrix 发送匿名统计数据和使用情况信息以提高 Citrix 产品的质量和性能。

默认情况下，安装 StoreFront 时会自动为您注册 CEIP。大约在您安装 StoreFront 七天后第一次上载数据。可以在注册表设置中更改此默认设置。如果在安装 StoreFront 之前更改注册表设置，则将使用该值。如果在升级 StoreFront 之前更改注册表设置，则将使用该值。

> 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。

控制自动上载分析数据的注册表设置（默认值为 1）：


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

默认情况下，**Enabled** 属性在注册表中处于隐藏状态。当它保持未指定时，启用自动上载功能。

使用 PowerShell 时，以下 cmdlet 禁用在 CEIP 中注册：

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

> 注意：
>
> 注册表设置控制同一台服务器上所有组件的匿名统计数据和使用情况信息的自动上载。例如，如果您已将 StoreFront 和 Delivery Controller 安装在同一台服务器上，并决定使用注册表设置选择退出 CEIP ，则选择退出将应用到这两个组件。

从 **StoreFront** 收集的 **CEIP** 数据

下表提供了收集的匿名信息的类型示例。数据中不包含任何识别出您是客户的详细信息。

数据	说明
StoreFront 版本	指示安装的 StoreFront 版本的字符串。例如，“3.8.0.0”
应用商店计数	表示部署中的应用商店数量的计数器。
服务器组中的服务器计数	表示服务器组中的服务器数量的计数器。
每个应用商店的 Delivery Controller 计数	指示可供部署中每个应用商店使用的 Delivery Controller 数量的数值列表。
启用 HTTPS	指示是否为部署启用 HTTPS 的字符串（“True”或“False”）。
Citrix Receiver for Web 的 HTML5 设置	字符串列表，指示每个 Receiver for Web 站点的 HTML5 Receiver 设置（“Always”、“Fallback”或“Off”）。
为 Citrix Receiver/Workspace 应用程序启用的工作区控制	布尔值列表，指示是否为每个 Receiver for Web 站点启用“工作区控制”（“True”或“False”）。
为应用商店启用远程访问	字符串列表，指示是否为部署中的每个应用商店启用“远程访问”（“ENABLED”或“DISABLED”）。
网关计数	表示部署中配置的 Citrix Gateway 数量的计数器。

Citrix Analytics 服务

April 17, 2024

如果您是 Monitor 客户，并且具有本地 StoreFront 部署，则可以配置 StoreFront，以便将数据发送到 Monitor 中的 Citrix Analytics 服务。配置后，Citrix Workspace 应用程序和 Web 浏览器会将用户事件发送到 Citrix Analytics 进行处理。Citrix Analytics 聚合有关用户、应用程序、端点、网络和数据的衡量指标，以全面了解用户行为。要在 Citrix Analytics 文档中阅读有关此功能的信息，请参阅使用 StoreFront 载入 Virtual Apps and Desktops 站点。

要配置此行为，请执行以下操作：

- 从 Citrix Analytics 下载配置文件。
- 使用 PowerShell 将 Citrix Analytics 数据导入到本地 StoreFront 部署中。

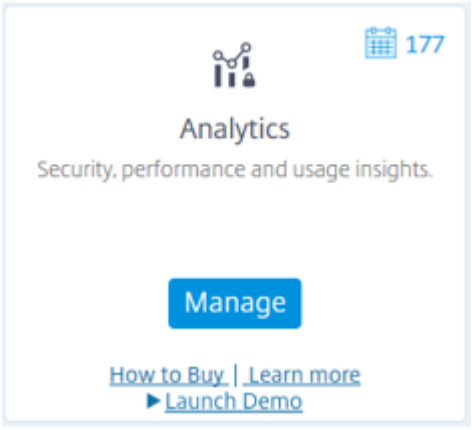
配置 StoreFront 后，当 Citrix Analytics 服务请求时，Citrix Workspace 应用程序可以从 StoreFront 应用商店发送数据。

> 重要提示：
>
> 要想使此功能正常工作并使用 Monitor 服务，您的 StoreFront 部署必须能够通过端口 443 联系以下地址：
>
> - `https://*.cloud.com`
> - `https://*.citrixdata.com`

从 Citrix Analytics 下载配置文件

> 重要提示：
>
> 初始配置需要包含敏感信息的配置文件。下载后保持文件安全。请勿与组织外部的任何人共享此文件。配置后，可以删除此文件。如果需要在另一台计算机上重新应用配置，可以从 Citrix Analytics 服务管理控制台重新下载该文件。

1. 使用管理员帐户登录到 Monitor (`https://citrix.cloud.com/`)。
2. 选择一个 Monitor 客户。
3. 单击管理打开 Citrix Analytics 服务管理控制台。



4. 在 Citrix Analytics 服务管理控制台中，选择设置 **>** 数据源。
5. 在“Virtual Apps and Desktops”卡中，选择 (⊠) 菜单图标，然后选择连接 **StoreFront** 部署。
6. 在“连接 StoreFront 部署”页面上，选择下载文件以下载 *StoreFrontConfigurationFile.json* 文件。

示例配置文件

```
{

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

<!--NeedCopy-->
```

其中

customerId 是当前 Monitor 客户的唯一 ID。

cwsServiceKey 是标识当前 Monitor 客户帐户的唯一键。

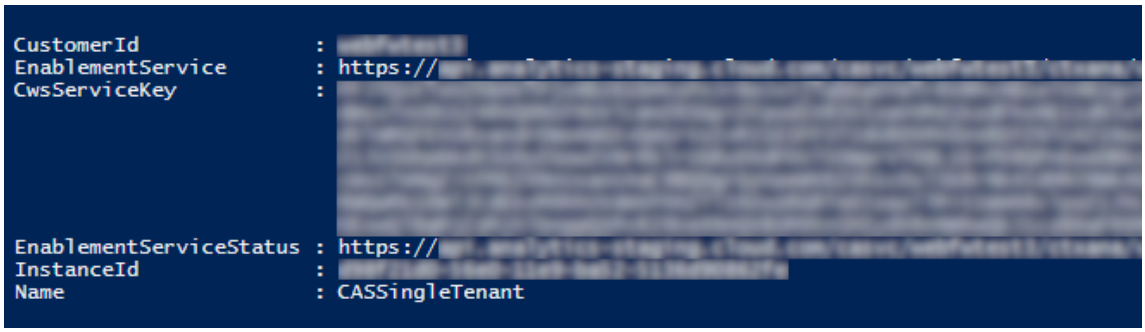
instanceID 是生成的 ID，用于对从 Citrix Workspace 应用程序发送到 Citrix Analytics 的请求进行签名（确保安全）。如果您向 Monitor 注册多个 StoreFront 服务器或服务器组，则每个服务器或服务器组都具有唯一的 instanceID。

将 **Citrix Analytics** 数据导入到 **StoreFront** 部署中

1. 将 *StoreFrontConfigurationFile.json* 文件复制到本地 StoreFront 服务器（或 StoreFront 服务器组中的一个服务器）上的合适的文件夹。以下命令假定该文件保存到桌面。
2. 打开 PowerShell ISE 并选择以管理员身份运行。
3. 运行以下命令：

```
Import-STFCasConfiguration -Path "$Env:UserProfile\Desktop\
   StoreFrontConfigurationFile.json"
Get-STFCasConfiguration
<!--NeedCopy-->
```

4. 此命令返回导入数据的副本，并在 PowerShell 控制台中显示该数据。



> 注意：
>
> 安装在 Windows Server 2012 R2 上的本地 StoreFront 服务器可能需要手动安装 C++ 运行时软件组件，以便它们可以注册到 CAS。如果在安装 Citrix Virtual Apps and Desktops 期间安装了 StoreFront，则不需要执行此步骤，因为 CVAD Metainstaller 已安装 C++ 运行时组件。如果仅使用未安装 C++ 运行时的 CitrixStoreFront-x64.exe Metainstaller 安装了 StoreFront，则在导入 CAS 配置文件后，它可能无法注册到 Monitor。

将 **Citrix Analytics** 数据传播到 **StoreFront** 服务器组

如果要对 StoreFront 服务器组执行这些操作，则必须将导入的 Citrix Analytics 数据传播到服务器组的所有成员。在单个 StoreFront 服务器部署中不需要执行此步骤。

要传播数据，请使用以下方法之一：

- 使用 StoreFront 管理控制台。
- 使用 PowerShell cmdlet **Publish-STFServerGroupConfiguration**。

检查 **StoreFront** 服务器组 **ID**

要检查您的部署是否已成功注册到 Citrix Analytics 服务，可以使用 PowerShell 来发现部署的 ServerGroupID。

1. 登录到您的 StoreFront 服务器或服务器组中的一台 StoreFront 服务器。
2. 打开 PowerShell ISE 并选择以管理员身份运行。
3. 运行以下命令：

```
$WebConfigPath = "C:\Program Files\Citrix\Receiver StoreFront\
    Framework\FrameworkData\Framework.xml"
$XMLObject = (Get-Content $WebConfigPath) -as [Xml]
$XMLObject.framework.properties.property
<!--NeedCopy-->
```

例如，这些命令生成如下所示的输出：

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

停止从 **StoreFront** 向 **Citrix Analytics** 发送数据

1. 打开 PowerShell ISE 并选择以管理员身份运行。
2. 运行以下命令：

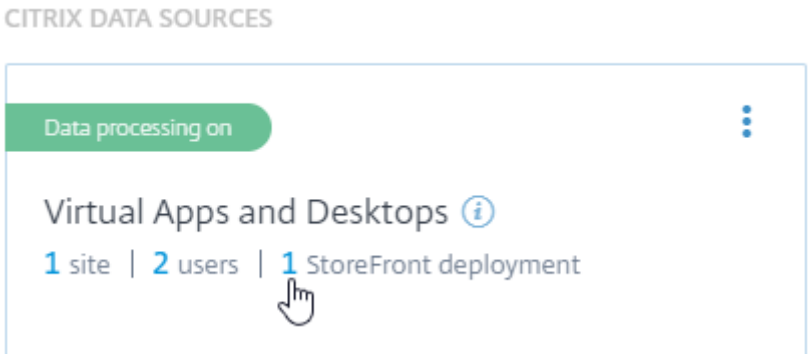
   ```
   Remove-STFCasConfiguration
   ```

   ```
   Get-STFCasConfiguration
   ```

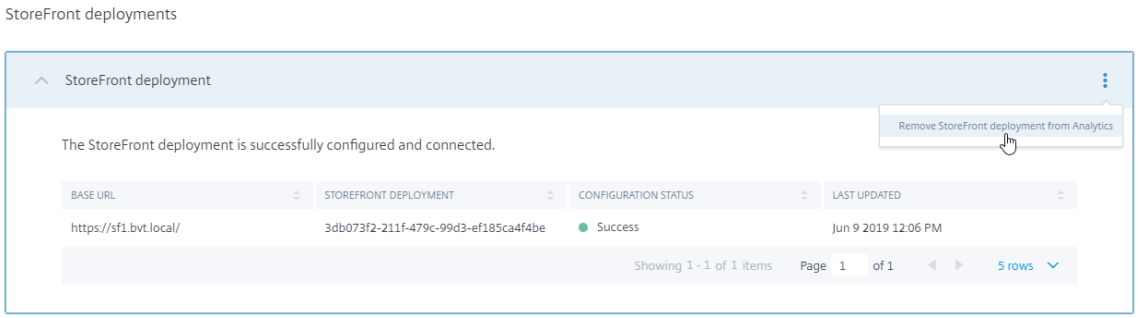
   如果以前导入的 Citrix Analytics 数据已被成功删除，**Get-STFCasConfiguration** 将不返回任何内容。
3. 如果要对 StoreFront 服务器组执行这些操作，请传播所做的更改并从服务器组的所有成员中删除导入的 Citrix Analytics 数据。在服务器组中的一个服务器上，运行以下命令：

   ```
   Publish-STFServerGroupConfiguration
   ```
4. 在任何其他服务器组成员上，运行以下命令以确认已成功从组中的所有服务器中删除 Citrix Analytics 配置：

   ```
   Get-STFCasConfiguration
   ```
5. 使用管理员帐户登录到 Monitor (`https://citrix.cloud.com/`)。
6. 选择一个 Monitor 客户。
7. 单击管理打开 Citrix Analytics 服务管理控制台。
8. 在 Citrix Analytics 服务管理控制台中，选择设置 **>** 数据源。
9. 在 Virtual App and Desktops 卡中，选择 StoreFront 部署计数：



10. 通过引用其主机基本 URL 和 ServerGroupID 来确定要删除的 StoreFront 部署。
11. 在 (⊠) 菜单中，选择从 **Analytics** 中删除 **StoreFront** 部署。



> 注意：
>
> 如果要从服务器端而非从 Citrix Analytics 中删除配置，StoreFront 部署条目将保留在 Citrix Analytics 中，但不会从 StoreFront 接收任何数据。如果仅从 Citrix Analytics 中删除配置，则 StoreFront 部署条目将在下次应用程序池回收时重新添加（在 IIS 重置时或每 24 小时自动完成）。

将 **StoreFront** 配置为使用 **Web** 代理联系 **Monitor** 并注册到 **Citrix Analytics**

如果 StoreFront 位于 Web 代理后面的主机 Web 服务器上，注册到 Citrix Analytics 将失败。如果 StoreFront 管理员在其 Citrix 部署中使用 HTTP 代理，绑定到 Internet 的 StoreFront 流量必须通过 Web 代理传输，然后才能到达云中的 Citrix Analytics。StoreFront 不会自动使用托管操作系统的代理设置；需要进行额外的配置来指示应用商店通过 Web 代理发送出站流量。可以通过向应用商店 web.config 文件中添加新部分来配置 <system.net> 代理配置。请对 StoreFront 服务器上将用于将数据发送到 Citrix Analytics 的每个应用商店执行此操作。

方法 **1**：通过 **PowerShell** 为一个或多个应用商店设置应用商店代理配置（推荐）

运行 PowerShell 脚本 Config-StoreProxy.ps1 会为一个或多个应用商店自动执行此过程，并自动插入有效 XML 以配置 <system.net>。该脚本还将应用商店 web.config 文件备份到当前用户的桌面，从而允许在必要时还原未修改的 web.config 文件。

> 注意：
>
> 多次运行脚本可能会导致添加 <system.net> XML 的多个副本。每个应用商店应该只有 <system.net> 的一个条目。添加多个副本会阻止应用商店代理配置正常工作。

1. 打开 PowerShell ISE 并选择以管理员身份运行。
2. 将 `$Stores = @("Store","Store2")` 设置为包括您希望使用 Web 代理配置的应用商店。
3. 请指定以下任一项：
   - IP 地址，或
   - Web 代理的 FQDN
4. 运行以下 PowerShell：

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

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

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

    foreach($Store in $Stores)
    {

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

         if(!(Test-Path "$env:UserProfile\desktop$Store"))
         {

             Write-Host "Creating $env:UserProfile\desktop$Store\
                directory for backup..." -ForegroundColor "Yellow"
             New-Item -Path "$env:UserProfile\desktop$Store" -
                ItemType "Directory" | Out-Null
             Write-Host "`n"
```



```
28          }
29
30
31          Write-Host "Copying c:\inetpub\wwwroot\Citrix$Store\web.
                config to $env:UserProfile\desktop$Store..." -
                ForegroundColor "Yellow"
32          Copy-Item -Path "c:\inetpub\wwwroot\Citrix$Store\web.
                config" -Destination "$env:UserProfile\desktop$Store" -
                Force | Out-Null
33
34          if(Test-Path "$env:UserProfile\desktop$Store\web.config")
35          {
36
37              Write-Host "$env:UserProfile\desktop$Store\web.config
                    file backed up" -ForegroundColor "Green"
38          }
39
40          else
41          {
42
43              Write-Host "$env:UserProfile\desktop$Store\web.config
                    file NOT found!" -ForegroundColor "Red"
44          }
45
46          Write-Host "`n"
47
48          Write-Host "Setting the proxy server to $ProxyAddress for
                Store $Store..." -ForegroundColor "Yellow"
49          Write-Host "`n"
50
51          $StoreConfigPath = "c:\inetpub\wwwroot\Citrix$Store\web.
                config"
52          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
53
54          if([string]::IsNullOrEmpty($ProxyFQDN))
55          {
56
57              $ProxyServer = ("HTTP://$ProxyIP"+":"+$ProxyPort)
58          }
59
60          else
61          {
62
63              $ProxyServer = ("HTTP://$ProxyFQDN"+":"+$ProxyPort)
64          }
65
66
67          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
68
69          # Create 3 elements
70          $SystemNet = $XMLObject.CreateNode("element","system.net",
                "")
71          $DefaultProxy = $XMLObject.CreateNode("element","
```



```
            defaultProxy","")
72          $Proxy = $XMLObject.CreateNode("element","proxy","")
73          $Proxy.SetAttribute("proxyaddress","$ProxyServer")
74          $Proxy.SetAttribute("bypassonlocal","true")
75
76          # Move back up the XML tree appending new child items in
                reverse order
77          $DefaultProxy.AppendChild($Proxy)
78          $SystemNet.AppendChild($DefaultProxy)
79          $XMLObject.configuration.AppendChild($SystemNet)
80
81          # Save the modified XML document to disk
82          $XMLObject.Save($StoreConfigPath)
83
84          Write-Host "Getting the proxy configuration for c:\inetpub
                \wwwroot\Citrix$Store..." -ForegroundColor "Yellow"
85          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
86          $ConfiguredProxyServer = $XMLObject.configuration.'system.
                net'.defaultProxy.proxy.proxyaddress | Out-Null
87          Write-Host ("Configured proxy server for Store $Store"+":
                "+ $ConfiguredProxyServer) -ForegroundColor "Green"
88          Write-Host "`n"
89       }
90
91      Write-Host "Restarting IIS..." -ForegroundColor "Yellow"
92      IISReset /RESTART
93   }
94
95
96  Set-StoreProxyServer -Stores $Stores -ProxyFQDN $ProxyFQDN -
        ProxyPort $ProxyPort
97  # OR
98  Set-StoreProxyServer -Stores $Stores -ProxyIP $ProxyIP -ProxyPort
        $ProxyPort
99  <!--NeedCopy-->
```

5. 检查 C:\inetpub\wwwroot\Citrix< Store>\web.config 现在是否包含在 web.config 文件末尾的新 <system.net> 部分中。

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

6. 按照将 Citrix Analytics 数据导入到 StoreFront 部署中所述导入 Citrix Analytics 数据。

方法 **2**：在应用商店 **web.config** 文件中手动添加 **<system.net>** 部分

必须对 StoreFront 服务器上将用于将数据发送到 Citrix Analytics 的每个应用商店执行此操作。

1. 备份应用商店的 web.config 文件，并将其复制到 C:\inetpub\wwwroot\Citrix< Store>\web.config 之外的其他位置。
2. 使用 FQDN 和端口组合或使用 IP 和端口组合通过代理设置修改以下 XML。

   例如，如果使用 FQDN 和端口组合，请使用以下 <system.net> 元素：

```
<system.net>
    <defaultProxy>
    <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
       bypassonlocal="true" />
    </defaultProxy>
</system.net>
<!--NeedCopy-->
```

   例如，如果使用 IP 和端口组合，请使用以下 <system.net> 元素：

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

3. 在应用商店 web.config 文件的末尾，插入适当的 <system.net> 元素，如下所示：

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

Insert the <system.net> element here

</configuration>
<!--NeedCopy-->
```


4. 按照将 Citrix Analytics 数据导入到 StoreFront 部署中所述导入 Citrix Analytics 数据。

使用 **HTTPS** 保护 **StoreFront** 的安全

April 17, 2024

Citrix 强烈建议使用 HTTPS 来确保 StoreFront 与用户设备之间的通信安全。这样可以确保在客户端与 StoreFront 之间发送的密码和其他数据经过加密。此外，普通的 HTTP 连接可能会受到各种攻击（例如中间人攻击）的破坏，尤其是在从公共 Wi-Fi 热点等不安全的位置建立连接时。如果没有合适的 IIS 配置，StoreFront 将使用 HTTP 进行通信。

根据您的配置，用户可以通过网关或负载平衡器访问 StoreFront。您可以在网关或负载平衡器上终止 HTTPS 连接。但是，在这种情况下，Citrix 仍然建议您使用 HTTPS 保护网关与 StoreFront 之间的连接安全。

如果没有为 HTTPS 配置 StoreFront，则会显示以下警告：

（状态警告“服务使用 HTTP 而非 HTTPS”）

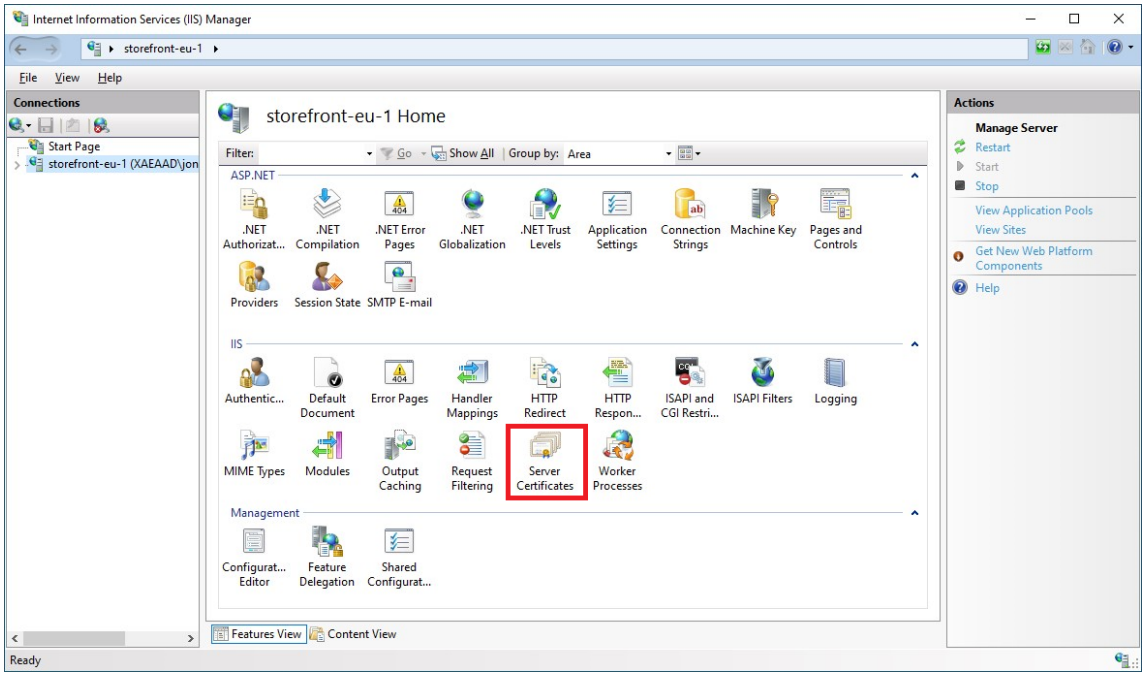
创建证书

- 请确保用于访问 StoreFront 的 FQDN 作为使用者备用名称 (SAN) 包含在 DNS 字段中。如果您使用的是负载平衡器，则同时包括单个服务器的 FQDN 和负载平衡器 FQDN
- 使用第三方 CA（例如 Verisign）或组织的企业根 CA 对证书进行签名。
- 以 PFX 格式导出证书（包括私钥）。

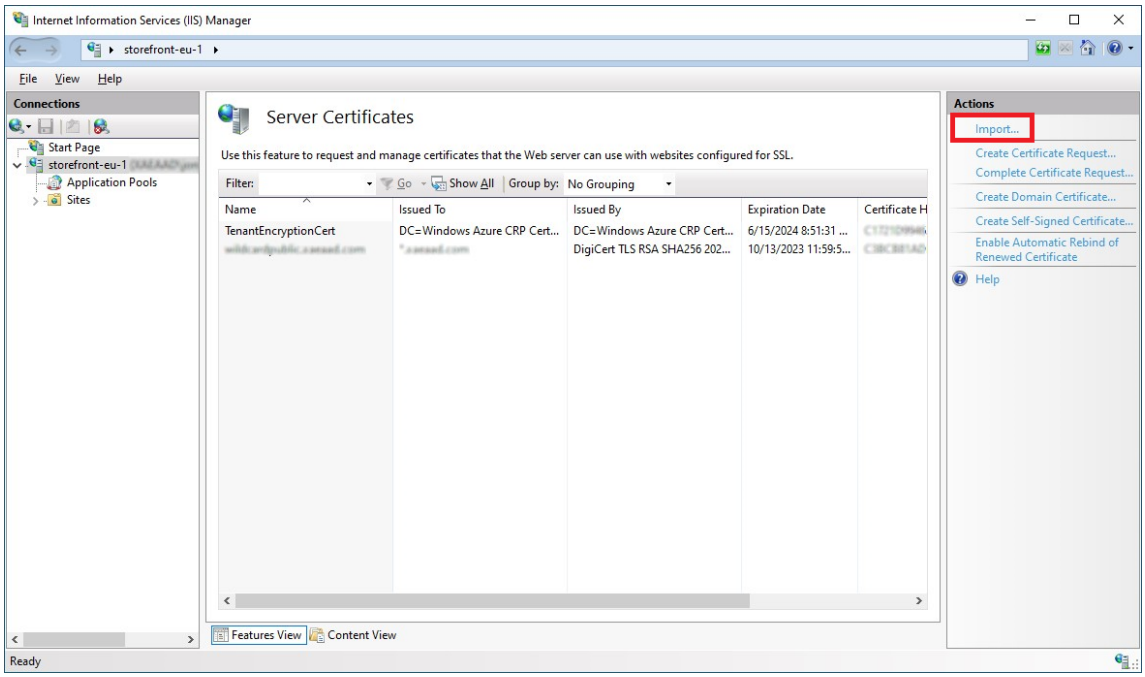
为 **HTTPS** 配置 **IIS**

要在 StoreFront 服务器上为 HTTPS 配置 Microsoft Internet Information Services (IIS)，请执行以下操作：

1. 打开 Internet Information Services (IIS) 管理器模块
2. 在左侧的树形视图中，选择服务器。
3. 在右侧窗格中，双击服务器证书

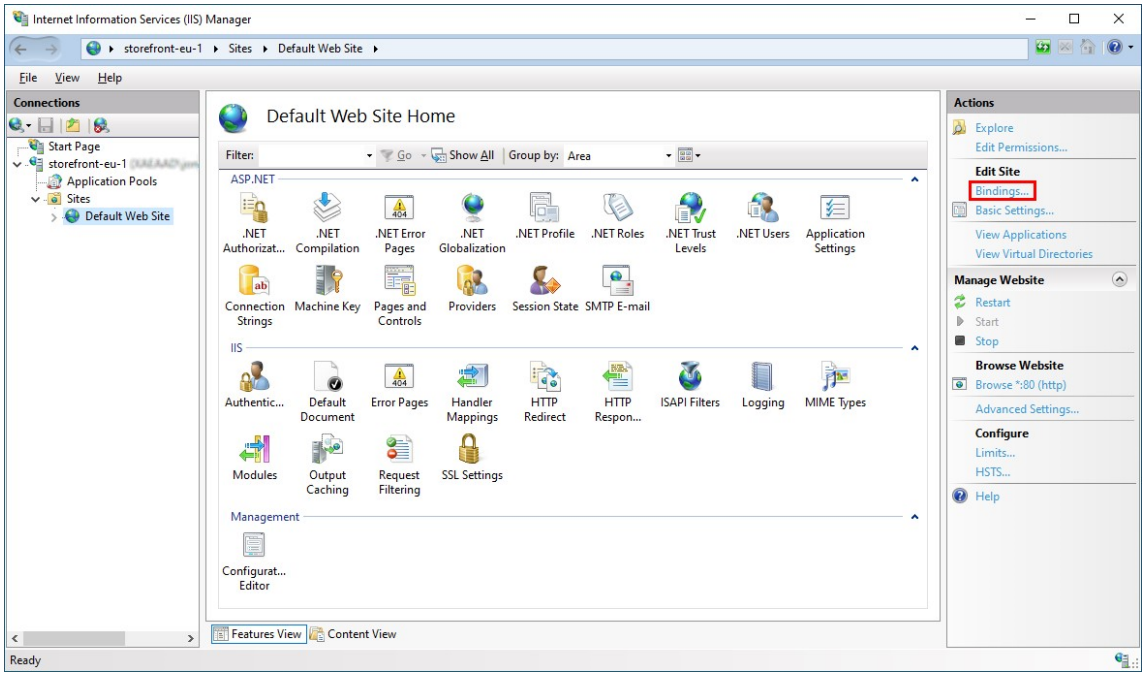


4. 在“服务器证书”屏幕中，您可以导入现有证书或者创建新证书。



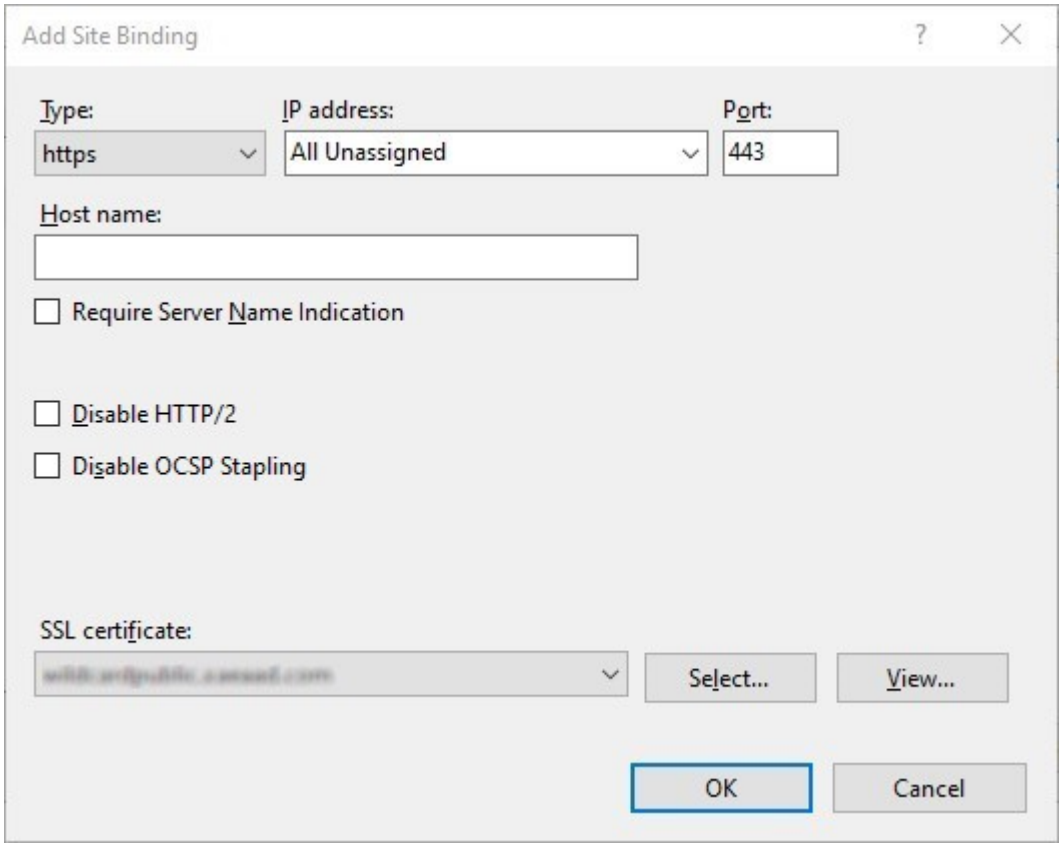
5. 在左侧的树形视图中，选择默认 **Web** 站点（或相应的 Web 站点）

6. 在“操作”窗格中，单击绑定…

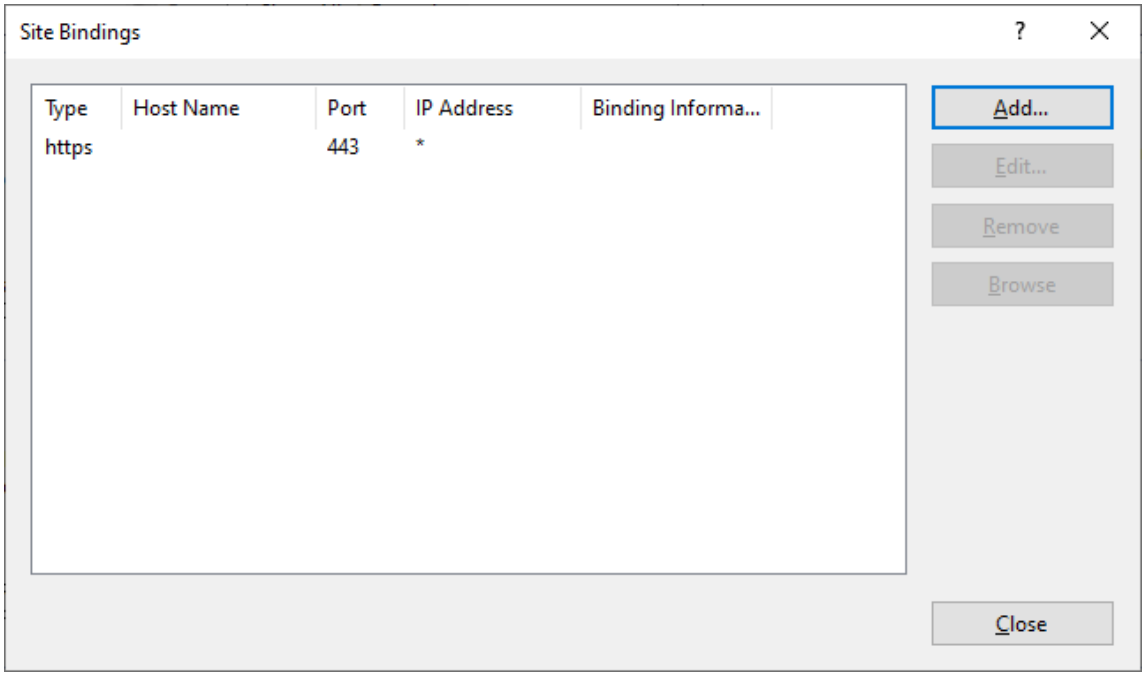


7. 在绑定窗口中，单击添加…
8. 在类型下拉列表中，选择 **https**
9. 在 Windows Server 2022 或更高版本中，单击禁用旧版 **TLS** 以禁用版本低于 1.2 的 TLS。

   在较旧的 Windows Server 版本中，可以使用 Windows 注册表设置禁用旧版 TLS 版本，请参阅 Windows Server 文档。
10. 选择之前导入的证书。按确定



11. 要删除 HTTP 访问权限，请选择“HTTP”，然后单击删除。

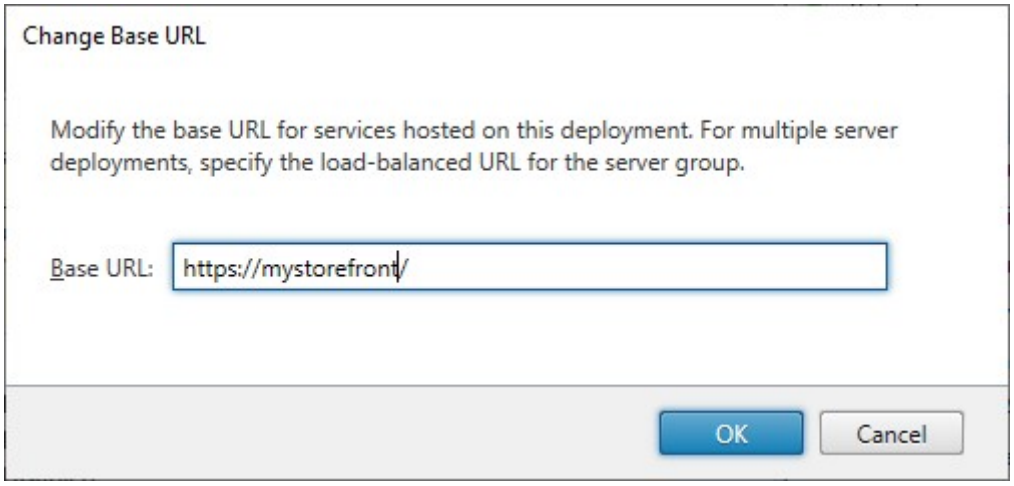


将 **StoreFront** 服务器基本 **URL** 从 **HTTP** 更改为 **HTTPS**

如果在未首先安装和配置 SSL 证书的情况下安装和配置 Citrix StoreFront，StoreFront 将使用 HTTP 进行通信。

如果稍后安装和配置 SSL 证书，请使用以下过程来确保 StoreFront 及其服务使用 HTTPS 连接。

1. 在 Citrix StoreFront 管理控制台中，在左侧窗格中选择服务器组。
2. 在“操作”窗格中，选择更改基本 **URL**。
3. 更新基本 URL 以启动 `https:`，然后单击确定。



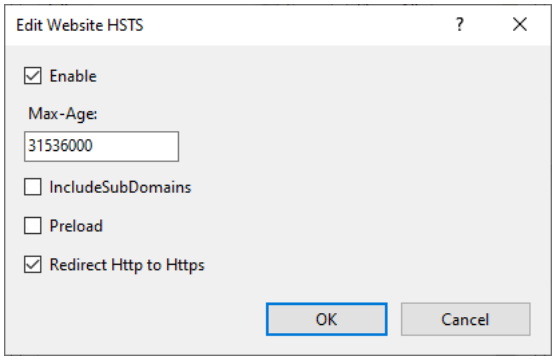
HSTS

即使您在服务器端启用了 HTTPS，用户的客户端设备也容易受到攻击。例如，中间人攻击者可以欺骗 StoreFront 服务器并诱使用户通过普通 HTTP 连接到欺骗服务器。然后，他们可以访问敏感信息，例如用户的证书。解决方案是确保用户的浏览器不会尝试通过 HTTP 访问 RfWeb 服务器。您可以通过 HTTP 严格传输安全性 (HSTS) 来实现这一点。

启用 HSTS 后，服务器会向 Web 浏览器指示只应通过 HTTPS 向 Web 站点发出请求。如果用户尝试使用 HTTP 访问 URL，浏览器将自动切换到使用 HTTPS。这样可以确保安全连接的客户端验证以及在 IIS 中进行服务器端验证。Web 浏览器将在配置的时间段内保持此验证。

在 Windows Server 2019 及更高版本上：

1. 打开 **Internet Information Services (IIS)** 管理器
2. 选择默认 **Web** 站点（或相应的 Web 站点）。
3. 在右侧的操作窗格中，单击 **HSTS**…
4. 勾选启用，输入最长保留时间，例如 31536000（表示一年），然后勾选 **Redirect HTTP to HTTPS**（将 HTTP 重定向到 HTTPS）。
5. 按确定



> 注意：
>
> 启用 HSTS 会影响同一域中的所有 Web 站点。例如，如果可以通过 https://www.company.com/Citrix/StoreWeb 访问 Web 站点，则 HSTS 策略将应用到 https://www.company.com 下的所有 Web 站点，这可能并不需要。

保护 **StoreFront** 部署的安全

April 17, 2024

本文重点介绍在部署和配置 StoreFront 时可能会影响系统安全的几方面内容。

最终用户与 **StoreFront** 之间的通信

Citrix 建议使用 HTTPS 来确保用户的设备与 StoreFront 之间的通信安全。这样可以确保在客户端与 StoreFront 之间发送的密码和其他数据经过加密。此外，普通的 HTTP 连接可能会受到各种攻击（例如中间人攻击）的破坏，尤其是在从公共 Wi-Fi 热点等不安全的位置建立连接时。如果没有合适的 IIS 配置，StoreFront 将使用 HTTP 进行通信。

根据您的配置，用户可以通过网关或负载平衡器访问 StoreFront。您可以在网关或负载平衡器上终止 HTTPS 连接。但是，在这种情况下，Citrix 仍然建议您使用 HTTPS 保护网关或负载平衡器与 StoreFront 之间的连接安全。

要启用 HTTPS、禁用 HTTP 并启用 HSTS，请参阅使用 HTTPS 保护 StoreFront 的安全。

StoreFront 与 **Citrix Virtual Apps and Desktops** 服务器之间的通信

Citrix 建议使用 HTTPS 协议来保护 StoreFront 与您的 Citrix Virtual Apps and Desktops Delivery Controller 之间的数据传输安全。请参阅在 Controller 上安装 TLS 服务器证书。StoreFront 不支持在 StoreFront 与 Delivery Controller 之间使用 TLS 1.0 或 TLS 1.1 协议。或者，您可以使用 IPSec 配置 Windows 来保护服务器之间的通信。

可以配置 Delivery Controller 和 StoreFront 以确保只有可信 StoreFront 服务器才能与 Delivery Controller 通信，请参阅管理安全密钥。

StoreFront 与 Cloud Connector 的通信

Citrix 建议使用 HTTPS 协议来保护 StoreFront 与您的 Cloud Connector 之间的数据传输安全。请参阅 How to Enable SSL on Cloud Connectors to Secure XML Traffic（如何在 Cloud Connector 上启用 SSL 以保护 XML 流量的安全）。StoreFront 不支持在 StoreFront 与 Cloud Connector 之间使用 TLS 1.0 或 TLS 1.1 协议。或者，您可以使用 IPSec 配置 Windows 来保护服务器之间的通信。

远程访问

Citrix 不建议将您的 StoreFront 服务器直接暴露给 Internet。Citrix 建议使用 Citrix Gateway 为远程用户提供身份验证和访问权限。

Microsoft Internet Information Services (IIS) 强化

可以配置具有受限 IIS 配置的 StoreFront。请注意，这不是默认 IIS 配置。

文件扩展名

可以使用请求筛选来配置允许使用的文件扩展名列表以及禁止未列出的文件扩展名列表。请参阅 IIS 文档。

StoreFront 需要以下文件扩展名：

- .（空扩展名）
- .appcache
- .aspx
- “cr”，
- .css
- .dtd
- .png
- .htm
- .html
- ica
- .ico
- .jpg
- .js
- .png
- .svg
- .txt
- .xml

如果为应用商店 Web 站点启用了 Citrix Workspace 应用程序的下载或升级，StoreFront 还要求使用以下文件扩展名：

- .dmg
- .exe

如果启用了适用于 HTML5 的 Citrix Workspace 应用程序，StoreFront 还要求使用以下文件扩展名：

- .eot
- .ttf
- .woff
- .wasm

动词

可以使用请求筛选来配置允许使用的动词列表以及禁止使用未列出的动词。请参阅 IIS 文档。

- GET
- POST
- HEAD

URL 中的非 **ASCII** 字符

如果您确保应用商店名称和 Web 站点名称仅使用 ASCII 字符，StoreFront URL 将不包含 ASCII 字符。您可以使用请求筛选来禁止使用非 ASCII 字符。请参阅 IIS 文档。

MIME 类型

可以删除与以下文件扩展名对应的操作系统 shell MIME 类型：

- .exe
- .dll
- .com
- .bat
- .csh

请参阅 IIS 文档。

删除 **X-Powered-By** 标头

默认情况下，IIS 通过添加值为 `ASP.NET` 的 `X-Powered-By` 标头来报告其正在使用 ASP.NET。可以将 IIS 配置为删除此标头。请参阅 IIS 自定义标头文档。

删除 **IIS** 版本附带的 **Server** 标头

默认情况下，IIS 通过添加 `Server` 标头来报告 IIS 版本。可以将 IIS 配置为删除此标头。请参阅 IIS 请求筛选文档。

将 **StoreFront Web** 站点移至单独的分区

您可以将 StoreFront Web 站点托管在与系统文件不同的分区上。在 IIS 中，在创建 StoreFront 部署之前，您必须在相应的分区上移动默认 **Web** 站点或者创建单独的站点。

IIS 功能

有关 StoreFront 安装和使用的 IIS 功能列表，请参阅系统要求。可以删除其他 IIS 功能。

尽管 StoreFront 不直接使用 ISAPI 过滤器，但该功能是 ASP.NET 所必需的，因此无法卸载。

处理程序映射

StoreFront 需要以下处理程序映射。可以删除其他处理程序映射。

- ExtensionlessUrlHandler-Integrated-4.0
- PageHandlerFactory-Integrated-4.0
- StaticFile

请参阅 IIS 处理程序文档。

ISAPI 过滤器

StoreFront 不需要任何 ISAPI 过滤器。可以删除所有 ISAPI 过滤器。请参阅 IIS ISAPI 过滤器文档。

.NET 授权规则

默认情况下，IIS 服务器将“.NET 授权规则”设置为“允许所有用户”。默认情况下，StoreFront 使用的 Web 站点会继承此配置。

如果您在服务器级别删除或更改.NET 授权规则，则必须覆盖 StoreFront 使用的 Web 站点上的规则，为“所有用户”添加允许规则并删除任何其他规则。

应用程序池

StoreFront 将创建以下应用程序池：

- Citrix 配置 API
- Citrix Delivery Services 身份验证
- Citrix Delivery Services 资源
- 和 Citrix Receiver for Web

请勿更改每个 IIS 应用程序使用的应用程序池或每个池的标识。如果您使用多个站点，则无法将每个站点配置为使用单独的应用程序池。

在“Recycling settings”（回收设置）下，您可以设置应用程序池空闲超时和虚拟内存限制。请注意，当“Citrix Receiver for Web”应用程序池回收时，它会导致通过 Web 浏览器登录的用户被注销，因此它默认设置为每天 02:00 回收以最大限度地减少中断。如果您更改任何回收设置，则可能会导致用户在一天中的其他时间被注销。

必需设置

- 请勿更改 IIS 身份验证设置。StoreFront 管理身份验证并使用适当的身份验证设置配置 StoreFront 站点的目录。
- 对于 **SSL Settings**（SSL 设置）下的 StoreFront 服务器，请勿选择 **Client certificates: Require**（客户端证书: 必需）。StoreFront 安装配置具有此设置的 StoreFront 站点的恰当页面。
- StoreFront 需要 cookie 来获取会话状态和其他功能。在某些目录中，在 **Session State**（会话状态）的 **Cookie Settings**（cookie 设置）下，**Mode**（模式）必须设置为 **Use Cookies**（使用 cookie）。
- StoreFront 要求将 **.NET Trust Level**（.NET 信任级别）设置为 **Full Trust**（完全信任）。请勿将.NET 信任级别设置为任何其他值。

服务

StoreFront 安装将创建以下 Windows 服务：

- Citrix Configuration Replication (NT SERVICE\CitrixConfigurationReplication)
- Citrix Cluster Join (NT SERVICE\CitrixClusterService)
- Citrix Peer Resolution (NT SERVICE\Citrix Peer Resolution Service)
- Citrix Credential Wallet (NT SERVICE\CitrixCredentialWallet)
- Citrix Subscriptions Store (NT SERVICE\CitrixSubscriptionsStore)
- Citrix Default Domain Services (NT SERVICE\CitrixDefaultDomainService)

这些帐户作为 `Network Service` 登录。请勿更改此配置。

如果您为 XenApp 6.5 配置了 StoreFront Kerberos 约束委派，此操作还会创建 Citrix StoreFront Protocol Transition Service (NT SERVICE\CitrixStoreFrontProtocolTransition)。此服务作为 `NT AUTHORITY\SYSTEM` 运行。请勿更改此配置。

用户权限分配

将“用户权限分配”的默认值修改为其他值可能会导致 StoreFront 出现问题。特别是：

- Microsoft IIS 作为 StoreFront 安装的一部分启用。Microsoft IIS 向内置组 IIS_IUSRS 授予登录权限作为批处理作业登录以及权限身份验证后模拟客户端。这是正常的 Microsoft IIS 安装行为。请不要更改这些用户权限。请参阅 Microsoft 文档了解详细信息。
- 安装 StoreFront 时，它会创建应用程序池，IIS 会向其授予用户权限 **Log on as a service**（作为服务登录）、**Adjust memory quotas for a process**（为进程调整内存配额）、**Generate security audits**（生成安全审核）以及 **Replace a process level token**（替换进程级令牌）。
- 要使服务器加入服务器组，管理员组必须具有 **Restore files and directories**（还原文件和目录）、**Access this computer from the network**（从网络访问此计算机）以及 **Manage auditing and security log**（管理审核和安全日志）的权限。
- 要让用户使用用户名和密码身份验证（直接或通过网关）登录，除非您已将 StoreFront 配置为通过 Delivery Controller 验证密码，否则他们必须拥有“允许本地登录”的权限。

这不是一个综合性列表，可能需要其他用户访问权限。

配置组成员身份

配置 StoreFront 服务器组时，以下服务将添加到管理员安全组：

- Citrix Configuration Replication (NT SERVICE\CitrixConfigurationReplication)
- Citrix Cluster Join (NT SERVICE\CitrixClusterService)。此服务仅在组中的服务器上可见，并且仅在加入操作过程中运行。

StoreFront 需要这些组成员身份才能正确运行，以便执行以下操作：

- 创建、导出、导入和删除证书以及设置对证书的访问权限
- 读取和写入 Windows 注册表
- 添加和删除全局程序集缓存 (GAC) 中的 Microsoft .NET Framework 程序集
- 访问文件夹 **Program Files\Citrix**<*StoreFrontLocation*>
- 添加、修改和删除 IIS 应用程序池标识和 IIS Web 应用程序
- 添加、修改和删除本地安全组和防火墙规则
- 添加和删除 Windows 服务以及 PowerShell 管理单元
- 注册 Microsoft Windows Communication Framework (WCF) 端点

在 StoreFront 的更新中，此操作列表如有更改，恕不另行通知。

StoreFront 安装还将创建以下本地安全组：

- CitrixClusterMembers

- CitrixCWServiceReadUsers
- CitrixCWServiceWriteUsers
- CitrixDelegatedAuthenticatorUsers
- CitrixDelegatedDirectoryClaimFactoryUsers
- CitrixPNRSReplicators
- CitrixPNRSUsers
- CitrixStoreFrontAdministrators
- CitrixSubscriptionServerUsers
- CitrixSubscriptionsStoreServiceUsers
- CitrixSubscriptionsSyncUsers

StoreFront 负责维护这些安全组的成员身份。这些安全组用于 StoreFront 内部的访问控制，不适用于文件和文件夹等 Windows 资源。请勿修改这些组成员身份。

StoreFront 中的证书

服务器证书

在 StoreFront 中，服务器证书用于计算机标识和传输层安全性 (TLS) 传输安全性。如果决定启用 ICA 文件签名，StoreFront 还可以使用证书对 ICA 文件进行数字签名。

有关详细信息，请参阅最终用户与 StoreFront 之间的通信以及 Ica 文件签名。

令牌管理证书

身份验证服务和应用商店都需要使用证书进行令牌管理。StoreFront 会在创建身份验证服务或应用商店时生成一个自签名的证书。不应将 StoreFront 生成的自签名证书用于任何其他用途。

Citrix 交付服务证书

StoreFront 在自定义 Windows 证书存储 (Citrix 交付服务) 中存储了多个证书。Citrix Configuration Replication Service、Citrix Credential Wallet 服务和 Citrix Subscriptions Store 服务都使用这些证书。群集中的每个 StoreFront 服务器都具有这些证书的副本。这些服务不依赖 TLS 进行安全通信，并且这些证书不用作 TLS 服务器证书。这些证书是在创建 StoreFront 应用商店或安装 StoreFront 时创建的。请勿修改此 Windows 证书存储的内容。

代码签名证书

StoreFront 在 <*InstallDirectory*>\Scripts 下的文件夹中存储了多个 PowerShell 脚本 (.ps1)。默认 StoreFront 安装不使用这些脚本。这些脚本简化了不经常执行的特定任务的配置步骤。这些脚本已签名，允许 StoreFront 支持

PowerShell 执行策略。我们建议使用 **AllSigned** 策略。（限制策略不受支持，因为这会阻止执行 PowerShell 脚本。）StoreFront 不会更改 PowerShell 执行策略。

虽然 StoreFront 不安装“受信任的发布者”存储中的代码签名证书，但是，Windows 仍然能够自动在此处添加代码签名证书。通过始终运行选项执行 PowerShell 脚本时会出现此问题。（如果选择永不运行选项，证书将被添加到“不信任的证书”存储中，并且 StoreFront PowerShell 脚本将不执行。）将代码签名证书添加到“受信任的发布者”存储中后，Windows 不再检查其是否过期。可以在完成 StoreFront 任务后从“受信任的发布者”存储中删除此证书。

禁用旧版 **TLS**

Citrix 建议您在 Windows Server 上禁用 TLS 1.0 和 1.1 以进行客户端和服务器通信。可以通过组策略或者 Windows 注册表设置来执行此操作。请参阅 Microsoft 文档。

StoreFront 安全分离

如果您在与 StoreFront 相同的 Web 域（域名和端口均相同）中部署任何 Web 应用程序，则这些 Web 应用程序中存在的任何安全风险可能会潜在地降低 StoreFront 部署的安全性。如果环境中需要更大程度的安全隔离，Citrix 建议您在单独的 Web 域中部署 StoreFront。

ICA 文件签名

StoreFront 提供了使用服务器上的指定证书对 ICA 文件进行数字签名的选项，以便支持此功能的 Citrix Workspace 应用程序版本能够验证文件是否来自受信任的来源。可以使用 StoreFront 服务器上运行的操作系统所支持的任何哈希算法（包括 SHA-1 和 SHA-256）对 ICA 文件进行签名。有关详细信息，请参阅启用 ICA 文件签名。

用户更改密码

可以允许使用 Active Directory 域凭据通过 Web 浏览器登录的用户随时或仅当过期时更改自己的密码。但是，这会将敏感的安全功能暴露给那些可访问使用该身份验证服务的任何应用商店的用户。如果贵组织的安全策略将用户密码更改功能保留为仅供内部使用，请确保用户无法从企业网络外部访问任何应用商店。创建身份验证服务时，默认配置会阻止用户更改自己的密码，即使密码已到期亦如此。有关详细信息，请参阅允许用户更改密码。

自定义设置

为增强安全性，请勿写入从服务器加载内容或脚本且不受您控制的自定义设置。请将内容或脚本复制到从中创建自定义设置的 Web 站点自定义文件夹。如果为 HTTPS 连接配置了 StoreFront，请确保指向自定义内容或脚本的所有链接也使用 HTTPS。

安全标题

通过 Web 浏览器查看应用商店 Web 站点时，StoreFront 会返回以下与安全相关的标题，这些标题对 Web 浏览器施加了限制。

标题名称	值	说明
`content-security-policy`	`frame-ancestors 'none'`	这样可以防止其他站点将 StoreFront Web 站点嵌入到框架中，从而避免单击劫持攻击。StoreFront 使用内联脚本和样式，因此无法使用屏蔽这些脚本和样式的 content-security-policy。StoreFront Web 站点仅显示管理员配置的内容，不显示用户输入的任何内容，因此无需阻止内联脚本。
`X-Content-Type-Options`	`nosniff`	这样可以避免 MIME 类型探查。
`X-Frame-Options`	`deny`	这样可以防止其他站点将 StoreFront Web 站点嵌入到框架中，从而避免单击劫持攻击。它已被 `content-security-policy` 到 `frame-ancestors 'none'` 弃用，但一些不支持 `content-security-policy` 的较旧浏览器可以理解
`X-XSS-Protection`	`1; mode=block`	某些浏览器用来缓解 XSS（跨站脚本）攻击

cookie

StoreFront 使用多个 cookie。Web 站点的运营中使用的一些 cookie 如下所示：

cookie	说明
`ASP.NET_SessionId`	跟踪用户的会话，包括身份验证状态。已设置 `HttpOnly`。

cookie	说明
`CtxsAuthId`	为了防止会话固定攻击，StoreFront 还会跟踪用户是否使用此 cookie 进行身份验证。它已设置 `HttpOnly`。
`CsrfToken`	用于防止通过标准 Cookie-to-header 令牌模式伪造跨站点请求。服务器在 cookie 中设置令牌。客户端从 cookie 中读取令牌，并将该令牌包含在查询字符串或后续请求中的标头中。此 cookie 必须未设置 `HttpOnly`，以便 JavaScript 客户端能够读取。
`CtxsDeviceId`	识别设备。已设置 `HttpOnly`。

StoreFront 设置了许多其他 cookie 来跟踪用户状态，其中一些 cookie 需要由 JavaScript 读取，因此未设置 `HttpOnly`。这些 cookie 不包含与身份验证或其他机密信息有关的任何信息。

其他安全信息

> 注意：
>
> 此信息可能会随时更改，恕不另行通知。

出于监管原因，您的组织可能希望对 StoreFront 执行安全扫描。上述配置选项有助于消除安全扫描报告中的某些发现。

如果安全扫描程序和 StoreFront 之间存在网关，特定发现可能会与网关有关，而非与 StoreFront 本身有关。安全扫描报告通常不会区分这些发现（例如，TLS 配置）。因此，安全扫描报告中的技术说明可能会引起误解。

基于电子邮件的帐户发现

February 22, 2024

可以配置基于电子邮件的帐户发现，以使第一次在设备上安装 Citrix Workspace 应用程序的用户可以通过输入电子邮件地址来设置其帐户，而不需要知晓应用商店 URL。

在初始配置过程中，Citrix Workspace 应用程序会提示用户输入电子邮件地址或应用商店 URL。如果用户输入电子邮件地址，Citrix Workspace 应用程序会在多个位置查找电子邮件域以确定 StoreFront 服务器。然后，它会列出所有可见的应用商店供用户从中进行选择。

Citrix 建议使用 Global App Config Service 来配置电子邮件发现。作为替代方案，您可以使用 DNS SVR 记录或 DNS 别名来配置电子邮件发现。

Global App Config Service

要使用 Glboal App Cofig Service 配置电子邮件发现，请参阅设置基于电子邮件的发现。

DNS SVR 记录记录

作为 Global App Config Service 的替代方案，您可以使用 DNS SVR 记录来配置 Citrix Workspace 应用程序应为电子邮件域使用哪个 StoreFront 服务器。

在您的电子邮件域的 DNS 服务器上，添加具有以下属性的 **SRV** 记录：

属性	值
服务	_citrixreceiver
Proto	TCP
目标	Citrix Gateway 设备（用于同时支持本地和远程用户）或 StoreFront 服务器（用于仅支持本地用户）的完全限定域名 (FQDN) 和端口，格式为 *servername.domain:port*。

如果您的环境中同时包括内部和外部 DNS 服务器，可以添加内部 DNS 服务器上用于指定 StoreFront 服务器 FQDN 的 SRV 记录以及外部服务器上用于指定 Citrix Gateway FQDN 的其他记录。通过此配置，可以为本地用户提供 StoreFront 详细信息，而远程用户将接收 Citrix Gateway 连接信息。

DNS discoverReceiver 记录

作为其他方法的备用方法，您可以在电子邮件域上创建 StoreFront 服务器的 DNS 别名 `discoverReceiver`。例如，如果您的电子邮件域为 `example.com`，则创建一个名为 `discoverReceiver.example.com` 的 DNS 别名。如果在指定域中未找到 SRV 记录，则 Citrix Workspace 应用程序将搜索名为 discoverReceiver 的计算机，以识别 StoreFront 服务器。

如果您使用此机制，请确保将 `discoverReceiver` 作为使用者备用名称包含在 StoreFront 服务器的 HTTPS 证书中。

创建新部署

December 5, 2023

1. 如果 Citrix StoreFront 管理控制台在安装 StoreFront 后未打开，请在 Windows“开始”屏幕或“应用程序”屏幕中，找到并单击 Citrix StoreFront 磁贴。
2. 在 Citrix StoreFront 管理控制台的结果窗格中，单击创建新部署。
3. 如果有多个 IIS 站点，请从 **IIS** 站点下拉列表中选择要使用的站点。
4. 如果使用单个 StoreFront 服务器，请输入服务器 URL 基本 **URL**。如果您要在负载平衡器后面配置多个 StoreFront 服务器，请输入负载平衡 URL 作为基本 **URL**。

   如果尚未设置负载平衡环境，请输入服务器 URL。可以随时修改部署的基本 URL。
5. 单击下一步，然后按照创建应用商店中的说明配置您的第一个应用商店。
6. 完成所有配置步骤后，单击创建以创建部署和应用商店。
7. StoreFront 显示其创建的应用商店的摘要。单击完成。

使用 **PowerShell SDK** 创建新部署

要使用 PowerShell SDK 创建部署，请调用 cmdlet Add-STFDeployment。

多个 **Internet Information Services (IIS) Web** 站点

StoreFront 允许您在每个 Windows 服务器的不同 IIS Web 站点中部署不同的应用商店，以便每个应用商店都具有不同的主机名和证书绑定。

要创建多个 Web 站点，请参阅 Microsoft IIS 文档。

无法使用管理控制台创建多个 StoreFront 部署；必须使用 PowerShell SDK。例如，要创建两个 IIS Web 站点部署，一个用于应用程序，一个用于桌面，请使用以下命令：

```
Add-STFDeployment -SiteID 1 -HostBaseURL "https://apps.example.com"
Add-STFDeployment -SiteID 2 -HostBaseURL "https://desktops.example.com"
<!--NeedCopy-->
```

启用多个站点后，StoreFront 将禁用管理控制台，并且无法将 StoreFront 恢复到单站点模式。必须使用 StoreFront SDK 配置站点，并在每个命令中包括 `SiteID`。

加入现有服务器组

April 17, 2024

在要添加到组的服务器上安装 StoreFront 之前，请确保：

- 确保要添加的服务器正在运行与组中其他服务器相同的操作系统版本，并且区域设置也相同。不支持包含多种操作系统版本和区域设置的 StoreFront 服务器组。
- 确保 StoreFront 在所添加服务器上 IIS 中的相对路径也与组中的其他服务器相同。

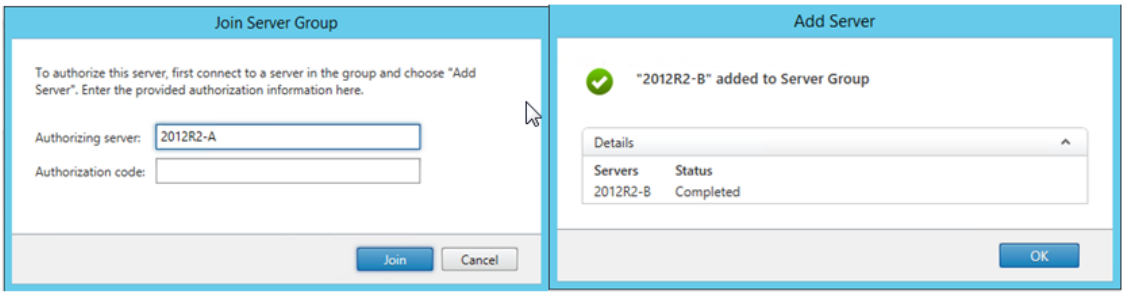
> 注意：
>
> 有关服务器组大小的建议，请参阅 StoreFront 服务器组。

如果要添加的 StoreFront 服务器以前属于服务器组，并且已被删除，则在其能够重新添加到相同或不同的服务器组之前，必须将 StoreFront 服务器重置为出厂默认状态。请参阅将服务器重置为出厂默认设置

> 重要提示：
>
> 向服务器组中添加新服务器时，添加的 StoreFront 服务帐户将作为新服务器上本地管理员组的成员。这些服务需要本地管理员权限才能加入服务器组并与其同步。如果您使用组策略防止向本地管理员组添加新成员，或者如果您限制了服务器上本地管理员组的权限，StoreFront 将无法加入服务器组。

1. 如果 Citrix StoreFront 管理控制台在安装 StoreFront 后未打开，请在 Windows“开始”屏幕或“应用程序”屏幕中，找到并单击 Citrix StoreFront 磁贴。
2. 在 Citrix StoreFront 管理控制台的结果窗格中，单击加入现有服务器组。
3. 登录到 StoreFront 部署中您要加入的服务器，然后打开 Citrix StoreFront 管理控制台。在控制台的左侧窗格中选择“服务器组”节点，然后在“操作”窗格中单击添加服务器。记下显示的授权代码。
4. 返回到新服务器，然后在加入服务器组对话框的授权服务器框中指定现有服务器的名称。输入从该服务器获取的授权代码，然后单击加入。

   加入组之后，新服务器的配置将相应更新以与现有服务器的配置匹配。新服务器的详细信息将更新到服务器组内的所有其他服务器中。



要管理多服务器部署，请一次仅使用一台服务器以更改服务器组的配置。确保 Citrix StoreFront 管理控制台未在部署中的任何其他服务器上运行。必须将对配置所做的任何更改传播到组中的其他服务器，以确保整个部署内的配置保持一致。

升级 StoreFront

February 22, 2024

升级将保留您的 StoreFront 配置，并且保持用户的收藏夹完好无损。相比之下，卸载 StoreFront 会删除 StoreFront 和关联的服务、站点、收藏夹（在独立服务器上）以及关联的配置。

支持升级路径

您可以从以下位置升级到 StoreFront 2203 最新版 CU：

- StoreFront 2203 LTSR（初始版本或任何 CU）
- StoreFront 1912 LTSR（任何 CU）
- StoreFront 3.12 LTSR CU9

要从 3.12 CU9 之前的版本进行升级，必须先升级到 StoreFront 3.12 CU9。

> 警告：
>
> 从 1912 之前的版本升级时，部署中的所有桌面设备站点都会自动删除。作为替代方案，Citrix 建议对所有未加入域的用例使用 Citrix Workspace 应用程序 Desktop Lock。

须知

- StoreFront 不支持包含不同产品版本的多服务器部署，因此，授予对部署的访问权限之前，必须将服务器组中的所有服务器升级到相同的版本。
- StoreFront 不支持包含不同服务器操作系统的多服务器部署，因此，某个服务器组中的所有服务器都必须位于相同的 Windows 服务器操作系统中。
- 多服务器部署不支持同时升级，必须按顺序升级服务器。
- 在 StoreFront 升级运行之前，它会执行一些升级前检查。如果任何升级前检查失败，升级将不启动，并且会通知您失败。您的 StoreFront 安装保持不变。修复故障原因后，重新运行升级。
- 如果 StoreFront 升级本身失败，则现有 StoreFront 安装可能会丢失其初始配置。将 StoreFront 安装还原到功能状态，然后重新运行升级。要将 StoreFront 还原到功能状态，请考虑以下方法：
  - 还原升级前创建的 VM 快照，
  - 导入升级前导出的 StoreFront 配置（请参阅导出和导入 StoreFront 配置，
  - 执行对 StoreFront 升级问题进行故障排除中的故障排除建议。
- 在 Citrix Virtual Apps and Desktops metainstaller 中发生的任何 StoreFront 升级失败都将在对话框中报告，其中包含指向相关故障日志的链接。

准备好升级

在开始升级之前，我们建议您执行以下步骤，以防止升级失败：

- 升级前规划备份策略。
- 确认您未尝试从生命周期已结束的 StoreFront 版本进行升级。有关详细信息，请参阅 CTX200356。
- 验证您仅从受支持的 StoreFront 版本升级到当前版本。
- 从 Citrix Web 站点下载 StoreFront 安装程序。

升级单台 **StoreFront** 服务器

1. 通过创建 VM 快照备份服务器。
2. 导出现有 StoreFront 配置。如果一个服务器组中有多台服务器，则只能从一台服务器中导出服务器组配置。如果已在它们之间传播所有更改，服务器组中的所有服务器将保持相同的配置副本。使用此备份，您可以轻松构建新服务器组。这样在出现问题时就可以轻松还原配置。请注意，您只能将此备份还原到运行与从中导出的版本相同的服务器上。
3. 如果您对 `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data` 中的文件（例如，default.ica 和 usernamepassword.tfrm）进行了修改，请为每个应用商店备份这些文件。升级后，您可以还原它们以恢复进行的修改。
4. 请通过从任何负载平衡器中删除服务器或者以其他方式阻止连接来阻止用户建立连接。
5. 重新启动服务器。
6. 确保没有正在运行的应用程序，包括 StoreFront 管理控制台、命令行和 PowerShell Windows 或者任何其他可能锁定 StoreFront 文件的应用程序。这样才能确保在升级期间，安装程序可以访问所有 StoreFront 文件。如果安装程序无法访问任何文件，则将无法替换这些文件，并且升级会失败，从而导致删除现有 StoreFront 配置。
7. 确保在包含 StoreFront 文件的目录中没有打开任何 Windows 资源管理器或命令提示符。
8. 禁用所有防病毒应用程序。
9. 运行所需版本的 StoreFront 的安装文件。

升级 **StoreFront** 服务器组

升级 StoreFront 服务器组涉及使用其中一个服务器从组中删除其他服务器。删除的服务器会保留与该组相关的配置，从而防止其加入到新的服务器组。必须先将其重置为出厂默认状态，或者在其上重新安装 StoreFront，才能将其重新用于构建新服务器组，或者将其用作独立的 StoreFront 服务器。不支持同步升级 StoreFront 服务器组中的服务器。

示例 **1**：在计划维护停机期间升级三节点 **StoreFront** 服务器组

这描述了在计划停机期间升级由三台服务器 A、B 和 C 组成的 StoreFront 服务器组。

1. 通过禁用负载平衡 URL 来禁用用户对服务器组的访问。这将阻止用户在升级过程中连接到部署。

2. 使用服务器 A 从组中删除服务器 B 和 C。

   服务器 B 和 C 现在从服务器组“孤立”。

3. 请按照升级单台 StoreFront 服务器中的说明升级服务器 A。
4. 确保服务器 A 已成功升级。
5. 在服务器 B 和 C 上，卸载当前安装的 StoreFront 版本并安装新版本的 StoreFront。
6. 将服务器 B 和 C 加入升级后的服务器 A，以创建升级后的服务器组。此服务器组由一个升级后的服务器 (A) 和两个新安装的服务器（B 和 C）组成。

   加入现有服务器组过程会自动将所有配置数据和订阅数据传播到新的服务器 B 和 C 中。

7. 检查所有服务器是否正常运行。
8. 通过启用负载平衡 URL 来启用用户对升级后的服务器组的访问。

示例 **2**：在非计划维护停机期间升级三节点 **StoreFront** 服务器组

这描述了在非计划停机期间升级由三台服务器 A、B 和 C 组成的 StoreFront 服务器组。

升级服务器组之前：

1. 使用 **Export-STFConfiguration**导出 StoreFront 配置。此备份是必需的，因为服务器在该过程的稍后阶段将进行出厂重置，这会删除配置数据。
2. 使用 **Export-STFStoreSubscriptions** 从服务器 A 中导出订阅数据。此备份是必需的，因为服务器在该过程的稍后阶段将进行出厂重置，这会删除订阅数据。请参阅管理应用商店的订阅数据。
3. 请通过将服务器 C 从负载平衡器中删除来禁用用户对该服务器的访问权限。这可以防止用户在升级过程中连接到服务器 C。负载平衡器继续向服务器 A 和 B 发送请求。
4. 使用服务器 A 从组中删除服务器 C。
   服务器 A 和 B 继续提供对用户资源的访问权限。服务器 C 现在是从服务器组中孤立的，并且正在重置为出厂状态。
5. 使用 **Clear-STFDeployment** 将孤立服务器 C 重置为出厂默认状态。
6. 使用 **Import-STFConfiguration** 导入 StoreFront 配置（以前导出的）到服务器 C 中。服务器 C 现在具有与旧服务器组相同的配置。以后没有必要重复此步骤。只有一台服务器需要配置数据的副本才能将其传播到加入该组的任何其他服务器。
7. 请按照升级单台 StoreFront 服务器中的说明升级服务器 C。服务器 C 现在具有与旧服务器组相同的配置，并升级到新版本的 StoreFront。
8. 导入订阅数据（以前导出的）到服务器 C 中。无需稍后再次重复此步骤。只有一台服务器需要订阅数据的副本才能将其传播到加入该组的任何其他服务器。
9. 使用服务器 B 重复执行步骤 3、4、5 和 7（请勿重复执行步骤 6）。在此期间，只有服务器 A 为用户提供对资源的访问权限。因此，建议在安静的工作期间执行此步骤，此时 StoreFront 服务器组上的负载应该是最低的。
10. 使用加入现有服务器组流程将服务器 B 加入到服务器 C 中。这将为当前版本的 StoreFront（服务器 A）提供单个服务器部署，并在新 StoreFront 版本（服务器 B 和 C）上提供新的双节点服务器组。

11. 将服务器 B 和 C 添加到负载平衡服务中，以便其能够从服务器 A 接管。
12. 将服务器 A 从负载平衡器中删除，以便将用户定向到新升级的服务器 B 和 C。
13. 使用服务器 A 重复执行步骤 3、4、5 和 7（请勿重复执行步骤 6）。服务器组升级过程现已完成。服务器 A、B 和 C 具有来自原始组的相同配置和订阅数据。

> 注意：
>
> 在服务器 A 是唯一可访问的服务器时的短暂过程中，订阅可能会丢失（步骤 9）。这可能会导致新服务器组在升级后具有略微过时的订阅数据库副本，并且任何新的订阅记录都将丢失。
>
> 这不会对功能产生影响，因为订阅数据对于用户登录和启动资源来说不是必不可少的。但是，在服务器 A 恢复出厂状态并加入新升级的组后，用户需要再次订阅资源。虽然不大可能丢失超过几条订阅记录，但这可能是升级实时 StoreFront 生产环境而不会停机造成的后果。

如果升级失败

1. 在 *C:\Windows\Temp\StoreFront* 中，打开最新的 *CitrixMsi*.log*，并搜索任何异常错误。

   Thumbs.db 访问异常：由 *C:\inetpub\wwwroot\citrix* 或其子目录中的 *thumbs.db* 文件导致的。删除找到的任何 *thumbs.db* 文件。

   使用过程中无法获取独占文件访问权限异常：还原快照/备份（如果可用），或者重新启动服务器，并手动停止任何 StoreFront 服务。

   无法启动服务异常：还原快照/备份（如果可用），或者安装.NET Framework 4.5 的完整版本（而非客户端配置文件）。

2. 如果 *CitrixMsi*.log* 中没有异常错误，请检查服务器的事件查看器 **>** 交付服务是否存在包含上述异常错误消息的任何错误。按照相应的建议进行操作。
3. 如果事件查看器中没有异常错误，请检查 *C:\Program Files\Citrix\Receiver StoreFront\logs* 中是否存在包含上述异常错误消息的任何错误。按照相应的建议进行操作。

有关日志文件的更多详细信息，请参阅安装日志。

将服务器重置为出厂默认设置

April 17, 2024

在某些情况下，需要将 StoreFront 安装重置为其初始安装状态。例如，在将 StoreFront 服务器重新添加到服务器组之前，这是必需的。

可以执行手动卸载和重新安装操作，但这更耗时，并且可能会导致其他不可预见的问题。相反，您可以运行 **Clear-STFDeployment** PowerShell cmdlet，以将 StoreFront 服务器重置为出厂默认状态。

1. 确保 StoreFront 管理控制台已关闭。
2. 打开 PowerShell ISE 并选择以管理员身份运行。
3. 设置 PowerShell 路径：

```
$env:PSModulePath = [Environment]::GetEnvironmentVariable('
    PSModulePath','Machine')
<!--NeedCopy-->
```

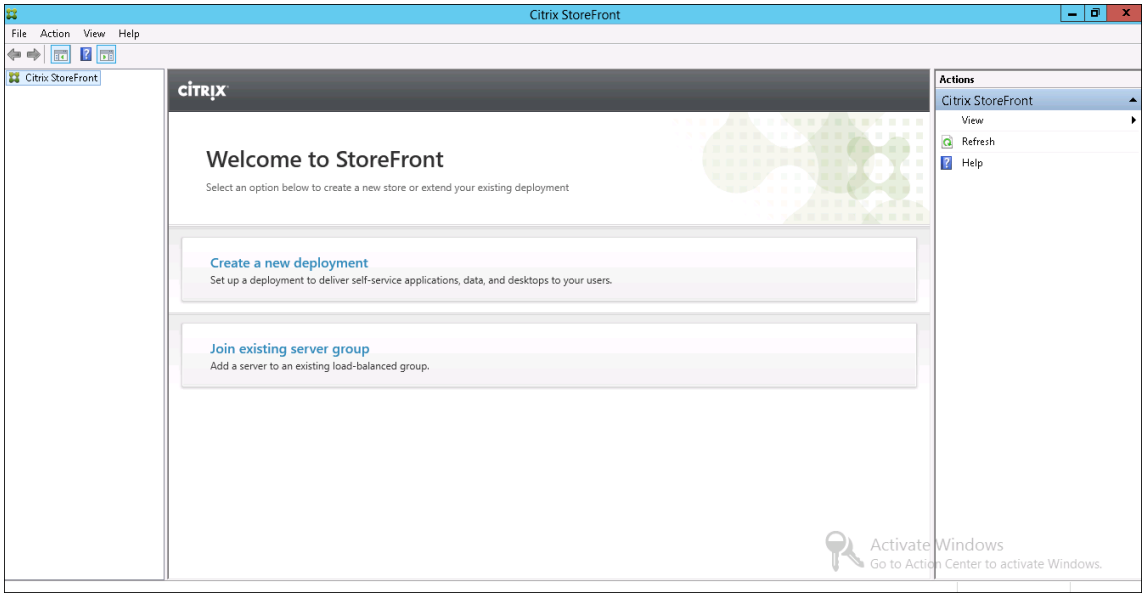
4. 导入 Citrix StoreFront 模块。

```
Import-Module citrix.storefront -verbose
<!--NeedCopy-->
```

5. 导入模块后，运行 **Clear-STFDeployment** 命令以将 StoreFront 服务器重置为默认设置：

```
Clear-STFDeployment -Confirm $False
<!--NeedCopy-->
```

6. 命令成功完成后，打开 StoreFront 管理控制台并确认所有设置都已重置。创建新部署或加入现有服务器组选项可用。



卸载 **StoreFront**

February 22, 2024

除产品本身外，卸载 StoreFront 将删除身份验证服务、应用商店、Citrix Receiver for Web 站点、XenApp Services URL 以及关联的配置。此外，还将删除包含用户的应用程序订阅数据的订阅应用商店服务。在单服务器部署中，用

户应用程序订阅的详细信息因此将丢失。但是，在多服务器部署中，这些数据将保留在组中的其他服务器上。卸载 StoreFront 时，不会从服务器中删除 StoreFront 安装程序要求的必备项，例如，.NET Framework 功能和 Web 服务器 (IIS) 角色服务。

1. 使用具有本地管理员权限的帐户登录 StoreFront 服务器。
2. 如果 StoreFront 管理控制台处于打开状态，请将其关闭。
3. 关闭任何可能已通过其 PowerShell SDK 管理 StoreFront 的 PowerShell 会话。
4. 打开开始菜单，按设置（齿轮图标），然后转到应用程序。
5. 在程序和功能窗口中，选择 **Citrix StoreFront**，然后单击卸载，以删除服务器中的所有 StoreFront 组件。
6. 在卸载 **Citrix StoreFront** 对话框中，单击是。卸载完成后，单击确定。

手动删除 **StoreFront**

卸载 StoreFront 后，为确保完全移除 StoreFront，请执行以下操作：

1. 删除 Web 服务器角色。
2. 删除文件夹 *C:\Program Files\Citrix\Receiver StoreFront*。
3. 删除 *C:\Program Files\Citrix\StoreFront Install* 下的所有子目录。
4. 删除文件夹 *C:\Inetpub*。

您现在可以重新安装 StoreFront。

安装日志

有关日志文件的更多详细信息，请参阅安装日志。

配置身份验证和委派

February 22, 2024

您可以使用多种身份验证和委派方法，具体取决于您的需求。

Method（方法）	详细信息
配置身份验证	配置用户可以使用哪些方法通过 Citrix Workspace 应用程序登录 StoreFront。
智能卡身份验证	设置智能卡身份验证。
用户名和密码身份验证	允许用户使用其 Active Directory 用户名和密码进行身份验证，并配置用于更改密码和密码过期日期通知的选项。

Method（方法）	详细信息
域直通身份验证	允许 Windows 设备使用其 Windows 凭据进行单点登录。
SAML 身份验证	使用 SAML 将身份验证委托给第三方身份提供程序。
联合身份验证服务配置	将 StoreFront 配置为与联合身份验证服务集成以便单点登录 VDA

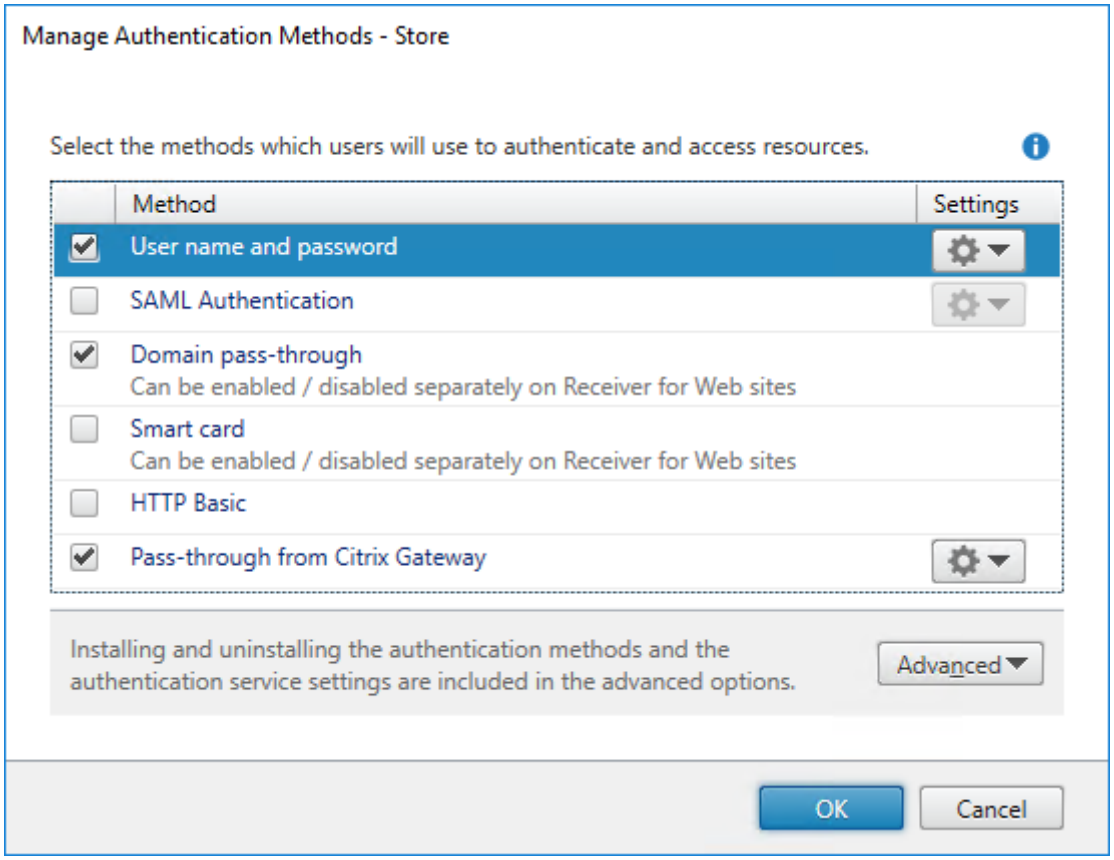
配置身份验证

April 17, 2024

管理身份验证方法

对于每个应用商店，您可以选择一种或多种身份验证方法，这些方法可以在通过 Citrix Workspace 应用程序登录应用商店时使用。

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点，然后在操作窗格中单击管理身份验证方法。
2. 指定要为用户启用的访问方法。



- 选中用户名和密码复选框以启用显式 Active Directory 用户名和密码身份验证。有关详细信息，请参阅用户名和密码身份验证。
- 选择 **SAML** 身份验证复选框以支持与 SAML 身份提供程序的集成。有关详细信息，请参阅 SAML 身份验证。
- 选中域直通以启用从用户设备直通 Active Directory 域凭据。有关详细信息，请参阅域直通身份验证。
- 选中智能卡以启用智能卡身份验证。有关详细信息，请参阅智能卡身份验证。
- 选中 **HTTP Basic** 以启用 HTTP Basic 身份验证。用户将向 StoreFront 服务器的 IIS Web 服务器进行身份验证。
- 选择从 **Citrix Gateway** 直通以启用从 Citrix Gateway 直通身份验证。如果用户通过启用了身份验证的 Citrix Gateway 连接到 StoreFront，请启用此选项。有关详细信息，请参阅从 Citrix Gateway 直通。

修改应用商店的身份验证方法也会更新通过 Web 浏览器访问应用商店时使用的身份验证方法。要更改通过 Web 浏览器登录时使用的身份验证方法，请参阅身份验证方法。

使用 **PowerShell SDK** 管理身份验证方法

要使用 PowerShell SDK 配置身份验证，请执行以下操作：

1. 调用 Get-STFAuthenticationService 以获取应用商店或虚拟目录的身份验证服务并查看其当前配置。
2. 在身份验证服务上，启用或禁用所需的身份验证协议。要获取可用协议的列表，请运行 Get-STFAuthenticationServiceProtocol。要启用协议，请运行带要启用的协议列表的 Enable-

STFAuthenticationServiceProtocol。要启用协议，请运行带要禁用的协议列表的 Disable-STFAuthenticationServiceProtocol。

3. 配置您已启用的身份验证协议。有关详细信息，请参阅每个协议的相关文档。

共享身份验证服务设置

可以通过执行“共享身份验证服务设置”任务指定要共享身份验证服务的应用商店，从而实现在这些应用商店之间进行单点登录。

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点，然后在结果窗格中选择一个应用商店。在操作窗格中，单击管理身份验证方法。
2. 在高级下拉菜单中，选择共享身份验证服务设置。
3. 单击使用共享身份验证服务复选框，并从应用商店名称下拉菜单中选择一个应用商店。

> 注意：
>
> 共享身份验证服务与专用身份验证服务之间不存在功能差异。多个应用商店共享的身份验证服务被视为共享身份验证服务，并且任何配置更改都会影响对使用共享身份验证服务的所有应用商店的访问。

智能卡身份验证

April 17, 2024

用户在访问应用商店时其使用智能卡和 PIN 进行身份验证。安装 StoreFront 时，智能卡身份验证默认情况下处于禁用状态。可以为通过 Citrix Workspace 应用程序、Web 浏览器和 XenApp Services URL 连接到应用商店的用户启用智能卡身份验证。

使用智能卡身份验证可简化用户的登录过程，同时还能提高用户访问基础结构的安全性。对内部企业网络的访问受基于证书的使用公钥基础结构的双重身份验证所保护。私钥受硬件控制保护，离不开智能卡。使用智能卡和 PIN，用户可以方便地从一系列的企业设备访问其桌面和应用程序。

可以使用智能卡实现 StoreFront 对用户的身份验证，以访问 Citrix Virtual Apps and Desktops 提供的桌面和应用程序。登录 StoreFront 的智能卡用户还可以访问 Endpoint Management 提供的应用程序。但是，用户必须重新进行身份验证才能访问使用客户端证书身份验证的 Endpoint Management Web 应用程序。

要启用智能卡身份验证，必须在包含 StoreFront 服务器的 Microsoft Active Directory 域或与 StoreFront 服务器域具有直接双向信任关系的域中配置用户的帐户。支持涉及双向信任的多林部署。

对 StoreFront 使用智能卡身份验证的配置取决于用户设备、安装的客户端以及设备是否已加入域。在本上下文中，已加入域表示设备已加入包含 StoreFront 服务器的 Active Directory 林中的一个域。

为 Citrix 环境配置智能卡文档介绍了如何为 Citrix 部署配置使用特定智能卡类型的智能卡。类似的步骤适用于其他供应商提供的智能卡。

必备条件

- 确保在计划部署 StoreFront 服务器的 Microsoft Active Directory 域或者与 StoreFront 服务器域具有直接双向信任关系的域内配置所有用户的帐户。
- 如果您计划启用智能卡直通身份验证，请确保您的智能卡读卡器类型、中间件类型和配置以及中间件 PIN 缓存策略允许这种验证方式。
- 在提供用户桌面和应用程序并运行 Virtual Delivery Agent 的虚拟机或物理机上安装供应商的智能卡中间件。有关将智能卡与 Citrix Virtual Desktops 结合使用的详细信息，请参阅智能卡。
- 请确保正确配置了您的公钥基础结构。确认针对 Active Directory 环境正确配置了帐户映射的证书并且可以成功执行用户证书验证。

配置 **StoreFront**

- 必须将 HTTPS 用于 StoreFront 和用户设备之间的通信，以启用智能卡身份验证。请参阅使用 HTTPS 保护 StoreFront 的安全。
- 要在通过 Citrix Workspace 应用程序连接到应用商店时启用智能卡身份验证，请在身份验证方法中勾选或取消勾选智能卡。
- 默认情况下，为应用商店启用智能卡身份验证也会为该应用商店的所有 Web 站点启用智能卡身份验证。您可以在 Manage Receiver for Web Sites Authentication methods（管理 Receiver for Web 站点身份验证方法）选项卡上为特定 Web 站点单独启用或禁用智能卡身份验证。
- 如果您同时配置了智能卡以及用户名和密码身份验证，系统最初会提示用户使用智能卡和 PIN 码进行登录，但在智能卡出现任何问题时可以选择使用显式身份验证。

