citrix

StoreFront 1912 LTSR

Contents

新增功能

June 29, 2021

StoreFront 1912 LTSR

累积更新 3 (CU3) 是 StoreFront 1912 LTSR 的最新更新。

支持基于 **Chromium** 的 **Microsoft Edge** 浏览器

现在，基于 Chromium 的 Microsoft Edge 浏览器可以通过内部网络连接和 Citrix Gateway 访问 Citrix Receiver for Web 站点。

StoreFront 协议处理程序支持现在包括安装了适用于 **Android** 的 **Workspace** 应用程序的 **Chrome** 设备

当 Chrome 设备上的用户打开 Citrix Receiver for Web 站点，并且安装了适用于 Android 的 Citrix Workspace 应用程序 1912 或更高版本时，浏览器会在启动时使用适用于 Android 的 Citrix Workspace 应用程序自动打开 ICA 文件。

在 Chrome 设备上使用 Chrome 浏览器时，适用于 Android 的客户端检测工作流程（确定是否安装了适用于 Android 的 Citrix Workspace 应用程序）现在与适用于 Windows 的 Citrix Workspace 应用程序和适用于 Mac 的 Citrix Workspace 应用程序相同。在早期版本中，Chrome 设备上的用户需要先手动打开下载的 ICA 文件。

支持应用程序保护策略

StoreFront 1912 支持应用程序保护策略，以增强其他 Citrix 组件（例如 Citrix Workspace 应用程序和 Citrix Virtual Apps and Desktops Delivery Controller）也支持应用程序保护功能时的安全性。应用程序保护策略在交付组级别设置，Citrix Virtual Apps and Desktops 决定是否使用应用程序保护策略。您无需在 StoreFront 中手动启用应用程序保护功能。当 StoreFront 从支持应用程序保护策略的 Citrix Workspace 应用程序收到包含 HTTP 标头 X-Citrix-AppProtection-Capable 的请求时，StoreFront 会自动向 Citrix Virtual Apps and Desktops 发送智能访问标记，指示其支持应用程序保护策略。有关使用应用程序保护策略配置交付组的详细信息，请参阅应用程序保护。

桌面设备站点不再受支持

Citrix Virtual Apps and Desktops 7 1811 中已宣布弃用针对用户在桌面设备站点上访问桌面的 StoreFront 支持。在本版本中，不再支持桌面设备站点，我们建议对所有未加入域的用例使用 Citrix Workspace 应用程序 Desktop Lock。

> 警告：
>
> 升级到 StoreFront 1912 时，部署中的所有桌面设备站点都会自动删除。请参阅 升级 StoreFront。

StoreFront PowerShell SDK

StoreFront PowerShell SDK 已重新发布为版本 1912。您无法再使用 PowerShell 创建或管理桌面设备站点。

累积更新 **3 (CU3)**

June 29, 2021

发布日期：May 12, 2021

关于此版本

StoreFront 1912 LTSR 累积更新 3 (CU3) 修复了自 1912 LTSR CU2 发布以来报告的 10 个问题。

StoreFront 1912 LTSR 累积更新 2 (CU2)

StoreFront 1912 LTSR 累积更新 1 (CU1)

StoreFront 1912 LTSR（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

1912 LTSR CU3 中已修复的问题

June 28, 2021

比较对象：StoreFront 1912 LTSR CU2

StoreFront 1912 LTSR CU3 包含 1912 LTSR 初始版本、CU1 版本、CU2 版本中包含的所有修复以及以下新修复：

- 登录 StoreFront 时，可能会出现以下错误消息：

  无法完成您的请求

  枚举启用了详细日志记录的应用程序并且任何带命令行参数的枚举应用程序都包含 **{** 时会出现此问题。[CVADHELP-16227]
- StoreFront 不会通过“支持统一用户体验”中介绍的自定义代码隐藏在特色类别中显示的所有应用程序中的应用程序。[CVADHELP-16577]
- 使用 Internet Explorer 启动 10 个以上的应用程序时，可能会出现一个额外的滚动条。[CVADHELP-16605]

- 启用套接字池后，尝试登录 StoreFront 可能会失败，并显示以下错误消息：

  无法完成您的请求

  TCP 动态端口耗尽时会出现此问题。

  [CVADHELP-16625]

- 从版本 7.15 LTSR CU4 升级 StoreFront 后，具有相同主机名的 VDI 桌面可能会按随机顺序而非序列顺序出现。[CVADHELP-16723]

- 尝试从启用了应用程序保护功能的交付组启动预配的 VDI 桌面可能会失败。可能会观察到以下行为：

  - 使用适用于 Windows 的 Citrix Workspace 应用程序启动桌面时，将出现一个旋转的圆圈，直到 StoreFront 超时为止。
  - 使用适用于 Mac 的 Citrix Workspace 应用程序启动桌面时，将显示以下错误消息：

    无法完成您的请求

  [CVADHELP-16800]

- 如果某个 XML Broker 无法正确运行，用户在登录后将看不到应用程序和桌面，即使存在多个正常运行的 XML Broker 时亦如此。

  此时将显示以下错误消息：

  您的登录已过期。请重新登录以继续。

  [CVADHELP-17017]

- 安装 StoreFront 1912 LTSR CU2 或将其升级到该版本之后，加入 StoreFront 服务器组可能会失败。此外，配置更改可能不会传播到其他服务器。[CVADHELP-17107]

- 选择 Citrix Gateway 的使用情况或角色为仅限 **HDX** 路由或身份验证和 **HDX** 路由时，Citrix Gateway 对象的 Secure Ticket Authority 更新可能不会反映在应用商店服务的 web.config 文件中。配置了多个最佳网关时会出现此问题。[CVADHELP-17112]

- 首次通过 Citrix Receiver 使用 SAML 身份验证单击 Web 站点快捷方式可能需要多次尝试。[CVADHELP-17137]

累积更新 **2 (CU2)**

December 2, 2020

发布日期：2020 年 11 月 19 日

关于此版本

StoreFront 1912 LTSR 累积更新 2 (CU2) 修复了自 1912 LTSR CU1 发布以来报告的九个问题。

StoreFront 1912 LTSR 累积更新 1 (CU1)

StoreFront 1912 LTSR（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

1912 LTSR CU2 中已修复的问题

December 2, 2020

比较对象：StoreFront 1912 LTSR CU1

StoreFront 1912 LTSR CU2 包含 1912 LTSR 初始版本、CU1 版本中包含的所有修复以及以下新修复：

- StoreFront 应用商店自 StoreFront 1903 以来一直在使用统一用户体验。一些客户报告说，统一体验在“类别”视图中显示子类别的方式对于其业务流程来说非最佳，而且这会使用户感到困惑。在此版本中，Citrix StoreFront 管理控制台为应用商店提供了使用“折叠”类别视图的选项。

  折叠的类别视图会隐藏任何子类别的内容，直到将其打开，并提供“浏览路径记录”导航。有关折叠的“类别”视图的详细信息以及配置该视图的详细信息，请参阅支持统一用户体验。**Set-STFWebReceiverUserInterface** PowerShell 命令带有一个用于控制类别视图的新 `CategoryViewCollapsed` 参数，请参阅 Citrix StoreFront 1912 SDK PowerShell 模块。[LCM-8241]

- 当应用商店文件夹中存在自定义配置文件时，自定义文件可能会替换应用商店文件夹中 web.config 文件的内容。升级 StoreFront 时会出现此问题。[CVADHELP-13485]
- 在 StoreFront 控制台中，尝试将包含下划线 (_) 的域名添加到可信域列表可能会失败。[CVADHELP-14213]
- Citrix StoreFront 可能无法枚举应用程序。当 StoreFront 连接到具有不受支持的证书策略扩展的证书链的 Delivery Controller 时会出现此问题。[CVADHELP-14328]
- StoreFront Web 应用商店中不枚举受应用程序保护策略保护的应用程序。如果在受支持的 Citrix Workspace 应用程序版本中添加两个以上的应用商店站点，则会出现此问题。[CVADHELP-14637]
- 尝试使用快捷方式启动应用程序时，该应用程序将显示为未定义，对于非 Citrix Endpoint Management 应用程序，将显示安装按钮 [CVADHELP-14808]
- 在 macOS 上，客户端检测可能会失败并显示以下错误：无法打开 URL。单击检测 **Receiver** 按钮时，StoreFront 会将客户端重定向到错误消息。[CVADHELP-15073]
- 尝试使用适用于 Mac 的 Citrix Workspace 应用程序启动会话可能会失败。如果会话来自启用了应用程序保护功能的交付组，则会出现此问题。[CVADHELP-15751]

- 在 StoreFront 应用商店中，顶层应用程序可能会在“类别”视图中的子类别下列出。[CVADHELP-16179]

累积更新 **1 (CU1)**

June 5, 2020

发布日期：May 7, 2020

关于此版本

StoreFront 1912 LTSR 累积更新 1 (CU1) 修复了自首次发布 1912 LTSR 以来报告的八个以上的问题。

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

1912 LTSR CU1 中已修复的问题

October 15, 2020

比较对象：StoreFront 1912 LTSR 初始版本

StoreFront 1912 LTSR CU1 包含 1912 LTSR 初始版本中包含的所有修复以及以下新修复：

- 当您使用第三方应用程序作为身份提供程序 (IdP) 时，安全断言标记语言 (SAML) 身份验证可能会失败。此时将显示以下错误消息：

  `There was a failure with the mapped account`. [CVADHELP-13396]

- 登录到 StoreFront 时，应用程序枚举可能需要很长时间才能完成。如果以 `domain\username` 格式键入您的用户名，并将用户身份验证委派给 Delivery Controller，则会出现此问题。[CVADHELP-13891]

- 刷新 Citrix Workspace 应用程序后，用于查看每个应用程序详细信息的详细信息选项可能会消失。如果您首次登录或添加帐户信息，则在初始刷新时不会出现此问题。但是，在后续刷新时会出现此问题。[CVADHELP-13949]

- 非英语版本的 StoreFront Metainstaller 可能无法正确显示某些字符串。[CVADHELP-14030]

- 当 Citrix Cloud Connector 与 Citrix Virtual Apps and Desktops 服务之间的连接中断时，尝试通过 StoreFront 启动已发布的应用程序或桌面可能会失败。[CVADHELP-14075]

- 通过 Citrix Gateway 的连接可能会失败，并显示以下错误消息：

  `Cannot Complete Request`.

  使用 PowerShell 命令添加全局服务器负载平衡 (GSLB) URL 后，会出现此问题。[CVADHELP-14354]

- 安装 Delivery Controller 时，默认情况下可能不安装 StoreFront。要进行安装，请使用 Citrix Virtual Apps and Desktops metainstaller 中的 Citrix StoreFront 选项。[LCM-7335]
- 此版本包含解决安全漏洞的修复。有关详细信息，请参阅知识中心文章 CTX277455。[LCM-7272]

新增功能

July 27, 2020

1912 LTSR 中的新增功能

StoreFront 1912 版包括以下新增功能和增强功能：

StoreFront 协议处理程序支持现在包括安装了适用于 **Android** 的 **Workspace** 应用程序的 **Chrome** 设备

当 Chrome 设备上的用户打开 Citrix Receiver for Web 站点，并且安装了适用于 Android 的 Citrix Workspace 应用程序 1912 或更高版本时，浏览器会在启动时使用适用于 Android 的 Citrix Workspace 应用程序自动打开 ICA 文件。

在 Chrome 设备上使用 Chrome 浏览器时，适用于 Android 的客户端检测工作流程（确定是否安装了适用于 Android 的 Citrix Workspace 应用程序）现在与适用于 Windows 的 Citrix Workspace 应用程序和适用于 Mac 的 Citrix Workspace 应用程序相同。在早期版本中，Chrome 设备上的用户需要先手动打开下载的 ICA 文件。

支持应用程序保护策略

StoreFront 1912 支持应用程序保护策略，以增强其他 Citrix 组件（例如 Citrix Workspace 应用程序和 Citrix Virtual Apps and Desktops Delivery Controller）也支持应用程序保护功能时的安全性。应用程序保护策略在交付组级别设置，Citrix Virtual Apps and Desktops 决定是否使用应用程序保护策略。您无需在 StoreFront 中手动启用应用程序保护功能。当 StoreFront 从支持应用程序保护策略的 Citrix Workspace 应用程序收到包含 HTTP 标头 X-Citrix-AppProtection-Capable 的请求时，StoreFront 会自动向 Citrix Virtual Apps and Desktops 发送智能访问标记，指示其支持应用程序保护策略。有关使用应用程序保护策略配置交付组的详细信息，请参阅应用程序保护。

要在 **StoreFront** 服务器上启用应用程序保护，请在 StoreFront 服务器上运行以下 PowerShell 命令：`Add-STFFeatureState -Name "Citrix.StoreFront.AppProtectionPolicy.Control" -IsEnabled $True`。（在多服务器 StoreFront 部署中，必须手动将这些更改传播到服务器组中的所有其他服务器。请参阅 将本地更改传播到服务器组。）

要验证是否在 **StoreFront** 服务器上启用了该功能，请使用以下 PowerShell 命令：`Get-STFFeatureState -Name "Citrix.StoreFront.AppProtectionPolicy.Control`。

桌面设备站点不再受支持

Citrix Virtual Apps and Desktops 7 1811 中已宣布弃用针对用户在桌面设备站点上访问桌面的 StoreFront 支持。在本版本中，不再支持桌面设备站点，我们建议对所有未加入域的用例使用 Citrix Workspace 应用程序 Desktop Lock。