将 **Delivery Controller** 配置为信任 **StoreFront**

使用智能卡身份验证时，StoreFront 无权访问用户的凭据，因此无法向 Citrix Virtual Apps and Desktops 进行身份验证。因此，您必须将 Delivery Controller 配置为信任来自 StoreFront 的请求，请参阅 Citrix Virtual Apps and Desktops 安全注意事项和最佳做法。

通过 **Citrix Gateway** 进行远程访问

对于远程访问，您可以在 Citrix Gateway 上启用智能卡，然后使用委派身份验证启用对 StoreFront 的直通身份验证。有关更多详细信息，请参阅网关直通。

为确保用户在建立与其资源的连接时不会在虚拟服务器上收到额外的凭据提示，请创建第二个网关并在安全套接字层 (SSL) 参数中禁用客户端身份验证。有关详细信息，请参阅配置智能卡身份验证。通过使用智能卡身份验证的 Citrix Gateway 访问 StoreFront 时。通过此虚拟服务器配置最佳网关路由，以便连接到为应用商店提供桌面和应用程序的部署。有关详细信息，请参阅为应用商店配置最佳 HDX 路由。

单点登录到 **VDA**

您可以通过直接传递用户的智能卡凭据来启用到 VDA 的单点登录。可以通过 Web 浏览器或适用于 Windows 的 Citrix Workspace 应用程序访问应用商店，但资源必须在适用于 Windows 的 Citrix Workspace 应用程序中打开。在其他操作系统上或者通过浏览器访问资源时，用户在连接到 VDA 时必须重新输入其凭据。

1. 请在安装适用于 Windows 的 Citrix Workspace 时包括单点登录组件并将其配置为执行单点登录。请参阅配置域直通身份验证。
2. 使用文本编辑器打开应用商店的 default.ica 文件。请参阅默认 ica
3. 要为不通过 Citrix Gateway 访问应用商店的用户启用智能卡凭据直通功能，请在 [Application] 部分中添加以下设置。

   ```
   DisableCtrlAltDel=Off
   ```

   此设置适用于此应用商店的所有用户。要对桌面和应用程序同时启用域直通和使用智能卡进行直通身份验证，则必须为每种身份验证方法创建单独的应用商店。然后，将用户定向到与其身份验证方法所对应的应用商店。
4. 要为通过 Citrix Gateway 访问应用商店的用户启用智能卡凭据直通功能，请在 [Application] 部分中添加以下设置。

   ```
   UseLocalUserAndPassword=On
   ```

   此设置适用于此应用商店的所有用户。要为部分用户启用直通身份验证，而要求其他用户登录才可访问其桌面和应用程序，必须为每组用户创建单独的应用商店。然后，将用户定向到与其身份验证方法所对应的应用商店。

使用 **FAS** 单点登录到 **VDA**

或者，在使用本地安装的 Citrix Workspace 应用程序但不使用适用于 HTML5 的 Citrix Workspace 应用程序时，您可以将联合身份验证服务配置为单点登录到 VDA。

重要注意事项

使用智能卡进行用户身份验证以访问 StoreFront 时需满足和遵循以下要求和限制。

- 要使用虚拟专用网络 (VPN) 通道进行智能卡身份验证，用户必须安装 Citrix Gateway 插件或通过 Web 页面进行登录，并在执行每个步骤时都使用智能卡和 PIN 进行身份验证。使用 Citrix Gateway 插件通过直通身份验证访问 StoreFront 不适用于智能卡用户。
- 可以在同一用户设备上使用多个智能卡和多个读卡器，但是，如果启用了通过智能卡直通身份验证，则用户必须确保在访问桌面或应用程序时只插入一个智能卡。
- 在应用程序中使用智能卡时（例如，进行数字签名或加密时），用户可能会看到额外的要求插入智能卡或输入 PIN 的提示。同时插入多个智能卡时可能会发生这种情况。配置设置（例如，通常使用组策略配置的 PIN 缓存等中间件设置）也会导致出现这种情况。当智能卡已插入读卡器中，但仍提示插入智能卡时，用户必须单击“取消”。如果提示用户输入 PIN，则必须再次输入 PIN。

- 如果为使用加入了域的设备但不通过 Citrix Gateway 访问应用商店的适用于 Windows 的 Citrix Workspace 应用程序用户启用了对 Citrix Virtual Apps and Desktops 使用智能卡进行直通身份验证，此设置将应用到应用商店的所有用户。要对桌面和应用程序同时启用域直通和使用智能卡进行直通身份验证，则必须为每种身份验证方法创建单独的应用商店。然后，用户必须连接到与其身份验证方法所对应的应用商店。
- 如果为使用加入了域的设备并通过 Citrix Gateway 访问应用商店的适用于 Windows 的 Citrix Workspace 应用程序用户启用了对 Citrix Virtual Apps and Desktops 使用智能卡进行直通身份验证，此设置将应用到应用商店的所有用户。要为某些用户启用直通身份验证，但要求其他用户登录到桌面和应用程序，必须为每组用户创建单独的应用商店。然后，将用户定向到与其身份验证方法所对应的应用商店。
- 只能为每个 XenApp Services URL 配置一种身份验证方法，而且每个应用商店只能使用一个 URL。如果除了智能卡身份验证以外，您还需要启用其他类型的身份验证，则必须为每种身份验证方法创建单独的应用商店，每个应用商店都具有一个 XenApp Services URL。然后，将用户定向到与其身份验证方法所对应的应用商店。
- 安装 StoreFront 时，Microsoft Internet Information Services (IIS) 中的默认配置仅要求 StoreFront 身份验证服务的证书身份验证 URL 的 HTTPS 连接提供客户端证书。对于任何其他 StoreFront URL，IIS 不要求提供客户端证书。此配置能够让智能卡用户在智能卡出现问题时，可以选择回退至显式身份验证。根据相应的 Windows 策略设置而定，用户也可以移除智能卡，而不需要重新进行身份验证。

  如果您决定将 IIS 配置为要求所有 StoreFront URL 的 HTTPS 连接提供客户端证书，则必须将身份验证服务和应用商店放置在同一服务器上。必须使用对所有应用商店都有效的客户端证书。使用此 IIS 站点配置时，智能卡用户无法通过 Citrix Gateway 进行连接，也无法回退至显式身份验证。如果从设备上移除了智能卡，用户必须重新登录。

域直通身份验证

April 17, 2024

用户向其加入了域的 Windows 计算机进行身份验证，这些用户的凭据会用于自动将其登录到 Citrix Workspace 应用程序中。适用于 Windows 的 Citrix Workspace 应用程序以及 Windows 上的以下 Web 浏览器都支持此功能：

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

StoreFront 配置

要为适用于 Windows 的 Citrix Workspace 应用程序启用域直通，请在身份验证方法中选择域直通。

默认情况下，为应用商店启用域直通身份验证也会针对该应用商店的所有 Web 站点为适用于 HTML5 的 Citrix Workspace 应用程序启用域直通身份验证。您可以在 Manage Receiver for Web Sites Authentication methods（管理 Receiver for Web 站点身份验证方法）选项卡上为特定 Web 站点禁用域直通身份验证。

将 **Delivery Controller** 配置为信任 **StoreFront**

使用域直通身份验证时，StoreFront 无权访问用户的凭据，因此无法向 Citrix Virtual Apps and Desktops 进行身份验证。因此，您必须将 Delivery Controller 配置为信任来自 StoreFront 的请求，请参阅 Citrix Virtual Apps and Desktops 安全注意事项和最佳做法。

单点登录到 **VDA**

必须使用带有启用单点登录组件的适用于 Windows 的 Citrix Workspace 应用程序才能单点登录到 VDA，请参阅配置域直通身份验证。如果使用适用于 HTML5 的 Citrix Workspace 应用程序，则必须将其配置为连接到适用于 Windows 的 Citrix Workspace 应用程序中的资源，而非连接到浏览器。

适用于 **Windows** 的 **Citrix Workspace** 应用程序配置

要使用适用于 Windows 的 Citrix Workspace 应用程序启用域直通以单点登录到应用商店和 VDA，请参阅适用于 Windows 的 Citrix Workspace 应用程序文档。

适用于 **HTML5** 的 **Citrix Workspace** 应用程序配置

您可能需要更新用户的 Web 浏览器配置以允许进行域直通身份验证。可以使用域直通通过 Web 浏览器登录到应用商店。要单点登录到 VDA，用户必须在适用于 Windows 的 Citrix Workspace 应用程序中打开资源，而非在 Web 浏览器中打开资源。

Internet Explorer、**Edge** 和 **Chrome**　大多数 Web 浏览器使用 Windows Internet Explorer 区域配置来决定是否启用单点登录。默认情况下，它仅对本地 Intranet 区域中的站点启用。要将您的站点添加到 Intranet 区域，请执行以下操作：

1. 打开“控制面板”
2. 打开“Internet 选项”
3. 转到安全选项卡。
4. 选择本地 **Intranet**
5. 单击站点。
6. 单击高级。
7. 添加您的 StoreFront Web 站点。

可以使用组策略部署这些设置。

FireFox 修改浏览器的高级设置以信任 StoreFront Web 站点 URI 进行单点登录。

> 警告：
>
> 错误地编辑高级设置可能会导致严重问题。自行承担编辑风险。

1. 在要使用域直通进行身份验证的计算机上打开 Firefox。
2. 在地址栏中，键入 about:config。
3. 单击“I accept the risk!”（我接受风险!）。
4. 在搜索栏中，键入 negotiate。
5. 双击 network.negotiate-auth.delegation-uris。
6. 输入您的企业 Windows 域（例如 mydomain.com）的名称。
7. 单击“确定”。
8. 双击 network.negotiate-auth.trusted-uris。
9. 输入您的企业 Windows 域（例如 mydomain.com）的名称。
10. 单击“确定”。
11. 关闭并重新启动 Firefox。

使用 **FAS** 单点登录到 **VDA**

或者，在使用本地安装的 Citrix Workspace 应用程序但不使用适用于 HTML5 的 Citrix Workspace 应用程序时，您可以将联合身份验证服务配置为单点登录到 VDA。

从 **Citrix Gateway** 直通

April 17, 2024

用户向 Citrix Gateway 验证身份后，即可在访问自己的应用商店时自动登录。在首次配置对应用商店的远程访问时，Citrix Gateway 直通身份验证方法默认情况下处于启用状态。用户可以使用 Citrix Workspace 应用程序或 Web 浏览器通过 Citrix Gateway 连接到应用商店。有关针对 Citrix Gateway 配置 StoreFront 的详细信息，请参阅配置 Citrix Gateway。

StoreFront 支持使用针对以下 Citrix Gateway 身份验证方法进行直通。

- 域 用户使用其 Active Directory 用户名和密码登录。
- **RSA** 用户使用派生自令牌代码（由安全令牌生成）的通行码登录 Citrix Gateway，有时还会结合使用 PIN 码。如果您启用了仅通过安全令牌进行直通身份验证，请确保您设置为可用的资源不需要额外或附加形式的身份验证，例如用户的 Microsoft Active Directory 域凭据。
- 智能卡 用户使用智能卡登录
- **RSA +** 域 登录到 Citrix Gateway 的用户需要输入域凭据和安全令牌通行码。

如果您在 Citrix Gateway 上禁用了身份验证或者禁用了单点登录，则不使用直通，并且您必须配置其他身份验证方法之一。

如果您为从 Citrix Workspace 应用程序访问应用商店的远程用户配置了为 Citrix Gateway 执行双来源身份验证，则必须在 Citrix Gateway 上创建两个身份验证策略。将 RADIUS（远程身份验证拨入用户服务）配置为主要身份验证方法，将 LDAP（轻型目录访问协议）配置为辅助方法。将凭据索引修改为在会话配置文件中使用辅助身份验证方法，以便将 LDAP 凭据传递到 StoreFront。将 Citrix Gateway 设备添加到 StoreFront 配置时，请将“登录类型”设置为“域和安全令牌”。有关详细信息，请参阅http://support.citrix.com/article/CTX125364

要启用通过 Citrix Gateway 对 StoreFront 进行的多域身份验证，请在每个域的 Citrix Gateway LDAP 身份验证策略中将“SSO Name Attribute”（SSO 名称属性）设置为 userPrincipalName。可以要求用户在 Citrix Gateway 登录页面中指定一个域，以便确定要使用的相应 LDAP 策略。在为指向 StoreFront 的连接配置 Citrix Gateway 会话配置文件时，不要指定单点登录域。您必须在各个域之间配置信任关系。确保不要将用户限制为只能访问显式可信域，以便他们可以从任何域登录到 StoreFront。

在 Citrix Gateway 部署支持的情况下，您可以使用 SmartAccess 并根据 Citrix Gateway 会话策略来控制用户对 Citrix Virtual Apps and Desktops 资源的访问。

启用网关直通

要在通过 Workspace 应用程序连接时为应用商店启用或禁用网关直通身份验证，请在身份验证方法窗口中勾选或取消勾选从 **Citrix Gateway** 直通。

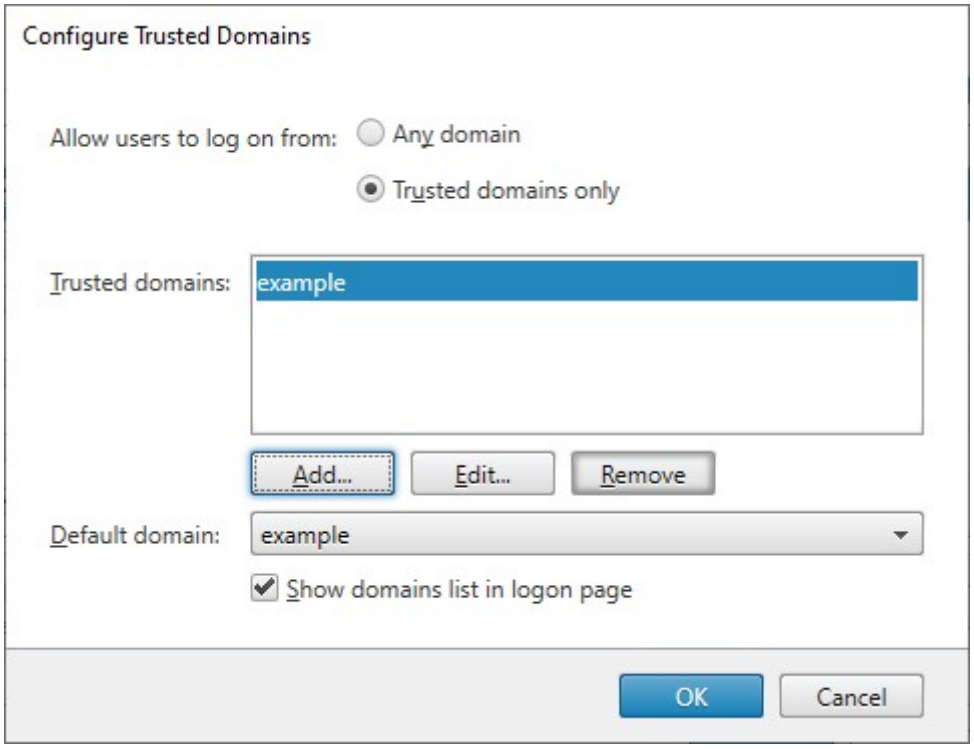
默认情况下，为应用商店启用 Citrix Gateway 直通身份验证也会为该应用商店的所有 Web 站点启用 Citrix Gateway 直通身份验证。您可以在身份验证方法选项卡上为特定 Web 站点禁用用户名和密码身份验证。

配置可信用户域

如果您的 Citrix Gateway 配置为使用 LDAP 身份验证，则可以限制对特定域的访问。

1. 在“管理身份验证方法”窗口中，在从 **Citrix Gateway** 直通 > 设置下拉菜单中选择配置可信域。
2. 选择仅限可信域，然后单击添加输入可信域的名称。在该域中具有帐户的用户能够登录所有使用此身份验证服务的应用商店。要修改域名，请在“可信域”列表中选择相应的条目，然后单击编辑。要禁止某个域中的用户帐户访问应用商店，请在列表中选择该域并单击删除。

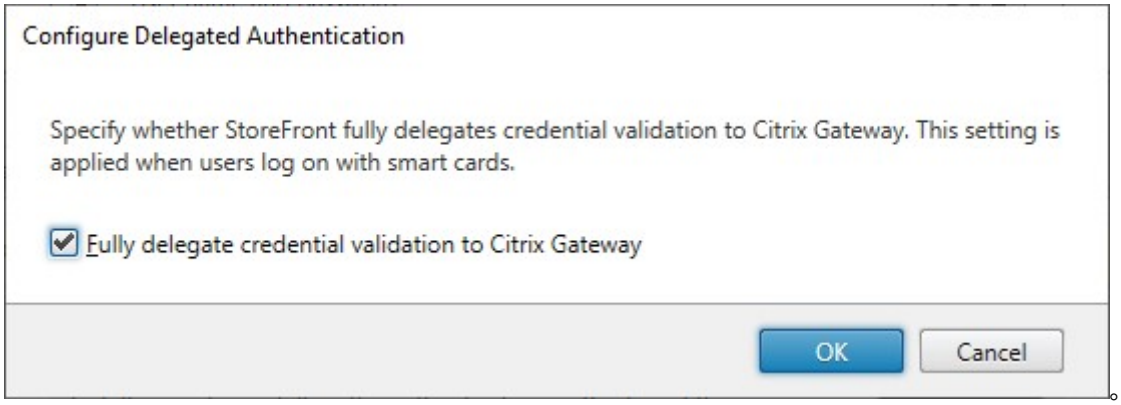
   您指定域名的方式将决定用户输入凭据时必须采用的格式。如果希望用户按照域用户名格式输入凭据，请将 NetBIOS 名称添加到列表中。如果要求用户按照用户主体名称格式输入其凭据，请将完全限定的域名添加到列表中。如果希望用户既能按照域用户名格式又能按照用户主体名称格式输入凭据，则必须同时将 NetBIOS 名称和完全限定的域名添加到列表中。
3. 如果配置多个可信域，请从默认域列表中选择用户登录时默认选择的域。
4. 如果要在登录页面上列出可信域，请选中“在登录页面中显示域列表”复选框。



将凭据验证委派给 **Citrix Gateway**

默认情况下，StoreFront 会验证从网关收到的用户名和密码。如果您的 Citrix Gateway 配置为使用智能卡等无密码身份验证方法，则必须配置 StoreFront，使其不验证凭据，因此依赖于 Gateway 的身份验证。在这种情况下，建议您在配置网关时输入回调 URL，这样 StoreFront 就可以验证来自网关的请求，请参阅管理 Citrix Gateway。

1. 在管理身份验证方法窗口中，在从 **Citrix Gateway** 直通 > 设置下拉菜单中，选择配置委派身份验证。
2. 勾选完全将凭据验证委派给 **Citrix Gateway**。



PowerShell SDK

要将应用商店配置为使用 PowerShell SDK 将身份验证委派给网关，请使用 cmdlet STFCitrixAGBasicOptions 将 `CredentialValidationMode` 设置为 `Auto`。要将 StoreFront 配置为验证凭据，请将 `CredentialValidationMode` 设置为 `Password`。

允许用户在登录时更改过期的密码

如果您的 Citrix Gateway 配置为使用 LDAP（用户名和密码）身份验证，则可以将 NetScaler 配置为允许在登录时更改过期的密码。

1. 登录 NetScaler 管理 Web 站点
2. 在侧面菜单上，转到身份验证 > 控制板。
3. 单击身份验证服务器。
4. 在其他设置下，勾选允许更改密码。

允许用户在登录后更改密码

使用从 **Citrix Gateway** 直通时，Citrix Gateway 将负责处理身份验证。您可以将 StoreFront 配置为允许用户在登录后更改密码。此功能仅在通过浏览器（而非本地安装的 Workspace 应用程序）访问 StoreFront 应用商店时可用。

默认 StoreFront 配置可防止用户更改其密码，即使密码已过期亦如此。如果决定启用此功能，请确保服务器所在域的策略允许用户更改其密码。如果用户可以访问使用此身份验证服务的任何应用商店，则允许用户更改其密码会将敏感的安全功能暴露给这些用户。如果贵组织的安全策略将用户密码更改功能保留为仅供内部使用，请确保用户无法从企业网络外部访问任何应用商店。

1. 在管理身份验证方法窗口中，在从 **Citrix Gateway** 直通 > 设置下拉菜单中，选择管理密码选项
2. 要允许用户更改密码，请选择允许用户更改密码复选框。

> 注意：
>
> 如果选中或取消选中允许用户更改密码，这也会影响用户名和密码身份验证的管理密码选项下的设置。

PowerShell SDK

要使用 PowerShell SDK 修改更改密码选项，请使用 cmdlet Set-STFExplicitCommonOptions。

将 **Delivery Controller** 配置为信任 **StoreFront**

当网关配置为进行 LDAP 身份验证时，它会将凭据传递到 StoreFront。对于其他身份验证方法，StoreFront 无法访问凭据，因此无法向 Citrix Virtual Apps and Desktops 进行身份验证。因此，您必须将 Delivery Controller 配置为信任来自 StoreFront 的请求，请参阅 Citrix Virtual Apps and Desktops 安全注意事项和最佳做法。

使用联合身份验证服务单点登录到 **VDA**

当网关配置为进行 LDAP 身份验证时，它会将凭据传递到 StoreFront，以便可以单点登录 VDA。对于其他身份验证方法，StoreFront 无权访问凭据，因此默认情况下单点登录不可用。您可以使用联合身份验证服务提供单点登录。

SAML 身份验证

April 17, 2024

SAML（安全声明标记语言）是标识和身份验证产品使用的开放标准。使用 SAML，您可以将 StoreFront 配置为将用户重定向到外部身份提供程序进行身份验证。

> 注意
>
> 将 StoreFront 配置为进行 SAML 身份验证以进行内部访问。要进行外部访问，请将 Citrix Gateway 配置为进行 SAML 身份验证，然后将 StoreFront 配置为进行网关直通身份验证。

StoreFront 需要符合 SAML 2.0 标准的身份提供程序 (IdP)，例如：

- 使用 SAML 绑定（而非 WS-Federation 绑定）的 Microsoft AD 联合身份验证服务。有关详细信息，请参阅 AD FS 部署和 AD FS 操作。
- Citrix Gateway（配置为 IdP）。
- Microsoft Entra ID。有关详细信息，请参阅 CTX237490。

SAML 断言必须包含包含用户 UPN 的 `saml:Subject` 属性。

要在通过 Workspace 应用程序连接时为应用商店启用或禁用 SAML 身份验证，请在身份验证方法窗口中选择 **SAML** 身份验证。默认情况下，为应用商店启用 SAML 身份验证也会为该应用商店的所有 Web 站点启用 SAML 身份验证。可以在身份验证方法选项卡上为特定 Web 站点独立配置 SAML。

StoreFront SAML 端点

要配置 SAML，您的身份提供程序可能需要以下端点：

- 实体 ID 的 URL。这是应用商店的身份验证服务的路径，通常为 https://[storefront host]/Citrix/[StoreName]Auth
- 声明使用者服务的 URL，通常为 https://[storefront host]/Citrix/[StoreName]Auth/SamlForms/AssertionConsume
- 元数据服务，通常为 https://[storefront host]/Citrix/[StoreName]Auth/SamlForms/ServiceProvider/Metadata

此外，还有一个测试端点，通常为 https://[storefront host]/Citrix/[StoreName]Auth/SamlTest

可以使用以下 PowerShell 脚本列出指定应用商店的端点。

```
# Change this value for your Store
$storeVirtualPath = "/Citrix/Store"

$auth = Get-STFAuthenticationService -Store (Get-STFStoreService -
    VirtualPath $storeVirtualPath)
$spId = $auth.AuthenticationSettings["samlForms"].SamlSettings.
    ServiceProvider.Uri.AbsoluteUri
$acs = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
    VirtualPath + "/SamlForms/AssertionConsumerService")
$md = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
    VirtualPath + "/SamlForms/ServiceProvider/Metadata")
$samlTest = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
    VirtualPath + "/SamlTest")
Write-Host "SAML Service Provider information:
Entity ID: $spId
Assertion Consumer Service: $acs
Metadata: $md
Test Page: $samlTest
<!--NeedCopy-->
```

输出示例：

```
SAML Service Provider information:
Entity ID: https://storefront.example.com/Citrix/StoreAuth
Assertion Consumer Service: https://storefront.example.com/Citrix/
    StoreAuth/SamlForms/AssertionConsumerService
Metadata: https://storefront.example.com/Citrix/StoreAuth/SamlForms/
    ServiceProvider/Metadata
Test Page: https://storefront.example.com/Citrix/StoreAuth/SamlTest
<!--NeedCopy-->
```


使用元数据交换进行配置

为了简化配置，您可以在身份提供程序与服务提供商（在本例中为 StoreFront）之间交换元数据（标识符、证书、端点和其他配置）。

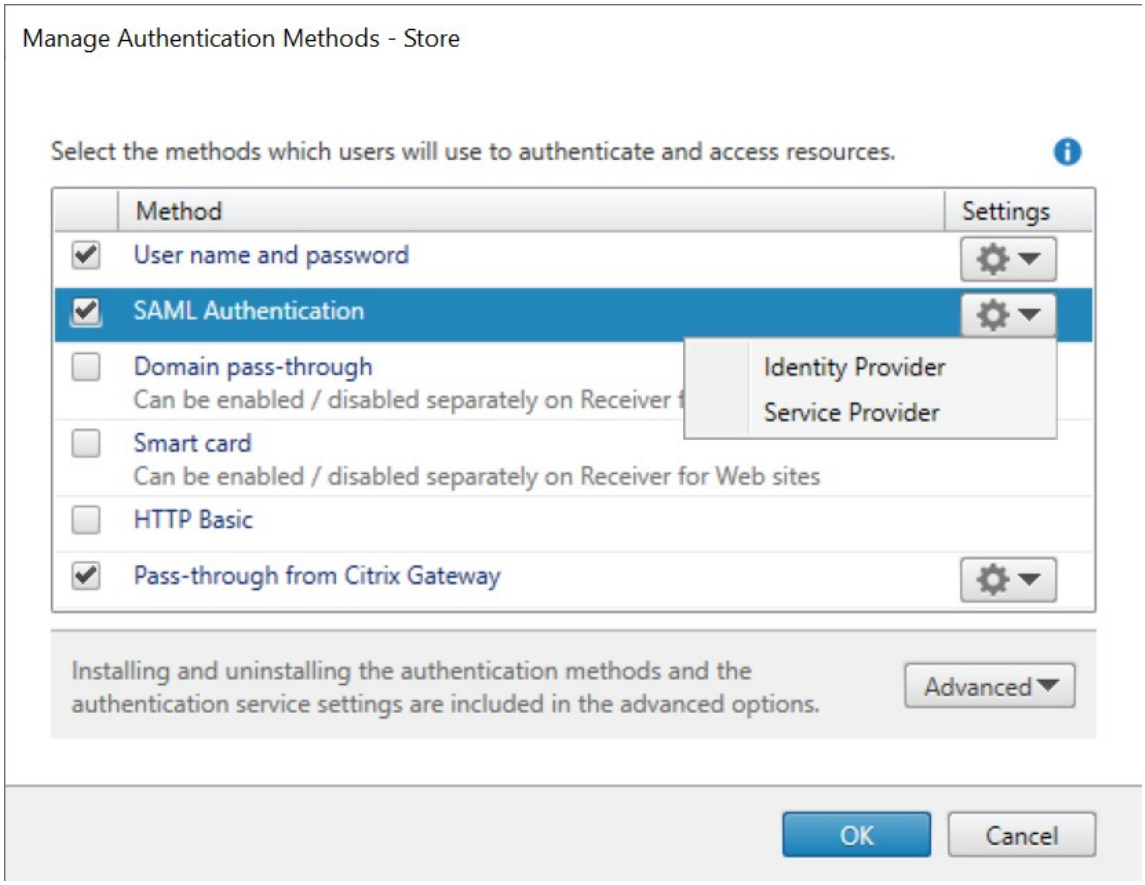
如果您的身份提供程序支持元数据导入，则可以将其指向 StoreFront 元数据端点。注意：这必须通过 HTTPS 执行。

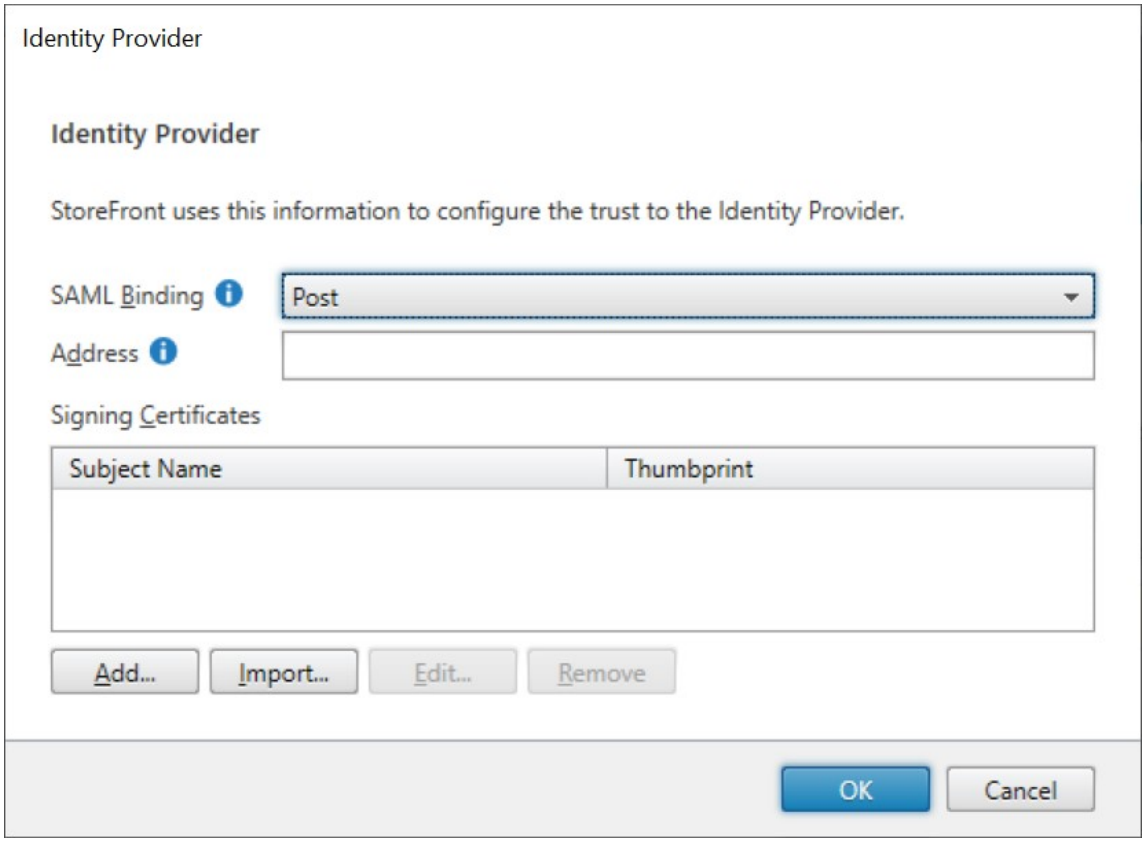
要使用来自身份提供程序的元数据配置 StoreFront，请使用 Update-STFSamlIdPFromMetadata cmdlet，例如：

```
Get-Module "Citrix.StoreFront*" -ListAvailable | Import-Module

# Remember to change this with the virtual path of your Store.
$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$auth = Get-STFAuthenticationService -StoreService $store

# To read the metadata directly from the Identity Provider, use the following:
# Note again this is only allowed for https endpoints
Update-STFSamlIdPFromMetadata -AuthenticationService $auth -Url https://example.com/FederationMetadata/2007-06/FederationMetadata.xml

# If the metadata has already been download, use the following:
# Note: Ensure that the file is encoded as UTF-8
Update-STFSamlIdPFromMetadata -AuthenticationService $auth -FilePath "C:\Users\exampleusername\Downloads\FederationMetadata.xml"
<!--NeedCopy-->
```

配置身份提供程序

1. 单击 **SAML** 身份验证行中的设置下拉列表，然后单击身份提供程序。

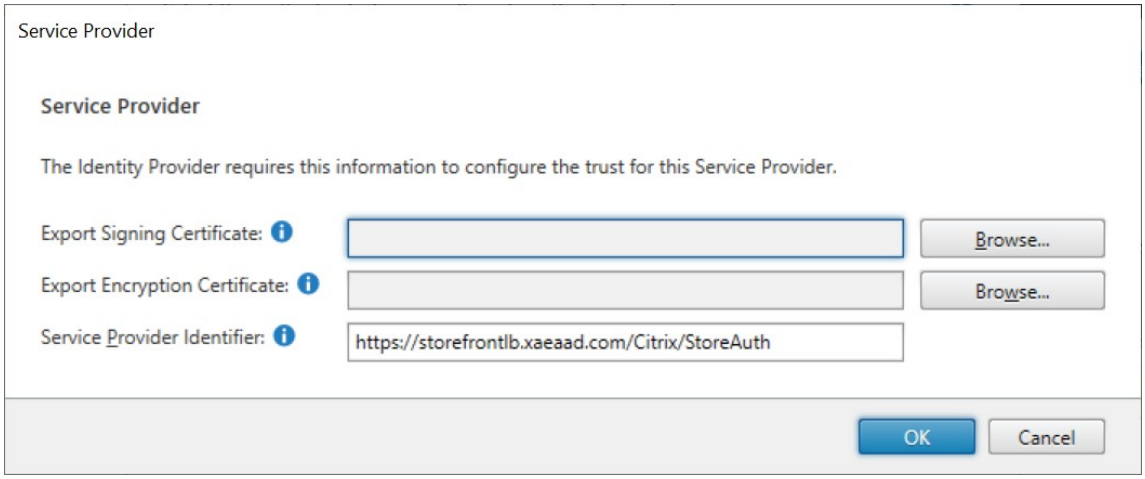




2. 选择发布或重定向的 **SAML** 绑定。
3. 输入身份提供程序的地址。
4. 导入用于对 SAML 令牌进行签名的证书。
5. 按确定保存更改。

配置服务提供商

1. 单击 **SAML** 身份验证行中的设置下拉列表，然后单击服务提供商。



2. （可选）选择用于对发送给身份提供程序的消息进行签名的导出签名证书。
3. （可选）选择用于解密收到的身份提供程序发送的消息的导出加密证书。
4. 服务提供商标识符已预先填充了应用商店的身份验证服务。
5. 按确定保存更改。

PowerShell SDK

使用 PowerShell SDK：

- 要导入签名证书，请调用 cmdlet Import-STFSamlSigningCertificate。
- 要导入加密证书，请调用 cmdlet Import-STFSamlEncryptionCertificate。

测试

要测试 SAML 集成，请执行以下操作：

1. 转至 SAML 测试页面，请参阅 StoreFront SAML 端点。
2. 这会将您重定向到身份提供程序。输入您的凭据。
3. 您将被重定向回显示身份声明和断言的测试页面。

将 Delivery Controller 配置为信任 StoreFront

使用 SAML 身份验证时，StoreFront 无权访问用户的凭据，因此无法向 Citrix Virtual Apps and Desktops 进行身份验证。因此，您必须将 Delivery Controller 配置为信任来自 StoreFront 的请求，请参阅 Citrix Virtual Apps and Desktops 安全注意事项和最佳做法。

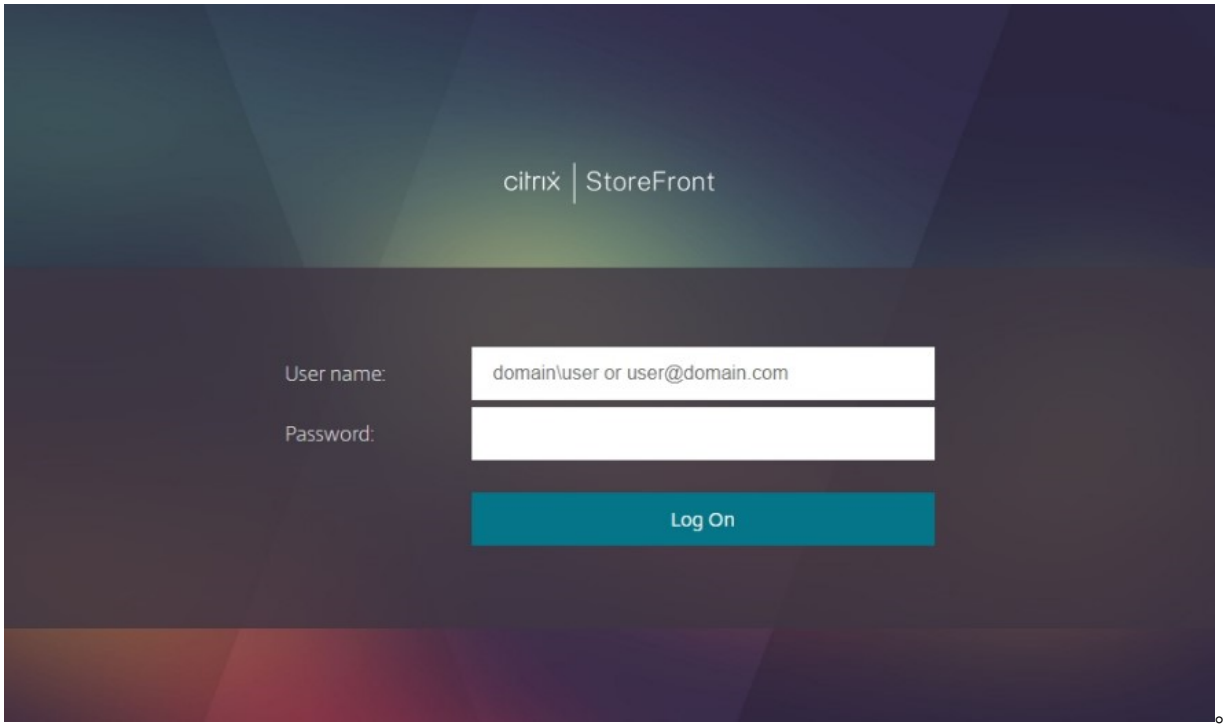
使用联合身份验证服务单点登录到 **VDA**

使用 SAML 身份验证时，StoreFront 无权访问用户的凭据，因此默认情况下单点登录到 VDA 功能不可用。您可以使用联合身份验证服务提供单点登录。

用户名和密码身份验证

April 17, 2024

通过用户名和密码身份验证，用户可以输入其 Active Directory 凭据。



要在通过 Workspace 应用程序连接时为应用商店启用或禁用用户名和密码身份验证，请在身份验证方法窗口中勾选或取消勾选用户名和密码。

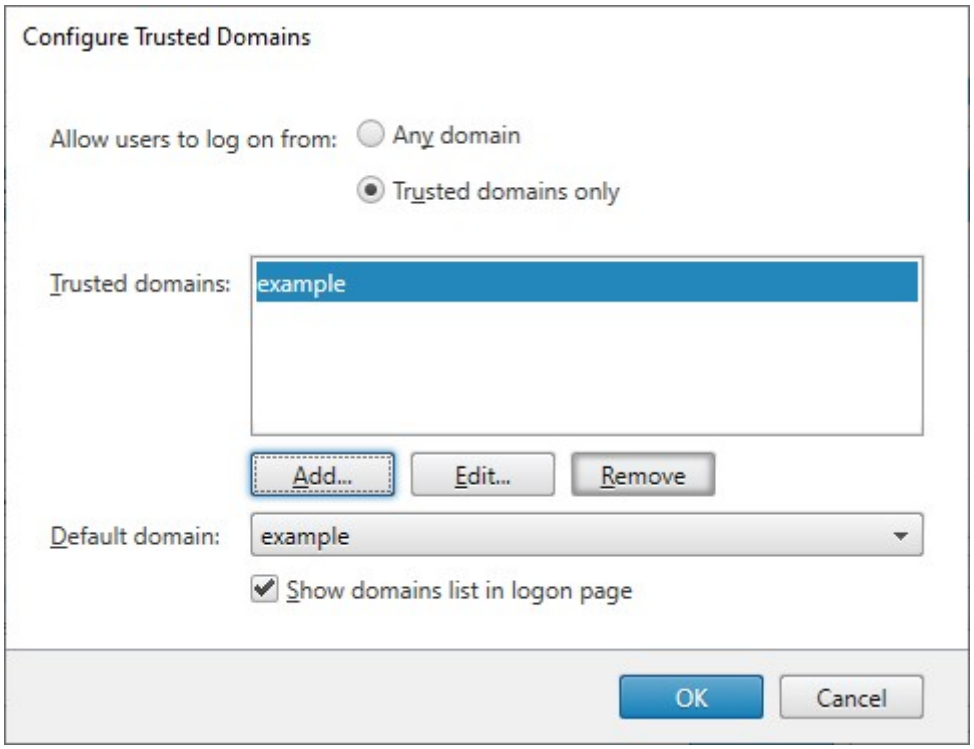
默认情况下，为应用商店启用用户名和密码身份验证也会为该应用商店的所有 Web 站点启用用户名和密码身份验证。可以在 Manage Receiver for Web Sites Authentication methods（管理 Receiver for Web 站点身份验证方法）选项卡上禁用特定 Web 站点的用户名和密码身份验证。

配置可信用户域

可以将应用商店的访问权限限制到使用来自特定可信域的凭据登录的用户。

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择“应用商店”节点，然后在结果窗格中选择适当的身份验证方法。在“操作”窗格中，单击管理身份验证方法。
2. 在用户名和密码 **>** 设置列表中，选择配置可信域。
3. 选择仅限可信域，然后单击添加输入可信域的名称。在该域中具有帐户的用户能够登录所有使用此身份验证服务的应用商店。要修改域名，请在“可信域”列表中选择相应的条目，然后单击编辑。要禁止某个域中的用户帐户访问应用商店，请在列表中选择该域并单击删除。

   您指定域名的方式将决定用户输入凭据时必须采用的格式。如果希望用户按照域用户名格式输入凭据，请将 NetBIOS 名称添加到列表中。如果要求用户按照用户主体名称格式输入其凭据，请将完全限定的域名添加到列表中。如果希望用户既能按照域用户名格式又能按照用户主体名称格式输入凭据，则必须同时将 NetBIOS 名称和完全限定的域名添加到列表中。
4. 如果配置多个可信域，请从默认域列表中选择用户登录时默认选择的域。
5. 如果要在登录页面上列出可信域，请选中“在登录页面中显示域列表”复选框。



允许用户更改密码

可以允许用户随时更改自己的密码。也可以只允许密码已过期的用户更改密码。这表示您可以确保用户绝不会因密码过期而无法访问其桌面和应用程序。

以下客户端提供更改密码功能：

Citrix Workspace 应用程序	如果在 StoreFront 上启用，用户可以更改已过期的密码	系统会通知用户密码将过期	如果在 StoreFront 上启用，用户可以在密码过期之前更改密码
Windows	是		
Mac	是		
Android			
iOS			
Linux	是		
Web	是	是	是

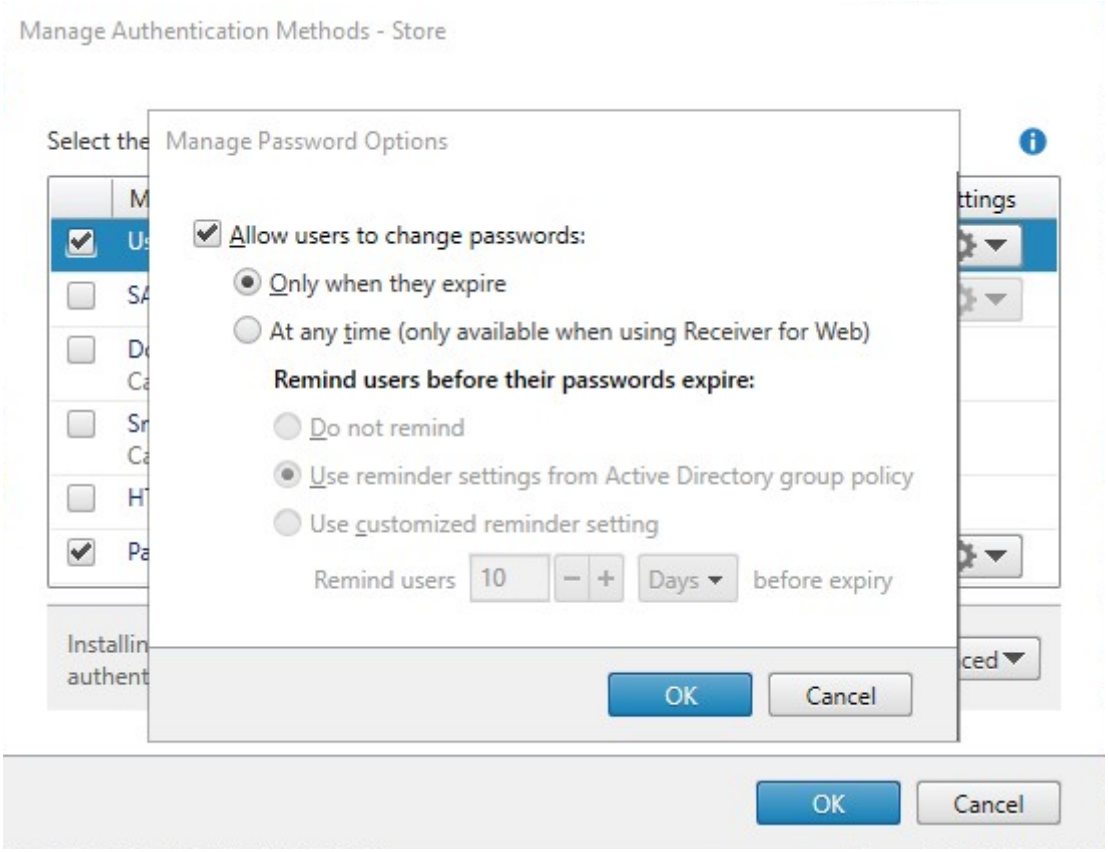
默认配置可防止 Citrix Workspace 应用程序和 Web 浏览器用户更改自己的密码，即使密码已过期亦如此。如果决定启用此功能，请确保服务器所在域的策略允许用户更改其密码。如果用户可以访问使用此身份验证服务的任何应用商店，则允许用户更改其密码会将敏感的安全功能暴露给这些用户。如果贵组织的安全策略将用户密码更改功能保留为仅供内部使用，请确保用户无法从企业网络外部访问任何应用商店。

如果您允许用户随时更改自己的密码，密码即将过期的本地用户在登录时会看到一条警告。默认情况下，向用户发出通知的时间段由相应的 Windows 策略设置决定。或者，您可以配置自定义通知周期。

1. 在管理身份验证方法窗口中，从用户名和密码 > 设置下拉菜单中，选择管理密码选项
2. 要允许用户更改密码，请选中允许用户更改密码复选框。

   > 注意：
   > 如果选择此选项，则必须自行安排支持方案，以为由于密码过期而无法访问桌面和应用程序的用户提供支持。

3. 选择是允许用户 **Only when they expire**（仅在密码过期时）更改密码，还是允许用户 **At any time**（随时）更改密码。
4. 选择是否在用户密码过期之前提醒用户。



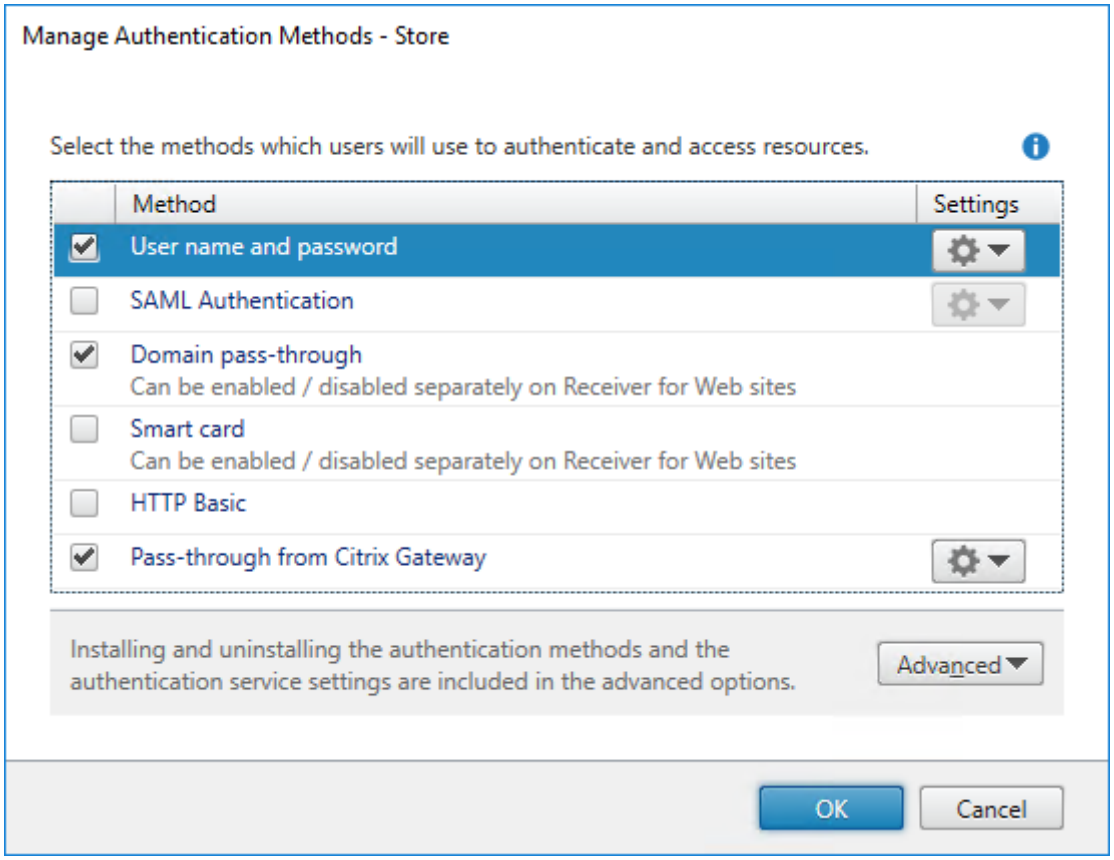
> 备注 **1**:
>
> StoreFront 不支持 Active Directory 中的细化密码策略。
>
> 备注 **2**:
>
> 确保 StoreFront 服务器上有足够的磁盘空间来存储所有用户的配置文件。为检查用户的密码是否即将过期，StoreFront 会在服务器上为该用户创建一个本地配置文件。StoreFront 必须能够与域控制器进行通信，才能更改用户的密码。
>
> 注意 **3**:
>
> 如果您随时启用或禁用更改密码功能，这也会影响从 Citrix Gateway 直通身份验证的管理密码选项下的设置。

凭据密码验证

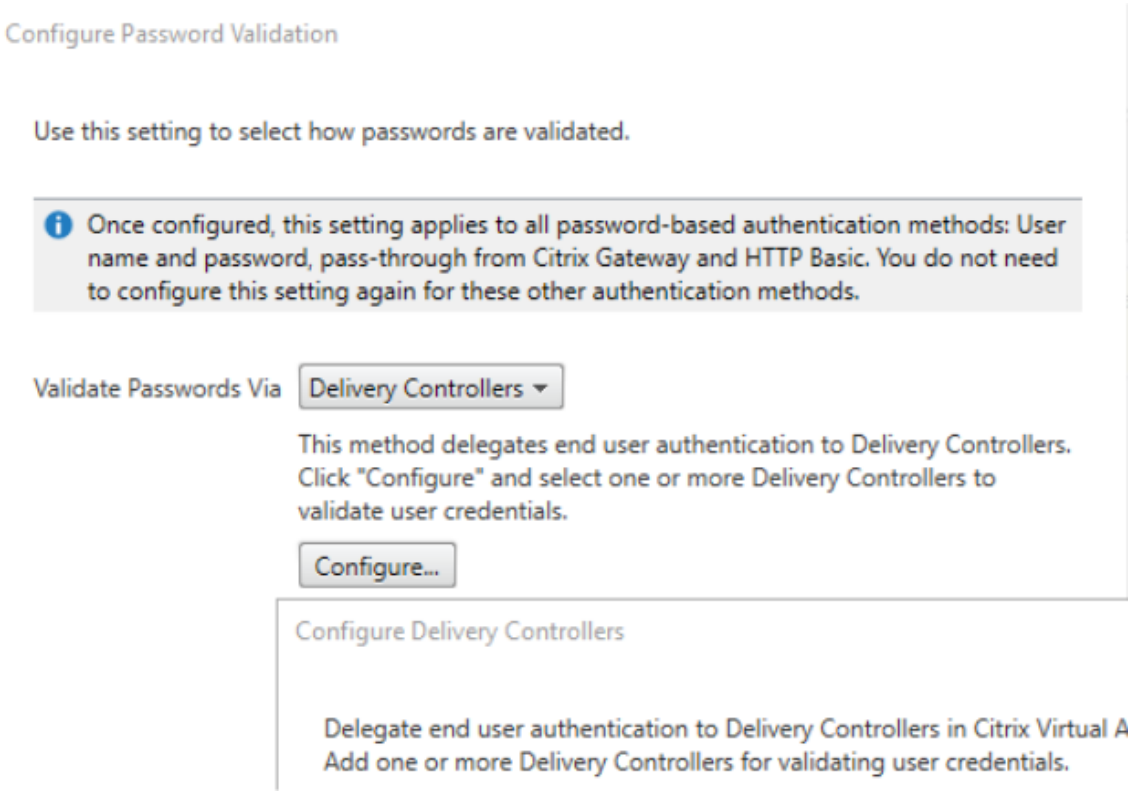
通常情况下，StoreFront 直接与 Active Directory 进行通信以验证凭据。

如果 StoreFront 与 Citrix Virtual Apps and Desktops 位于不同的域，并且无法设置 Active Directory 信任，则可以将 StoreFront 配置为使用 Citrix Virtual Apps and Desktops Delivery Controller 来验证用户名和密码凭据：

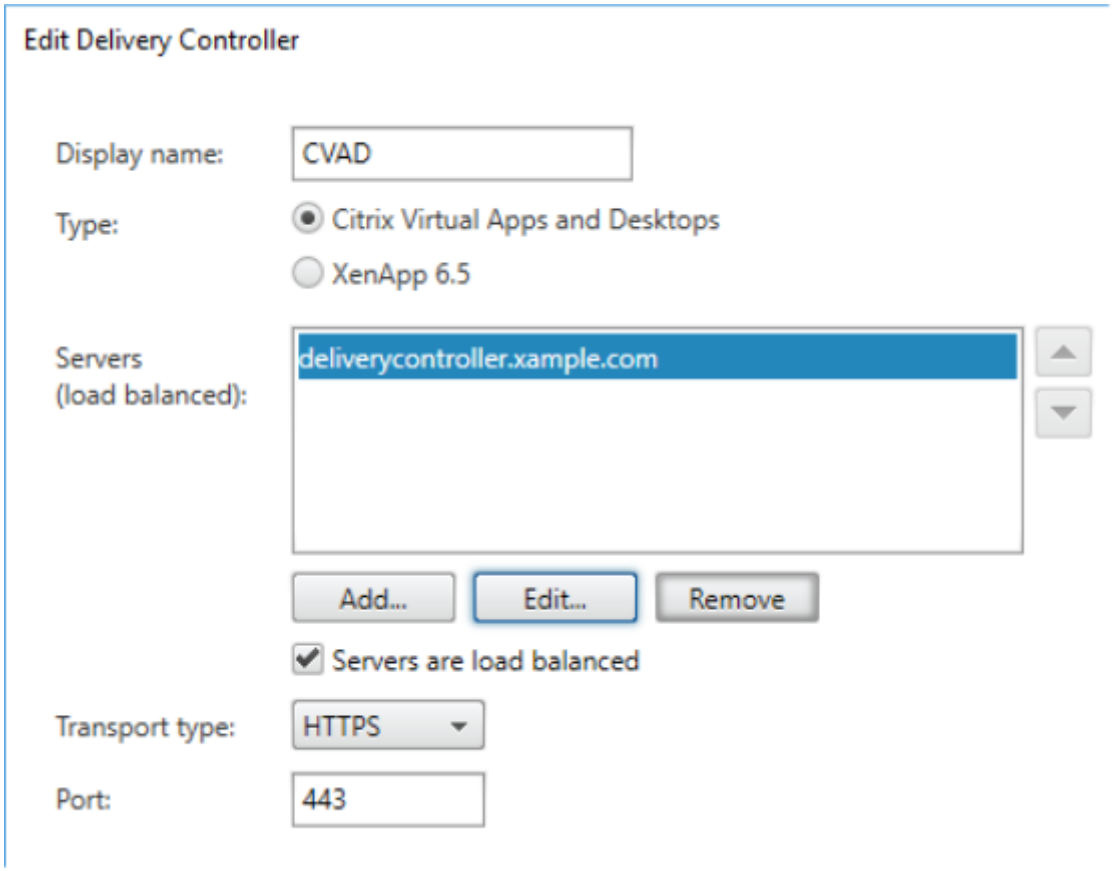
1. 在管理身份验证方法窗口中，从用户名和密码 **>** 设置下拉菜单中选择配置密码验证。



2. 在 **Validation Password Via**（验证密码方式）列表中，选择 **Delivery Controllers**（Delivery Controller），然后单击 **Configure**（配置）。



3. 按照 **Configure Delivery Controllers**（配置 Delivery Controller）屏幕上的说明添加一个或多个 **Delivery Controller** 用于验证用户凭据，然后单击 **OK**（确定）。



使用 **Active Directory**

1. 在管理身份验证方法页面上，从用户名和密码 > 设置列表中选择配置密码验证。
2. 在 **Validation Password Via**（验证密码方式）下拉菜单中，选择 **Active Directory**，然后单击 **OK**（确定）。

单点登录到 VDA

当用户启动资源时，StoreFront 使用用户登录到应用商店时使用的凭据单点登录到 VDA。

自定义登录屏幕

登录屏幕是基于模板生成的，该模板通常位于 C:\inetpub\wwwroot\Citrix\[应用商店名称]Auth\App_Data\Templates\Userna
您可以自定义该屏幕。

标题文本

当用户登录到应用商店时，默认情况下，登录对话框中不显示任何标题文本。可以显示文本“请登录”或编写自己的自定义消息：

1. 使用文本编辑器打开身份验证服务的 UsernamePassword.tfrm 文件。
2. 在此文件中查找以下行。

```
@* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
<!--NeedCopy-->
```

3. 删除前导和尾随前导 **@*** 及尾随 ***@**，取消语句的注释状态。

```
@Heading("ExplicitAuth:AuthenticateHeadingText")
<!--NeedCopy-->
```

Citrix Workspace 应用程序用户在登录使用此身份验证服务的应用商店时，将看到默认的标题文本“请登录”，或者此文本的相应本地化版本。

4. 要修改标题文本，请使用文本编辑器打开用于身份验证服务的 *ExplicitFormsCommon.xx.resx* 文件，该文件通常位于 C:\inetpub\wwwroot\Citrix\[Store name]Auth\App_Data\resources\ 目录中。
5. 在此文件中查找以下元素。编辑 <value> 元素中的文本，以修改用户在访问使用此身份验证服务的应用商店时在登录对话框中看到的主题文本。

```
<data name="AuthenticateHeadingText" xml:space="preserve">
    <value>My Company Name</value>
</data>
<!--NeedCopy-->
```

要为使用其他区域设置的用户修改登录对话框标题文本，请编辑已本地化的文件 *ExplicitAuth.languagecode.resx*，其中 **languagecode** 为区域设置标识符。

阻止适用于 **Windows** 的 **Citrix Workspace** 应用程序缓存密码和用户名

默认情况下，适用于 Windows 的 Citrix Workspace 应用程序会在用户登录 StoreFront 应用商店时存储其密码。为防止适用于 Windows 的 Citrix Workspace 应用程序缓存用户的密码，您可以编辑身份验证服务的文件。

1. 使用文本编辑器打开文件 inetpub\wwwroot\Citrix\[Store name]Auth\App_Data\Templates\UsernamePassword
2. 在此文件中查找以下行。

```
@SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey:
    "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked:
    ControlValue("SaveCredentials"))
<!--NeedCopy-->
```

3. 按如下所示，注释掉语句。

```
<!-- @SaveCredential(id: @GetTextValue("saveCredentialsId"),
    labelKey: "ExplicitFormsCommon:SaveCredentialsLabel",
    initiallyChecked: ControlValue("SaveCredentials")) -->
<!--NeedCopy-->
```


用户每次登录使用此身份验证服务的应用商店时都必须输入其密码。

默认情况下，适用于 Windows 的 Citrix Workspace 应用程序会自动填充上次输入的用户名。要禁止填充用户名字段，或者了解隐藏缓存密码的替代机制，请参阅阻止适用于 Windows 的 Citrix Workspace 应用程序缓存密码和用户名。

通过 **Citrix Gateway** 进行远程访问

可以配置 Citrix Gateway，以便用户使用其域用户名和密码登录网关。这些凭据将传递给 StoreFront 以登录到应用商店。要将 Citrix Gateway 配置为进行 LDAP 用户名和密码身份验证，请参阅 NetScaler 文档 - LDAP 身份验证。要配置 StoreFront，请参阅从 Citrix Gateway 直通。

联合身份验证服务配置

April 17, 2024

使用诸如 SAML 之类的身份验证方法时，如果用户不直接在 Citrix Workspace 应用程序中输入凭据，则默认情况下无法单点登录 VDA。在这些情况下，您可以使用联合身份验证服务 (FAS) 通过证书身份验证为 VDA 提供单点登录。

要将 FAS 与 StoreFront 配合使用，必须使用 PowerShell SDK 配置 StoreFront。请使用 Set-STFClaimsFactoryNames 将声明工厂设置为 `FASClaimsFactory`，使用 Set-STFStoreLaunchOptions 将 VDA 登录数据登录提供程序设置为 `FASLogonDataProvider`。

例如，要为应用商店启用 FAS，请执行以下操作：

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]
$auth = Get-STFAuthenticationService -StoreService $store
Set-STFClaimsFactoryNames -AuthenticationService $auth -
    ClaimsFactoryName "FASClaimsFactory"
Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider "
    FASLogonDataProvider"
<!--NeedCopy-->
```

要为应用商店禁用 FAS，请执行以下操作：

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]
$auth = Get-STFAuthenticationService -StoreService $store
Set-STFClaimsFactoryNames -AuthenticationService $auth -
    ClaimsFactoryName "standardClaimsFactory"
Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
<!--NeedCopy-->
```

替换相应虚拟路径的 `[VirtualPath]`，例如 `/Citrix/Store`。

要配置 FAS 服务器列表以及其他设置，必须使用组策略。有关更多详细信息，请参阅 FAS 文档。

通过浏览器使用域直通或智能卡进行身份验证时不使用 FAS。

配置和管理应用商店

February 22, 2024

在 Citrix StoreFront 中，可以创建和管理用于将 Citrix Virtual Apps and Desktops 中的应用程序和桌面汇集在一起的应用商店，从而使用户能够按需、自助访问这些资源。

任务	详细信息
创建应用商店	可以根据需要配置多个其他应用商店。
配置应用商店	配置应用商店设置
删除应用商店	删除不需要的应用商店。
为用户导出应用商店预配文件	生成包含应用商店连接详细信息的文件，其中包括为应用商店配置的所有 Citrix Gateway 部署和信标点。
向用户公告和隐藏应用商店	在用户将 Citrix Workspace 应用程序配置为使用基于电子邮件的帐户发现或 FQDN 时禁止向用户呈现应用商店以添加到其帐户中。
配置 Kerberos 委派	配置 StoreFront 是否使用 Kerberos 委派向 Delivery Controller 进行身份验证。
管理通过应用商店提供的资源	在应用商店中添加或删除资源。
管理通过 Citrix Gateway 对应用商店的远程访问	为从公用网络连接的用户配置通过 Citrix Gateway 对应用商店的访问。
证书吊销列表 (CRL) 检查	将 StoreFront 配置为使用已发布的证书吊销列表 (CRL) 检查 CVAD Delivery Controller 所使用的 TLS 证书的状态。
将两个 StoreFront 应用商店配置为共享公用订阅数据存储	将两个 StoreFront 应用商店配置为共享公用订阅数据存储。
启用或禁用收藏夹	为应用商店启用或禁用收藏夹。
管理应用商店的订阅数据	查看、导入、导出和清除订阅数据（收藏夹）。
将两个 StoreFront 应用商店配置为共享公用订阅数据存储	将两个应用商店配置为共享公用订阅数据库。
使用 Microsoft SQL Server 存储收藏夹数据	使用外部 SQL Server 数据库存储订阅（收藏夹）数据。
Citrix Virtual Apps and Desktops 配置	配置影响资源在应用商店 Web 站点中的显示方式的 Citrix Virtual Apps and Desktops 设置
高级应用商店设置	配置高级应用商店设置。
最佳 HDX 路由	配置使用哪个网关连接到哪些资源。

任务	详细信息
默认 ica 设置	通过将 HDX 设置添加到 default.ica 来配置这些设置
ICA 文件签名	配置 ica 文件签名
Windows 快捷方式	配置适用于 Windows 的 Citrix Workspace 应用程序如何为喜爱的和必需的应用程序创建“开始”菜单和桌面快捷方式。

创建应用商店

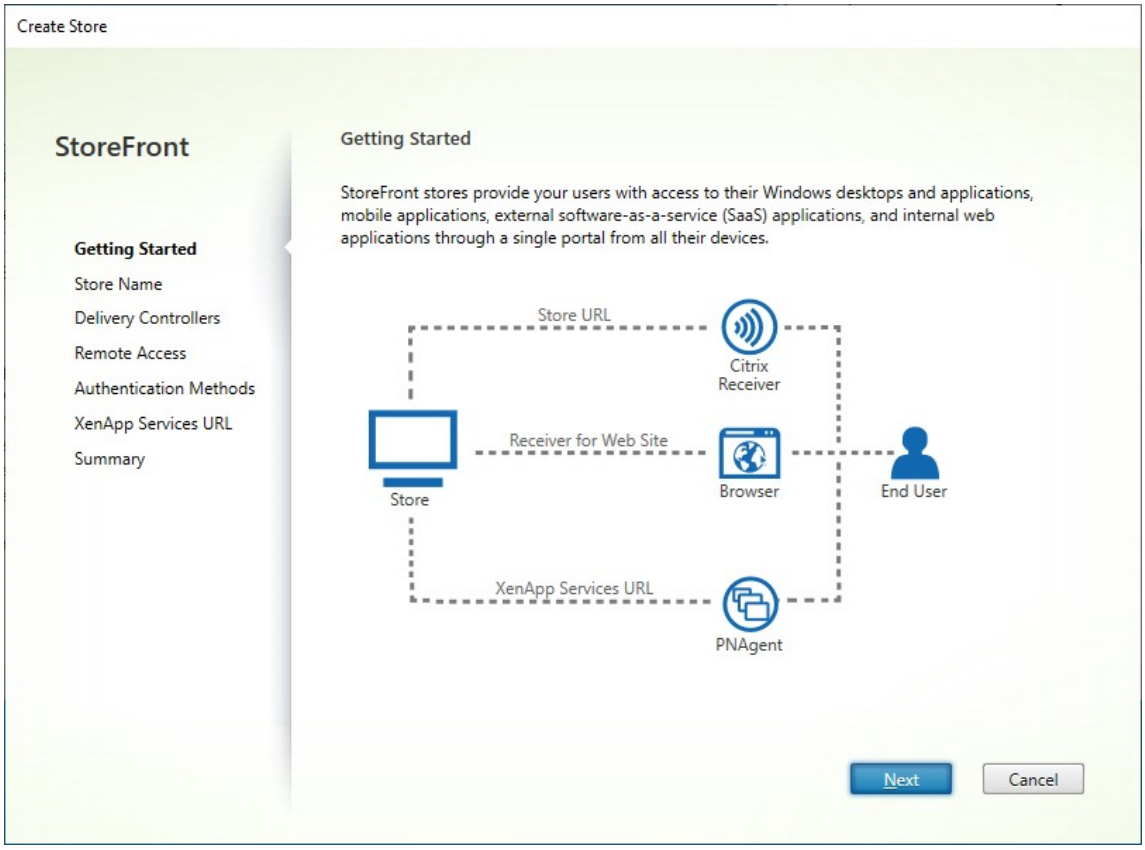
April 17, 2024

可以根据需要创建任意数量的应用商店；例如，可以为特定用户组创建应用商店，或者将一组特定资源归入一组。

> 重要提示：
>
> 在多服务器部署中，请一次仅使用一台服务器以更改服务器组的配置。确保 Citrix StoreFront 管理控制台未在部署中的任何其他服务器上运行。完成后，请
> 将对配置所做的更改传播到服务器组，以便更新部署中的其他服务器。

要创建应用商店，需要确定并配置与服务器（用于提供希望通过应用商店获得的资源）间的通信。然后，配置通过 Citrix Gateway 对该应用商店进行远程访问（可选）。

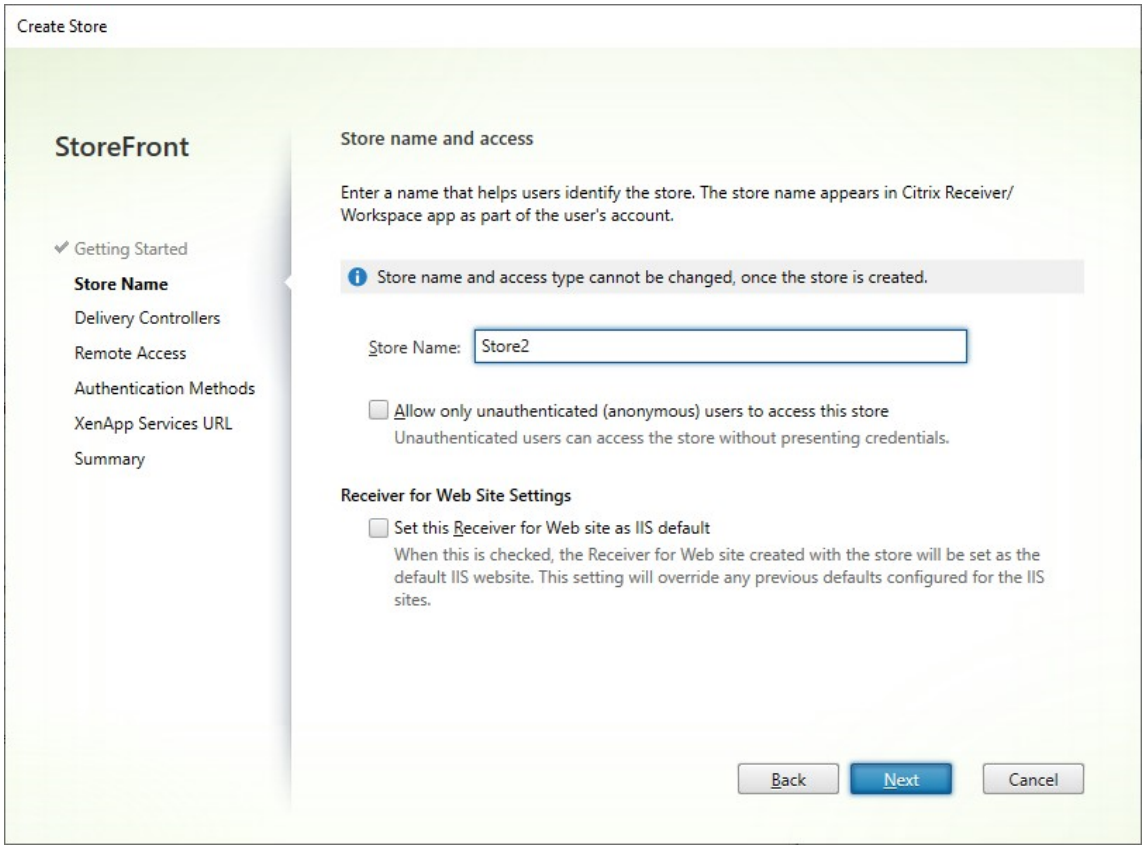
1. 在操作窗格中，单击创建应用商店。



单击 **Next**（下一步）

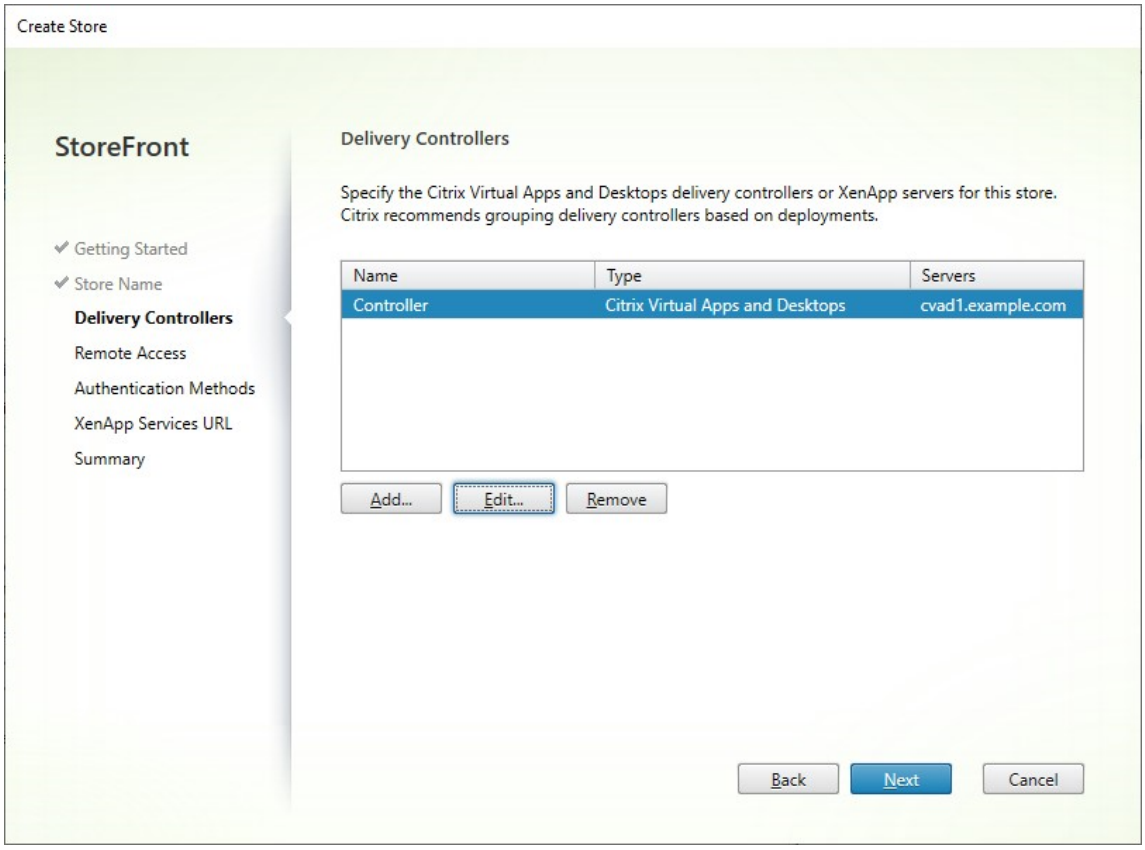
2. 在应用商店名称选项卡上，填写以下内容：

   - 输入应用商店名称
   - 如果您希望允许用户匿名或未经身份验证访问应用商店，请勾选仅允许未经身份验证的用户访问此应用商店。创建未经身份验证的应用商店时，身份验证方法和远程访问页面不可用，左侧和“操作”窗格中的服务器组节点将替换为更改基本 **URL**。（这是唯一可用的选项，因为服务器组在未加入域的服务器中不可用。）



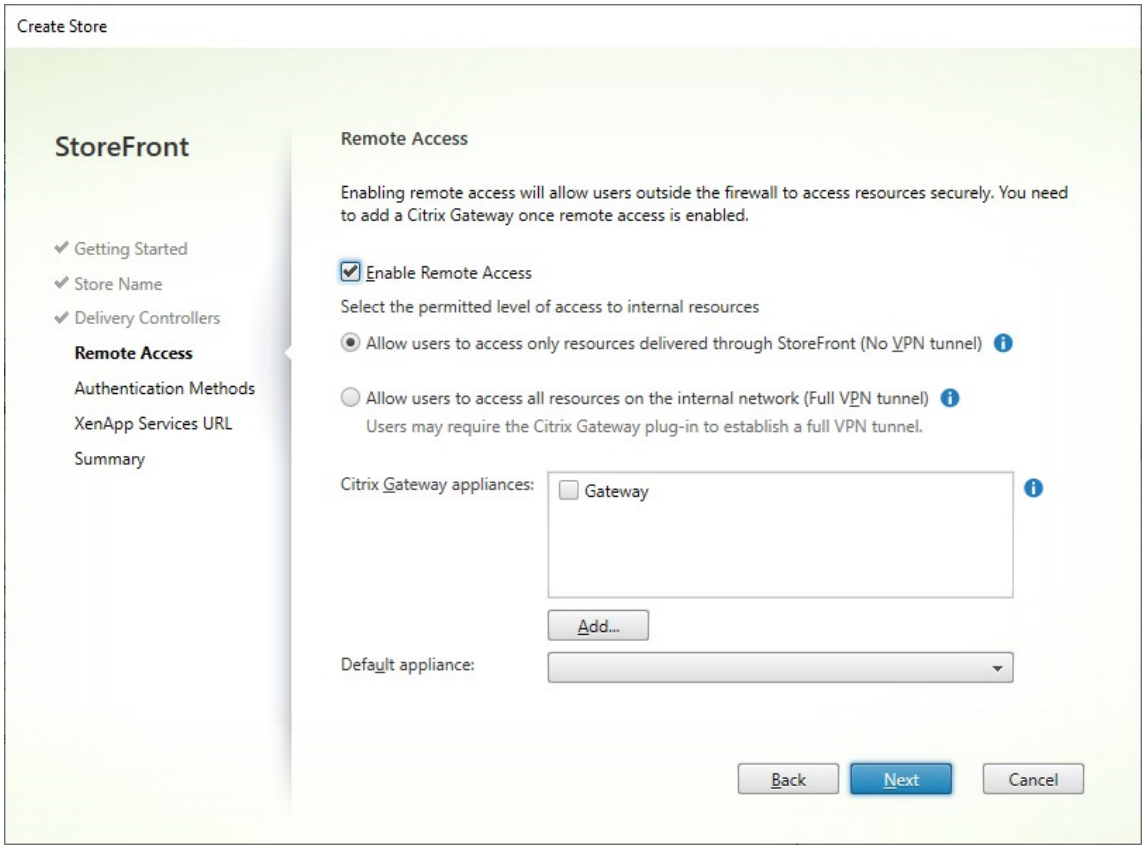
单击 **Next**（下一步）

3. 在 **Delivery Controller** 选项卡上，为您的虚拟桌面和应用程序添加资源源。有关更多详细信息，请参阅管理应用商店中提供的资源



单击下一步。

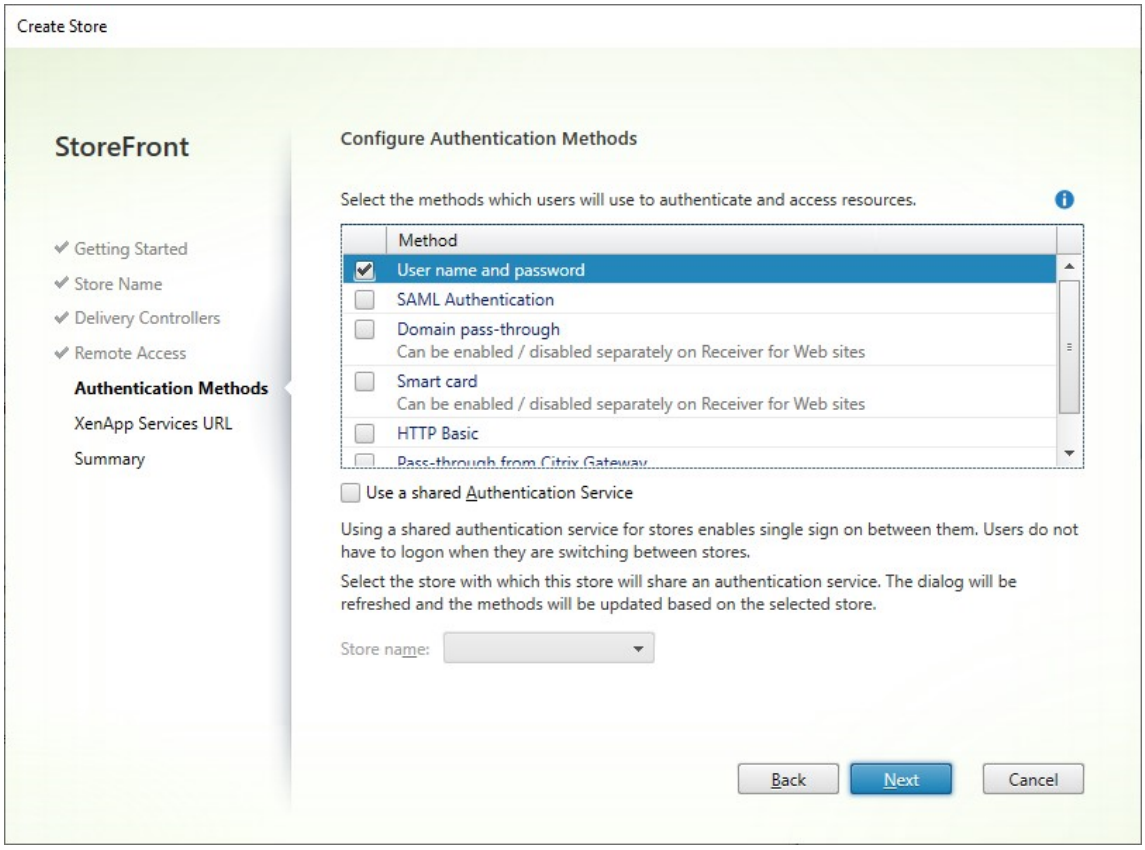
4. 在远程访问选项卡上，选择是否要通过 Citrix Gateway 提供应用商店。有关更多详细信息，请参阅通过 Citrix Gateway 管理对应用商店的远程访问。



5. 在身份验证方法选项卡上，选择用户用来向应用商店验证身份的方法，然后单击下一步。

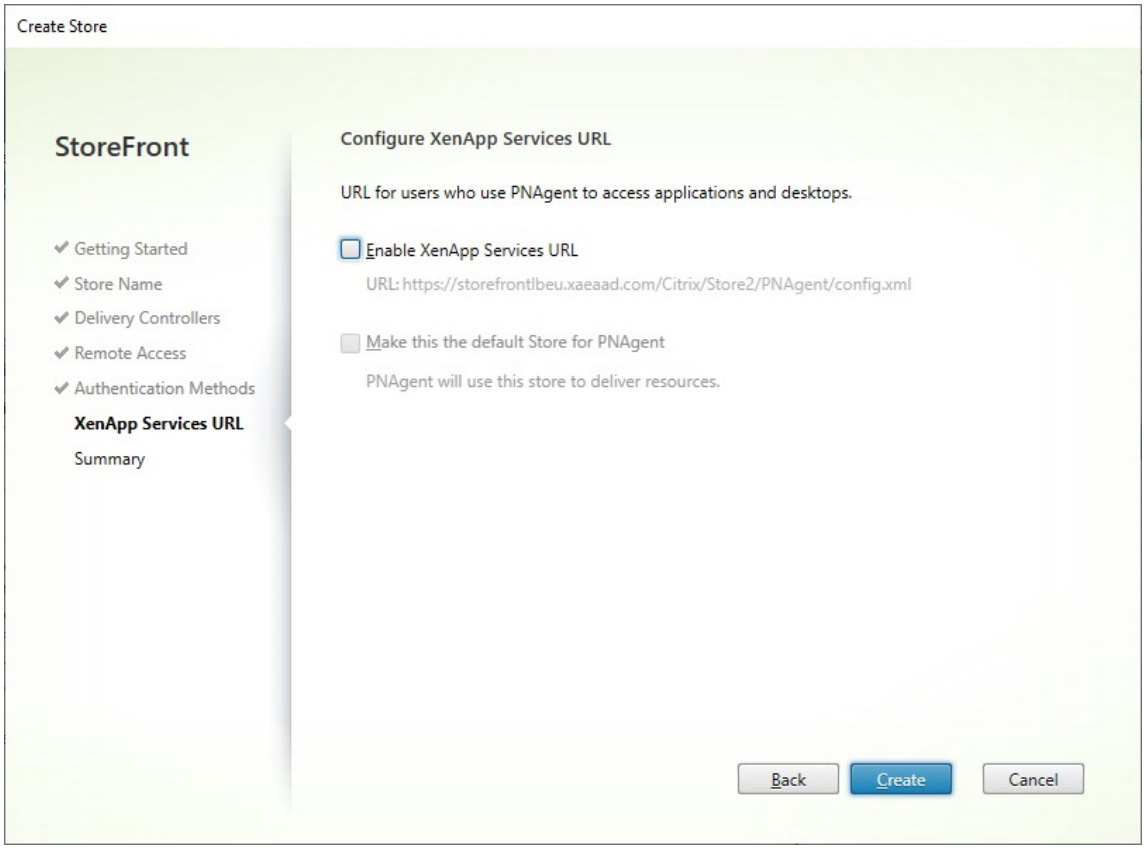
   有关可用身份验证方法的更多详细信息，请参阅配置身份验证服务。

   可以与其他应用商店共享身份验证配置，而非为此应用商店单独配置身份验证方法。为此，请勾选使用共享身份验证服务，然后选择现有应用商店。



单击 **Next**（下一步）

6. 在 **XenApp Services URL** 选项卡上，如果您有需要 PNAgent 的旧设备，请选中启用 **XenApp Services URL**，否则请取消勾选。



单击创建

7. 创建了应用商店时，单击完成。

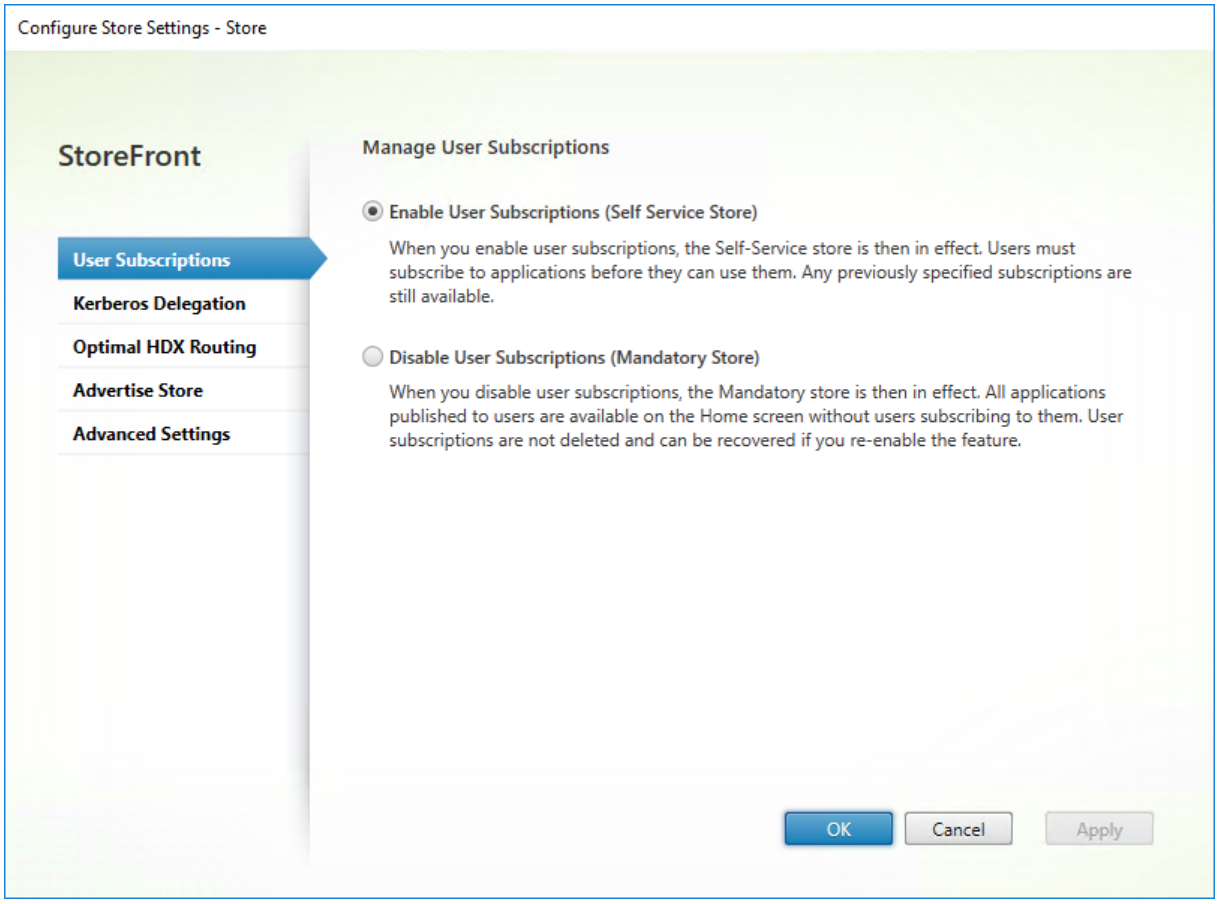
创建新应用商店时，它还会创建一个新 Web 站点以允许用户访问该应用商店。您可以配置此 Web 站点或者创建其他 Web 站点。

配置应用商店

April 17, 2024

要修改应用商店，请执行以下操作：

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点，然后在操作窗格中单击配置应用商店设置。
2. 转到用户订阅选项卡以配置是否启用收藏夹。
3. 转到 Kerberos 委派选项卡，配置应用商店是否使用 Kerberos 委派向 Delivery Controller 进行身份验证。
4. 转到最佳 HDX 路由选项卡，根据应用程序和桌面的位置配置用于启动应用程序和桌面的网关。
5. 转到公告应用商店选项卡，配置 Workspace 应用程序在用户输入 FQDN 或电子邮件地址时是否向用户公告应用商店。

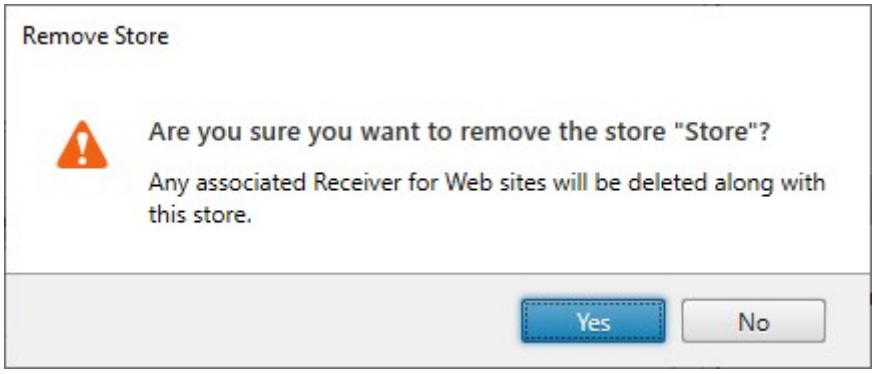


删除应用商店

April 17, 2024

要删除应用商店，请执行以下操作：

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点
2. 在操作窗格中，单击删除应用商店
3. 在确认窗口中，单击是。



当您删除应用商店时，所有关联的 Web 站点也将删除。

为用户导出应用商店预配文件

February 22, 2024

您可以生成包含应用商店连接详细信息的文件，其中包括为应用商店配置的所有 Citrix Gateway 部署和信标点。将这些文件提供给用户，以便用户能够利用应用商店的详细信息自动配置 Citrix Workspace 应用程序。用户在通过 Web 浏览器访问应用商店时，还可以下载 Citrix Workspace 应用程序预配文件。

> 重要提示：
>
> 在多服务器部署中，请一次仅使用一台服务器以更改服务器组的配置。确保 Citrix StoreFront 管理控制台未在部署中的任何其他服务器上运行。完成后，请
> 将对配置所做的更改传播到服务器组，以便更新部署中的其他服务器。

1. 要生成包含多个应用商店的详细信息的预配文件，请在“操作”窗格中单击导出多应用商店预配文件，然后选择要包含在此文件中的应用商店。
2. 单击导出并使用扩展名.cr 将预配文件保存到网络中的合适位置。

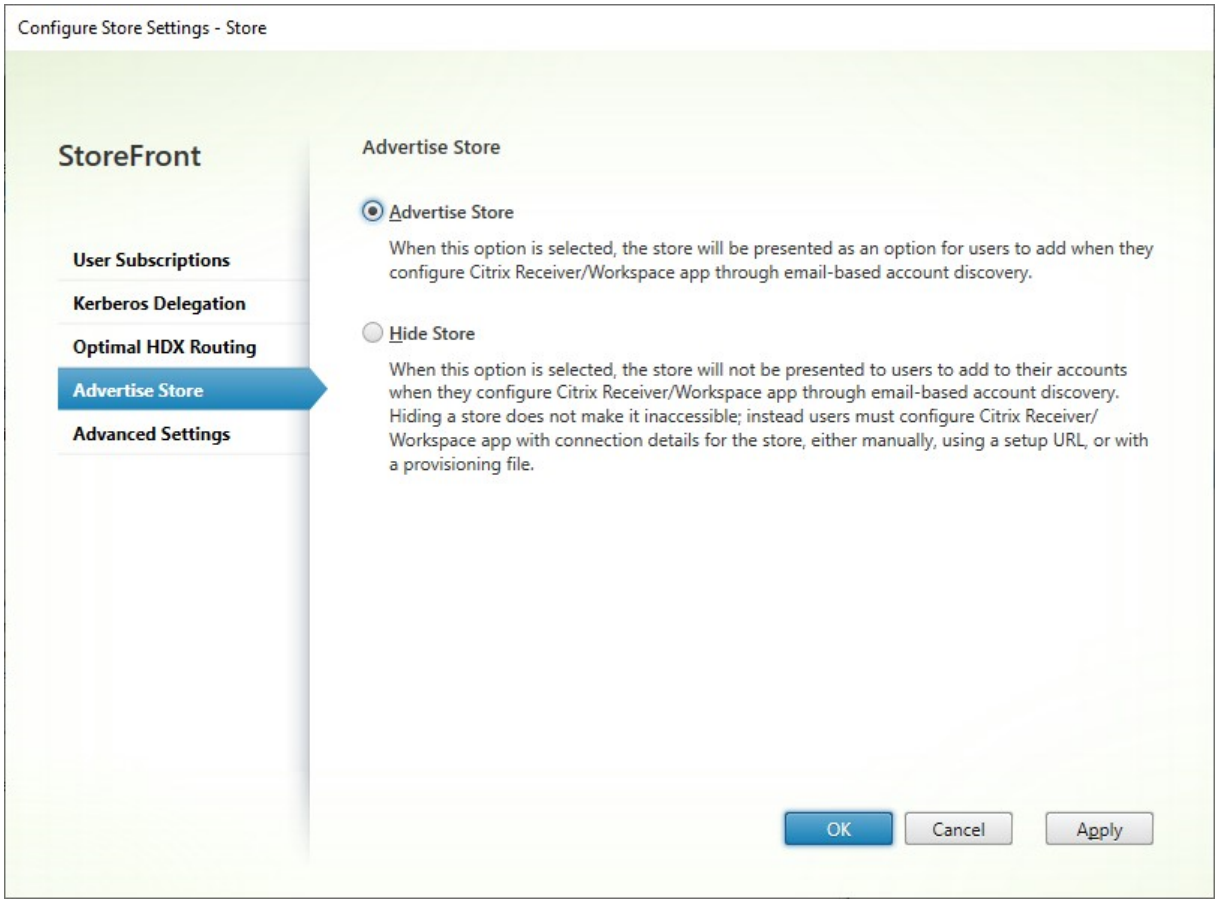
向用户公告和隐藏应用商店

April 17, 2024

您可以在用户将 Citrix Workspace 应用程序配置为使用基于电子邮件的帐户发现或 FQDN 时选择是否向用户呈现应用商店以添加到其帐户中。默认情况下，创建应用商店后，该应用商店将显示为一个选项，用户可以在发现了托管该应用商店的 StoreFront 部署时将其添加到 Citrix Receiver 中。隐藏应用商店并不是将应用商店设置为无法访问，而是用户必须为 Citrix Workspace 应用程序手动配置（使用设置 URL 或预配文件）应用商店的连接详细信息。

> 重要提示：
>
> 在多服务器部署中，请一次仅使用一台服务器以更改服务器组的配置。确保 Citrix StoreFront 管理控制台未在部署中的任何其他服务器上运行。完成后，请
> 将对配置所做的更改传播到服务器组，以便更新部署中的其他服务器。

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点，然后在操作窗格中单击配置应用商店设置 > 公告应用商店。
2. 在公告应用商店页面上，选择公告应用商店或隐藏应用商店。



Kerberos 委派

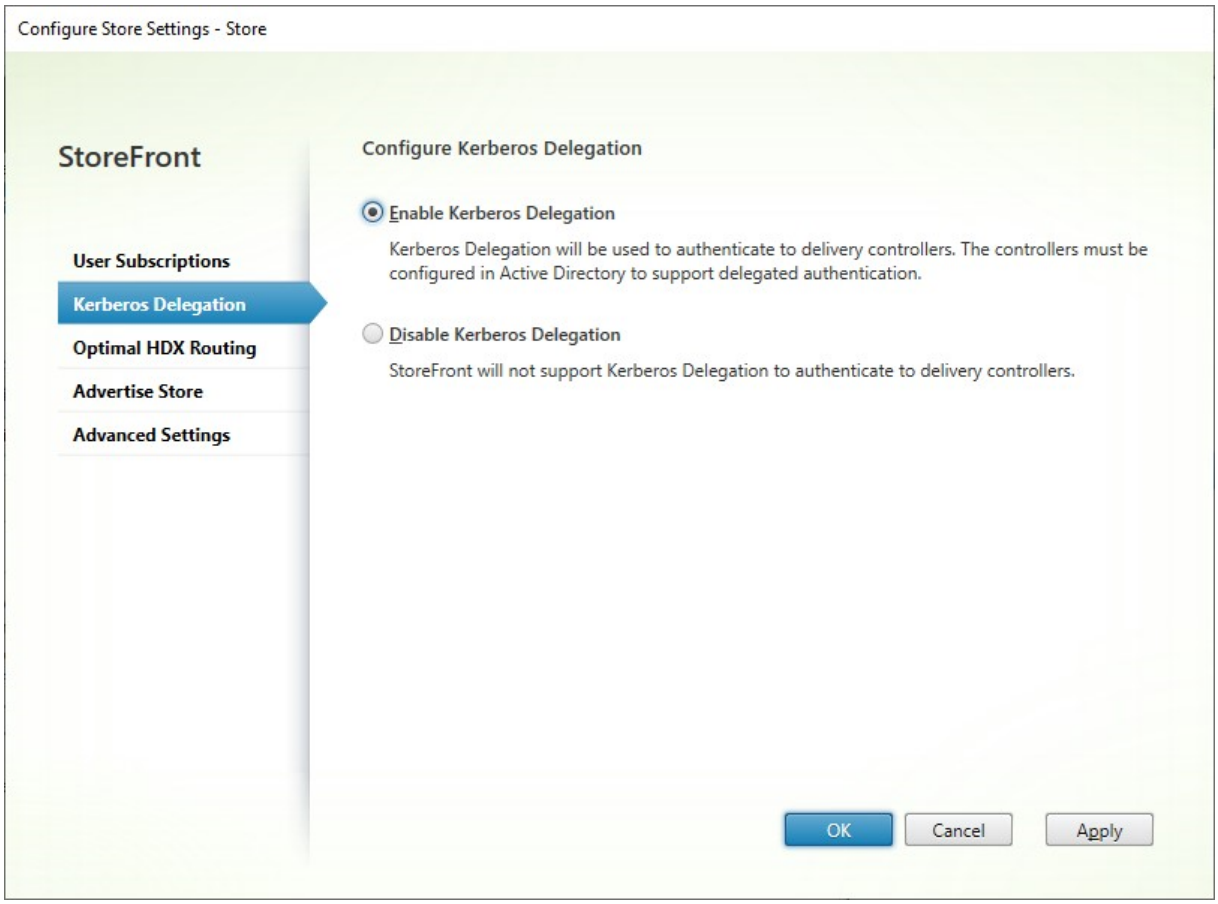
April 17, 2024

> 注意：
>
> Kerberos 只能与 XenApp 6.5 及更早版本一起使用。

直接或通过 Citrix Gateway 使用域直通或智能卡身份验证时，StoreFront 没有用户的凭据，因此无法使用用户的

凭据向 Delivery Controller 进行身份验证。使用 XenApp 6.5 及更早版本时，您可以启用 Kerberos 委派，以允许 StoreFront 模拟用户向 Delivery Controller 进行身份验证。这需要在 Active Directory 中配置委派。

1. 选择一个应用商店，然后在“操作”窗格中单击配置应用商店设置。
2. 选择 **Kerberos** 委派选项卡。
3. 选择是启用 **Kerberos** 委派还是禁用 **Kerberos** 委派。
4. 按应用或确定保存所做的更改。



PowerShell SDK

要配置 Kerberos 委派，请使用带参数 `-KerberosDelegation` 的 cmdlet Set-STFStoreService

管理通过应用商店提供的资源

April 17, 2024

使用管理 **Delivery Controller** 屏幕可添加、修改和删除 Citrix Virtual Apps and Desktops、Citrix Desktops as a Service 和 Citrix Secure Private Access 提供的资源馈送。

查看资源源

1. 在 Citrix StoreFront 管理控制台中，在左侧窗格中选择应用商店节点。
2. 在结果窗格中选择一个应用商店
3. 在操作窗格中，单击管理 **Delivery Controller**。

使用 **PowerShell SDK** 查看资源源

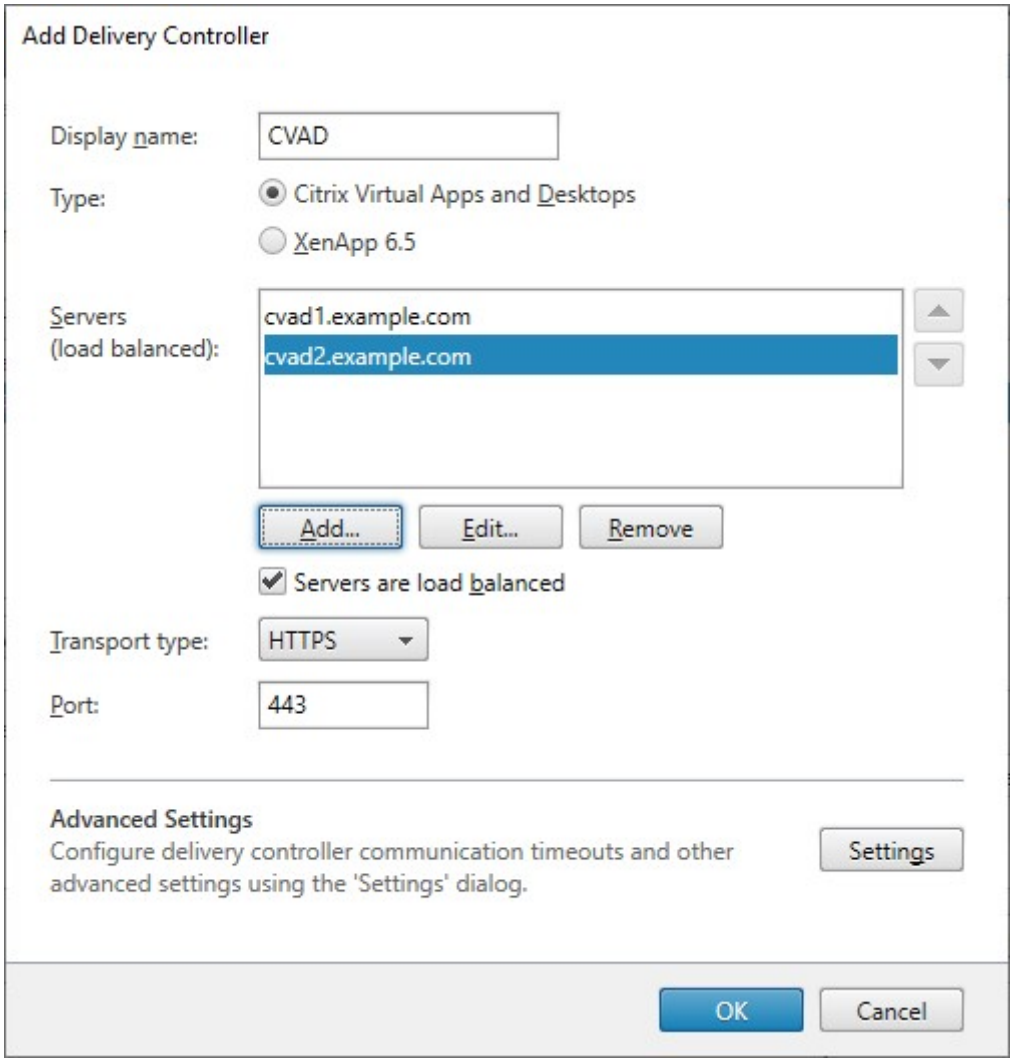
在 PowerShell SDK 中，使用 Get-STFStoreFarm 命令列出所有资源源或者特定的资源源。

添加资源源

为 **Citrix Virtual Apps and Desktops** 添加资源源

1. 在管理 **Delivery Controller** 屏幕中，单击添加。
2. 输入可帮助您识别源的显示名称。
3. 选择类型为 **Citrix Virtual Apps and Desktops**。
4. 在服务器下，单击添加，然后输入 Delivery Controller 的名称。对每个 Delivery Controller 重复此操作。Citrix 建议您至少有两台服务器用于负载平衡或故障转移。
5. Citrix 建议您选择服务器已实现负载平衡选项。这会导致 StoreFront 在每次启动时从列表中随机选择服务器，从而在所有 Delivery Controller 或连接器之间分发负载。如果未选择此选项，服务器列表将按优先级顺序视为故障转移列表。在这种情况下，全部启动都发生在列表中的第一个活动的 Delivery Controller 或连接器上。如果该服务器脱机，全部启动将使用列表中的第二个服务器进行，依此类推。
6. 在 **Transport type**（传输类型）列表中，选择 StoreFront 用于与服务器进行通信的连接类型。
   - 要通过未加密的连接发送数据，请选择 **HTTP**。如果选择此选项，则必须自行安排安全方案，以保护 StoreFront 与服务器之间连接的安全。
   - 要通过 TLS 连接发送数据，请选择 **HTTPS**（推荐）。如果为 Citrix Virtual Apps and Desktops 服务器选择此选项，请确保将 Citrix XML Service 设置为与 Microsoft Internet Information Services (IIS) 共享其端口，并将 IIS 配置为支持 HTTPS。

> 注意：
>
> 如果您使用 HTTPS 来保护 StoreFront 与服务器之间的连接安全，请确保在服务器列表中指定的名称与这些服务器的证书上的名称完全一致（包括大小写）。



1. 指定 StoreFront 连接服务器所用的端口。默认端口 80 用于建立 HTTP 连接，端口 443 用于建立 HTTPS 连接。指定的端口必须是 Citrix XML Service 使用的端口。

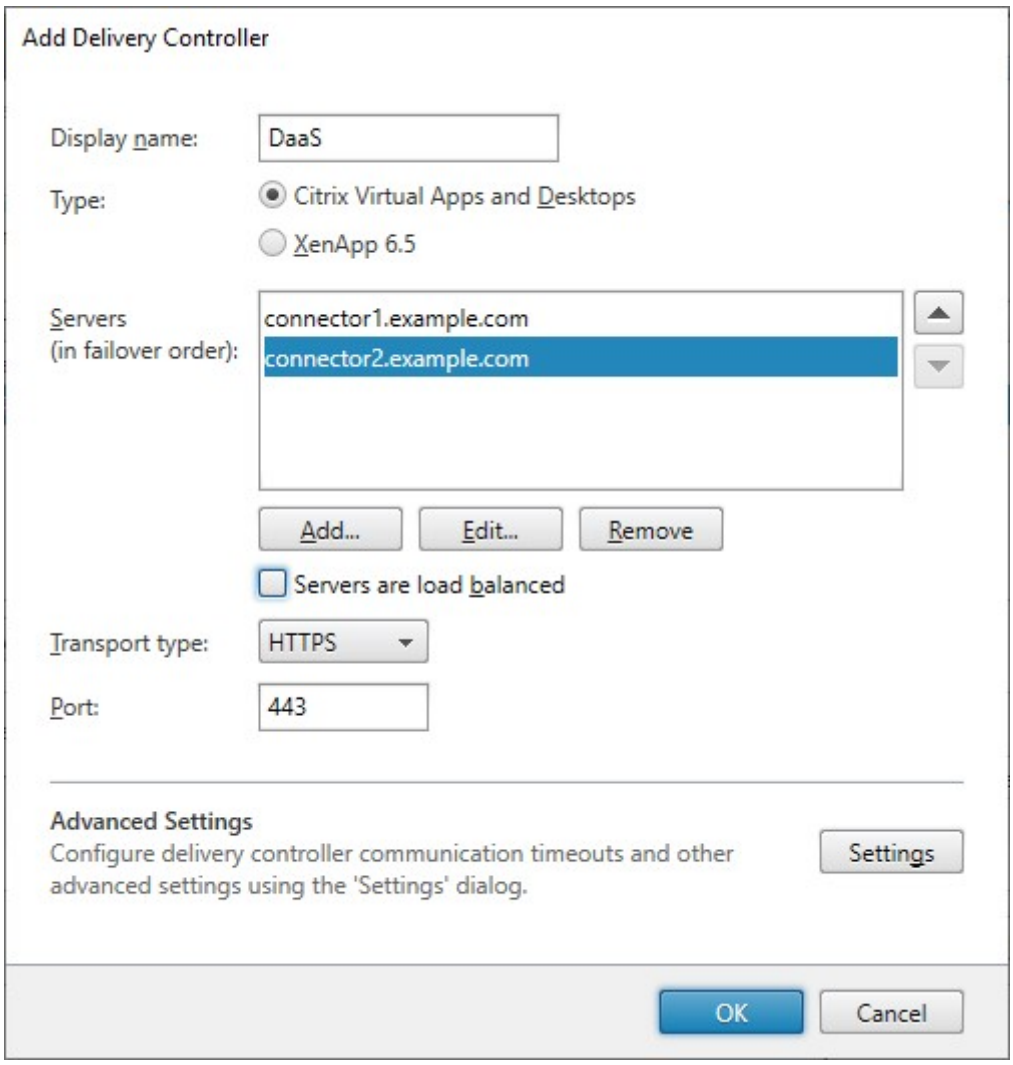
为 **Citrix Desktops as a Service** 添加资源源

1. 在管理 **Delivery Controller** 屏幕中，单击添加。
2. 输入可帮助您识别源的显示名称。
3. 选择类型为 **Citrix Virtual Apps and Desktops**。
4. 在服务器下，单击添加，然后输入 Cloud Connector 的名称。对每台服务器或连接器重复此操作。Citrix 建议您至少有两个连接器以实现冗余。如果您有多个资源位置，Citrix 建议您添加所有资源位置中的 Cloud Connector 并启用高级运行状况检查。这样可以确保在停机期间，StoreFront 可以使用本地主机缓存在适当的位置启动 VDA。

5. 如果您有来自多个位置的连接器，Citrix 建议您将 StoreFront 服务器的延迟最低的连接器放置到列表顶部，并清除服务器已实现负载平衡选项。由于连接器仅将信息代理到 DaaS Delivery Controller，因此使用负载平衡的好处有限。
6. 在 **Transport type**（传输类型）列表中，选择 StoreFront 用于与服务器进行通信的连接类型。
   - 要通过未加密的连接发送数据，请选择 **HTTP**。如果选择此选项，则必须自行安排安全方案，以保护 StoreFront 与 Cloud Connector 之间连接的安全。
   - 要通过安全的 HTTPS 连接发送数据，请选择 **HTTPS**。如果选择此选项，则必须确保将 Cloud Connector 配置为使用 HTTPS。

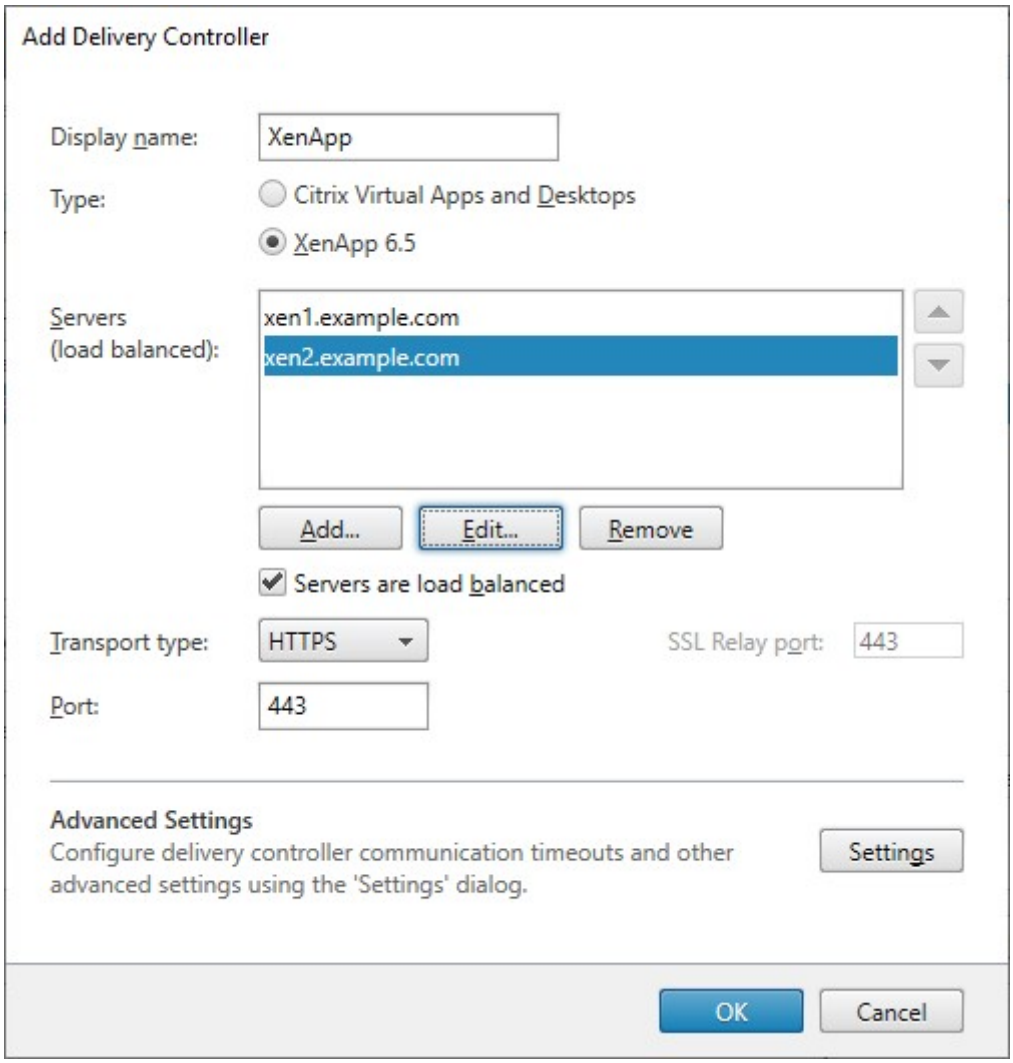
   > 注意：
   >
   > 如果您使用 HTTPS 来保护 StoreFront 与服务器之间的连接安全，请确保在服务器列表中指定的名称与这些服务器的证书上的名称完全一致（包括大小写）。

7. 指定 StoreFront 连接服务器所用的端口。默认端口 80 用于建立 HTTP 连接，端口 443 用于建立 HTTPS 连接。



为 **XenApp 6.5** 添加资源源

1. 输入可帮助您识别源的显示名称。
2. 选择 **Citrix Secure Private Access** 作为类型。
3. 输入 **Citrix Secure Private Access** 服务器名称。
4. 在 **Transport type**（传输类型）列表中，选择 StoreFront 用于与服务器进行通信的连接类型。
   - 要通过未加密的连接发送数据，请选择 **HTTP**。如果选择此选项，则必须自行安排安全方案，以保护 StoreFront 与服务器之间连接的安全。
   - 要通过使用安全套接字层 (SSL) 或传输层安全性 (TLS) 的安全 HTTP 连接发送数据，请选择 **HTTPS**。
   - 要通过与 Citrix Virtual Apps 服务器之间使用 SSL Relay 的安全连接发送数据，以执行主机身份验证和数据加密，请选择 SSL Relay。还必须输入 SSL 中继端口
5. 指定 StoreFront 连接服务器所用的端口。默认端口 80 用于建立 HTTP 或 SSL 中继连接，端口 443 用于建立 HTTPS 连接。



使用 **PowerShell SDK** 创建资源源

要添加资源源，请使用命令 Add-STFStoreFarm

- 对于 Citrix Virtual Apps and Desktops 或 Citrix 桌面即服务，请将 `FarmType` 设置为 `XenDesktop`。
- 对于 XenApp 6.5，请将 `FarmType` 设置为 `XenApp`。

修改资源源

在管理 **Delivery Controller** 屏幕中，选择一个资源源并单击添加。

使用 **PowerShell SDK** 修改资源源

要使用 PowerShell 修改资源源，请使用命令 Set-STFStoreFarm

删除资源源

在管理 **Delivery Controller** 屏幕中，选择一个资源源并单击删除。

使用 **PowerShell SDK** 删除资源源

要使用 PowerShell 删除资源源，请使用命令 Remove-STFStoreFarm

配置服务器跳过行为

为了提高某些资源提供服务器不可用时的性能，StoreFront 会临时绕过无法响应的服务器。绕过某个服务器时，StoreFront 将忽略该服务器，不使用它来访问资源。使用以下参数可指定跳过行为的持续时间：

- 所有失败跳过的持续时间指定某个特定 Delivery Controller 的所有服务器都被跳过时，StoreFront 用来代替跳过持续时间的缩短的持续时间（以分钟为单位）。默认值为 0 分钟。
- 跳过持续时间指定 StoreFront 尝试与单个服务器通信失败后跳过该服务器的时间（以分钟为单位）。默认跳过持续时间为 60 分钟。

指定“所有失败跳过的持续时间”时的注意事项

设置较大的所有失败跳过的持续时间值可以降低特定 Delivery Controller 不可用产生的影响，但这也会产生负面影响，即临时网络中断或服务器不可用后用户在指定持续时间内不可使用此 Delivery Controller 中的资源。为应用商店配置许多 Delivery Controller 时，请考虑使用更大的所有失败跳过的持续时间值，尤其是对于非业务关键型 Delivery Controller。

设置较小的所有失败跳过的持续时间值会提高该 Delivery Controller 所提供的资源的可用性；但是，如果为应用商店配置了许多 Delivery Controller，并且其中一些不可用，客户端超时可能会增加。配置的场不多以及用于业务关键型 Delivery Controller 时，可以保留默认值 0 分钟。

更改绕过参数

1. 在 Citrix StoreFront 管理控制台中，在左侧窗格中选择应用商店节点。
2. 在结果窗格中选择一个应用商店。
3. 在操作窗格中，单击管理 **Delivery Controller**。
4. 选择一个 Controller，单击编辑，然后单击编辑 **Delivery Controller** 屏幕上的设置。
5. 在“高级设置”下，单击设置。
6. 在“配置高级设置”对话框中：

    a) 在所有失败跳过的持续时间行中，单击第二列并输入 Delivery Controller 的所有服务器响应失败后将 Delivery Controller 视为脱机的时间（以分钟为单位）。
    b) 在跳过持续时间行中，单击第二列并输入单台服务器响应失败后将其视为脱机的时间（以分钟为单位）。

将用户映射到资源源

默认情况下，访问某个应用商店的用户会看到为该应用商店配置的所有资源源所提供的所有资源的聚合。要为不同用户提供不同资源，可以配置单独的应用商店或分隔 StoreFront 部署。或者，您可以根据用户的 Microsoft Active Directory 组成员身份提供对特定部署的访问权限。这样，就可以通过单个应用商店为不同用户组配置不用体验。

例如，可以将所有用户的公用资源汇集在一个部署中，而将“财务”部门的财务应用程序汇集在另一个部署中。在这种配置下，如果用户不是“财务”用户组的成员，那么该用户在访问应用商店时将只会看到公用资源。而“财务”用户组的成员将同时看到公用资源和财务应用程序。

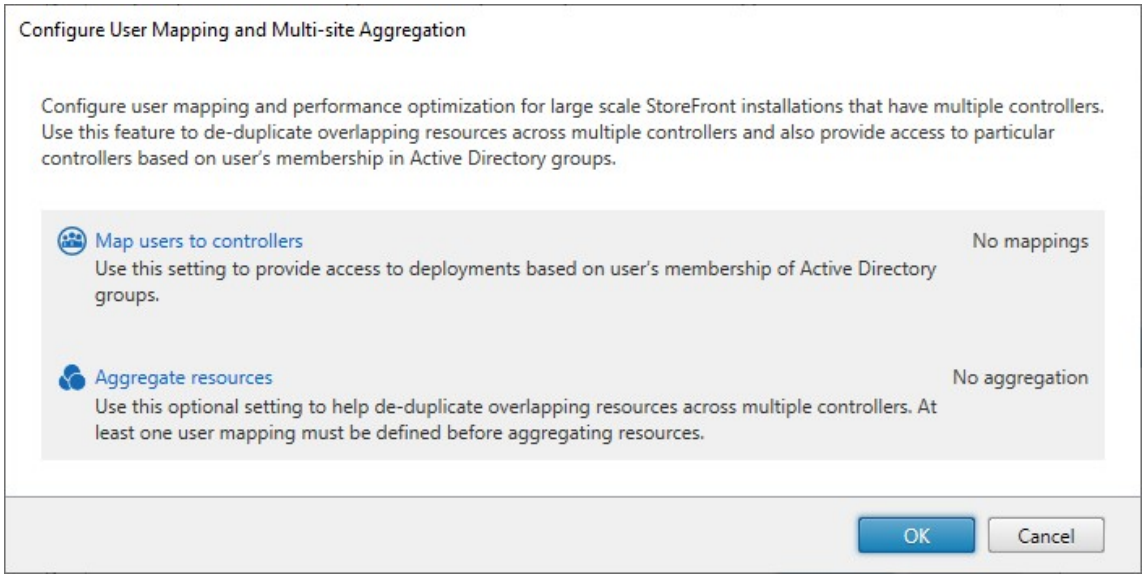
或者，可以为超级用户创建一个提供与其他部署相同资源的部署，但使用速度更快、功能更强大的硬件。这可以为业务关键型用户（如管理团队）提供更好的体验。所有用户在登录到应用商店时都会看到相同的桌面和应用程序，但“管理”用户组的成员将优先连接到由高级用户部署提供的资源。

> 注意：
>
> 这会筛选整个资源源。此外，在资源源中，可以在 Citrix Virtual Apps and Desktops Studio 配置中按用户组筛选应用程序。

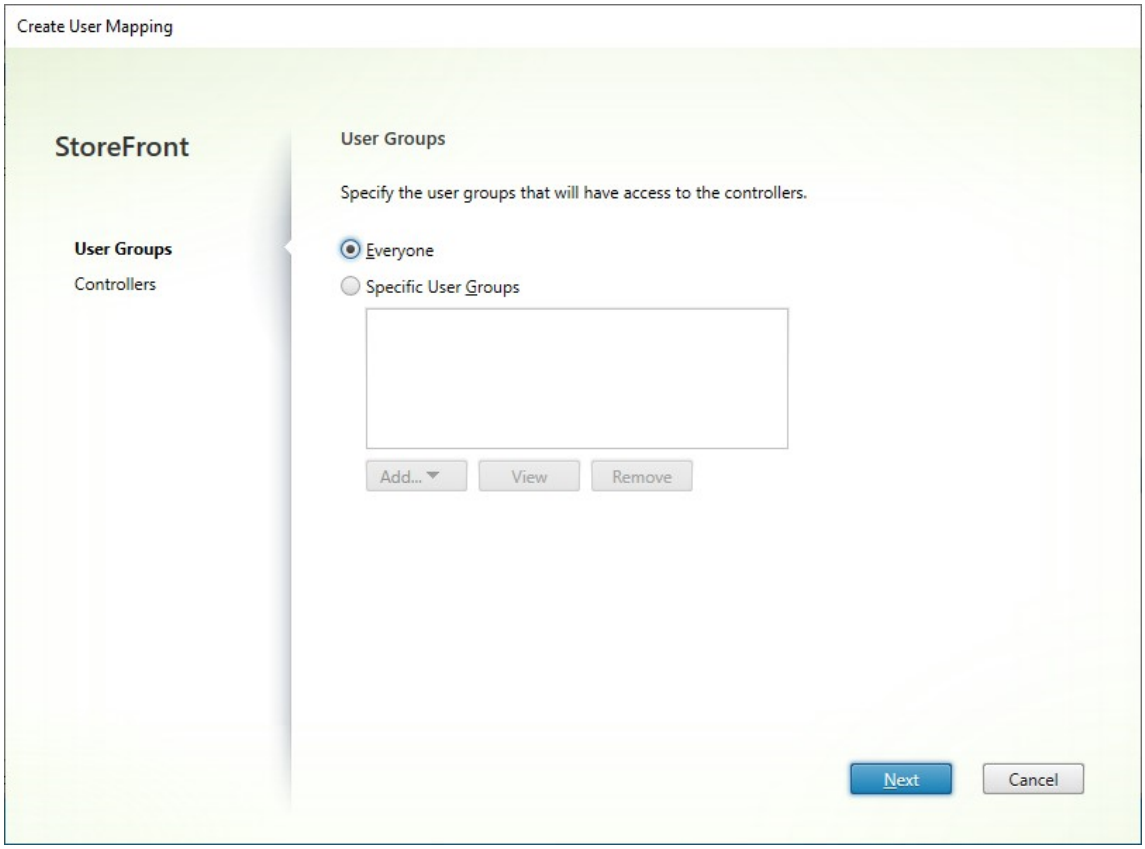
要为特定用户组配置特定的资源源，请执行以下操作：

1. 在管理 **Delivery Controller** 屏幕中，在用户映射和多站点聚合配置下，单击配置。只有在配置了两个或更多资源源时此选项才可用。

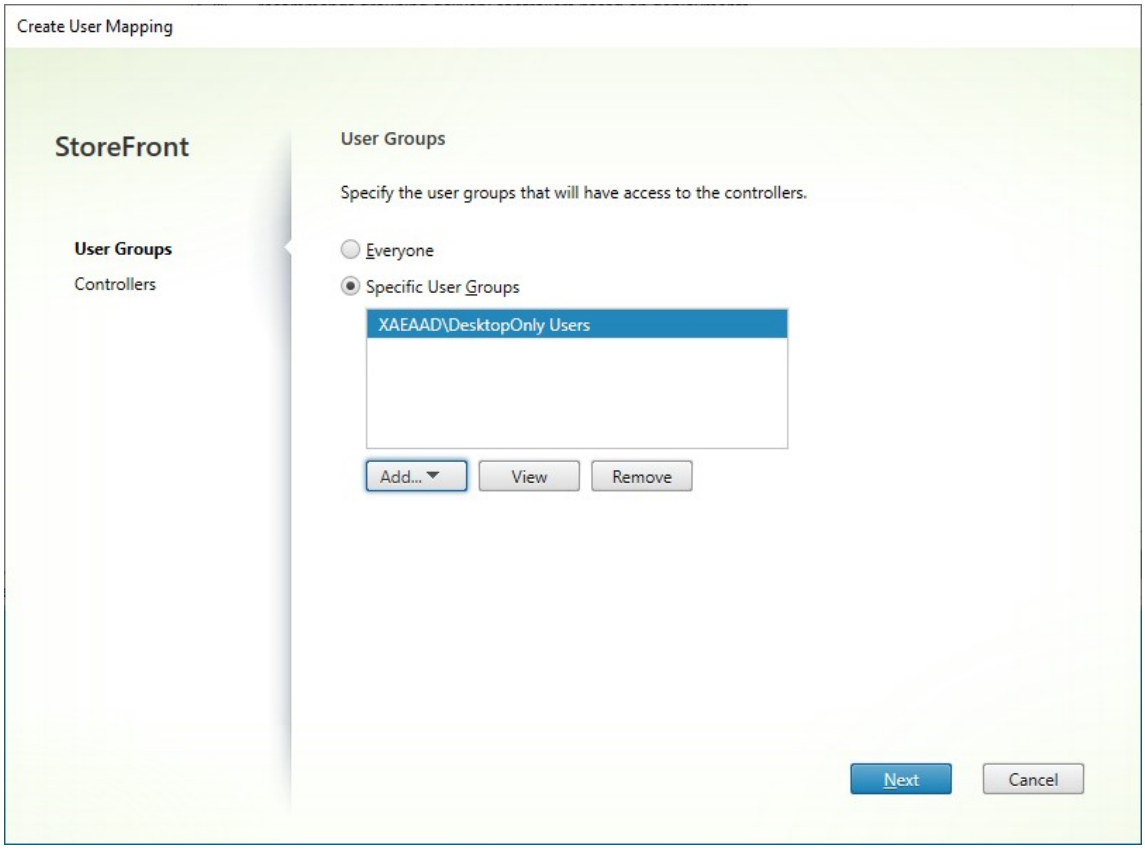
    这将打开配置用户映射和多站点聚合屏幕。



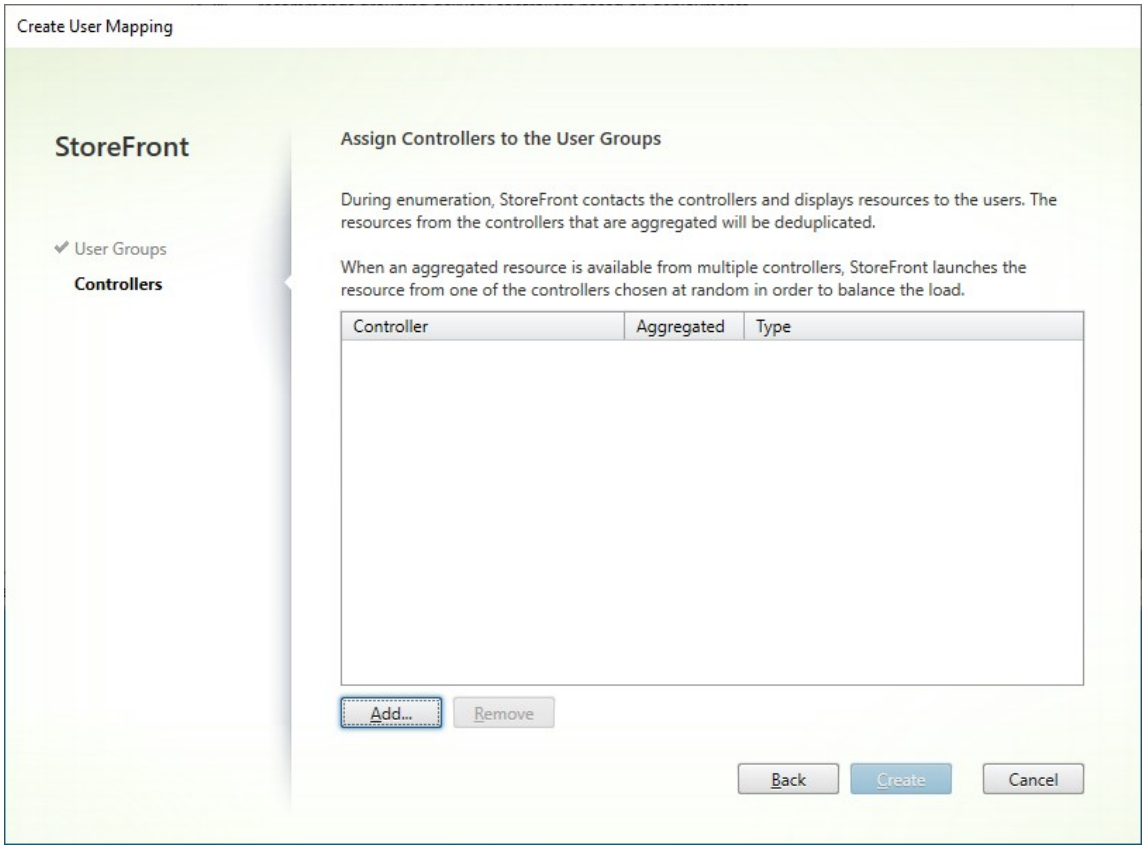
2. 单击 **Map users to controllers**（将用户映射到 Controller）。这将打开创建用户映射屏幕以创建您的第一个映射。稍后您将能够创建更多映射。



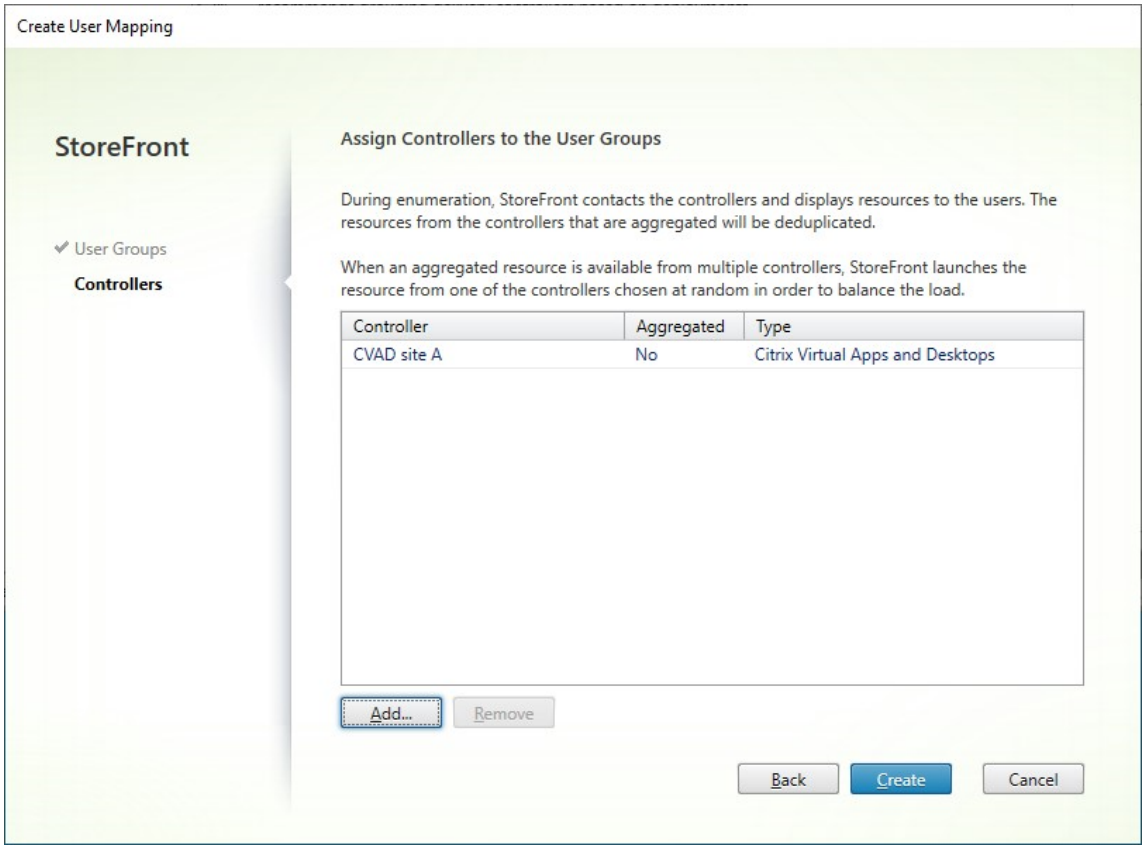
3. 选择所有人，或者选择特定用户组，然后添加一个或多个组。



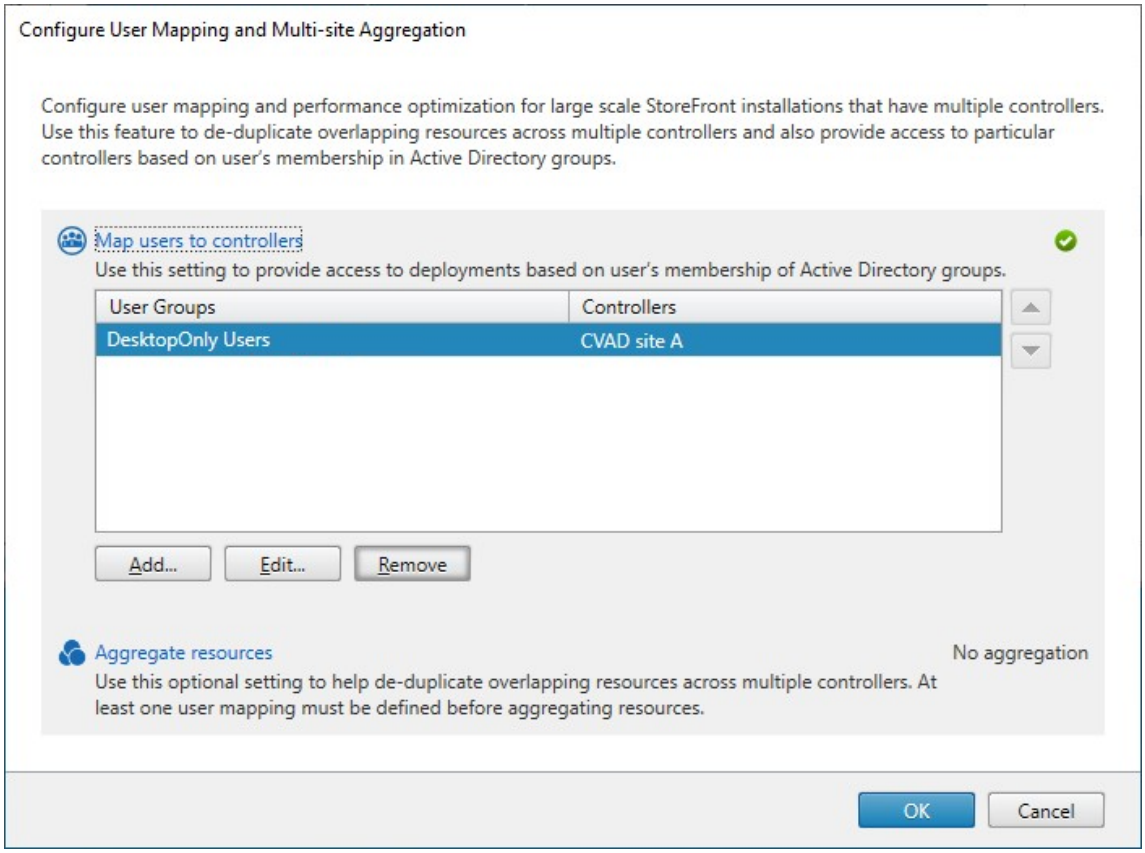
4. 单击下一步。这将带您进入 **Controller** 选项卡。



5. 单击添加，然后再添加一个或多个 Controller。



6. 单击创建。



7. 单击添加…根据需要创建更多映射。

使用 **PowerShell SDK** 将用户映射到资源

可以使用 PowerShell SDK 将用户映射到资源

1. 对于每个资源源，请创建一个 EquivalentFarmset。所有资源源都必须是场集的一部分，否则任何用户都无法使用这些资源源。请调用带以下参数的 New-STFEquivalentFarmset：

   - `Name` - EquivalentFarmSet 的唯一名称
   - `PrimaryFarms` - 非聚合资源源（场）的名称。

2. 对于需要访问资源源的不同集合的每组用户，请在这些用户与每个 EquivalentFarmSet 之间创建映射。要创建 UserFarmMapping，请调用带以下参数的 Add-STFUserFarmMapping：

   - `StoreService` - 要将 UserFarmMapping 添加到的应用商店服务。
   - `Name` - 映射的唯一名称。
   - `GroupMembers` - 包含作为映射的一部分的用户组的名称和 SID 的哈希表。名称仅用于显示；SID 定义组。要添加所有用户，请在哈希表中创建一个包含名称 `Everyone` 和值 `Everyone` 的条目。
   - `EquivalentFarmSet` - 在上一步中创建的 EquivalentFarmSet。

   您必须确保每个资源源（场）都包含在至少一个 UserFarmMapping 中，否则任何用户都将无法访问该资源。

多站点聚合

默认情况下，StoreFront 会枚举所有为应用商店提供桌面和应用程序的部署，并将所有这些资源视为不同资源。这意味着，如果多个部署提供相同资源，那么用户会看到每个资源都对应一个图标，因此当这些资源的名称相同时，这可能会让用户产生困惑。设置高可用的多站点配置时，可以对交付相同桌面或应用程序的 Citrix Virtual Apps and Desktops 部署进行分组，以便为用户聚合相同的资源。分组的部署不必相同，但是资源必须在每台服务器上具有相同名称和路径才能进行聚合。

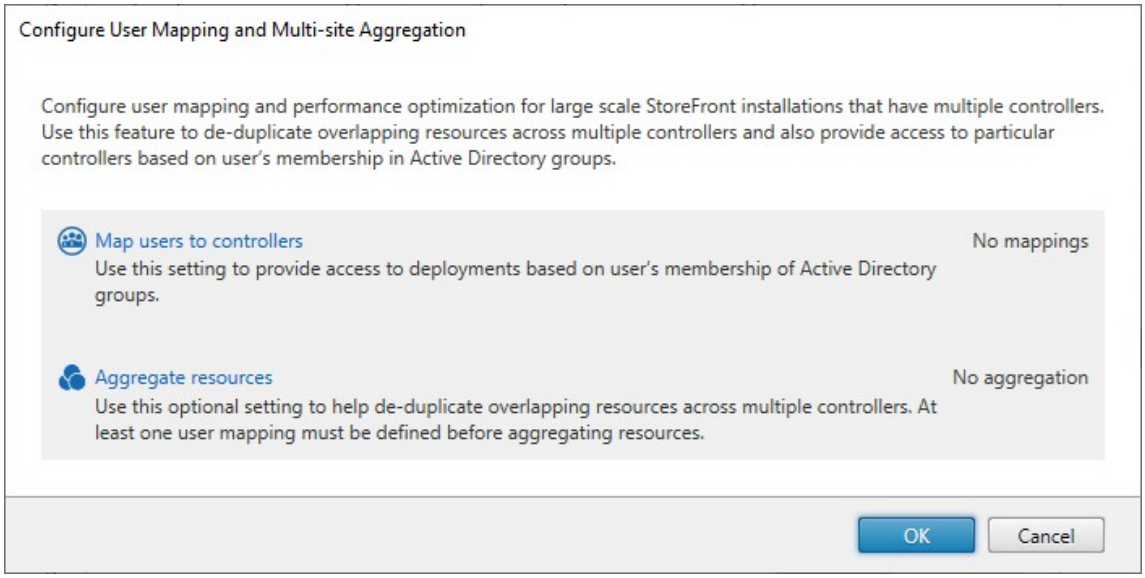
启用多站点聚合后，如果某个桌面或应用程序是为特定应用商店配置的多个 Citrix Virtual Apps and Desktops 部署提供的，StoreFront 会对该资源的所有实例进行聚合，并向用户呈现一个图标。用户启动聚合资源时，StoreFront 会根据服务器可用性、用户是否已具有活动会话以及在配置中指定的排列顺序来确定最适合用户的资源实例。

对于无法响应请求的服务器，StoreFront 会动态监视这些服务器是否过载或暂时不可用。在重新建立通信之前，用户将被定向到其他服务器中的资源实例。如果提供资源的服务器支持，StoreFront 会尝试重用现有会话来交付其他资源。如果用户已经在一个也提供请求资源的部署中具有活动会话，并且会话与该资源兼容，则 StoreFront 会重用该会话。将每个用户的会话数量降到最少不但可以缩短启动其他桌面或应用程序的时间，而且还可以更高效地使用产品许可证。

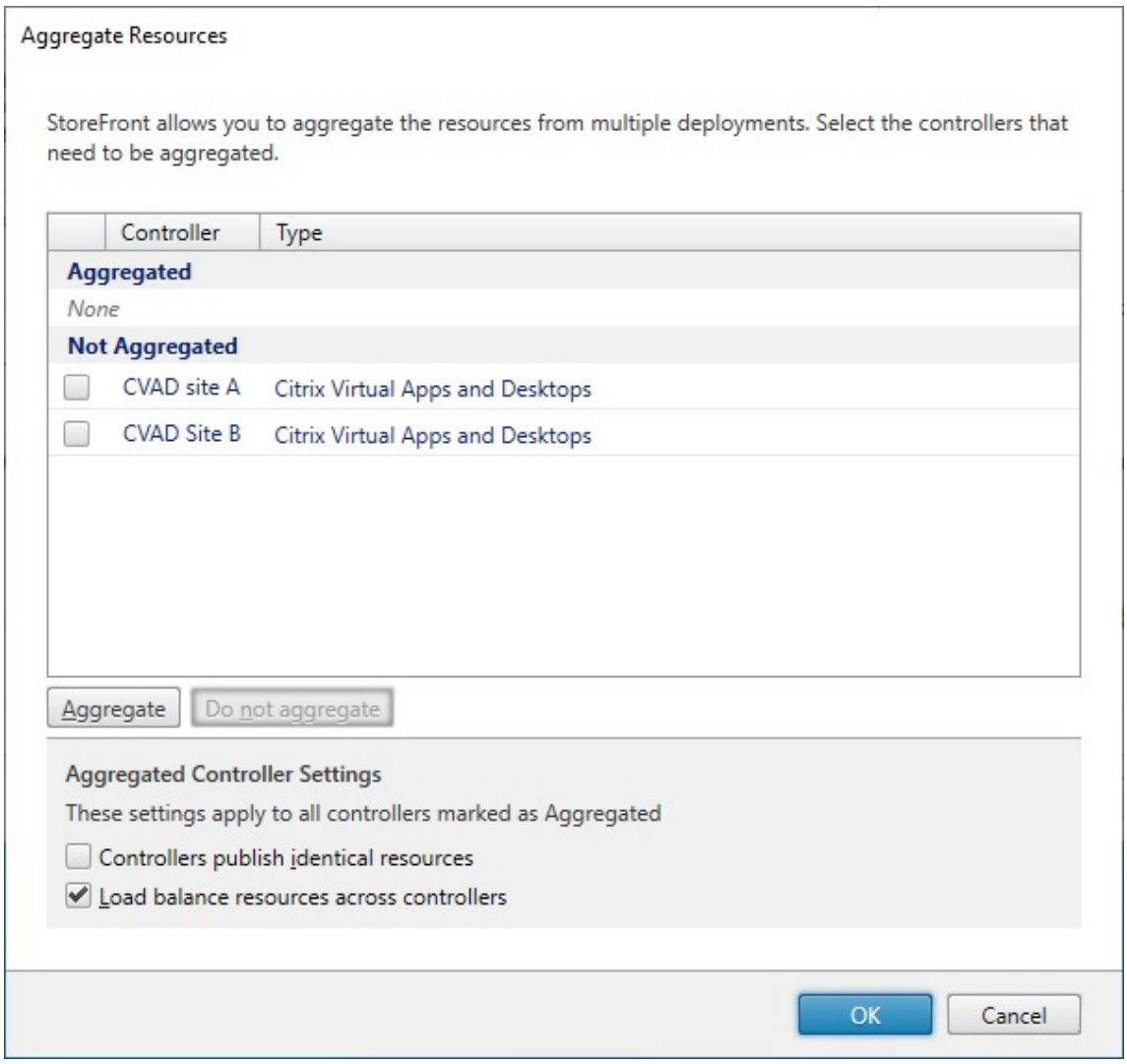
检查完可用性和现有用户会话后，StoreFront 将使用在配置中指定的排列顺序来确定用户要连接到的部署。如果为用户提供了多个等效部署，则可以指定将用户连接到第一个可用部署，或随机连接到列表中的任何部署。将用户连接到第一个可用部署可以最大限度地减少当前用户数所使用的部署数量。随机连接用户可以在所有可用部署中更均匀地分布用户。

可以覆盖单个 Citrix Virtual Apps and Desktops 资源的指定部署排序，以定义用户在访问特定桌面或应用程序时所连接的首选部署。例如，这样可允许您指定用户优先连接到专门为交付特定桌面或应用程序而提供的部署，而对其他资源使用其他部署。为此，可将字符串 `KEYWORDS:Primary` 附加到首选部署中相应桌面或应用程序的说明的末尾，并将 `KEYWORDS:Secondary` 附加到其他部署中相应资源的说明的末尾。无论在配置中指定的部署顺序为何，都将尽可能地将用户连接到提供主要资源的部署。首选部署不可用时，用户将被连接到提供辅助资源的部署。

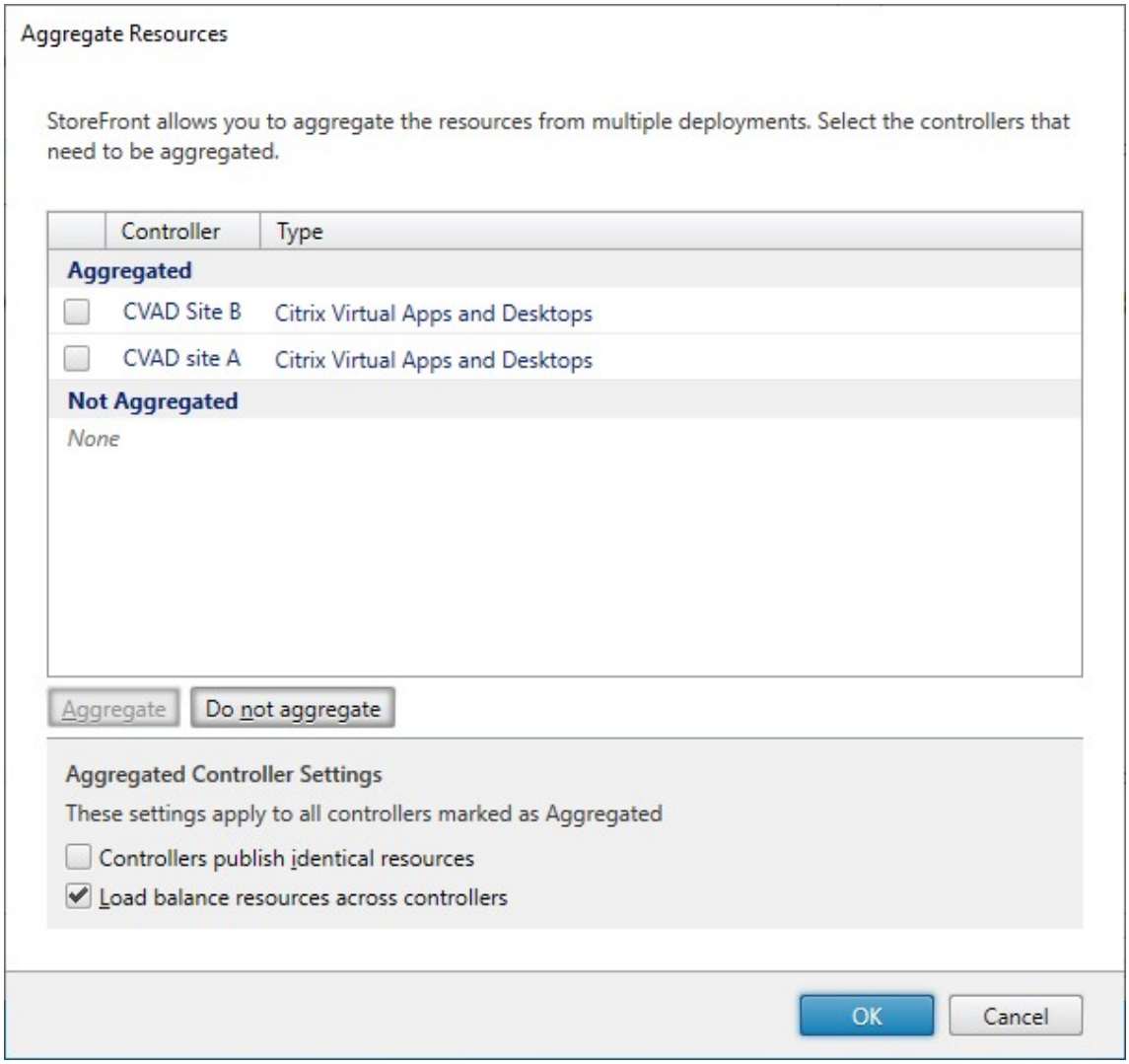
1. 在 管理 **Delivery Controller** 屏幕中，在用户映射和多站点聚合配置下，单击配置。只有在配置了两个或更多资源源时此选项才可用。



2. 单击聚合资源。这将显示聚合资源屏幕。



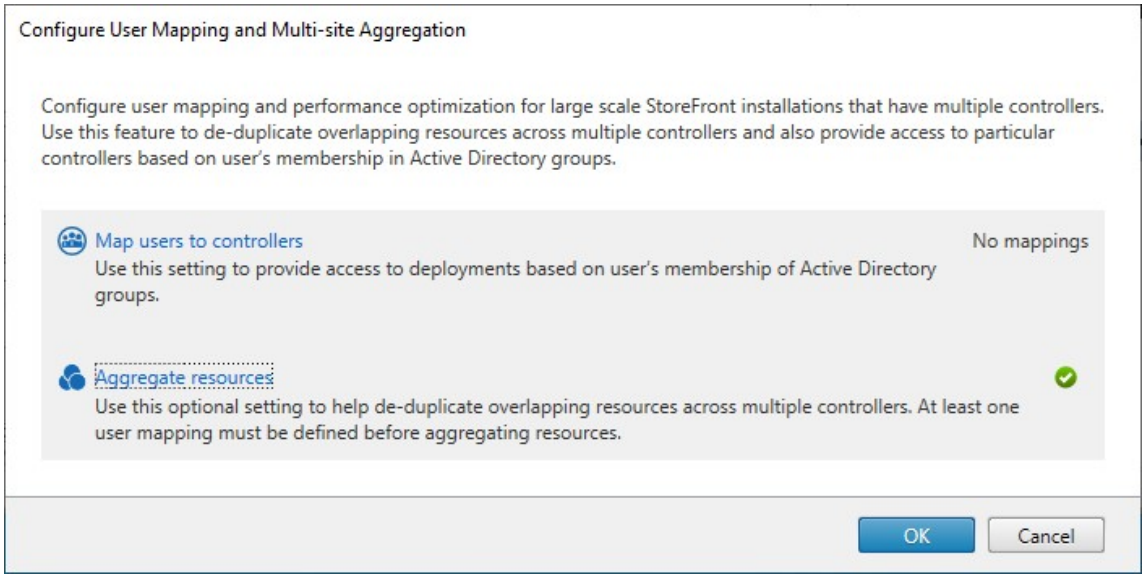
3. 选择具有相同资源的资源源，然后单击聚合。



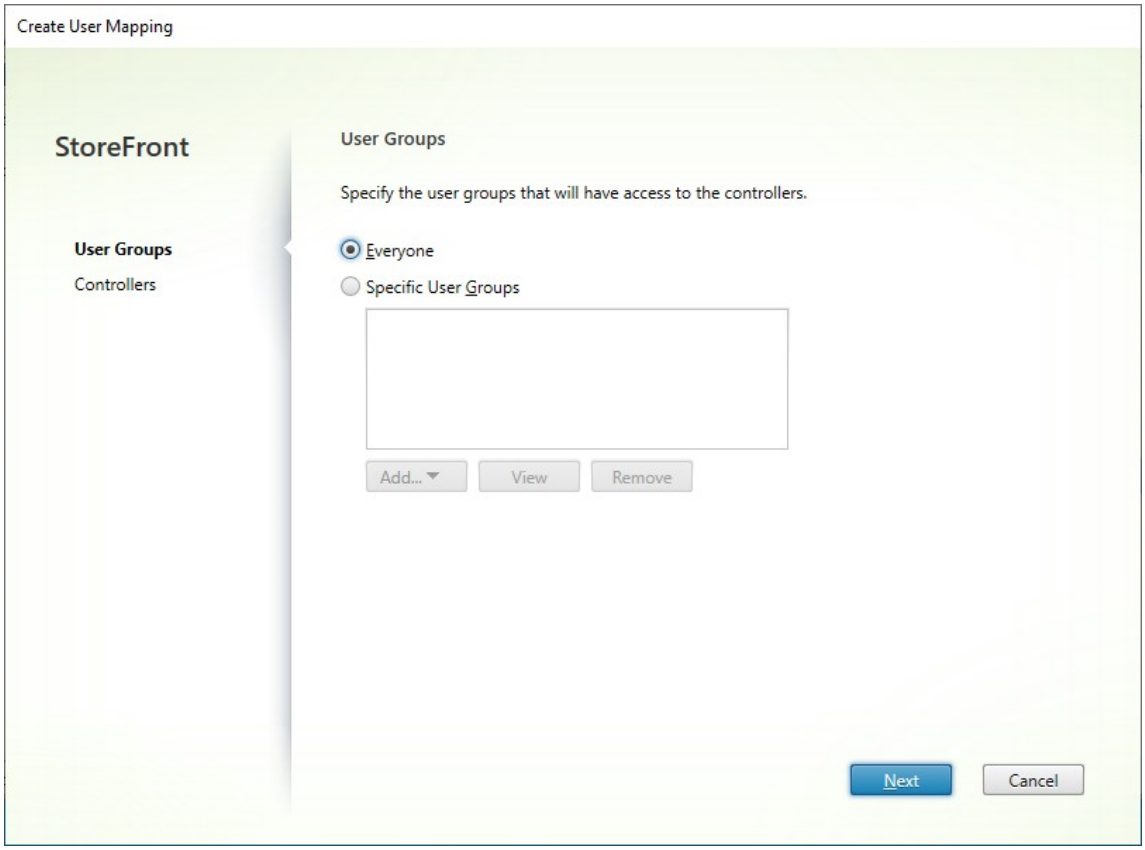
4. 根据需要选择聚合 **Controller** 设置选项：

   - **Controller** 发布相同的资源 - 选中时，StoreFront 将枚举仅来自聚合组中的其中一个 Controller 的资源。如果未选中，StoreFront 将枚举聚合集中的所有 Controller 中的资源（以聚合用户的可用资源的完整集）。选择此选项能够在枚举资源时提高性能，但我们不建议选中，除非您确认所有聚合源中的资源列表都相同。
   - 在 **Controller** 之间对资源进行负载平衡 - 选中时，将在可用 Controller 之间平均分发启动。如果未选中，启动将被定向到在用户映射对话框屏幕中指定的第一个 Controller，如果启动失败，则故障转移到后续 Controller。

5. 单击确定返回到配置用户映射和多站点聚合屏幕。现在已勾选聚合资源。



6. 聚合了资源时，默认情况下，任何用户都无法访问这些资源，因此您必须添加用户映射。单击 **Map users to controllers**（将用户映射到 Controller）。这将打开创建用户映射屏幕。

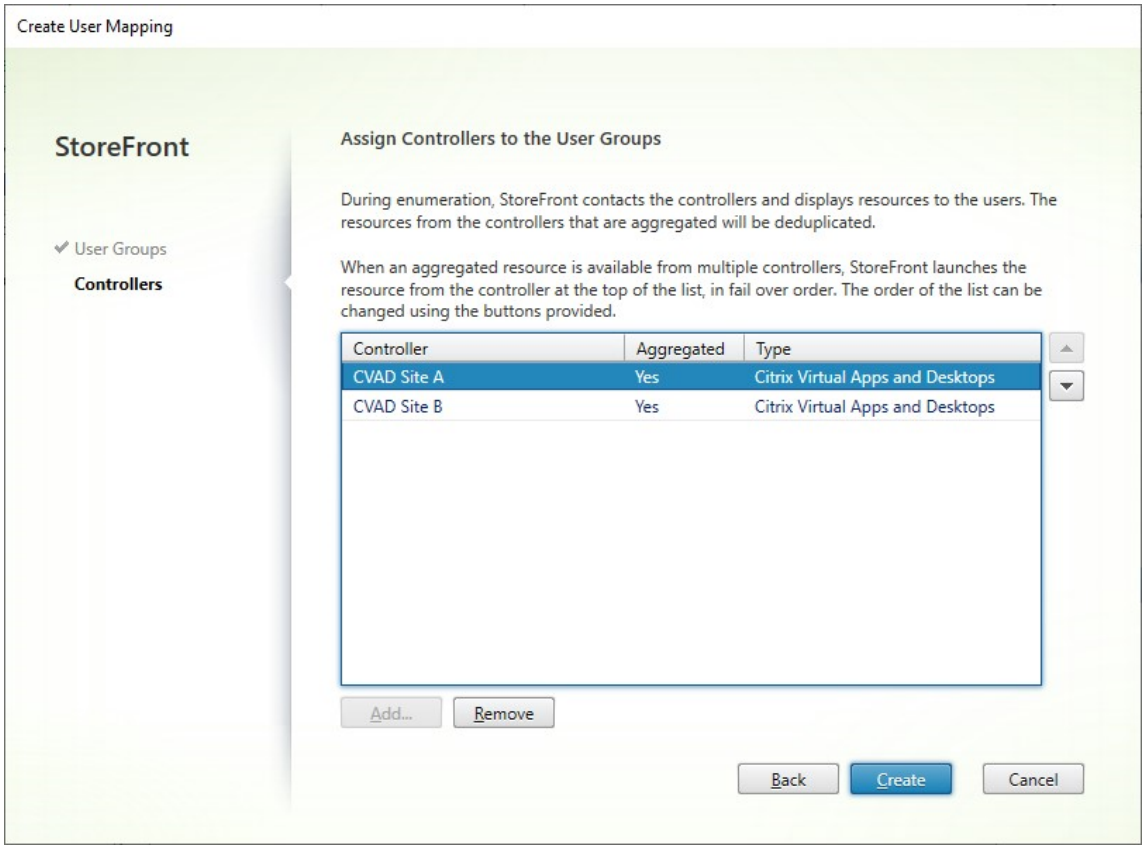


7. 选择所有人，或者选择特定用户组，然后添加一个或多个组。例如，您可能希望选择一个代表特定位置中的用户的组。

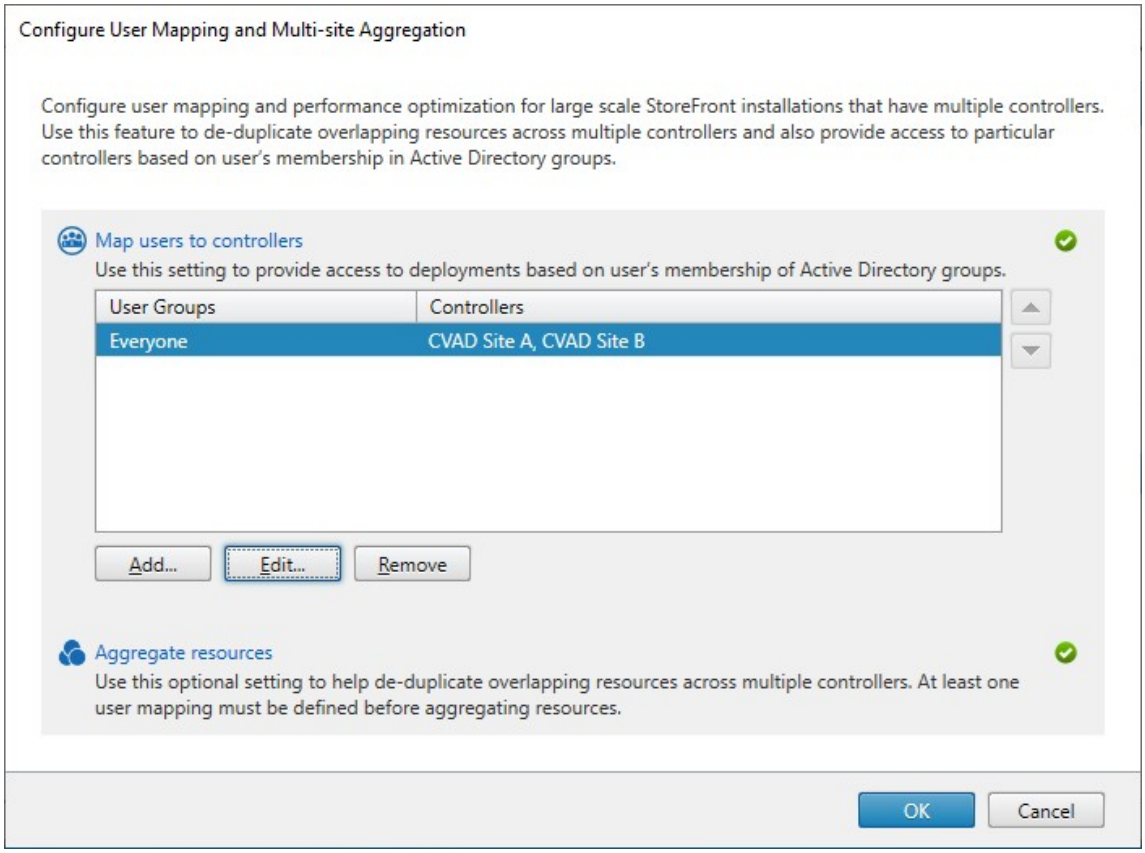
8. 添加聚合的资源源。您必须添加所有聚合的资源源，所有未包含的资源源都将变为“未聚合”。您还可以包括非聚

合资源。

9. 如果您没有勾选在 **Controller** 之间对资源进行负载平衡，则可以选择 StoreFront 应优先启动资源的顺序。



10. 按创建返回到配置用户映射和多站点聚合。



11. 根据需要添加更多映射。请务必将每个资源源映射到一个用户组，否则任何人都无法使用这些资源。
12. 单击确定。

使用 **PowerShell SDK** 进行高级配置

可以使用 StoreFront 管理控制台配置许多常见的多站点和高可用性操作。您还可以使用 PowerShell SDK 来配置 StoreFront，它提供了下列额外的功能：

- 能够为聚合指定多个部署组。
  - 管理控制台仅允许一组部署，这足够适用于大多数情况。
  - 对于包含多个具有几组非连续资源的部署的应用商店，多个编组可能会提高性能。
- 能够为聚合部署指定复杂的首选项顺序。管理控制台允许平衡聚合部署的负载或者将其用作单个故障转移列表。使用 PowerShell，您可以拥有多组源，它们已实现负载平衡，可以在不同的组之间进行故障转移。

> 警告：
>
> 使用 PowerShell 配置高级多站点选项后，无法使用管理控制台修改这些选项。

1. 决定要使用哪个聚合组。在聚合组中，具有相同显示名称的应用程序聚合为一个图标。每个聚合组都需要一个名称。在管理控制台中，您只能创建一个聚合组。通过 PowerShell，您可以定义多个聚合组。

2. 对于每个聚合组，请创建一个或多个 EquivalentFarmset，列出要聚合的资源源（在 SDK 中称为场）。如果将聚合组中的不同资源源分配给不同的用户，则必须为每组用户创建单独的 EquivalentFarmSet，但共享相同的 `AggregationGroupName`。要创建 EquivalentFarmSet，请调用带以下参数的 New-STFEquivalentFarmset：

    - `Name` - EquivalentFarmset 的唯一名称。
    - `AggregationGroupName` - 场集所属的聚合组的名称。
    - `LoadBalanceMode` - `LoadBalanced` 或 `Failover`。
    - `PrimaryFarms` - 您希望聚合的场。如果 `LoadBalanceMode` 为 `Failover`，请务必按要求的顺序列出场。如果聚合组有多个 EquivalentFarmSet，则在评估使用哪个资源源启动资源时，会将此顺序与在 UserFarmMapping 中定义的 IndexNumber 相结合。
    - `BackupFarms` - 在没有主场可用的情况下使用的场列表。此功能已弃用。取而代之的是添加 IndexNumber 较高的其他 EquivalentFarmSet。

3. 对于不属于聚合组的每个资源源，请在不指定 `AggregationGroupName` 的情况下创建 EquivalentFarmset。所有资源源都必须是场集的一部分。请调用带以下参数的 New-STFEquivalentFarmset：

    - `Name` - EquivalentFarmSet 的唯一名称
    - `PrimaryFarms` - 非聚合场的名称。

4. 对于需要访问资源源的不同集合的每组用户，请在这些用户与每个 EquivalentFarmSet 之间创建映射。要创建 UserFarmMapping，请调用带以下参数的 Add-STFUserFarmMapping：

    - `StoreService` - 要将 UserFarmMapping 添加到的应用商店服务。
    - `Name` - 映射的唯一名称。
    - `GroupMembers` - 包含作为映射的一部分的用户组的名称和 SID 的哈希表。名称仅用于显示；SID 定义组。要添加所有用户，请在哈希表中创建一个包含名称 `Everyone` 和值 `Everyone` 的条目。
    - `EquivalentFarmSet` - 在上一步中创建的 EquivalentFarmSet。
    - `IndexNumber` - 设置资源源的评估顺序。这设置了使用哪个资源源启动资源的优先顺序。

    您必须确保每个资源源（场）都包含在至少一个 UserFarmMapping 中，否则任何用户都将无法访问该资源。

管理通过 **Citrix Gateway** 对应用商店的远程访问

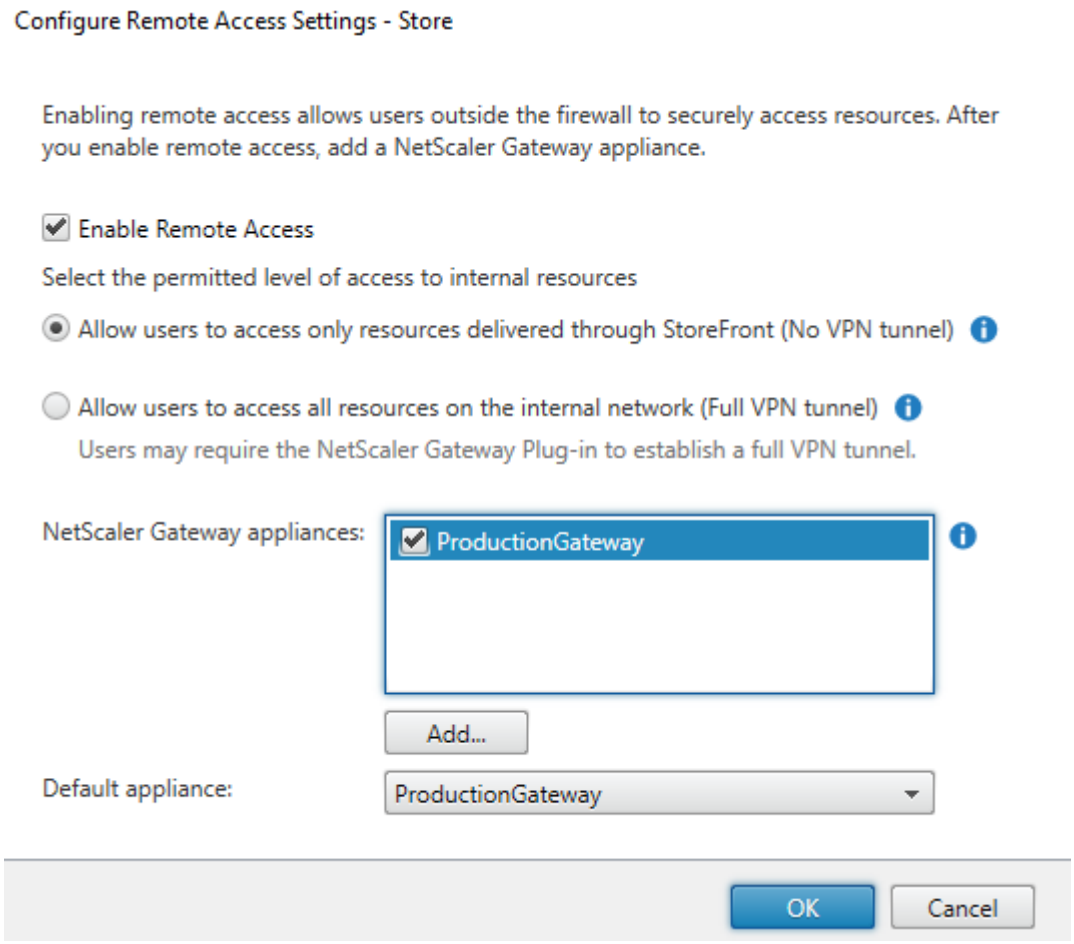
April 17, 2024

可以通过执行“远程访问设置”任务为从公用网络连接的用户配置通过 Citrix Gateway 对应用商店的访问。无法对未经身份验证的应用商店应用通过 Citrix Gateway 进行远程访问。

> 重要提示：
>
> 在多服务器部署中，请一次仅使用一台服务器以更改服务器组的配置。确保 Citrix StoreFront 管理控制台未在

> 部署中的任何其他服务器上运行。完成后，请
> 将对配置所做的更改传播到服务器组，以便更新部署中的其他服务器。

1. 在 Citrix StoreFront 管理控制台的右侧窗格中选择“应用商店”节点，然后在结果窗格中选择一个应用商店。在“操作”窗格中，单击配置远程访问设置。



2. 在“配置远程访问设置”对话框中，指定从公用网络连接的用户是否以及如何能够通过 Citrix Gateway 访问应用商店。

   - 要将应用商店设置为对公共网络中的用户不可用，请务必不选中启用远程访问。这样，只有内部网络的本地用户才能够访问应用商店。
   - 要启用远程访问，请选中启用远程访问。
     - 要使通过该应用商店交付的资源可通过 Citrix Gateway 访问，请选择无 **VPN** 通道。用户使用 ICAProxy 或无客户端 VPN (cVPN) 登录到 Citrix Gateway，不需要使用 Citrix Gateway 插件来建立完整的 VPN。
     - 要通过安全套接字层 (SSL) 虚拟专用网络 (VPN) 通道获得该应用商店以及内部网络中的其他资源，请选择完整 **VPN** 通道。用户需要使用 Citrix Gateway 插件创建 VPN 通道。

   允许对应用商店进行远程访问时，将自动启用从 **Citrix Gateway** 直通身份验证方法。用户向 Citrix

Gateway 验证身份后，即可在访问自己的应用商店时自动登录。

3. 如果已启用远程访问，请从 **Citrix Gateway** 设备列表中选择用户可通过其访问应用商店的部署。先前为该应用商店和其他应用商店配置的所有部署都将显示在列表中，以供选择。如果要向列表中添加更多部署，请单击添加，然后按照添加 Citrix Gateway 中的步骤进行操作。
4. 如果通过在列表中选择多个条目启用通过多个设备进行访问，请指定用于从 Citrix Workspace 应用程序访问该应用商店的默认设备。
5. 单击确定保存配置并关闭“配置远程访问”对话框。

Citrix Workspace 应用程序使用信标点确定用户是连接到本地网络还是公用网络，然后选择相应的访问方法。有关更改信标点的详细信息，请参阅配置信标点。

默认情况下，StoreFront 使用网关，用户通过该网关连接到应用商店来启动资源。要将 StoreFront 配置为使用备用网关或不使用网关启动资源，请参阅最佳 HDX 路由。

证书吊销列表 (CRL) 检查

April 17, 2024

简介

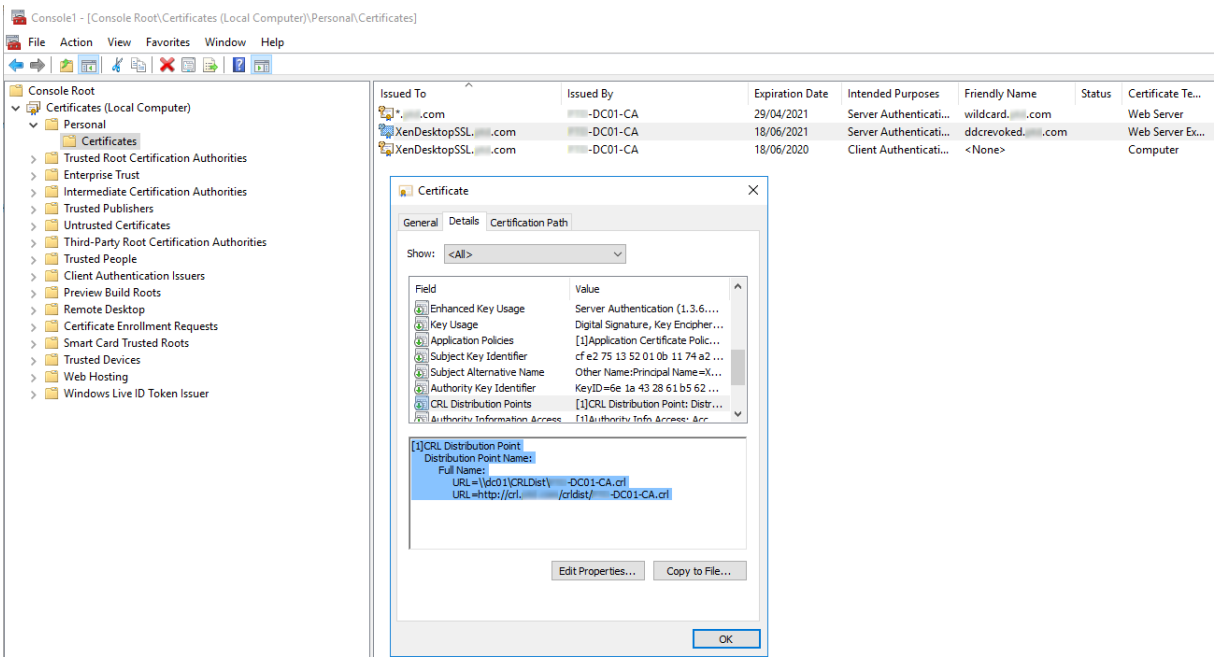
您可以将 StoreFront 配置为使用已发布的证书吊销列表 (CRL) 检查 CVAD Delivery Controller 所使用的 TLS 证书的状态。如果出现以下情况，您可能需要吊销证书访问权限：