> 警告：
>
> 升级到 StoreFront 1912 时，部署中的所有桌面设备站点都会自动删除。请参阅 升级 StoreFront。

StoreFront PowerShell SDK

StoreFront PowerShell SDK 已重新发布为版本 1912。您无法再使用 PowerShell 创建或管理桌面设备站点。

1912 LTSR 中已修复的问题

June 5, 2020

以下问题自版本 1909 起已修复：

- 本地 StoreFront 无法在 MMC 中为 Web 链接添加启动网关。[WSP-4368]
- LCM-6351：升级 DDC 后，不会删除 CitrixPrivilegedService_x64.msi 的旧注册表项。[WSP-4785]
- 尝试使用 Citrix Virtual Apps and Desktops 7 1906 metainstaller 将 StoreFront 升级到版本 1906 时，如果您的 StoreFront 服务器上安装了 VMware VMTools v10.3.，升级将失败。StoreFront 通过独立的 StoreFront 1906 安装程序成功升级，但 StoreFront 1906 未添加到 Windows 的“添加/删除程序列表”中。[WSP-4895]
- 用于截断长应用程序名称的自定义不再适用于 X1.1 Purple UI。[WSP-4899]
- 如果 KCD 服务处于“已停止”状态，升级历史记录中包含 2.6、3.0.1、3.5、3.8 升级到 3.12 CU* 及更高版本可能会失败。[WSP-5160]
- 更新 `http://downloadplugins.citrix.com` 以交付 Citrix Workspace 应用程序，而非使用已结束生命周期的 Citrix Receiver。[WSP-5303]

已知问题

June 28, 2021

本版本中存在以下已知问题。

StoreFront 1912 CU3 中的已知问题

- 无法在不同产品版本之间导出\导入 StoreFront 配置。出于此限制目的，StoreFront 1912 LTSR 的初始版本和后续累积更新被视为不同的产品版本。因此，例如，您可以在 StoreFront 1912 LTSR 初始版本与 1912 LTSR 初始版本之间导出和导入配置，以及在版本 1912 LTSR CU1 与 1912 LTSR CU1 之间导出和导入配置，但不能在版本 1912 LTSR CU2 与 1912 LTSR CU3 之间导出和导入配置。[LCM-7104]
- 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 (#985d94)。

  要解决此问题，请通过将以下行添加到应用商店 Web 的自定义文件夹中的 CSS 样式表（例如 C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css）来指定所需的颜色：[LCM-9536]

```
.theme-header-selection-color.selected
{
 background-color:<desired color>;  }
```

StoreFront 1912 CU2 中的已知问题

- 尝试将 StoreFront 服务器加入现有服务器组（该组使用具有德语、西班牙语或法语区域设置的受支持操作系统）失败。使用支持的操作系统和其他区域设置的服务器组尝试加入成功。[CVADHELP-17107]
- StoreFront 应用商店中的应用程序无法枚举和启动，并报告 SSL 连接错误。如果在 Windows Server 2016 或 Windows Server 2019 上安装了 Delivery Controller，并且 StoreFront 安装在 Windows Server 2012 R2 上，则会出现此问题。要解决此问题，密码套件顺序列表必须包含 TLS_ECDHE_* 密码套件，并且这些密码套件必须位于任何其他密码套件之前。[LCM-9305]
- StoreFront 应用商店中的应用程序无法枚举和启动，并报告 SSL 连接错误。如果您使用 Citrix ADC 负载平衡功能将负载分发到 Delivery Controller 服务器，并且 StoreFront 正在使用 HTTPS 与负载平衡 Delivery Controller 服务进行通信，则会出现此问题。要解决此问题，Citrix ADC 上的密码套件顺序列表必须仅包含 TLS_ECDHE_* 密码套件。如果在 Citrix ADC 或 StoreFront 中将 Delivery Controller 服务器分配为 STA 服务器（位于站点外部），StoreFront 上的密码套件顺序列表还必须包含 TLS_ECDHE_* 密码套件，并且这些密码套件必须位于任何其他密码套件之前。[LCM-9308]

StoreFront 1912 CU1 中的已知问题

累积更新 1 中未发现新的已知问题。

StoreFront 1912 中的已知问题

- 在 Windows 中禁用了 TLS 1.0，并且 Windows Server 使用.NET 4.5 Framework 服务器时，StoreFront 服务器组的成员之间的订阅传播将失败。默认情况下，.NET 4.5 Framework 仅使用 TLS 1.0。此问题的解决

方法为，将服务器上的.NET Framework 升级到 4.7 或更高版本（默认使用 TLS 1.2）。[STF-2413]

- 智能卡身份验证和 Microsoft Edge 存在一个已知的第三方问题。要解决此问题，请使用 Internet Explorer。[DNA-47809]
- 工作区控制仅重新连接到一个应用程序会话，而非连接到工作区中的所有应用程序。如果使用 Chrome 访问 Receiver for Web 站点，则会出现此问题。要解决此问题，请在每个断开的应用程序上单击“重新连接”。[DNA-25140、DNA-22561]
- 在 Windows Server 2012 R2 上安装 StoreFront 时，它可能无法注册到 Citrix Analytics Service (CAS)。当 C ++ 运行时软件组件尚未安装时，会发生这种情况。StoreFront 独立安装程序不会安装这些组件。解决该问题的简单方法是在安装 StoreFront 之前或之后安装 C++ 运行时。[WSP-4412]

第三方声明

June 5, 2020

StoreFront 可能包含根据以下文档中定义的条款进行许可的第三方软件：

StoreFront 第三方声明 （PDF 下载）

系统要求

June 29, 2021

规划安装时，Citrix 建议 StoreFront 服务器至少使用 6 GB 内存。订阅应用商店服务最低需要 5 MB 磁盘空间，另外，每 1000 个应用程序订阅大约需要 8 MB 磁盘空间。所有其他硬件规格必须满足所安装操作系统的最低要求。

> 注意：
>
> 不支持从现在已结束使用的旧版当前版本升级到最新的当前版本。有关详细信息，请参阅CTX200356。

Citrix 已测试过，可以支持在以下平台上安装 StoreFront：

- Windows Server 2019 Datacenter Edition 和 Standard Edition
- Windows Server 2016 Datacenter Edition 和 Standard Edition
- Windows Server 2012 R2 Datacenter Edition 和 Standard Edition

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。多服务器部署中的所有服务器必须运行相同的操作系统版本，且具有相同的区域设置。

不支持包含多种操作系统版本和区域设置的 StoreFront 服务器组。StoreFront 服务器组中的服务器数量没有限制。但是，从基于模拟的容量预测来看，包含三个以上服务器的服务器组不具有优势。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），但服务器组可以跨越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最低延迟条件。请参阅 可扩展性。

必须在 Web 服务器上安装 Windows PowerShell（版本 4.0 或更高版本）以及 Microsoft 管理控制台（3.0 或更高版本），才能安装 StoreFront。这些都是 Windows Server 的默认组件。

StoreFront 安装程序会在安装 StoreFront 之前检查是否已安装并启用以下必备项。默认情况下，这些必备项由操作系统作为功能包提供。如果 StoreFront 安装程序检测到这些必备项中的任何一项缺失或已禁用，则会自动安装并启用这些必备项：

- Microsoft .NET Framework（版本 4.5.1 或更高版本）
- Microsoft ASP.NET（版本 4.5 或更高版本）
- Microsoft Visual C++ 2017 (x64) Runtime (v141)
- Microsoft Internet Information Services (IIS)

  IIS 由 Web 服务器 “Windows Server” 角色添加，其版本取决于所选操作系统。（仅供参考）StoreFront 安装程序添加了以下 IIS 角色：

  - Web-Static-Content
  - Web-Default-Doc
  - Web-Http-Errors
  - Web-Http-Redirect
  - Web-Http-Logging
  - Web-Mgmt-Console
  - Web-Scripting-Tools
  - Web-Windows-Auth
  - Web-Basic-Auth
  - Web-AppInit
  - Web-Asp-Net45
  - Net-Wcf-Tcp-PortSharing45

  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 Receiver 和 Citrix Workspace 应用程序的各版本使用，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

您可以选择使用 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 服务器要求

StoreFront 应用商店将来自以下产品的桌面和应用程序聚合在一起。

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

* 有关在长期服务 (LTSR) 环境中使用此当前版本 (CR) 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 要求

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

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

适用于 **HTML5** 的 **Citrix Workspace** 应用程序的要求

要支持用户使用在 Receiver for Web 站点上运行的适用于 HTML5 的 Citrix Workspace 应用程序访问桌面和应用程序，还需要满足以下要求。

对于内部网络连接，适用于 HTML5 的 Citrix Workspace 应用程序支持访问以下产品所提供的桌面和应用程序。

- Citrix Virtual Apps and Desktops 7 1912 LTSR
- Citrix Virtual Apps and Desktops 7 1909
- Citrix Virtual Apps and Desktops 7 1906

- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp 和 XenDesktop 7.15 LTSR
- XenApp 和 XenDesktop 7.6 LTSR

> 注意：
>
> 适用于 HTML5 的 Citrix Workspace 应用程序仅在配置了与托管这些资源的 VDA 的安全连接后，才使用内部网络连接启动桌面和应用程序。不能使用与托管应用程序和桌面的 VDA 的 HTTP 连接。

对于企业网络外部的远程用户，适用于 HTML5 的 Citrix Workspace 应用程序支持通过以下版本的 Citrix Gateway 和 NetScaler Gateway 访问桌面和应用程序。

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

对于通过 Citrix Gateway 连接的用户，适用于 HTML5 的 Citrix Workspace 应用程序支持访问以下产品所提供的桌面和应用程序。

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

用户设备要求

StoreFront 提供了许多不同的方式供用户访问自己的桌面和应用程序。Citrix Workspace 应用程序用户可以通过 Citrix Workspace 应用程序访问应用商店，也可以使用 Web 浏览器登录 Citrix Receiver for Web 站点以访问应用商店。对于无法安装 Citrix Workspace 应用程序但具有兼容 HTML5 的 Web 浏览器的用户，可以在您的 Citrix Receiver for Web 站点上启用适用于 HTML5 的 Citrix Workspace 应用程序，使这些用户可以直接在 Web 浏览器中访问桌面和应用程序。

运行 Citrix Desktop Lock 的 PV 的用户以及无法升级的旧版 Citrix 客户端必须通过应用商店的 XenApp Services URL 进行连接。

如果要向用户交付 Microsoft Application Virtualization (App-V) 序列，还需要安装受支持的 Microsoft Application Virtualization Desktop Client 版本。有关详细信息，请参阅管理流应用程序。用户无法通过 Citrix Receiver for Web 站点访问脱机应用程序或 App-V 序列。

使用 **Citrix Workspace** 应用程序访问 **StoreFront** 应用商店

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 应用程序和 Citrix Receiver 生命周期日期，请参阅 https://www.citrix.com/support/product-lifecycle/milestones/receiver.html。

可以使用 Citrix Gateway 插件、ICA 代理或无客户端 VPN (cVPN) 通过 Citrix Gateway 连接到 StoreFront 应用商店。请参阅 统一用户体验。

通过 **Citrix Receiver for Web** 站点访问应用商店

要通过内部网络连接和 Citrix Gateway 访问 Citrix Receiver for Web 站点，请使用以下浏览器的最新版本：

在 **Windows** 中

- Internet Explorer 11
- MS Edge（基于 Chromium）
- Google Chrome
- Mozilla Firefox

在 **Mac** 上

- Safari
- Google Chrome
- Mozilla Firefox

在 **Linux** 中

- Google Chrome
- Mozilla Firefox

可以使用 Citrix Gateway 插件、ICA 代理或无客户端 VPN (cVPN) 通过 Citrix Gateway 建立连接。此外，需要具有特定版本的 Citrix Gateway 才允许从企业网络外部建立连接。有关详细信息，请参阅基础结构要求。

通过 **Citrix Receiver for Web** 站点启动资源

Citrix Receiver for Web 站点支持通过本地安装的 Citrix Workspace 应用程序启动，或者通过适用于 HTML5 的 Citrix Workspace 应用程序启动。上面列出的所有浏览器均符合 HTML5 标准，并支持 HTML5 资源启动。根据 Receiver for Web 配置，最终用户可以在两种启动方法之间切换。

通过 **XenApp Services URL** 访问应用商店

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。如果支持，可以使用 Citrix Gateway 插件和无客户端访问通过 Citrix Gateway 建立连接。

智能卡要求

将 **Citrix Receiver for Windows 4.x** 以及适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1808** 或更高版本与智能卡结合使用

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。

通过 **Citrix Gateway** 进行身份验证

公用网络中通过智能卡进行身份验证的用户可以使用以下版本的 Citrix Gateway 访问 StoreFront。

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

Citrix Analytics 服务要求

可以配置 Citrix StoreFront，以便 Citrix Workspace 应用程序可以将数据发送到 Citrix Analytics 服务。配置详细信息在 Citrix Analytics 服务中进行介绍。以下场景支持此功能：

- 通过在 HTML5 兼容的浏览器中浏览到 Citrix Receiver for Web 站点访问的应用商店。使用本机 Citrix Workspace 应用程序或使用 HTML5 启动资源时，提供 Citrix Analytics 服务数据。
- 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。

规划 **StoreFront** 部署

April 12, 2021

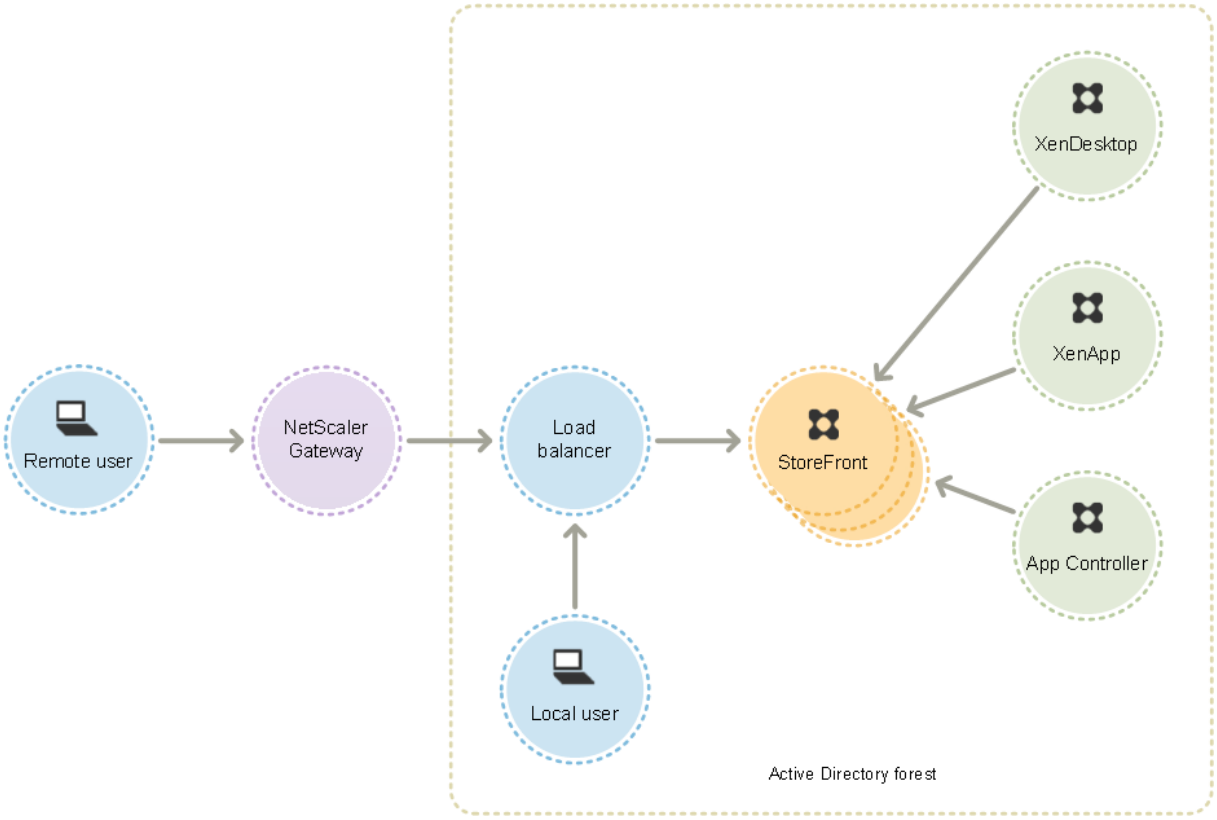
StoreFront 使用 Microsoft Internet Information Services (IIS) 上运行的 Microsoft .NET 技术提供将资源聚合在一起的企业应用商店，并使其可供用户访问。StoreFront 与 Citrix Virtual Apps and Desktops 部署相集成，为用户提供单一的自助访问点，以访问其桌面和应用程序。

StoreFront 包含以下核心组件：

- 身份验证服务可对用户进行身份验证，使其能够访问 Microsoft Active Directory，从而确保用户无需重新登录即可访问自己的桌面和应用程序。有关详细信息，请参阅用户身份验证。
- 应用商店枚举并聚合 Citrix Virtual Apps and Desktops 中的桌面和应用程序。用户通过 Citrix Workspace 应用程序、Citrix Receiver for Web 站点和 XenApp Services URL 访问应用商店。有关详细信息，请参阅用户访问选项。
- 订阅应用商店服务记录用户应用程序订阅的详细信息并更新其设备，以确保提供一致的漫游体验。有关增强用户体验的详细信息，请参阅优化用户体验。

StoreFront 可以在单台服务器上进行配置，也可以配置为多服务器部署。多服务器部署不但提供额外的容量，而且具有更高的可用性。StoreFront 的模块式体系结构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。

下图显示了一个典型的 StoreFront 部署。



负载平衡

对于多服务器部署，需要使用 Citrix ADC 或 Windows 网络负载平衡等软件来实现外部负载平衡。可以为服务器之间的故障转移配置负载平衡环境，以提供容错部署。有关 Citrix ADC 负载平衡的详细信息，请参阅负载平衡。有关 Windows 网络负载平衡的详细信息，请参阅 https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831698(v=ws.11)。

对于具有成千上万个用户的部署或出现高负载的部署（例如，当大量用户在一段很短的时间内登录时），建议将请求的活动负载平衡从 StoreFront 发送到 Citrix Virtual Desktops 站点和 Citrix Virtual Apps 场。请使用具有内置 XML 监视器和会话一致性的负载平衡器，例如 Citrix ADC。

如果部署了 SSL 终止负载平衡器，或者需要执行故障排除，可以使用 PowerShell cmdlet **Set-STFWebReceiverCommunication**。

语法：

```
1 Set-STFWebReceiverCommunication [-WebReceiverService] <
    WebReceiverService> [[-Loopback] <On | Off | OnUsingHttp>] [[-
    LoopbackPortUsingHttp] <Int32>]
```

有效值包括：

- **On** - 这是新 Citrix Receiver for Web 站点的默认值。Citrix Receiver for Web 使用来自基本 URL 的架构（HTTPS 或 HTTP）和端口号，但会将主机替换为环回 IP 地址以与 StoreFront Service 进行通信。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。
- **OnUsingHttp** - Citrix Receiver for Web 使用 HTTP 和环回 IP 地址与 StoreFront Service 进行通信。如果您使用的是 SSL 终止负载平衡器，请选择此值。此外，如果端口不是默认端口 80，还必须指定 HTTP 端口。
- **Off** - 此值将关闭环回，且 Citrix Receiver for Web 使用 StoreFront 基本 URL 与 StoreFront Service 通信。如果执行原位升级，这是用于避免现有部署中断的默认值。

例如，如果您使用的是 SSL 终止负载平衡器，IIS 配置为对 HTTP 使用端口 81，并且 Citrix Receiver for Web 站点的路径为 /Citrix/StoreWeb，则可以运行以下命令来配置 Citrix Receiver for Web 站点：

```
$wr = Get-STFWebReceiverService -VirtualPath /Citrix/StoreWeb
Set-STFWebReceiverCommunication -WebReceiverService $wr -Loopback
    OnUsingHttp -LoopbackPortUsingHttp 81
```

> 注意：
>
> 请关闭环回以使用 Fiddler 等任何 Web 代理工具来捕获 Citrix Receiver for Web 与 StoreFront Service 之间的网络流量。

Active Directory 注意事项

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。

用户连接

在生产环境中，Citrix 建议使用 HTTPS 以确保 StoreFront 与用户设备之间的通信安全。要使用 HTTPS，StoreFront 要求将托管身份验证服务和相关应用商店的 IIS 实例配置为支持 HTTPS。如果没有合适的 IIS 配置，StoreFront 将使用 HTTP 进行通信。可以随时从 HTTP 更改为 HTTPS，只要相应的 IIS 配置已就位即可。

如果您计划支持从企业网络外部访问 StoreFront，则需要使用 Citrix Gateway 来为远程用户提供安全的连接。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。

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。例如，这可用于允许在同一 StoreFront 服务器组上绑定多个 Storefront URL 和证书。

首先，请创建两个 Web 站点（默认 Web 站点除外）。在 IIS 中创建多个 Web 站点后，请使用 PowerShell SDK 在其中每个 IIS Web 站点中创建一个 StoreFront 部署。有关在 IIS 中创建 Web 站点的详细信息，请参阅创建 Web 站点。

> 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。

示例：创建两个 **IIS Web** 站点部署，一个用于应用程序，一个用于桌面

```
Add-STFDeployment -SiteID 1 -HostBaseURL ”https://www.storefront.app.com”
Add-STFDeployment -SiteID 2 -HostBaseURL ”https://www.storefront.desktop.com”
```

StoreFront 会在检测到多个站点时禁用管理控制台并针对该影响显示一条消息。

有关详细信息，请参阅安装和配置之前。

可扩展性

StoreFront 服务器组支持的 Citrix Workspace 应用程序用户数取决于所使用的硬件和用户活动的级别。根据模拟的用户登录活动，如果要枚举 100 个已发布的应用程序，并启动一种资源，需要一台 StoreFront 服务器以便每小时启用多达 30000 个用户连接，建议该服务器最低配备两个在底层双 Intel Xeon L5520 2.27Ghz 处理器服务器上运行的虚拟 CPU。

要每小时启用多达 60000 个用户连接，需要一个包含两台配置相似的服务器的服务器组；要每小时启用多达 90000 个连接，需要三个节点；要每小时启用多达 120000 个连接，需要四个节点；要每小时启用多达 150000 个连接，需要五个节点；要每小时启用多达 175000 个连接，需要六个节点。

还可以通过向系统中分配更多虚拟 CPU 来增加单台 StoreFront 服务器的吞吐量：要每小时启用多达 55000 个用户连接，需要分配四个虚拟 CPU，要每小时启用多达 80000 个用户连接，需要分配八个虚拟 CPU。

系统要求中介绍了每个 StoreFront 服务器的最低建议内存分配。使用 Citrix Receiver for Web 时，除分配基础内存外，请额外为每个用户的每个资源分配 700 字节内存。此处 “资源” 是指分配给用户的已发布应用程序或桌面。同样，使用 Citrix Workspace 应用程序时，除了本版本的 StoreFront 的基本内存要求外，请将环境设计为允许每个用户的每种资源额外具有 700 字节内存。

例如，如果将一个应用程序和两个桌面分配给一个用户并为三个用户提供访问权限，则最低额外内存将为：

```
(700 Byte x 1 “application” + 700 Byte x 2 “desktops”)x 3 “users”/1000 = 6.3 KB.
```

由于您的使用模式与上述模拟可能会有所差异，您的服务器在每小时支持的用户连接数可能会大于或小于上述数字。

> 重要：
>
> 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。
>
> 不支持包含混合操作系统版本或混合操作系统语言或区域设置配置的 StoreFront 服务器组。

超时注意事项

StoreFront 应用商店与其所通信的服务器之间偶尔会出现网络问题或其他问题，从而导致用户延迟或故障。可以使用应用商店的超时设置来调整此行为。如果指定短超时设置，StoreFront 将快速终止一台服务器并尝试另一台服务器。例如，这在出于故障转移的目的配置多台服务器时非常有用。

如果指定更长的超时，StoreFront 将等待更长时间以便单台服务器做出响应。在网络或服务器的可靠性不确定以及经常出现延迟的情况下，这极其有利。

Citrix Receiver for Web 也有一个超时设置，用于控制 Citrix Receiver for Web 站点等待应用商店作出响应的时间。将此超时设置设为大于等于应用商店超时的值。超时设置越长，容错能力越强，但用户所经历的延迟可能越长。超时设置越短，用户延迟越短，但他们所遇到的故障可能越多。

有关设置超时的信息，请参阅通信超时持续时间和服务器重试次数和通信超时持续时间和重试次数。

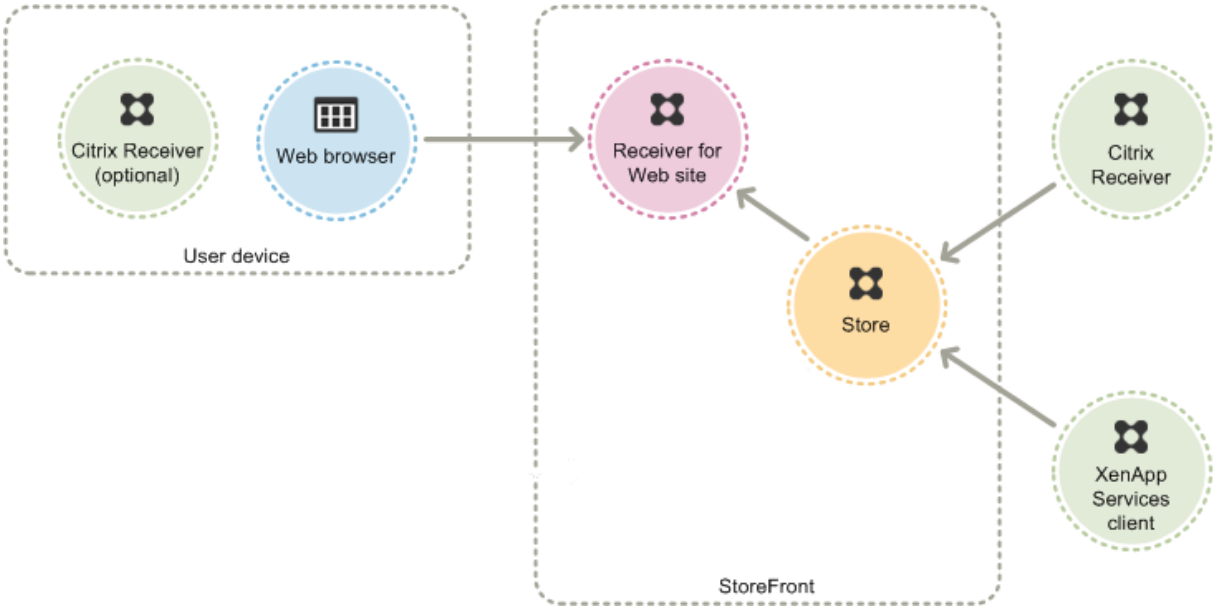
用户访问选项

June 29, 2021

用户可以通过三种不同的方法访问 StoreFront 应用商店。

- Citrix Receiver 或 Citrix Workspace 应用程序 - 具有兼容版本的 Citrix Receiver/Citrix Workspace 应用程序的用户可以通过 Citrix Receiver 或 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。
- Citrix Receiver for Web 站点 - 具有兼容 Web 浏览器的用户可以通过浏览 Citrix Receiver for Web 站点访问 StoreFront 应用商店。默认情况下，用户还需要具有兼容版本的 Citrix Receiver 或 Citrix Workspace 应用程序，才能访问桌面和应用程序。但是，您可以将 Citrix Receiver for Web 站点配置为允许用户使用与 HTML5 兼容的浏览器来访问其资源，而不必安装 Citrix Receiver 或 Citrix Workspace 应用程序。创建新应用商店时，默认情况下将为应用商店创建 Citrix Receiver for Web 站点。
- XenApp Services URL - 使用运行 Citrix Desktop Lock 的已加入域的桌面设备和重用 PC 机的用户，以及使用无法升级的旧版 Citrix 客户端的用户，可以使用应用商店的 XenApp Services URL 访问应用商店。创建新应用商店时，将默认启用 XenApp Services URL。