- 您认为私钥已被盗用
- CA 被盗用
- 附属关系已更改
- 证书已被取代

> 注意：
>
> 仅当使用 StoreFront 与 Citrix Virtual Apps and Desktops Delivery Controller 之间的 HTTPS 连接时，本主题才相关。与 Delivery Controller 的 HTTP 连接不需要证书，因此此处所述的应用商店的 -CertRevocationPolicy 设置不起作用。
>
> StoreFront 支持使用 CRL 分发点 (CDP) 证书
> 扩展和本地安装的证书吊销列表 (CRL) 进行
> 证书吊销检查。StoreFront 仅支持完全 CRL：不支持增量 CLR。

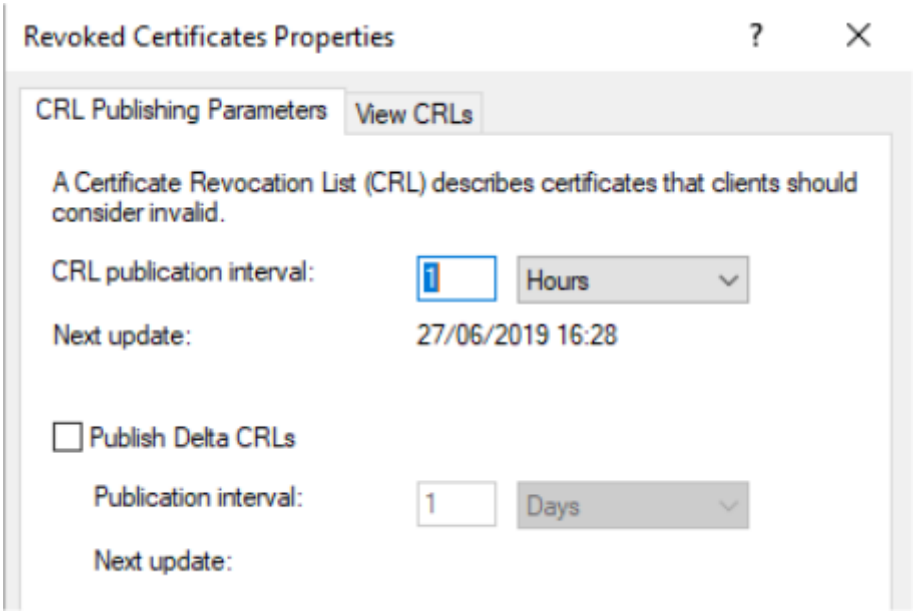
CRL 分发点 (CDP) 扩展

StoreFront 不会枚举 Citrix Virtual Apps and Desktops Delivery Controller 中使用已吊销证书（其序列号在已发布的 CRL 中列出）的资源。要检测哪些证书已被吊销，StoreFront 必须能够使用在 CDP 证书扩展中定义的 URL 之一来访问已发布的 CRL。



CRL 发布间隔

要使 StoreFront 在 Delivery Controller 上更快速地检测已吊销的证书，请缩短 CA 的 CRL 发布间隔。编辑 CLR 分发点扩展程序的属性，以设置适合公钥基础结构的较低 CLR 发布间隔值。



客户端 **CRL** 缓存

Windows 公钥基础结构客户端在本地缓存 CRL。在本地缓存的 CRL 过期之前，不会下载更新的 CRL。

StoreFront 对证书吊销列表 **(CRL)** 的访问权限

证书吊销检查取决于 StoreFront 能不能访问 CRL。请仔细考虑 StoreFront 如何联系 Web 服务器或发布 CRL 的证书颁发机构 (CA)，以及 StoreFront 如何接收 CRL 更新。

Delivery Controller 上的内部企业 **CA** 和专用证书　要使用专有 CA 和证书，StoreFront 需要正确配置的企业 CA 和已发布的 CRL，它可以在组织和内部网络中访问这些 CA 和 CRL。有关配置企业 CA 以发布 CDP 扩展程序的信息，请参考 Microsoft 文档。可能需要重新颁发 Delivery Controller 上的所有证书，这些证书在 CA 配置为包含 CDP 扩展程序之前就已经存在。

StoreFront 和 Citrix Virtual Apps and Desktops 服务器通常位于无法访问 Internet 的独立专用网络中。在这种情况下，应使用专用 CA。

Delivery Controller 上的外部公共 **CA** 和公用证书　StoreFront 服务器和 Citrix Virtual Apps and Desktops Delivery Controller 可以使用公用 CA 颁发的证书。StoreFront 必须能够使用 CDP 扩展程序中引用的 URL 通过 Internet 联系公用 CA 的 Web 服务器。如果在吊销公用证书后，StoreFront 无法使用 CDP URL 下载 CRL 副本，则 StoreFront 无法执行 CRL 检查。

证书吊销策略设置

使用 Citrix StoreFront PowerShell cmdlet **Get-STFStoreFarmConfiguration** 和 **Set-STFStoreFarmConfiguration** 为应用商店设置证书吊销策略。运行 **Get-Help Set-STFStoreFarmConfiguration -detailed** 将显示 PowerShell 帮助和包含 -CertRevocationPolicy 选项的示例。有关这些 StoreFront PowerShell cmdlet 的详细信息信息，请参阅 Citrix StoreFront SDK PowerShell 模块。

-CertRevocationPolicy 选项可以设置为以下值：

设置	说明
NoCheck	StoreFront 不会在 Delivery Controller 上检查证书的吊销状态。StoreFront 仍会枚举使用已吊销证书的 Delivery Controller 中的资源。此为默认设置。

设置	说明
MustCheck	这是最安全的选项。StoreFront 将尝试通过联系在 Delivery Controller 上的证书的 CDP 扩展中引用的 URL 来获取 CRL。如果 CRL 不可用或 Delivery Controller 上正在使用的证书已被吊销，StoreFront 将无法从 Delivery Controller 执行枚举操作。该 URL 可以指向内部 Web 服务器（如果证书是专用的），也可以指向公用 Internet Web 服务器（如果证书由公用 CA 颁发）。
FullCheck	StoreFront 将尝试联系 Delivery Controller 证书的 CDP 扩展中发布的 URL。如果 StoreFront 无法从这些 URL 获取 CRL 副本，则它仍然允许枚举 Delivery Controller 中的资源。如果 StoreFront 成功获取 CRL，并且 Delivery Controller 的证书已被吊销，则 StoreFront 不会枚举资源。该 URL 可以指向内部 Web 服务器（如果证书是专用的），也可以指向公用 Internet Web 服务器（如果证书由公用 CA 颁发）。
NoNetworkAccess	仅检查在本地导入到 StoreFront 服务器上的 Citrix Delivery Services 证书存储中的 CRL。StoreFront 不会尝试联系在 CDP 扩展中指定的任何 URL。如果 StoreFront 无法获取 CRL 的本地副本，则它仍然允许枚举 Delivery Controller 中的资源。如果 StoreFront 成功从 Citrix Delivery Services 证书存储中获取 CRL 的本地副本，并且 Delivery Controller 的证书已被吊销，则 StoreFront 不会枚举资源。

为证书吊销检查配置存储

要为应用商店设置证书吊销策略，请使用以管理员身份运行打开 PowerShell ISE，然后运行以下 PowerShell cmdlet。如果您有多个应用商店，请对所有应用商店重复此过程。-CertRevocationPolicy 是应用商店级别的设置，它会影响为 $StoreVirtualPath 中指定的应用商店配置的所有 Delivery Controller。

```
$SiteID = 1
$StoreVirtualPath = "/Citrix/Store"
$StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
$StoreVirtualPath
Set-STFStoreFarmConfiguration -StoreService $StoreObject -
    CertRevocationPolicy "MustCheck"
<!--NeedCopy-->
```

要检查是否已正确应用该设置，或查看当前的

-CertRevocationPolicy 配置，请运行以下命令：

```
(Get-STFStoreFarmConfiguration -StoreService $StoreObject).
   CertRevocationPolicy
<!--NeedCopy-->
```

在 **StoreFront** 服务器上使用本地导入的 **CRL**

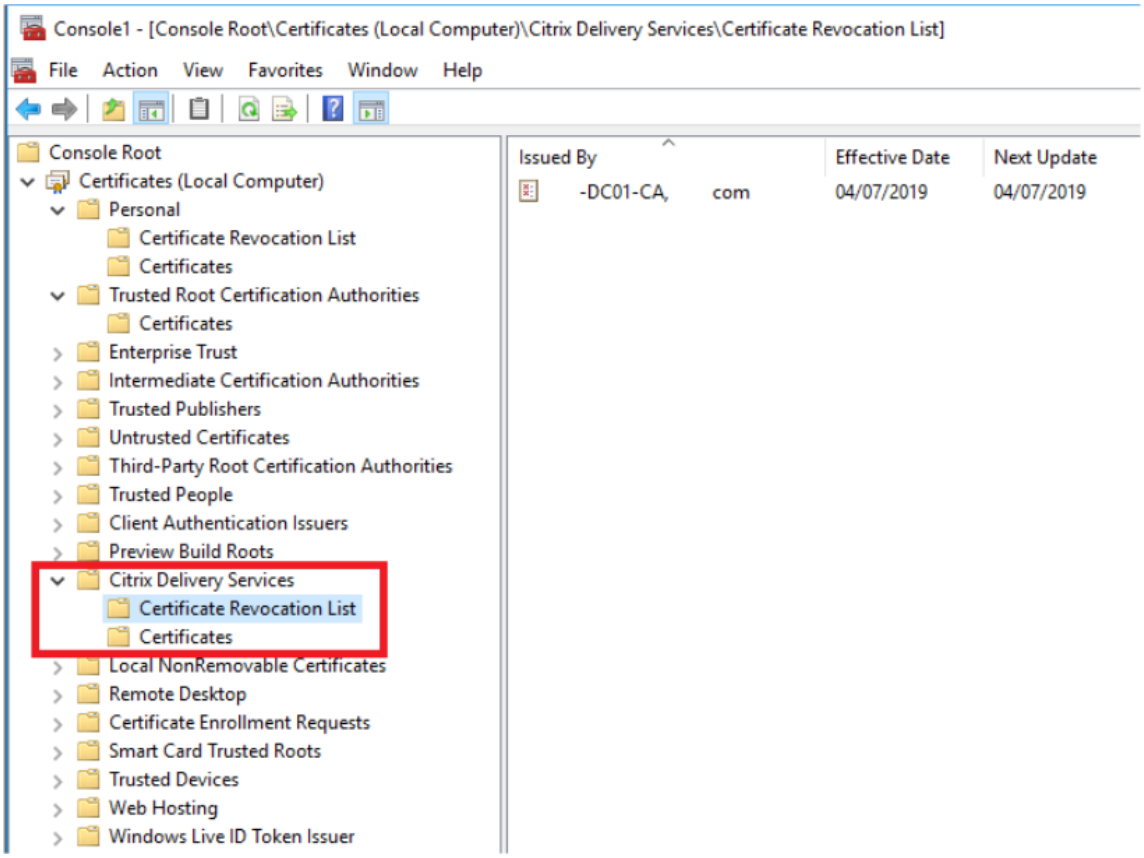
支持使用本地导入的 CRL，但 Citrix 不建议这样做，
因为：

- 它们很难在大型企业部署（可能涉及多个 StoreFront 服务器组）中进行管理和更新。
- 与在整个 Active Directory 域上使用 CDP 扩展程序和发布的 CRL 相比，每次吊销证书时在每个 StoreFront 服务器上手动更新 CRL 更低效。

如果 -CertRevocationPolicy 设置为“NoNetworkAccess”，并且您有办法将 CRL 高效地分发给所有 StoreFront 服务器，则可以使用本地安装的或更新后的 CRL。

使用本地导入的 **CLR**

1. 将 CRL 复制到 StoreFront 服务器的桌面。如果 StoreFront 服务器是某个服务器组的一部分，请将其复制到该组中的所有 StoreFront 服务器中。
2. 打开 MMC 管理单元，然后选择文件 **>** 添加/删除管理单元 **>** 证书 **>** 计算机帐户 **> Citrix Delivery Services** 证书存储。
3. 右键单击并选择所有任务 **>** 导入，然后浏览到.CRL 文件并选择选择所有文件 **>** 打开 **>** 将所有的证书都放入下列存储 **> Citrix Delivery Services** 中。



通过 **PowerShell** 或命令行将 **CRL** 添加到 **Citrix Delivery Services** 证书存储中

1. 登录到 StoreFront 并将.CRL 文件复制到当前
   用户的桌面。
2. 打开 PowerShell ISE 并选择以管理员身份运行。
3. 运行以下命令：

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

如果成功，则返回以下内容：

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

您可以使用此命令作为示例，通过脚本将 CRL 自动分发到
部署中的所有 StoreFront 服务器。

使用 **Delivery Controller** 进行 **XML** 身份验证

您可以配置 StoreFront 以委派 Citrix Virtual Apps and Desktops Delivery Controller 对用户进行身份验证。如果 Delivery Controller 上的证书已被吊销，用户将无法登录到 StoreFront。这种行为是正常的，因为如果 Citrix Virtual Apps and Desktops Delivery Controller（负责对 Active Directory 用户进行身份验证）上的证书已被吊销，Active Directory 用户应该无法登录到 StoreFront。

委托 **Delivery Controller** 对用户进行身份验证

1. 按照上一部分为证书吊销检查配置存储中所述，为存储配置证书吊销。
2. 按照基于 XML Service 的身份验证中所述的过程，将 Delivery Controller 配置为使用 HTTPS。

为证书吊销检查配置 **XML** 身份验证服务

仅当您在部署中使用 XML 身份验证时，才需要执行这些步骤。

> 注意：
>
> StoreFront 支持两种用于将应用商店映射到身份验证服务的模型。推荐的方法是在应用商店与身份验证服务之间进行一对一映射。在这种情况下，您必须对所有应用商店及其各自的身份验证服务执行此部分中的步骤。
>
> 请务必将证书吊销模式设置为与应用商店和身份验证服务所用模式相同的值。或者，如果所有应用商店的身份验证配置都相同，则可以将多个应用商店配置为共享同一个身份验证服务。

身份验证服务 PowerShell cmdlet 没有与 **Set-STFStoreFarmConfiguration** 等效的命令，因此需要使用稍微不同的 PowerShell 方法。使用之前的部分中介绍的相同证书吊销策略设置。

1. 打开 PowerShell ISE 并选择以管理员身份运行。

```
$SiteID = 1
$StoreVirtualPath = "/Citrix/Store"
$AuthVirtualPath = "/Citrix/StoreAuth"
<!--NeedCopy-->
```

2. 选择要用于 XML 身份验证的应用商店服务、身份验证服务和 Delivery Controller。确保已为应用商店配置 Delivery Controller。

```
$StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
    $StoreVirtualPath
$FarmObject = Get-STFStoreFarm -StoreService $StoreObject -
    FarmName "CVAD"
$AuthObject = Get-STFAuthenticationService -SiteID $SiteID -
    VirtualPath $AuthVirtualPath
<!--NeedCopy-->
```


3. 直接修改身份验证服务的 CertRevocationPolicy
   属性。

```
$AuthObject.FarmsConfiguration.CertRevocationPolicy = "FullCheck"
$AuthObject.Save()
Enable-STFXmlServiceAuthentication -AuthenticationService
    $AuthObject -Farm $FarmObject
<!--NeedCopy-->
```

4. 确认您设置的证书吊销模式正确无误。

```
$AuthObject = Get-STFAuthenticationService -SiteID 1 -VirtualPath
    $AuthVirtualPath
$AuthObject.FarmsConfiguration.CertRevocationPolicy
<!--NeedCopy-->
```

预期的 **Windows** 事件查看器错误

启用 CRL 检查时，StoreFront 服务器上的 Windows 事件查看器中会报告错误。

要打开事件查看器，请执行以下操作：

- 在 StoreFront 服务器上，键入运行。
- 键入 **eventvwr**，然后按 Enter 键。
- 在应用程序和服务中，查找 Citrix Delivery Services 事件。

示例错误：存储无法使用已吊销的证书联系 **Delivery Controller**

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

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

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

示例错误：如果用户因 **XML** 身份验证失败而无法登录，则从 **Receiver for Web** 中删除

```
An unexpected response was received during the authentication process.

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



```
6
7  General Authentication Failure
8
9  ExplicitResult.State: 5
10
11 AuthenticationControllerRequestUrl:
12 https://storefront.example.com/Citrix/StoreWeb/ExplicitAuth/
       LoginAttempt
13
14 ActionType: LoginAttempt
15
16 at
17 Citrix.Web.AuthControllers.Controllers.ExplicitAuthController.
       GetExplicitAuthResult(ActionType
18 type, Dictionary`2 postParams)
19 <!--NeedCopy-->
```

将两个 **StoreFront** 应用商店配置为共享公用订阅数据存储

February 22, 2024

StoreFront 安装过程会在每台 StoreFront 服务器上本地安装 Windows 数据存储，以维护其订阅数据。在 StoreFront 服务器组环境中，每台服务器还维护其应用商店所使用的订阅数据的副本。此数据传播到其他服务器以维护整个组上的用户订阅。默认情况下，StoreFront 为每个应用商店都创建一个数据存储。每个订阅数据存储均独立于每个其他应用商店进行更新。

需要不同的配置设置时，管理员通常使用两个不同的应用商店配置 StoreFront，一个用于通过 Citrix Gateway 在外部访问资源，另一个则用于通过企业 LAN 在内部访问资源。只需更改应用商店 web.config 文件，即可将“外部”和“内部”应用商店配置为共享公用订阅数据存储。

在涉及两个应用商店及其对应订阅数据存储的默认情况下，用户必须订阅同一资源两次。用户从企业网络内部和外部访问同一资源时，将两个应用商店配置为共享公用订阅数据库可改善和简化漫游体验。有了共享的订阅数据存储，用户最初订阅新资源时使用的是“外部”还是“内部”应用商店将无关紧要。

- 每个应用商店都有一个 web.config 文件，该文件位于 C:\inetpub\wwwroot\citrix<storename> 中。
- 每个应用商店 web.config 都包含订阅应用商店服务的客户端端点。

```
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1
__Citrix_<StoreName>"authenticationMode="windows"transferMode="
Streamed">
```

每个应用商店的订阅数据位于以下位置：

```
C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\
SubscriptionsStore\1__Citrix_<StoreName>
```


要使两个应用商店共享订阅数据存储，只需将一个应用商店指向另一应用商店的订阅服务端点。如果是服务器组部署，所有服务器都将具有相同的已定义应用商店对和其所共享的共享数据存储的相同副本。

> 注意：
>
> 每个应用商店上配置的 Citrix Virtual Apps and Desktops 控制器必须完全匹配；否则，可能会出现两个应用商店上的资源订阅集合不一致的情况。仅当两个应用商店位于同一 StoreFront 服务器或服务器组部署上时，才支持数据存储共享。

StoreFront 订阅数据存储端点

1. 在单个 StoreFront 部署上，使用记事本打开外部应用商店 web.config 文件并搜索 clientEndpoint。例如：

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

2. 更改外部应用商店端点以与内部应用商店端点保持一致：

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

3. 如果使用 StoreFront 服务器组，请将对主节点的 web.config 文件所做的所有更改传播到所有其他节点。

两个应用商店现已设置为共享内部应用商店订阅数据存储。

管理应用商店的收藏夹

February 22, 2024

可以使用 PowerShell cmdlet 管理旖旎公用商店的订阅数据（收藏夹）。

> 注意：
>
> 使用 StoreFront 管理控制台或 PowerShell 可管理 StoreFront。请勿同时使用这两种方法。使用 PowerShell 更改 StoreFront 配置之前，请始终关闭 StoreFront 管理控制台。Citrix 还建议您在进行更改之前备份现有订

> 阅数据，以便能够回滚到前一个状态。

清除订阅数据

您的部署中的每个应用商店都存在一个包含订阅数据的文件夹和数据存储。

1. 在 StoreFront 服务器上停止 Citrix Subscriptions Store 服务。如果 Citrix Subscriptions Store 服务正在运行，则无法删除任何应用商店的订阅数据。
2. 找到 StoreFront 服务器上的订阅应用商店文件夹：`C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>`
3. 删除订阅应用商店文件夹的内容，但不删除文件夹本身。
4. 在 StoreFront 服务器上重新启动 Citrix Subscriptions Store 服务。

在 StoreFront 3.5 或更高版本中，可以使用以下 PowerShell 脚本清除应用商店的订阅数据。以具有停止或启动服务以及删除文件权限的管理员身份运行此 PowerShell 函数。此 PowerShell 函数可实现与手动执行上述步骤相同的结果。

Citrix Subscriptions Store 服务必须正在服务器上运行，才能成功运行 cmdlet。

```
function Remove-SubscriptionData
{

    [CmdletBinding()]

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

    $SubsService = "Citrix Subscriptions Store"

    # Path to Subscription Data in StoreFront version 2.6 or later

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

    Stop-Service -displayname $SubsService

    Remove-Item $SubsPath -Force -Verbose

    Start-Service -displayname $SubsService

    Get-Service -displayname $SubsService
 }


Remove-SubscriptionData -Store "YourStore"
<!--NeedCopy-->
```


导出订阅数据

可以使用以下 PowerShell cmdlet 获取制表符分隔的.txt 文件格式的应用商店订阅数据的备份。

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

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

如果要管理多服务器部署，可以在 StoreFront 服务器组内的任意服务器上运行此 PowerShell cmdlet。服务器组中的每台服务器都会维持与其对等服务器相同的订阅数据的同步副本。如果您认为自己遇到 StoreFront 服务器之间的订阅同步问题，请从组中的所有服务器中导出数据并进行比较以查看差异。

还原订阅数据

使用 Restore-STFStoreSubscriptions 可覆盖您的现有订阅数据。可以使用之前通过 Export-STFStoreSubscriptions 创建的制表符分隔的.txt 文件备份还原应用商店的订阅数据。

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

有关 Restore-STFStoreSubscriptions 的详细信息，请参阅 https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/2203/Restore-STFStoreSubscriptions/

还原单个 **StoreFront** 服务器上的数据

在单服务器部署中，不需要关闭 Subscriptions Store 服务。也不需要在还原订阅数据之前清除现有订阅数据。

还原 **StoreFront** 服务器组中的数据

要将订阅数据还原到服务器组，需要执行以下操作。

包含三台 StoreFront 服务器的示例服务器组部署。

- StoreFrontA
- StoreFrontB
- StoreFrontC

1. 备份三台服务器中的任意服务器的现有订阅数据。
2. 停止服务器 StoreFrontB 和 C 上的 Subscriptions Store 服务。此操作将阻止服务器在 StoreFrontA 更新期间发送或接收订阅数据。

3. 清理服务器 StoreFrontB 和 C 中的订阅数据。这可以防止还原的订阅数据出现不一致的情况。
4. 使用 **Restore-STFStoreSubscriptions cmdlet** 还原 StoreFrontA 上的数据。不需要停止 Subscriptions Store 服务，也不需要清理 StoreFrontA 上的订阅数据（这些数据在还原操作期间被覆盖）。
5. 重新启动服务器 StoreFrontB 和 StoreFrontC 上的 Subscriptions Store 服务。这些服务器之后可以从 StoreFrontA 接收数据的副本。
6. 等待所有服务器之间发生同步。所需的时间取决于 StoreFrontA 上存在的记录数量。如果所有服务器都位于本地网络连接中，同步通常会快速发生。跨广域网连接的订阅同步可能需要较长时间。
7. 从 StoreFrontB 和 C 中导出数据以确认同步已完成，或者查看应用商店订阅计数器。

导入订阅数据

如果应用商店中没有订阅数据，请使用 **Import-STFStoreSubscriptions**。此 cmdlet 还允许您将订阅数据从一个应用商店传输到另一个应用商店，或者将订阅数据导入到新预配的 StoreFront 服务器。

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

有关 Import-STFStoreSubscriptions 的详细信息，请参阅 https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/2203/Import-STFStoreSubscriptions/

订阅数据文件详细信息

订阅数据文件为文本文件，每个用户订阅在其中占一行。每行均为以制表符分隔的值序列：

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

其中：

- `<user-identifier>` - 必选。标识用户的字符序列。此标识符是用户的 Windows 安全标识符。
- `<resource-id>` - 必选。标识所订阅资源的字符序列。
- `<subscription-id>` - 必选。唯一标识订阅的字符序列。此值未使用（尽管数据文件中必须存在一个值）。
- `<subscription-status>` - 必选。订阅的状态：已订阅或已取消订阅。
- `<property-name>` 和 `<property-value>` - 可选。零对或多对属性名称/值对的序列。它们表示与 StoreFront 客户端（通常为 Citrix Workspace 应用程序）的订阅相关联的属性。具有多个值并且以名称相同的多个名称/值对表示的属性（例如，“…MyProp A MyProp B …”表示具有值 A、B 的属性 MyProp）。

示例

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

StoreFront 服务器磁盘上订阅数据的大小

记录数	大小 (MB)
0	6.02
1000	7.02
10000	40.00
100000	219.00
200000	358.00
500000	784.00
8000000	1213.02
1000000	1597.15
1300000	1919.15
1500000	2205.15
2000000	2915.15

导入和导出**.txt** 文件的大小

记录数	大小 (MB)
0	0.00
1000	0.13
10000	1.30
100000	12.80
200000	25.60
500000	64.10
8000000	102.00
1000000	1128.00

记录数	大小 (MB)
1300000	166.00
1500000	192.00
1700000	218.00
2000000	256.00

应用商店订阅计数器

可以使用 Microsoft Windows 性能监视器计数器（开始 **>** 运行 **> perfmon**）显示（例如）服务器上的订阅记录总数或 StoreFront 服务器组之间同步的记录数量。

使用 **PowerShell** 查看订阅计数器

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

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

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

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number
     Subscriptions Transferred"
<!--NeedCopy-->
```

使用 **Microsoft SQL Server** 存储订阅数据

April 17, 2024

> 注意：
>
> 本文档假定 MS SQL Server 和 T-SQL 查询的基本知识。在尝试遵循本文档之前，管理员必须很方便地配置、使用和管理 SQL Server。

简介

ESENT 是 Windows 可以使用的嵌入式事务性数据库引擎。默认情况下，所有版本的 StoreFront 都支持使用内置 ESENT 数据库。如果将应用商店配置为使用 SQL 连接字符串，用户还可以连接到 Microsoft SQL Server 实例。

将 StoreFront 切换到使用 SQL 而非 ESENT 的主要优势是 T-SQL 更新语句允许您管理、修改或删除订阅记录。如果使用 SQL，则无需在对订阅数据执行细微更改时导出、修改和重新导入整个 ESENT 订阅数据。

要将现有订阅数据从 ESENT 迁移到 Microsoft SQL Server，需要将从 StoreFront 导出的平面 ESENT 数据转换为 SQL 友好格式以便批量导入。对于没有任何新订阅数据的新部署，不需要执行此步骤。数据转换步骤只需执行一次。本文介绍了可以在版本 3.5 之后的所有 StoreFront 版本中使用的受支持的配置，其中引入了本文中引用的 -STF PowerShell SDK。

> 注意：
>
> 由于网络中断，连接到 StoreFront 用于存储订阅数据的 SQL Server 实例失败，不会导致 StoreFront 部署无法使用。中断只会导致用户体验暂时降低；在恢复与 SQL Server 的连接之前，用户无法添加、删除或查看收藏的资源。在中断期间仍然可以枚举和启动资源。预期的行为与使用 ESENT 时 Citrix Subscription Store 服务停止时的行为相同。
>
> 提示：
>
> 使用 KEYWORDS:Auto 或 KEYWORDS:Mandatory 配置的资源在使用 ESENT 或 SQL 时的行为方式相同。用户首次登录时，如果其中一个关键字包含在用户的资源中，则会自动创建新的 SQL 订阅记录。

ESENT 和 **SQL Server** 的优势

ESENT	SQL
默认设置，不需要添加任何配置即可使用 StoreFront “开箱即用”。	使用 T-SQL 查询可以轻松操作或更新更易于管理的数据和订阅数据。允许删除或更新每个用户的记录 允许通过简单的方法计算每个应用程序、Delivery Controller 或用户的记录。允许通过简单的方法删除已离开公司/组织的用户的不必要的用户数据。允许通过简单的方法更新 Delivery Controller 引用，例如当管理员切换到使用聚合或预配新的 Delivery Controller 时。
使用订阅同步和提取计划在不同的服务器组之间配置复制更加简单。请参阅配置订阅同步	与 StoreFront 分离，因此无需在 StoreFront 升级之前备份订阅数据，因为数据是在单独的 SQL Server 上维护的。订阅备份独立于 StoreFront，并使用 SQL 备份策略和机制。
不需要订阅管理时，SQL 非必需。如果订阅数据永远不需要更新，ESENT 可能会满足客户的需求。	由服务器组的所有成员共享的订阅数据的单个副本，因此服务器之间出现数据差异或数据同步问题的可能性较小。

ESENT 和 **SQL Server** 的缺点

ESENT	SQL
没有简单的方法来轻松、精确地管理订阅数据。要求在导出的.txt 文件中执行订阅操作。必须导出并重新导入整个订阅数据库。可能需要使用查找和替换技术更改数以千计的记录，此技术需要大量人力，并且可能容易出错。 必须在服务器组中的每个 StoreFront 服务器上维护 ESENT 数据库的副本。在极少数情况下，此数据库可能会在服务器组内或不同服务器组之间脱离同步。	需要基本的 SQL 专业知识和基础结构。可能需要购买 SQL 许可证，这会增加 StoreFront 部署的总拥有成本。尽管 Citrix Virtual Apps and Desktops 数据库实例也可以与 StoreFront 共享，以降低成本。 在服务器组之间复制订阅数据是一项重要的部署任务。它需要多个 SQL 实例和每个数据中心之间的事务复制。这需要专门的 MS SQL 专业知识。 需要从 ESENT 进行数据迁移以及转换为 SQL 友好的格式。此过程仅需执行一次。 可能需要额外的 Windows 服务器和许可证。 部署 StoreFront 的额外步骤。

部署方案

> 注意：
>
> 如果要支持用户订阅，在 StoreFront 中配置的每个应用商店都需要 ESENT 数据库或 Microsoft SQL 数据库。存储订阅数据的方法是在 StoreFront 中的商店级别设置的。

Citrix 建议所有应用商店数据库都驻留在同一 Microsoft SQL Server 实例上，以降低管理复杂性并缩小配置错误的范围。

多个应用商店可以共享同一个数据库，前提是它们都配置为使用相同的连接字符串。如果这些应用商店使用不同的 Delivery Controller 也没关系。共享数据库的多个应用商店的缺点是无法判断每个订阅记录对应的应用商店。

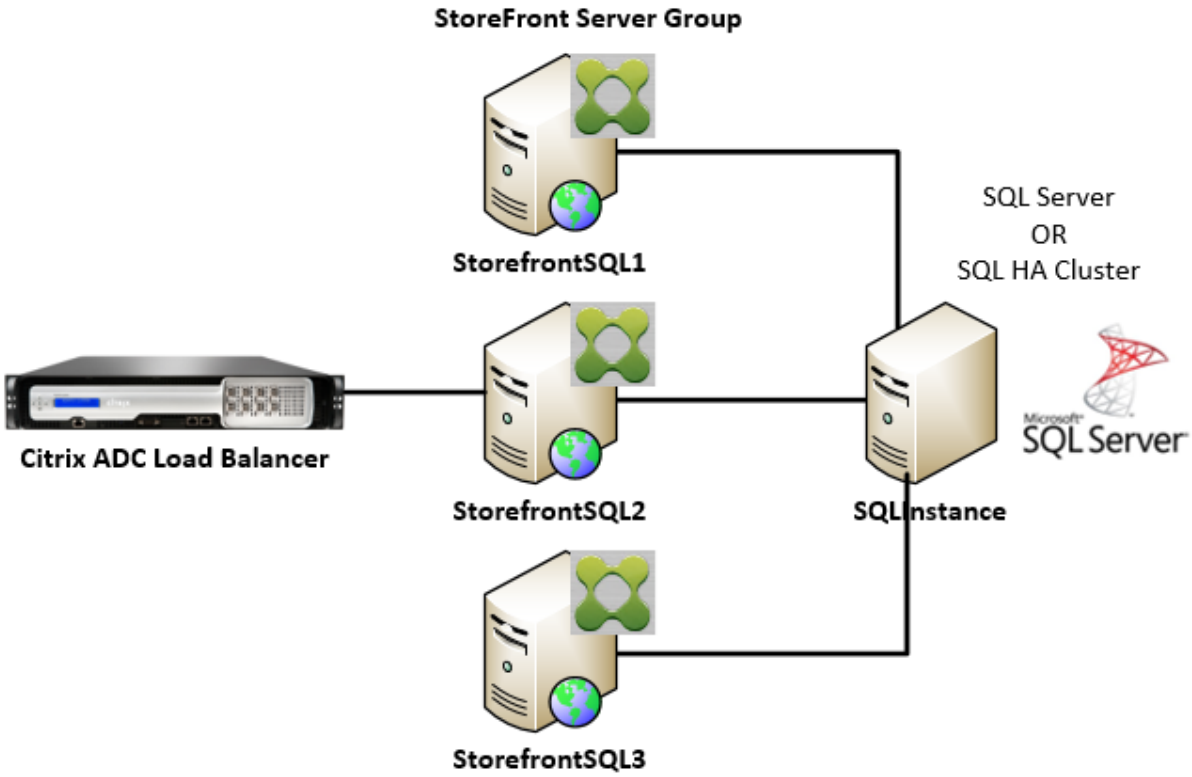
在具有多个应用商店的单个 StoreFront 部署中，技术上可以将两种数据存储方法组合起来。可以将一个应用商店配置为使用 ESENT，将另一个应用商店配置为使用 SQL。由于管理复杂性增加以及配置错误的范围，建议不要这样做。

有四种方案可用于在 SQL
Server 中存储订阅数据：

方案 **1**：使用 **ESENT** 的单个 **StoreFront** 服务器或服务器组（默认） 默认情况下，自版本 2.0 以来的所有 StoreFront 版本都使用平面 ESENT 数据库在服务器组成员之间存储和复制订阅数据。服务器组的每个成员都维护订阅数据库的相同副本，该副本与服务器组的所有其他成员同步。此方案不需要执行任何其他步骤即可配置。此方案适用于大多数客户，这些客户不期望经常更改 Delivery Controller 名称，或者不需要对其订阅数据执行频繁的管理任务，例如删除或更新旧用户订阅。

方案 **2**：安装单个 **StoreFront** 服务器和本地 **Microsoft SQL Server** 实例　StoreFront 使用本地安装的 SQL Server 实例，并且两个组件位于同一服务器上。此方案适用于简单的单一 StoreFront 部署，在此类部署中，客户可能需要频繁更改 Delivery Controller 名称，或者需要对其订阅数据执行频繁的管理任务，例如删除或更新旧用户订阅，但不需要高可用性 StoreFront 部署。Citrix 不建议对服务器组使用此方案，因为它会在托管 Microsoft SQL 数据库实例的服务器组成员上造成单一故障点。此方案不适用于大型企业部署。

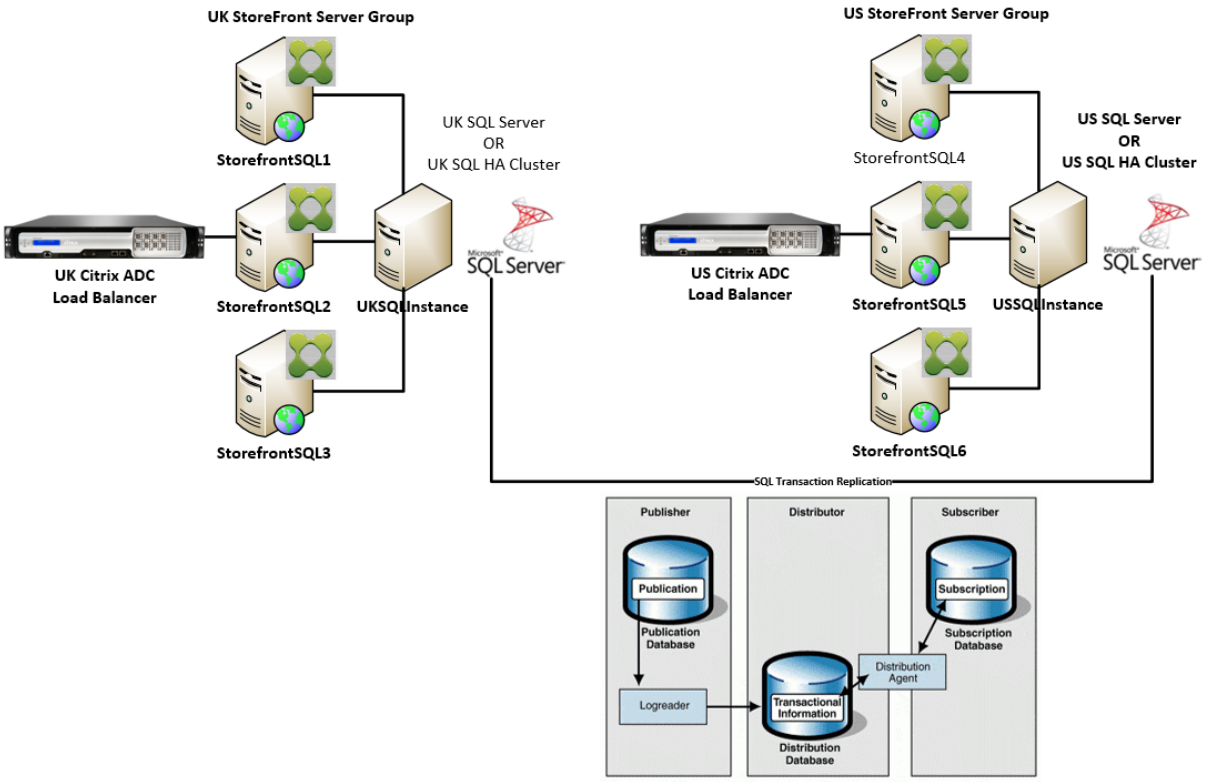
方案 **3**：配置为高可用性的 **StoreFront** 服务器组和专用 **Microsoft SQL Server** 实例（推荐）　所有 StoreFront 服务器组成员连接到同一个专用的 Microsoft SQL Server 实例或 SQL 故障转移群集。此方案是最适合大型企业部署的模型，在此类部署中，Citrix 管理员希望频繁更改 Delivery Controller 名称或希望对其订阅数据执行频繁的管理任务，例如删除或更新旧用户订阅并要求高可用性。



方案 **4**：每个服务器组中的每个数据中心中的多个 **StoreFront** 服务器组和一个专用 **Microsoft SQL Server** 实例

> 注意：
>
> 这是一个高级配置。只有当您是熟悉事务复制的经验丰富的 SQL Server 管理员，并且具备成功部署事务复制的必要技能时才尝试此操作。

这与方案 3 相同，但将其扩展到不同的远程数据中心中需要多个 StoreFront 服务器组的情况。Citrix 管理员可以选择在相同或不同数据中心中的不同服务器组之间同步订阅数据。数据中心中的每个服务器组连接到自己的专用 Microsoft SQL Server 实例，以实现冗余、故障转移和性能。此方案需要大量额外的 Microsoft SQL Server 配置和基础结构。它完全依赖于 Microsoft SQL 技术来复制订阅数据及其 SQL 事务。



资源

可以从 https://github.com/citrix/sample-scripts/tree/master/storefront 下载以下脚本来帮助您：

配置脚本

- **Set-STFDatabase.ps1** - 为每个应用商店设置 MS SQL 连接字符串。在 StoreFront 服务器上运行。
- **Add-LocalAppPoolAccounts.ps1** - 授予本地 StoreFront 服务器的应用程序池对 SQL 数据库的读取和写入访问权限。在 SQL Server 上运行方案 2。
- **Add-RemoteSFAccounts.ps1** - 授予服务器组中的所有 StoreFront 服务器对 SQL 数据库的读取和写入访问权限。在 SQL Server 上运行方案 3。
- **Create-StoreSubscriptionsDB-2016.sql** - 创建 SQL 数据库和架构。在 SQL Server 上运行。

数据转换和导入脚本

- **Transform-SubscriptionDataForStore.ps1** - 将 ESENT 中的现有订阅数据导出并转换为 SQL 友好的格式以便导入。
- **Create-ImportSubscriptionDataSP.sql** - 创建一个存储过程来导入 Transform-SubscriptionDataForStore.ps1 转换的数据。使用 Create-StoreSubscriptionsDB-2016.sql 创建数据库架构后，在 SQL Server 上运行此脚本一次。

在 **SQL Server** 上配置 **StoreFront** 服务器的本地安全组

方案 **2**：安装单个 **StoreFront** 服务器和本地 **Microsoft SQL Server** 实例

在 Microsoft SQL Server 上创建一个名为 <SQLServer>\StoreFrontServers 的本地安全组，并为 IIS APPPOOL\DefaultAppPool 和 IIS APPPOOL\Citrix Receiver for Web 添加虚拟帐户以允许本地安装的 StoreFront 读取和写入 SQL。此安全组在创建应用商店订阅数据库架构的.SQL 脚本中引用，因此请确保组名称匹配。

可以下载脚本 Add-LocalAppPoolAccounts.ps1 来帮助您。

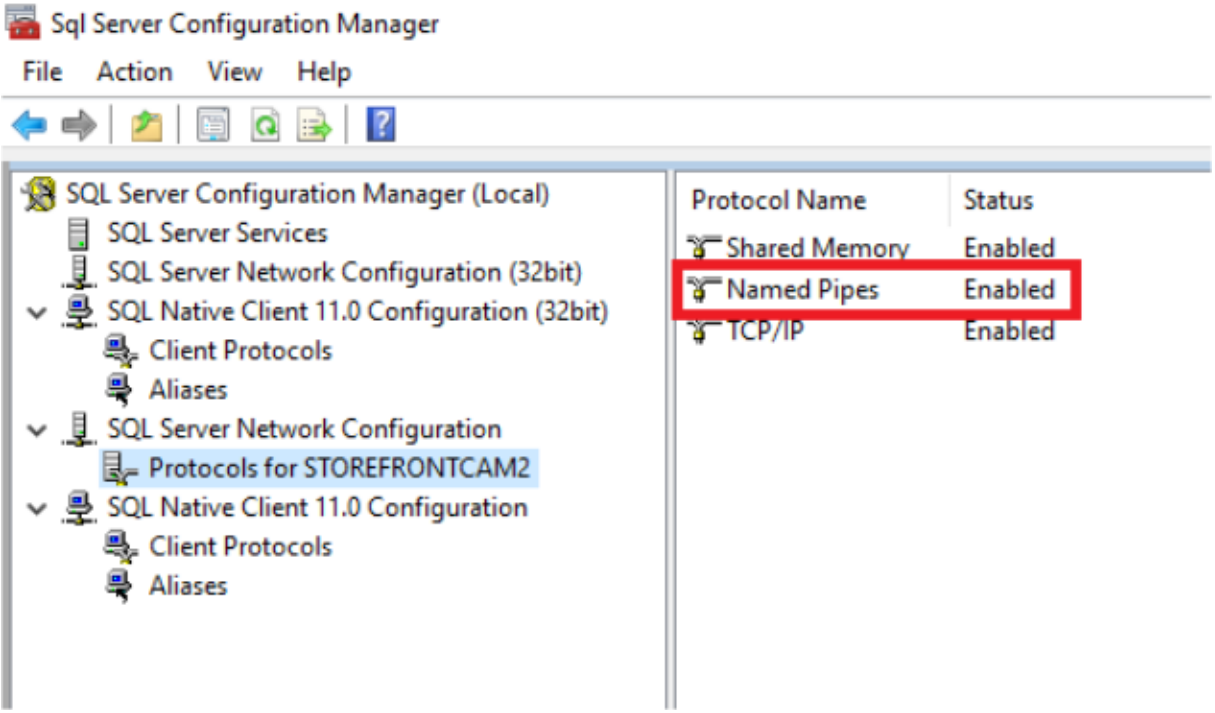
在运行 *Add-LocalAppPoolAccounts.ps1* 脚本之前安装 StoreFront。该脚本取决于查找 IIS APPPOOL\Citrix Receiver for Web 虚拟 IIS 帐户的能力，该帐户在安装并配置 StoreFront 之前不存在。IIS APPPOOL\DefaultAppPool 是通过安装 IIS Web 服务器角色自动创建的。

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

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

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

else
{

Write-Host "Creating $LocalGroupName local security group" -
    ForegroundColor "Yellow"

# Create Local User Group
$Computer = [ADSI]"WinNT://$env:ComputerName,Computer"
$LocalGroup = $Computer.Create("group",$LocalGroupName)
$LocalGroup.setinfo()
$LocalGroup.description = $Description
$Localgroup.SetInfo()
Write-Host "$LocalGroupName local security group created" -
    ForegroundColor "Green"
 }

$Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"

# Add IIS APPPOOL\DefaultAppPool
$objAccount = New-Object System.Security.Principal.NTAccount("IIS
    APPPOOL\DefaultAppPool")
$StrSID = $objAccount.Translate([System.Security.Principal.
    SecurityIdentifier])
```



```
$DefaultSID = $StrSID.Value

$Account = [ADSI]"WinNT://$DefaultSID"
$Group.Add($Account.Path)

# Add IIS APPPOOL\Citrix Receiver for Web
$objAccount = New-Object System.Security.Principal.NTAccount("IIS
    APPPOOL\Citrix Receiver for Web")
$StrSID = $objAccount.Translate([System.Security.Principal.
    SecurityIdentifier])
$WebRSID = $StrSID.Value

$Account = [ADSI]"WinNT://$WebRSID"
$Group.Add($Account.Path)

Write-Host "AppPools added to $LocalGroupName local group" -
    ForegroundColor "Green"
<!--NeedCopy-->
```

使用 SQL Server 配置管理器在本地 SQL 实例中启用命名管道。StoreFront 与 SQL Server 之间的进程间通信需要命名管道。



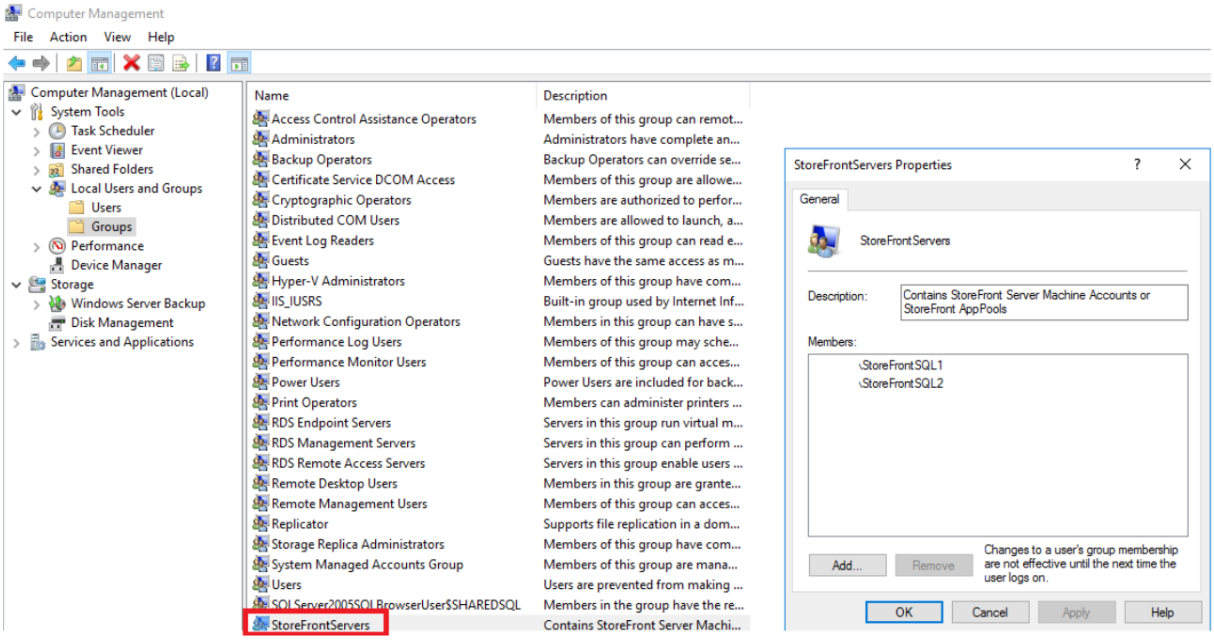
确保正确配置 Windows 防火墙规则以允许使用特定端口或动态端口建立 SQL Server 连接。请参阅 Microsoft 文档，了解如何在您的环境中执行此操作。

> 提示：
>
> 如果连接到本地 SQL 实例失败，请检查 localhost 或连接字符串中使用的 <hostname> 是否解析为正确的 IPv4 地址。Windows 可能会尝试使用 IPv6 而非 IPv4，并且 localhost 的 DNS 解析可能会返回::1 而非正确

> 的 StoreFront 和 SQL Server 的 IPv4 地址。可能需要在主机服务器上完全禁用 IPv6 网络堆栈才能解决此问题。

方案 **3**：**StoreFront** 服务器组和专用 **Microsoft SQL Server** 实例

在 Microsoft SQL Server 上创建一个名为 <SQLServer>\StoreFrontServers 的本地安全组，并添加 StoreFront 服务器组的所有成员。此安全组稍后在 **Create-StoreSubscriptionsDB-2016.sql** 脚本中引用，该脚本将在 SQL 中创建订阅数据库架构。



将所有 StoreFront 服务器组域计算机帐户添加到 <SQLServer>\StoreFrontServers 组中。如果 SQL Server 使用 Windows 身份验证，则只有组中列出的 StoreFront 服务器域计算机帐户才能读取和写入 SQL 中的订阅记录。脚本 Add-RemoteSFAccounts.ps1 中提供的以下 PowerShell 函数将创建本地安全组，并向其添加两个名为 StoreFrontSQL1 和 StoreFrontSQL2 的 StoreFront 服务器。

```
function Add-RemoteSTFMachineAccounts
{

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

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

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

```

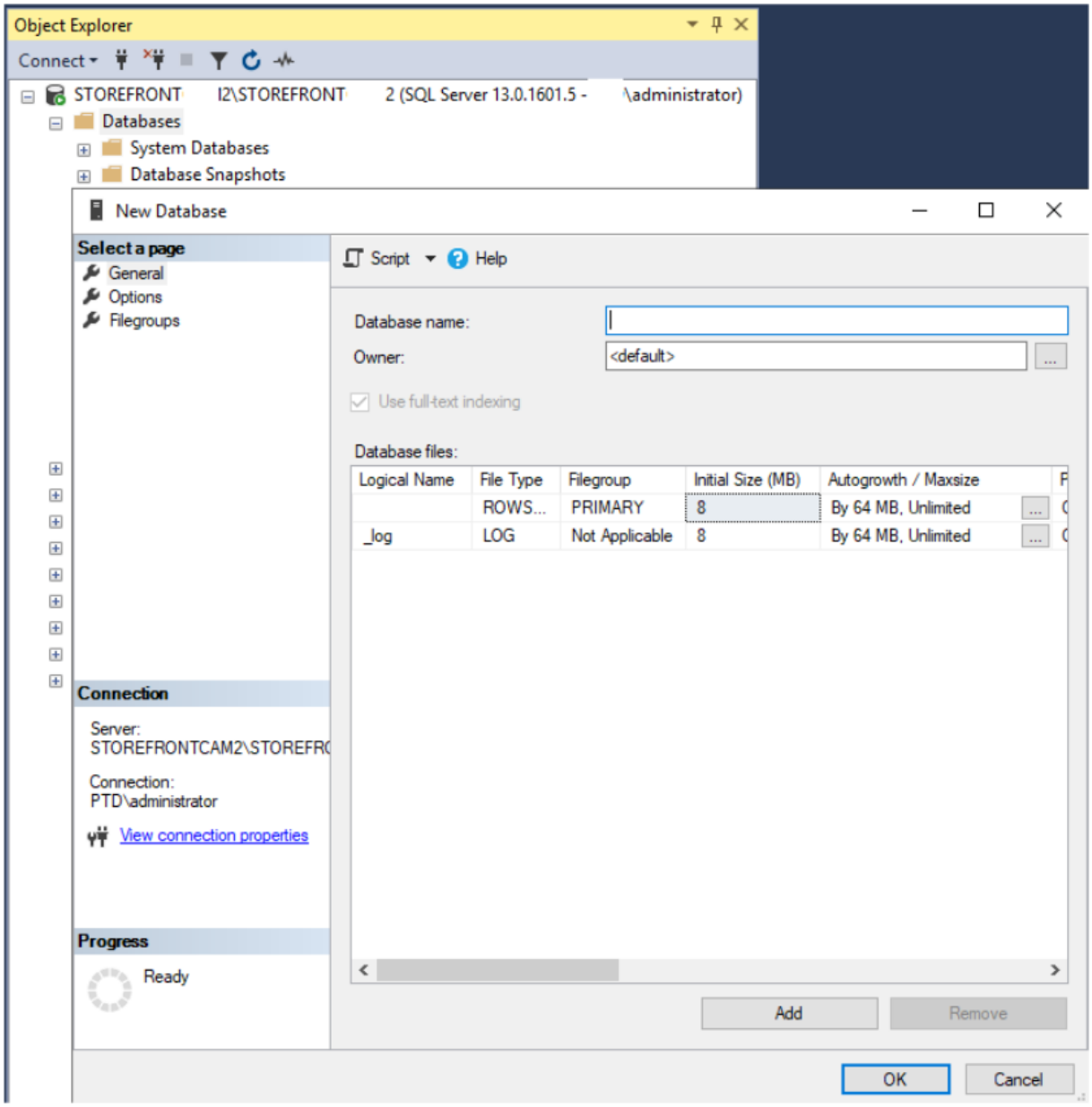


```
16      Write-Host "$LocalGroupName already exists!" -ForegroundColor "
            Yellow"
17   }
18
19  else
20  {
21
22      Write-Host "Creating $LocalGroupName local group" -ForegroundColor
            "Yellow"
23
24      # Create Local Security Group
25      $Computer = [ADSI]"WinNT://$env:ComputerName,Computer"
26      $LocalGroup = $Computer.Create("group",$LocalGroupName)
27      $LocalGroup.setinfo()
28      $LocalGroup.description = $Description
29      $Localgroup.SetInfo()
30  Write-Host "$LocalGroupName local group created" -ForegroundColor "
        Green"
31   }
32
33  Write-Host "Adding $StoreFrontServers to $LocalGroupName local group" -
        ForegroundColor "Yellow"
34
35  foreach ($StoreFrontServer in $StoreFrontServers)
36  {
37
38      $Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"
39      $Computer = [ADSI]"WinNT://$Domain/$StoreFrontServer$"
40      $Group.Add($Computer.Path)
41   }
42
43  Write-Host "$StoreFrontServers added to $LocalGroupName" -
        ForegroundColor "Green"
44   }
45
46  Add-RemoteSTFMachineAccounts -Domain "example" -StoreFrontServers @("
        StoreFrontSQL1","StoreFrontSQL2")
47  <!--NeedCopy-->
```

在 **Microsoft SQL Server** 中为每个应用商店配置订阅数据库架构

在您的 Microsoft SQL Server 上创建一个命名实例，供 StoreFront 使用。将.SQL 脚本中的路径设置为与 SQL 版本的安装位置或其数据库文件的存储位置相对应。示例脚本 Create-StoreSubscriptionsDB-2016.sql 使用 SQL Server 2016 Enterprise。

通过右键单击数据库，然后选择新建数据库，使用 SQL Server Management Studio (SSMS) 创建空数据库。



键入数据库名称以匹配您的应用商店，或选择其他名称，例如 *STFSubscriptions*。

在运行脚本之前，对于 StoreFront 部署中的每个应用商店，请修改示例脚本中的引用以匹配您的 StoreFront 和 SQL 部署。例如，修改：

- 为您创建的每个数据库命名，以便与 `USE [STFSubscriptions]` 中的 StoreFront 中的商店名称相匹配。
- 将数据库.mdf 和.ldf 文件的路径设置为数据库的存储位置。

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

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

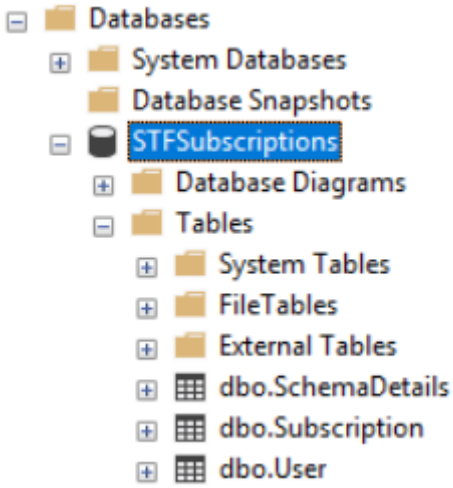


```
STFSubscriptions.ldf
```

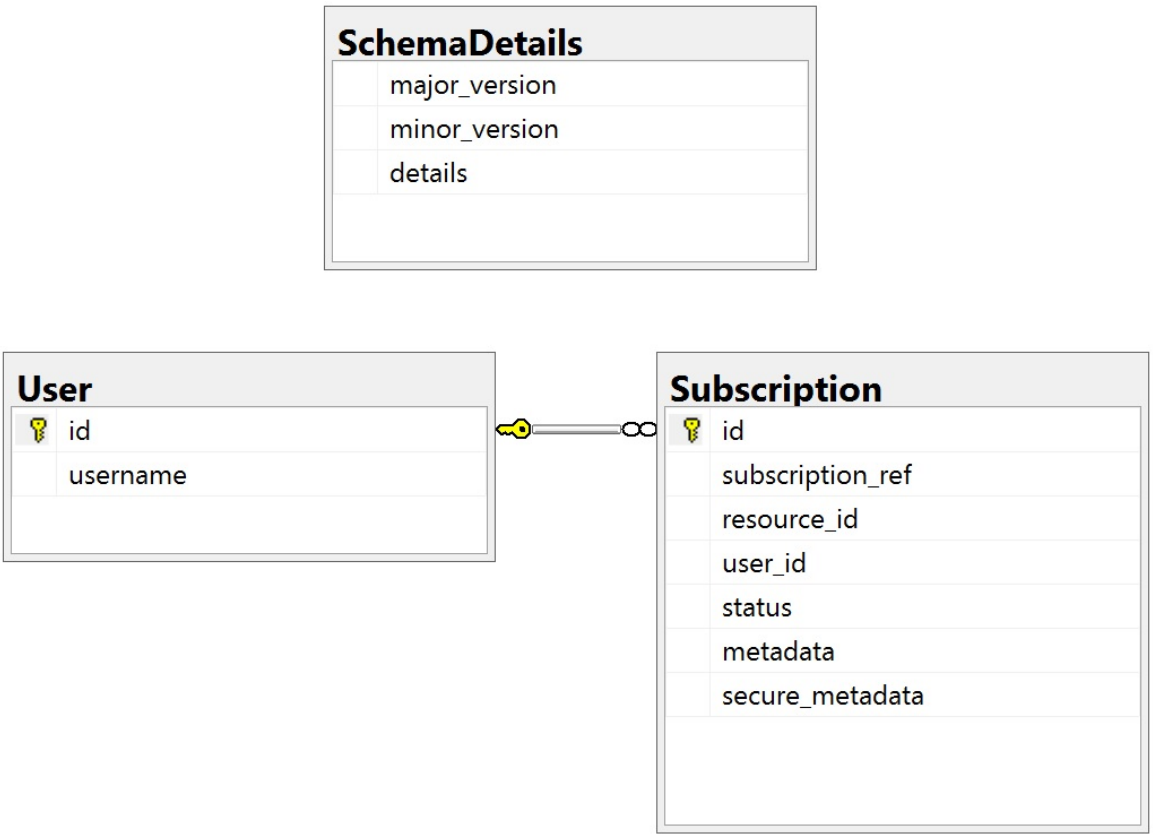
- 在脚本中设置对 SQL Server 名称的引用：

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

ALTER LOGIN [SQL2016\StoreFrontServers]
```

运行脚本。成功配置架构后，将创建三个数据库表：*SchemaDetails*、订阅和用户。



下面的数据库示意图显示了 *Create-StoreSubscriptionsDB-2016.sql* 脚本创建的订阅数据库架构：



为每个 **StoreFront** 应用商店配置 **SQL Server** 连接字符串

场景 **1**

> 提示：
>
> 存储在 ESENT 数据库中的磁盘上的原始订阅数据不会被销毁或删除。如果您决定从 Microsoft SQL Server 还原到使用 ESENT，则可以删除存储连接字符串并简单地切换回使用原始数据。ESENT 中将不存在 SQL 用于应用商店时创建的任何其他订阅，并且用户将看不到这些新的订阅记录。所有原始订阅记录仍将存在。

在应用商店上重新启用 **ESENT** 订阅　打开 PowerShell ISE 并选择以管理员身份运行。

使用 **-UseLocalStorage** 选项指定要在以下方面重新启用 ESENT 订阅的应用商店：

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

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

# Removes the SQL DB Connection string and reverts back to using ESENT
```



```
Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
    UseLocalStorage
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
<!--NeedCopy-->
```

方案 **2**、**3** 和 **4**

打开 PowerShell ISE 并选择以管理员身份运行。

指定要为使用 **$StoreVirtualPath** 设置连接字符串的应用商店

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

# For a remote database instance
$ConnectionString = "Server=$DBServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;"
<!--NeedCopy-->
```

或者

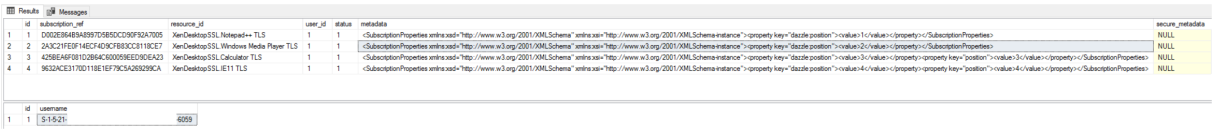
```
# For a locally installed database instance
$ConnectionString = "$DBLocalServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;"

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

如果要将部署中的每个应用商店全部配置为使用 SQL 连接字符串，请对其重复执行此过程。

将现有数据从 **ESENT** 迁移到 **Microsoft SQL Server**

要将现有 ESENT 数据迁移到 SQL，需要执行一个两步数据转换过程。提供了两个脚本来帮助您执行这一一次性操作。如果 StoreFront 和 SQL 实例中的连接字符串配置正确，则所有新订阅都会以正确的格式在 SQL 中自动创建。迁移后，历史 ESENT 订阅数据将转换为 SQL 格式，用户还可以查看其先前订阅的资源。

示例：同一域用户的四个 **SQL** 订阅



步骤 **1** 使用 **Transform-SubscriptionDataForStore.ps1** 脚本将 **ESENT** 数据转换为 **SQL** 友好的格式以便批量导入　登录到要从中转换 ESENT 数据的 StoreFront 服务器。

服务器组的任何成员都适用，前提是这些成员都包含相同数量的订阅记录。

打开 PowerShell ISE 并选择以管理员身份运行。

运行将 <StoreName>.txt 文件从 ESENT 数据库导出到当前用户桌面的脚本 Transform-SubscriptionDataForStore.ps1。

PowerShell 脚本对处理的每个订阅行提供详细反馈，以帮助调试并帮助您评估操作是否成功。这可能需要很长时间才能处理。

脚本完成后，转换后的数据将写入到当前用户的桌面上的 <StoreName>SQL.txt。该脚本汇总了唯一用户记录的数量和处理的订阅总数。

对要迁移到 SQL Server 的每个应用商店重复执行此过程。

步骤 **2** 使用 **T-SQL** 存储过程批量 **SQL** 导入转换后的数据　每个应用商店的数据必须一次导入一个应用商店。

将在步骤 1 中创建的 <StoreName>SQL.txt 文件从 StoreFront 服务器的桌面复制到 Microsoft SQL Server 上的 C:\，并将其重命名为 SubscriptionsSQL.txt。

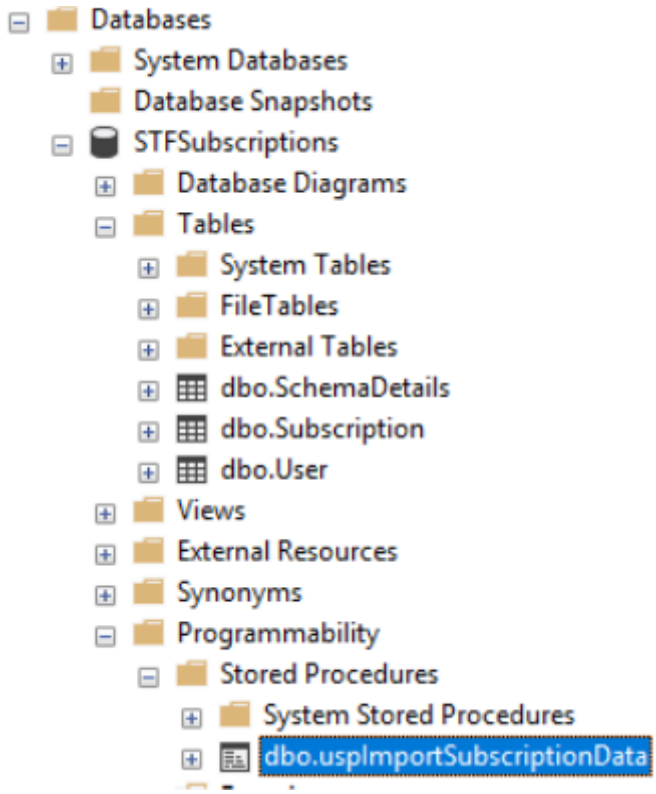
Create-ImportSubscriptionDataSP.sql 脚本将创建一个 T-SQL 存储过程以批量导入订阅数据。该将本将删除每个唯一用户的重复条目，以便将生成的 SQL 数据正确规范化并拆分为正确的表。

在执行 *Create-ImportSubscriptionDataSP.sql* 之前，请更改 `USE [STFSubscriptions]` 以匹配要在其下创建存储过程的数据库。

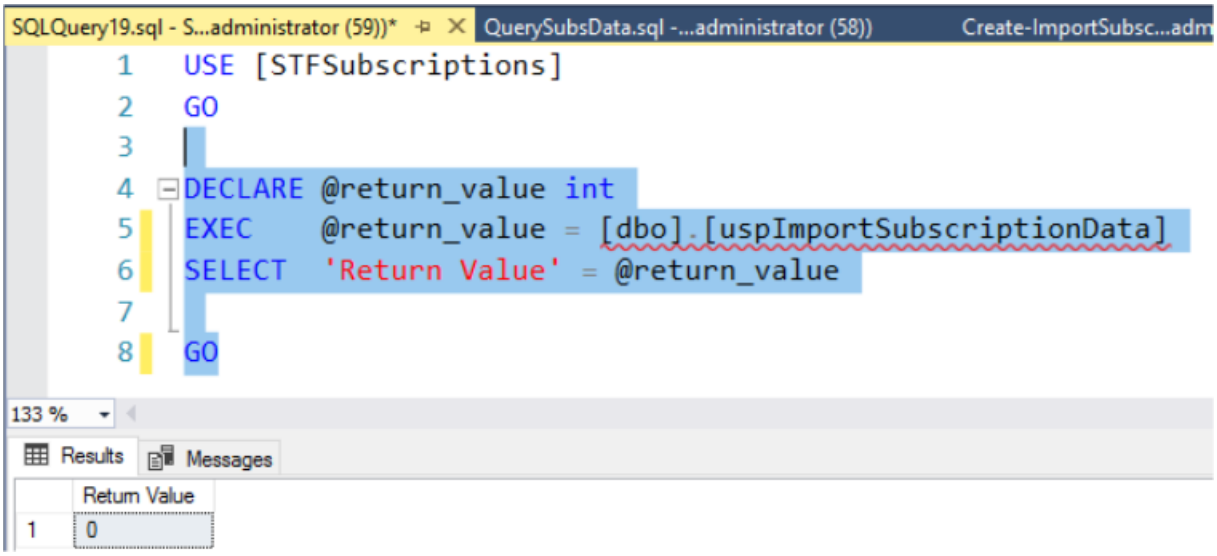
使用 SQL Server Management Studio 打开 *Create-ImportSubscriptionDataSP.sql* 文件，并在其中执行代码。此脚本将 *ImportSubscriptionDataSP* 存储过程添加到您之前创建的数据库中。

成功创建存储过程后，SQL 控制台中将显示以下消息，并将 ImportSubscriptionDataSP 存储过程添加到数据库中：

```
Commands completed successfully.
```

右键单击存储过程以执行该过程，然后选择执行存储过程并单击确定。



返回值 0 表示所有数据都已成功导入。导入时的任何问题都会记录到 SQL 控制台。存储过程成功运行后，将 Transform-SubscriptionDataForStore.ps1 提供的订阅记录的总数和唯一用户与下面两个 SQL 查询的结果进行比较。两个总数应匹配。

来自转换脚本的订阅总数应与 SQL 报告的总数相匹配

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



```
<!--NeedCopy-->
```

转换脚本中的唯一用户数应与 SQL 报告的用户表中的记录数相匹配

```
SELECT COUNT(*) AS TotalUsers
FROM [User]
<!--NeedCopy-->
```

如果转换脚本显示 100 个唯一用户和 1000 条总订阅记录，SQL 应在成功迁移后显示相同的两个数字。

登录 StoreFront 以检查现有用户是否能够查看其订阅数据。当用户订阅或取消订阅其资源时，将在 SQL 中更新现有订阅记录。还会在 SQL 中创建新用户和订阅记录。

步骤 **3** 对导入的数据运行 **T-SQL** 查询

> 注意：
>
> 所有 Delivery Controller 名称都区分大小写，并且必须与 StoreFront 中使用的大小写和名称完全匹配。

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

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

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

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

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



```
10
11 -- Get all subscription records for a particular application
12 Use [STFSubscriptions]
13 SELECT * FROM [Subscription]
14 WHERE [resource_id] = ' DeliveryController.Application'
15 <!--NeedCopy-->
```

使用 T-SQL 更新或删除现有订阅记录

> 免责声明：
>
> 所有示例 SQL 更新和删除语句的使用风险完全由您自行承担。因错误使用提供的示例而导致您的订阅数据的任何丢失或意外更改，Citrix 概不负责。提供以下 T-SQL 语句作为启用要执行的简单更新的指南。在尝试更新订阅或删除过时的记录之前，备份 SQL 数据库完全备份中的所有订阅数据。未能执行必要的备份可能会导致数据丢失或损坏。在对生产数据库执行您自己的 T-SQL UPDATE 或 DELETE 语句之前，请对虚拟数据或远离实时生产数据库的生产数据的冗余副本对其进行测试。
>
> 注意：
>
> 所有 Delivery Controller 名称都区分大小写，并且必须与 StoreFront 中使用的大小写和名称完全匹配。

```
1 -- Update the delivery controller used in all subscriptions.
2 Use [STFSubscriptions]
3 UPDATE [Subscription]
4 SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
     NewDeliveryController.')
5 WHERE [resource_id] LIKE 'OldDeliveryController.%'
6 <!--NeedCopy-->
```

```
1 -- After enabling multi-site aggregation, update the resource_id
2 Use [STFSubscriptions]
3 UPDATE [Subscription]
4 SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
     DefaultAggregationGroup.')
5 WHERE [resource_id] LIKE 'OldDeliveryController.%'
6 <!--NeedCopy-->
```

```
1 -- Delete all subscription records for a particular Delivery Controller
2 Use [STFSubscriptions]
3 DELETE FROM [Subscription]
4 WHERE [resource_id] LIKE 'DeliveryController.%'
5 <!--NeedCopy-->
```

```
1 -- OR for aggregated resources use the name of the aggregation group
2 Use [STFSubscriptions]
3 DELETE FROM [Subscription]
4 FROM [Subscription]
5 WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'
6 <!--NeedCopy-->
```



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

```
-- Delete all subscription records for an application published via a
    specific delivery controller
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] = 'DeliveryController.Application'
<!--NeedCopy-->
```

```
-- Delete all subscription records for a particular user SID
-- relies on cascade to delete records from [Subscription]
Use [STFSubscriptions]
DELETE FROM [User]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'
<!--NeedCopy-->
```

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

Use [STFSubscriptions]
DELETE FROM [Subscription]
DBCC CHECKIDENT ([Subscription], RESEED, 0)
DELETE FROM [User]
DBCC CHECKIDENT ([User], RESEED, 0)
<!--NeedCopy-->
```

启用或禁用收藏夹

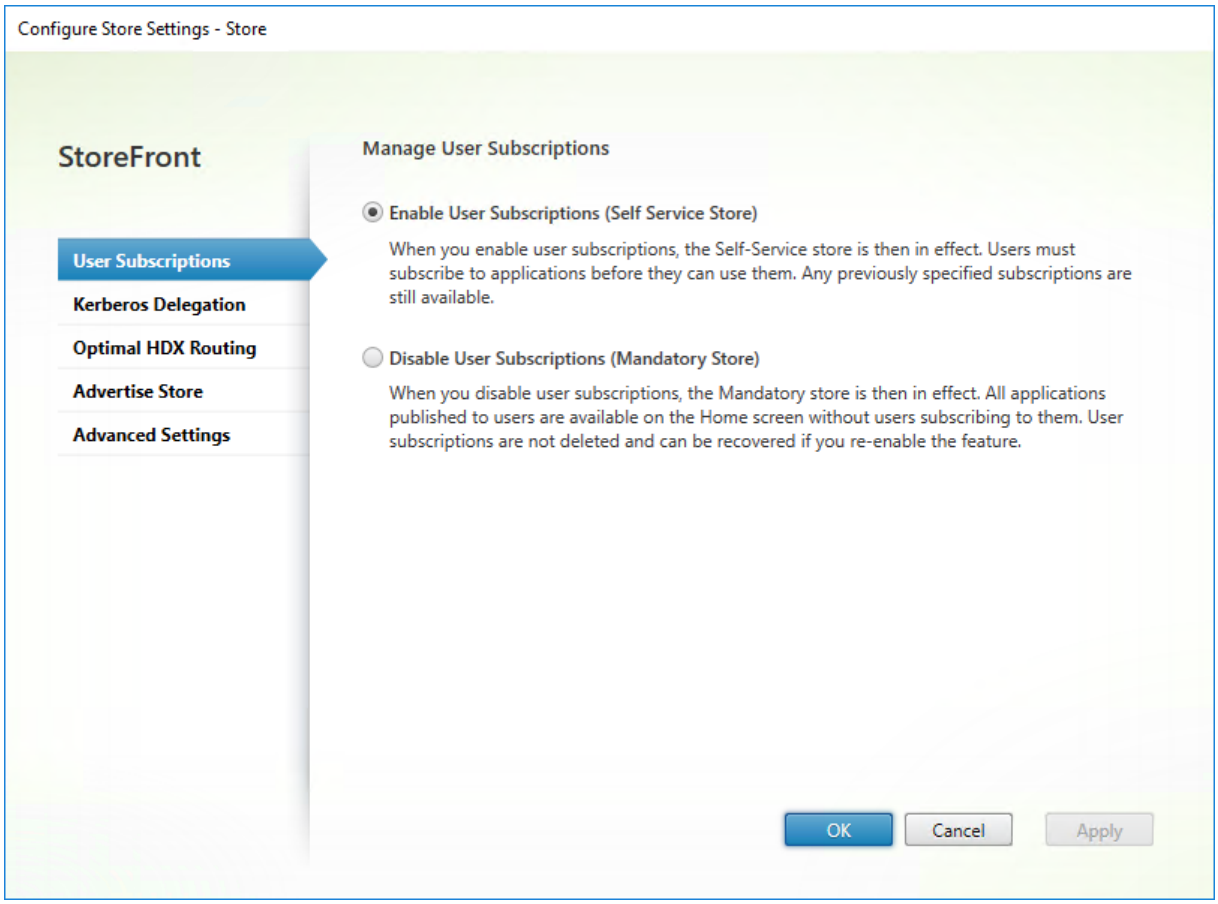
April 17, 2024

请使用“用户订阅”屏幕选择以下选项之一：

- 允许用户创建和删除收藏夹（自助服务应用商店）。用户可以通过单击应用程序磁贴上的星号来收藏应用程序。用户可以再次单击星号取消收藏应用程序。收藏的应用程序显示在主页选项卡上。
- 禁用收藏夹（强制性应用商店）。用户不能收藏或取消收藏应用程序。不显示主页选项卡。

禁用订阅不会删除应用商店订阅数据。重新启用对应用商店的订阅将允许用户在下次登录时查看其收藏夹。

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点，然后在结果窗格中选择一个应用商店。在操作窗格中，单击配置应用商店设置
2. 单击用户订阅选项卡以关闭或打开用户收藏夹功能。
3. 选择启用用户订阅 (自助服务应用商店) 以启用收藏夹。
4. 选择禁用用户订阅 (强制性应用商店) 以禁用收藏夹。



或者，您可以使用 PowerShell cmdlet Get-STFStoreService 为应用商店配置用户订阅，例如：

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
    yourstore>"
Set-STFStoreService -StoreService $StoreObject -LockedDown $True -
    Confirm:$False
<!--NeedCopy-->
```

Citrix Virtual Apps and Desktops 配置

April 17, 2024

通过 Citrix Virtual Apps and Desktops 或 Citrix Desktops as a Service 交付应用程序时，请考虑使用以下选项

来增强用户通过您的应用商店访问其应用程序时的体验。有关交付应用程序的详细信息，请参阅应用程序。

- 在应用程序名称 **(**面向用户**)** 字段中，输入您希望在应用商店 Web 站点中显示的应用程序名称。
- 在说明和关键字字段中，输入当您展开应用程序详细信息时应用商店 Web 站点上显示的说明以及任何关键字。
- 选择应用程序图标可帮助用户直观地识别 StoreFront Web 站点上的应用程序。
- 在应用程序类别字段中，根据需要输入类别。在类别名称中包含 \ 以创建文件夹层次结构。例如，您可以根据类型对应用程序进行分组，也可以为贵组织内的各种用户角色分别创建文件夹。在应用商店 Web 站点的应用程序选项卡中，类别视图显示类别列表以及每种类别中的应用程序。

关键字

可以通过将字符串 `KEYWORDS:[keywordname]` 附加到应用程序说明，向应用程序或桌面中添加关键字。多个关键字之间只能用空格进行分隔；例如 `KEYWORDS:Accounts Featured`。可以通过多种方式使用关键字：

- 筛选应用程序 - 请参阅高级应用商店设置)。
- 创建精选应用程序组。
- 有些关键字具有特殊含义。

关键字名称	说明
强制	将应用程序添加到“主页”选项卡。与收藏夹不同，用户无法从“主页”选项卡中删除必需的应用程序。如果为应用商店禁用了收藏夹，则无效。
自动	当用户登录应用商店时，该应用程序会自动收藏并添加到其“主页”选项卡中。用户可以取消收藏此类应用程序。如果为应用商店禁用了收藏夹，则无效。
TreatAsApp	应用到桌面以强制 StoreFront 将其视为应用程序。桌面显示在应用程序选项卡上，而非显示在桌面选项卡上。此外，当用户登录到应用商店 Web 站点时，桌面不会自动启动，也不会通过 Desktop Viewer 进行访问，即使针对其他桌面为站点进行了此项配置。
prefer=”*application*“	其中 *application* 标识本地安装的应用程序。仅适用于 Windows 上的 Citrix Workspace 应用程序。这指定当本地安装的应用程序版本与交付的等同实例都可用时，应优先使用前者。有关详细信息，请参阅配置本地应用程序访问应用程序。
Primary 和 **Secondary**	使用多站点聚合时，指定了关键字 **primary** 的聚合将始终优先于使用关键字 **secondary** 的聚合。

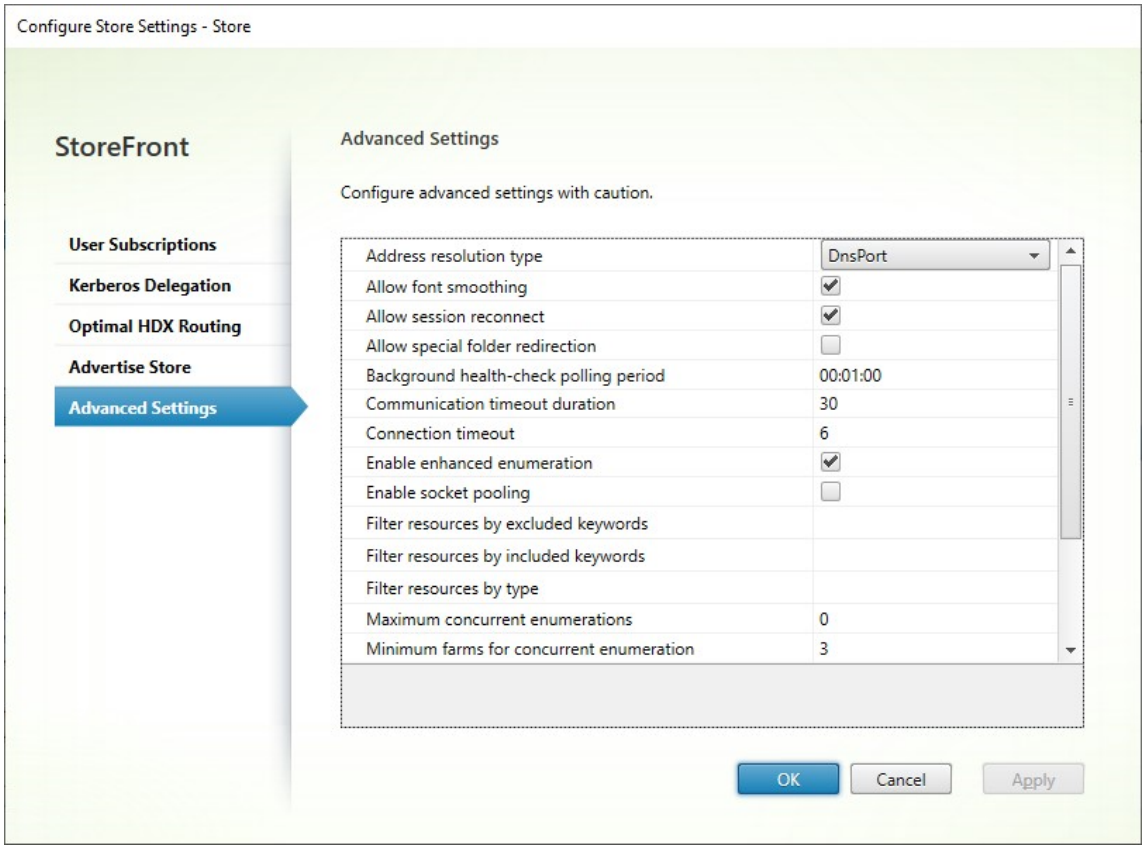
高级应用商店设置

April 17, 2024

可以使用“配置应用商店设置”中的“高级设置”页面配置最高级的应用商店属性。某些设置只能使用 PowerShell 进行修改。

> 重要：
>
> 在多服务器部署中，请一次仅使用一台服务器以更改服务器组的配置。确保 Citrix StoreFront 管理控制台未在部署中的任何其他服务器上运行。完成后，请将对配置所做的更改传播到服务器组，以便更新部署中的其他服务器。

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择“应用商店”节点，在中间窗格中选择一个应用商店，然后在“操作”窗格中选择 配置应用商店设置。
2. 在配置应用商店设置页面上，选择高级设置并进行所需的更改。



3. 单击确定以保存更改。

地址解析类型

可以指定要从服务器请求的地址类型。默认格式为 DnsPort。

在高级设置窗口中，从地址解析类型下拉列表中选择一个值。

- Dns
- DnsPort
- IPV4
- IPV4Port
- 点
- DotPort
- Uri
- NoChange

允许应用字体平滑

可以指定是否要为 HDX 会话应用字体平滑。默认值为开。

在高级设置窗口中，选择允许应用字体平滑选项，然后单击确定。

允许重新连接会话

可以指定是否要重新连接 HDX 会话。默认值为开。

在高级设置窗口中，选择允许重新连接会话选项。

允许特殊文件夹重定向

配置了特殊文件夹重定向时，用户可以将服务器的 Windows 特殊文件夹映射到其本地计算机的文件夹。特殊文件夹是指标准 Windows 文件夹（如 *\Documents* 和 *\Desktop*），无论是什么操作系统，它们始终以相同方式显示。

在高级设置窗口中，选择或取消选择允许特殊文件夹重定向选项以启用或禁用特殊文件夹重定向，然后单击确定。

高级运行状况检查

StoreFront 对每个 Citrix Virtual Apps and Desktops Delivery Controller 和 Cloud Connector 运行定期运行状况检查，以降低间歇性服务器可用性的影响。使用高级运行状况检查，StoreFront 会执行更深入的检查，更有可能检测到任何问题。

通过 Cloud Connector 连接到 Citrix 桌面即服务时，高级运行状况检查还有一个好处，即可以检索与哪些 VDA 与 Cloud Connector 位于同一位置有关的更多信息。如果 Cloud Connector 无法连接 Citrix 桌面即服务，Cloud Connector 将使用其本地主机缓存来加快与位于同一位置的 VDA 的连接速度。StoreFront 使用高级运行状况检查结果中的其他信息联系最合适的联机连接器以启动应用程序和桌面。

为了确保中断期间的资源可用性，而无需在每个资源域（资源位置）中发布资源，请务必在所有 StoreFront 服务器上将资源源配置为包括所有资源位置中的所有 Cloud Connector 并启用高级运行状况检查功能。

高级运行状况检查默认处于禁用状态。Citrix 建议您在所有 StoreFront 部署中启用高级运行状况检查。要启用高级运行状况检查，请使用 PowerShell 命令 Set-STFStoreFarmConfiguration。例如：

```
$storeService = Get-STFStoreService  -VirtualPath '/Citrix/Store'
Set-STFStoreFarmConfiguration $storeService -AdvancedHealthCheck $true
<!--NeedCopy-->
```

后台运行状况检查轮询期限

StoreFront 对每个 Citrix Virtual Apps and Desktops Delivery Controller 和 Cloud Connector 运行定期运行状况检查，以降低间歇性服务器可用性的影响。默认为每分钟 (00:01:00)。在高级设置窗口中，为后台运行状况检查轮询周期指定时间，然后单击确定控制运行状况检查的频率。启用了高级运行状况检查时，不建议将轮询周期设置为较低的值，因为这可能会影响性能。

通信超时期限

默认情况下，StoreFront 向为应用商店提供资源的服务器所发出的连接请求会在 30 秒后超时。在通信尝试失败 1 次后，服务器被视为不可用。在高级设置窗口中，更改默认时间，然后单击确定更改这些设置。

连接超时

可以指定与 Delivery Controller 建立初始连接时等待的秒数。默认值为 6。

在高级设置窗口中，指定建立初始连接时等待的秒数，然后单击确定

启用增强枚举

此选项控制 StoreFront 在多个 Citrix Virtual Apps and Desktops 站点中枚举应用程序和桌面时是同时还是按顺序查询 Delivery Controller。跨多个站点聚合资源时，并发枚举可以更快地响应用户查询。选择此选项时（默认设置），StoreFront 会同时向所有 Delivery Controller 发出枚举请求，并在全部响应时聚合响应。可以使用并发枚举数上限和并发枚举的场数量下限选项来调整此行为。

在高级设置窗口中，选择（或取消选择）启用增强枚举选项，然后单击确定。

启用套接字池

默认情况下，套接字池在应用商店中处于禁用状态。启用套接字池后，StoreFront 会保留一个套接字池，而不是在每次需要时创建一个套接字，并在连接关闭时将其返回至操作系统。启用套接字池可增强性能，尤其是对于安全套接字层

(SSL) 连接。要启用套接字池，请编辑应用商店配置文件。在高级设置窗口中，选择启用套接字池选项，然后单击确定以启用套接字池。

文件类型关联

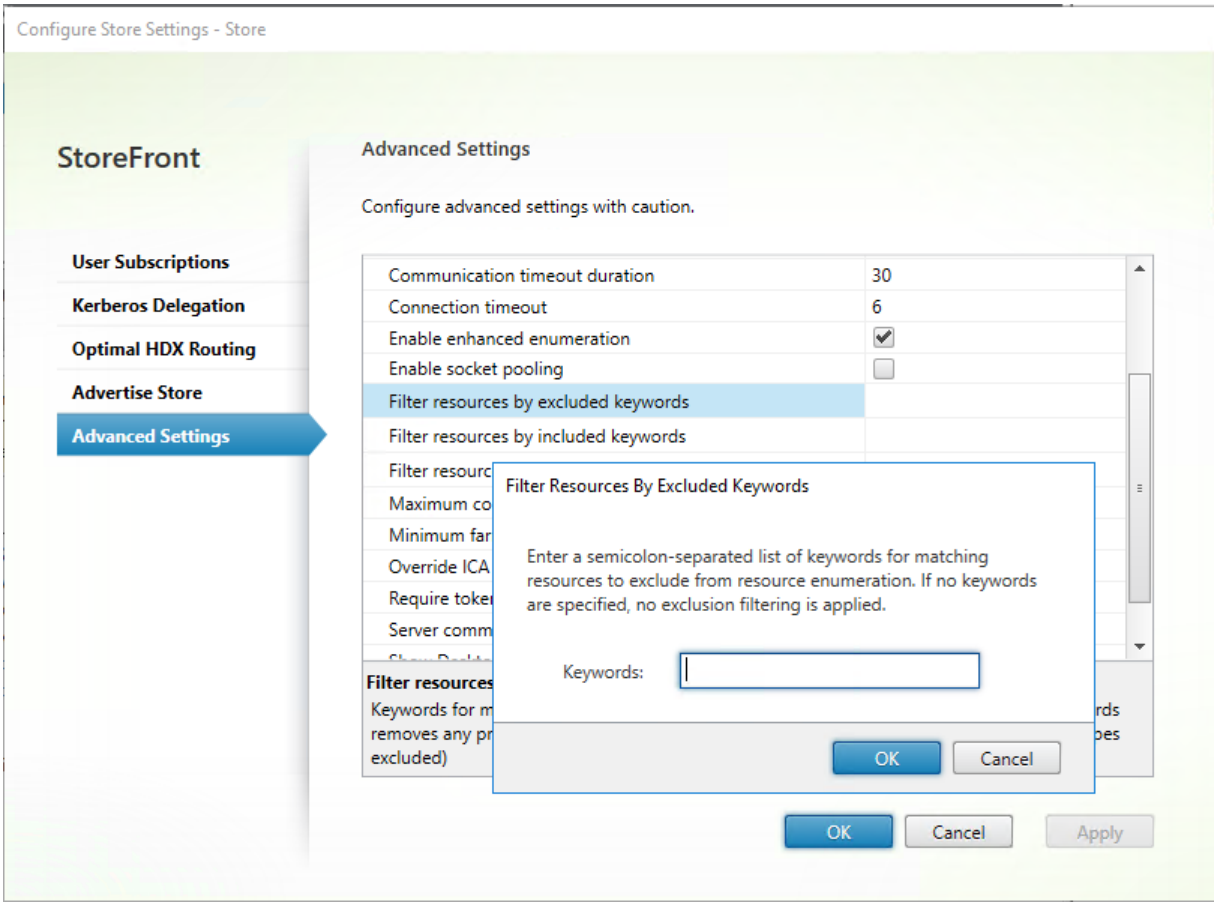
默认情况下，文件类型关联在应用商店中处于启用状态，这样，当用户打开相应类型的本地文件时，系统会将内容无缝重定向到用户订阅的应用程序。要启用禁用文件类型关联，请使用 PowerShell 命令 Set-STFStoreFarmConfiguration。例如：