下图显示了用户可用来访问 StoreFront 应用商店的选项：



Citrix Receiver 或 Citrix Workspace 应用程序

从 Citrix Receiver 或 Citrix Workspace 应用程序用户界面访问应用商店时，可以提供最佳的用户体验和最强大的功能。有关可用于以这种方式访问应用商店的 Citrix Receiver 或 Citrix Workspace 应用程序版本，请参阅系统要求。除非另行说明，否则本文档中 “Citrix Workspace 应用程序” 的提及也表示受支持的 Citrix Receiver 版本。

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。

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：
>
> 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 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序文档中的 使用命令行参数配置和安装。

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，Citrix Receiver for Web 站点为用户提供的预配文件仅适用于为其配置了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 Receiver for 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 Mac OS 的用户，您可以使用 Citrix Receiver for Mac 或适用于 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。

手动配置

更高级的用户可以通过在 Citrix Workspace 应用程序中输入应用商店 URL 来创建新帐户。有关详细信息，请参阅 Citrix Workspace 应用程序文档。

基于电子邮件的帐户发现

首次在设备上安装 Citrix Workspace 应用程序的用户可以通过输入电子邮件地址来设置帐户，前提是用户已从 Citrix Web 站点或您的内部网络中托管的 Citrix Workspace 应用程序下载页面下载了 Citrix Workspace 应用程序。可以在 Microsoft Active Directory 域名系统 (DNS) 服务器上为 Citrix Gateway 或 StoreFront 配置服务位置 (SRV) 定位器资源记录。用户无需知道应用商店的详细访问信息，而只需要在 Citrix Workspace 应用程序初始配置过程中输入其电子邮件地址。Citrix Workspace 应用程序将与电子邮件地址中指定的域所对应的 DNS 服务器联系，并获得您添加到 SRV 资源记录中的详细信息。然后，用户将通过 Citrix Workspace 应用程序获得可访问应用商店的列表。

配置基于电子邮件的帐户发现

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。如果从 Citrix Web 站点或内部网络中托管的 Citrix Workspace 应用程序下载页面下载 Citrix Workspace 应用程序，则用户无需知道其应用商店的访问详细信息即可安装和配置 Citrix Workspace 应用程序。如果 Citrix Workspace 应用程序是从任何其他位置（例如 Receiver for Web 站点）下载的，则可以使用基于电子邮件的帐户发现。请注意，从 Citrix Receiver for Web 下载的 *ReceiverWeb.exe* 或 *ReceiverWeb.dmg* 不提示用户配置应用商店。用户仍然可以使用“添加帐户”并输入其电子邮件地址

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。用户输入电子邮件地址后，Citrix Workspace 应用程序会与电子邮件地址中指定的域所对应的 Microsoft Active Directory 域名系统 (DNS) 服务器进行联系，以获得用户可选择的可用应用商店的列表。

要允许 Citrix Workspace 应用程序根据用户的电子邮件地址查找可用应用商店，应在 DNS 服务器上配置 Citrix Gateway 或 StoreFront 的服务位置 (SRV) 定位器资源记录。或者，也可以在名为 discoverReceiver.domain 的服务器上部署 StoreFront，其中 domain 为用户电子邮件帐户所属的域。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。

您必须在 Citrix Gateway 设备或 StoreFront 服务器上安装有效的服务器证书，才能启用基于电子邮件的帐户发现。指向根证书的完整链也必须有效。为获得最佳用户体验，请安装具有 discoverReceiver.domain 的“使用者”或“使用者可选名称”条目的证书，其中 domain 为用户电子邮件帐户所属的域。虽然您可以为包含用户的电子邮件帐户的域使用通配符证书，但是必须首先确保贵公司的安全策略允许部署此类证书。也可以使用用户电子邮件帐户所属域的其他证书，但是当 Citrix Workspace 应用程序第一次连接到 StoreFront 服务器时，用户将看到一个证书警告对话框。基于电子邮件的帐户发现不能与任何其他证书身份验证一起使用。

要为从企业网络外部进行连接的用户启用基于电子邮件的帐户发现，还必须为 Citrix Gateway 配置详细的 StoreFront 连接信息。有关详细信息，请参阅使用基于电子邮件的发现连接到 StoreFront。

将 **SRV** 记录添加到 **DNS** 服务器

1. 在 Windows 开始屏幕中，单击管理工具，然后在管理工具文件夹中，单击 **DNS**。
2. 在 **DNS** 管理器的左侧窗格中，在正向或反向查找区域中选择您的域。右键单击域，然后选择其他新记录。
3. 在资源记录类型对话框中，选择服务位置 **(SRV)**，然后单击创建记录。
4. 在新建资源记录对话框的服务框中，输入主机值 **_citrixreceiver**。
5. 在协议框中输入值 **_tcp**。
6. 在提供此服务的主机框中，以 *servername.domain:port* 形式指定 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。

   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。
7. 如果针对 Citrix Gateway 设备配置了一条 SRV 记录，则应在会话配置文件或全局设置中将 StoreFront 连接详细信息添加到 Citrix Gateway 中。

Citrix Receiver for Web 站点

具有兼容 Web 浏览器的用户可以通过浏览 Citrix Receiver for Web 站点访问 StoreFront 应用商店。创建新应用商店时，将自动为应用商店创建一个 Citrix Receiver for Web 站点。Citrix Receiver for Web 站点的默认配置要求用户必须安装兼容版本的 Citrix Workspace 应用程序，才能访问自己的桌面和应用程序。有关可用于访问 Citrix Receiver for Web 站点的 Citrix Workspace 应用程序和 Web 浏览器组合的详细信息，请参阅用户设备要求。

默认情况下，当用户通过运行 Windows 或 Mac OS X 的计算机访问 Citrix Receiver for Web 站点时，此站点将尝试确定用户设备上是否已安装 Citrix Workspace 应用程序。如果检测不到 Citrix Workspace 应用程序，系统将提示用户下载并安装适合其平台的 Citrix Workspace 应用程序。默认下载位置为 Citrix Web 站点，但您也可以将安装文件复制到 StoreFront 服务器，并为用户提供这些本地文件。通过在本地存储 Citrix Workspace 应用程序安装文件，您可以将站点配置为向使用旧客户端的用户提供一个选项，使其升级到服务器上的版本。有关配置 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序和 Citrix Receiver for Mac 或适用于 Mac 的 Citrix Workspace 应用程序部署的详细信息，请参阅配置 Citrix Receiver for Web 站点。

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

适用于 HTML5 的 Citrix Workspace 应用程序是 StoreFront 的一个组件，默认与 Citrix Receiver for Web 站点相集成。可以在 Citrix Receiver for Web 站点上启用适用于 HTML5 的 Citrix Workspace 应用程序，以便无法安装 Citrix Workspace 应用程序的用户仍然可以访问其资源。使用适用于 HTML5 的 Citrix Workspace 应用程序时，用户可以直接在 HTML5 兼容的 Web 浏览器中访问桌面和应用程序，而无需安装 Citrix Workspace 应用程序。创建站点时，默认情况下，将禁用适用于 HTML5 的 Citrix Workspace 应用程序。有关启用适用于 HTML5 的 Citrix Workspace 应用程序的详细信息，请参阅 citrix-receiver-download-page-template.html。

要使用适用于 HTML5 的 Citrix Workspace 应用程序访问自己的桌面和应用程序，用户必须使用与 HTML5 兼容的浏览器访问 Citrix Receiver for Web 站点。有关可以与适用于 HTML5 的 Citrix Workspace 应用程序一起使用的操作系统和 Web 浏览器的详细信息，请参阅用户设备要求。

内部网络用户和通过 Citrix Gateway 连接的远程用户均可使用适用于 HTML5 的 Citrix Workspace 应用程序。对于来自内部网络的连接，适用于 HTML5 的 Citrix Workspace 应用程序仅支持对 Citrix Receiver for Web 站点支持的一部分产品所提供的桌面和应用程序进行访问。如果您在配置 StoreFront 时选择适用于 HTML5 的 Citrix Workspace 应用程序作为选项，则通过 Citrix Gateway 连接的用户将能够访问各种产品提供的资源。需要将特定版本的 Citrix Gateway 与适用于 HTML5 的 Citrix Workspace 应用程序结合使用。有关详细信息，请参阅基础结构要求。

对于内部网络中的本地用户，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，必须在您的 Citrix Virtual Apps and Desktops 服务器上启用 “ICA WebSockets 连接” 策略。确保您的防火墙及其他网络设备允许访问在策略中指定的适用于 HTML5 的 Citrix Workspace 应用程序端口。有关详细信息，请参阅WebSocket 策略设置。

默认情况下，适用于 HTML5 的 Citrix Workspace 应用程序会在新浏览器选项卡中启动桌面和应用程序。但是，当用户通过快捷方式使用适用于 HTML5 的 Citrix Workspace 启动资源时，桌面或应用程序会替换现有浏览器选项卡中的 Citrix Receiver for Web 站点，而不是显示在新选项卡中。您可以配置适用于 HTML5 的 Citrix Workspace 应用程序，使资源始终与 Receiver for Web 站点在同一选项卡中启动。有关详细信息，请参阅配置适用于 HTML5 的 Citrix Workspace 应用程序对浏览器选项卡的使用。

资源快捷方式

您可以生成 URL，利用该 URL 可以访问通过 Citrix Receiver for Web 站点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 Receiver for Web 站点，如果用户尚未登录，可以在该站点登录。Citrix 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。有关生成资源快捷方式的详细信息，请参阅配置 Citrix Receiver for Web 站点。

与从 Citrix Receiver for Web 站点访问的所有桌面和应用程序一样，用户必须已安装 Citrix Workspace 应用程序或者能够使用适用于 HTML5 的 Citrix Workspace 应用程序，才能通过快捷方式访问资源。Citrix Receiver for Web 站点使用的方法取决于站点配置，是否可以在用户设备上检测到 Citrix Workspace 应用程序以及是否使用了兼容

HTML5 的浏览器。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 Receiver for Web 站点添加到“本地 Intranet”或“可信站点”区域，以避免执行此额外步骤。默认情况下，当用户通过快捷方式访问 Citrix Receiver for Web 站点时会禁用工作区控制和自动桌面启动。

在创建应用程序快捷方式时，请确保 Citrix Receiver for Web 站点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，如果通过 Citrix Receiver for Web 站点提供单个桌面组中某个桌面的多个实例，则不能单独为每个实例都创建单独的快捷方式。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。有关详细信息，请参阅 http://support.citrix.com/article/CTX123610。

自定义站点

Citrix Receiver for Web 站点提供了一种用户界面自定义机制。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。

重要注意事项

通过 Citrix Receiver for Web 站点访问应用商店的用户可以获得在 Citrix Workspace 应用程序内部访问应用商店时所能使用的许多功能（例如应用程序同步）。决定是否使用 Citrix Receiver for Web 站点向用户提供应用商店访问权限时，请考虑以下限制。

- 通过每个 Citrix Receiver for Web 站点只能访问一个应用商店。
- Citrix Receiver for Web 站点无法启动安全套接字层 (SSL) 虚拟专用网络 (VPN) 连接。未使用 VPN 连接通过 Citrix Gateway 进行登录的用户无法访问 App Controller 要求使用 VPN 连接进行访问的 Web 应用程序。
- 通过 Citrix Receiver for Web 站点访问应用商店时，订阅的应用程序不会显示在 Windows 开始菜单中。
- 无法在本地文档与通过 Citrix Receiver for Web 站点访问的托管应用程序之间建立文件类型关联。
- 不能通过 Citrix Receiver for Web 站点访问脱机应用程序。
- Citrix Receiver for Web 站点不支持集成到应用商店中的 Citrix Online 产品。Citrix Online 产品必须随 App Controller 交付或作为托管应用程序提供，以支持通过 Citrix Receiver for Web 站点进行访问。
- 如果 VDA 为 XenApp 7.6 或 XenDesktop 7.6，并且启用了 SSL，或者如果用户使用 Citrix Gateway 进行连接，则可以通过 HTTPS 连接使用适用于 HTML5 的 Citrix Workspace 应用程序。
- 要在使用 HTTPS 连接时结合使用适用于 HTML5 的 Citrix Workspace 应用程序和 Mozilla Firefox，用户必须在 Firefox 地址栏中键入 `about:config`，并将 `network.websocket.allowInsecureFromHTTPS` 首选项设置为 true。

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 Citrix Receiver for Windows 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[秒]://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。

用户身份验证

June 29, 2021

StoreFront 为访问应用商店的用户提供了多种不同的身份验证方法，但并不是所有方法都可用，具体取决于用户的访问方法及其网络位置。出于安全原因，在创建第一个应用商店时，某些身份验证方法默认情况下处于禁用状态。有关启

用和禁用用户身份验证方法的详细信息，请参阅创建和配置身份验证服务。

用户名和密码

用户在访问应用商店时将输入其凭据以进行身份验证。默认情况下会启用显式身份验证。所有用户访问方法都支持显式身份验证。

当用户利用 Citrix Gateway 访问 Citrix Receiver for Web 时，Citrix Gateway 将处理登录，并且密码将在过期时更改。用户可以通过 Citrix Receiver for Web 用户界面选择更改密码。选择更改密码后，Citrix Gateway 会话将终止，用户必须重新登录。Citrix Receiver for Linux 或适用于 Linux 的 Citrix Workspace 应用程序用户只能更改过期密码。

SAML 身份验证

用户向 SAML 身份提供程序验证身份后，即可在访问自己的应用商店时自动登录。StoreFront 可以支持直接在企业网络中进行 SAML 身份验证，无需通过 Citrix Gateway。StoreFront 仅支持服务提供商启动（SP 启动）的登录，但不支持身份提供商启动（IdP 启动）的登录。

SAML（安全声明标记语言）是身份和身份验证产品（例如 Microsoft AD FS（Active Directory 联合身份验证服务））使用的开放式标准。通过 StoreFront 集成 SAML 身份验证后，管理员可以允许用户（例如）登录其企业网络一次，然后获取对其已发布的应用程序的单点登录。

要求：

- Citrix 联合身份验证服务 (FAS)的实现。除非安装 FAS，否则用户启动应用程序或桌面时不会进行单点登录 (SSO) 身份验证，因此他们每次都需要输入凭据。
- 符合 SAML 2.0 标准的身份提供程序 (IdPs)：
  - 仅使用 SAML 绑定（不使用 WS-Federation 绑定）的 Microsoft AD FS v4.0 (Windows Server 2016)。有关详细信息，请参阅AD FS 部署和AD FS 操作。
  - Microsoft AD FS v3.0 (Windows Server 2012 R2)
  - Citrix Gateway（配置为 IdP）
- 在新部署中（请参阅创建新部署）或在现有部署中（请参阅配置身份验证服务），使用 StoreFront 管理控制台在 StoreFront 中配置 SAML 身份验证。还可以使用 PowerShell cmdlet 配置 SAML 身份验证，请参阅 StoreFront SDK。
- Citrix Receiver for Windows（4.6 及更高版本）或适用于 Windows 的 Citrix Workspace 应用程序，或者 Citrix Receiver for Web。

当前 Receiver for Web 站点支持 SAML 身份验证与 Citrix Gateway 结合使用。

域直通

用户向其加入域的 Windows 计算机验证身份后，即可在访问自己的应用商店时使用其凭据自动登录。

安装 StoreFront 时，域直通身份验证默认情况下处于禁用状态。可以为通过 Citrix Workspace 应用程序和 XenApp Services URL 连接到应用商店的用户启用域直通身份验证。Citrix Receiver for Web 站点支持在已加入域的 Windows 客户端计算机上对 Internet Explorer、Microsoft Edge、Mozilla Firefox 和 Google Chrome 进行域直通身份验证。

启用域直通身份验证

1. 在用户设备上安装 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序，或者适用于 Windows 的 Citrix 联机插件。确保已启用直通身份验证。
2. 在管理控制台中的 “Citrix Receiver for Web 站点” 节点中，启用域直通身份验证。
3. 在 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序上配置 SSON，如配置域直通身份验证中所述。适用于 HTML5 的 Citrix Workspace 应用程序不支持域直通身份验证。
4. Windows 的默认行为是 “仅在 Intranet 区域中自动登录”。对于 Internet Explorer、Mozilla Firefox 和 Google Chrome，请使用 “Internet 选项” 将 Citrix Receiver for Web 站点配置为 Intranet 站点，或为受信任的区域启用自动登录。对于 Microsoft Edge，必须将 Citrix Receiver for Web 站点配置为 Intranet 站点。
5. 对于 Mozilla Firefox，请修改浏览器高级设置以信任 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序 URI。

   > 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。

   a) 启动 Firefox，在地址栏中输入 **about:config** 并选择 “我接受风险!”
   b) 在搜索框中键入 **ntlm**。
   c) 双击 network.automatic-ntlm-auth.trusted-uris，然后在弹出对话框中键入 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序站点 URL。
   d) 单击确定。

从 **Citrix Gateway** 直通

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 Citrix Receiver for Web 站点通过 Citrix Gateway 连接到应用商店。有关配置 StoreFront 以支持 Citrix Gateway 的详细信息，请参阅添加 Citrix Gateway 连接。

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

- 安全令牌。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，在某些情况下还会结合使用 PIN。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。
- 域和安全令牌。登录到 Citrix Gateway 的用户需要输入域凭据和安全令牌通行码。

- 客户端证书。用户登录到 Citrix Gateway，并根据提供给 Citrix Gateway 的客户端证书的属性进行身份验证。可以配置客户端证书身份验证，以允许用户使用智能卡登录到 Citrix Gateway。也可以将客户端证书身份验证与其他身份验证类型结合使用，以提供双来源身份验证。

StoreFront 使用 Citrix Gateway 身份验证服务为远程用户提供直通身份验证，以便这些用户只需输入一次凭据。但是，直通身份验证默认情况下仅对支持密码登录到 Citrix Gateway 的用户。要为智能卡用户配置从 Citrix Gateway 到 StoreFront 的直通身份验证，需要将凭据验证委派给 Citrix Gateway。有关详细信息，请参阅创建和配置身份验证服务。

用户可以使用 Citrix Gateway 插件通过安全套接字层 (SSL) 虚拟专用网络 (VPN) 通道以直通身份验证的方式从 Citrix Workspace 应用程序连接到应用商店。无法安装 Citrix Gateway 插件的远程用户可以使用无客户端访问，以直通身份验证的方式从 Citrix Workspace 应用程序连接到应用商店。要使用无客户端访问连接到应用商店，用户需要使用支持无客户端访问的 Citrix Workspace 应用程序版本。

此外，您还可以允许以直通身份验证的方式对 Citrix Receiver for Web 站点执行无客户端访问。为此，应将 Citrix Gateway 配置为安全远程代理。用户直接登录 Citrix Gateway，并使用 Citrix Receiver for Web 站点访问应用程序，而无需再次进行身份验证。

采用无客户端访问的形式连接到 App Controller 资源的用户仅能访问外部软件即服务 (SaaS) 应用程序。要访问内部 Web 应用程序，远程用户必须使用 Citrix Gateway 插件。

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 向 StoreFront 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。有关 SmartAccess 的详细信息，请参阅 SmartAccess 如何适用于 Citrix Virtual Apps and Desktops。

智能卡

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、Citrix Receiver for Web 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 App Controller 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 App Controller Web 应用程序。

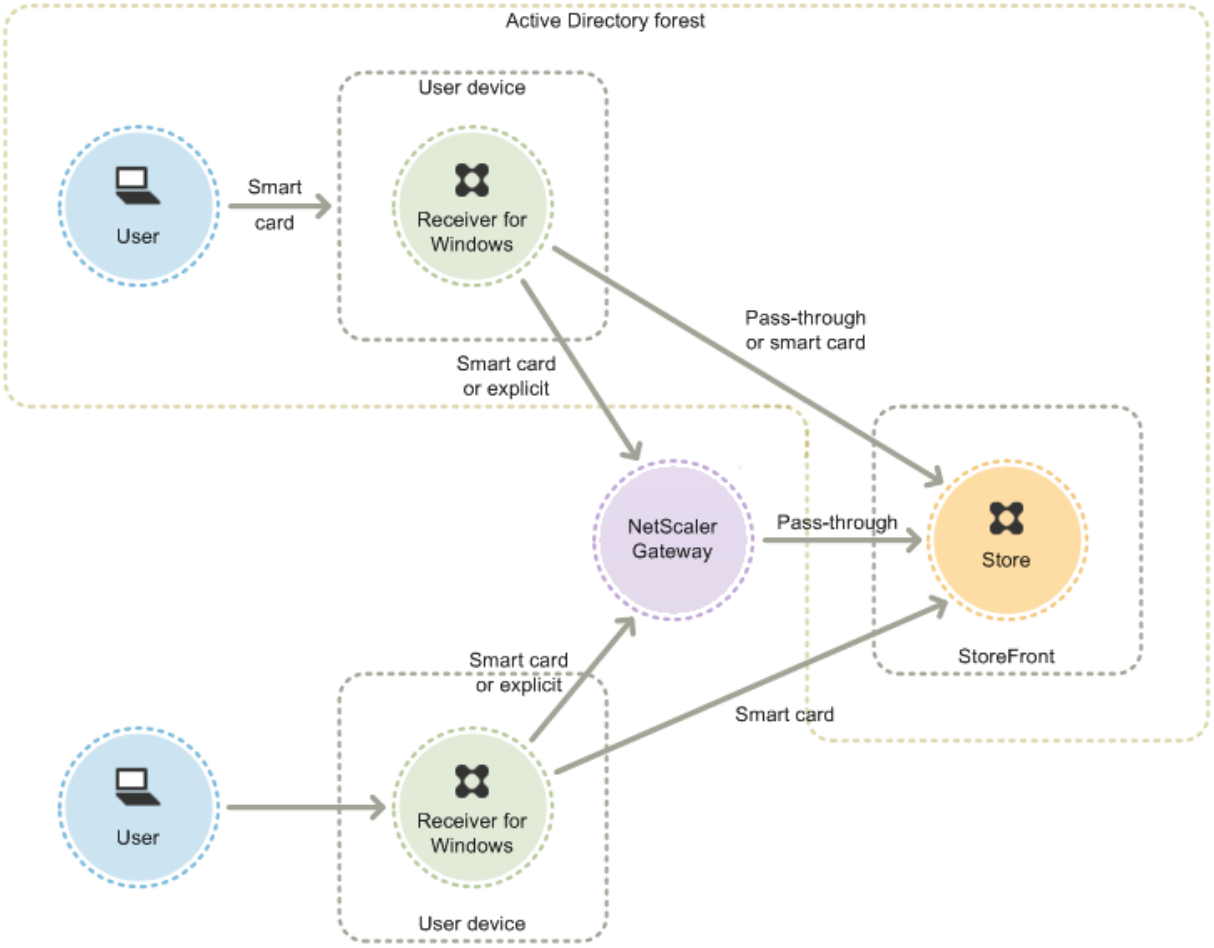
要启用智能卡身份验证，必须在包含 StoreFront 服务器的 Microsoft Active Directory 域或与 StoreFront 服务器域具有直接双向信任关系的域中配置用户的帐户。支持涉及双向信任的多林部署。

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。

对 **Citrix Receiver for Windows** 或适用于 **Windows** 的 **Citrix Workspace** 应用程序使用智能卡

使用运行 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序的设备的用户可以使用智能卡直接进行身份验证，或通过 Citrix Gateway 进行身份验证。既可以使用加入域的设备，也可以使用未加入域的设备，但用户体验稍有不同。

下图显示了通过 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序实现智能卡身份验证的选项。



对于使用已加入域的设备的用户，可以配置智能卡身份验证，以便系统仅提示用户输入凭据一次。用户将使用其智能卡和 PIN 登录设备，进行适当配置后，不会再次提示输入 PIN。用户在访问其桌面和应用程序时，会在无提示情况下向 StoreFront 进行身份验证。为此，可以为 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序配置直通身份验证并启用向 StoreFront 的域直通身份验证。

用户登录其设备，然后使用其 PIN 向 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序验证身份。尝试启动应用程序和桌面时，不再显示 PIN 提示。

由于未加入域的设备的用户将直接登录 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序，因此，您可以允许用户回退至显式身份验证。如果同时配置了智能卡和显式身份验证，则系统最初会提示用户使用智能卡和 PIN 进行登录，但在智能卡出现问题时可以选择使用显式身份验证。

通过 Citrix Gateway 进行连接的用户必须至少使用其智能卡和 PIN 登录两次，才能访问其桌面和应用程序。对于加入域的设备和未加入域的设备均是如此。用户使用智能卡和 PIN 进行身份验证，如果进行适当配置，用户在访问其桌面或应用程序时只会收到再次输入 PIN 的提示。为此，应启用通过 Citrix Gateway 进行针对 StoreFront 的直通身份验证并将凭据验证工作委派给 Citrix Gateway。然后，创建额外的 Citrix Gateway 虚拟服务器，用来将用户连接路由到资源。对于加入域的设备，还必须为 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序配置直通身份验证。