```
$storeService = Get-STFStoreService  - VirtualPath '/Citrix/Store'
Set-STFStoreFarmConfiguration $storeService -EnableFileTypeAssociation
    $false
<!--NeedCopy-->
```

过滤资源 (按排除的关键字)

可以按排除的关键字过滤匹配的资源。指定排除关键字将删除以前配置的所有包含关键字。默认设置为“不过滤 (不排除任何资源类型)”。

在高级设置窗口中，选择过滤资源 (按排除的关键字)，单击此选项的右侧，在输入关键字框中输入以分号分隔的关键字列表，然后单击确定。



要使用 PowerShell 更改设置，请使用带参数 `-FilterByKeywordsExclude` 的 cmdlet Set-STFStoreEnumerationOptions。

以下关键字属于保留关键字，不能用于过滤：

- 自动
- 强制

过滤资源 (按包括的关键字)

可以按包含关键字过滤匹配的资源。指定包含关键字将删除以前配置的所有排除关键字。默认设置为“不过滤 (不排除任何资源类型)”。

1. 在高级设置窗口中，找到过滤资源 (按包括的关键字) 行。
2. 单击右侧栏打开过滤资源 (按包括的关键字) 窗口。
3. 在输入关键字框中输入以分号分隔的关键字列表
4. 单击确定。

要使用 PowerShell 更改设置，请使用带参数 `-FilterByKeywordsInclude` 的 cmdlet Set-STFStoreEnumerationOptions。

以下关键字属于保留关键字，不能用于过滤：

- 自动
- 强制

过滤资源 (按类型)

选择要在资源枚举中包含的资源类型。默认设置为“不过滤 (包括所有资源类型)”。

在高级设置窗口中，选择过滤资源 (按类型)，单击此选项的右侧，选择要在枚举中包括的资源类型，然后单击确定。

要使用 PowerShell 更改设置，请使用带参数 `-FilterByTypesInclude` 的 cmdlet Set-STFStoreEnumerationOptions，指定资源类型（应用程序、桌面或文档）的阵列。

并发枚举数上限

指定发送到全部 Delivery Controller 的并发请求数上限。此选项在启用了启用增强枚举选项时生效。默认设置为“0 (无限制)”。

在高级设置窗口中，选择并发枚举数上限，输入一个数字，然后单击确定。

并发枚举的场数量下限

指定触发并发枚举所需的 Delivery Controller 的最小数量。此选项在启用了启用增强枚举选项时生效。默认值为 3。

在高级设置窗口中，选择并发枚举的场数量下限，输入一个数字，然后单击确定。

覆盖 ICA 客户端名称

使用 Web 浏览器生成的唯一 ID 覆盖.ica 启动文件中的客户端名称设置。如果禁用，Citrix Workspace 应用程序将指定客户端名称。默认值为关。

在高级设置窗口中，选择覆盖 **ICA** 客户端名称选项，然后单击确定。

要求令牌一致

如果启用此项，StoreFront 强制用于身份验证的网关与用于访问应用商店的网关保持一致。如果值不一致，用户必须重新进行身份验证。必须为智能访问启用此选项。如果用户通过禁用了身份验证的网关访问应用商店，则必须禁用此功能。默认值为开。

在高级设置窗口中，选择要求令牌一致选项，然后单击确定。

服务器通信尝试次数

指定尝试与 Delivery Controller 进行通信的次数，超过此次数后，会将其标记为不可用。默认值为 1。

在高级设置窗口中，选择服务器通信尝试次数，输入一个数字，然后单击确定。

对旧版客户端显示 **Desktop Viewer**

指定用户从旧版客户端访问其桌面时是否显示 Citrix Desktop Viewer 窗口和工具栏。默认值为关。

在高级设置窗口中，选择对旧版客户端显示 **Desktop Viewer** 选项，然后单击确定。

将桌面视为应用程序

指定在访问应用商店时，是否将桌面显示在“应用程序”视图中，而非“桌面”视图中。默认值为关。

在高级设置窗口中，选择将桌面视为应用程序选项，然后单击确定。

为应用商店配置最佳 **HDX** 路由

April 17, 2024

配置最佳 Citrix Gateway 路由，以优化从 HDX Engine 路由到使用 StoreFront 的 Citrix Virtual Apps and Desktops 发布的应用程序的 ICA 连接处理。通常情况下，站点的最佳网关布置在相同的地理位置。

只需为用户访问 StoreFront 所用的设备不是最佳网关的部署定义最佳 Citrix Gateway 设备。如果启动应通过创建启动请求的网关定向回来，StoreFront 会自动执行此操作。

可以将网关映射到特定的 Delivery Controller 或区域。区域是一组 Delivery Controller，通常代表某个地理位置的数据中心。资源域是在 Citrix Virtual Apps and Desktops 中定义的，在 StoreFront 中定义的任何资源域都必须与在 Citrix Virtual Apps and Desktops 中定义的资源域名称完全匹配。可以将一个最佳网关映射到多个区域，但您通常应使用一个区域。一个区域通常代表某个地理位置的一个数据中心。预期每个区域至少有一个最佳 Citrix Gateway，用于与该区域中的资源建立 HDX 连接。

有关区域的详细信息，请参阅区域。

使用场的示例场景

1 x UK 网关 -> 1 x UK StoreFront

- 英国本地的应用程序和桌面
- 仅用于英国故障转移的位于美国的应用程序和桌面

1 x US 网关 -> 1 x US StoreFront

- 美国本地的应用程序和桌面
- 仅用于美国故障转移的位于英国的应用程序和桌面

位于英国的网关使用位于英国的 StoreFront 提供对在英国托管的资源（例如应用程序和桌面）的远程访问。

位于英国的 StoreFront 在其 Delivery Controller 列表中同时定义了位于英国和位于美国的 Citrix Gateway 以及位于英国和美国的 Controller。UK 用户通过其地理位置布置的网关、StoreFront 和场访问远程资源。如果其 UK 资源不可用，作为临时故障转移备用方法，他们可以连接到 US 资源。

在未启用最佳网关路由的情况下，所有 ICA 启动都将通过创建启动请求的位于英国的网关传递，而不考虑资源所在的地理区域。默认情况下，创建启动请求时，创建请求的网关由 StoreFront 动态识别。最佳网关路由会覆盖此设置，并强制通过与提供应用程序和桌面的 US 场距离最近的网关建立 US 连接。

> 注意：
>
> 对于每个 StoreFront 应用商店，只能为每个站点映射一个最佳网关。

使用区域的示例场景

1 x CAMZone -> 2 x UK StoreFront

- 英国剑桥：应用程序和桌面
- 美国东部劳德代尔堡：应用程序和桌面
- 印度班加罗尔：应用程序和桌面

1 x FTLZone -> 2 x US StoreFront

- 美国东部劳德代尔堡：应用程序和桌面
- 英国剑桥：应用程序和桌面
- 印度班加罗尔：应用程序和桌面

1 x BGLZone -> 2 x IN StoreFront

- 印度班加罗尔：应用程序和桌面
- 英国剑桥：应用程序和桌面
- 美国东部劳德代尔堡：应用程序和桌面

图 1. 非最佳网关路由

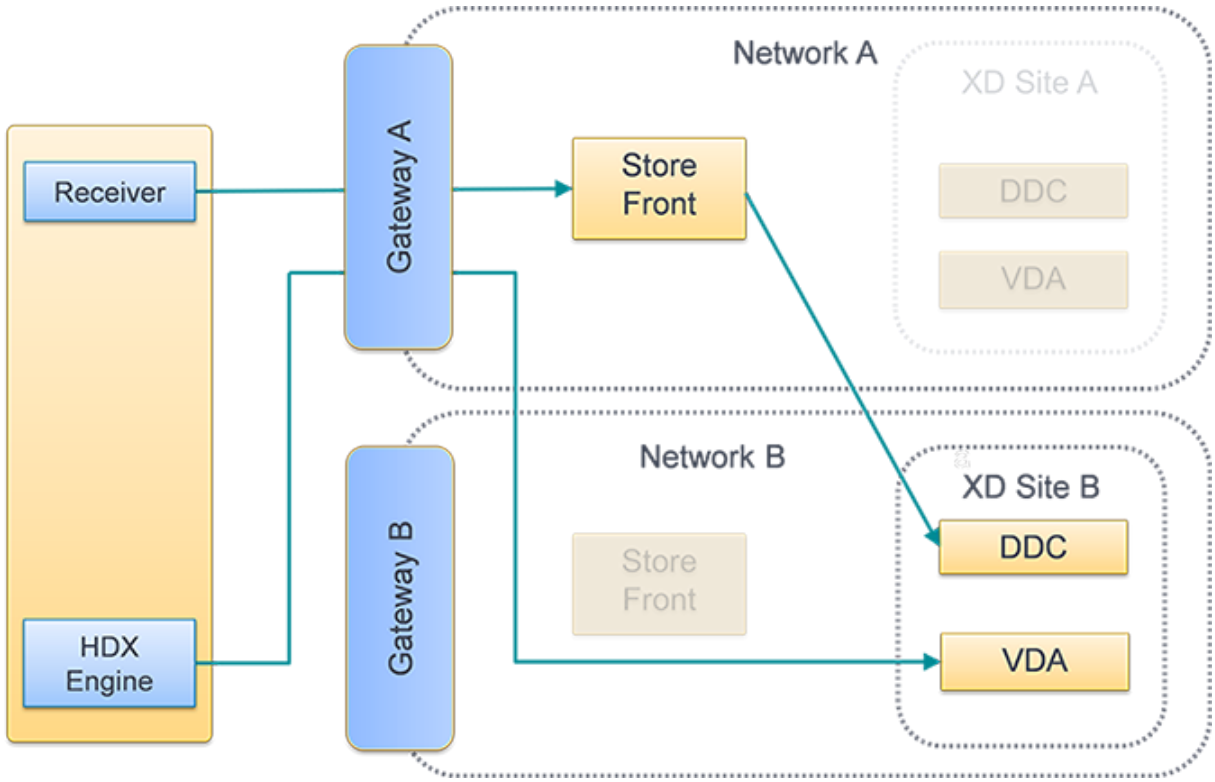
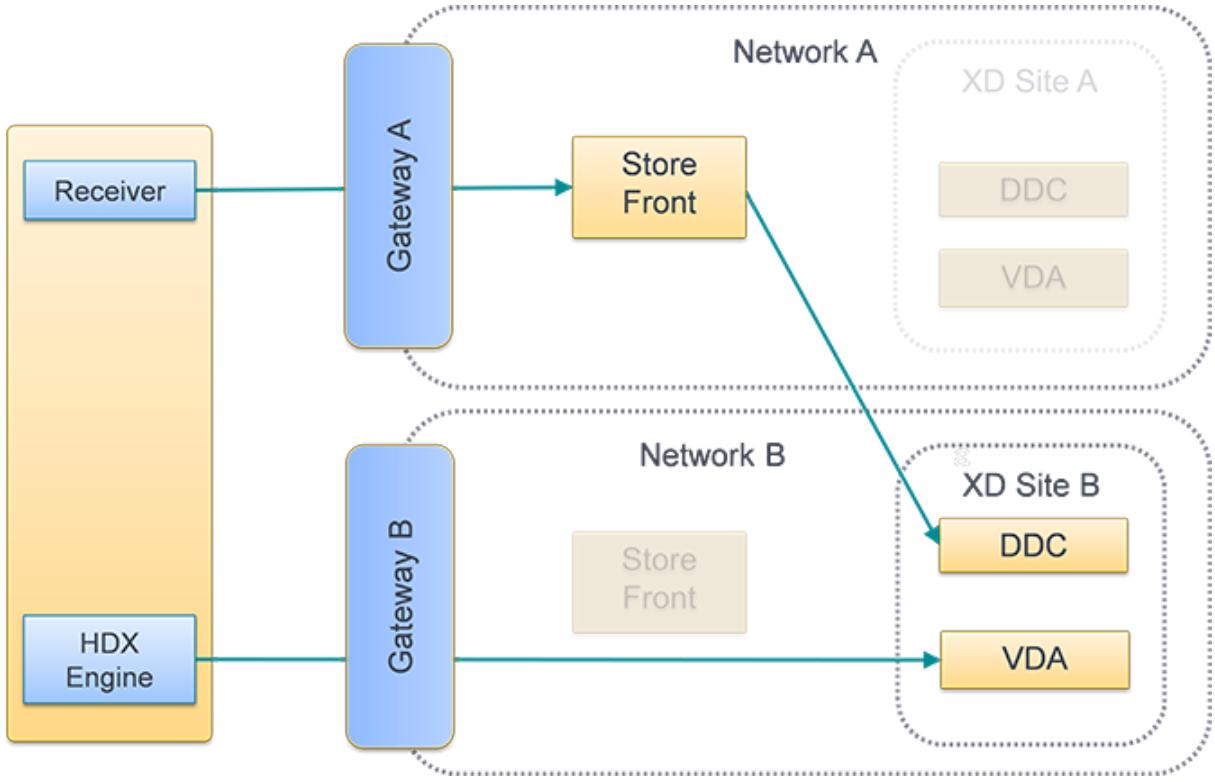


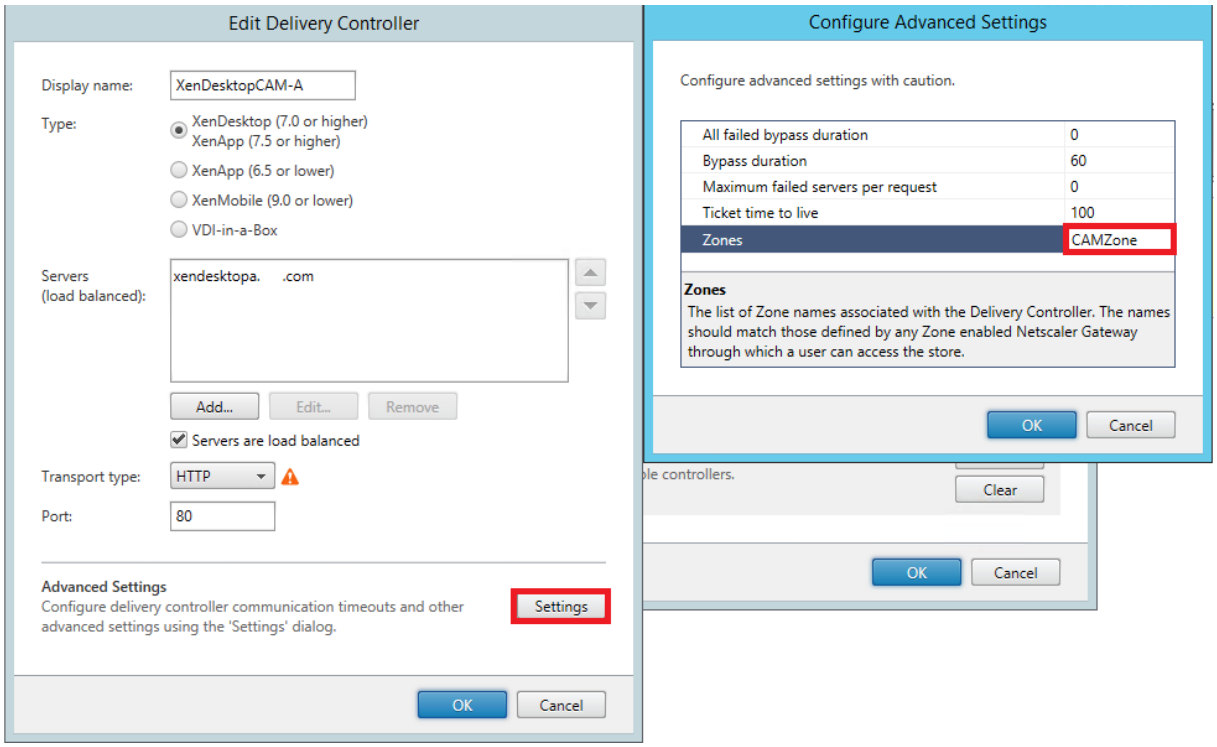
图 2. 最佳网关路由



将 **Delivery Controller** 放置到区域中

在要放置到区域中的每个 Delivery Controller 上设置区域属性。

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点，然后在操作窗格中单击管理 **Delivery Controller**。
2. 选择一个 Controller，单击编辑，然后单击编辑 **Delivery Controller** 屏幕上的设置。
3. 在区域行中，单击第二列。
4. 在 **Delivery Controller** 区域名称屏幕上单击添加，然后添加一个区域名称。

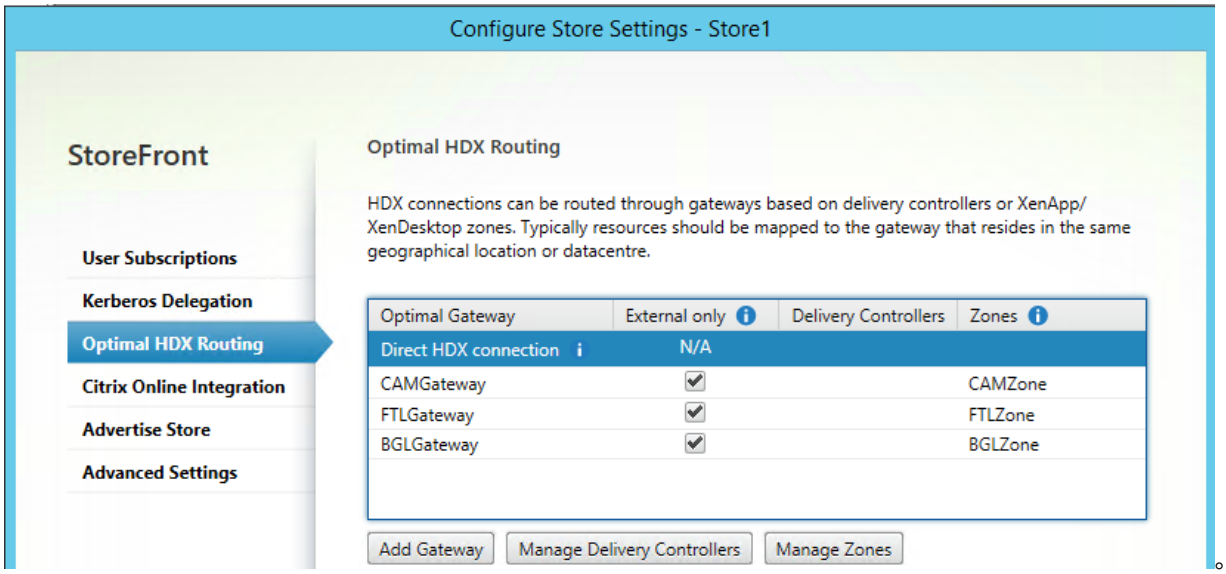


配置最佳 **HDX** 路由

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点，然后在结果窗格中选择一个应用商店。在操作窗格中，单击配置应用商店设置。
2. 选择最佳 **HDX** 路由选项卡。
3. 选择网关。
    a) 要在访问特定 Delivery Controller 中的资源时使用网关，请单击管理 **Delivery Controller**，然后勾选一个或多个 Delivery Controller
    b) 要在访问区域中的一组 Delivery Controller 中的资源时使用网关，请单击管理区域并输入一个或多个区域。
    c) 默认情况下，添加 Delivery Controller 或区域后，仅限外部处于勾选状态，这意味着 StoreFront 仅使用网关为通过网关连接到 StoreFront 的用户启动 StoreFront。如果您还希望使用网关为直接连接到

StoreFront 而无需通过网关连接的用户启动资源，请取消选中仅限外部。

4. 如果您希望始终不使用网关而是直接连接到某些资源，即使是通过网关远程访问 StoreFront 的用户，也请选择 **Direct HDX** 连接并选择一些 Delivery Controller 或区域。



使用 **PowerShell** 为应用商店配置最佳 **Citrix Gateway** 路由

- 要为应用商店配置最佳网关路由，请使用 Register-STFStoreOptimalLaunchGateway。
- 要删除应用商店的最佳网关路由，请使用 Unregister-STFStoreOptimalLaunchGateway。
- 要查看应用商店的最佳路由，请使用 Get-STFStoreRegisteredOptimalLaunchGateway。

订阅同步

April 17, 2024

StoreFront 会自动在 StoreFront 服务器组中的服务器之间同步订阅。如果您有多个服务器组（通常位于不同的地理位置），则可以配置来自不同 StoreFront 部署中的应用商店的用户订阅的定期拉取同步。这必须使用 PowerShell 来完成。

> 注意：
>
> StoreFront 和 PowerShell 控制台不能同时打开。使用 PowerShell 控制台管理 StoreFront 配置之前，请始终关闭 StoreFront 管理控制台。同样，打开 StoreFront 控制台之前，请关闭 PowerShell 的所有实例。

建立订阅同步时，请注意，必须在已同步应用商店（包括大小写）之间使用相同的名称命名配置的 Delivery Controller。Delivery Controller 名称未完全重复可能会导致用户在已同步的应用商店中具有不同的订阅。如果从聚合资源同步

订阅，两个应用商店使用的聚合组的名称也必须匹配。Delivery Controller 名称和聚合组名称区分大小写；例如，*CVAD_US* 与 *Cvad_Us* 不同。

1. 使用具有本地管理员权限的帐户启动 Windows PowerShell ISE。
2. 要配置同步，请使用 Publish-STFServerGroupConfiguration 命令。可以指定开始时间和重复时间间隔，也可以指定时间列表。例如，要在 08:00 开始同步，然后每隔 30 分钟同步一次：

```
Add-STFSubscriptionSynchronizationSchedule -RecurringStartTime
    08:00:00 -RecurringInterval 30
<!--NeedCopy-->
```

   我们建议您错开提取计划，以避免两个服务器组尝试同时从对方提取订阅数据。例如，每隔 60 分钟从每个服务器组提取数据的计划将按如下所示进行配置。服务器组 1 在 01:00、02:00 和 03:00 等从服务器组 2 中提取数据，依此类推。服务器组 2 在 01:30、02:30、03:30 等从服务器组 1 中提取数据。

3. 要指定包含要同步的应用商店的远程 StoreFront 部署，请键入以下命令。必须为 StoreFront 服务器组所在的每个数据中心配置此选项，以便其可以从其他远程数据中心提取订阅数据。请参阅以下美国和英国数据中心示例：

   - 在美国数据中心 StoreFront 服务器上运行，以从英国数据中心服务器提取数据：

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

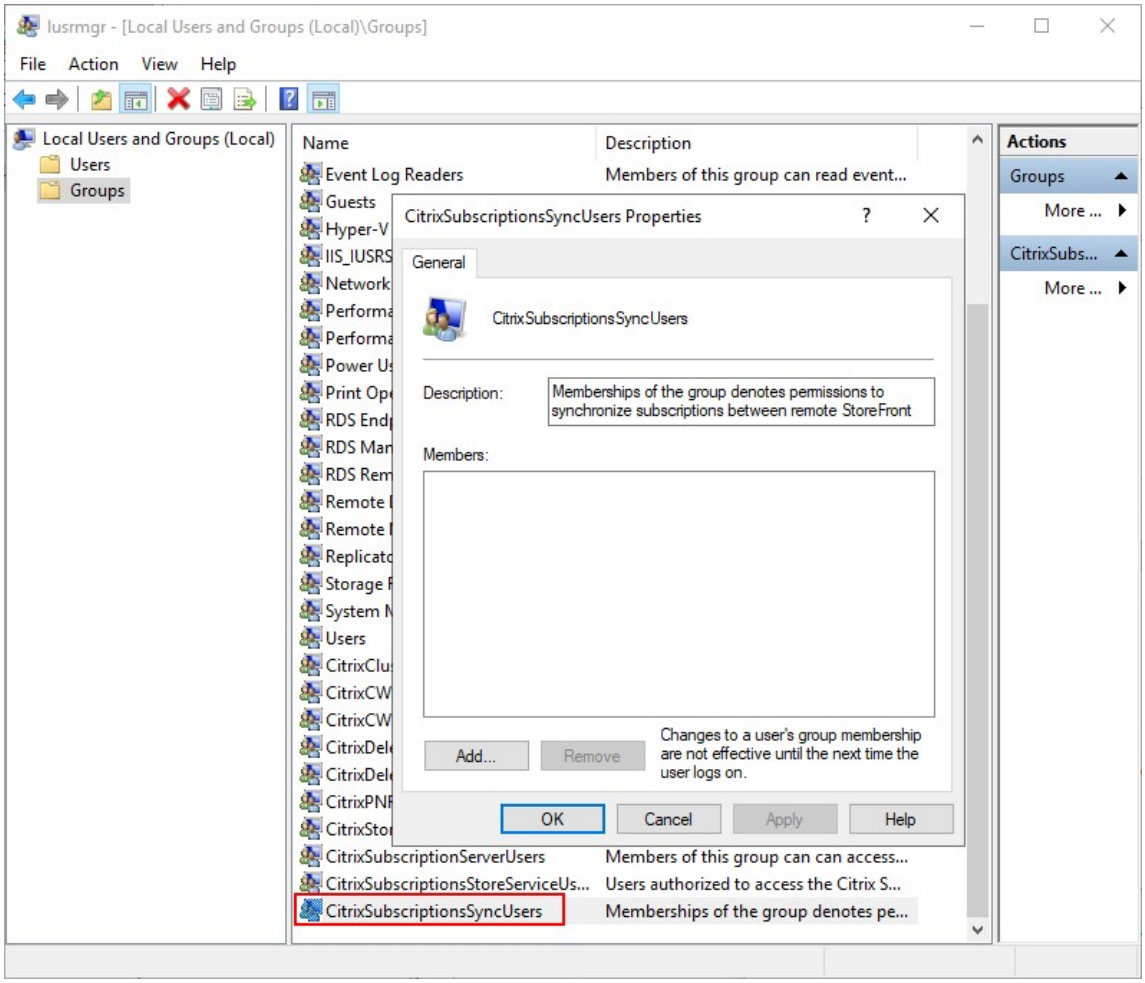
   - 在英国数据中心 StoreFront 服务器上运行，以从美国数据中心服务器提取数据：

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

   其中 *FriendlyName* 为一个帮助用户识别远程部署的名称，*RemoteStoreFrontAddress* 为远程部署的 StoreFront 服务器或负载平衡的服务器组的 FQDN。要在两个或多个应用商店之间同步应用程序订阅，要同步的所有应用商店在其各自的 StoreFront 部署中必须具有相同的名称。

4. 将远程部署中的每个 StoreFront 服务器的 Microsoft Active Directory 域计算机帐户添加到当前服务器上的本地 Windows 用户组 CitrixSubscriptionSyncUsers 中。

   这允许当前服务器在配置同步计划后从 CitrixSubscriptionSyncUsers 中列出的远程服务器中提取新的或更新的订阅数据。有关修改本地用户组的详细信息，请参阅 https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772524(v=ws.11)。



5. 按预期配置计划后，请使用 Citrix StoreFront 管理控制台或以下 PowerShell 将订阅同步计划和源传播到组中的所有其他服务器。

```
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

有关在多服务器 StoreFront 部署中传播更改的详细信息，请参阅配置服务器组。

6. 要删除现有订阅同步计划，请运行以下命令，然后将配置更改传播到部署中的其他 StoreFront 服务器。

```
Clear-STFSubscriptionSynchronizationSchedule
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

7. 要删除特定的订阅同步源，请运行以下命令，然后将配置更改传播到部署中的其他 StoreFront 服务器。

```
Remove-STFSubscriptionSynchronizationSource -FriendlyName "
    SyncFromUKStore"
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

8. 要删除所有现有的订阅同步源，请运行以下命令，然后将配置更改传播到部署中的其他 StoreFront 服务器。


```
Clear-STFSubscriptionSynchronizationSource
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

9. 要列出当前为您的 StoreFront 部署配置的订阅同步计划，请运行以下命令。

```
Get-STFSubscriptionSynchronizationSchedule
<!--NeedCopy-->
```

10. 要列出当前为您的 StoreFront 部署配置的订阅同步源，请运行以下命令。

```
Get-STFSubscriptionSynchronizationSource
<!--NeedCopy-->
```

配置会话设置

April 17, 2024

当用户启动应用程序时，StoreFront 会生成一个文档（称为 ica 文件），其中包含 Citrix Workspace 应用程序启动和配置该会话所需的所有设置。

在大多数情况下，建议使用 Citrix Virtual Apps and Desktops 策略或 Citrix DaaS 策略修改会话设置。但是，在某些情况下，覆盖特定应用商店的这些设置非常有用。如果应用商店聚合了来自多个站点的资源，并且您希望将相同的设置应用到该应用商店的所有资源，这可能非常有用。

要定义应用商店的会话设置，请执行以下任一操作：

- 使用 Global App Config Service。这是 Citrix Cloud 上的一项服务。有关详细信息，请参阅使用 Global App Configuration Service 配置 Citrix Workspace 应用程序。
- 在 StoreFront 服务器上，将设置添加到应用商店的 default.ica 文件中。

您可以在 StoreFront 服务器的 `\inetpub\wwwroot\Citrix\[StoreName]\App_Data` 目录中找到 default.ica。

有关可用设置的列表，请参阅 ICA 设置参考。某些设置全局应用。您还可以通过添加名称与在 Studio 中配置的应用程序名称完全匹配的部分来添加适用于特定应用程序的分区。

示例：在窗口化模式下启动记事本

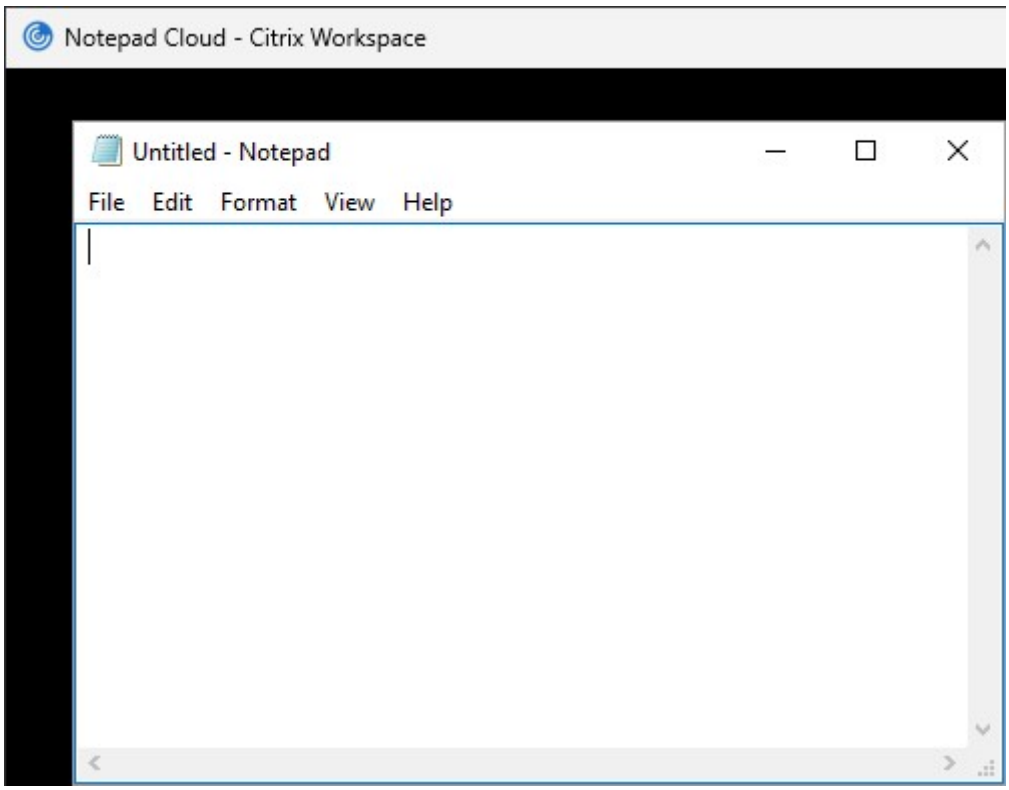
要将应用程序配置为在窗口化模式下启动，请在 default.ica 中为该应用程序添加一个包含以下设置的部分：

- TWIMode - 设置为“关”以启用窗口化模式。
- DesiredHRES - 可选的水平像素数。

- DesiredVRES - 可选的垂直像素数。

例如：

```
[Notepad]
TWIMode=Off
DesiredHRES=1024
DesiredVRES=768
<!--NeedCopy-->
```



ICA 文件签名

April 17, 2024

StoreFront 提供了对 ICA 文件进行数字签名的选项，以便支持此功能的 Citrix Workspace 应用程序版本能够验证文件是否来自可信来源。在 StoreFront 中启用文件签名功能后，系统将使用来自 StoreFront 服务器个人证书存储的证书对用户启动应用程序时生成的 ICA 文件进行签名。可以使用 StoreFront 服务器上运行的操作系统支持的任何哈希算法对 ICA 文件进行签名。不支持 ICA 文件签名服务功能或未配置为支持此功能的客户端将忽略数字签名。如果签名过程失败，生成的 ICA 文件将不带数字签名，并发送到 Citrix Workspace 应用程序，由 Citrix Workspace 应用程序的配置决定是否接受未签名的文件。

要通过 StoreFront 将证书用于 ICA 文件签名服务，该证书中必须包含私钥且处于允许的有效期内。如果证书中包含密

钥用法扩展，则此扩展必须允许将密钥用于数字签名。如果包含经过扩展的密钥用法扩展，则必须将其设置为支持代码签名或服务器身份验证。

对于 ICA 文件签名服务，Citrix 建议使用从公共证书颁发机构或贵组织的私有证书颁发机构获得的代码签名或 SSL 签名证书。如果无法从证书颁发机构获得恰当的证书，则可以使用现有 SSL 证书（例如服务器证书），或者创建一个新的根证书颁发机构证书并将其分发给用户设备。

默认情况下，ICA 文件签名服务在应用商店中处于禁用状态。要启用 ICA 文件签名服务功能，您需要编辑应用商店配置文件并执行 Windows PowerShell 命令。有关在适用于 Windows 的 Citrix Workspace 应用程序中启用 ICA 文件签名的详细信息，请参阅 ICA 文件签名。

> 注意：
>
> StoreFront 和 PowerShell 控制台不能同时打开。使用 PowerShell 控制台管理 StoreFront 配置之前，请始终关闭 StoreFront 管理控制台。同样，打开 StoreFront 控制台之前，请关闭 PowerShell 的所有实例。

1. 确保要用于对 ICA 文件进行签名的证书在 StoreFront 服务器上的 Citrix 交付服务证书存储中可用，而在当前用户的证书存储中不可用。
2. 使用 `Set-STFStoreService` PowerShell cmdlet 启用签名：

```
$storeService = Get-STFStoreService
Set-STFStoreService $storeService -IcaFileSigning $true -
    IcaFileSigningCertificateThumbprint [certificatethumbprint]
<!--NeedCopy-->
```

   其中 **[certificatethumbprint]** 是通过哈希算法生成的证书数据的摘要（或指纹）。

   如果您想使用 SHA-1 以外的哈希算法，请根据需要添加一个设置为 sha256、sha384 或 sha512 的参数 **IcaFileSigningHashAlgorithm**。

Citrix Workspace 应用程序配置

February 22, 2024

Global App Config Service

Global App Config Service 是一项用于管理 Citrix Workspace 应用程序配置的云服务。在您的 Citrix Cloud 帐户中，可以申领应用商店 URL 并为每个应用商店定义配置。有关更多详细信息，请参阅为本地应用商店配置设置。

应用商店帐户设置

作为 Global App Config Service 的替代方案，您可以通过应用商店帐户设置配置 Citrix Workspace 应用程序。当用户向本地安装的 Citrix Workspace 应用程序中添加应用商店时，它会检索 StoreFront 的应用商店帐户设置。这可

能包括配置属性，例如告知适用于 Windows 的 Citrix Workspace 应用程序是否应为应用程序创建开始菜单快捷方式。有关属性的详细信息，请参阅 Workspace 应用程序文档，例如使用 StoreFront 帐户设置自定义应用程序快捷方式的位置。

要修改这些设置，请执行以下操作：

1. 打开 `C:\inetpub\wwwroot\Citrix\Roaming` 中的 web.config 文件。
2. 在 `<Accounts>` 部分中，找到您希望更改的应用商店的元素 `<account ... name="Store"...>`。
3. 在 `Account` 部分下，找到 `<annotatedServices>/<annotatedServiceRecord>/<metadata>/<properties>` 部分。
4. 在 `<clear/>` 元素之后，在表单 `<property name="[name]"value="[value]"/>` 中添加属性。例如：

```
<properties>
    <clear/>
    <property name="PutShortcutsOnDesktop" value="true"/>
    <property name="DesktopDir" value="Citrix Applications"/>
</properties>
<!--NeedCopy-->
```

> 重要
>
> 在多服务器部署中，请一次仅使用一台服务器来更改服务器组的配置。确保 Citrix StoreFront 管理控制台未在部署中的任何其他服务器上运行。完成后，请将对配置所做的更改传播到服务器组，以便更新部署中的其他服务器。

Workspace 应用程序 Web 站点

要配置本地安装的 Citrix Workspace 应用程序使用的 Web 站点配置，请参阅配置 Workspace 应用程序 Web 站点。

管理 Web 站点

September 29, 2023

您可以为每个应用商店配置一个或多个 Web 站点，用户可以通过浏览器或 Citrix Workspace 应用程序访问这些站点。

使用 StoreFront 管理控制台可以执行以下任务：

任务	详细信息
创建 Web 站点	创建 Web 站点，使用户能够通过 Web 页面或 Workspace 应用程序访问应用商店。
配置 Web 站点	修改 Web 站点的设置。
删除 Web 站点	删除 Citrix Receiver for Web 站点。
配置 Workspace 应用程序 Web 站点	从 Citrix Workspace 应用程序内部选择要使用的 Web 站点。

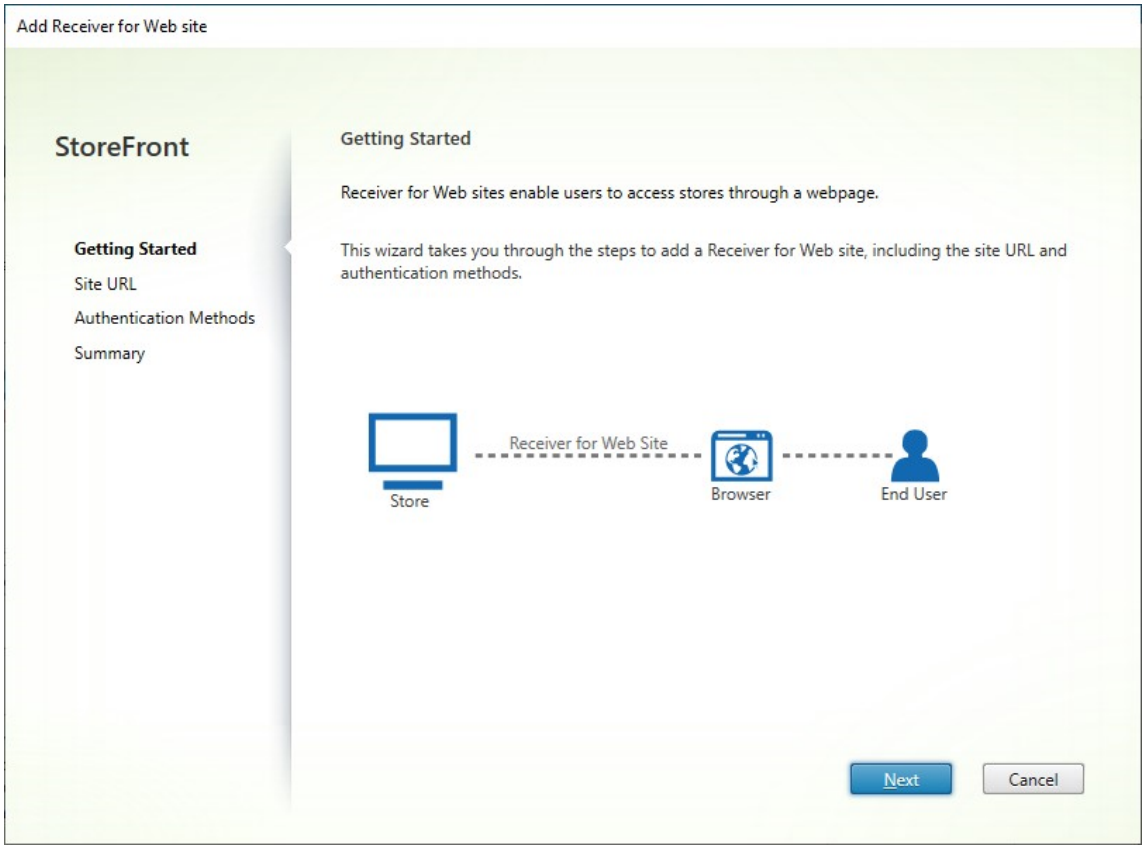
创建 **Web** 站点

April 17, 2024

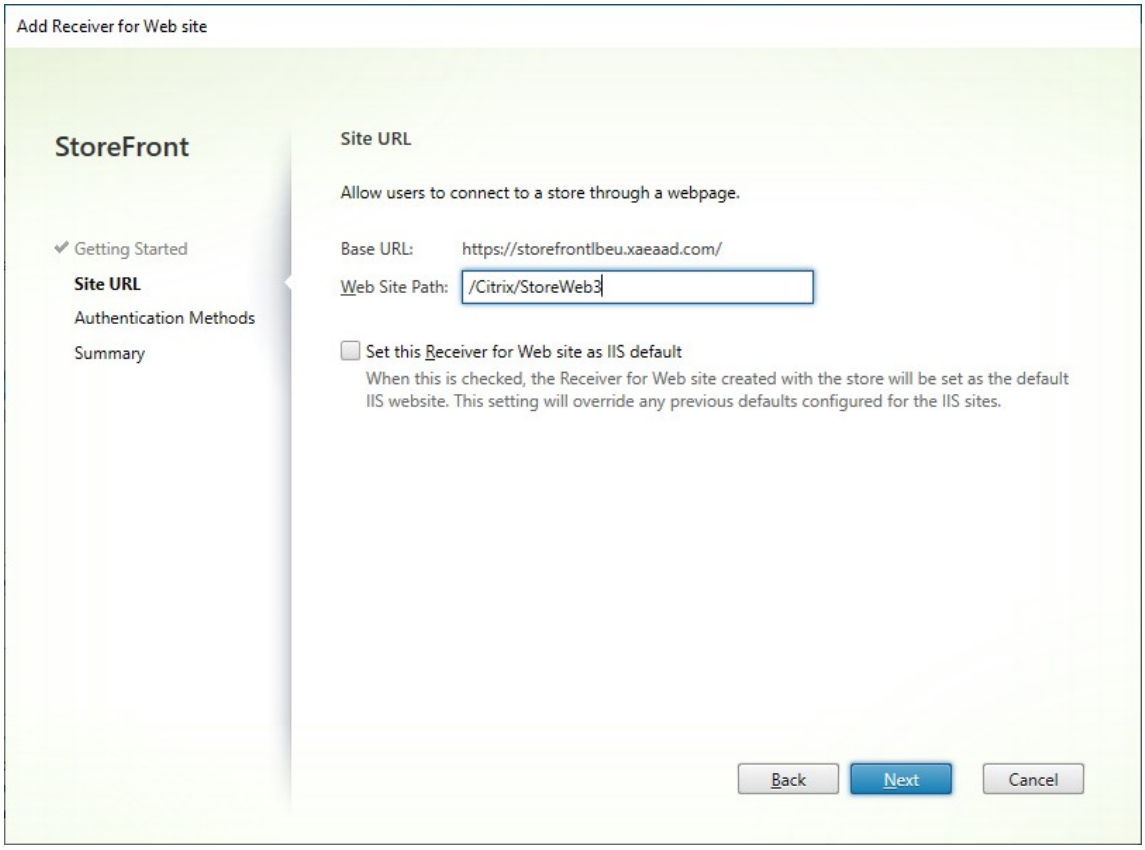
创建应用商店时，会自动为其创建 Web 站点。您可以向现有应用商店中添加其他 Web 站点。这允许您为用户提供具有不同配置的不同 URL。但是，由于 Citrix Workspace 应用程序配置为为一个应用商店使用一个特定的 Web 站点，因此只能通过 Web 浏览器访问多个 Web 站点，请参阅配置 Workspace 应用程序 Web 站点。

> 重要提示：
>
> 在多服务器部署中，请一次仅使用一台服务器以更改服务器组的配置。确保 Citrix StoreFront 管理控制台未在部署中的任何其他服务器上运行。完成后，请
> 将对配置所做的更改传播到服务器组，以便更新部署中的其他服务器。

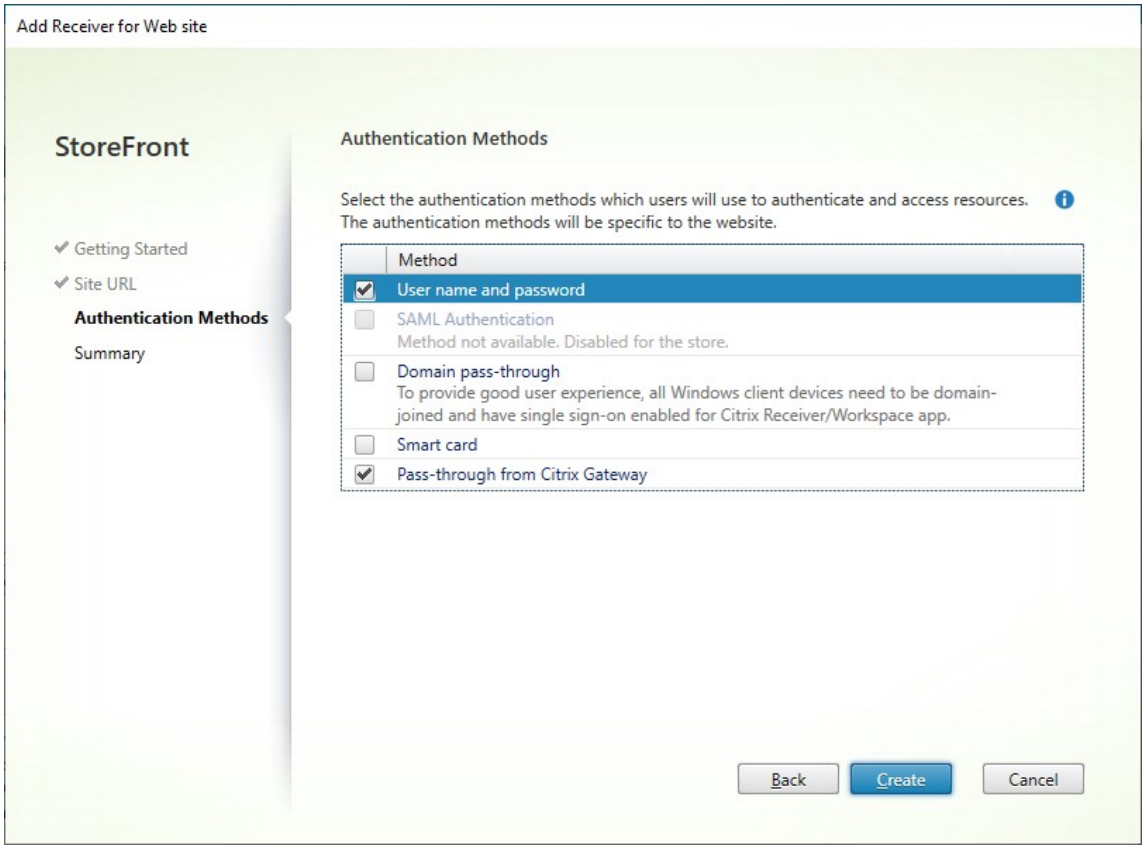
1. 在管理控制台中，选择要为其创建 Web 站点的应用商店，然后在“操作”窗格中单击管理 **Receiver for Web** 站点。
2. 单击添加，然后单击下一步。



3. 键入所需的 **Web** 站点路径，选择是否要将其作为基本 URL 的默认 Web 站点，然后单击下一步。



4. 勾选或取消选中所需的身份验证方法。有些方法只有在已经为应用商店配置后才可用。按下一步。



5. 创建了站点时，单击完成。
6. 选择新创建的站点，然后按编辑以根据需要配置您的 Web 站点，请参阅配置 Web 站点。

使用 **PowerShell SDK** 创建 **Web** 站点

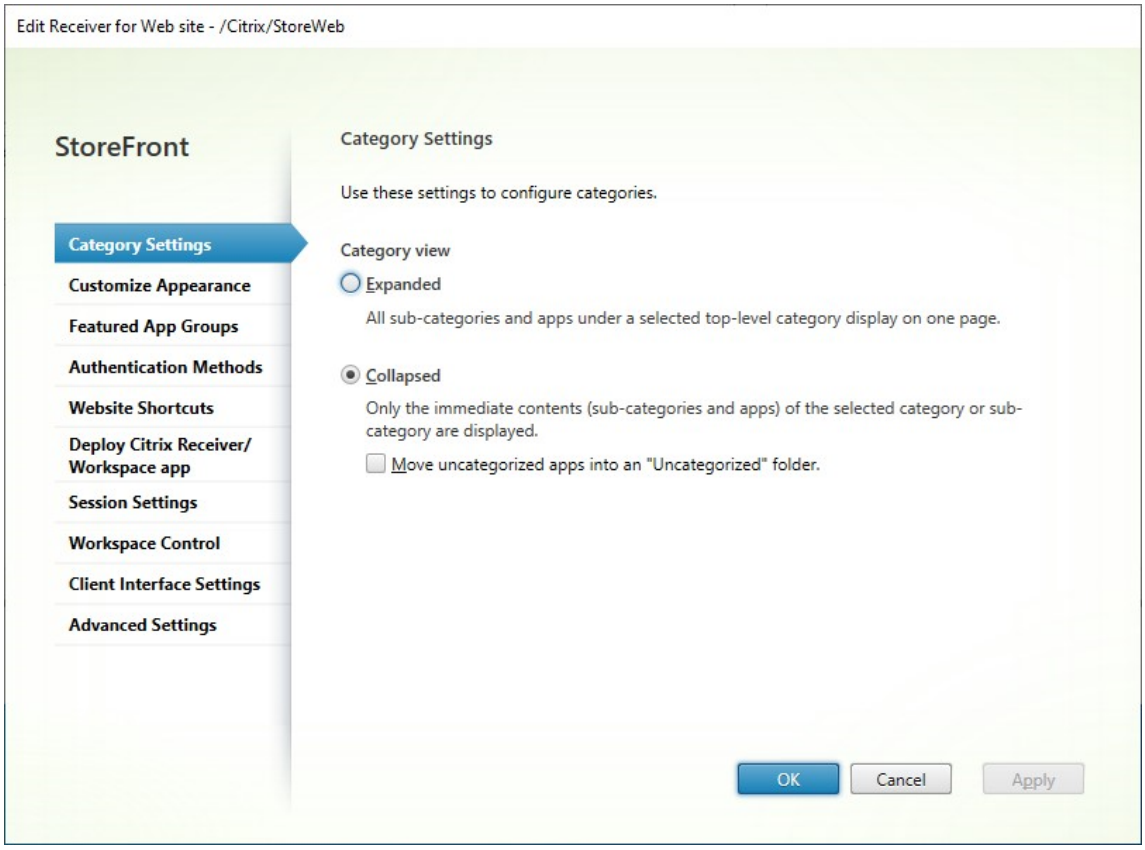
要使用 PowerShell SDK 创建 Web 站点，请调用 Add-STFWebReceiverService cmdlet。

配置 **Web** 站点

April 17, 2024

要配置 Web 站点，请执行以下操作：

1. 在左侧窗格中选择应用商店节点，在操作窗格中单击管理 **Receiver for Web** 站点。
2. 选择一个 Web 站点并按配置…



3. 修改相应选项卡上的设置。

   - 类别设置
   - 自定义外观
   - 精选应用程序组
   - 身份验证方法
   - Web 站点快捷方式
   - 部署 Citrix Receiver/Workspace 应用程序
   - 会话设置
   - 工作区控制
   - 客户端界面设置
   - 高级设置

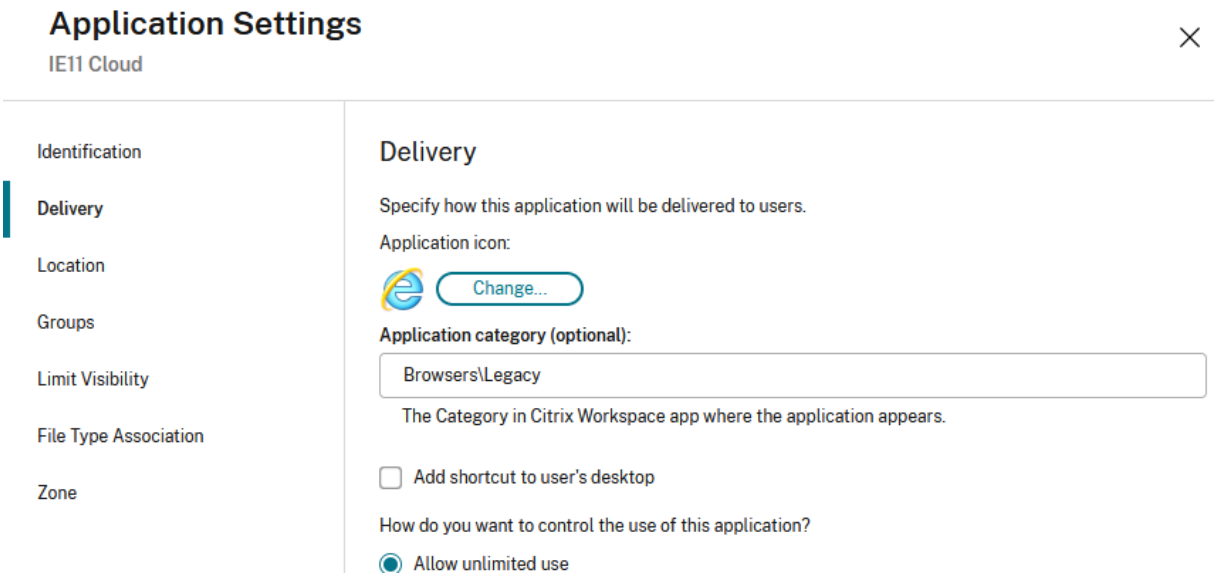
4. 完成您的更改后，单击确定。

> 重要提示：
>
> 在多服务器部署中，请一次仅使用一台服务器以更改服务器组的配置。确保 Citrix StoreFront 管理控制台未在部署中的任何其他服务器上运行。完成后，请
> 将对配置所做的更改传播到服务器组，以便更新部署中的其他服务器。

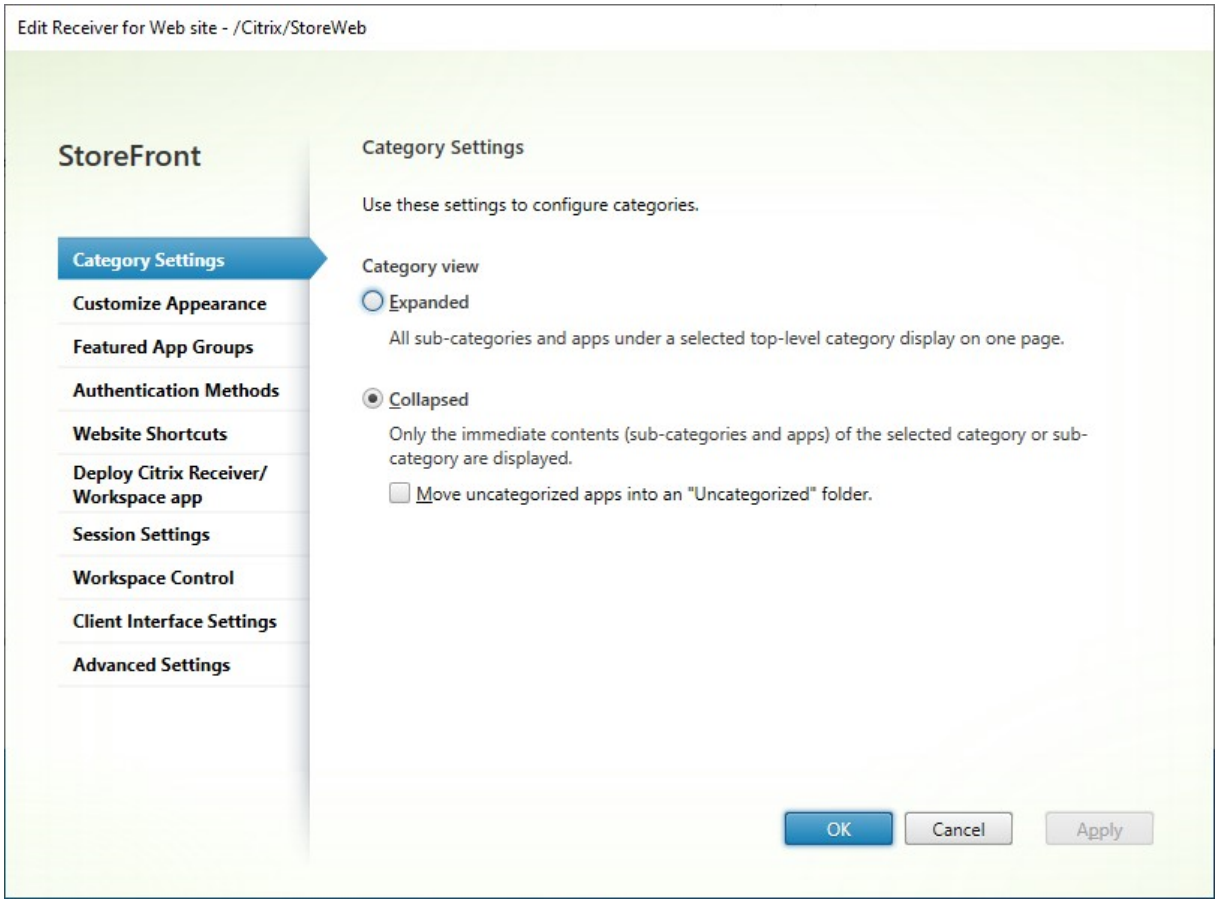
类别设置

April 17, 2024

在 Citrix Virtual Apps and Desktops 中，您可以按应用程序一文中的说明将每个应用程序分配到一个类别。使用 \ 符号创建类别的文件夹层次结构。在 StoreFront 中，您可以配置此文件夹层次结构的显示方式。



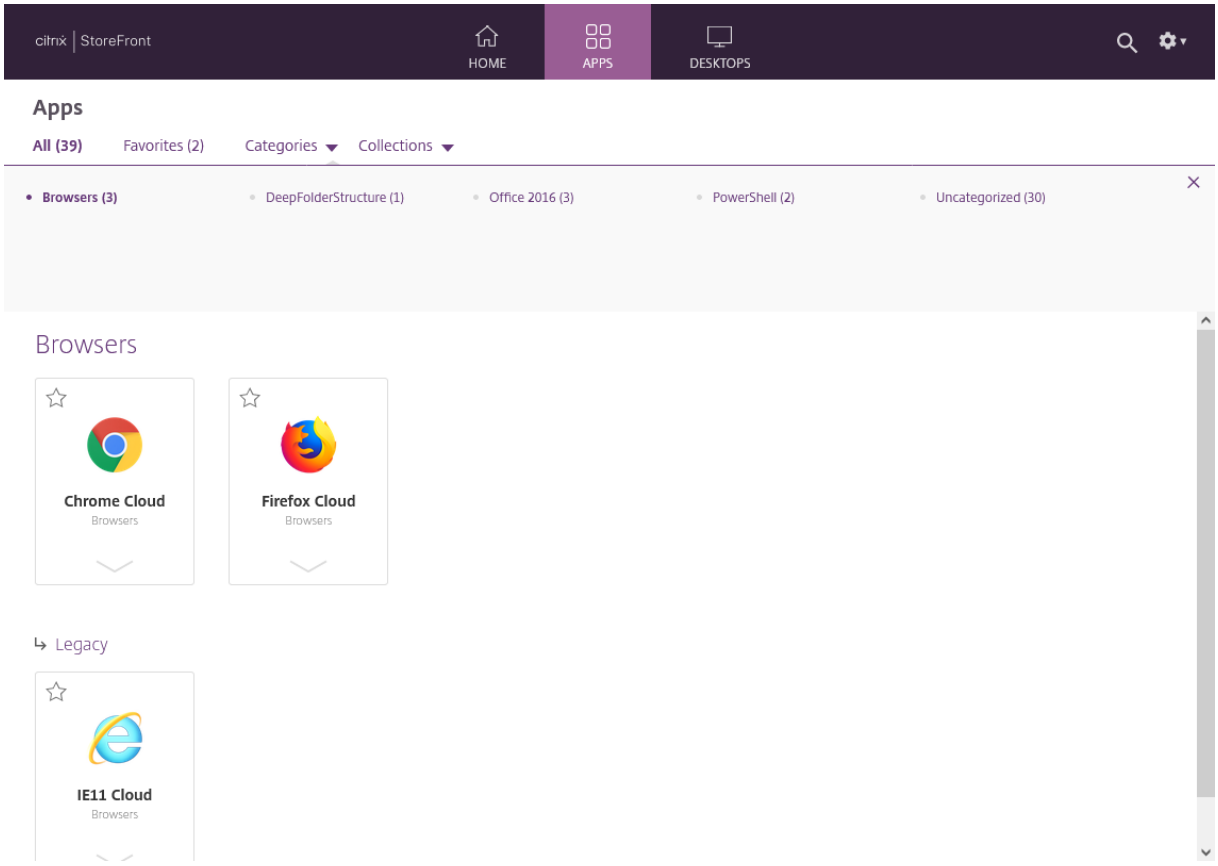
要修改类别设置，请转到编辑 Receiver for Web 站点，然后选择类别设置选项卡。



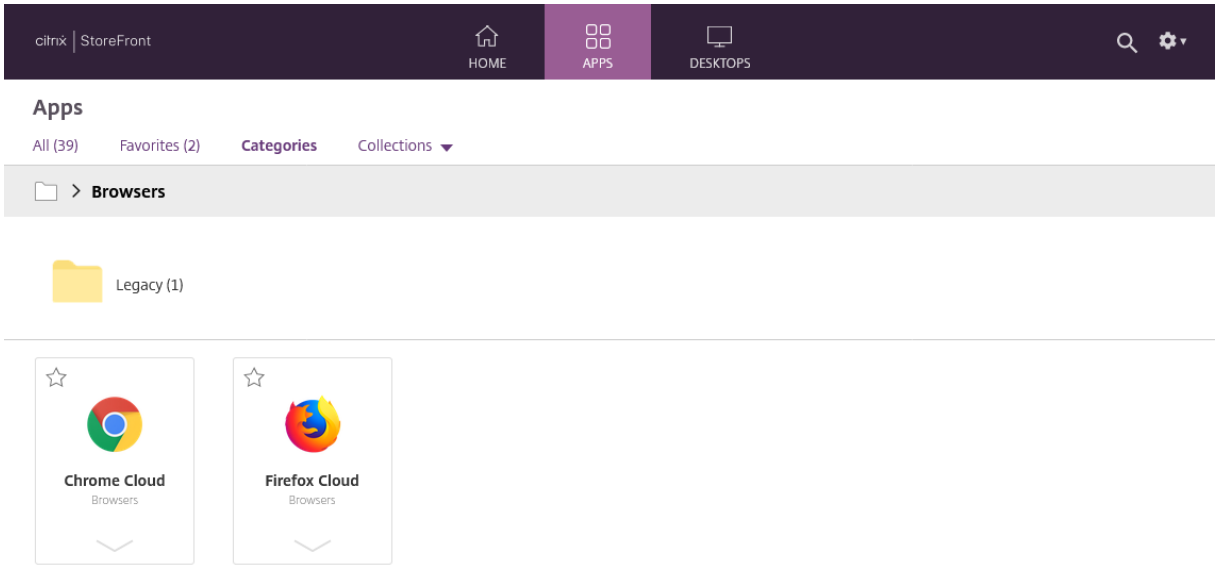
“类别”视图

在展开的视图中，StoreFront 显示顶层类别列表。当用户单击顶层类别时，StoreFront 将在一个页面上显示所有子类别中的所有应用程序。

例如，如果您有一个子类别为“Legacy”（旧版）的浏览器，它将在一个页面上显示所有浏览器，包括“旧版”下的浏览器：

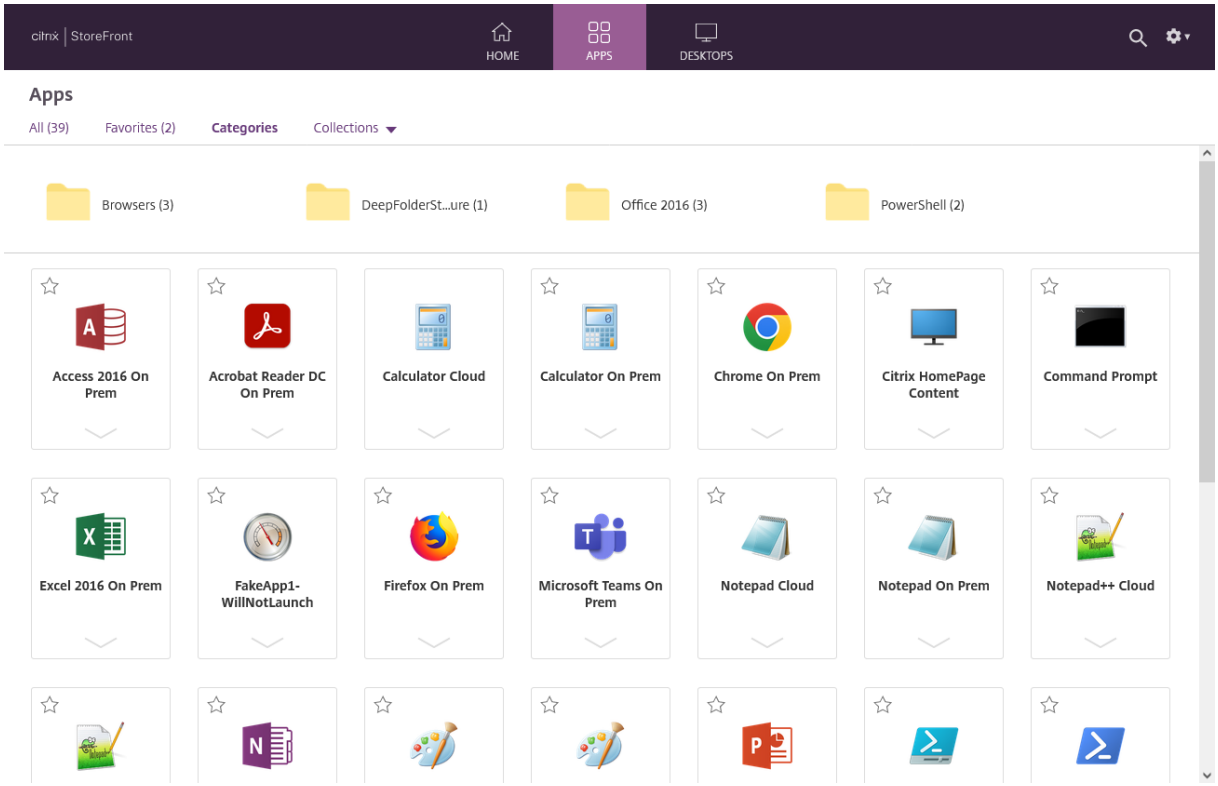


在折叠的视图中，StoreFront 最初显示顶层类别的列表，也可以显示所有未分类的应用程序。当用户单击某个类别时，StoreFront 仅显示所选类别的即时内容（子类别和应用程序）。用户可以单击每个子类别以展开内容。

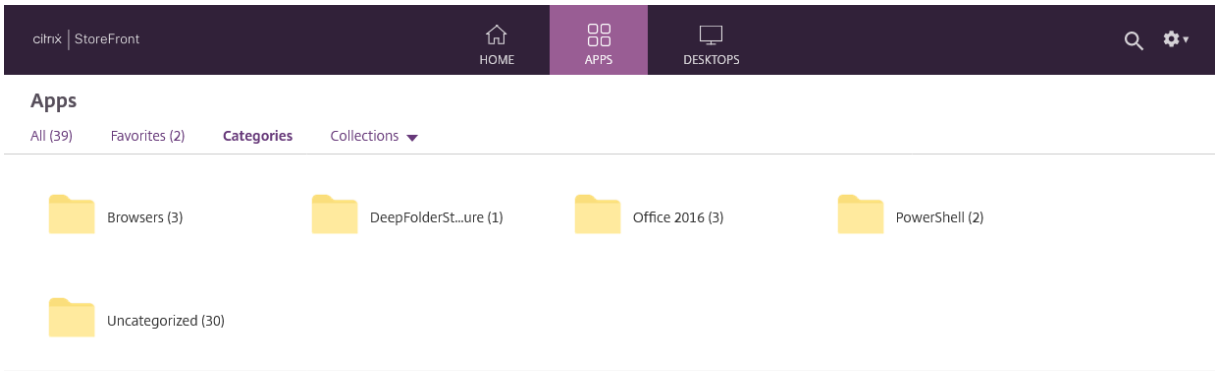


未分类的应用程序

在折叠的视图中，取消选中将未分类的应用程序移动到“未分类”文件夹中选项，以在初始视图中显示所有没有类别的应用程序和桌面。这种行为与早期版本的 StoreFront 类似。



在折叠的视图中，选中将未分类的应用程序移动到“未分类”文件夹中，将所有没有类别的应用程序和桌面移至单独的未分类文件夹。



使用 **PowerShell SDK** 配置类别设置

要使用 PowerShell SDK 启用或禁用类别视图，请调用带参数 `EnableAppsFolderView` 的 cmdlet Set-STFWebReceiverUserInterface。

要使用 PowerShell SDK 更改类别视图，请调用带参数 `CategoryViewCollapsed` 的 cmdlet Set-STFWebReceiverUserInterface。

自定义外观

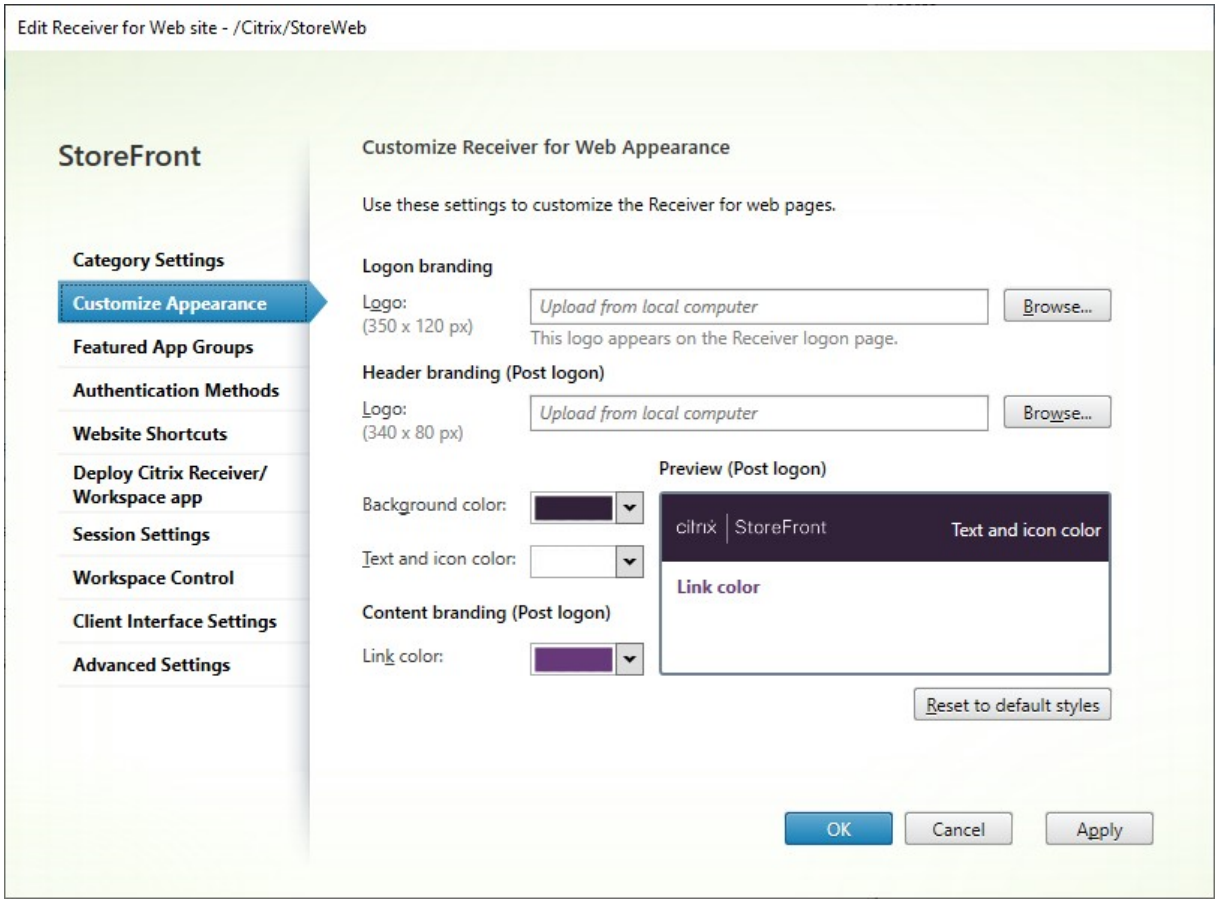
April 17, 2024

您可以修改应用商店 Web 站点内使用的徽标和颜色。

编辑徽标和颜色

要自定义外观，请转到编辑 Receiver for Web 站点，然后选择自定义外观选项卡。您可以修改以下内容：

- **Logon branding logo**（登录外观方案徽标）- 登录屏幕上显示的徽标。通过 Citrix Gateway 登录时不会显示该信息。按浏览…，然后选择类型为.jpg、.jpeg、.png、.png 或.bmp 的文件。建议您使用大小为 350 像素 x 120 像素的图像。
- 标头外观方案徽标。登录后显示在左上角的徽标。按浏览…，然后选择类型为.jpg、.jpeg、.png、.png 或.bmp 的文件。建议您使用大小为 340 像素 x 80 像素的图像。
- 背景色 - 页面顶部导航部分的背景色。
- 文本和图标颜色 - 页面顶部导航部分中的文本和图标颜色。
- 链接颜色 - 用于突出显示当前选定项目的颜色。



使用 **PowerShell SDK** 编辑徽标和颜色

使用 PowerShell SDK 调用 cmdlet Set-STFWebReceiverSiteStyle。

将外观重置为默认值

按重置为默认样式可将徽标和颜色恢复为默认样式。

使用 **PowerShell SDK** 将外观重置为默认值

使用 PowerShell SDK 调用 cmdlet Clear-STFWebReceiverSiteStyle。

使用 **JavaScript** 和 **CSS** 自定义

可以使用 StoreFront 客户端 UI 自定义 API 进一步自定义 Web 站点。

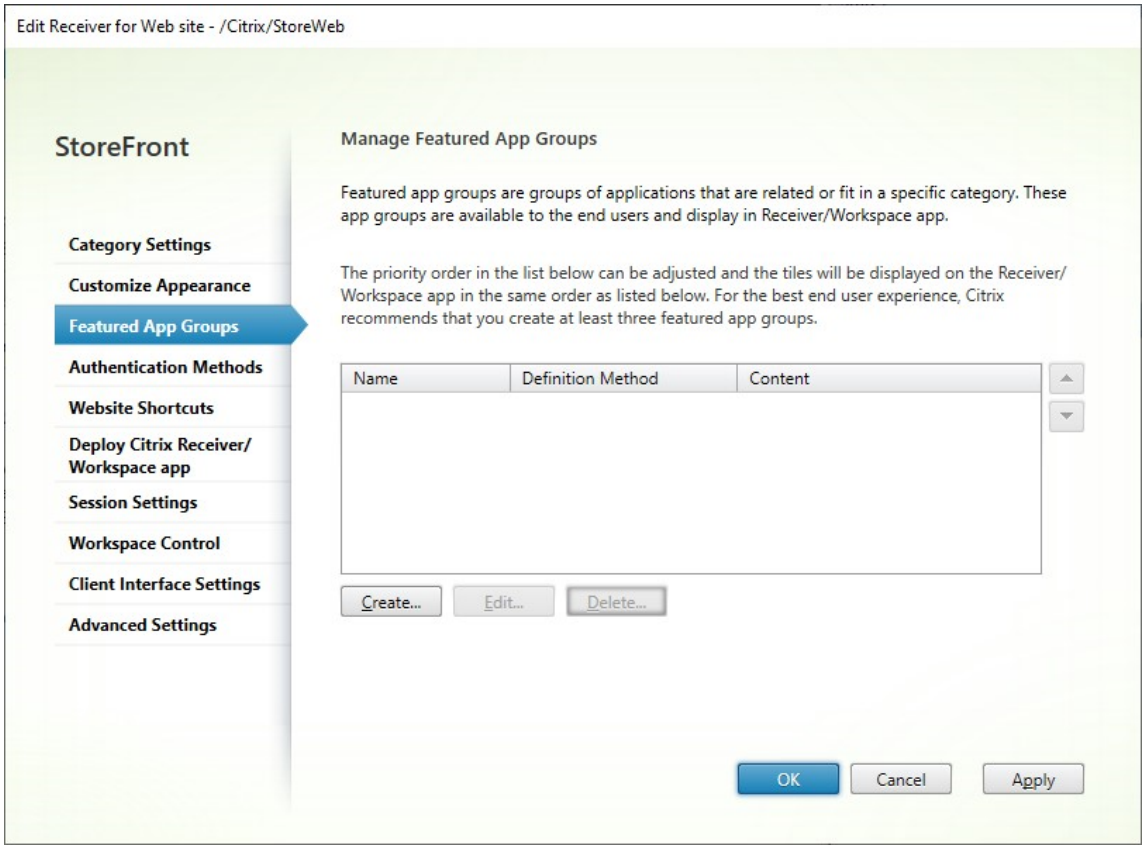
精选应用程序组

April 17, 2024

您可以为最终用户创建适合特定类别或与之相关的产品精选应用程序组。例如，您可以创建一个销售部门精选应用程序组，其中包含该部门使用的应用程序。您可以在 StoreFront 管理控制台中，通过使用应用程序名称或使用在 Studio 控制台中定义的关键字或应用程序类别来定义精选应用程序。

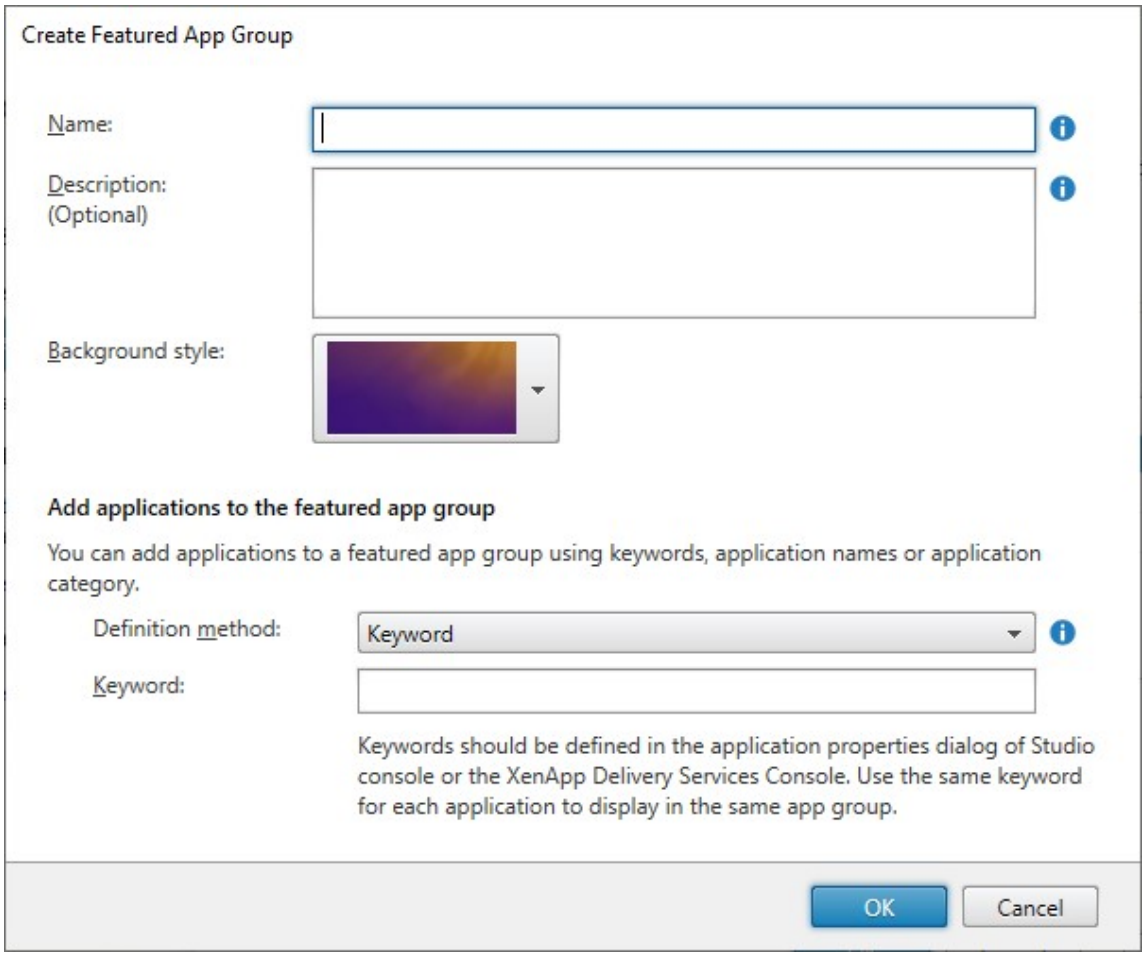
创建精选应用程序组

1. 在编辑 Receiver for Web 站点屏幕中，选择精选应用程序组选项卡。



2. 单击创建以定义新的精选应用程序组。
3. 指定精选应用程序组的名称、说明（可选）、背景和精选应用程序组的定义方法。您可以选择关键字、应用程序名称或应用程序类别。

选项	说明
关键字	根据关键字匹配应用程序，Studio 通过在应用程序的说明中包含关键字进行定义，例如“Use to send and receive emails KEYWORDS:collaboration”（用于发送和接收电子邮件 KEYWORDS:collaboration）
应用程序类别	匹配在 Studio 中输入的特定应用程序类别中的应用程序。
应用程序名称	使用应用程序名称定义精选应用程序组。所有与“创建精选应用程序组”对话框屏幕中包含的名称匹配的应用程序名称都包含在此精选应用程序组中。StoreFront 不支持在应用程序名称中使用通配符。匹配不区分大小写，但是采用全字匹配。例如，如果您键入 Excel，StoreFront 会匹配名称为 Microsoft Excel 2013 的已发布应用程序，但是键入 Exc 不匹配任何内容。

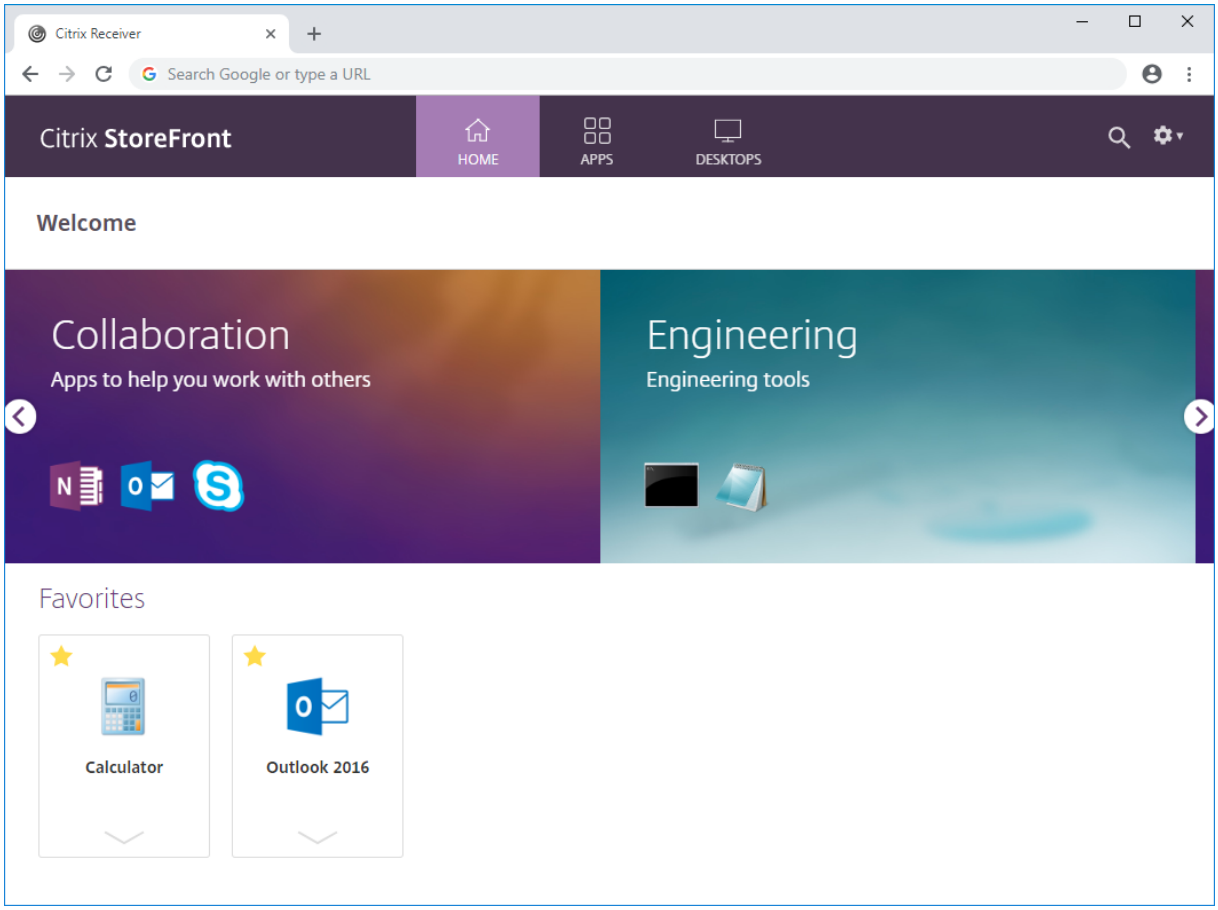


4. 单击 **OK**（确定）

示例：

我们创建了两个精选应用程序组：

- Collaboration（协作）- 通过匹配 Studio 中的 **Collaboration**（协作）类别中的应用程序创建的。
- Engineering（工程）- 通过为应用程序组命名并指定应用程序名称的集合创建的。



使用 **PowerShell SDK** 创建精选应用程序组

要使用 PowerShell SDK 添加功能应用程序组，请使用 cmdlet New-STFWebReceiverFeaturedAppGroup。

编辑精选应用程序组

在编辑 Receiver for Web 站点屏幕中，选择精选应用程序组选项卡。选择要编辑的组，然后单击编辑…

使用 **PowerShell SDK** 编辑精选应用程序组

要使用 PowerShell SDK 修改功能应用程序组，请使用 cmdlet Set-STFWebReceiverFeaturedAppGroup。

删除精选应用程序组

在编辑 Receiver for Web 站点屏幕中，选择精选应用程序组选项卡。选择要编辑的组，然后单击删除…

使用 **PowerShell SDK** 删除精选应用程序组

使用 PowerShell SDK 时，要删除功能应用程序组，请使用 cmdlet Remove-STFWebReceiverFeaturedAppGroup，要删除所有精选应用程序组，请使用 cmdlet Clear-STFWebReceiverFeaturedAppGroup。

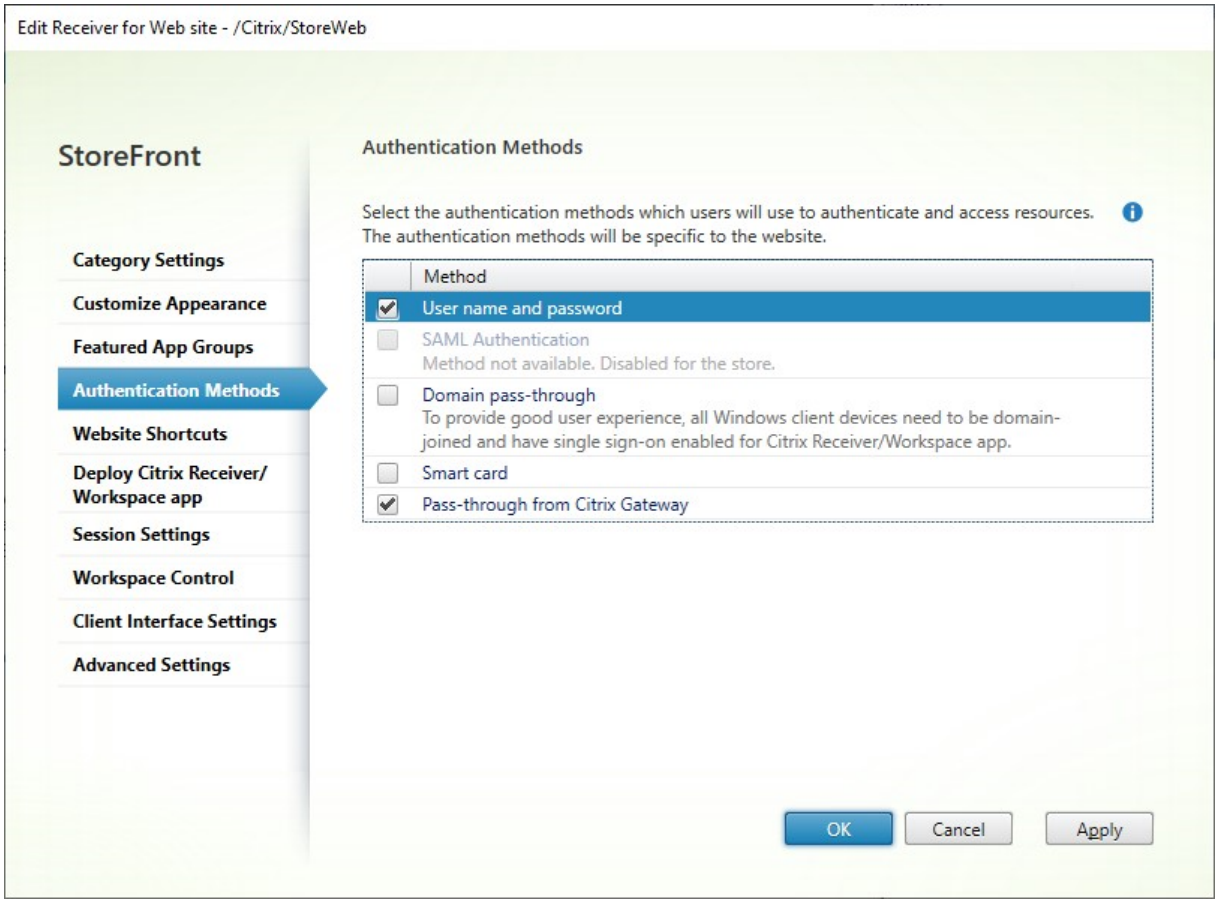
身份验证方法

April 17, 2024

要配置应用商店可用的身份验证方法，请参阅配置身份验证。您可以为特定的 Web 站点替换其中一些设置。这些替代仅在通过 Web 浏览器使用 HTML5 版 Citrix Workspace 应用程序时适用。本地安装的 Citrix Workspace 应用程序使用应用商店中的设置，而非 Web 站点上的设置。

> 警告：
> 每当您更改应用商店的身份验证方法时，都会覆盖该应用商店的所有 Web 站点的设置，因此必须重新应用任何更改。

要修改身份验证方法，请转到编辑 Receiver for Web 站点，然后选择身份验证方法选项卡。



- 选中用户名和密码复选框可启用显式身份验证。请参阅用户名和密码身份验证。此选项仅在为应用商店启用后才可用。
- 选择 **SAML** 身份验证复选框以支持与 SAML 身份提供程序的集成。请参阅 SAML 身份验证。此选项仅在已经为应用商店启用后才可用。
- 选中域直通以启用从用户设备直通 Active Directory 域凭据。请参阅域直通身份验证。此选项仅在已经为应用商店启用后才可用。
- 选中智能卡以启用智能卡身份验证。请参阅智能卡身份验证。
- 选择从 **Citrix Gateway** 直通以启用从 Citrix Gateway 直通身份验证。如果用户通过启用了身份验证的 Citrix Gateway 连接到 StoreFront，请启用此选项。请参阅从 Citrix Gateway 直通。

使用 **PowerShell SDK** 进行配置

要使用 PowerShell SDK 配置可用的身份验证方法，请使用 cmdlet Set-STFWebReceiverAuthenticationMethods。

Web 站点快捷方式

April 17, 2024

使用 Web 站点快捷方式可以向用户提供从内部网络中托管的可信 Web 站点快速访问桌面和应用程序的功能。生成可通过 Citrix Receiver for Web 站点访问的资源的 URL，然后将这些链接嵌入到您的 Web 站点中。用户单击某个链接时会重定向到 Receiver for Web 站点，如果用户尚未登录，可以在该站点登录。Receiver for Web 站点会自动启动资源。对于应用程序，如果用户之前未订阅应用程序，则会进行订阅。

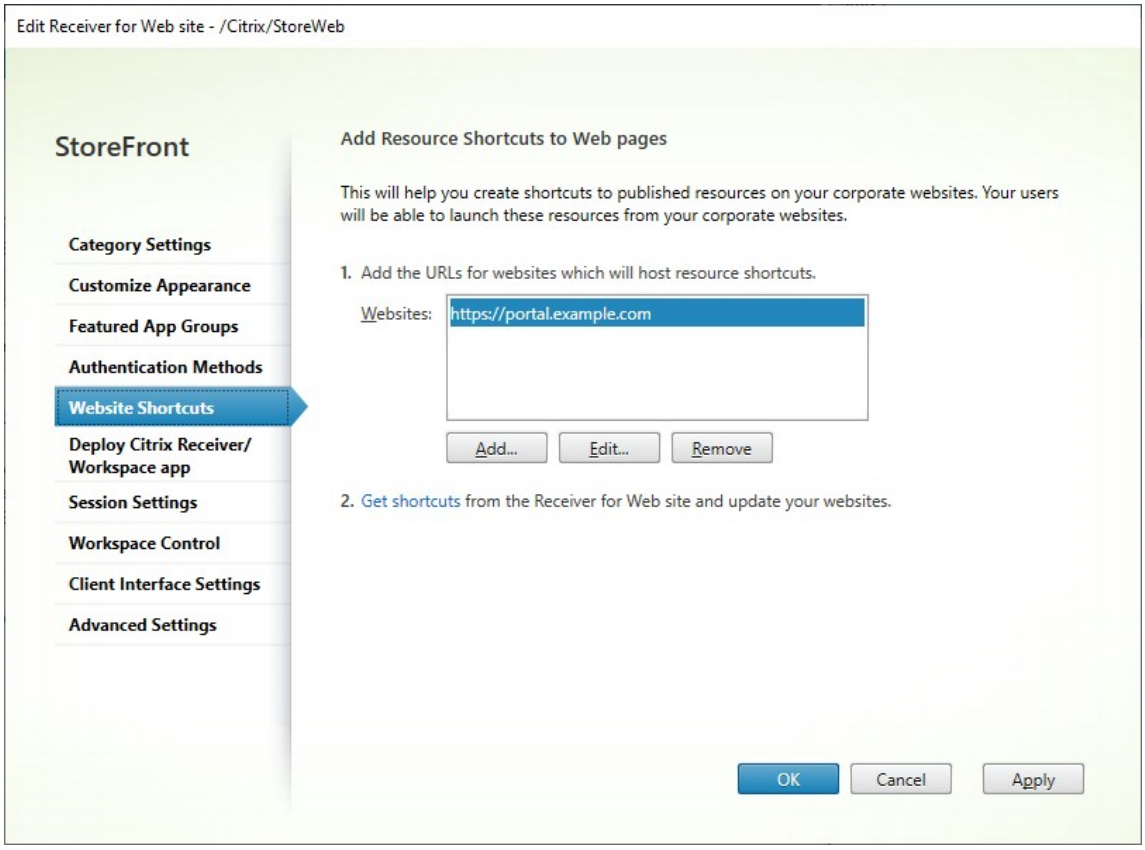
在生成资源快捷方式之前，必须使用 Citrix StoreFront 管理控制台或 PowerShell 将主机 Web 站点的 URL 添加到可信 *URL* 列表中。

默认情况下，如果用户尝试从不受信任的 Web 站点启动资源快捷方式，StoreFront 会警告用户，但用户仍然可以选择启动资源。要停止显示这些警告，请在“应用商店”窗格中单击管理 **Receiver for Web** 站点 **>** 单击配置 **>** 选择高级设置 **>** 取消选择提示快捷方式不受信任选项。

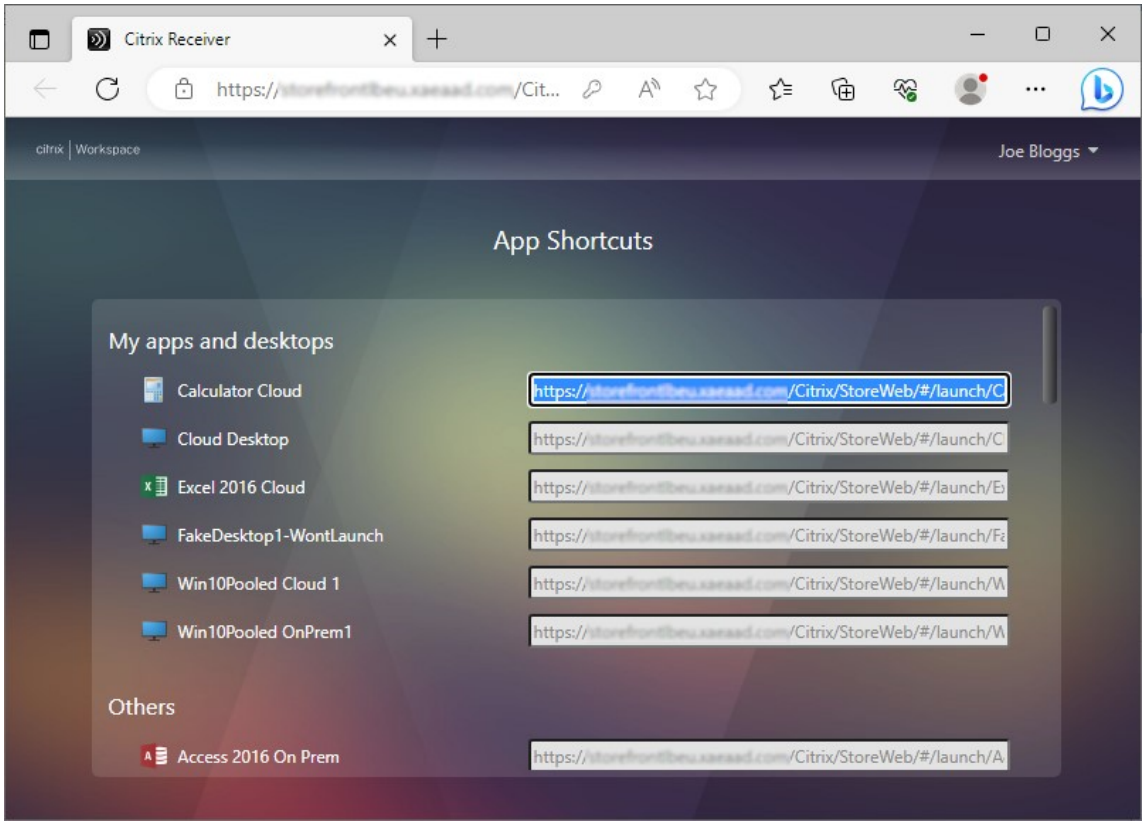
出于安全原因，Internet Explorer 可能会提示用户确认是否要启动通过快捷方式访问的资源。请指示您的用户在 Internet Explorer 中将 StoreFront 服务器 FQDN 添加到“本地 Intranet”或“可信站点”区域，以避免出现此额外步骤。

使用管理控制台添加可信 Web 站点

1. 在编辑 Receiver for Web 站点屏幕中，选择 **Web** 站点快捷方式选项卡。



2. 单击添加输入计划用于托管快捷方式的 Web 站点的 URL。URL 必须以 *http[s]://hostname[:port]* 形式指定，其中 hostname 是 Web 站点主机的完全限定域名，port 是在协议的默认端口不可用时用来与主机通信的端口。Web 站点上特定页面的路径不是必填项。要修改 URL，请在 Web 站点列表中选择相应的条目，然后单击编辑。对于不再希望用来托管 Citrix Receiver for Web 站点所提供资源的快捷方式的 Web 站点，可在列表中选择其对应的条目，然后单击删除以删除该 Web 站点的 URL。
3. 单击 **Get shortcuts**（获取快捷方式），然后复制您的 Web 站点所需的 URL。



使用 **PowerShell SDK** 添加可信 **Web** 站点

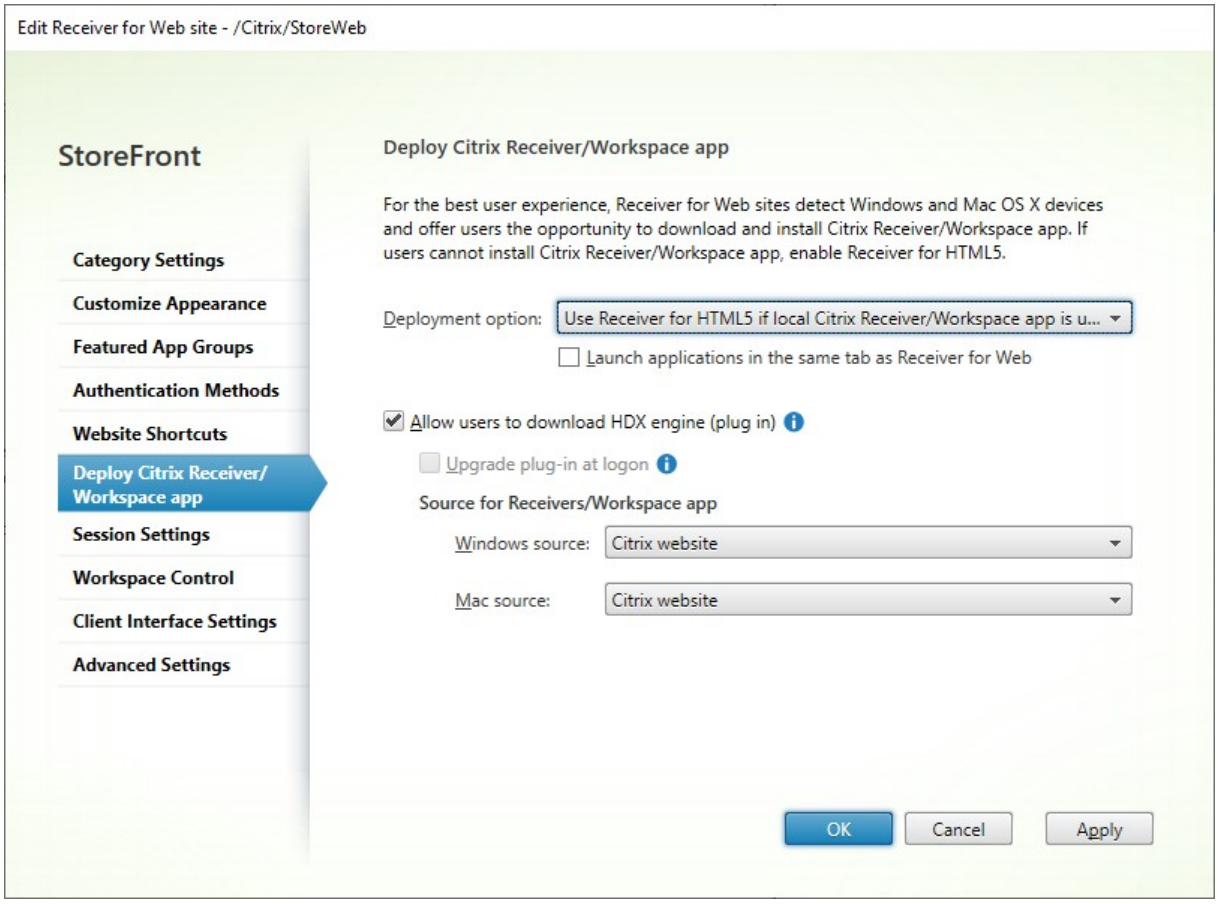
可以使用 Set-STFWebReceiverApplicationShortcuts PowerShell cmdlet 添加可信 URL。

Citrix Workspace 应用程序部署

April 17, 2024

默认情况下，当用户首次在 Windows、macOS 或 Linux 上使用 Web 浏览器浏览到应用商店时，StoreFront 会自动尝试确定是否已在本地安装 Citrix Workspace 应用程序。

如果检测不到本地部署的 Citrix Workspace 应用程序，则会提示用户下载并安装该应用程序。默认下载位置为 Citrix Web 站点，但您也可以在 StoreFront 服务器或其他位置托管安装程序。无法在本地安装 Citrix Workspace 应用程序的用户可以通过其 Web 浏览器使用适用于 HTML5 的 Citrix Workspace 应用程序。



要修改部署选项，请转到编辑 Receiver for Web 站点，然后选择部署 **Citrix Receiver/Workspace** 应用程序选项卡。

部署选项

- 如果您希望用户始终通过 Web 浏览器访问资源而不提示用户在本地下载并安装 Citrix Workspace 应用程序，请选择始终使用 **Receiver for HTML5**。选择此选项后，适用于 HTML5 的 Workspace 用户始终直接通过自己的浏览器访问资源。
- 如果您希望应用商店 Web 站点提示用户在本地下载并安装 Citrix Workspace 应用程序，但在无法安装 Citrix Workspace 应用程序时回退以通过浏览器访问资源，请选择如果本地 **Receiver** 不可用，则使用 **Receiver for HTML5**。对于未安装 Citrix Workspace 应用程序的用户，每当其登录站点时，都会提示其下载并安装 Citrix Workspace 应用程序。
- 如果希望站点始终通过本地安装的 Citrix Workspace 应用程序访问资源，请选择本地安装。系统会提示用户下载并安装适合其平台的 Citrix Workspace 应用程序。用户可以继续通过 Web 浏览器访问应用商店，但是当启动资源时，它会在本地安装的 Workspace 应用程序中打开。

在同一个选项卡中启动应用程序

如果您选择了始终使用 **Receiver for HTML5** 或如果本地 **Receiver** 不可用，则使用 **Receiver for HTML5**，默认情况下，在浏览器中启动的资源会打开一个新浏览器选项卡。如果您希望在同一个选项卡中打开资源，替换适用于 HTML5 的 Workspace 应用程序，请选择在与 **Receiver for Web** 相同的选项卡中启动应用程序。

允许用户下载适用于 **Windows** 或 **Mac** 的 **Citrix Workspace** 应用程序

如果您选择本地安装或如果本地 **Receiver** 不可用，则使用 **Receiver for HTML5** 并启用了允许用户下载 **HDX Engine (**插件**)**，当适用于 HTML5 的 Workspace 应用程序未检测到本地安装的 Workspace 应用程序时，用户可以选择下载适用于 Windows 或 Mac 的 Citrix Workspace 应用程序。

登录时升级 **Workspace** 应用程序

如果选择登录时升级插件，适用于 HTML5 的 Workspace 应用程序将在用户登录时提供用于升级本地安装的 Citrix Workspace 应用程序客户端的选项。用户可以选择跳过升级，但除非清除其浏览器 cookie，否则不会再次提示用户升级。要启用此功能，请确保 StoreFront 服务器上存在可用的 Citrix Workspace 应用程序文件。

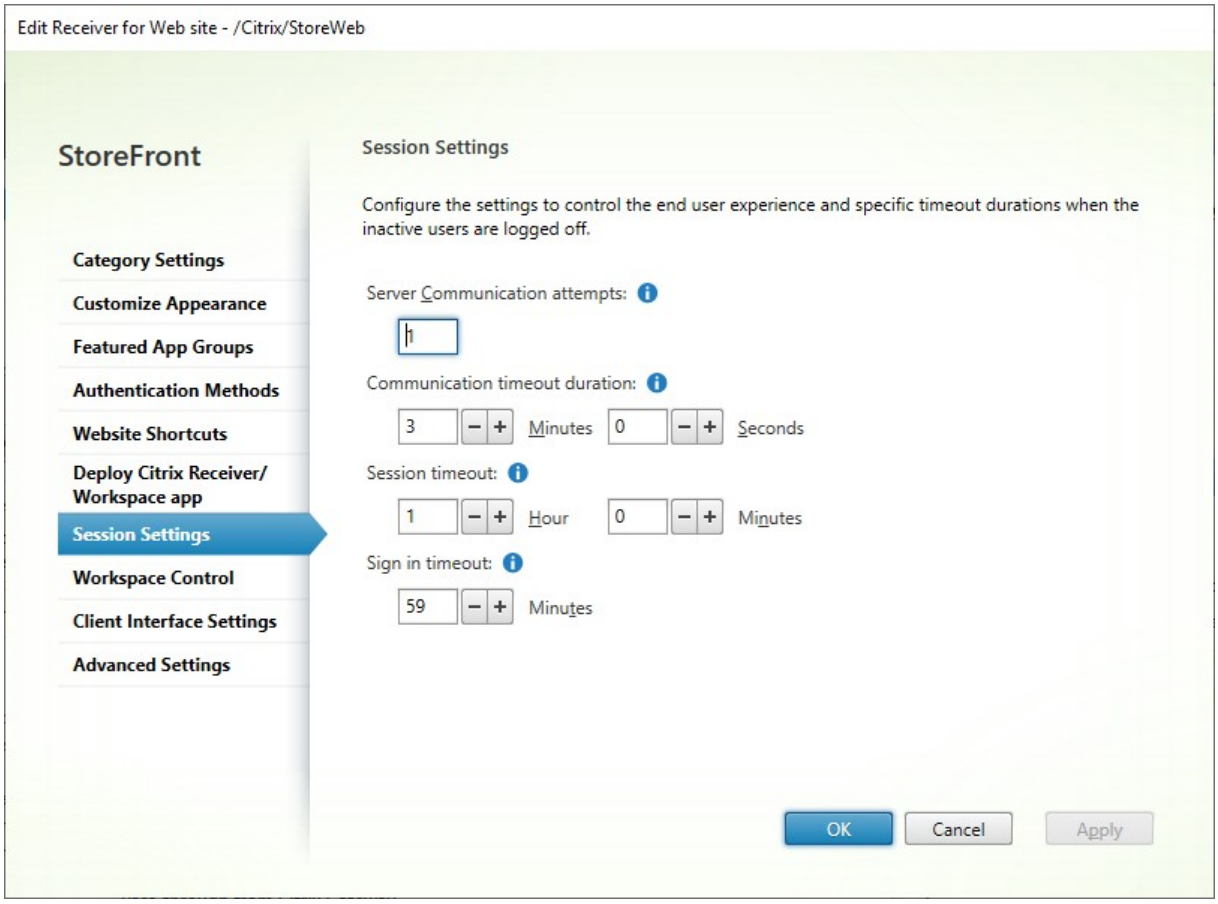
下载源

当最终用户单击下载按钮时，您可以选择将其重定向到 Citrix Web 站点还是直接从服务器下载文件。您可以选择 **Citrix Web** 站点、**StoreFront** 服务器上的本地文件或远程服务器上的文件 **(**通过 **URL)**。

配置会话设置

April 17, 2024

要修改会话设置，请转到编辑 Receiver for Web 站点屏幕，选择会话设置选项卡。



服务器通信尝试次数

在 Web 代理与应用商店服务之间尝试调用的次数，位于 StoreFront 内部。通常无需修改此设置。

通信超时持续时间

允许在 Web 代理与应用商店服务之间进行调用的时间，位于 StoreFront 内部。通常无需修改此设置。

会话不活动超时

通过 Web 浏览器访问 StoreFront 应用商店时，在一段时间不活动后，用户会看到消息由于不活动，您的会话已超时。您可以更改会话超时以适合用户的使用模式。这不会影响 Citrix Workspace 应用程序。

或者，也可以使用 PowerShell。例如，要将 Web 站点“/Citrix/StoreWeb”的超时时间设置为 30 分钟：