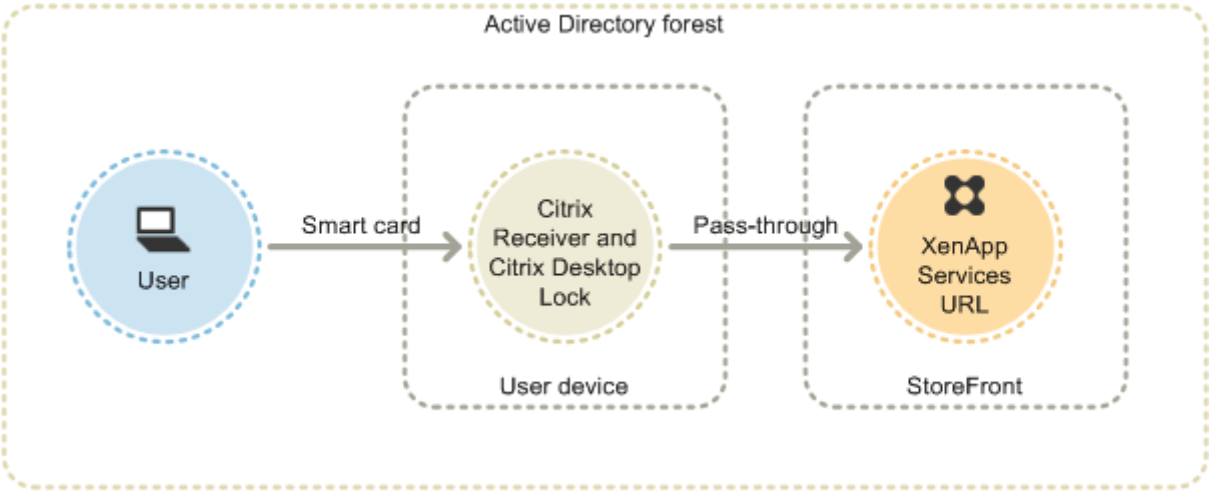
> 注意：
>
> 如果使用的是 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序，则可以设置第二个虚拟服务器并使用最佳网关路由功能，这样在启动应用程序和桌面时，不需要再提示输入 PIN。

用户可以使用智能卡和 PIN 或使用显式凭据登录 Citrix Gateway。这允许您为用户提供选项，以回退至使用显式身份验证进行 Citrix Gateway 登录。可以配置从 Citrix Gateway 到 StoreFront 的直通身份验证，并将智能卡用户的凭据验证委派给 Citrix Gateway，这样用户就可以无提示地向 StoreFront 进行身份验证。

对 **XenApp Services URL** 使用智能卡

运行 Citrix Desktop Lock 的 PC 的用户可以使用智能卡进行身份验证。与其他访问方法不同，当智能卡身份验证被配置为支持 XenApp Services URL 时，会自动启用智能卡凭据直通功能。

下图显示了如何从运行 Citrix Desktop Lock 的已加入域的设备进行智能卡身份验证。



用户使用智能卡和 PIN 登录到设备。随后，Citrix Desktop Lock 通过 XenApp Services URL 无提示地进行 StoreFront 对用户的身份验证。用户在访问桌面和应用程序时会自动进行身份验证，不会再次提示其输入 PIN。

对 **Citrix Receiver for Web** 使用智能卡

可以从 StoreFront 管理控制台启用向 Citrix Receiver for Web 的智能卡身份验证。

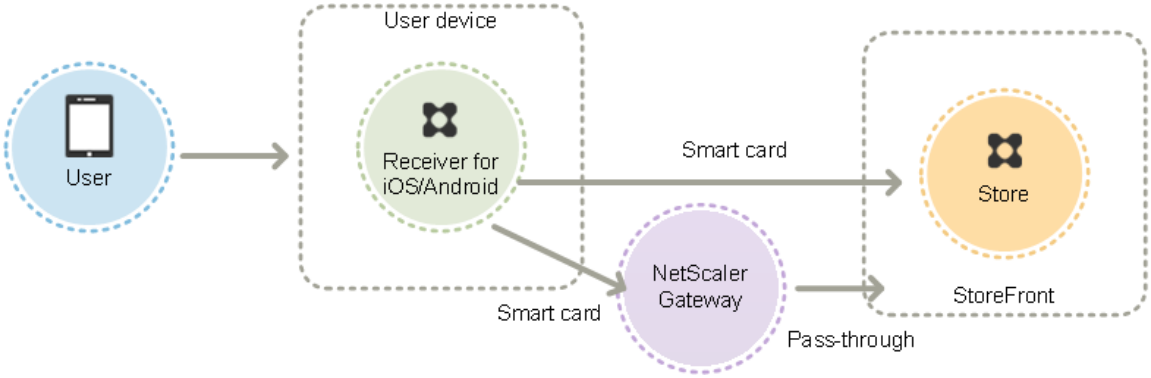
1. 在左侧面板中选择 Citrix Receiver for Web 节点。
2. 选择要使用智能卡身份验证的站点。
3. 在右侧面板中选择选择身份验证方法任务。
4. 选中弹出对话框屏幕中的“智能卡”复选框，然后单击“确定”。

如果为使用已加入域的设备但不通过 Citrix Gateway 访问应用商店的 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序用户启用了向 Citrix Virtual Apps and Desktops 使用智能卡进行直通身份验证，则此设置将应用于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。

如果为使用已加入域的设备通过 Citrix Gateway 访问应用商店的 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序用户启用了向 Citrix Virtual Apps and Desktops 使用智能卡进行直通身份验证，则此设置将应用于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。

对适用于 **iOS** 和 **Android** 的 **Citrix Workspace** 应用程序使用智能卡

使用运行适用于 iOS 和 Android 的 Citrix Workspace 应用程序的设备的用户可以使用智能卡直接进行身份验证，或通过 Citrix Gateway 进行身份验证。可以使用未加入域的设备。



如果在本地网络中存在设备，用户最少会收到两次登录提示。用户向 StoreFront 验证身份或最初创建应用商店时，会收到输入智能卡 PIN 码的提示。进行适当配置后，用户仅在访问其桌面和应用程序时，再次收到输入 PIN 的提示。为此，应启用针对 StoreFront 的智能卡身份验证，并在 VDA 上安装智能卡驱动程序。

使用这些 Citrix Workspace 应用程序，您可以选择指定智能卡或域凭据。如果您创建了应用商店以使用智能卡或希望使用域凭据连接到同一应用商店，则必须在未打开智能卡的情况下添加单独的应用商店。

通过 Citrix Gateway 进行连接的用户必须至少使用其智能卡和 PIN 登录两次，才能访问其桌面和应用程序。用户使用智能卡和 PIN 进行身份验证，如果进行适当配置，用户在访问其桌面或应用程序时只会收到再次输入 PIN 的提示。为此，应启用通过 Citrix Gateway 进行针对 StoreFront 的直通身份验证并将凭据验证工作委派给 Citrix Gateway。然后，创建额外的 Citrix Gateway 虚拟服务器，用来将用户连接路由到资源。

用户可以使用智能卡和 PIN 或使用显式凭据登录到 Citrix Gateway，具体视您为连接指定身份验证的方式而定。可以配置从 Citrix Gateway 到 StoreFront 的直通身份验证，并将智能卡用户的凭据验证委派给 Citrix Gateway，这样用户就可以无提示地向 StoreFront 进行身份验证。如果要更改身份验证方法，必须先删除连接，然后再重新创建。

对 **Citrix Receiver for Linux** 或适用于 **Linux** 的 **Citrix Workspace** 应用程序使用智能卡

使用运行 Citrix Receiver for Linux 或适用于 Linux 的 Citrix Workspace 应用程序的设备的用户可以像未加入域的 Windows 设备的用户那样，使用智能卡直接进行身份验证。即使用户使用智能卡向 Linux 设备进行身份验证，Citrix Receiver for Linux 或适用于 Linux 的 Citrix Workspace 应用程序也无法获得或重用输入的 PIN。

采用与 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序相同的方式为服务器端组件配置智能卡。请参阅配置智能卡身份验证，有关使用智能卡的说明，请参阅 Citrix Receiver for Linux。

用户最少会收到一次登录提示。用户登录其设备，然后使用其智能卡和 PIN 向 Citrix Receiver for Linux 或适用于 Linux 的 Citrix Workspace 应用程序验证身份。用户在访问其桌面和应用程序时，不会再次收到输入 PIN 的提示。为此，应启用针对 StoreFront 的智能卡身份验证。

由于用户直接登录到 Citrix Receiver for Linux 或适用于 Linux 的 Citrix Workspace 应用程序，因此，您可以允许用户回退至显式身份验证。如果同时配置了智能卡和显式身份验证，则系统最初会提示用户使用智能卡和 PIN 进行登录，但在智能卡出现问题时可以选择使用显式身份验证。

通过 Citrix Gateway 进行连接的用户必须至少使用其智能卡和 PIN 登录一次，才能访问其桌面和应用程序。用户使用智能卡和 PIN 进行身份验证，如果进行适当配置，用户在访问其桌面或应用程序时不会收到再次输入 PIN 的提示。为

此，应启用通过 Citrix Gateway 进行针对 StoreFront 的直通身份验证并将凭据验证工作委派给 Citrix Gateway。然后，创建额外的 Citrix Gateway 虚拟服务器，用来将用户连接路由到资源。

用户可以使用智能卡和 PIN 或使用显式凭据登录 Citrix Gateway。这允许您为用户提供选项，以回退至使用显式身份验证进行 Citrix Gateway 登录。可以配置从 Citrix Gateway 到 StoreFront 的直通身份验证，并将智能卡用户的凭据验证委派给 Citrix Gateway，这样用户就可以无提示地向 StoreFront 进行身份验证。

XenApp Services 支持站点不支持 Citrix Receiver for Linux 或适用于 Linux 的 Citrix Workspace 应用程序的智能卡。

同时为服务器和 Citrix Workspace 应用程序启用智能卡支持后，假设智能卡证书的应用程序策略允许使用，则可以使用智能卡执行以下操作：

- 智能卡登录身份验证。使用智能卡向 Citrix Virtual Apps and Desktops 服务器验证用户身份。
- 智能卡应用程序支持。允许支持智能卡的已发布应用程序访问本地智能卡设备。

对 **XenApp Services** 支持使用智能卡

登录 XenApp Services 支持站点以启动应用程序和桌面的用户可以使用智能卡进行身份验证，具体视特定硬件、操作系统和 Citrix Workspace 应用程序而定。用户访问 XenApp Services 支持站点并成功输入智能卡和 PIN 时，PNA 将确定用户身份、向 StoreFront 进行用户身份验证并返回可用资源。

要使直通和智能卡身份验证生效，您必须启用 “Trust requests sent to the XML service”（信任发送到 XML Service 的请求）。

使用 Delivery Controller 上具有本地管理员权限的帐户启动 Windows PowerShell，然后在命令提示窗口处输入以下命令，以使 Delivery Controller 信任发送自 StoreFront 的 XML 请求。以下过程适用于 XenApp 7.5 到 7.8 以及 XenDesktop 7.0 到 7.8。

1. 加载 Citrix cmdlet，方法是键入 `asnp Citrix*.`（包括句点）。
2. 键入 `Add-PSSnapin citrix.broker.admin.v2`。
3. 键入 `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True`。
4. 关闭 PowerShell。

有关配置 XenApp Services 支持智能卡身份验证方法的信息，请参阅配置 XenApp Services URL 的身份验证。

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。智能卡已插入读卡器时收到插入智能卡提示的用户必须单击取消。如果提示用户输入 PIN，则必须再次输入 PIN。
- 如果为使用已加入域的设备但不通过 Citrix Gateway 访问应用商店的 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序用户启用了向 Citrix Virtual Apps and Desktops 使用智能卡进行直通身份验证，则此设置将应用于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。
- 如果为使用已加入域的设备通过 Citrix Gateway 访问应用商店的 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序用户启用了向 Citrix Virtual Apps and Desktops 使用智能卡进行直通身份验证，则此设置将应用于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。

优化用户体验

June 29, 2021

StoreFront 中包括一些用于增强用户体验的功能。默认情况下，这些功能在您创建新应用商店及其关联的 Citrix Receiver for Web 站点和 XenApp Services URL 时进行配置。

工作区控制

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。

默认情况下，对 Citrix Receiver for Web 站点以及通过 XenApp Services URL 与应用商店建立的连接，启用工作区控制功能。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，假设一个用户通过 Citrix Receiver for Web 站点或 XenApp Services URL 登录到一个应用商店，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。对于 Citrix Receiver for Web 站点，必须使用相同的浏览器登录，启动应用程序，然后从中注销。

不能配置或禁用 XenApp Services URL 的工作区控制。有关配置 Citrix Receiver for Web 站点的工作区控制的详细信息，请参阅配置工作区控制。

在 Citrix Receiver for Web 站点上使用工作区控制，需要满足并遵循以下要求和限制。

- 从托管桌面和应用程序访问 Citrix Receiver for Web 站点时，工作区控制功能不可用。
- 对于从 Windows 设备访问 Citrix Receiver for Web 站点的用户，仅当以下情况下才启用工作区控制功能：站点可以检测用户设备上是否已安装 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 Citrix Receiver for 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 Citrix Receiver for 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。Citrix Receiver for Web 站点无法断开或关闭使用不同浏览器启动的资源，以及使用 Citrix Workspace 应用程序从桌面或开始菜单本地启动的资源。

内容重定向

如果用户已订阅相应的应用程序，内容重定向功能将允许使用订阅的应用程序在用户设备上打开本地文件。要启用本地文件重定向，应在 Citrix Virtual Apps and Desktops 中将应用程序与所需文件类型相关联。默认情况下，将为新应用商店启用文件类型关联。有关详细信息，请参阅 禁用文件类型关联。