```
$rfw = Get-STFWebReceiverService '/Citrix/StoreWeb'
Set-STFWebReceiverService $rfw -SessionStateTimeout 30
<!--NeedCopy-->
```


如果您修改会话超时以使其大于身份验证令牌生存时间或 Maximum token lifetime（令牌最长生存时间），这也会更新身份验证令牌生存时间和令牌最长生存时间以使其匹配。

身份验证令牌生存时间

用户通过浏览器访问 StoreFront 应用商店时，默认情况下，无论有任何活动，用户都会在八小时后注销。这不会影响 Citrix Workspace 应用程序。要延长此超时时间，请执行以下操作：

1. 在 StoreFront 中，导航到 **c:\inetpub\wwwroot\Citrix<StoreWeb>**。
2. 打开文件 `web.config`。
3. 找到相应的条目：**<authentication tokenLifeTime="08:00:00"method="Auto"/>**
4. 将 **tokenLifeTime** 更改为所需的值。要输入 1 天或更大的值，请使用格式 `d.h:m:s`。

如果将会话超时时间增加到 20 小时以上，还必须延长身份验证服务的最长令牌使用时间。

身份验证服务的最长令牌使用时间

身份验证服务颁发通过 Web 浏览器或 Citrix Workspace 应用程序连接到应用商店时使用的令牌。对于 Citrix Workspace 应用程序，这是唯一需要更新的登录超时时间。通过浏览器访问 StoreFront 时，此超时与其他超时一起使用。与本页面上描述的其他设置不同，这适用于应用商店的所有 Web 站点。

使用 Citrix Gateway 前往 StoreFront 时，Citrix Gateway 拥有用户凭据，并对 StoreFront 进行 SSO。如果 StoreFront 令牌到期，StoreFront 将发出 CitrixAG Basic 质询，Citrix Gateway 将提供登录 StoreFront 所需的凭据。因此，如果您还使用 Citrix Gateway，还需要配置自己的会话超时时间。

1. 对于安装在 StoreFront 服务器上的 Citrix Workspace 应用程序，请导航到应用商店的身份验证服务的路径 **c:\inetpub\wwwroot\Citrix\<Store>Auth**（这可能是多种身份验证服务之一，具体取决于您拥有的应用商店数量）。
2. 在 `web.config` 文件中，找到 **Authentication Token Producer** 服务，然后在其中找到 `id` 与 **Authentication Token Producer** 的 id 匹配的 `add` 元素。在以下示例中，您需要在 `id="f7cac185-57c1-4629-a33c-88a89dd4295d"encipherId="2948f7ad-735e-4e03-8e01-8d4f5d3ca75b"` 中使用 `add` 元素：

```
1 <service id="f7cac185-57c1-4629-a33c-88a89dd4295d" displayName="
     Authentication Token Producer">
2      <relyingParties signingId="2948f7ad-735e-4e03-8e01-8
          d4f5d3ca75b" defaultLifetime="01:00:00" maxLifetime="
          01:00:00">
3      <clear />
4      <add id="f7cac185-57c1-4629-a33c-88a89dd4295d" encipherId="
          2948f7ad-735e-4e03-8e01-8d4f5d3ca75b" defaultLifetime="
          01:00:00" maxLifetime="20:00:00" />
5 <!--NeedCopy-->
```


3. 将 **maxLifetime** 更改为所需的值。默认值为 20:00:00。要输入 1 天或更大的值，请使用格式 dd.hh:mm:ss。
4. 运行 **iisreset** 命令以应用所做的更改。运行此命令会从 Citrix StoreFront Web 注销用户，但不会影响其当前的 ICA 会话。

工作区控制

April 17, 2024

当用户在设备间移动时，工作区控制可确保他们所用的应用程序能够随他们移动。用户可以跨多个设备一直使用同一应用程序，而不必在每次登录到新设备时重新启动其所有应用程序。例如，这可以让医院的医生在各个工作站之间移动访问患者数据时节省很多时间。

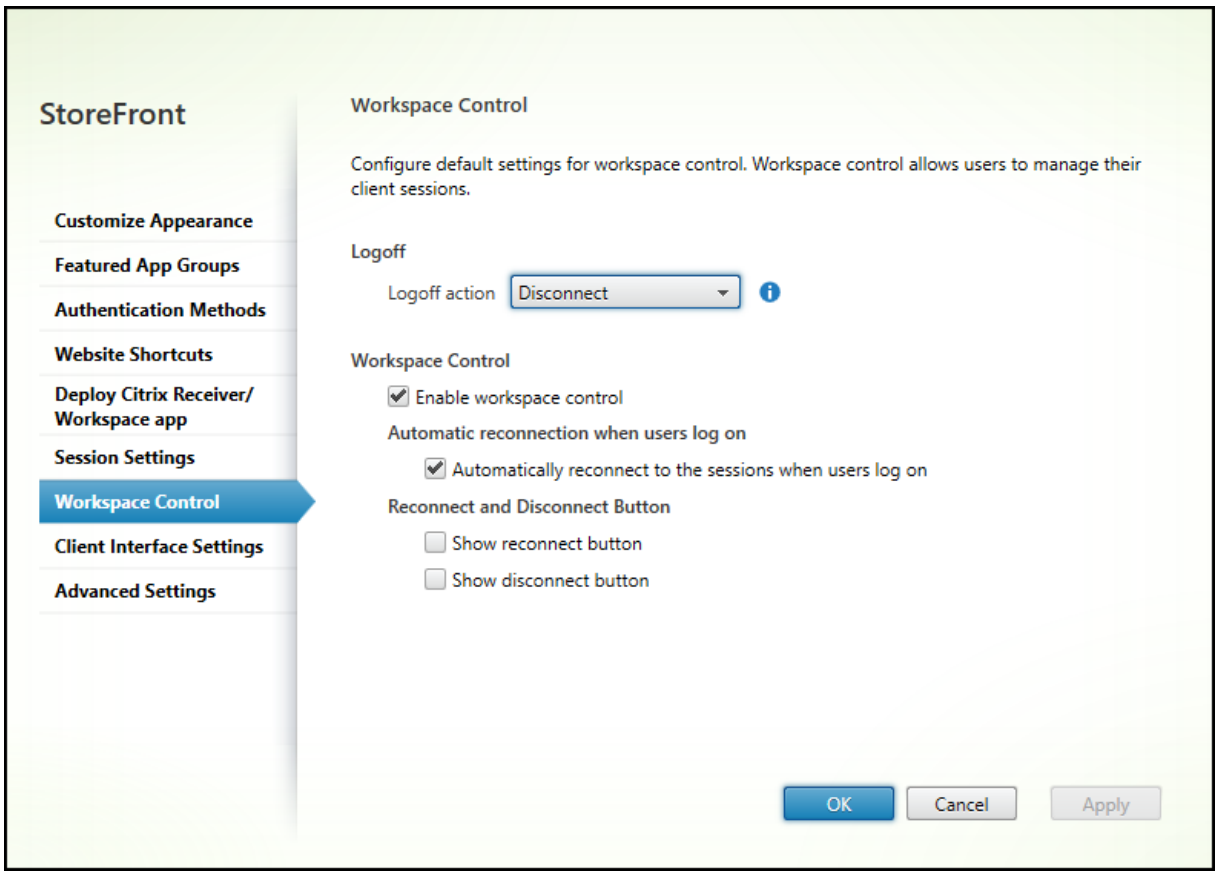
当用户登录时，会自动重新连接到他们正在运行的应用程序。例如，假设用户登录到某个应用商店并启动了一些应用程序。如果该用户随后使用相同的访问方法但在另一台设备上登录到同一应用商店，则正在运行的应用程序会自动传输到新设备。当用户从某个特定应用商店注销时，该用户在该应用商店中启动的所有应用程序都会自动断开连接，但不会关闭。如果通过 Web 浏览器访问应用商店，则必须使用相同的浏览器登录、启动应用程序和注销。

在适用于 **HTML5** 的 **Workspace** 应用程序中配置工作区控制

StoreFront 管理控制台中的工作区控制设置仅在通过 Web 浏览器访问应用商店时适用。这受以下要求和限制的约束：

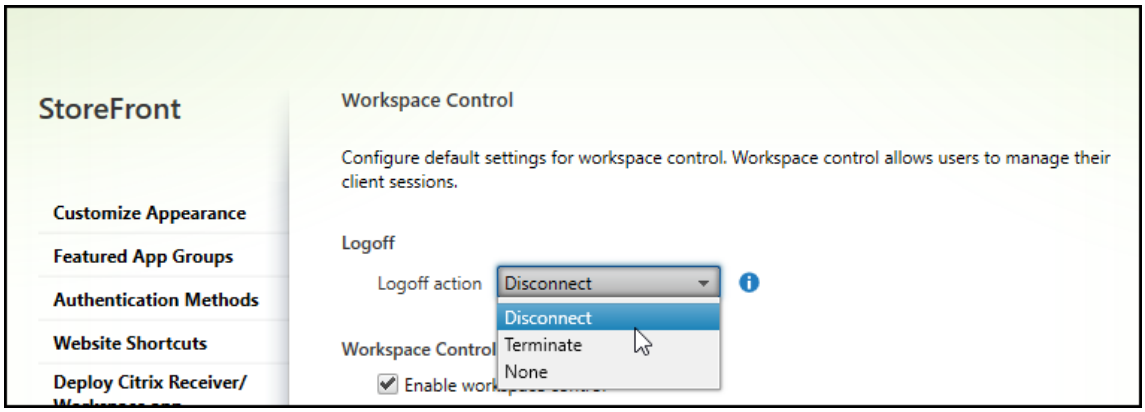
- 当适用于 HTML 的 Workspace 应用程序在托管桌面或应用程序中运行时，工作区控制不可用。
- 对于从 Windows 设备访问 Web 站点的用户，仅当以下情况下才能启用工作区控制功能：站点可以检测用户的设备上是否已安装适用于 Windows 的 Citrix Workspace 应用程序，或者使用适用于 HTML5 的 Citrix Workspace 应用程序访问资源。
- 要重新连接到已断开的应用程序，通过 Internet Explorer 访问 Web 站点的用户必须将该站点添加到“本地 Intranet”或“可信站点”区域。
- 如果仅有一个桌面可供配置为在用户登录时自动启动一个桌面的 Web 站点上的用户使用，该用户的应用程序将不重新连接，而无论工作区控制配置如何设置。
- 用户从其应用程序断开时使用的浏览器必须与最初启动时使用的浏览器相同。适用于 HTML5 的 Citrix Workspace 应用程序无法断开或关闭使用不同的浏览器启动的资源，也无法断开或关闭使用 Citrix Workspace 应用程序从桌面或“开始”菜单本地启动的资源。
- 当资源在同一个浏览器选项卡中打开时，工作区控制功能不可用。要对此进行配置，请参阅 Citrix Workspace 应用程序部署。

要在通过 Web 浏览器访问应用商店时修改工作区控制设置，请在编辑 Receiver for Web 站点屏幕上选择工作区控制。



请按如下所示配置工作区控制的设置：

- 指定注销操作。注销操作如下：
  - 断开连接：当您从站点注销时，应用程序和桌面会话将自动与客户端设备断开连接。
  - 终止：当您从站点注销时，应用程序和桌面会话将在服务器上自动终止。
  - 无：当您从站点注销时，应用程序和桌面会话将保持运行。



- 选中启用工作区控制复选框。
- 选中 **Automatic reconnections when users logon**（用户登录时自动重新连接）下的用户登录时自动重新连接到会话。

使用 **PowerShell SDK** 配置工作区控制

可以使用 PowerShell cmdlet Set-STFWebReceiverUserInterface 配置工作区控制。

在适用于 **Windows** 的 **Workspace** 应用程序中配置工作区控制

要在适用于 Windows 的 Workspace 中配置工作区控制，请参阅管理工作区控制重新连接。

在适用于 **Mac** 的 **Workspace** 应用程序中配置工作区控制

要在适用于 Mac 的 Workspace 中配置工作区控制，请参阅配置工作区控制设置。

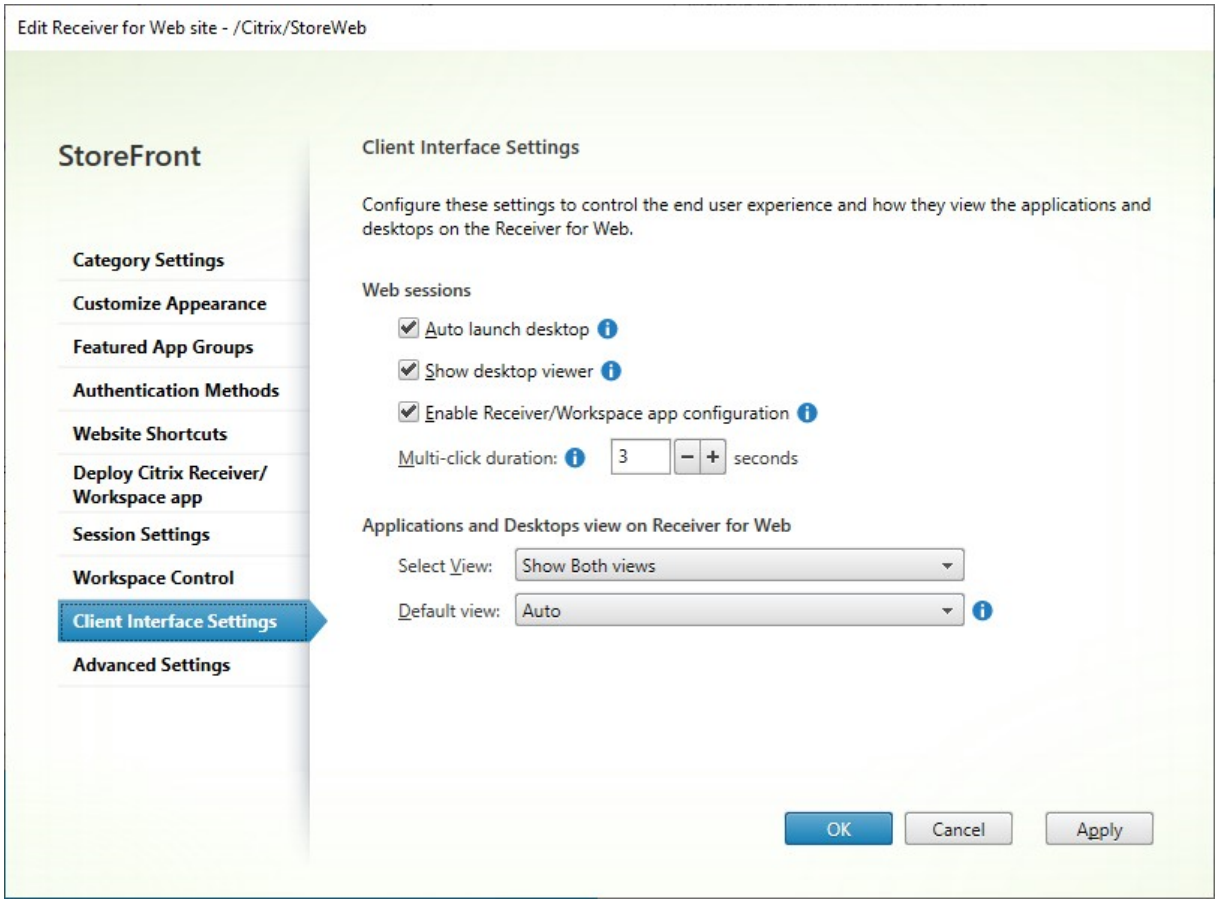
在所有应用程序中禁用工作区控制

要在 StoreFront 中跨 Workspace 应用程序禁用会话重新连接，则无论这些应用程序如何配置，都请转到高级设置选项卡并取消选中允许会话重新连接。

客户端界面设置

April 17, 2024

要从编辑 Receiver for Web 站点屏幕中修改客户端接口设置，请选择客户端接口设置选项卡。



自动启动桌面

如果启用了此设置并且用户只有一个桌面，该桌面将在用户登录时启动。

要使用 PowerShell SDK 更改自动启动桌面设置，请调用带参数 `AutoLaunchDesktop` 的 cmdlet Set-STFWebReceiverUserInterface。

此设置仅对适用于 HTML5 的 Citrix Workspace 应用程序适用。它不适用于本地安装的 Citrix Workspace 应用程序。

显示 **Desktop Viewer**

Desktop Viewer 是一个工具栏，可让您轻松访问 HDX 首选项。使用此设置可选择是否显示。

多击持续时间

防止用户在配置的持续时间内多次启动同一个应用程序。这仅应用于 HTML5 版 Citrix Workspace 应用程序，不应用于本机 Citrix Workspace 应用程序。

要使用 PowerShell SDK 更改多击持续时间，请调用带参数 `MultiClickTimeout` 的 cmdlet Set-STFWebReceiverUserInterface。
此设置仅对适用于 HTML5 的 Citrix Workspace 应用程序适用。它不适用于本地安装的 Citrix Workspace 应用程序。

启用 **Receiver/Workspace** 应用程序配置

如果选中，HTML5 版 Citrix Workspace 应用程序将提供预配文件，使用户能够自动为关联的应用商店配置本机 Citrix Workspace 应用程序。这些预配文件包含提供站点资源的应用商店的连接详细信息，其中包括为应用商店配置的所有 Citrix Gateway 部署和信标点的详细信息。

要使用 PowerShell SDK 更改此选项，请调用带参数 `ReceiverConfigurationEnabled` 的 cmdlet Set-STFWebReceiverUserInterface。

应用程序和桌面视图

如果同时提供桌面和应用程序，Citrix Workspace 应用程序在默认情况下将分别显示桌面视图和应用程序视图。收藏夹显示在主页视图中。用户登录该站点后，将首先看到主页视图。

从选择视图下拉列表中，选择是显示应用程序还是桌面，或者同时显示两者。

从默认视图下拉列表中，选择用户登录时显示的视图。

选项	说明
自动	显示主页视图
应用程序	显示应用程序视图
桌面	显示桌面视图

要使用 PowerShell SDK 更改这些选项，请调用带参数 `ShowAppsView`、`ShowDesktopsView` 和 `DefaultView` 的 cmdlet Set-STFWebReceiverUserInterface。

删除 **Web** 站点

September 29, 2023

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点，选择要为其创建 Citrix Receiver for Web 站点的应用商店，然后在操作窗格中单击管理 **Receiver for Web** 站点。
2. 选择一个站点，然后单击删除。如果删除站点，用户将无法再使用该 Web 页面访问应用商店。

配置 **Workspace** 应用程序 **Web** 站点

September 29, 2023

使用 StoreFront 创建新应用商店时，会自动创建一个 Web 站点并将其与应用商店关联。应用商店有多个 Web 站点时，请选择用户使用 Citrix Workspace 应用程序访问应用商店时显示哪个 Web 站点。

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点。
2. 在中心窗格中选择一个应用商店，然后在操作窗格中单击配置统一体验。如果您未创建 Citrix Receiver for Web Web 站点，则将显示一条消息，其中包含指向“添加 Receiver for Web 站点”向导的链接。
3. 选择您希望 Citrix Workspace 应用程序客户端在用户访问此应用商店时显示的 Web 站点。
4. 单击确定。

配置服务器组

April 17, 2024

可通过执行下面的任务来修改多服务器 StoreFront 部署的设置。要管理多服务器部署，一次请仅使用一台服务器更改服务器组的配置。确保 Citrix StoreFront 管理控制台未在部署中的任何其他服务器上运行。必须将对配置所做的任何更改传播到组中的其他服务器，以确保整个部署内的配置保持一致。

必须配置包含在 StoreFront 安装位置和 IIS Web 站点设置方面（例如物理位置和站点 ID）都相同的 StoreFront 服务器组的服务器。

向服务器组中添加服务器

可以通过执行“添加服务器”任务获取授权代码，以便能够将新安装的 StoreFront 服务器加入到现有部署中。有关将新服务器添加到现有 StoreFront 部署中的详细信息，请参阅加入现有服务器组。请参阅规划 StoreFront 部署的可扩展性部分，评估您的组中所需的服务器数量。

从服务器组中删除服务器

可以通过执行删除服务器任务从多服务器 StoreFront 部署中删除服务器。除了正在运行任务的服务器之外，可以删除组内的任何其他服务器。从多服务器部署中删除服务器之前，应先将其从负载平衡环境中删除。

在重新添加已删除的 StoreFront 服务器之前，必须将其重置为出厂默认状态。请参阅将服务器重置为出厂默认设置

将本地更改传播到服务器组

传播更改任务可用于更新多服务器 StoreFront 部署中所有其他服务器的配置，使其与当前服务器的配置保持一致。手动启动配置信息的传播，以便您能够控制组中的服务器何时以及是否使用配置更改进行更新。运行此任务时，在更新完组内的所有服务器之前，您不能执行进一步更改。

> 重要提示：
>
> 在传播过程中丢弃在组中的其他服务器上所做的任何更改。如果更新某个服务器的配置，请将所做的更改传播到组中的其他服务器，以避免在之后从部署中的另一个服务器传播更改时，这些更新会丢失。

在组中的服务器之间传播的信息包括以下内容：

- 所有 web.config 文件的内容，其中包含 StoreFront 配置。
- `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients` 的内容，例如 `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\Windows\CitrixWorkspaceAppWeb.exe` 和 `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\MAC\CitrixWorkspaceAppWeb.dmg`。
- `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\contrib` 的内容。
- `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\custom folder` 的内容，例如复制的图像和 customisation.js 文件。
- Citrix Delivery Services 证书存储的内容，但任何手动导入的证书吊销列表 (CRL) 除外。（有关分发本地 CRL 的详细信息，请参阅证书吊销列表 (CRL) 检查。

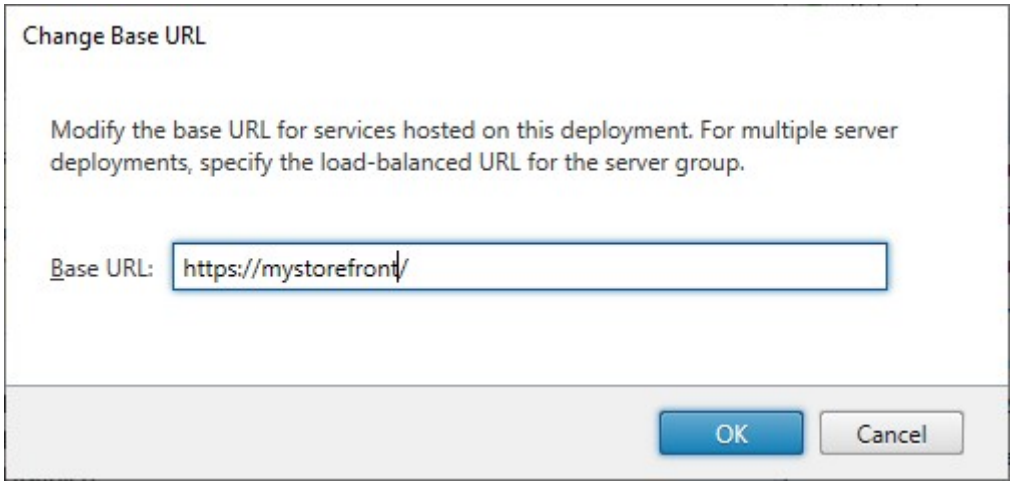
> 注意：
>
> 订阅数据与其他服务器同步，与传播更改机制无关。它会自动发生，而不启动传播更改任务。

更改部署的基本 **URL**

基本 URL 用作部署中托管的应用商店和其他 StoreFront 服务的 URL 的根目录。对于多服务器部署，请指定负载平衡 URL。

要更改基本 URL，请执行以下操作：

1. 在 Citrix StoreFront 管理控制台的左侧窗格中，选择服务器组节点。
2. 在操作窗格中，单击更改基本 **URL**…
3. 输入新 URL
4. 按确定。



与 Citrix Gateway 和 Citrix ADC 集成

April 17, 2024

将 Citrix Gateway 与 StoreFront 结合使用可以为企业网络外部的用户提供安全的远程访问，并利用 Citrix ADC 提供负载平衡。

任务	详细信息
添加 Citrix Gateway	向您的 Citrix ADC 添加网关，然后在 StoreFront 中对其进行配置
导入 Citrix Gateway	从 Citrix Gateway 中导出配置并将其导入到 StoreFront 中
管理 Citrix Gateway	添加、删除和编辑 Citrix Gateway 连接设置
使用 Citrix ADC 进行负载平衡	在 StoreFront 服务器组之前将 Citrix 配置为负载平衡器
为 Citrix ADC 和 StoreFront 配置委派表单身份验证 (DFA)	
使用不同的域进行身份验证	配置 StoreFront 和 Citrix Gateway，以便用户首先在一个域上使用网关进行身份验证，然后在另一个域上向 StoreFront 进行身份验证。
配置信标点	配置 Citrix Workspace 应用程序可以用来确定信标 URL 是在公司网络内部还是外部。
创建内部和外部使用的单个 FQDN	创建单个完全限定的域名 (FQDN)，该域名可以直接从公司网络内访问应用商店，也可以通过 Citrix Gateway 远程访问应用商店。

导入 **Citrix Gateway**

April 17, 2024

Citrix Gateway 管理控制台中配置的远程访问设置必须与 StoreFront 中配置的远程访问设置相同。本文介绍如何导入 Citrix Gateway 虚拟服务器的详细信息，以便正确配置 Citrix Gateway 和 StoreFront 使其能够配合使用。

要求

- 要将多个网关虚拟服务器导出为 ZIP 文件，需要 NetScaler 11.1.51.21 或更高版本。

  > 注意：
  >
  > Citrix ADC 设备只能导出使用 Citrix Virtual Apps and Desktops 向导创建的网关虚拟服务器。

- DNS 必须能够解析且 StoreFront 必须能够联系 Citrix ADC 设备生成的 ZIP 文件中的 GatewayConfig.json 文件中的所有 STA (Secure Ticket Authority) 服务器 URL。
- Citrix ADC 设备生成的 ZIP 文件中的 GatewayConfig.json 文件必须包含 StoreFront 服务器上的现有 Citrix Receiver for Web 站点的 URL。Citrix ADC 11.1 及更高版本会在生成要导出的 ZIP 文件之前通过联系 StoreFront 服务器并枚举所有现有应用商店和 Citrix Receiver for Web 站点处理好这一点。
- StoreFront 必须能够将 DNS 中的回调 URL 解析为网关 VPN 虚拟服务器 IP 地址，以便使用导入网关进行的身份验证能够成功。

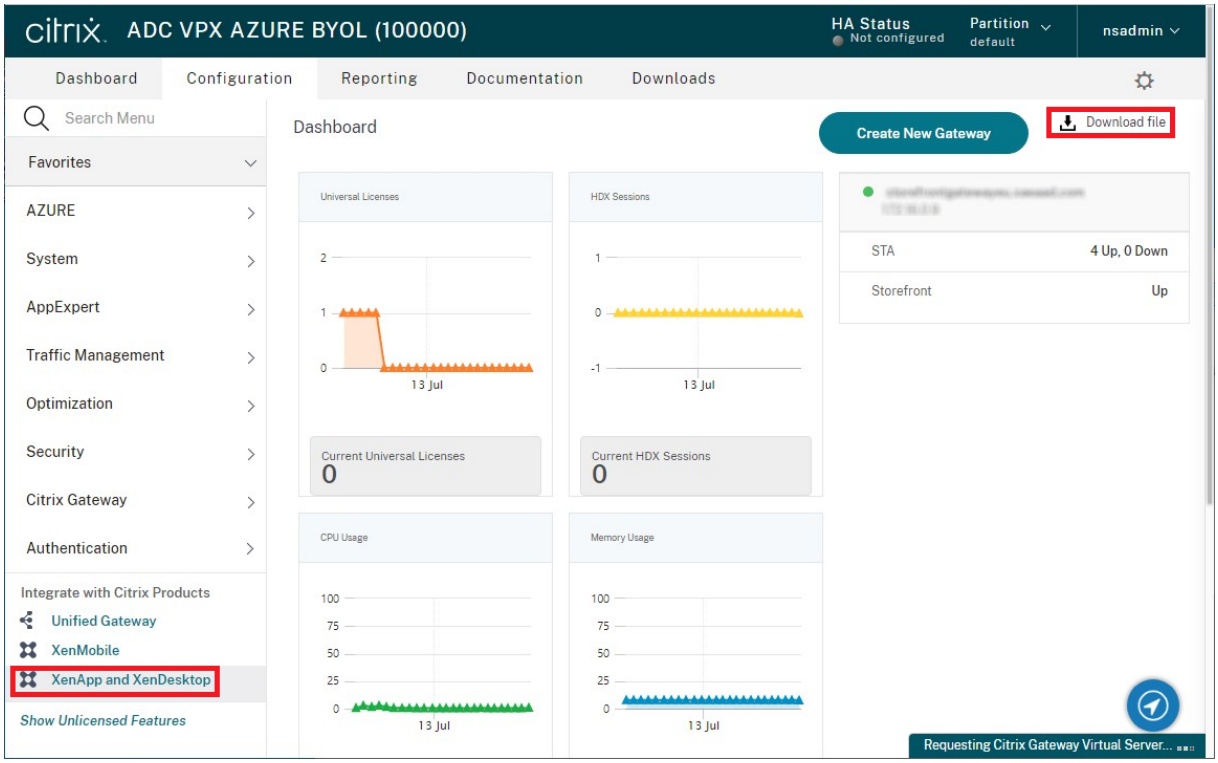
  您使用的回调 URL 和端口组合通常与网关 URL 和端口组合相同，只要 StoreFront 可以解决此 URL。

  或

  如果您在您的环境中使用不同的外部和内部 DNS 命名空间，回调 URL 和端口组合可能与网关 URL 和端口组合不同。如果您的网关位于 DMZ 中并使用 <example.com> URL，而 StoreFront 位于您的企业专用网络中并使用 <example.local> URL，则您可以使用 <example.local> 回调 URL 指回 DMZ 中网关虚拟服务器。

从 **Citrix Gateway** 导出配置

1. 登录 Citrix ADC。
2. 转到“配置”选项卡
3. 在“与 Citrix 产品集成”下，单击“XenApp 和 XenDesktop”
4. 在右上角，单击“下载文件”。



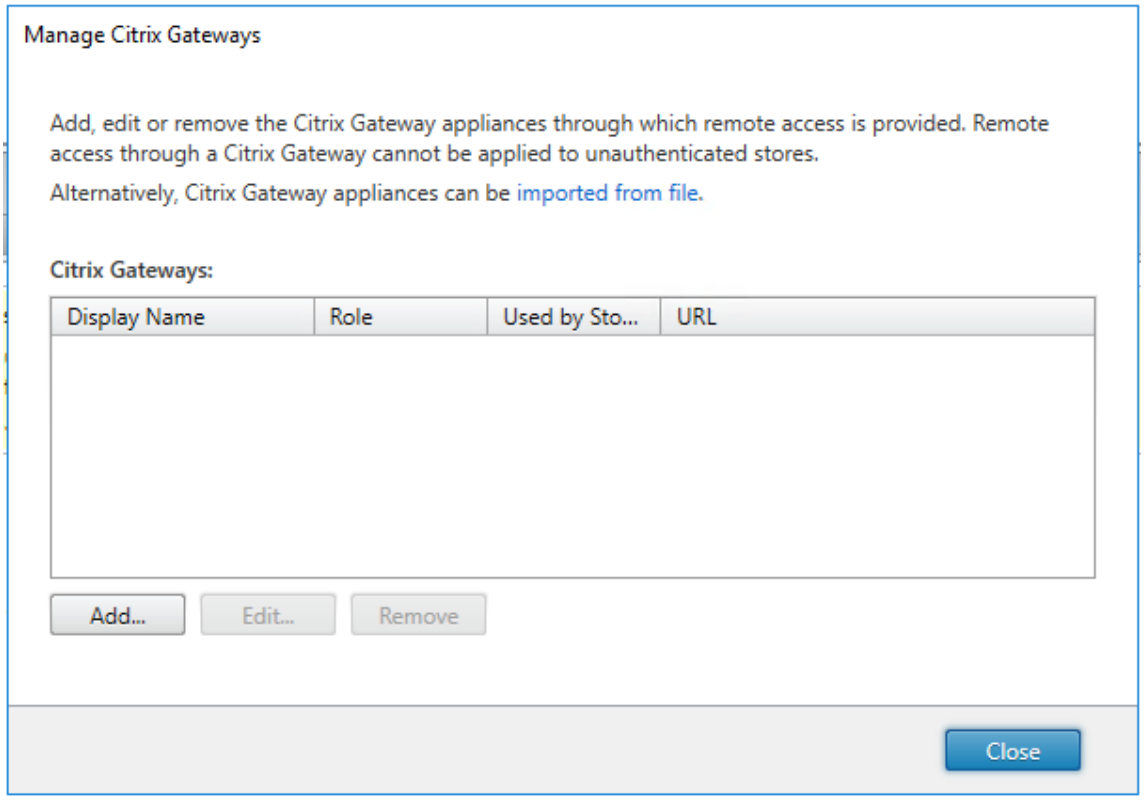
1. 选择是要下载所有网关的配置，还是要下载特定网关的配置。

使用控制台导入 **Citrix Gateway**

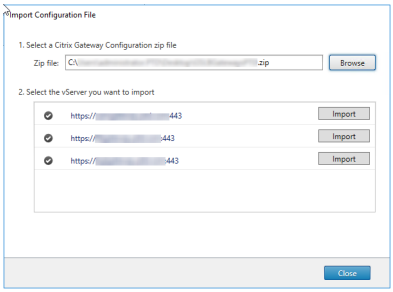
可以使用相同的导入文件导入一个或多个 Citrix Gateway 虚拟服务器配置。如果您有来自不同 Citrix ADC 设备的多个网关虚拟服务器，则必须使用多个导入文件。

> 重要提示：
>
> Citrix 不支持手动编辑从 Citrix Gateway 导出的配置文件。

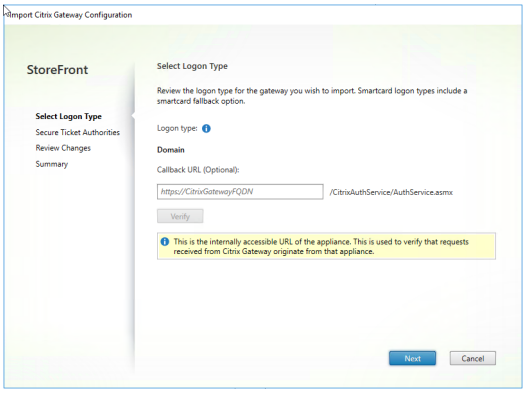
1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店，然后在操作窗格中单击管理 **Citrix Gateway**。
2. 在“管理 Citrix Gateway”屏幕中，单击从文件中导入链接。



3. 浏览到 Citrix Gateway 虚拟服务器配置文件。
4. 将显示所选 ZIP 文件中的网关虚拟服务器列表。请选择您要导入的网关虚拟虚拟服务器并单击导入。如果重复导入某个虚拟服务器，则“导入”按钮将显示为“更新”。如果选择更新，您以后可以选择覆盖网关或创建新网关。



5. 查看所选网关的登录类型，如果需要，请指定一个回调 **URL**。登录类型是在 Citrix Gateway 设备上为 Citrix Workspace 应用程序用户配置的身份验证方法。某些登录类型需要回调 URL（参见表格）。
    - 单击验证检查回调 URL 是否有效且是否可从 StoreFront 服务器访问。

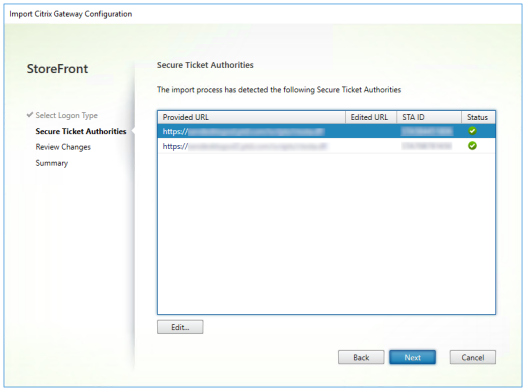


控制台中的登录类型	**JSON** 文件中的 **LogonType**	需要回调 **URL**
域	域	否
域和安全令牌	DomainAndRSA	否
安全令牌	RSA	是
智能卡 - 不回退	智能卡	是
智能卡 - 域	SmartCardDomain	是
智能卡 - 域和安全令牌	SmartCardDomainAndRSA	是
智能卡 - 安全令牌	SmartCardRSA	是
智能卡 - SMS 身份验证	SmartCardSMS	是
SMS 身份验证	SMS	是

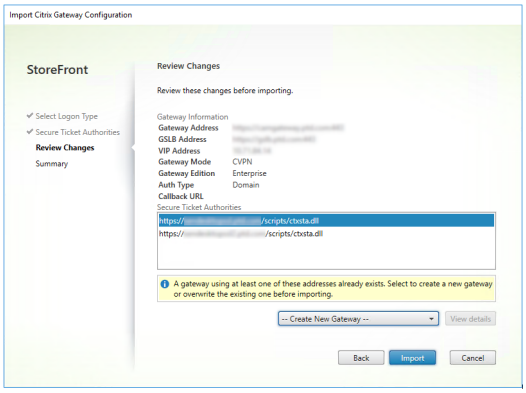
如果需要回调 URL，StoreFront 将基于在 ZIP 文件中找到的网关 URL 自动填充“回调 URL”。可以将此更改为指回正确的 Citrix Gateway VIP 的任何有效的 URL。对于 GSLB 网关，您导入的每个网关都需要唯一的回调 URL。

要使用智能访问或无密码身份验证，需要回调 URL。

6. 单击下一步。
7. StoreFront 使用 DNS 联系 ZIP 文件中列出的所有 STA (Secure Ticket Authority) 服务器 URL，并验证它们是否是正常运行的 STA 票据记录服务器。如果一个或多个 STA URL 无效，导入将不会继续。



8. 单击下一步。
9. 查看导入的详细信息。如果已存在具有相同网关 URL 和端口组合（网关 URL: 端口）的网关，请使用下拉框来选择一个网关将其覆盖，或创建一个新网关。



StoreFront 使用“网关 URL: 端口”组合来确定您尝试导入的网关是否匹配您可能希望更新的现有网关。如果某个网关具有不同的“网关 URL: 端口”组合，StoreFront 会将其视为新网关。此网关设置表显示了可以更新哪些设置。

网关设置	可以更新
网关 URL: 端口组合	否
GSLB URL	是
NetScaler 信任证书和指纹	是
回调 URL	是
Receiver for Web 站点 URL	是
网关地址/VIP	是
STA URL 和 STA ID	是
所有登录类型	是

10. 单击导入。如果 StoreFront 服务器属于某个服务器组，则会显示一条消息，提醒您将导入的网关设置传播到组中其他服务器。
11. 单击完成。

要导入另一个虚拟服务器配置，请重复上面的步骤。

> 注意：
>
> 应用商店的默认网关是 Citrix Workspace 应用程序尝试通过其连接的网关，除非将其配置为使用不同的网关。如果没有为应用商店配置网关，则从 ZIP 文件导入的第一个网关将成为 Citrix Workspace 使用的默认网关。导入后续网关不会更改已为应用商店设置的默认网关。

使用 **PowerShell** 导入多个 **Citrix Gateway**

Read-STFNetScalerConfiguration

- 将 ZIP 文件复制到当前登录的 StoreFront 管理员的桌面。
- 将 Citrix Gateway 虚拟服务器配置文件 ZIP 文件的内容读入内存，并使用三个网关的索引值查看该包中所含的这些网关。

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"
<!--NeedCopy-->
```

使用 **Read-STFNetScalerConfiguration** cmdlet 查看内存中从 NetScaler ZIP 导入包读入的三个网关对象。

```
$ImportedGateways.Document.Gateways[0]
$ImportedGateways.Document.Gateways[1]
$ImportedGateways.Document.Gateways[2]

GatewayMode             : CVPN
CallbackUrl             :
GslbAddressUri          : https://gslb.example.com/
AddressUri              : https://emeagateway.example.com/
Address                 : https://emeagateway.example.com:443
GslbAddress             : https://gslb.example.com:443
VipAddress              : 10.0.0.1
Stas                    : {
 STA298854503, STA909374257 }

StaLoadBalance          : True
CertificateThumbprints  : {
 F549AFAA29EBF61E8709F2316B3981AD503AF387 }

GatewayAuthType         : Domain
GatewayEdition          : Enterprise
ReceiverForWebSites     : {
 Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
    ReceiverForWebSite }
```



```
23
24
25 GatewayMode            : CVPN
26 CallbackUrl            :
27 GslbAddressUri         : https://gslb.example.com/
28 AddressUri             : https://emeagateway.example.com/
29 Address                : https://emeagateway.example.com:444
30 GslbAddress            : https://gslb.example.com:443
31 VipAddress             : 10.0.0.2
32 Stas                   : {
33  STA298854503, STA909374257 }
34
35 StaLoadBalance         : True
36 CertificateThumbprints : {
37  F549AFAA29EBF61E8709F2316B3981AD503AF387 }
38
39 GatewayAuthType        : DomainAndRSA
40 GatewayEdition         : Enterprise
41 ReceiverForWebSites    : {
42  Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
       ReceiverForWebSite }
43
44
45 GatewayMode            : CVPN
46 CallbackUrl            : https://emeagateway.example.com:445
47 GslbAddressUri         : https://gslb.example.com/
48 AddressUri             : https://emeagateway.example.com/
49 Address                : https://emeagateway.example.com:445
50 GslbAddress            : https://gslb.example.com:443
51 VipAddress             : 10.0.0.2
52 Stas                   : {
53  STA298854503, STA909374257 }
54
55 StaLoadBalance         : True
56 CertificateThumbprints : {
57  F549AFAA29EBF61E8709F2316B3981AD503AF387 }
58
59 GatewayAuthType        :SmartCard
60 GatewayEdition         : Enterprise
61 ReceiverForWebSites    : {
62  Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
       ReceiverForWebSite }
63
64 <!--NeedCopy-->
```

未指定 **CallbackURL** 的 **Import-STFNetScalerConfiguration**

将 ZIP 文件复制到当前登录的 StoreFront 管理员的桌面。将 Citrix Gateway 配置 ZIP 导入包的内容读入内存，并使用三个网关的索引值查看该包中所含的这些网关。


```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"
<!--NeedCopy-->
```

使用 **Import-STFNetScalerConfiguration** cmdlet 并指定所需的网关索引将三个新网关导入 StoreFront。使用 **-Confirm:$False** 参数可防止 Powershell GUI 提示您允许导入每个网关。如果您要谨慎地一次导入一个网关，请删除此项。

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -Confirm:$False
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -Confirm:$False
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -Confirm:$False
<!--NeedCopy-->
```

指定您自己的 **CallbackURL** 的 **Import-STFNetScalerConfiguration**

使用 **Import-STFNetScalerConfiguration** cmdlet 将三个新网关导入 StoreFront，并使用 -callbackURL 参数指定所选项的回调 URL。

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

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.com:443 -
    Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.com:444 -
    Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.com:445 -
    Confirm:$False
<!--NeedCopy-->
```

Import-STFNetScalerConfiguration 覆盖导入文件中存储的身份验证方法，并指定您自己的 **CallbackURL**

使用 **Import-STFNetScalerConfiguration** cmdlet 将三个新网关导入 StoreFront，并使用 -callbackURL 参数指定所选项的回调 URL。

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

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:443" -Confirm:$False
```



```
4
5 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
     GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://
     emeagatewaycb.example.com:444" -Confirm:$False
6
7 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
     GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://
     emeagatewaycb.example.com:445" -Confirm:$False
8 <!--NeedCopy-->
```

配置 **Citrix Gateway**

April 17, 2024

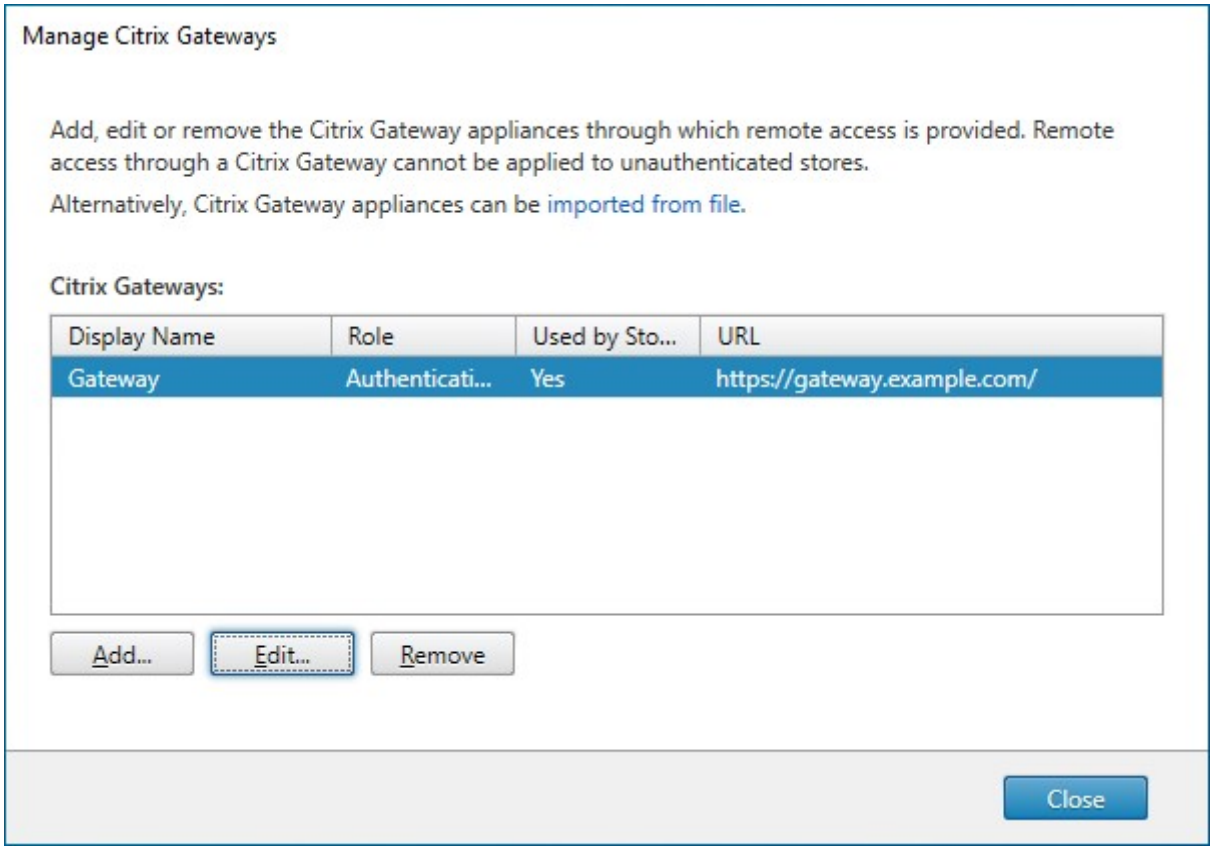
使用 Citrix Gateway 提供对 StoreFront 的远程访问。Citrix Gateway 在硬件或软件 Citrix ADC 或 Citrix Gateway 设备上运行。

有关配置您的网关的详细信息，请参阅将 NetScaler Gateway 与 StoreFront 集成。

必须在 StoreFront 中配置您的网关，StoreFront 才允许通过该网关进行访问。

查看网关

要查看在 StoreFront 中配置的网关，请在 Citrix StoreFront 管理控制台的左侧窗格中选择“应用商店”节点，然后单击管理 **Citrix Gateway**。这将显示管理 **Citrix Gateway** 窗口。



PowerShell

要获取网关及其配置的列表，请调用 Get-STFRoamingGateway。

添加 **Citrix Gateway**

> 重要提示：
>
> 在多服务器部署中，请一次仅使用一台服务器以更改服务器组的配置。确保 Citrix StoreFront 管理控制台未在部署中的任何其他服务器上运行。完成后，请
> 将对配置所做的更改传播到服务器组，以便更新部署中的其他服务器。

1. 在管理 **Citrix Gateway** 窗口中，单击添加。
2. 在“常规设置”选项卡上，输入设置，然后按下一步。
   - 为 Citrix Gateway 部署指定便于用户识别的显示名称。

     用户将在 Citrix Workspace 应用程序中看到您指定的显示名称，因此，请在该名称中包含相关信息，以帮助用户决定是否使用该部署。例如，可以在 Citrix Gateway 部署的显示名称中包含地理位置信息，以便用户能够轻松识别最便于其所在位置使用的部署。

- 输入网关的 URL。

  StoreFront 部署的完全限定的域名 (FQDN) 必须唯一，并且不同于 Citrix Gateway 虚拟服务器的 FQDN。不支持对 StoreFront 和 Citrix Gateway 虚拟服务器使用相同的 FQDN。网关将 URL 添加到 `X-Citrix-Via` HTTP 标头中。StoreFront 使用此标头来确定正在使用的网关。

  使用 GUI 只能添加单个网关 URL。如果一个网关可以通过多个 URL 访问，则除了该 URL 之外，您需要使用相同的配置两次添加同一个网关。要简单配置，您可以配置用于访问网关的辅助 URL。此选项在使用 GUI 时不可用，因此必须使用 PowerShell 进行配置。应在运行任何 PowerShell 命令之前关闭管理控制台。例如，如果您在全局服务器负载平衡器后面有多个网关，则通常同时添加 GSLB URL 和可用于访问每个特定区域性网关的 URL 将非常有用，例如用于测试或故障排除。创建网关后，您可以使用 `Set-STFRoamingGateway` 添加其他 URL，使用 `-GSLBurl` 参数添加辅助 URL。尽管该参数调用了 `GSLBurl`，但它可用于您希望添加第二个 URL 的任何情况。例如：

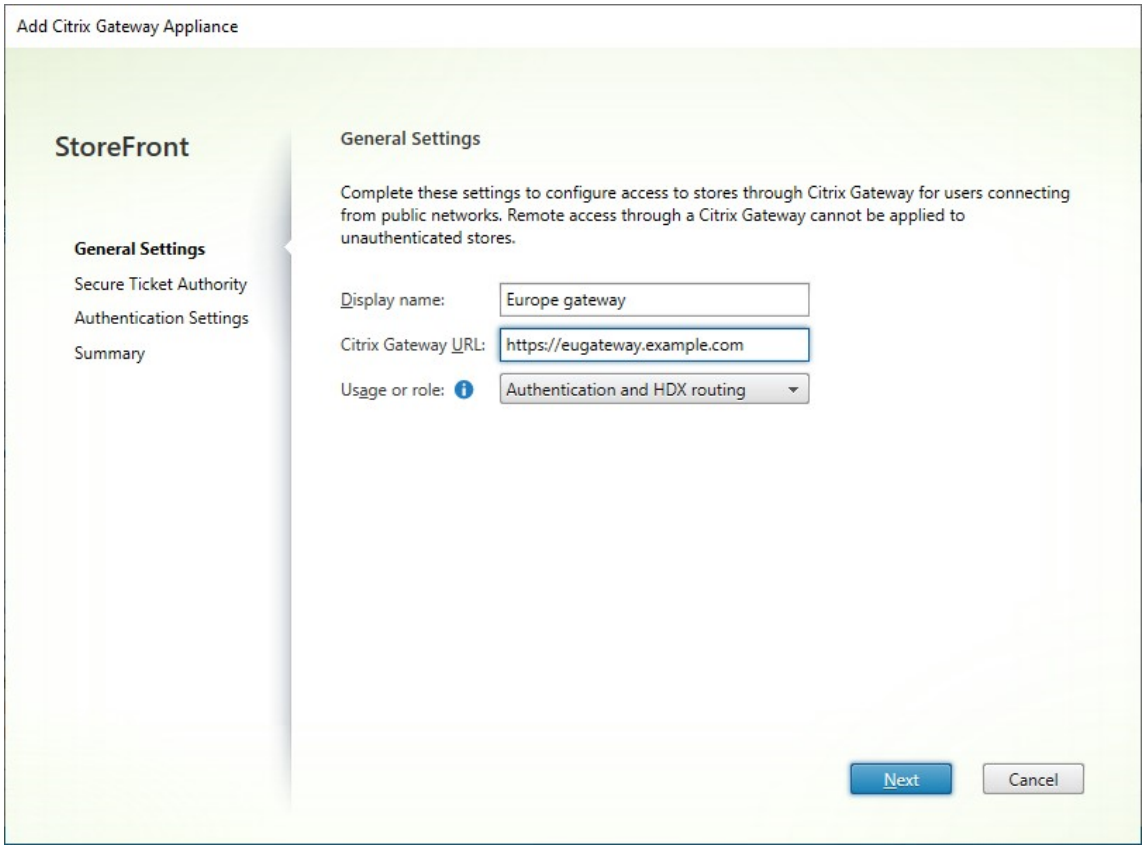
  ```
  1   Set-STFRoamingGateway -Name "Europe Gateway" -GSLBurl "
         eugateway.example.com" -GatewayUrl "gslb.example.com"
  2  <!--NeedCopy-->
  ```

  > 注意：
  >
  > 在本示例中，`GSLBurl` 参数包含区域 URL，而 `GatewayUrl` 参数包含 GSLB URL，这与直觉背道而驰。在大多数情况下，URL 的处理方式相同，如果只能通过 Web 浏览器访问应用商店，则可以采用任何一种方式对其进行配置。但是，通过 Citrix Workspace 应用程序访问 StoreFront 时，它会从 StoreFront 中读取 `GatewayUrl`，然后将其用于远程访问，最好将其配置为始终连接到 GSLB URL。

  如果您需要两个以上的 URL，则需要将其配置为单独的网关。

- 选择用法或作用：

用法或作用	说明
身份验证和 HDX 路由	使用网关提供对 StoreFront 的远程访问权限以及对 VDA 的访问权限。
仅限身份验证	如果网关仅用于远程访问 StoreFront，请选择此选项。
仅限 HDX 路由	如果网关仅用于提供对 VDA 的 HDX 访问权限，例如，在没有 StoreFront 实例的站点上，请选择此选项。

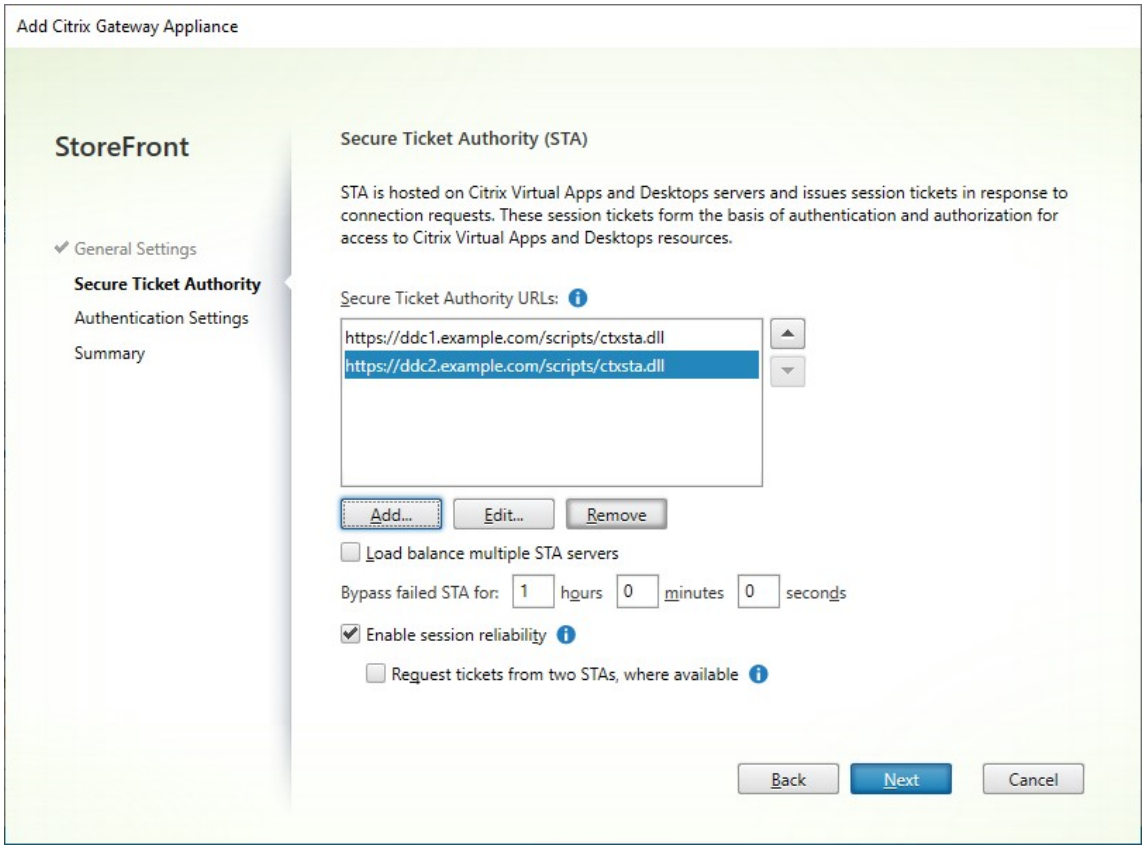


3. 填写 **Secure Ticketing Authority** 选项卡上的设置。

   Secure Ticketing Authority 根据连接请求签发会话票据。这些会话票据构成了对访问 Citrix Virtual Apps and Desktops 资源进行身份验证和授权的基础。

   - 请输入至少一个 Secure Ticket Authority 服务器 URL。如果您使用的是 Citrix Virtual Apps and Desktops，则可以将 Delivery Controller 用作 STA。如果您使用的是 Citrix 桌面即服务，则可以输入 Cloud Connector，代理会向 Citrix Cloud Ticketing Authority 提出请求。此列表中的条目必须与在 Citrix Gateway 中配置的列表完全匹配。
   - 勾选平衡多个 **STA** 服务器的负载以在 STA 服务器之间分发请求。如果未勾选，StoreFront 将按服务器列出的顺序试用服务器。
   - 如果 StoreFront 无法访问 STA 服务器，它会在一段时间内避免使用该服务器。默认情况下，此时间为 1 小时，但您可以自定义此值。
   - 如果要确保 Citrix Virtual Apps and Desktops 在 Citrix Workspace 应用程序尝试自动重新连接时保持断开连接的会话处于打开状态，请选中“启用会话可靠性”复选框。如果配置了多个 STA，并且希望确保会话可靠性始终可用，请选中从两个 **STA (**如果可用**)** 请求票据复选框。

     选中“从两个 STA (如果可用) 请求票据”复选框后，StoreFront 将从两个不同的 STA 获取会话票据，这样，即使一个 STA 在会话过程中变得不可用，用户会话也不会中断。如果由于任何原因无法与两个 STA 进行通信，StoreFront 将回退到使用单个 STA。



填写完设置后，按下一步

4. 在身份验证设置选项卡上填写设置。

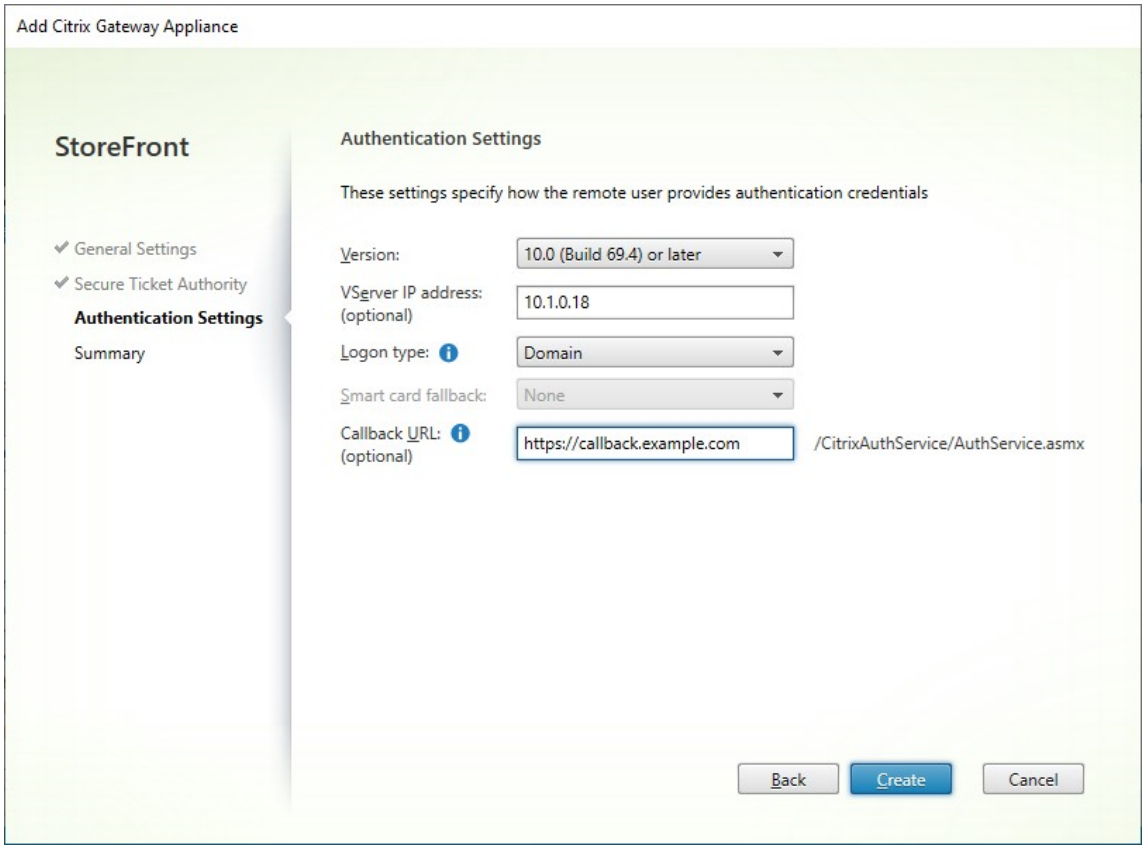
   - 选择 NetScaler 版本。
   - 如果有多个网关具有相同的 URL（通常是在使用全局服务器负载平衡器时），并且您输入了回调 URL，则必须输入该网关的 VIP。这允许 StoreFront 使用回调 URL 确定请求来自哪个网关，从而确定要联系哪个服务器。否则，您可以将其留空。
   - 从登录类型列表中选择在设备上为 Citrix Workspace 应用程序用户配置的身份验证方法。

   您所提供的有关 Citrix Gateway 设备配置的信息将添加到应用商店的预配文件中。这使 Citrix Workspace 应用程序能够在首次联系设备时发送相应的连接请求。

   - 如果系统要求用户输入其 Microsoft Active Directory 域凭据，请选择域。
   - 如果系统要求用户输入从安全令牌获得的令牌代码，请选择安全令牌。
   - 如果系统要求用户同时输入域凭据和从安全令牌获得的令牌代码，请选择域和安全令牌。
   - 如果系统要求用户输入通过短信发送的一次性密码，请选择 SMS 身份验证。
   - 如果系统要求用户提供智能卡并输入 PIN，请选择智能卡。

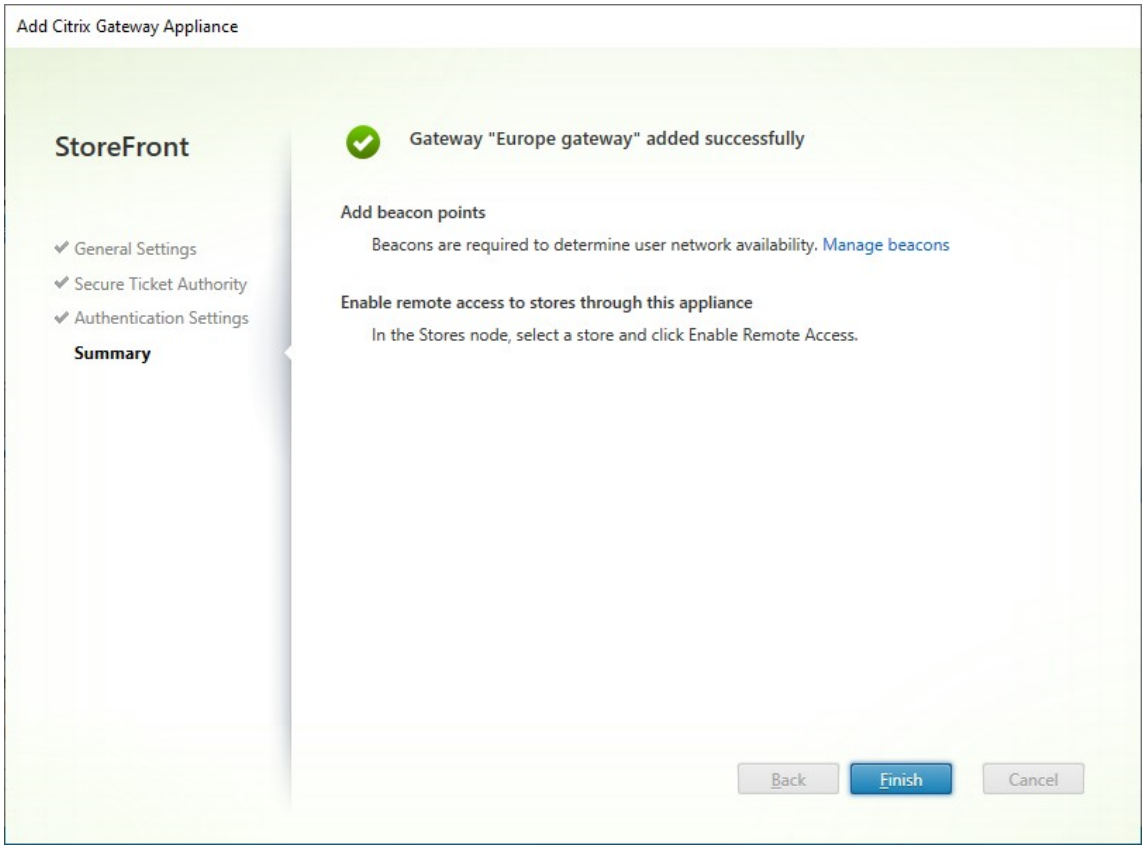
   如果为智能卡身份验证配置了辅助身份验证方法（当用户智能卡出现问题时可以回退到该方法），请从智能卡回退列表中选择辅助身份验证方法。

- （可选）在“回调 URL”框中输入网关的内部可访问 URL。这允许 StoreFront 联系 Citrix Gateway 身份验证服务，以验证从 Citrix Gateway 收到的请求是否来自该设备。对于智能访问和无密码身份验证场景（例如智能卡或 SAML），它是必需的，否则您可以将其留空。如果您有多个 Citrix Gateway 具有相同的 URL，则此 URL 必须用于特定的网关服务器。



填写完设置后，按下一步

5. 单击创建以应用配置。



6. 应用了部署后，单击完成。
7. 要使用户能够通过 Gateway 访问您的应用商店，请配置远程用户访问权限。

PowerShell SDK

要使用 PowerShell SDK 添加网关，请调用 cmdlet New-STFRoamingGateway。

编辑 Citrix Gateway

1. 在管理 **Citrix Gateway** 窗口中，单击要更改的网关，然后按编辑。

   有关参数的说明，请参阅添加 Citrix Gateway

2. 按保存以保存您的更改。

PowerShell SDK

要使用 PowerShell SDK 修改网关配置，请调用 cmdlet Set-STFRoamingGateway。

删除 **Citrix Gateway**

1. 在管理 **Citrix Gateway** 窗口中，单击要更改的网关，然后按删除。
2. 在确认窗口中，按是。

PowerShell SDK

要使用 PowerShell SDK 删除网关，请调用 Remove-STFRoamingGateway。

使用 **Citrix ADC** 进行负载平衡

April 17, 2024

本文提供在全部有效的负载平衡配置中部署包含两个或更多个 StoreFront 服务器的 StoreFront 服务器组的方法指导。本文提供有关如何将 Citrix ADC 设备配置为在服务器组中的 StoreFront 服务器之间对来自 Citrix Workspace 应用程序和 Web 浏览器的传入请求进行负载平衡的详细信息。

负载平衡部署的服务器证书要求

从商业证书颁发机构购买证书或通过您的企业证书颁发机构颁发证书之前，请考虑以下选项。

- 选项 **1**：在 Citrix ADC 设备负载平衡虚拟服务器 和 StoreFront 服务器组节点上均使用 **.example.com* 通配符证书。这样可以简化配置，将来无需替换证书即可以添加其他 StoreFront 服务器。
- 选项 **2**：在 Citrix ADC 设备负载平衡虚拟服务器 和 StoreFront 服务器组节点上均使用包含使用者可选名称 (SAN) 的证书。证书中包含匹配所有 StoreFront 服务器完全限定域名 (FQDN) 的其他 SAN 为可选，但是建议采用，因为这样可以在 StoreFront 部署中提供更大的灵活性。

为 **StoreFront** 服务器组负载平衡器创建 **DNS** 记录

为所选的共享 FQDN 创建 DNS A 和 PTR 记录。您网络内的客户端使用此 FQDN 访问使用 Citrix ADC 设备负载平衡器的 StoreFront 服务器组。

示例：`storefront.example.com` 解析为负载平衡虚拟服务器虚拟 IP (VIP)。

配置 **StoreFront** 服务器

您希望在其之间进行负载平衡的所有 StoreFront 服务器都应配置为 StoreFront 服务器组的一部分，该组在服务器之间同步配置，以确保其配置相同。有关向服务器组中添加服务器的更多详细信息，请参阅加入现有服务器组。

应将每台服务器配置为使用 HTTPS，以便对负载平衡器与 StoreFront 服务器之间的通信进行加密。请参阅使用 HTTPS 保护 StoreFront 的安全。证书必须包含负载平衡的 FQDN 作为公用名 (CN) 或者作为使用者备用名称 (SAN)。

将服务器组基本 URL 设置为负载平衡器的 URL。要修改基本 URL，请在 Citrix StoreFront 管理控制台的左侧窗格中右键单击服务器组，然后单击更改基本 **URL**。输入负载平衡器虚拟服务器的 URL。

（可选）将 **Citrix Service Monitor** 配置为使用 **HTTPS**

StoreFront 安装包括 **Citrix Service Monitor** Windows 服务。此服务没有其他服务依赖项，可以监视关键 StoreFront 服务的运行状况。这允许 Citrix ADC 和其他第三方应用程序监视 StoreFront 服务器部署的相对运行状况。

默认情况下，Monitor 在端口 8000 上使用 HTTP。可以选择将其更改为在端口 443 上使用 HTTPS。

1. 打开主 StoreFront 服务器上的 PowerShell 集成脚本环境 (ISE)，然后运行以下命令以将默认 Monitor 更改为 HTTPS 443：

```
$ServiceUrl = "https://localhost:443/StorefrontMonitor"
Set-STFServiceMonitor -ServiceUrl $ServiceUrl
Get-STFServiceMonitor
<!--NeedCopy-->
```

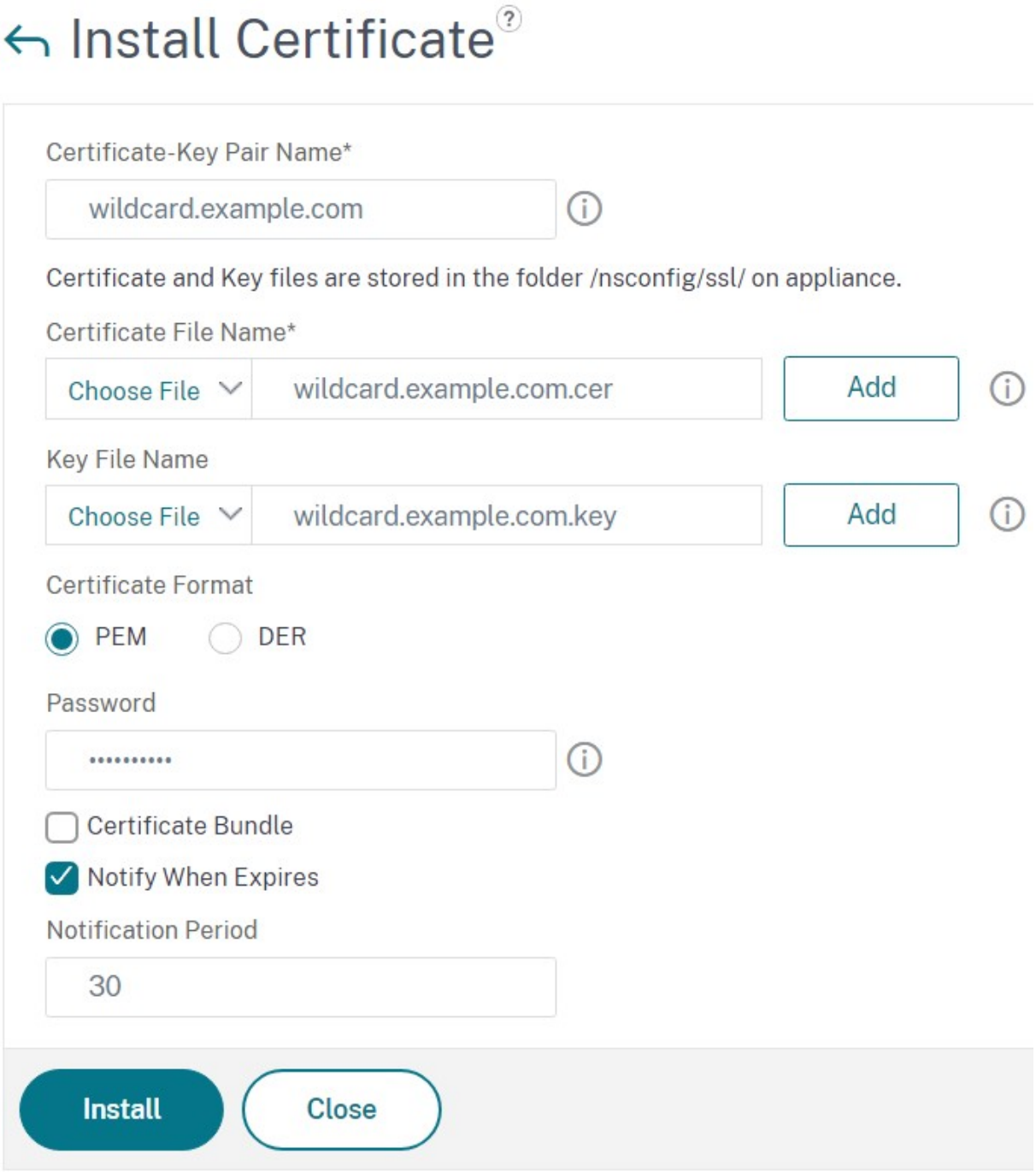
2. 完成后，将更改传播到 StoreFront 服务器组中的所有其他服务器。
3. 要在 Monitor 上执行快速测试，请在 StoreFront 服务器或可以通过网络访问 StoreFront 服务器的任何其他计算机上，将以下 URL 输入浏览器中。浏览器将返回每个 StoreFront 服务的状态的 XML 摘要。

```
https://<loadbalancingFQDN>/StoreFrontMonitor/GetSFServicesStatus
```

配置 **Citrix ADC** 负载平衡器

在 **Citrix ADC** 上配置服务器证书

1. 登录到 Citrix ADC 设备管理 GUI。
2. 选择 **Traffic Management**（流量管理）**> SSL > Certificates**（证书）**> Server Certificates**（服务器证书）
3. 单击安装。
4. 在安装服务器证书页面上，输入证书-密钥对名称，单击选择文件，然后浏览证书文件。如果证书文件不包含私钥，则此外您还需要选择密钥文件。

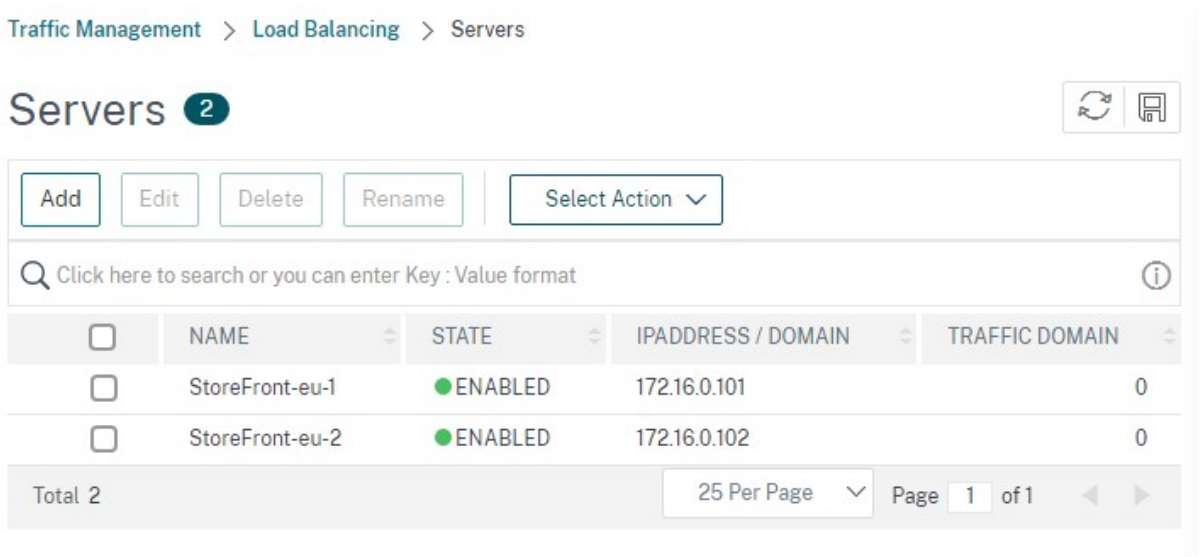


将单个 **StoreFront** 服务器节点添加到 **Citrix ADC** 设备负载平衡器

1. 导航到 **Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Servers**（服务器）。单击添加，添加要进行负载平衡的每台 StoreFront 服务器。

   示例 = 2 个名为 StoreFront-eu-1 和 StoreFront-eu-2 的 StoreFront 服务器

2. 使用基于 IP 的服务器配置，并输入每个 StoreFront 节点的服务器 IP 地址。



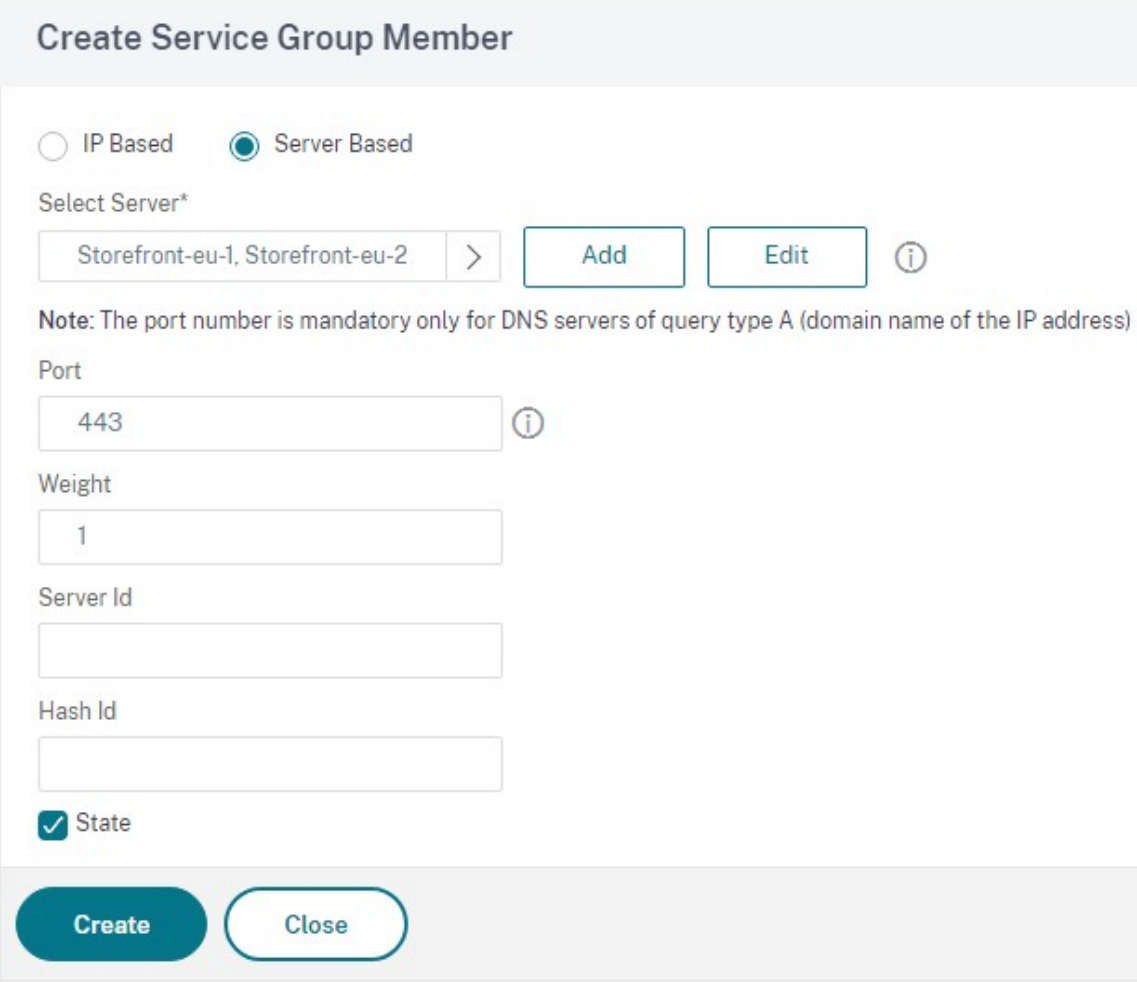
定义一个 **StoreFront** 监视程序，用于检查服务器组中所有 **StoreFront** 节点的状态

1. 登录到 Citrix ADC 管理 GUI。
2. 选择 **Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Monitors**（监视程序）**> Add**（添加），添加名为 *StoreFront* 的新监视程序，并接受所有默认设置。
3. 从 **Type**（类型）下拉菜单中，选择 **StoreFront**。
4. 如果您已将 StoreFront 监视程序配置为使用 HTTPS，请务必选择 **Secure**（安全）选项。否则，请将此选项保持未选中状态，然后输入端口 8000。
5. 选择 **Check Backend Services**（检查后端服务）选项。选中此选项将 StoreFront 服务器上运行的服务进行监视。通过探测 StoreFront 服务器上运行的 Windows 服务监视 StoreFront 服务，该操作会返回以下服务的状态：
   - W3SVC (IIS)
   - WAS（Windows 进程激活服务）
   - CitrixCredentialWallet
   - CitrixDefaultDomainService

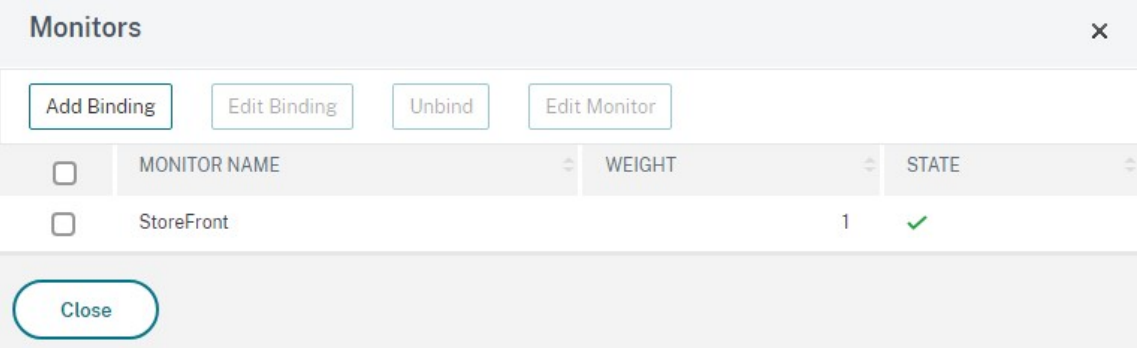
创建包含所有 **StoreFront** 服务器的服务组

1. 导航到 **Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Service Groups**（服务组）。按添加。要通过 HTTPS 连接到 StoreFront 服务器，请选择 SSL 协议。将其他设置保留为默认设置。按确定。
2. 在您的服务组中，在 **Service Group Members**（服务组成员）下，单击 **No Service Group Member**（无服务组成员）。

a) 单击 **Service Based**（基于服务）。
b) 选择您之前定义的所有服务器。
c) 要在负载平衡器与 StoreFront 服务器之间使用 SSL，请输入端口 443。否则，请输入端口 80。



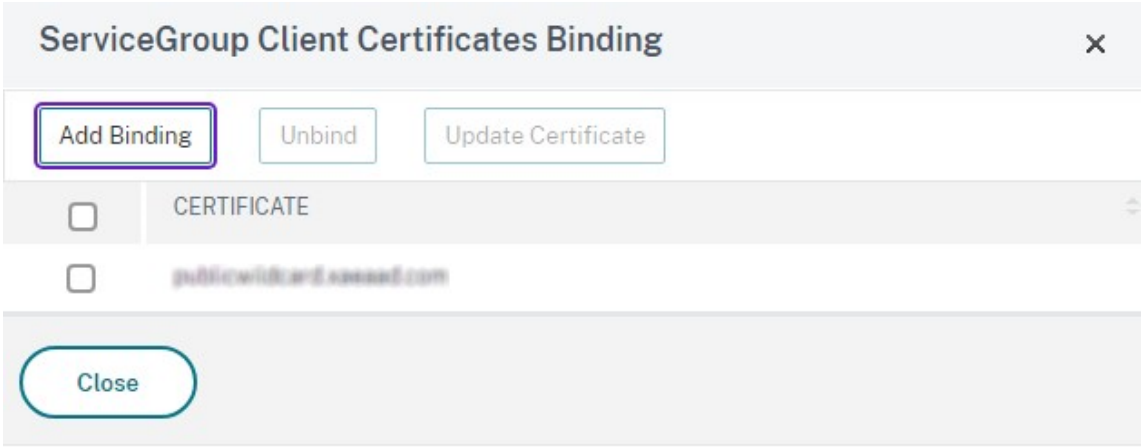
3. 添加 **Monitors**（监视程序）部分并选择您之前创建的 StoreFront 监视程序。



4. 添加 **Certificates**（证书）部分。

a) 绑定客户端证书。

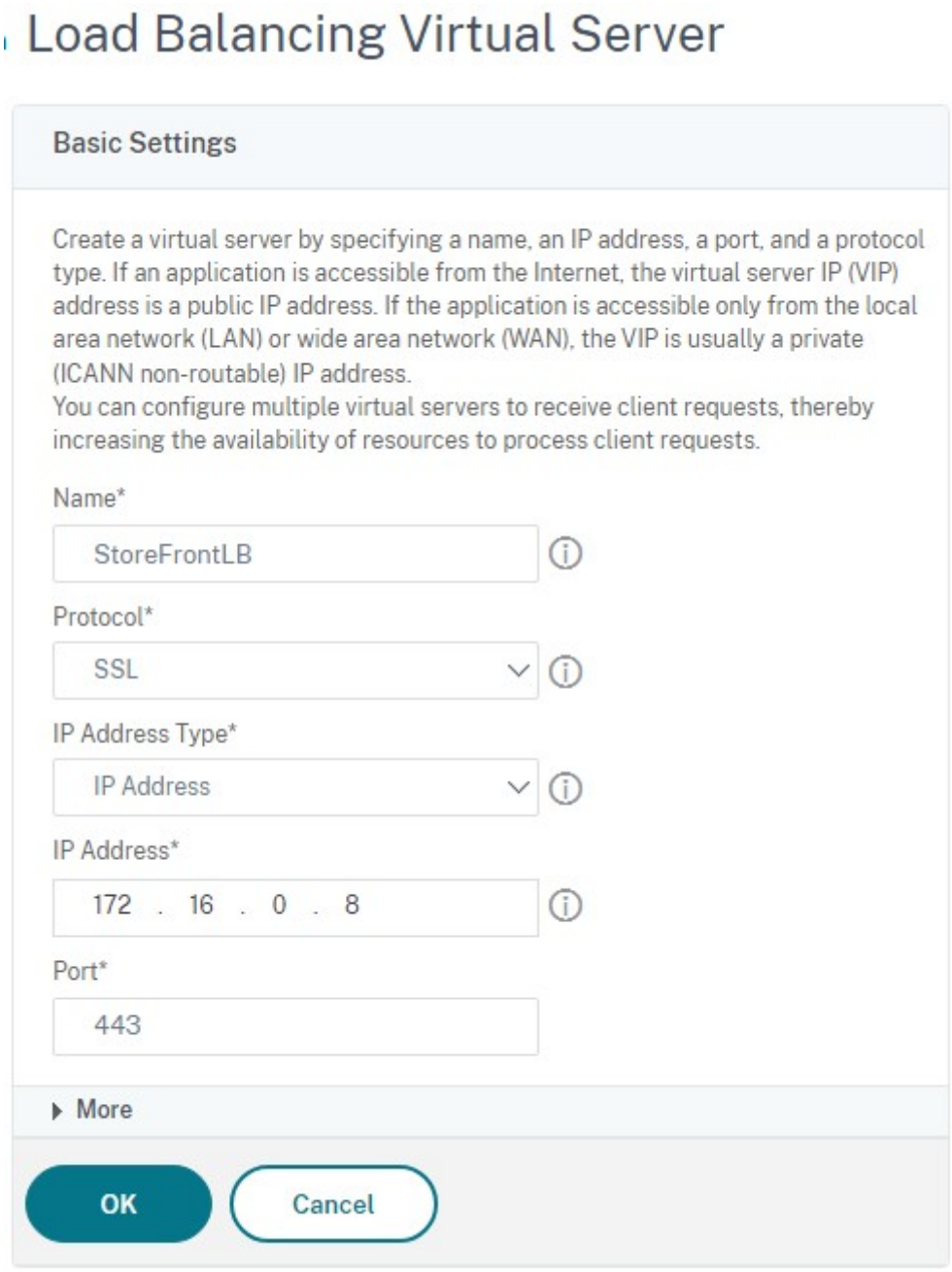
b) 绑定用于为您之前导入的服务器证书进行签名的 CA 证书，以及可能属于 PKI 信任链的任何其他 CA。



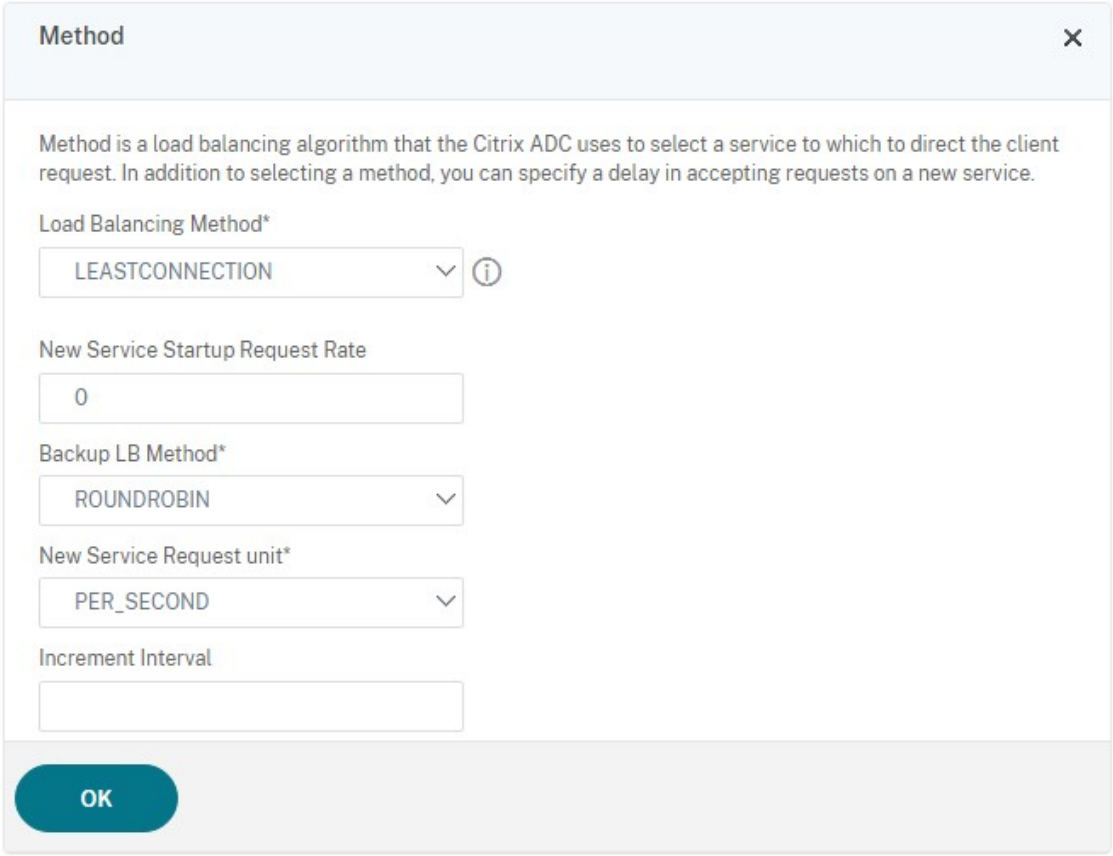
5. 添加 **Settings**（设置）部分。选择 **Insert Client IP Header**（插入客户端 IP 标头）并输入 **X-Forwarded-For** 的标头名称。这允许您在 Citrix Virtual Apps and Desktops 策略中使用客户端 IP 地址。

创建用于用户流量的负载平衡虚拟服务器

1. 登录到 Citrix ADC 设备管理 GUI。
2. 选择 **Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Virtual Servers**（虚拟服务器）**> Add**（添加），创建一个新的虚拟服务器。
3. 输入名称，选择 SSL 协议并输入端口。单击“确定”创建虚拟服务器。



4. 将您之前创建的服务组绑定到负载平衡虚拟服务器。
5. 绑定您之前绑定到服务组的同一服务器和 CA 证书。
6. 添加 **Method**（方法）部分并选择负载平衡方法。StoreFront 负载平衡的常用选项为 **round robin**（轮询）或 **least connection**（最少连接）。



7. 添加 **Persistance**（持久性）部分。

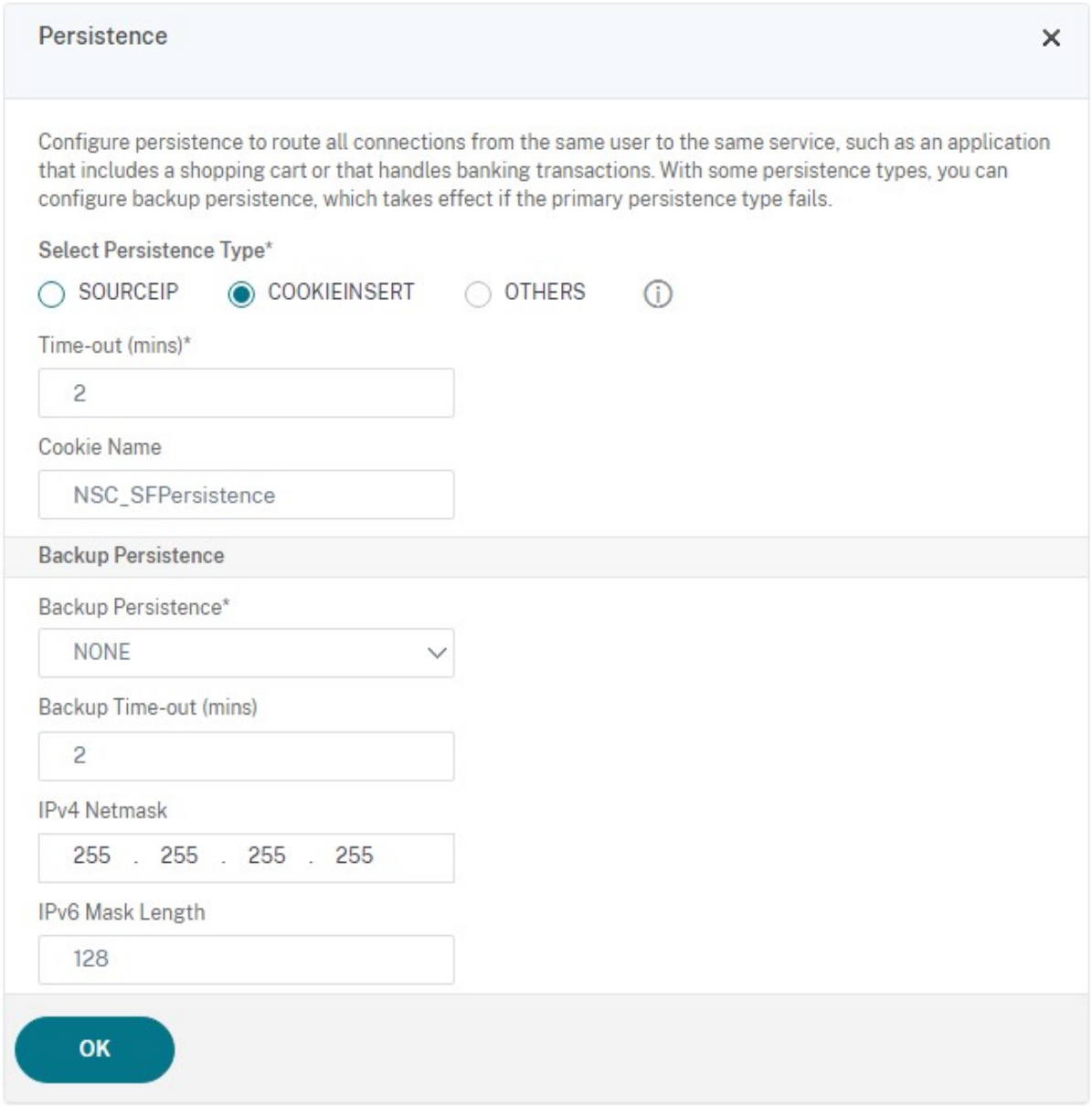
   a) 将持久性方法设置为 **COOKIEINSERT**。

   b) 将超时设置为与 StoreFront 中的会话超时相同，默认情况下为 20 分钟。

   c) 为该 Cookie 命名。例如，**NSC_SFPersistence**，这样可以使其在调试过程中易于识别。

   d) 将备份持久性设置为 **NONE**（无）。

> 注意：
>
> 如果不允许客户端存储 HTTP cookie，则后续请求不会含有 HTTP cookie，并且不使用“Persistence”（持久性）。



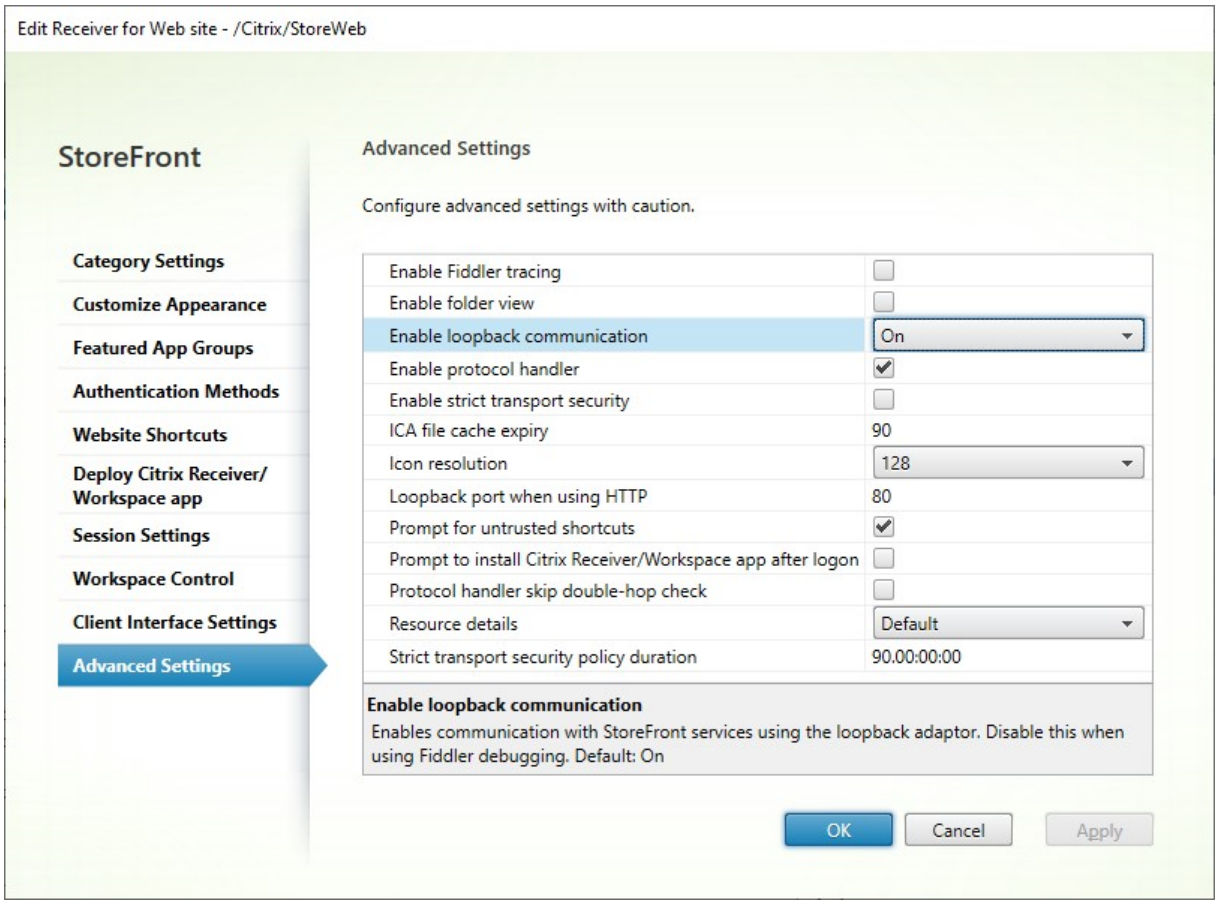
配置 **StoreFront** 环回

当基本地址为负载平衡器时，对于 StoreFront 服务之间的内部通信，它可能会导致流量路由到负载平衡器，并且可能会路由到另一台服务器。这会导致出现性能不佳和意外行为。请使用 StoreFront 设置启用环回通信来避免这种情况。默认情况下，此设置设为开，这意味着它会将服务地址的主机部分替换为环回 IP 地址 127.0.0.1，同时保持架构（HTTP 或 HTTPS）不变。此值适用于单服务器部署以及具有非 SSL 终止负载平衡器的部署。

如果负载平衡器终止 SSL 并通过 HTTP 与 StoreFront 通信（不推荐），则必须将 StoreFront 环回通信配置为 **OnUsingHttp**，这意味着 StoreFront 还会将架构从 HTTPS 更改为 HTTP。

1. 打开 Citrix StoreFront。

2. 对于每个应用商店，请转到管理 **Receiver for Web** 站点。对于每个 Web 站点，请转到配置。
3. 转至高级设置
4. 将启用环回通信设置更改为 **OnUsingHttp**。



如果负载平衡器终止 SSL 并通过 HTTP 与 StoreFront 通信（不推荐），则需要将 StoreFront 环回通信配置为 **OnUsingHttp**，这意味着 StoreFront 还会将架构从 HTTPS 更改为 HTTP。

配置 **Citrix ADC** 负载平衡器以实现服务器组之间的订阅同步

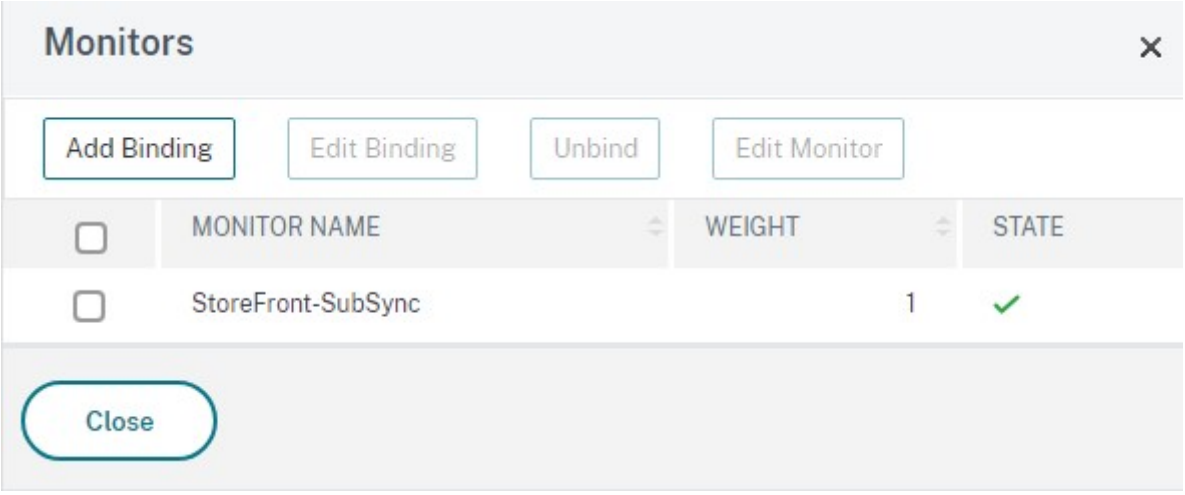
如果您的多站点部署由两个或多个 StoreFront 服务器组组成，则可以按重复计划使用提取策略在这些服务器组之间复制订阅数据。StoreFront 订阅复制使用 TCP 端口 808，因此，使用现有采用 HTTP 端口 80 或 HTTPS 443 的负载平衡虚拟服务器将失败。要为此服务提供高可用性，请在部署中的每个 Citrix ADC 设备上创建第二个虚拟服务器，以便为每个 StoreFront 服务器组负载平衡 TCP 端口 808。

配置用于订阅同步的服务组

1. 登录到 Citrix ADC 设备管理 GUI。
2. 选择 **Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Service Groups**（服务组）**> Add**（添加）。

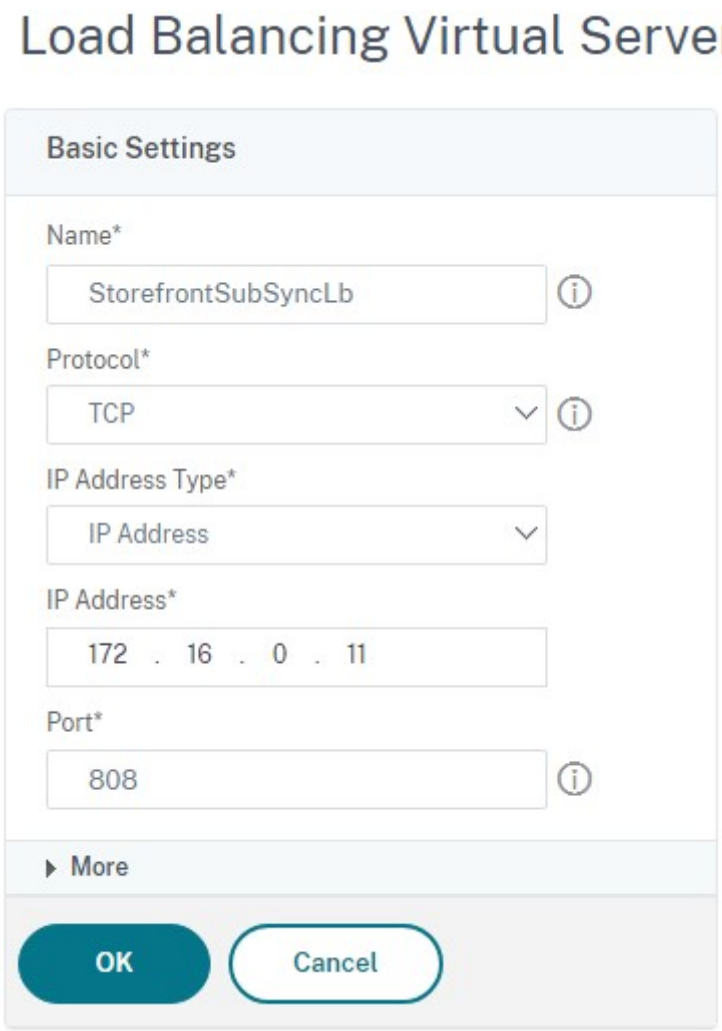
3. 输入服务组名称，将协议更改为 **TCP**，然后单击确定进行保存。
4. 在服务组成员部分中，添加您之前在“服务器”部分中定义的所有 StoreFront 服务器节点，并将端口指定为 **808**。
5. 添加监视器部分。

    a) 单击显示 **No Service Group to Monitor Binding**（无可监视绑定的服务组）的位置。
    b) 单击添加。输入监视程序名称并将其类型设置为 **TCP**。单击创建。
    c) 单击绑定。



为实现订阅同步创建负载平衡虚拟服务器

1. 登录到 Citrix ADC 设备管理 GUI。
2. 选择 **Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Virtual Servers**（虚拟服务器）**> Add**（添加），添加一个新的服务器。
3. 输入名称
4. 将协议更改为 **TCP**。
5. 输入 IP 地址。
6. 输入端口 **808**。



7. 单击确定。
8. 单击 **No Load Balancing Virtual Server ServiceGroup Binding**（无负载平衡虚拟服务器服务组绑定），选择您之前创建的服务组，然后单击 **Bind**（绑定）。
9. 添加 **Method**（方法）部分并将 **Load Balancing Method**（负载平衡方法）设置为 **ROUNDROBIN**
10. 单击完成以完成更改。

配置 **StoreFront** 以通过负载平衡器提取订阅数据

请参阅配置订阅同步。

配置复制计划时，请指定与订阅同步虚拟服务器虚拟负载平衡器 IP 地址匹配的服务器组地址。

为 **Citrix ADC** 和 **StoreFront** 配置委派表单身份验证 **(DFA)**

February 22, 2024

可扩展的身份验证为扩展基于 Citrix ADC 设备的表单和基于 StoreFront 的表单的身份验证提供了单个自定义点。要使用可扩展的身份验证 SDK 获得身份验证解决方案，必须在 Citrix ADC 设备与 StoreFront 之间配置委派表单身份验证 (DFA)。委派表单身份验证协议允许生成和处理要委派给另一组件的身份验证表单，包括凭据验证。例如，Citrix Gateway 将其身份验证委派给 StoreFront，StoreFront 再与第三方身份验证服务器或服务进行交互。

在 Citrix Gateway 上配置委派表单身份验证在 CTX200383 中进行介绍。

安装建议

- 要确保 Citrix ADC 设备与 StoreFront 之间的通信受到保护，请使用 HTTPS 代替 HTTP 协议。
- 对于群集部署，请确保在执行配置步骤之前，所有节点均已在 IIS HTTPS 绑定中安装和配置相同的服务器证书。
- 确保在 StoreFront 中配置 HTTPS 后，Citrix ADC 设备将 StoreFront 服务器证书的发行方作为可信证书颁发机构。

StoreFront 群集安装注意事项

- 将第三方身份验证插件安装在所有节点上，然后再将其联合到一起。
- 在一个节点上配置所有委派表单身份验证相关设置，然后将更改传播到其他节点。请参阅“启用委派表单身份验证”。

启用委派表单身份验证

因为 StoreFront 中没有用于设置 Citrix 预共享密钥设置的 GUI，所以请使用 PowerShell 控制台安装委派表单身份验证。

1. 安装委派表单身份验证。默认情况下其并未安装，您需要使用 PowerShell 控制台进行安装。

```
PS C:\Users\administrator.PTD.000> cd 'C:\Program Files\Citrix\
    Receiver StoreFront\Scripts'
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> & .\
    ImportModules.ps1
Adding snapins
Importing modules
Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.
    DeliveryServices.ConfigurationProvider.dll'
Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.
    DeliveryServices.ConfigurationProvider.dll'

```



```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Install-DSDFAServer
Id                              : bf694fbc-ae0a-4d56-8749-c945559e897a
ClassType                       : e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc
FrameworkController             : Citrix.DeliveryServices.Framework.FileBased.FrameworkController
ParentInstance                  : 8dd182c7-f970-466c-ad4c-27a5980f716c
RootInstance                    : 5d0cdc75-1dee-4df7-8069-7375d79634b3
TenantId                        : 860e9401-39c8-4f2c-928d-34251102b840
Data                            : {
  }

ReadOnlyData                    : {
 [Name, DelegatedFormsServer], [Cmdlet, Add-DSWebFeature], [Snapin, Citrix.DeliverySer
                                   vices.Web.Commands], [Tenant, 860e9401-39c8-4f2c-928d-34251102b840] }

ParameterData                   : {
 [FeatureClassId, e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc], [ParentInstanceId, 8dd182c7-f
                                   970-466c-ad4c-27a5980f716c], [TenantId, 860e9401-39c8-4f2c-928d-34251102b840] }

AdditionalInstanceDependencies : {
 b1e48ef0-b9e5-4697-af9b-0910062aa2a3 }

IsDeployed                      : True
FeatureClass                    : Citrix.DeliveryServices.Framework.Feature.FeatureClass
<!--NeedCopy-->
```

2. 添加 Citrix 可信客户端。配置 StoreFront 与 Citrix ADC 设备之间的共享秘密密钥（密码）。您的密码和客户端 ID 必须与在 Citrix ADC 设备中配置的相同。

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Add-DSCitrixPSKTrustedClient -clientId netscaler.fqdn.com -passphrase secret
<!--NeedCopy-->
```

3. 设置委派表单身份验证对话工厂，以将所有流量路由到自定义表单。要找到对话工厂，请在 C:\inetpub\wwwroot\Citrix\Authentication\web.config 中查找 ConversationFactory。以下是您可能看到的示例。

```
<example connectorURL="http://Example.connector.url:8080/adapters-
```



```
      sf-aaconnector-webapp">
1        <routeTable order="1000">
2          <routes>
3            <route name="StartExampleAuthentication" url="Example-
                Bridge-Forms/Start">
4              <defaults>
5                <add param="controller" value="
                    ExplicitFormsAuthentication" />
6                <add param="action" value="AuthenticateStart" />
7                <add param="postbackAction" value="Authenticate" />
8                <add param="cancelAction" value="CancelAuthenticate"
                     />
9                <add param="conversationFactory" value="
                    ExampleBridgeAuthentication" />
10               <add param="changePasswordAction" value="
                    StartChangePassword" />
11               <add param="changePasswordController" value="
                    ChangePassword" />
12               <add param="protocol" value="CustomForms" />
13             </defaults>
14           </route>
15 <!--NeedCopy-->
16
```

4. 在 PowerShell 中，设置委派表单身份验证对话工厂。在此示例中，设置为 ExampleBridgeAuthentication。

```
1 PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Set-
     DSDFAProperty -ConversationFactory ExampleBridgeAuthentication
2 <!--NeedCopy-->
```

PowerShell 的参数不区分大小写：**-ConversationFactory** 与 **-conversationfactory** 相同。

卸载 **StoreFront**

卸载 StoreFront 之前，请先卸载所有第三方身份验证插件，因为它将影响 StoreFront 的功能。

使用不同的域进行身份验证

April 17, 2024

某些组织配置了一些策略，这些策略不允许这些组织向第三方开发人员或合同工提供对生产环境中的已发布资源的访问权限。本文介绍如何在一个域内通过 Citrix Gateway 进行身份验证来提供对测试环境中的已发布资源的访问权限。您随后可以使用不同的域对 StoreFront 和 Receiver for Web 站点进行身份验证。对于通过 Receiver for Web 站点登录的用户，本文中介绍的“通过 Citrix Gateway 进行身份验证”不受支持。对于本机桌面或移动 Citrix Receiver 或 Citrix Workspace 应用程序，此身份验证方法不受支持。

设置测试环境

此示例使用名为 production.com 的生产域和名为 development.com 的测试域。

`production.com` 域

此示例中的 `production.com` 域的设置方式如下所示：

- Citrix Gateway 配置了 `production.com` LDAP 身份验证策略。
- 通过网关进行的身份验证使用 production\testuser1 帐户和密码进行。

`development.com` 域

此示例中的 `development.com` 域的设置方式如下所示：

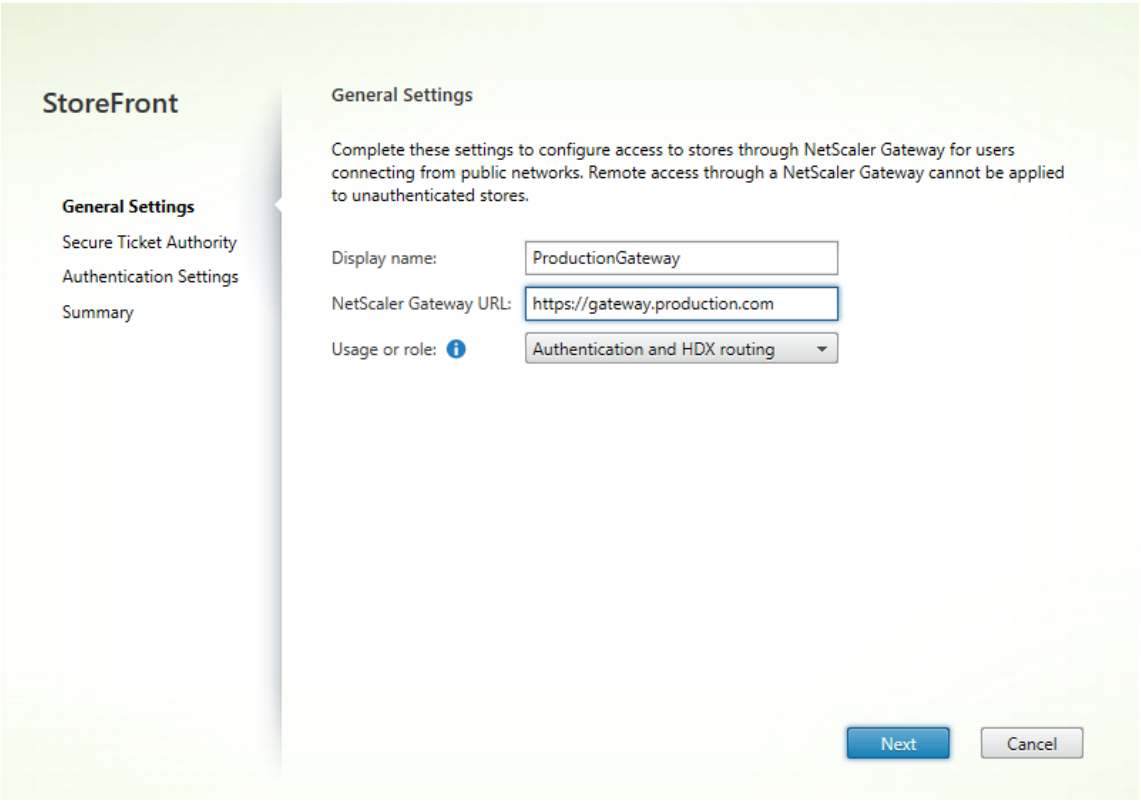
- StoreFront、Citrix Virtual App and Desktops 和 VDA 均位于 `development.com` 域中。
- 对 Citrix Receiver for Web 站点进行的身份验证使用 development\testuser1 帐户和密码进行。
- 这两个域之间不存在信任关系。

为应用商店配置 **Citrix Gateway**

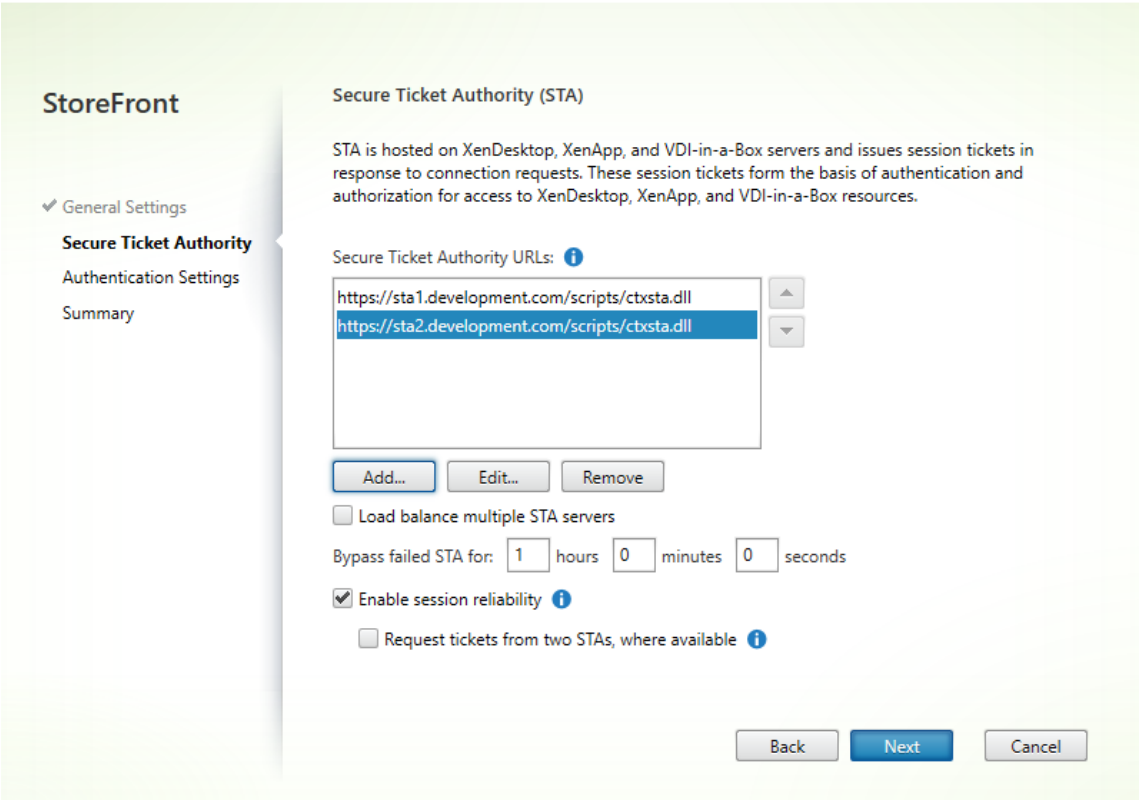
要为应用商店配置 Citrix Gateway，请执行以下操作：

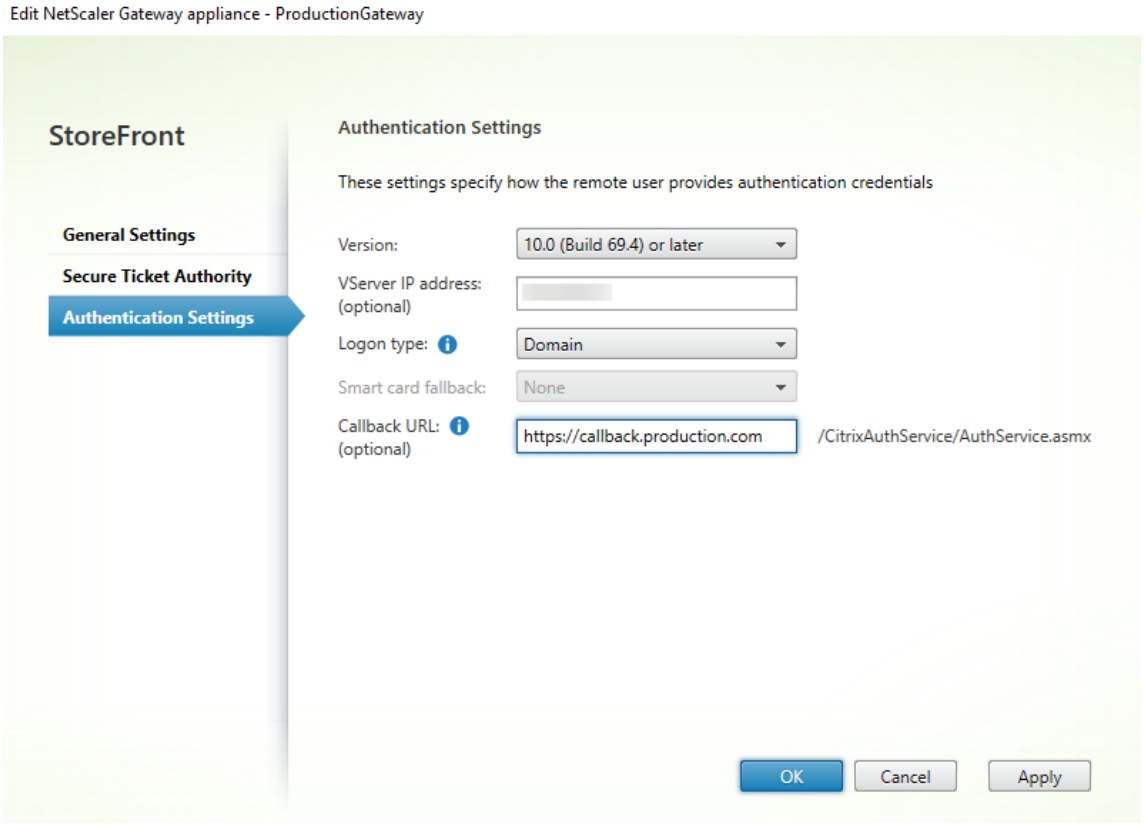
1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店，然后在操作窗格中单击管理 **Citrix Gateway**。
2. 在“管理 Citrix Gateway”屏幕中，单击添加。
3. 完成“常规设置”、“Secure Ticket Authority”和“身份验证”步骤。

Add NetScaler Gateway Appliance



Add NetScaler Gateway Appliance

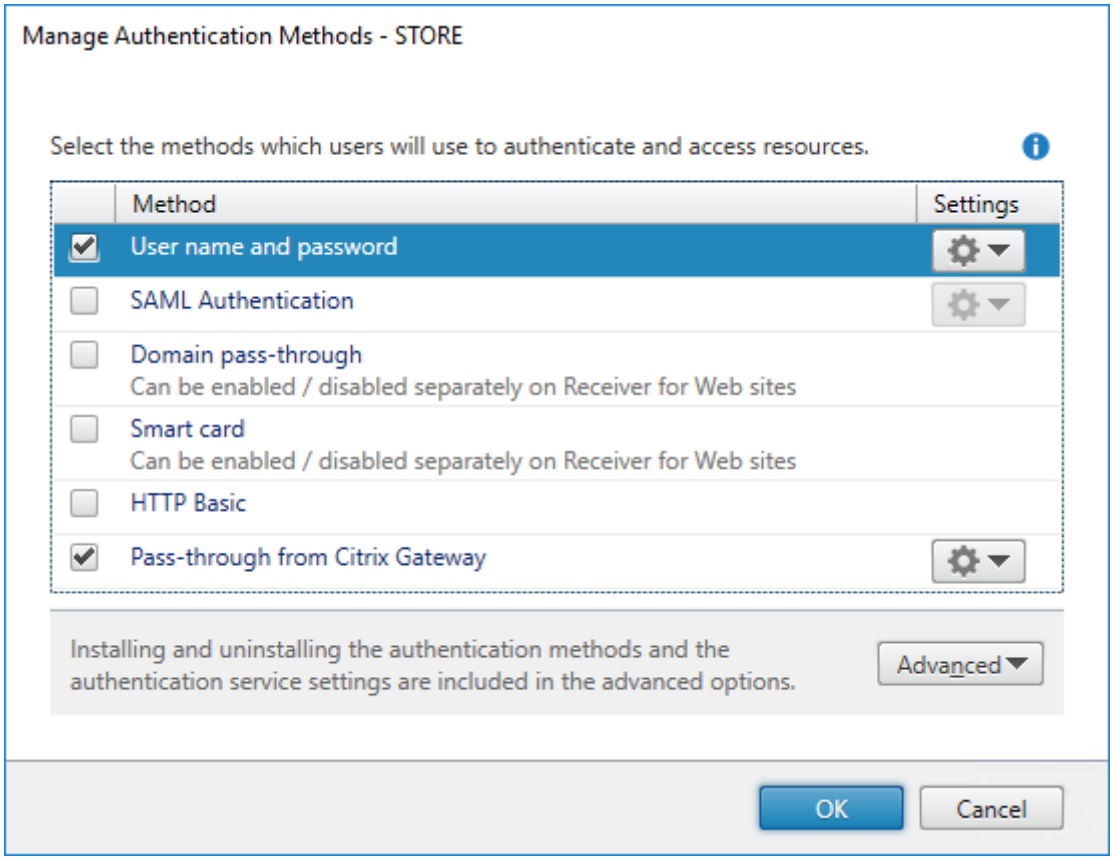




> 注意：
>
> 可能需要添加 DNS 条件转发器，以便这两个域中正在使用的 DNS 服务器可以解析另一个服务器上的 FQDN。Citrix ADC 设备必须能够使用其 `production.com` DNS 服务器解析 `development.com` 域中的 STA 服务器 FQDN。StoreFront 还应能够使用其 `development.com` DNS 服务器解析 `production.com` 域中的回调 URL。此外，还可以使用 `development.com` FQDN，该地址被解析为 Citrix Gateway 虚拟服务器的虚拟 IP (VIP)。

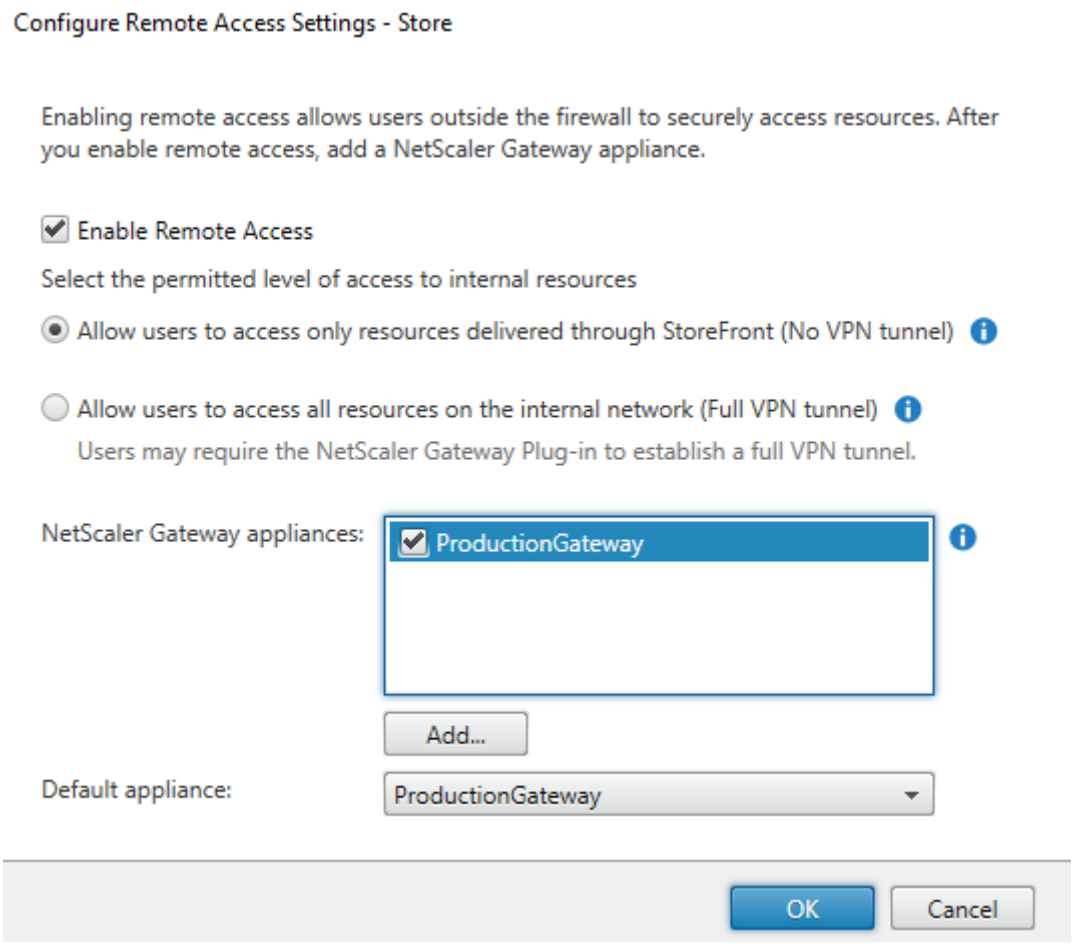
启用从 **Citrix Gateway** 直通

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店，然后在操作窗格中单击管理身份验证方法。
2. 在“管理身份验证方法”屏幕中，选择从 **Citrix Gateway** 直通。
3. 单击确定。



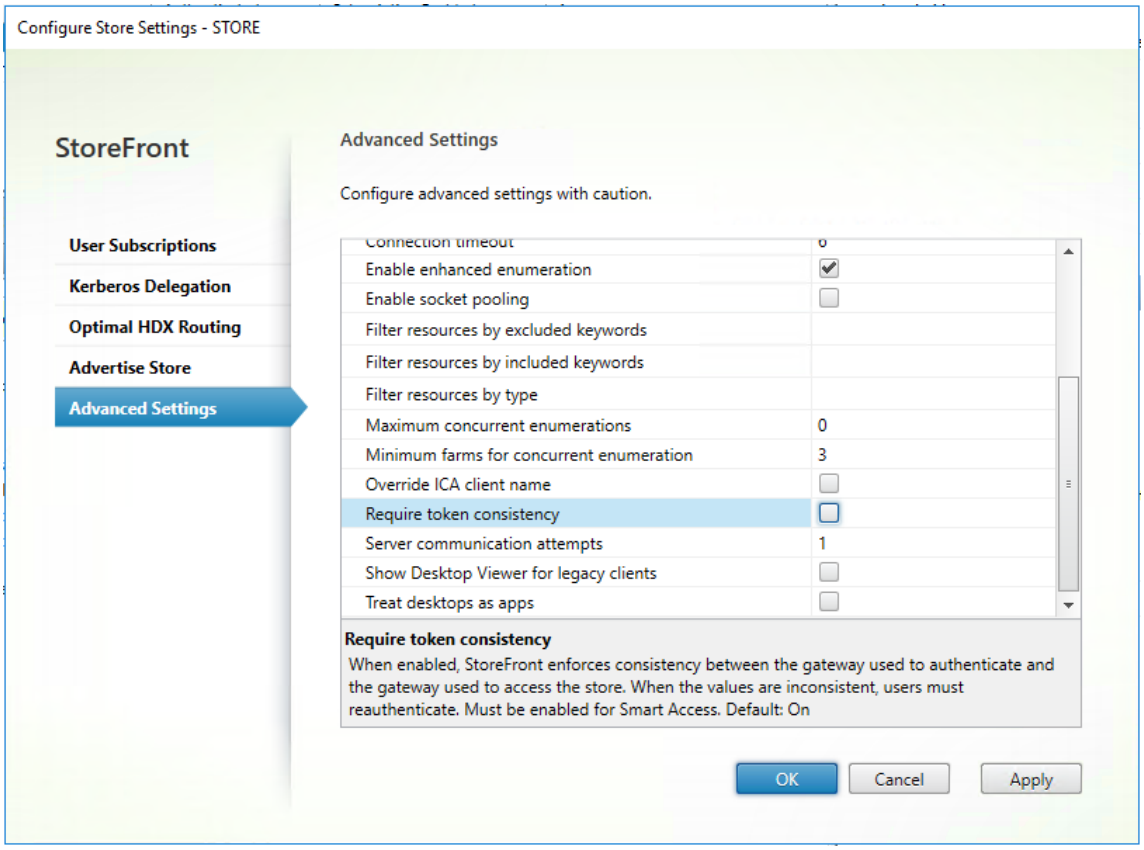
配置应用商店以便使用网关进行远程访问

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点，然后在结果窗格中选择一个应用商店。在操作窗格中，单击配置远程访问设置。
2. 选择启用远程访问。
3. 请确保您已在自己的应用商店中注册 Citrix Gateway。如果未注册 Citrix Gateway，STA 票证将不起作用。



禁用令牌一致

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点，然后在结果窗格中选择一个应用商店。在操作窗格中，单击配置应用商店设置。
2. 在“配置应用商店设置”页面上，选择高级设置。
3. 取消选中要求令牌一致复选框。有关详细信息，请参阅高级应用商店设置。



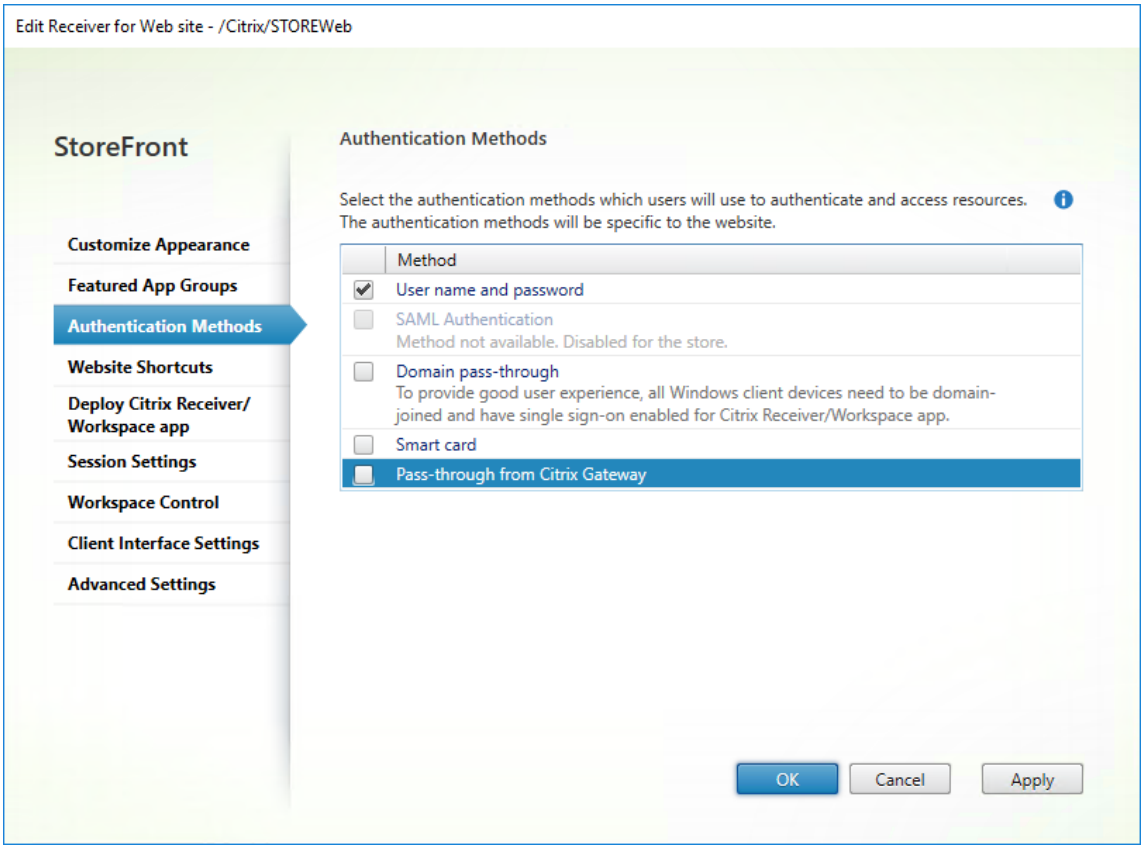
4. 单击确定。

> 注意：
>
> “要求令牌一致”设置默认处于选中状态。如果禁用此设置，用于 Citrix ADC 端点分析 (EPA) 的 SmartAccess 功能将停止运行。有关 SmartAccess 的详细信息，请参阅 CTX138110。

对 **Receiver for Web** 站点禁用从 **Citrix Gateway** 直通

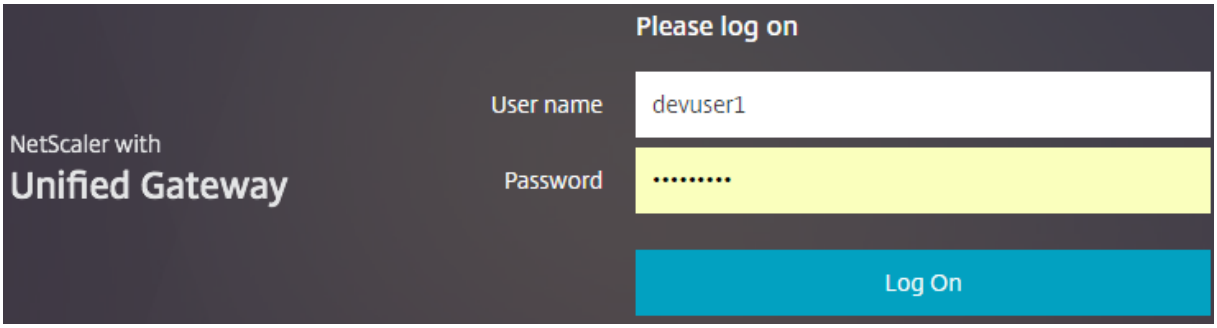
> 重要提示：
>
> 禁用从 Citrix Gateway 直通将阻止 Receiver for Web 尝试使用 `production.com` 域中不正确的凭据从 Citrix ADC 设备通过。禁用从 Citrix Gateway 直通会导致 Receiver for Web 提示用户输入凭据。这些凭据与用于通过 Citrix Gateway 登录的凭据不同。

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点。
2. 选择要修改的应用商店。
3. 在操作窗格中，单击管理 **Receiver for Web** 站点。
4. 在“管理身份验证方法”中，取消选择从 **Citrix Gateway** 直通。
5. 单击确定。

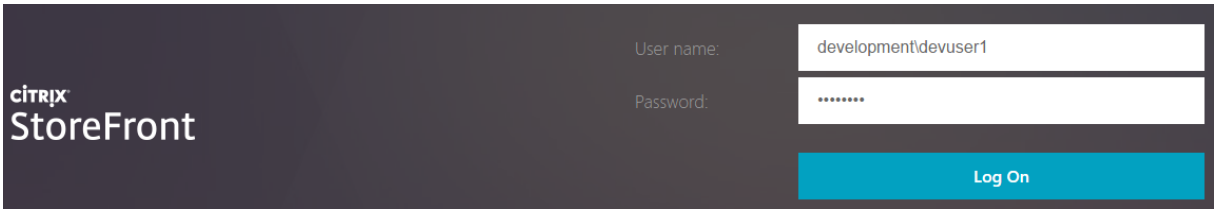


使用 **production.com** 用户和凭据登录网关

要进行测试，请使用 production.com 用户和凭据登录网关。



登录后，系统将提示用户输入 development.com 凭据。

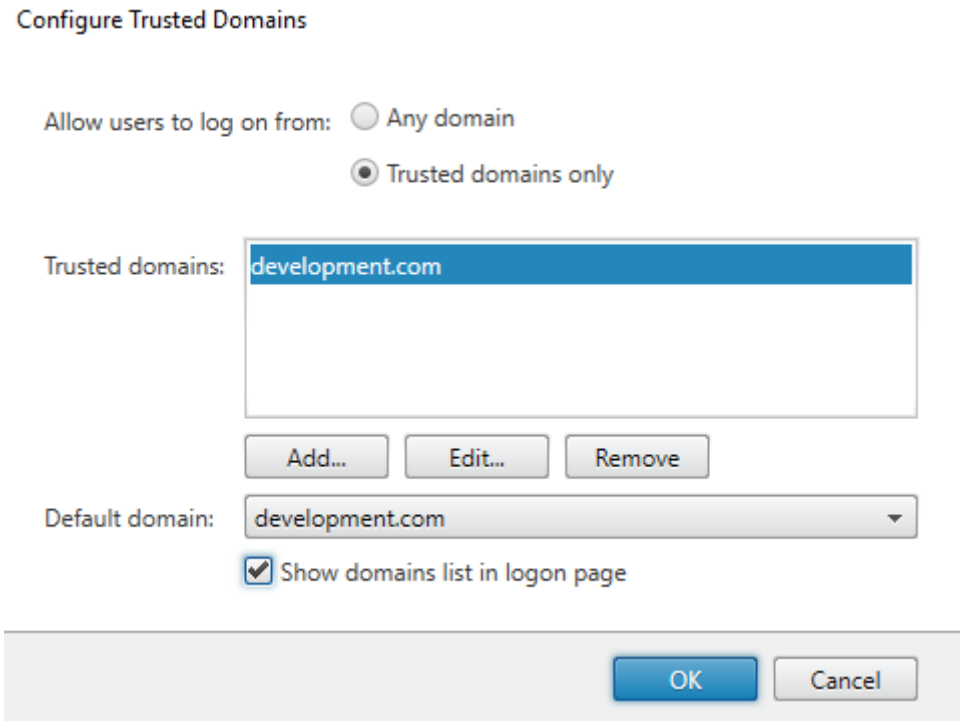


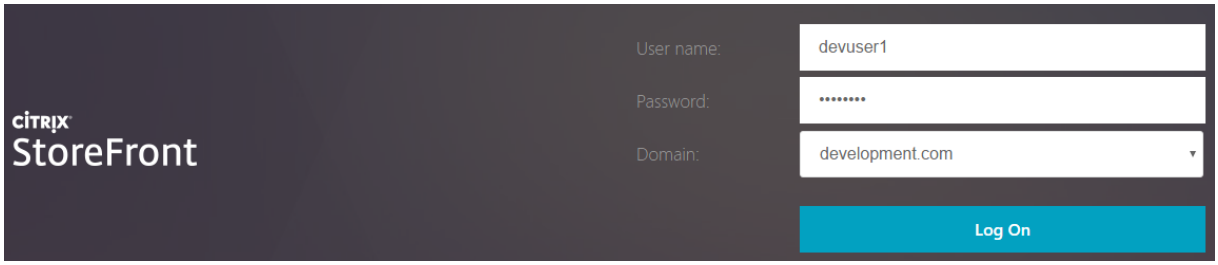
在 **StoreFront** 中添加可信域下拉列表（可选）

此设置为可选设置，但可以帮助阻止用户意外输入错误的域以通过 Citrix Gateway 进行身份验证。

如果用户名与这两个域的用户名相同，输入错误域的可能性更大。新用户通过 Citrix Gateway 登录时，也可能会使用新用户退出域。系统提示用户登录 Receiver for Web 站点时，这些用户随后也可能会忘记输入第二个域的域\用户名。

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店，然后在操作窗格中单击管理身份验证方法。
2. 选择用户名和密码旁边的下拉箭头。
3. 单击添加将 `development.com` 添加为可信域，然后选中在登录页面中显示域列表复选框。
4. 单击确定。

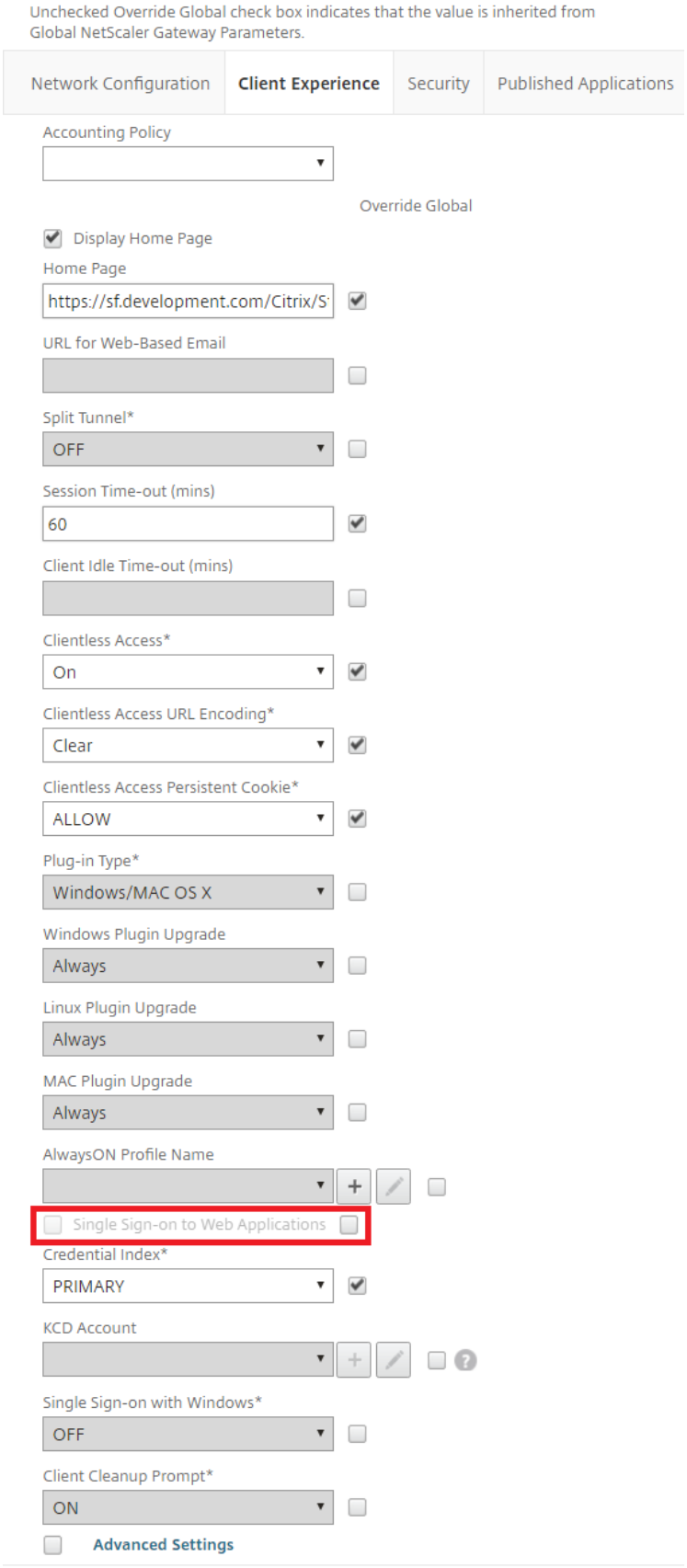


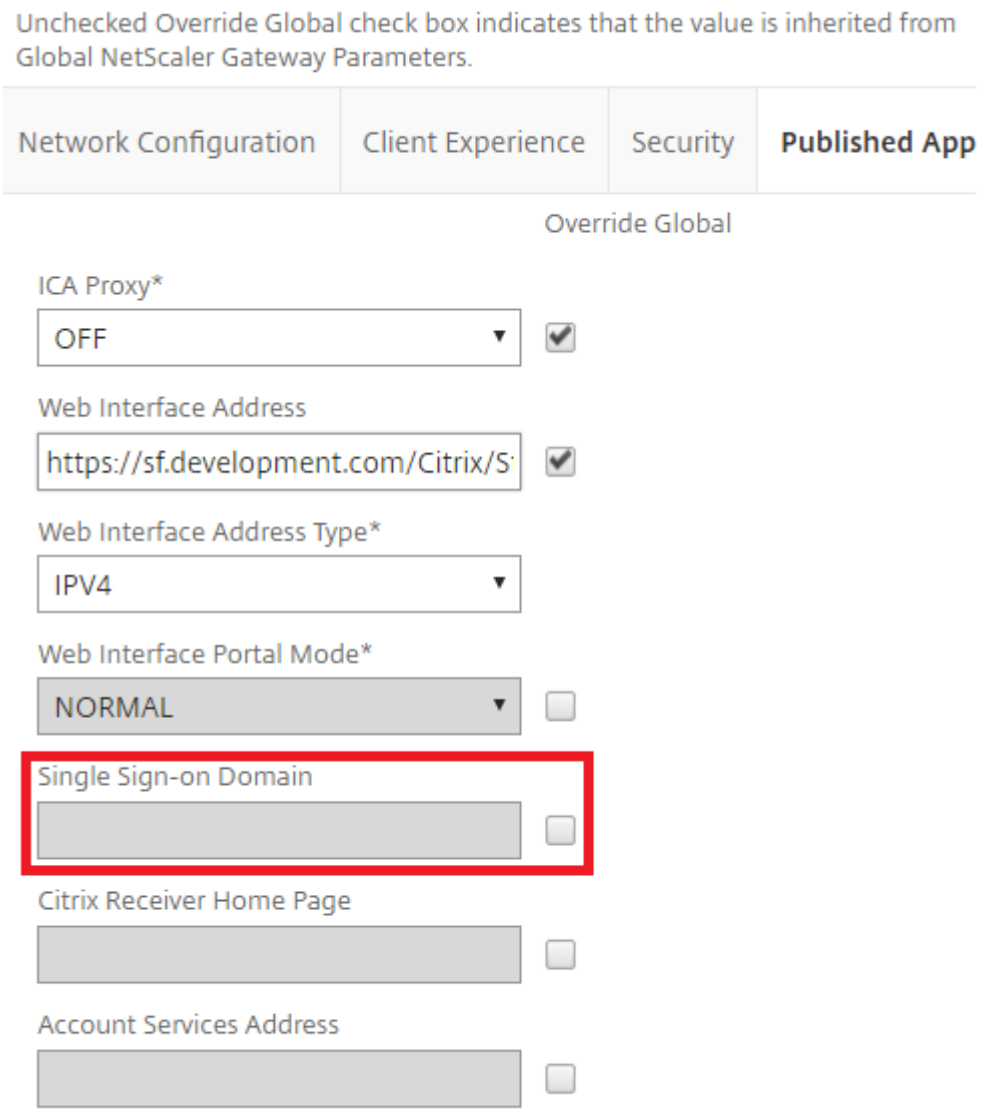


> 注意：
>
> 不建议在此身份验证场景中使用浏览器密码缓存。如果用户为两个不同的域帐户设置了不同的密码，密码缓存会导致体验较差。

Citrix Gateway 无客户端 **VPN (CVPN)** 会话操作策略

- 如果在您的 Citrix Gateway 会话策略中启用了“单点登录到 Web 应用程序”，Citrix ADC 设备向 Receiver for Web 发送的不正确的凭据将被忽略，因为您已在 Receiver for Web 站点上禁用从 **Citrix Gateway** 直通身份验证方法。无论此选项的设置为何，Receiver for Web 都会提示输入凭据。
- 在 Citrix ADC 设备中的“Client Experience”（客户端体验）和“Published App”（已发布的应用程序）选项卡中填充单点登录条目不会改变本文中介绍的行为。