用户更改密码

可以允许使用 Microsoft Active Directory 域凭据登录的 Citrix Receiver for Web 站点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。

即使您允许用户随时更改密码，登录到桌面设备站点的用户也只能更改过期的密码。桌面设备站点没有提供允许用户在登录后更改密码的控制项。

创建身份验证服务时，默认配置会禁止 Citrix Receiver for Web 站点用户更改自己的密码，即使密码已过期也是如此。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。StoreFront 必须能够与域控制器进行通信，才能更改用户的密码。

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。

Citrix Receiver for Web 站点桌面和应用程序视图

如果某个 Citrix Receiver for Web 站点同时提供桌面和应用程序，则该站点在默认情况下将分别显示桌面视图和应用程序视图。用户登录该站点后，将首先看到桌面视图。无论 Citrix Receiver for Web 站点是否也提供应用程序，只要用户只能使用一个桌面，该站点就会在用户登录时自动启动该桌面。您可以为 Citrix Receiver for Web 站点配置所显示的视图，还可以阻止站点为用户自动启动桌面。有关详细信息，请参阅 配置资源对用户的显示方式。

Citrix Receiver for Web 站点上视图的行为取决于所交付资源的类型。例如，要使应用程序出现在应用程序视图中，用户必须事先订阅这些应用程序，而对用户可用的所有桌面都将自动显示在桌面视图中。因此，用户不能从桌面视图中删除桌面，也不能通过拖放图标的方式对桌面进行重新组织。Citrix Virtual Desktops 管理员启用桌面重新启动功能后，桌面视图中会提供允许用户重新启动桌面的控制项。如果用户有权访问单个桌面组中某个桌面的多个实例，则 Citrix Receiver for Web 站点将在桌面名称后附加数字后缀，以便为用户区分这些桌面。

对于在 Citrix Workspace 应用程序中或通过 XenApp Services URL 连接到应用商店的用户，桌面和应用程序的显示方式及其行为将由所使用的 Citrix 客户端决定。

其他建议

通过 Citrix Virtual Apps and Desktops 交付应用程序时，请考虑通过您的应用商店增强用户访问其应用程序时的体验。有关交付应用程序的详细信息，请参阅创建交付组应用程序。

- 组织应用程序，以便用户在浏览可用资源时能够轻松查找所需内容。在 Citrix Virtual Apps and Desktops Studio 中分配给应用程序的应用程序类别在 Citrix Workspace 应用程序和 Citrix Receiver for Web 中显示为类别。例如，可以按类型对应用程序进行分类，也可以为组织中的不同用户角色创建类别。
- 确保在交付应用程序时添加有意义的说明，因为用户可以在 Citrix Workspace 应用程序中看到这些说明。
- 您可以指定所有用户都有一组核心应用程序，不能通过将字符串 `KEYWORDS:Mandatory` 附加到应用程序说明的末尾将其从 Citrix Workspace 应用程序主屏幕中删除。用户仍可使用自助服务用户界面添加更多应用程序或删除非强制性应用程序。
- 可以通过将字符串 `KEYWORDS:Auto` 附加到您在交付应用程序时所提供的说明的末尾，以自动为某个应用商店的所有用户订阅该应用程序。用户登录到该应用商店时，相应的应用程序将自动预配，而无需用户手动订阅。
- 要为某个应用商店的所有用户自动订阅由 App Controller 管理的 Web 应用程序或软件即服务 (SaaS) 应用程序，请在配置应用程序设置时选中应用程序在 **Citrix Receiver** 或 **Citrix Workspace** 应用程序中自动对所有用户可用复选框。
- 向用户公告 Citrix Virtual Apps and Desktops 应用程序，或者在 Citrix Workspace 应用程序的“精选”列表中列出常用的应用程序，以使其更易于查找。为此，请将字符串 `KEYWORDS:Featured` 附加到应用程序说明后面。

> 注意：
>
> 多个关键字之间只能用空格进行分隔；例如 `KEYWORDS:Auto Featured`。

- 默认情况下，Citrix Receiver for Web 站点对待 Citrix Virtual Apps and Desktops 托管的共享桌面的方式与对待其他桌面的方式相同。要更改此行为，请将字符串 `KEYWORDS:TreatAsApp` 附加到桌面说明的末尾。桌面将显示在 Citrix Receiver for Web 站点的应用程序视图中，而不是桌面视图中，用户在访问此桌面之前需要先订阅。此外，当用户登录到 Citrix Receiver for 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。
- 对于 Windows 用户，可以指定当本地安装版的应用程序与交付的等同实例都可用时，要优先使用前者。为此，请将字符串 `KEYWORDS:prefer="application"` 附加到应用程序说明的末尾，其中 *application* 是快捷方式文件名指定的本地应用程序名称中的一个或多个完整单词，或\开始菜单文件夹中本地应用程序的绝对路径（包括可执行文件名）。当用户使用此关键字订阅应用程序时，Citrix Workspace 应用程序会在用户设备上搜索指定名称或路径，以确定是否已在本地安装了此应用程序。如果找到了应用程序，Citrix Workspace 应用程序将为用户订阅该交付的应用程序，但不创建快捷方式。当用户从 Citrix Workspace 应用程序启动该交付的应用程序时，运行的将是本地安装的实例。有关详细信息，请参阅 配置应用程序交付。
- 在 Citrix Virtual Apps and Desktops 中，用户从已发布的桌面内部启动已发布的应用程序时，管理员可以控制该应用程序在该桌面会话中启动，还是在相同的交付组中作为已发布的应用程序启动。请在 Broker Service 中使用 PowerShell cmdlet 以及使用 Citrix Receiver for Windows (vPrefer) 中的策略设置来控制此行为。此功能仅在 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序启动已发布的应用程序时起作用。如果已发布的应用程序是在 Web 浏览器中通过 StoreFront 站点启动的，则不能用于在本地启动应用程序。在早期版本中，“双跃点”应用程序启动控制要求在 Studio 中使用 `KEYWORDS:Prefer` 标记。仍然可以使用 `KEYWORDS:Prefer` 标记。如果同时配置了 KEYWORDS 和 vPrefer 方法，vPrefer 的优先级更高。

  有关详细信息，请参阅 CTX232210、Citrix Virtual Apps and Desktops 文档中的应用程序一文以及 Citrix Receiver for Windows 文档。

StoreFront 的高可用性和多站点配置

June 5, 2020

StoreFront 包括许多功能，结合使用这些功能可以在为应用商店提供资源的各部署之间实现负载平衡和故障转移。还可以指定专用的灾难恢复部署，以提高恢复能力。利用这些功能，您可以配置跨多个站点的分布式 StoreFront 部署，从而实现应用商店的高可用性。有关详细信息，请参阅设置高可用多站点应用商店配置。

资源聚合

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。

如果为特定应用商店配置的多个 Citrix Virtual Apps and Desktops 部署提供同一桌面或应用程序，则 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。不能聚合 App Controller 应用程序。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。

将用户映射到资源

默认情况下，访问某一应用商店的用户会看到为该应用商店配置的所有部署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。但是，设置高可用的多站点配置时，可以根据用户在 Microsoft Active Directory 组中的成员身份来提供对特定部署的访问。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。

订阅同步

如果要使用户能够从不同 StoreFront 部署中的相似应用商店访问相同应用程序，则用户的应用程序订阅必须在各服务器组之间同步。否则，订阅了一个 StoreFront 部署中的应用商店的某一应用程序的用户在登录到另一个服务器组时，

可能还需要重新订阅该应用程序。要为在单独的 StoreFront 部署之间移动的用户提供无缝体验，可以将不同服务器组中各应用商店之间的用户应用程序订阅配置为定期同步。可以选择按特定间隔进行定期同步或者将同步安排在一天中的特定时间进行。有关详细信息，请参阅配置订阅同步。

专用灾难恢复资源

可以配置特定灾难恢复部署，此类部署只有在所有其他部署均不可用时才使用。通常，灾难恢复部署不与主部署搭配使用，只提供一部分通常可用的资源，而且还可能使用户体验下降。如果指定某一部署用于灾难恢复，则该部署将不能用于负载平衡或故障转移。除非所有其他配置了灾难恢复部署的部署均不可用，否则用户无法访问灾难恢复部署所提供的桌面和应用程序。

重新建立对任何其他部署的访问时，用户无法启动更多的灾难恢复资源，即使用户已经在使用这些资源。恢复对其他部署的访问之后，运行灾难恢复资源的用户与这些资源的连接并不会断开。但是，用户退出灾难恢复资源之后就无法再次启动这些资源。同样，如果随后任何其他部署恢复到可用状态，则 StoreFront 不会将现有会话再次用于灾难恢复部署。

最佳 **Citrix Gateway** 路由

如果已经为部署配置了单独的 Citrix Gateway 设备，则 StoreFront 允许您为用户定义用于访问提供应用商店资源的每个部署的最佳设备。例如，如果创建一个聚合来自两个地理位置的资源的应用商店，并为每个位置配置一个 Citrix Gateway 设备，则通过其中一个位置的设备进行连接的用户可以启动另一个位置的桌面或应用程序。但是，默认情况下，与资源之间的连接随后将通过用户最初连接的设备进行路由，因此必须穿过公司 WAN。

要改善用户体验并减少通过 WAN 的网络流量，可以为每个部署指定最佳 Citrix Gateway 设备。这样配置后，用户与资源的连接将自动通过与提供资源的部署对应的本地设备进行路由，而与用户访问应用商店时所用设备的位置无关。

对于内部网络中的本地用户需要登录到 Citrix Gateway 进行端点分析的这种特殊情况，也可以使用最佳 Citrix Gateway 路由。利用此配置，用户将通过 Citrix Gateway 设备连接到应用商店，但不需要通过该设备路由与资源的连接，因为用户位于内部网络中。在这种情况下，您启用最佳路由，但无需为部署指定设备，因此用户与桌面和应用程序的连接将直接进行路由，而不通过 Citrix Gateway。请注意，还必须为 Citrix Gateway 设备配置特定的内部虚拟服务器 IP 地址。此外，还需指定一个不可访问的内部信标点，以便始终提示 Citrix Workspace 应用程序连接到 Citrix Gateway，而不考虑用户的网络位置。

Citrix Gateway 全局服务器负载平衡

StoreFront 支持将 Citrix Gateway 部署配置为使用全局服务器负载平衡配置和多个具有一个完全限定的域名 (FQDN) 的设备。要进行用户身份验证以及通过适当的设备路由用户连接，StoreFront 必须能够区分各个设备。由于在全局服务器负载平衡配置中不能将设备 FQDN 用作唯一标识符，因此必须为 StoreFront 配置每个设备的唯一 IP 地址。通常，这是 Citrix Gateway 虚拟服务器的 IP 地址。

有关负载平衡的信息，请参阅使用 Citrix ADC 进行负载平衡。

重要注意事项

决定是否为应用商店设置高可用的多站点配置时，请考虑以下要求和限制。

- 桌面和应用程序必须在每台服务器上具有相同名称和路径才能进行聚合。另外，聚合资源的属性（如名称和图标）必须相同。否则，当 Citrix Workspace 应用程序枚举可用资源时，用户可能会看到其资源的属性发生变化。
- 不应聚合已分配的桌面，包括预先分配的桌面和首次使用时分配的桌面。请确保提供此类桌面的交付组在站点中的名称和路径与为聚合配置的名称和路径不同。
- 不能聚合 App Controller 应用程序。
- 如果将单独 StoreFront 部署中各应用商店之间的用户应用程序订阅配置为同步，则这些应用商店必须在每个服务器组中具有相同的名称。另外，服务器组都必须位于包含用户帐户的 Active Directory 域中，或者位于与用户帐户域之间存在信任关系的域中。
- 仅当等效部署集中的所有主站点都不可用时，StoreFront 才会提供对用于灾难恢复的备份部署的访问。如果备份部署在多个等效部署集之间共享，则只有在每个部署集中的所有主站点均不可用时，用户才可以访问灾难恢复资源。

安装、设置、升级和卸载

July 5, 2021

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. 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：
   >
   > - 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。

2. StoreFront 要求安装 Microsoft .NET Framework，如果尚未安装，可以从 Microsoft 下载。必须先安装 Microsoft .NET，才能安装 StoreFront。

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。

   a) 确保在 Citrix ADC 设备上启用负载平衡。

   b) 对于每个 StoreFront 服务器，根据需要使用 StoreFront 监视器类型创建各 HTTP 或 SSL 负载平衡服务。

c) 通过配置服务将客户端 IP 地址插入转发给 StoreFront 的请求的 X-Forwarded-For HTTP 标头中，覆盖任何全局策略。

StoreFront 需要使用用户的 IP 地址来与其资源建立连接。

d) 创建虚拟服务器并将服务绑定到虚拟服务器。

e) 在虚拟服务器上，使用客户端 **IP** 或 **Cookie** 插入方法配置持久性。确保生存时间 (TTL) 足够长，以使用户能够根据需要在尽可能长的时间内保持登录到服务器。

持久性可确保仅对初始用户连接进行负载平衡，此后来自该用户的后续请求将定向到同一台 StoreFront 服务器。

4. （可选）启用以下功能。

   - .NET Framework 功能 > .NET Framework、ASP.NET

   （可选）在 StoreFront 服务器上启用以下角色及其依赖项。

   - Web 服务器 (IIS) > Web 服务器 > 常见 HTTP 功能 > 默认文档、HTTP 错误、静态内容、HTTP 重定向
   - Web 服务器 (IIS) > Web 服务器 > 运行状况和诊断 > HTTP 日志记录
   - Web 服务器 (IIS) > Web 服务器 > 安全性 > 请求筛选、Windows 身份验证
   - Web 服务器 (IIS) > Web 服务器 > 应用程序开发 > .NET 扩展性、应用程序初始化、ASP.NET、ISAPI 扩展、ISAPI 筛选器

   StoreFront 安装程序将检查是否已启用上述所有功能和服务器角色。

5. 安装 StoreFront.