配置信标点

April 17, 2024

可以通过执行“管理信标”任务指定在内部网络内外用作信标点的 URL。Citrix Workspace 应用程序尝试联系信标点并根据响应来确定用户是连接到本地网络还是公用网络。用户访问桌面或应用程序时，位置信息将传递给提供资源的服务器，以便能够将相应的连接详细信息返回给 Citrix Workspace 应用程序。这样可以确保在用户访问桌面或应用程序时不会收到重新登录提示。

例如，如果可访问内部信标点，这表示用户已连接到本地网络。但是，如果 Citrix Workspace 应用程序无法联系内部

信标点，并且收到来自两个外部信标点的响应，这表示用户具有 Internet 连接，但位于企业网络外部。因此，用户必须通过 Citrix Gateway 连接到桌面和应用程序。用户访问桌面或应用程序时，提供资源的服务器将收到通知，通知其提供必须借助其对连接进行路由的 Citrix Gateway 设备的详细信息。这意味着用户在访问桌面或应用程序时不需要登录该设备。

默认情况下，StoreFront 设置：

- 指向部署的基本 URL 的内部信标。
- 指向 `http://ping.citrix.com` 的外部信标和您添加的第一个 Citrix Gateway 部署的 URL。

如果您更改了任何信标点，请确保用户将修改过的信标信息更新到 Citrix Workspace 应用程序中。用户可以从适用于 HTML5 的 Citrix Workspace 应用程序中获取更新后的 Citrix Workspace 应用程序预配文件。否则，可以为应用商店导出预配文件，并将此文件提供给用户。

> 重要：
>
> 在多服务器部署中，请一次仅使用一台服务器以更改服务器组的配置。确保 Citrix StoreFront 管理控制台未在部署中的任何其他服务器上运行。完成后，请
> 将对配置所做的更改传播到服务器组，以便更新部署中的其他服务器。

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点，然后在“操作”窗格中单击管理信标。
2. 指定要用作内部信标点的 URL。
   - 要使用 StoreFront 部署的服务器 URL 或负载平衡 URL，请选择使用服务 **URL**。
   - 要使用备用 URL，请选择指定信标地址，并输入内部网络中的一个高可用性 URL。
3. 单击添加输入外部信标点的 URL。要修改信标点，请选择“外部信标”列表中的 URL，然后单击编辑。在列表中选择一个 URL，然后单击删除以停止将该地址用作信标点。

   必须至少指定两个可从公用网络解析的高可用外部信标点。信标 URL 应为完全限定的域名 (`http://example.com`)，而非缩写形式的 NetBIOS 名称 (`http://example`)。以便 Citrix Workspace 应用程序能够确定用户是否位于 Internet 付费墙之后，例如在酒店或网吧中。在此类情况下，所有外部信标点将连接至同一个代理。

   > 注意：
   >
   > 请勿将您不拥有的第三方 Web 站点用作外部信标。请改为使用 `http://ping.citrix.com` 或者贵组织控制的 Web 站点。

创建内部和外部使用的单个 **FQDN**

February 22, 2024

您可以创建单个完全限定的域名 (FQDN)，该域名可以直接从公司网络内访问应用商店，也可以通过 Citrix Gateway 远程访问应用商店。

在以下文档中，它以以下示例为例：

- `https://storefront.example.com` 作为用户访问 StoreFront 时使用的单一 URL。在网络内部时，它会解析到 StoreFront 服务器或负载平衡器。在网络外部时，它会解析到网关。
- `https://storefrontcb.example.com` 作为回调 URL。这在内部解析到网关。只有智能访问或无密码身份验证需要。

服务器组基本 **URL**

将基本 URL 更改为单一 URL。请参阅更改部署的基本 URL。

Citrix Workspace 应用程序的 **StoreFront** 信标

本地安装的 Citrix Workspace 应用程序尝试联系信标点并根据响应来确定用户是连接到本地网络还是公用网络。

默认情况下，StoreFront 使用服务器组基本 URL 作为内部信标 URL。在此配置中，相同的 URL 在内部和外部均有效，因此不能用作信标。因此，必须将内部信标设置为一个您知道只能在内部进行访问的 URL。

请参阅配置信标。

外部 **DNS**

- storefront.example.com 解析为 Citrix Gateway 虚拟服务器的面向外部的 IP。

内部 **DNS**

- storefront.example.com 解析为 StoreFront 负载平衡器或单个 StoreFront 服务器 IP。
- storefrontcb.example.com 解析为网关虚拟服务器 VIP。如果 DMZ 与企业本地网络之间存在防火墙，则允许这样做。

导出和导入 **StoreFront** 配置

April 17, 2024

> 注意：
>
> 只能导入与目标 StoreFront 安装完全相同的 StoreFront 版本的 StoreFront 配置。针对此限制，每个累积更新都被视为不同的产品版本。

可以导出 StoreFront 部署的完整配置。这包括单个服务器部署和服务器组配置。如果现有部署已经存在于导入服务器上，当前配置将被擦除，然后替换为备份存档中包含的配置。如果目标服务器是全新的出厂默认安装，将使用存储在备份中的导入配置创建新部署。如果未加密，导出的配置备份将采用单个.zip 存档的形式存储，如果在创建时选择加密备份文件，导出的配置备份将以.ctxzip 的形式存储。

可以使用配置导出和导入的方案

- 仅备份处于工作状态和受信任状态的 StoreFront 部署。对配置所做的任何更改都需要创建新备份来替换旧备份。您无法修改现有备份，因为 backup.zip 文件的文件哈希可防止修改。
- 升级 StoreFront 之前进行备份以进行灾难恢复。
- 克隆现有的测试 StoreFront 部署以投入生产
- 通过将生产部署克隆到测试环境来创建用户接受环境。
- 在操作系统迁移期间移动 StoreFront，例如将托管操作系统从 Window Server 2019 升级到 Windows 2022。不支持原位操作系统升级。
- 在多地理部署（例如，具有多个数据中心的大型企业）中构建额外的服务器组。

导出和导入 **StoreFront** 配置时的注意事项

- 当前是否使用了任何 Citrix 已发布身份验证 SDK 示例，例如魔术字身份验证或第三方身份验证自定义？如果是，则必须在导入包含额外身份验证方法的配置之前，在所有导入服务器上安装这些包。如果某些导入服务器上未安装所需的身份验证 SDK 包，配置导入操作将失败。如果要将配置导入到服务器组中，请在组的所有成员上安装身份验证包。
- 可以加密或解密配置备份。导出和导入 PowerShell cmdlet 支持这两种用例。
- 可以在以后解密经过加密的备份 (.ctxzip)，但是 StoreFront 无法重新加密解密后的备份文件 (.zip)。如果需要使用经过加密的备份，请使用包含所选密码的 PowerShell 凭据对象重新执行导出。
- IIS 中当前已安装 StoreFront 的 Web 站点（导出服务器）的 SiteID 必须与 IIS 中需还原为已备份的 StoreFront 配置的目标 Web 站点（导入服务器）的 SiteID 匹配。

PowerShell cmdlet

Export-STFConfiguration

参数	说明
-TargetFolder (字符串)	备份存档的导出路径。示例:”$env:userprofile\desktop\”
-Credential（PSCredential 对象）	在导出时指定凭据对象以创建加密的.ctxzip 备份存档。PowerShell 凭据对象应包含用于加密和解密的密码。请勿同时使用 **-Credential** 和 **-NoEncryption** 参数。示例：$CredObject
-NoEncryption（开关）	指定备份存档应采用未加密的.zip 形式。请勿同时使用 **-NoEncryption** 和 **-Credential** 参数。
-ZipFileName (字符串)	StoreFront 配置备份存档的名称。请勿添加文件扩展名，例如.zip 或.ctxzip。系统根据导出期间指定的是 **-Credential** 参数还是 **-NoEncryption** 参数来自动添加文件扩展名。示例:”backup”
-Force（布尔值）	此参数自动覆盖与指定导出位置中已存在的现有备份文件同名的备份存档。

> 重要提示:
>
> StoreFront 3.5 中的 **SiteID** 参数在版本 3.6 中已弃用。在执行导入时，不再需要指定 **SiteID**，因为始终会使用备份存档中包含的 SiteID。请确保 SiteID 与已在导入服务器上的 IIS 中配置的现有 StoreFront Web 站点相匹配。不支持 **SiteID 1** 至 **SiteID 2** 的配置导入。

Import-STFConfiguration

参数	说明
-ConfigurationZip (字符串)	要导入的备份存档的完整路径。此值还应该包含文件扩展名。未加密的备份存档使用.zip，加密的备份存档使用.ctxzip。示例：`$env:userprofile\desktop\backup.ctxzip`
-Credential（PSCredential 对象）	指定在导入时解密经过加密的备份所使用的凭据对象。示例：`$CredObject`
-HostBaseURL (字符串)	如果包含此参数，则将使用您指定的主机基本 URL，而不使用导出服务器中的主机基本 URL。示例：`https://<importingserver>.example.com`

Unprotect-STFConfigurationBackup

参数	说明
-TargetFolder (字符串) -Credential（PSCredential 对象）	备份存档的导出路径。示例： $env:userprofile\desktop 使用此参数将创建加密备份存档的未加密副本。指定包含解密密码的 PowerShell 凭据对象。示例： `$CredObject`
-EncryptedConfigurationZip (字符串)	要解密的加密备份存档的完整路径。必须指定文件扩展名.ctxzip。示例：`$env:userprofile\\desktop\\backup.ctxzip`
-OutputFolder (字符串) -Force（布尔值）	创建加密备份存档 (.ctxzip) 的取消加密副本 (.zip) 的路径。最初的加密备份副本将保留，以便重复使用。请勿指定取消加密副本的文件名和文件扩展名。示例： $env:userprofile\desktop 此参数自动覆盖与指定导出位置中已存在的现有备份文件同名的备份存档。

配置导出和导入示例

将 **StoreFront cmdlet** 导入到当前的 **PowerShell** 会话

在 StoreFront 服务器上打开 PowerShell 集成脚本环境 (ISE) 并运行以下命令：

```
$env:PSModulePath = [Environment]::GetEnvironmentVariable('PSModulePath','Machine')
$SDKModules = 'C:\Program Files\Citrix\Receiver StoreFront\PowerShellSDK\Modules\Citrix.StoreFront'
Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose
Import-Module "$SDKModules.Authentication\Citrix.StoreFront.Authentication.psd1" -verbose
Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1" -verbose
Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -verbose
Import-Module "$SDKModules.WebReceiver\Citrix.StoreFront.WebReceiver.psd1" -verbose
<!--NeedCopy-->
```

单服务器场景

创建服务器 **A** 上现有配置的未加密备份并将其还原到相同的部署　导出要备份的服务器的配置。


```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop" -
    zipFileName "backup" -NoEncryption
<!--NeedCopy-->
```

将 backup.zip 文件复制到安全的位置。可以使用此备份进行灾难恢复，将服务器还原到以前的状态。

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://storefront.example.com"
<!--NeedCopy-->
```

备份服务器 **A** 上的现有配置并将其还原到服务器 **B** 以创建现有服务器的克隆　导出要备份的服务器的配置。

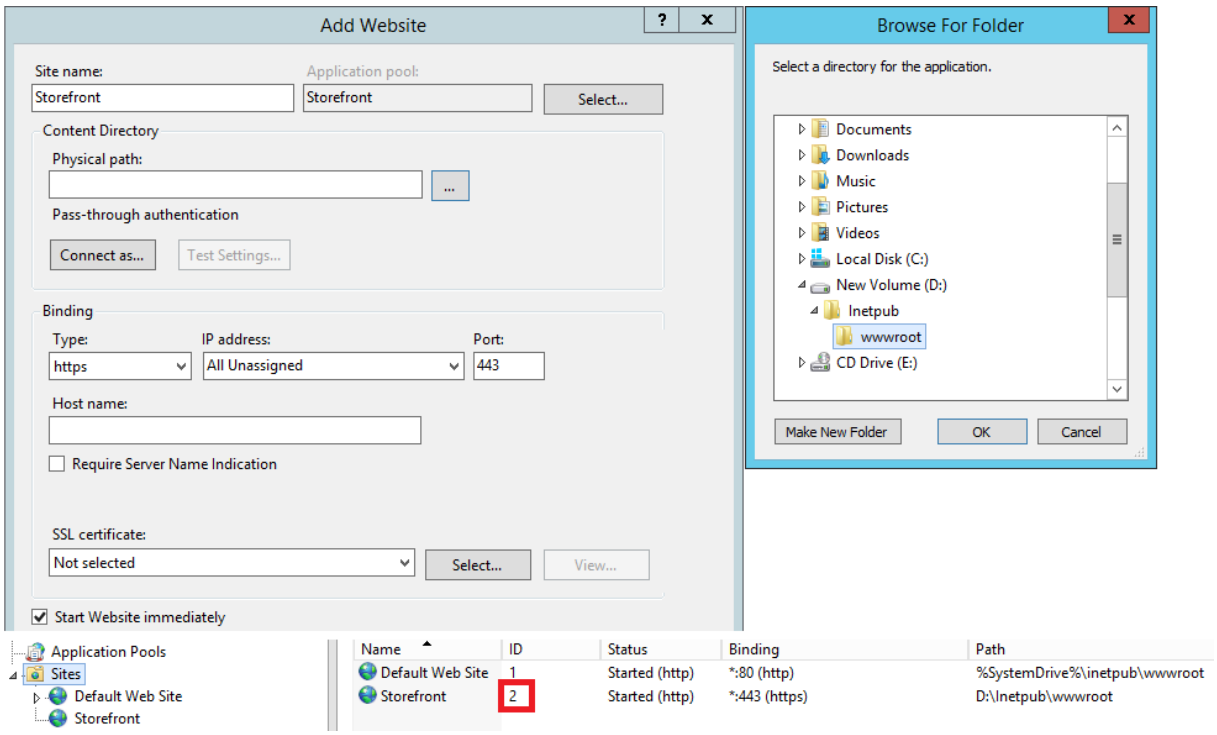
```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop" -
    zipFileName "backup" -NoEncryption
<!--NeedCopy-->
```

将 backup.zip 文件复制到服务器 B 的桌面。

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://serverB.example.com"
<!--NeedCopy-->
```

StoreFront 已经部署到 **IIS** 中的自定义 **Web** 站点上。将配置还原到另一个自定义 **Web** 站点部署上　服务器 A 具有部署到自定义 Web 站点位置上的 StoreFront，不使用 IIS 内的常用默认 Web 站点。在 IIS 内创建的第二个 Web 站点的 IIS SiteID 为 2。StoreFront Web 站点的物理路径可以位于另一个非系统驱动器上（例如 d:\）或默认的 c:\ 系统驱动器上，但应使用大于 1 的 IIS SiteID。

已在 IIS 中配置名为 StoreFront 的新 Web 站点，该站点使用 **SiteID = 2**。StoreFront 已经使用其位于驱动器 `d:\inetpub\wwwrooot` 上的物理路径部署到 IIS 中的自定义 Web 站点上。



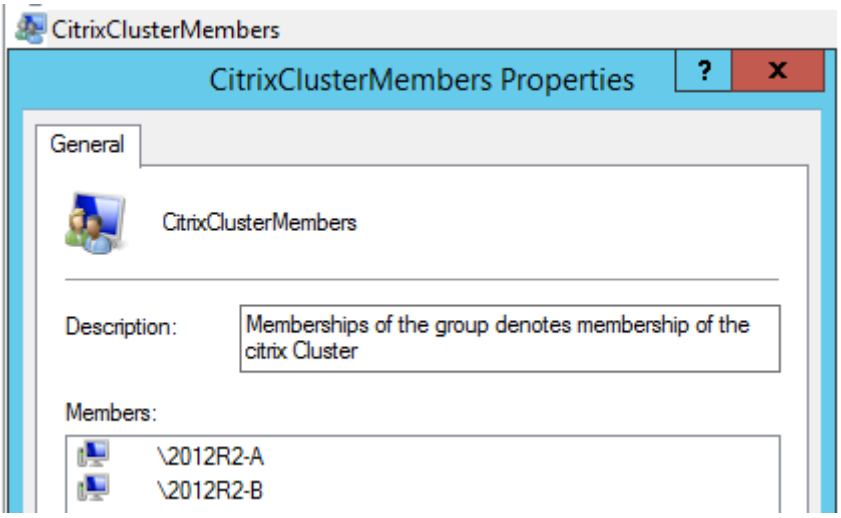
1. 导出服务器 A 配置的副本。
2. 在服务器 B 上，在 IIS 中配置一个名为 **StoreFront** 的新 Web 站点，该站点也使用 **SiteID 2**。
3. 将服务器 A 配置导入到服务器 B。使用备份中包含的站点 ID，且该站点 ID 必须与您要在其中导入 StoreFront 配置的目标 Web 站点相匹配。

```
Import-STFConfiguration -configurationZip "$env:userprofile\
    desktop\backup.ctxzip" -HostBaseURL "https://serverB.example.
    com"
<!--NeedCopy-->
```

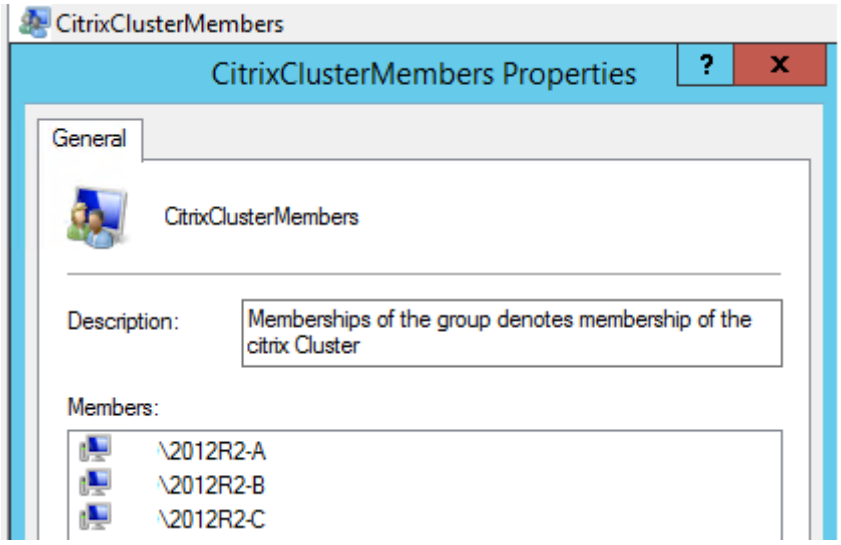
服务器组场景

场景 **1**：备份现有服务器组配置，然后将其还原到相同的服务器组部署中　当服务器组只有两个 StoreFront 服务器成员 (2012R2-A 和 2012R2-B) 时，已经执行过配置备份。执行备份时，备份存档内是一条仅包含两个原始服务器 2012R2-A 和 2012R2-B 的 **CitrixClusterMembership** 记录。执行初始备份后，由于业务需要，StoreFront 服务器组部署的规模增加，服务器组中又增加了另一个节点 2012R2-C。备份中保留的服务器组基础 StoreFront 配置已经发生变化。即使导入了仅包含两个初始服务器组节点的旧备份，但也必须维护三个服务器当前的 CitrixClusterMembership。在导入过程中，将保留当前的群集成员关系，然后在配置成功导入到主服务器上之后执行写回。如果在执行初始备份之后，从服务器组删除服务器组节点，导入还会保留当前的 CitrixClusterMembership。

1. 从 2012R2-A 中导出服务器组 1 配置，该服务器是用于管理整个服务器组的主服务器。



2. 然后将另一台服务器 2012R2-C 添加到现有服务器组中。



3. 必须将服务器组的配置还原到之前的某个已知工作状态。StoreFront 在导入过程中将备份三台服务器的当前 CitrixClusterMembership，并在导入成功后进行还原。

4. 将服务器组 1 配置重新导入到 2012R2-A 节点上。

```
Import-STFConfiguration -configurationZip "$env:userprofile\
    desktop\backup.ctxzip" -HostBaseURL "https://servergroup1.
    example.com"
<!--NeedCopy-->
```

5. 将新导入的配置传播到整个服务器组，从而使所有服务器在导入后具有一致的配置。

场景 **2**：备份服务器组 **1** 的现有配置，使用此备份在另一个出厂默认安装上创建新的服务器组。然后，可以将其他新服务器组成员添加到新的主服务器　创建包含两个新服务器（2012R2-C 和 2012R2-D）的服务器组 2。服务器组 2 配置将基于现有部署（即服务器组 1）的配置，服务器组 1 也包含两个服务器 2012R2-A 和 2012R2-B。创建新服务器组时

不使用备份存档中包含的 CitrixClusterMembership。始终备份当前的 CitrixClusterMembership 并在导入成功后进行还原。使用导入的配置创建新部署时，CitrixClusterMembership 安全组将仅包含导入服务器，直至将更多服务器加入新组。服务器组 2 是新部署，计划与服务器组 1 同时存在。指定 -HostBaseURL 参数。服务器组 2 将使用新的出厂默认 StoreFront 安装进行创建。

1. 从 2012R2-A 中导出服务器组 1 配置，该服务器是用于管理整个服务器组的主服务器。
2. 将服务器组 1 配置导入到节点 2012R2-C 上，此节点将作为管理新创建的服务器组 2 的主服务器。

```
Import-STFConfiguration -configurationZip "$env:userprofile\
    desktop\backup.ctxzip" -HostBaseURL "https://servergroup2.
    example.com"
<!--NeedCopy-->
```

3. 加入将要成为新服务器组 2 部署一部分的任何其他服务器。从服务器组 1 新导入的配置传播到服务器组 2 所有新成员的过程是自动的，该过程属于添加新服务器时的正常加入流程的一部分。

场景 **3**：备份服务器组 **A** 的现有配置，使用此备份覆盖现有服务器组 **B** 的配置　服务器组 1 和服务器组 2 已经存在于两个单独的数据中心内。很多 StoreFront 配置更改在服务器组 1 上进行，您应该将这些更改应用到另一个数据中心内的服务器组 2 中。您可以将更改从服务器组 1 导出到服务器组 2。请勿在服务器组 2 上的备份存档中使用 **CitrixClusterMembership**。导入时请指定 **-HostBaseURL** 参数，因为服务器组 2 主机基本 URL 不应该更改为与服务器组 1 当前所使用的 FQDN 相同。服务器组 2 为现有部署。

1. 从 2012R2-A 中导出服务器组 1 配置，该服务器是用于管理整个服务器组的主服务器。
2. 将服务器组 1 配置导入到节点 2012R2-C 上的出厂默认安装中，此节点将作为新服务器组 2 的主服务器。

```
Import-STFConfiguration -configurationZip "$env:userprofile\
    desktop\backup.zip" -NoEncryption -HostBaseURL "https://
    servergroup2.example.com"
<!--NeedCopy-->
```

创建服务器配置的加密备份

PowerShell 凭据对象由 Windows 帐户用户名和密码组成。PowerShell 凭据对象可确保密码在内存中处于安全状态。

> 注意：
>
> 要加密配置备份存档，只需要使用密码执行加密和解密。无需使用凭据对象内存储的用户名。必须在 PowerShell 会话内创建包含相同密码的凭据对象（同时用于导出和导入服务器）。在凭据对象内，可以指定任何用户。

PowerShell 要求您在创建新凭据对象时指定用户。为方便起见，此示例代码将获取当前登录的 Windows 用户。

在导出服务器上的 PowerShell 会话中创建 PowerShell 凭据对象。


```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential(
    $User,$Password)
<!--NeedCopy-->
```

将配置导出到 backup.ctxzip，这是一个加密的 zip 文件。

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop" -
    zipFileName "backup" -Credential $CredObject
<!--NeedCopy-->
```

在导入服务器上的 PowerShell 会话中创建相同的 PowerShell 凭据对象。

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.ctxzip" -Credential $CredObject -HostBaseURL "https://
    storefront.example.com"
<!--NeedCopy-->
```

取消保护现有加密备份存档

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential(
    $User,$Password)

Unprotect-STFConfigurationExport -encryptedConfigurationZip "$env:
    userprofile\desktop\backup.ctxzip" -credential $CredObject -
    outputFolder "c:\StoreFrontBackups" -Force
<!--NeedCopy-->
```

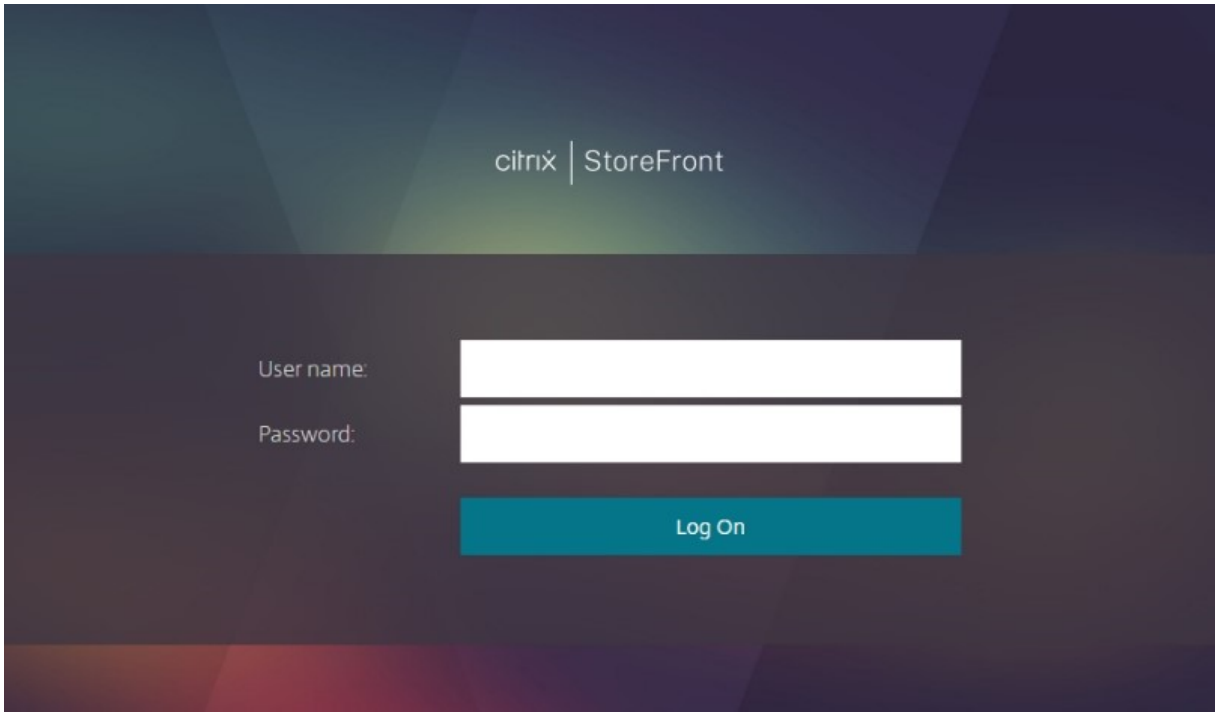
最终用户指南

April 17, 2024

本部分内容介绍通过 Web 浏览器或通过 Citrix Workspace 应用程序查看时应用商店的功能和外观。

登录

您可能需要登录，具体取决于身份验证方法以及是否启用了单点登录。

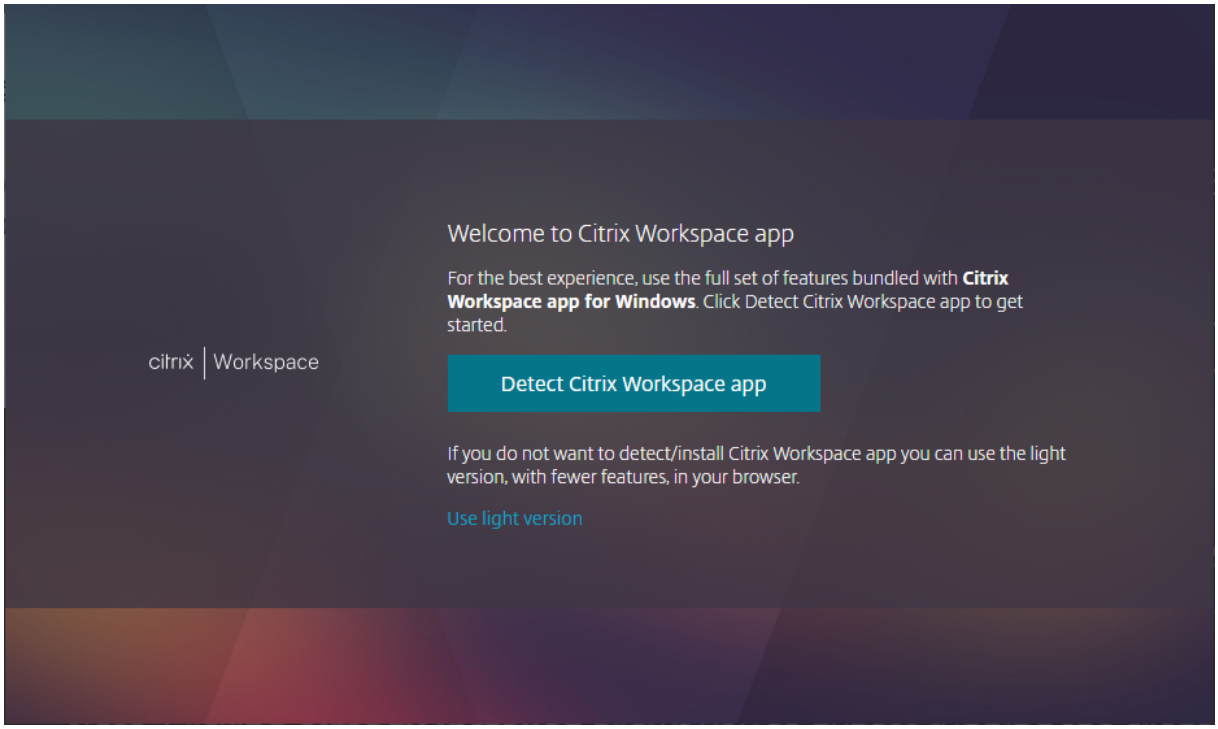


Citrix Workspace 应用程序检测

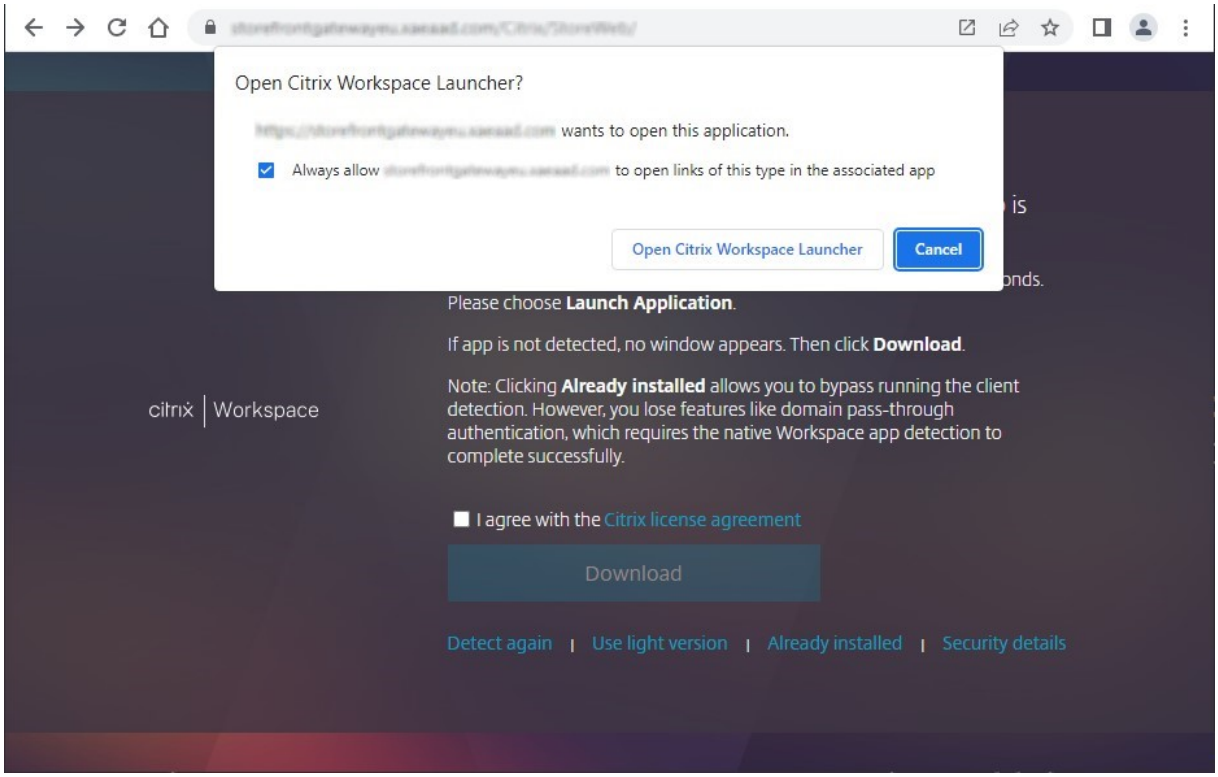
> 注意：
>
> 此步骤仅在通过 Web 浏览器访问应用商店时适用，在通过本地安装的 Citrix Workspace 应用程序访问应用商店时不适用。此步骤可能在登录之前或之后发生，具体取决于配置。

首次通过 Web 浏览器访问应用商店时或者清除 cookie 后，您可能会看到欢迎使用 **Citrix Workspace** 应用程序屏幕，具体取决于配置。执行以下操作之一：

- 如果您希望在本地安装的 Citrix Workspace 应用程序中启动资源，请单击检测 **Citrix Workspace** 应用程序。为了获得最佳体验，建议使用此方法。
- 单击使用简易版本（如果可用）将始终在浏览器中启动资源。



当您单击检测 **Citrix Workspace** 应用程序时，它会尝试检测本地安装的 Citrix Workspace 应用程序。首先，它尝试使用 Citrix Workspace Web 扩展。如果未安装或者检测不到本地安装的 Citrix Workspace 应用程序，它将尝试打开作为 Citrix Workspace 应用程序组件的 **Citrix Workspace Launcher**。如果安装了 Citrix Workspace 应用程序，您的浏览器会弹出一个窗口，要求运行 **Citrix Workspace Launcher**。单击打开 **Citrix Workspace** 启动器或打开链接（取决于浏览器）。建议您同时勾选始终允许域在关联的应用程序中打开此类链接，以避免每次启动资源时都出现此窗口。



如果检测到本地安装的 Citrix Workspace 应用程序，几秒钟后将会继续显示下一个屏幕。当您随后启动资源时，它将使用 Citrix Workspace Web 扩展或 Citrix Workspace Launcher（视检测到的内容而定）在本地安装的 Citrix Workspace 应用程序中打开资源。

如果未安装 Citrix Workspace 应用程序，或者您取消了 Launcher，则可以选择以下选项，具体取决于配置：

- 下载 - 从 Citrix Web 站点或 StoreFront 服务器下载 Citrix Workspace 应用程序。安装 Citrix Workspace 应用程序后，单击重新检测。
- 重新检测 - 尝试重新检测本地安装的 Citrix Workspace 应用程序。
- 使用简易版本 - 跳过 Workspace 应用程序检测，始终在 Web 浏览器中打开资源。
- 已安装 - 如果安装了不支持 Citrix Workspace Launcher 或 Citrix Workspace Web 扩展的旧版 Citrix Receiver，请使用此选项。如果选择此选项，则在启动虚拟应用程序或桌面时，您的浏览器会下载文件 **launch.ica**，可以使用 Citrix Receiver 打开该文件。此选项会导致功能减少，因此不建议使用。

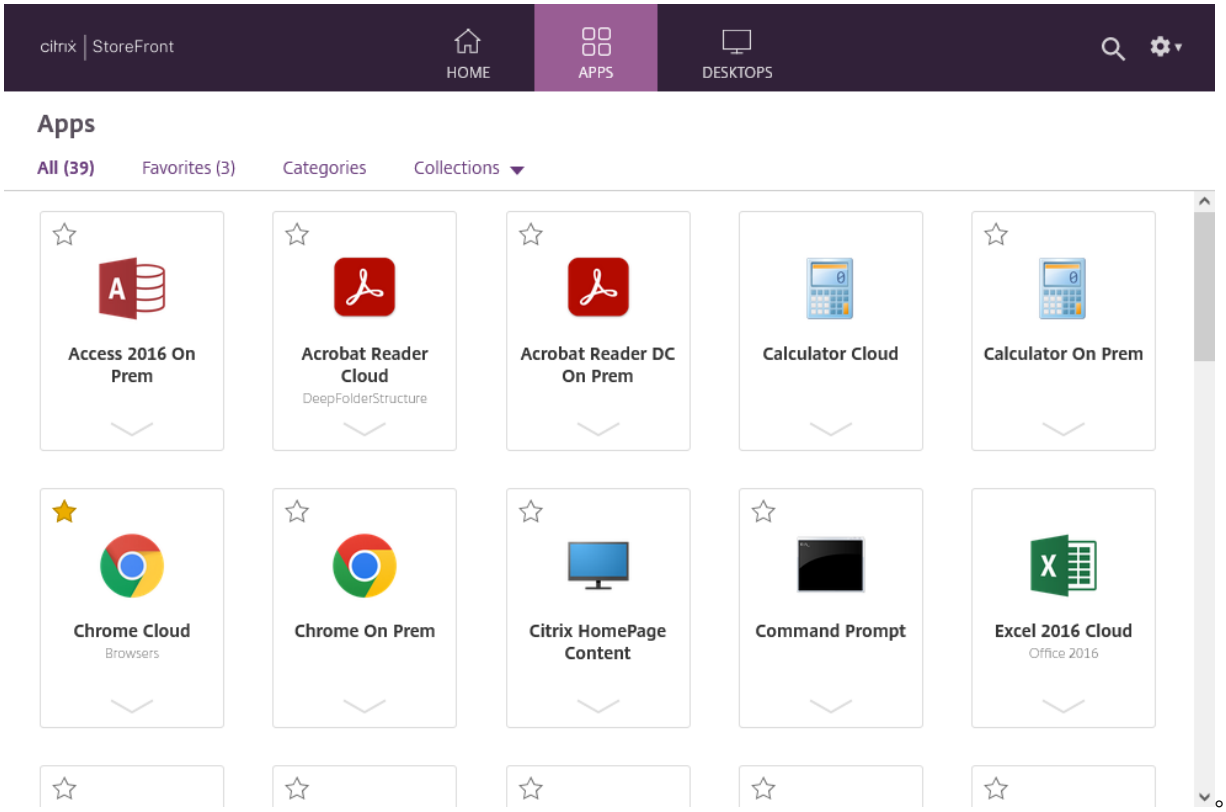
“主页”选项卡

主页选项卡显示所有精选应用程序组以及任何收藏的或必备的应用程序和桌面。仅当为应用商店启用了收藏夹时才会显示主页选项卡。

“应用程序”选项卡

应用程序选项卡有许多子视图：

- 全部 - 显示所有应用程序。
- 收藏夹 - 显示收藏的所有应用程序。
- 类别 - 显示类别和这些类别中的应用程序。类别的显示方式取决于类别设置。
- 集合显示精选应用程序组。



“桌面”选项卡

桌面选项卡有两个子视图：

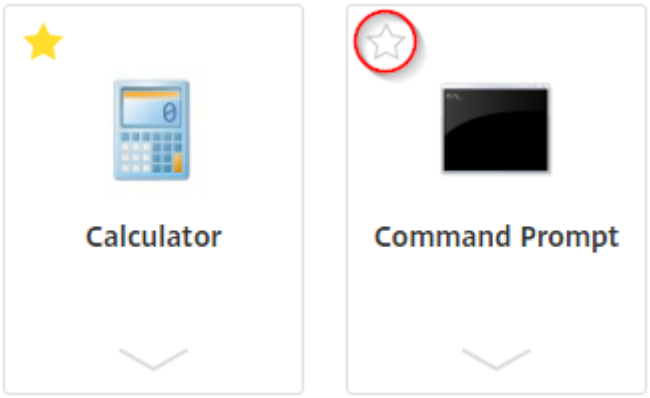
- 全部 - 显示所有桌面。
- 收藏夹 - 显示您收藏的桌面。

应用程序和桌面磁贴

单击某个图标可启动应用程序或桌面。

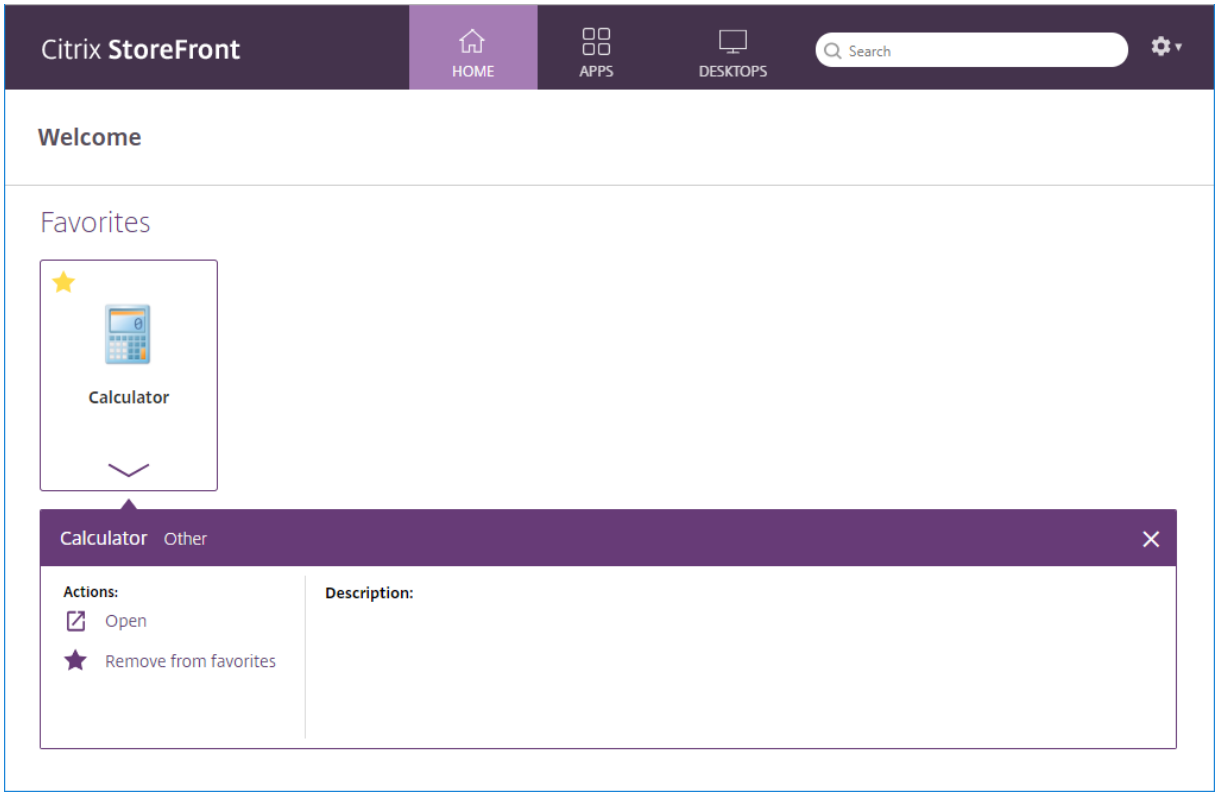
收藏夹

单击或轻按星形可收藏某个项目：



查看详细信息和操作

您可以展开每个图标下方的面板以显示应用程序的说明和操作。



可能有以下操作可用：

- 打开 - 启动或重新连接到应用程序或桌面。
- 添加到收藏夹 - 如果该项目不是收藏项，不是必需项，并且已为应用商店启用收藏夹，则将应用程序或桌面添加到您的收藏夹。
- 从收藏夹中删除 - 如果该项目是收藏项，不是必需项，并且已为应用商店启用收藏夹，则将该应用程序或桌面从您的收藏夹中删除。

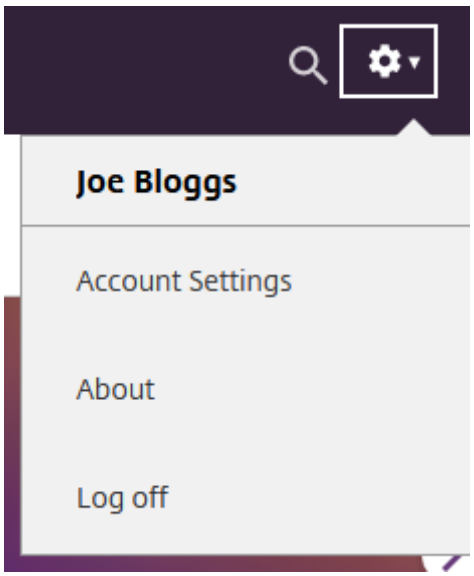
- 重新启动 - 对于可以重新启动的已分配桌面，此选项将重新启动桌面。

搜索

单击放大镜图标可显示搜索框。搜索所有应用程序、桌面和类别：

设置

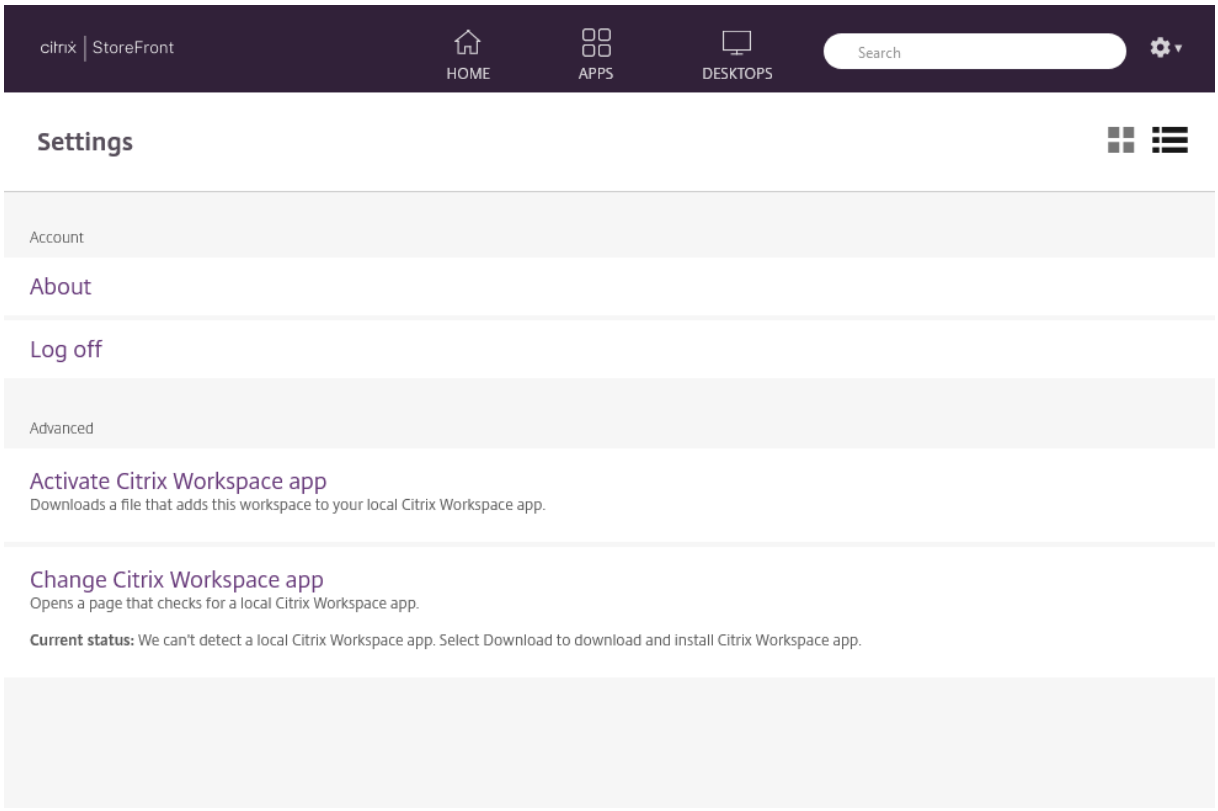
只有通过 Web 浏览器访问应用商店时，设置菜单才可用。



设置菜单有以下选项：

- 帐户设置 - 打开设置页面。
- 关于 - 显示有关应用程序的信息。
- 注销 - 注销 Web 站点。

帐户设置



以下选项可能可用：

连接。恢复任何已断开连接的会话。

断开连接。断开当前所有会话的连接并注销。

激活 **Citrix Workspace** 应用程序。下载用于将此应用商店添加到本地 Citrix Workspace 应用程序的文件。

更改 **Citrix Workspace** 应用程序。打开用于检查本地安装的 Citrix Workspace 应用程序的页面。此页面还允许用户在使用本地安装的 Citrix Workspace 应用程序启动资源与在 Web 浏览器中启动资源之间切换。

注销

要注销，请打开设置菜单并单击注销。这会将您退出应用商店。如果您连接到任何资源，根据配置，它将：

- 终止资源。
- 断开与资源的连接
- 保持资源处于连接状态。

StoreFront SDK

April 17, 2024

Citrix StoreFront 提供基于多个 Microsoft Windows PowerShell 2.0 模块的 SDK。通过 SDK，可以执行能够通过 StoreFront MMC 控制台完成的任务，也可以执行单独通过控制台无法完成的任务。

> 注意：
>
> PowerShell SDK 与 PowerShell 6 或更高版本不兼容。

有关 SDK 参考，请参阅 StoreFront SDK。

使用 SDK

SDK 由多个 PowerShell 管理单元组成，在安装和配置各种 StoreFront 组件时，安装向导会自动安装这些管理单元。

访问并运行 cmdlet：

1. 以管理员身份启动 PowerShell 命令行提示符或 **Windows PowerShell ISE**。

   必须在 StoreFront 服务器上使用多个本地管理员组运行 shell 或脚本。

2. 要在脚本内使用 SDK cmdlet，应在 PowerShell 中设置执行策略。

   有关 PowerShell 执行策略的详细信息，请参阅 Microsoft 文档。

3. 在 Windows PowerShell 控制台中使用 **Add -Module** 命令将需要的模块添加到 PowerShell 环境中。例如，键入：

   ```
   Import-Module Citrix.StoreFront
   ```

   要导入所有 cmdlet，请键入：

   ```
   Get-Module -ListAvailable | Where-Object { $_.Name.StartsWith("
   Citrix.StoreFront")} | Import-Module
   ```

导入后，可以访问 cmdlet 及其关联帮助。

SDK 入门

要创建脚本，请执行以下步骤：

1. 以所提供的 StoreFront 安装到 **%ProgramFiles%\Citrix\Receiver StoreFront\PowerShellSDK\Examples** 文件夹中的其中一个 SDK 为例。

2. 为帮助您自定义自己的脚本，请查看示例脚本以了解每个部分的作用。有关详细信息，请参阅示例用例，其中详细解释了脚本所进行的操作。
3. 转换并修改示例脚本，将其转变成更适用的脚本。为此，您需要：
    - 使用 PowerShell ISE 或类似的工具编辑脚本。
    - 使用变量分配要重复使用或修改的值。
    - 删除任何不需要的命令。
    - 请注意，可以通过前缀 STF 标识 StoreFront cmdlet。
    - 使用 **Get-Help** cmdlet 可提供 cmdlet 名称，使用 **-Full** 参数可获取特定命令的相关详细信息。

示例

> 注意：
>
> 创建脚本时，为确保始终获得最新的增强功能和修复，Citrix 建议您按照本主题中所述的步骤进行操作，而不要复制粘贴示例脚本。

示例	说明
创建简单部署	脚本：创建包含 StoreFront Controller 并且配置了一台 XenDesktop 服务器的简单部署。
创建远程访问部署	脚本：在以前的脚本基础上构建，以添加对部署的远程访问。
创建具有最佳启动网关的远程访问部署	脚本：在以前的脚本基础上构建，以添加首选最佳启动网关，从而实现更加卓越的用户体验。

示例：创建简单部署

下例显示了如何创建配置了一个 XenDesktop 控制器的简单部署。

在开始之前，请务必按照 SDK 入门中详述的步骤操作。可以使用介绍的方法对此示例进行自定义，以生成能够自动执行 StoreFront 部署的脚本。

> 注意：
>
> 为确保始终获得最新的增强功能和修复程序，Citrix 建议您按照本文档中所述的过程进行操作，而不是复制粘贴示例脚本。

了解脚本　本部分内容介绍由 StoreFront 生成的脚本的各部分的作用。这将有助于您自定义自己的脚本。

- 请设置错误处理要求并导入所需的 StoreFront 模块。在较新的 PowerShell 版本中，不需要导入。


```
Param(
    [Parameter(Mandatory=$true)]
    [Uri]$HostbaseUrl,
    [long]$SiteId = 1,
    [ValidateSet("XenDesktop","XenApp","AppController","VDIinaBox
        ")]
    [string]$Farmtype = "XenDesktop",
    [Parameter(Mandatory=$true)]
    [string[]]$FarmServers,
    [string]$StoreVirtualPath = "/Citrix/Store",
    [bool]$LoadbalanceServers = $false,
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP"
    )
    # Import StoreFront modules. Required for versions of
        PowerShell earlier than 3.0 that do not support
        autoloading
    Import-Module Citrix.StoreFront
    Import-Module Citrix.StoreFront.Stores
    Import-Module Citrix.StoreFront.Authentication
    Import-Module Citrix.StoreFront.WebReceiver
<!--NeedCopy-->
```

- 根据提供的 **$StoreVirtualPath** 自动创建身份验证和 Citrix Receiver for Web 服务的虚拟路径。**$StoreVirtualPath** 与 **$StoreIISpath** 等效，因为虚拟路径始终是 IIS 中的路径。因此，在 Powershell 中，它们具有一个值，例如 “/Citrix/Store”、“/Citrix/StoreWeb” 或 “/Citrix/StoreAuth”。

```
# Determine the Authentication and Receiver virtual path to use
    based of the Store
$authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"
$receiverVirtualPath = "$($StoreVirtualPath.TrimEnd('/'))Web"
<!--NeedCopy-->
```

- 准备创建新部署（如果尚不存在）以添加所需的 StoreFront Service。**-Confirm:$false** 不要求确认部署可以继续进行。

```
# Determine if the deployment already exists
$existingDeployment = Get-STFDeployment
if(-not $existingDeployment)
{

    # Install the required StoreFront components
    Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -
        Confirm:$false
 }

elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)
{

    # The deployment exists but it is configured to the desired
```



```
            hostbase url
14      Write-Output "A deployment has already been created with the
            specified hostbase url on this server and will be used."
15   }
16
17  else
18  {
19
20      Write-Error "A deployment has already been created on this
            server with a different host base url."
21   }
22
23  <!--NeedCopy-->
```

- 在指定的虚拟路径下创建新身份验证服务（如果不存在）。默认身份验证方法（即，用户名和密码）已启用。

```
1   # Determine if the authentication service at the specified
        virtual path exists
2   $authentication = Get-STFAuthenticationService -VirtualPath
        $authenticationVirtualPath
3   if(-not $authentication)
4   {
5
6       # Add an Authentication service using the IIS path of the
            Store appended with Auth
7       $authentication = Add-STFAuthenticationService
            $authenticationVirtualPath
8    }
9
10  else
11  {
12
13      Write-Output "An Authentication service already exists at the
             specified virtual path and will be used."
14   }
15
16  <!--NeedCopy-->
```

- 在指定的虚拟路径下创建配置了一个 XenDesktop 控制器且在阵列 **$XenDesktopServers** 中定义了服务器的新应用商店服务（如果尚不存在）。

```
1   # Determine if the store service at the specified virtual path
        exists
2   $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
3   if(-not $store)
4   {
5
6   # Add a Store that uses the new Authentication service configured
         to publish resources from the supplied servers
7   $store = Add-STFStoreService -VirtualPath $StoreVirtualPath -
        AuthenticationService $authentication -FarmName $Farmtype -
        FarmType $Farmtype -Servers $FarmServers -LoadBalance
        $LoadbalanceServers `
```



```
          -Port $Port -SSLRelayPort $SSLRelayPort -TransportType
              $TransportType
 }

else
{

    Write-Output "A Store service already exists at the specified
        virtual path and will be used. Farm and servers will be
       appended to this store."
    # Get the number of farms configured in the store
    $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.
       Count
    # Append the farm to the store with a unique name
    Add-STFStoreFarm -StoreService $store -FarmName "Controller$(
       $farmCount + 1)" -FarmType $Farmtype -Servers $FarmServers
        -LoadBalance $LoadbalanceServers -Port $Port `
        -SSLRelayPort $SSLRelayPort -TransportType $TransportType
 }

<!--NeedCopy-->
```

- 在指定的 IIS 虚拟路径下添加 Citrix Receiver for Web 服务以访问在上面创建的应用商店中发布的应用程序。

```
# Determine if the receiver service at the specified virtual path
    exists
$receiver = Get-STFWebReceiverService -VirtualPath
   $receiverVirtualPath
if(-not $receiver)
{

    # Add a Receiver for Web site so users can access the
       applications and desktops in the published in the Store
    $receiver = Add-STFWebReceiverService -VirtualPath
       $receiverVirtualPath -StoreService $store
 }

else
{

    Write-Output "A Web Receiver service already exists at the
       specified virtual path and will be used."
 }

<!--NeedCopy-->
```

- 为应用商店启用 XenApp Services，以便较旧的 Citrix Receiver 或 Citrix Workspace 应用程序客户端能够连接到已发布的应用程序。

```
# Determine if PNA is configured for the Store service
$storePnaSettings = Get-STFStorePna -StoreService $store
if(-not $storePnaSettings.PnaEnabled)
{
```



```
5
6   # Enable XenApp services on the store and make it the default for
        this server
7   Enable-STFStorePna -StoreService $store -AllowUserPasswordChange
        -DefaultPnaService
8    }
9
10  <!--NeedCopy-->
```

示例：创建远程访问部署

下例在以前的脚本基础上构建，以添加能够远程访问的部署。

在开始之前，请务必按照 SDK 入门中详述的步骤操作。可以使用介绍的方法对此示例进行自定义，以生成能够自动执行 StoreFront 部署的脚本。

> 注意：
>
> 为确保始终获得最新的增强功能和修复程序，Citrix 建议您按照本文档中所述的过程进行操作，而不是复制粘贴示例脚本。

了解脚本　本部分内容介绍由 StoreFront 生成的脚本的各部分的作用。这将有助于您自定义自己的脚本。

- 请设置错误处理要求并导入所需的 StoreFront 模块。在较新的 PowerShell 版本中，不需要导入。

```
1   Param(
2       [Parameter(Mandatory=$true)]
3       [Uri]$HostbaseUrl,
4       [Parameter(Mandatory=$true)]
5       [long]$SiteId = 1,
6       [string]$Farmtype = "XenDesktop",
7       [Parameter(Mandatory=$true)]
8       [string[]]$FarmServers,
9       [string]$StoreVirtualPath = "/Citrix/Store",
10      [bool]$LoadbalanceServers = $false,
11      [int]$Port = 80,
12      [int]$SSLRelayPort = 443,
13      [ValidateSet("HTTP","HTTPS","SSL")]
14      [string]$TransportType = "HTTP",
15      [Parameter(Mandatory=$true)]
16      [Uri]$GatewayUrl,
17      [Parameter(Mandatory=$true)]
18      [Uri]$GatewayCallbackUrl,
19      [Parameter(Mandatory=$true)]
20      [string[]]$GatewaySTAUrls,
21      [string]$GatewaySubnetIP,
22      [Parameter(Mandatory=$true)]
23      [string]$GatewayName
24  )
25  Set-StrictMode -Version 2.0
```



```
26
27  # Any failure is a terminating failure.
28  $ErrorActionPreference = 'Stop'
29  $ReportErrorShowStackTrace = $true
30  $ReportErrorShowInnerException = $true
31  # Import StoreFront modules. Required for versions of PowerShell
       earlier than 3.0 that do not support autoloading
32  Import-Module Citrix.StoreFront
33  Import-Module Citrix.StoreFront.Stores
34  Import-Module Citrix.StoreFront.Roaming
35  <!--NeedCopy-->
```

- 通过调用以前的示例脚本创建一个内部访问 StoreFront 部署。基本部署将扩展为支持远程访问。

```
1  # Create a simple deployment by invoking the SimpleDeployment
       example
2  $scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
       Definition -Parent
3  $scriptPath = Join-Path $scriptDirectory "SimpleDeployment.ps1"
4  & $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
       FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
       Farmtype $Farmtype `
5       -LoadbalanceServers $LoadbalanceServers -Port $Port  -
           SSLRelayPort $SSLRelayPort -TransportType $TransportType
6  <!--NeedCopy-->
```

- 获取根据更新需要在简单部署中创建的服务以支持远程访问场景。

```
1  # Determine the Authentication and Receiver sites based on the
       Store
2  $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
3  $authentication = Get-STFAuthenticationService -StoreService
       $store
4  $receiverForWeb = Get-STFWebReceiverService -StoreService $store
5  <!--NeedCopy-->
```

- 对 Citrix Receiver for Web 服务启用使用 Citrix Gateway 远程访问时所需的 CitrixAGBasic。从支持的协议中获取 Citrix Receiver for Web CitrixAGBasic 和 ExplicitForms 身份验证方法。

```
1  # Get the Citrix Receiver for Web CitrixAGBasic and ExplicitForms
       authentication method from the supported protocols
2  # Included for demonstration purposes as the protocol name can be
       used directly if known
3  $receiverMethods = Get-
       STFWebReceiverAuthenticationMethodsAvailable | Where-Object {
4   $_ -match "Explicit" -or $_ -match "CitrixAG"  }
5
6  # Enable CitrixAGBasic in Receiver for Web (required for remote
       access)
7  Set-STFWebReceiverService $receiverForWeb -AuthenticationMethods
       $receiverMethods
8  <!--NeedCopy-->
```


- 对身份验证服务启用 CitrixAGBasic。进行远程访问时需要启用。

```
# Get the CitrixAGBasic authentication method from the protocols
    installed.
# Included for demonstration purposes as the protocol name can be
     used directly if known
$citrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-
    Object {
 $_ -match "CitrixAGBasic"  }

# Enable CitrixAGBasic in the Authentication service (required
    for remote access)
Enable-STFAuthenticationServiceProtocol -AuthenticationService
    $authentication -Name $citrixAGBasic
<!--NeedCopy-->
```

- 添加远程访问网关，提供添加可选子网 IP 地址的操作，并在要远程访问的应用商店中注册该网关。

```
# Add a new Gateway used to access the new store remotely
Add-STFRoamingGateway -Name "NetScaler10x" -LogonType Domain -
    Version Version10_0_69_4 -GatewayUrl $GatewayUrl '
-CallbackUrl $GatewayCallbackUrl -SecureTicketAuthorityUrls
    $GatewaySTAUrls
# Get the new Gateway from the configuration (Add-
    STFRoamingGateway will return the new Gateway if -PassThru is
    supplied as a parameter)
$gateway = Get-STFRoamingGateway -Name $GatewayName
# If the gateway subnet was provided then set it on the gateway
    object
if($GatewaySubnetIP)
{

    Set-STFRoamingGateway -Gateway $gateway -SubnetIPAddress
        $GatewaySubnetIP
 }

# Register the Gateway with the new Store
Register-STFStoreGateway -Gateway $gateway -StoreService $store -
    DefaultGateway
<!--NeedCopy-->
```

示例：创建具有最佳启动网关的远程访问部署

下例在以前的脚本基础上构建，以添加能够远程访问的具有最佳启动网关的部署。

在开始之前，请务必按照 SDK 入门中详述的步骤操作。可以使用介绍的方法对此示例进行自定义，以生成能够自动执行 StoreFront 部署的脚本。

> 注意：
>
> 为确保始终获得最新的增强功能和修复程序，Citrix 建议您按照本文档中所述的过程进行操作，而不是复制粘贴

> 示例脚本。

了解脚本　本部分内容介绍由 StoreFront 生成的脚本的各部分的作用。这将有助于您自定义自己的脚本。

- 请设置错误处理要求并导入所需的 StoreFront 模块。在较新的 PowerShell 版本中，不需要导入。

```
Param(
    [Parameter(Mandatory=$true)]
    [Uri]$HostbaseUrl,
    [long]$SiteId = 1,
    [string]$Farmtype = "XenDesktop",
    [Parameter(Mandatory=$true)]
    [string[]]$FarmServers,
    [string]$StoreVirtualPath = "/Citrix/Store",
    [bool]$LoadbalanceServers = $false,
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP",
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$GatewaySTAUrls,
    [string]$GatewaySubnetIP,
    [Parameter(Mandatory=$true)]
    [string]$GatewayName,
    [Parameter(Mandatory=$true)]
    [Uri]$OptimalGatewayUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$OptimalGatewaySTAUrls,
    [Parameter(Mandatory=$true)]
    [string]$OptimalGatewayName
)
Set-StrictMode -Version 2.0
# Any failure is a terminating failure.
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
# Import StoreFront modules. Required for versions of PowerShell
    earlier than 3.0 that do not support autoloading
Import-Module Citrix.StoreFront
Import-Module Citrix.StoreFront.Stores
Import-Module Citrix.StoreFront.Roaming
<!--NeedCopy-->
```

- 调用到远程访问部署脚本中以配置基本部署并添加远程访问权限。

```
# Create a remote access deployment
$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
    Definition -Parent
```



```
$scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.ps1"
& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -Farmtype $Farmtype `
 -LoadbalanceServers $LoadbalanceServers -Port $Port  -SSLRelayPort $SSLRelayPort -TransportType $TransportType `
 -GatewayUrl $GatewayUrl -GatewayCallbackUrl $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -GatewayName $GatewayName
<!--NeedCopy-->
```

- 添加首选最佳启动网关并从所配置的网关列表中获取该网关。

```
# Add a new Gateway used for remote HDX access to desktops and apps
$gateway = Add-STFRoamingGateway -Name $OptimalGatewayName -LogonType UsedForHDXOnly -GatewayUrl $OptimalGatewayUrl -SecureTicketAuthorityUrls $OptimalGatewaySTAUrls -PassThru
<!--NeedCopy-->
```

- 获取应用商店服务以使用最佳网关，注册该网关并将其分配给从命名场进行的启动。

```
# Get the Store configured by SimpleDeployment.ps1
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
# Register the Gateway with the new Store for launch against all of the farms (currently just one)
$farmNames = @($store.FarmsConfiguration.Farms | foreach {
 $_.FarmName  }
)
Register-STFStoreOptimalLaunchGateway -Gateway $gateway -StoreService $store -FarmName $farmNames
<!--NeedCopy-->
```

StoreFront 故障排除

April 17, 2024

安装日志

安装或卸载 StoreFront 时，StoreFront 安装程序将在 *C:\Windows\Temp\StoreFront* 目录中创建以下日志文件。文件名称中包含时间戳，并将反映创建这些文件的组件。

- Citrix-DeliveryServicesRoleManager-*.log —交互式安装 StoreFront 时创建。
- Citrix-DeliveryServicesSetupConsole-*.log —无提示安装 StoreFront 及卸载 StoreFront（交互式或无提示）时创建。

- CitrixMsi-CitrixStoreFront-x64-*.log —安装和卸载 StoreFront（交互式或无提示）时创建。

事件日志

StoreFront 支持对身份验证服务、应用商店和 Receiver for Web 站点进行 Windows 事件日志记录。生成的所有事件都将写入到 StoreFront 应用程序日志中，可以通过应用程序和服务日志 **> Citrix** 交付服务或 **Windows** 日志 **>** 应用程序下的事件查看器查看这些事件。可以通过编辑身份验证服务、应用商店和 Receiver for Web 站点的配置文件，控制单个事件的重复日志条目数。

日志限制

1. 使用文本编辑器打开身份验证服务、应用商店或 Receiver for Web 站点的 *web.config* 文件，通常情况下，该文件分别位于 C:\inetpub\wwwroot\Citrix\Authentication、C:\inetpub\wwwroot\Citrix\storename 和 C:\inetpub\wwwroot\Citrix\storenameWeb\ 目录中，其中 storename 为创建应用商店时为其指定的名称。
2. 在此文件中查找以下元素。

   ```
   <logger duplicateInterval="00:01:00"duplicateLimit="10">
   ```

   在 StoreFront 的配置中，重复日志条目数默认限制为每分钟 10 条。
3. 更改 duplicateInterval 属性的值，以小时、分钟和秒为单位设置监视重复日志条目的时间段。使用 duplicateLimit 属性设置必须在指定时间间隔内记录的重复条目数，以便触发日志限制。

触发日志限制后，将记录一条警告消息，指出将禁止显示后续相同的日志条目。限制时段结束后将恢复常规日志记录，此时将记录一条信息性消息，指出将不再禁止显示重复的日志条目。

Powershell 和管理控制台日志

通过 PowerShell 或管理控制台所做的配置更改记录在 `C:\Program Files\Citrix\Receiver StoreFront\Admin\logs` 位置处。日志文件名称中包含命令操作和主题以及可用于区分命令顺序的时间戳。

诊断日志记录

默认情况下，诊断日志记录仅记录错误。要启用跟踪日志记录，请使用具有本地管理员权限的帐户，启动 Windows PowerShell 并使用带有以下参数的 `Set-STFDiagnostics` 命令：

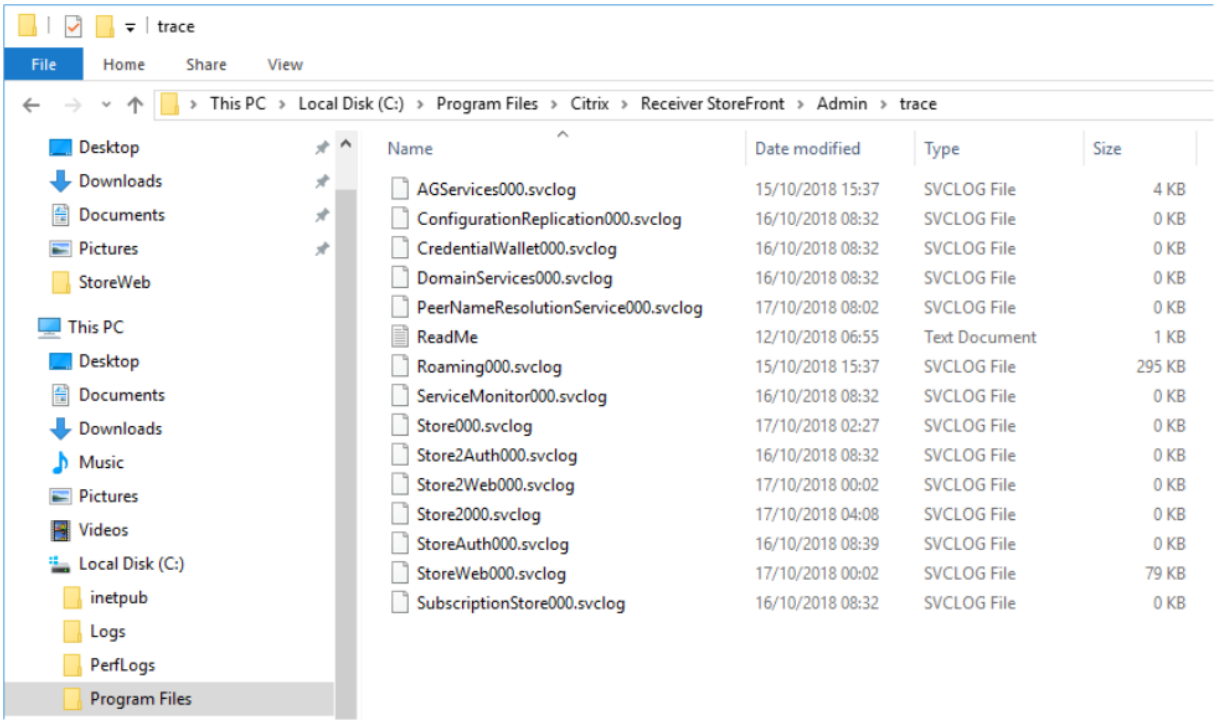
- **-All**。指示应更新所有实例和服务的跟踪的标志。

- **-TraceLevel**。要增加跟踪详细信息的级别，允许 -TraceLevel 使用以下值：Off、Error、Warning、Info 或 Verbose。由于可能生成大量的数据，因此跟踪可能会显著影响 StoreFront 的性能。除非进行故障排除时明确需要，否则，不建议使用 Info 或 Verbose 级别。

可选参数：

- **-FileSizeKb**。跟踪文件的大小以 KB 为单位。
- **-FileCount**。在磁盘中一次维护的跟踪文件数。
- **-confirm:$False**。禁止弹出 Windows 提示以允许 StoreFront cmdlet 每次都能运行。

跟踪输出发送至 `c:\Program Files\Citrix\Receiver StoreFront\admin\trace`



示例

要出于调试目的为所有服务启用 Verbose 级别的跟踪，请执行以下操作：

```
Set-STFDiagnostics -All -TraceLevel "Verbose" -confirm:$False
<!--NeedCopy-->
```

要禁用 Verbose 级别的跟踪并将跟踪级别设置回所有服务的默认值，请执行以下操作：

```
Set-STFDiagnostics -All -TraceLevel "Error" -confirm:$False
<!--NeedCopy-->
```

有关设置 Set-STFDiagnostics cmdlet 的详细信息，请参阅 StoreFront PowerShell SDK 文档。

Launch.ica 文件日志记录

当用户启动应用程序或桌面时，StoreFront 会生成一个名为 launch.ica 的文件，Workspace 应用程序会读取该文件以确定如何连接到应用程序或桌面。根据配置的不同，此文件可能会存储在内存中，因此无法直接访问。查看 launch.ica 的内容对诊断启动错误可能非常有用。

要启用 launch.ica 文件的日志记录，请完成以下步骤：

1. 使用注册表编辑器导航到以下注册表项：

   32 位系统：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging

   64 位系统：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging

2. 设置下面两个字符串密钥值：

   - LogFile=”日志文件的路径”
   - LogICAFile=true

   例如：

```
LogFile=C:\ica\ica.log
LogICAFile=true
<!--NeedCopy-->
```

> 注意：
>
> CTX200126 中进一步概述了如何在您的环境中将 ICA 文件用于除故障排除用途之外的任何其他目的。

第三方声明

February 22, 2024

StoreFront 可能包含根据以下条款许可使用的第三方软件组件。此列表是在截止到列出之日使用第三方软件生成的。此列表可能会随产品的特定版本而变化，并且可能不完整；此列表按“原样”提供。在适用法律允许的范围内，CITRIX 或其供应商对于此列表或其准确性或完整性，或者使用或分发此列表造成的结果概不负责，也不做任何明示、暗示、法定或其他形式的担保。使用或分发此列表表示您同意，在任何情况下，CITRIX 对于因使用或分发此列表造成的任何特殊的、直接的、间接的或后果性的损害或任何其他损害不承担任何法律责任。

Castle Windsor 3.3.0

版权所有 2004-2013 Castle Project - http://www.castleproject.org/

根据 Apache License 版本 2.0 获得许可

Microsoft Unity Application Block (Unity) 2.1

版权所有 © 2011 Microsoft Corporation。

根据 Microsoft Public License (MS-PL) 获得许可 https://msdn.microsoft.com/en-us/library/hh237493.aspx

Microsoft Patterns and Practices：Prism 2.2

版权所有 © 2010 Microsoft Corporation。

根据 Microsoft Public License (MS-PL) 获得许可 http://compositewpf.codeplex.com/releases/view/46046

Microsoft Patterns and Practices：Common Service Locator 1.0

版权所有 © Microsoft Corporation。

根据 Microsoft Public License (MS-PL) 获得许可

Microsoft .Net 参考来源

版权所有 © Microsoft Corporation。根据 MIT 许可证获得许可。

ManagedEsent 版本 1.9.4

版权所有 © Microsoft Corporation。

根据 Microsoft Public License (MS-PL) 获得许可 http://managedesent.codeplex.com/license

jQuery UI - v1.10.4 - 2014-03-12

http://jqueryui.com/

版权所有 2014 jQuery Foundation 及其他贡献者；MIT 许可

jQuery JavaScript Library v1.12.4

http://jquery.com/

包括 Sizzle.js

http://sizzlejs.com/

根据 MIT 许可证发布

http://jquery.org/license

日期：2016-05-20T17:17Z

jQuery jScrollPane v2.0.0beta11

jScrollPane - v2.0.0beta11 - 2011-07-04 http://jscrollpane.kelvinluck.com/

根据 MIT 和 GPL 许可证获得双重许可。

jquery.contextmenu.js

用于上下文菜单的 jQuery 插件

http://www.JavascriptToolbox.com/lib/contextmenu

根据 MIT 和 GPL 许可证获得双重许可。

适用于 **Hammer.JS** 的 **jQuery** 插件 **- v1.0.0 - 2014-01-02**

http://eightmedia.github.com/hammer.js

根据 MIT 许可证获得许可

jQuery MouseWheel

根据 MIT 许可证 (LICENSE.txt) 获得许可。

WPF Toolkit 3.5

WPF Toolkit (http://wpf.codeplex.com/) 版权所有 (c) 2006-2014 Microsoft

MS-PL 许可证 http://wpf.codeplex.com/license

扩展的 WPF Toolkit 3.0

版权所有 (C) 2007-2013 Xceed Software Inc.

本程序是根据 http://wpftoolkit.codeplex.com/license 上发布的 Microsoft Public License (Ms-PL) 的条款提供给您的。

如需更多功能、控件和快速的专业支持，请通过 http://xceed.com/wpf_toolkit 购买 Plus Edition

随时了解情况：在 Twitter 上关注 @datagrid 或者点赞 http://facebook.com/datagrids

WiX Toolset

版权所有 (c) Outercurve Foundation。Common Public License 版本 1.0。

CLR 安全性

版权所有 (c) Microsoft Corporation。Microsoft Limited Permissive License (MS-LPL)

Stack Exchange Redis 1.1

StackExchange.Redis.StrongName 1.1 https://stackexchange.github.io/StackExchange.Redis 版权所有 (c) 2014 Stack Exchange

根据 MIT 许可证获得许可

Newtonsoft JSON 9.0

版权所有 (c) 2007 James Newton-King

根据 MIT 许可证获得许可。

jQuery JavaScript Library v3.7.1

https://jquery.com/

版权所有 OpenJS Foundation 及其他贡献者

根据 MIT 许可证发布

https://jquery.org/license

日期：2023-08-28T13:37Z

jQuery UI - v1.13.2 - 2022-07-14

http://jqueryui.com

版权所有 jQuery Foundation 及其他贡献者；MIT 许可

Hammer.JS - v2.0.4 - 2014-09-28

Hammer.JS - v2.0.8 - 2016-04-23

http://hammerjs.github.io/

版权所有 (c) 2016 Jorik Tangelder;

根据 MIT 许可证获得许可

VelocityJS.org (1.5.0)

velocity-animate (C) 2014-2017 Julian Shapiro。

根据 MIT 许可证获得许可。有关详细信息，请参阅项目根目录中的 LICENSE 文件。

slick.js - 1.8.0

MIT 许可证 (MIT)

版权所有 (c) 2013-2016

jQuery UI Touch Punch 0.2.3

版权所有 2011—2014，Dave Furfero

根据 MIT 或 GPL 第 2 版许可证获得双重许可。

附录：引用的许可证

MIT 许可证

```
Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.
<!--NeedCopy-->
```

Apache 许可证，版本 **2.0**

```
                                 Apache License
                           Version 2.0, January 2004
                        http://www.apache.org/licenses/


TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction,
   and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by
   the copyright owner that is granting the License.
```



```
15
16      "Legal Entity" shall mean the union of the acting entity and all
17      other entities that control, are controlled by, or are under common
18      control with that entity. For the purposes of this definition,
19      "control" means (i) the power, direct or indirect, to cause the
20      direction or management of such entity, whether by contract or
21      otherwise, or (ii) ownership of fifty percent (50%) or more of the
22      outstanding shares, or (iii) beneficial ownership of such entity.
23
24      "You" (or "Your") shall mean an individual or Legal Entity
25      exercising permissions granted by this License.
26
27      "Source" form shall mean the preferred form for making modifications
            ,
28      including but not limited to software source code, documentation
29      source, and configuration files.
30
31      "Object" form shall mean any form resulting from mechanical
32      transformation or translation of a Source form, including but
33      not limited to compiled object code, generated documentation,
34      and conversions to other media types.
35
36      "Work" shall mean the work of authorship, whether in Source or
37      Object form, made available under the License, as indicated by a
38      copyright notice that is included in or attached to the work
39      (an example is provided in the Appendix below).
40
41      "Derivative Works" shall mean any work, whether in Source or Object
42      form, that is based on (or derived from) the Work and for which the
43      editorial revisions, annotations, elaborations, or other
            modifications
44      represent, as a whole, an original work of authorship. For the
            purposes
45      of this License, Derivative Works shall not include works that
            remain
46      separable from, or merely link (or bind by name) to the interfaces
            of,
47      the Work and Derivative Works thereof.
48
49      "Contribution" shall mean any work of authorship, including
50      the original version of the Work and any modifications or additions
51      to that Work or Derivative Works thereof, that is intentionally
52      submitted to Licensor for inclusion in the Work by the copyright
            owner
53      or by an individual or Legal Entity authorized to submit on behalf
            of
54      the copyright owner. For the purposes of this definition, "submitted
            "
55      means any form of electronic, verbal, or written communication sent
56      to the Licensor or its representatives, including but not limited to
57      communication on electronic mailing lists, source code control
            systems,
58      and issue tracking systems that are managed by, or on behalf of, the
```



```
    Licensor for the purpose of discussing and improving the Work, but
    excluding communication that is conspicuously marked or otherwise
    designated in writing by the copyright owner as "Not a Contribution.
        "

    "Contributor" shall mean Licensor and any individual or Legal Entity
    on behalf of whom a Contribution has been received by Licensor and
    subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of
    this License, each Contributor hereby grants to You a perpetual,
    worldwide, non-exclusive, no-charge, royalty-free, irrevocable
    copyright license to reproduce, prepare Derivative Works of,
    publicly display, publicly perform, sublicense, and distribute the
    Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of
    this License, each Contributor hereby grants to You a perpetual,
    worldwide, non-exclusive, no-charge, royalty-free, irrevocable
    (except as stated in this section) patent license to make, have made
        ,
    use, offer to sell, sell, import, and otherwise transfer the Work,
    where such license applies only to those patent claims licensable
    by such Contributor that are necessarily infringed by their
    Contribution(s) alone or by combination of their Contribution(s)
    with the Work to which such Contribution(s) was submitted. If You
    institute patent litigation against any entity (including a
    cross-claim or counterclaim in a lawsuit) alleging that the Work
    or a Contribution incorporated within the Work constitutes direct
    or contributory patent infringement, then any patent licenses
    granted to You under this License for that Work shall terminate
    as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the
    Work or Derivative Works thereof in any medium, with or without
    modifications, and in Source or Object form, provided that You
    meet the following conditions:

    (a) You must give any other recipients of the Work or
        Derivative Works a copy of this License; and

    (b) You must cause any modified files to carry prominent notices
        stating that You changed the files; and

    (c) You must retain, in the Source form of any Derivative Works
        that You distribute, all copyright, patent, trademark, and
        attribution notices from the Source form of the Work,
        excluding those notices that do not pertain to any part of
        the Derivative Works; and

    (d) If the Work includes a "NOTICE" text file as part of its
        distribution, then any Derivative Works that You distribute must
        include a readable copy of the attribution notices contained
```



```
110         within such NOTICE file, excluding those notices that do not
111         pertain to any part of the Derivative Works, in at least one
112         of the following places: within a NOTICE text file distributed
113         as part of the Derivative Works; within the Source form or
114         documentation, if provided along with the Derivative Works; or,
115         within a display generated by the Derivative Works, if and
116         wherever such third-party notices normally appear. The contents
117         of the NOTICE file are for informational purposes only and
118         do not modify the License. You may add Your own attribution
119         notices within Derivative Works that You distribute, alongside
120         or as an addendum to the NOTICE text from the Work, provided
121         that such additional attribution notices cannot be construed
122         as modifying the License.
123
124     You may add Your own copyright statement to Your modifications and
125     may provide additional or different license terms and conditions
126     for use, reproduction, or distribution of Your modifications, or
127     for any such Derivative Works as a whole, provided Your use,
128     reproduction, and distribution of the Work otherwise complies with
129     the conditions stated in this License.
130
131  5. Submission of Contributions. Unless You explicitly state otherwise,
132     any Contribution intentionally submitted for inclusion in the Work
133     by You to the Licensor shall be under the terms and conditions of
134     this License, without any additional terms or conditions.
135     Notwithstanding the above, nothing herein shall supersede or modify
136     the terms of any separate license agreement you may have executed
137     with Licensor regarding such Contributions.
138
139  6. Trademarks. This License does not grant permission to use the trade
140     names, trademarks, service marks, or product names of the Licensor,
141     except as required for reasonable and customary use in describing
            the
142     origin of the Work and reproducing the content of the NOTICE file.
143
144  7. Disclaimer of Warranty. Unless required by applicable law or
145     agreed to in writing, Licensor provides the Work (and each
146     Contributor provides its Contributions) on an "AS IS" BASIS,
147     WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
148     implied, including, without limitation, any warranties or conditions
149     of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
150     PARTICULAR PURPOSE. You are solely responsible for determining the
151     appropriateness of using or redistributing the Work and assume any
152     risks associated with Your exercise of permissions under this
            License.
153
154  8. Limitation of Liability. In no event and under no legal theory,
155     whether in tort (including negligence), contract, or otherwise,
156     unless required by applicable law (such as deliberate and grossly
157     negligent acts) or agreed to in writing, shall any Contributor be
158     liable to You for damages, including any direct, indirect, special,
159     incidental, or consequential damages of any character arising as a
160     result of this License or out of the use or inability to use the
```



```
   Work (including but not limited to damages for loss of goodwill,
   work stoppage, computer failure or malfunction, or any and all
   other commercial damages or losses), even if such Contributor
   has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
   the Work or Derivative Works thereof, You may choose to offer,
   and charge a fee for, acceptance of support, warranty, indemnity,
   or other liability obligations and/or rights consistent with this
   License. However, in accepting such obligations, You may act only
   on Your own behalf and on Your sole responsibility, not on behalf
   of any other Contributor, and only if You agree to indemnify,
   defend, and hold each Contributor harmless for any liability
   incurred by, or claims asserted against, such Contributor by reason
   of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS
<!--NeedCopy-->
```

Microsoft Public License (MS-PL)

```
This license governs use of the accompanying software. If you use the
   software, you accept this license. If you do not accept the license,
    do not use the software.

1. Definitions
The terms “reproduce,” “reproduction,” “derivative works,” and “
   distribution” have the
same meaning here as under U.S. copyright law.

A “contribution” is the original software, or any additions or
   changes to the software.

A “contributor” is any person that distributes its contribution under
    this license.

 “Licensed patents” are a contributor’ s patent claims that read
   directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including
   the license conditions and limitations in section 3, each
   contributor grants you a non-exclusive, worldwide, royalty-free
   copyright license to reproduce its contribution, prepare derivative
   works of its contribution, and distribute its contribution or any
   derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the
   license conditions and limitations in section 3, each contributor
   grants you a non-exclusive, worldwide, royalty-free license under
```



```
      its licensed patents to make, have made, use, sell, offer for sale,
      import, and/or otherwise dispose of its contribution in the software
       or derivative works of the contribution in the software.
18
19  3. Conditions and Limitations
20
21  (A) No Trademark License- This license does not grant you rights to use
       any contributors'  name, logo, or trademarks.
22
23  (B) If you bring a patent claim against any contributor over patents
      that you claim are infringed by the software, your patent license
      from such contributor to the software ends automatically.
24
25  (C) If you distribute any portion of the software, you must retain all
      copyright, patent, trademark, and attribution notices that are
      present in the software.
26
27  (D) If you distribute any portion of the software in source code form,
      you may do so only under this license by including a complete copy
      of this license with your distribution. If you distribute any
      portion of the software in compiled or object code form, you may
      only do so under a license that complies with this license.
28
29  (E) The software is licensed  "as-is."  You bear the risk of using it.
      The contributors give no express warranties, guarantees or
      conditions. You may have additional consumer rights under your local
       laws which this license cannot change. To the extent permitted
      under your local laws, the contributors exclude the implied
      warranties of merchantability, fitness for a particular purpose and
      non-infringement.
30  <!--NeedCopy-->
```