   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。

6. （可选）如果计划使用 HTTPS 来确保 StoreFront 与用户设备之间的连接安全，请将 Microsoft Internet Information Services (IIS) 配置为支持 HTTPS。

   智能卡身份验证必须使用 HTTPS。默认情况下，Citrix Workspace 应用程序需要使用 HTTPS 来连接应用商店。要配置 IIS，以便您可以在 StoreFront 中使用 HTTPS hostbaseURL，请创建与默认 Web 站点的 HTTPS 绑定，并将其链接到 StoreFront 服务器证书。有关将 HTTPS 绑定添加到 IIS 站点的详细信息，请参阅保护 StoreFront 部署的安全。

7. （可选）配置 传输层安全性 (TLS)。

8. 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。

9. 如果要使用多个 Internet Information Services (IIS) Web 站点，请在 IIS 中创建 Web 站点后，使用 PowerShell SDK 在其中每个 IIS Web 站点中创建一个 StoreFront 部署。有关详细信息，请参阅多个 Internet Information Services (IIS) Web 站点。

   > 注意：
   >
   > StoreFront 会在检测到多个站点时禁用管理控制台并针对该影响显示一条消息。

10. 使用 Citrix StoreFront 管理控制台配置您的服务器。

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。
> - 从 StoreFront 1912 LTSR CU1 开始，要首次在自定义位置安装 StoreFront，您必须使用 -INSTALLDIR 参数从命令提示符进行安装以指定该位置。请参阅 从命令提示窗口安装 StoreFront。

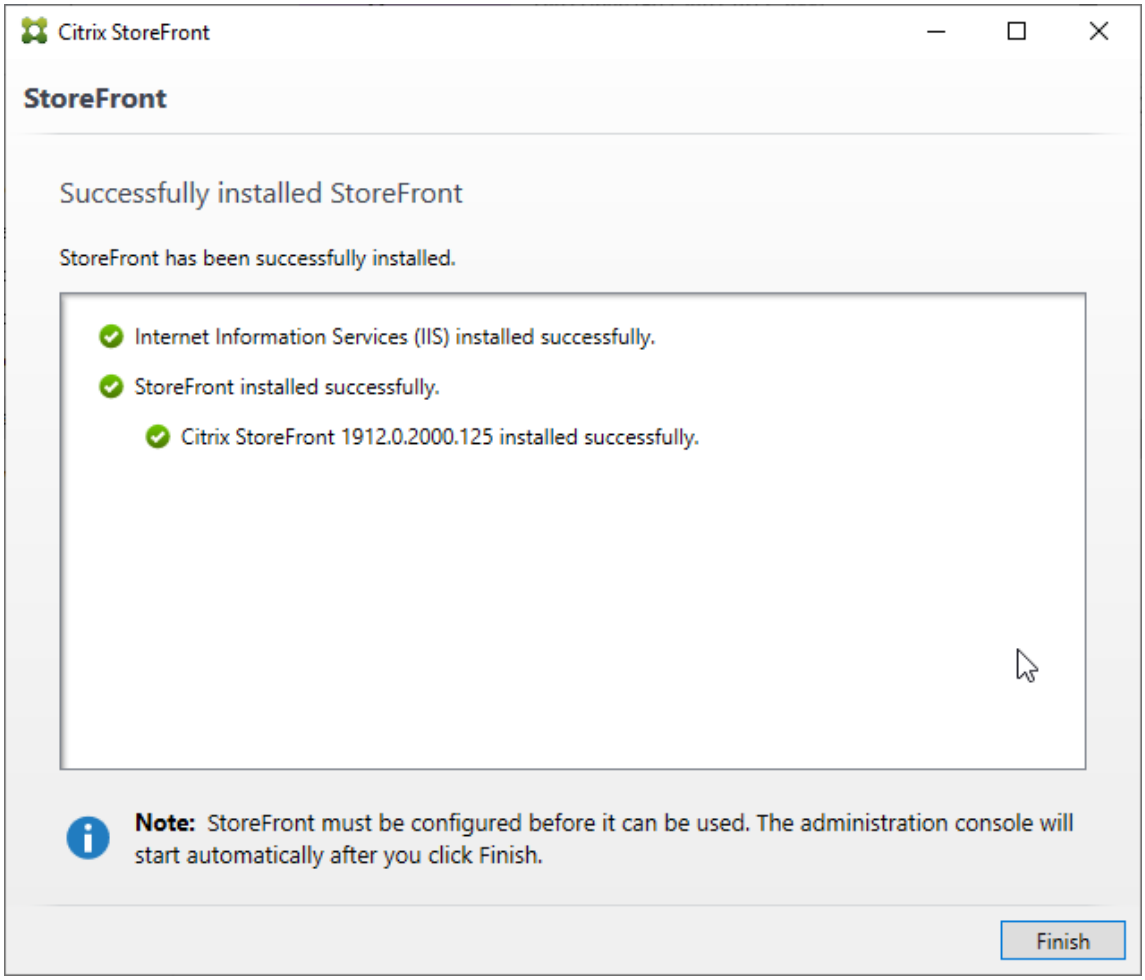
1. 从下载页面下载安装程序。
2. 使用具有本地管理员权限的帐户登录 StoreFront 服务器。
3. 请务必在服务器上安装所需的 Microsoft .NET Framework。
4. 找到 CitrixStoreFront-x64.exe，然后以管理员身份运行此文件。
5. 阅读并接受许可协议，然后单击下一步。
6. 如果显示检查必备项页面，请单击下一步。
7. 在已做好安装准备页面上，检查所列的安装必备项和 StoreFront 组件，然后单击安装。

   在安装组件之前，如果服务器尚未配置以下角色，则会启用这些角色。

   - Web 服务器 (IIS) > Web 服务器 > 常见 HTTP 功能 > 默认文档、HTTP 错误、静态内容、HTTP 重定向
   - Web 服务器 (IIS) > Web 服务器 > 运行状况和诊断 > HTTP 日志记录
   - Web 服务器 (IIS) > Web 服务器 > 安全性 > 请求筛选、Windows 身份验证
   - Web 服务器 (IIS) > 管理工具 > IIS 管理控制台、IIS 管理脚本和工具

   如果尚未配置以下功能，则同时会启用这些功能。

   - .NET Framework 功能 > .NET Framework、ASP.NET
8. 安装完成后，单击完成。Citrix StoreFront 管理控制台自动启动。您还可以从“开始”屏幕打开 StoreFront。



> 注意：
>
> 从 StoreFront 1912 年 LTSR CU1 开始，需要在安装 StoreFront 后重新启动。

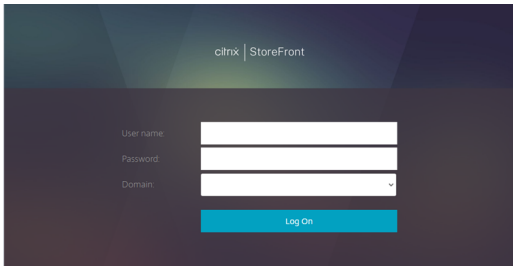
9. 在 Citrix StoreFront 管理控制台中，单击创建新部署。
   a) 在基本 **URL** 框中指定 StoreFront 服务器的 URL。
   b) 在应用商店名称页面上，指定应用商店的名称，然后单击下一步。

在 **Delivery Controller** 页面上，输入提供您希望在应用商店中提供的资源的 Citrix Virtual Apps and Desktops 部署。

1. 设置传输类型和端口，例如 HTTP 和端口 80，或 HTTPS 和端口 443，然后单击确定。
2. 在远程访问页面上，选择“无”。如果要使用 Citrix Gateway，请选择无 VPN 通道，然后输入网关详细信息。
3. 在远程访问页面上，选择“创建”。创建完应用商店之后，单击完成。

现在，用户已可以通过 Citrix Receiver for Web 站点访问您的应用商店，这使用户能够通过 Web 页面访问其桌面和应用程序。

此时将显示一个 URL，用户可使用该 URL 访问新应用商店的 Citrix Receiver for Web 站点。例如：`example.net/Citrix/StoreWeb/`。登录后，您将在 Citrix Workspace 应用程序中访问新的用户界面。



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]
```

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。安装位置必须是本地文件系统上现有驱动器的完全限定路径名，例如 “C:\ABC”。有效字符包括 a–z A–Z 0–9 . ~ \ - ( ) _ 和空格。不允许安装到用户配置文件文件夹的子目录中。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，如果 Citrix Receiver for Web 站点检测不到 Windows 或 Mac OS X 设备上的 Citrix Workspace 应用程序，系统将提示用户从 Citrix Web 站点下载和安装适合其平台的 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。将 *filelocation* 替换为包含要复制的安装文件的目录，并将 *filename* 替换为安装文件的名称。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 应用程序安装文件都包含在 Citrix Virtual Apps and Desktops 安装介质中。

CEIP

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
```

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。

数据	说明
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

如果您是 Citrix Cloud 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 Citrix Cloud 中的 Citrix Analytics 服务。配置后，Citrix Workspace 应用程序以及从 HTML5 兼容的浏览器访问的 Citrix Receiver for Web 站点将用户事件发送到 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 的载入 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。

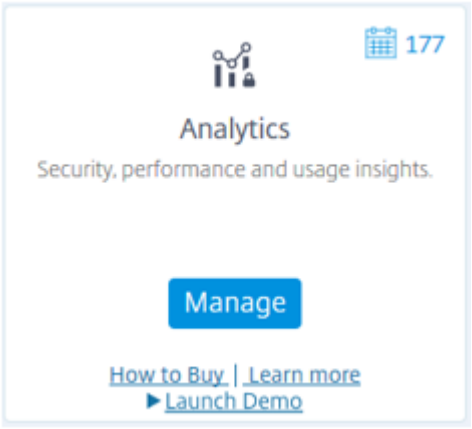
配置 StoreFront 后，当 Citrix Analytics 服务请求时，Citrix Workspace 应用程序可以从 StoreFront 应用商店发送数据。

> 重要：
>
> 为了此功能正常工作并使用 Citrix Cloud 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：
>
> 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 Citrix Cloud (`https://citrix.cloud.com/`)。
2. 选择 Citrix Cloud 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”
 }
```


其中

customerId 为当前 Citrix Cloud 客户的唯一 ID。

cwsServiceKey 为标识当前 Citrix Cloud 客户帐户的唯一密钥。

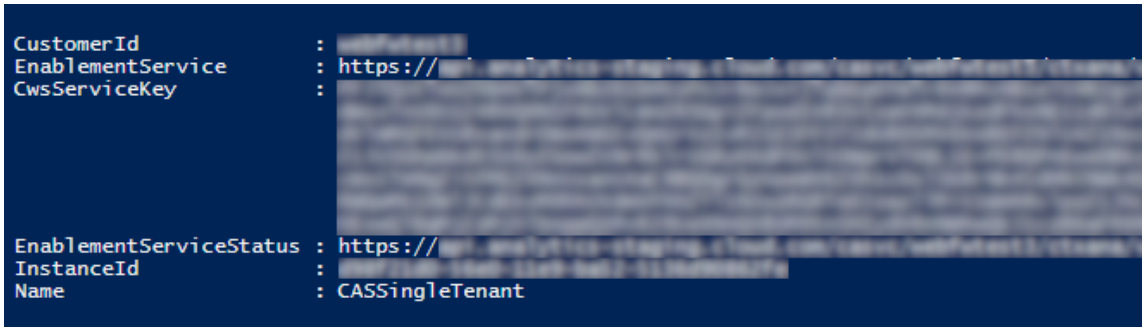
instanceID 是生成的 ID，用于对从 Citrix Workspace 应用程序发送到 Citrix Analytics 的请求进行签名（确保安全）。如果您向 Citrix Cloud 注册多个 StoreFront 服务器或服务器组，则每个服务器或服务器组都具有唯一的 instanceID。

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：

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

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 Citrix Cloud。

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
```

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
```

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
   ```

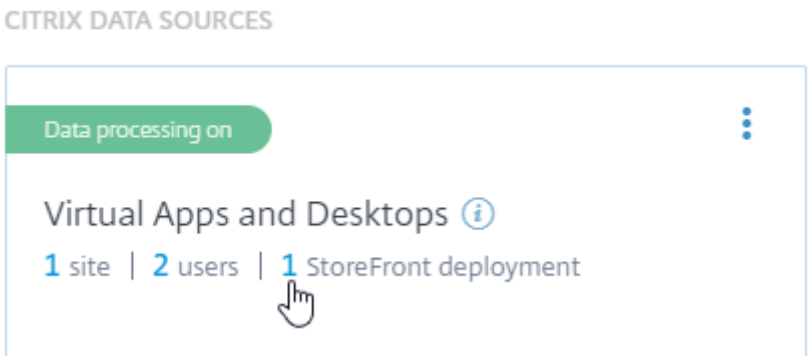
   如果以前导入的 Citrix Analytics 数据已被成功删除，**Get-STFCasConfiguration** 将不返回任何内容。
3. 如果要对 StoreFront 服务器组执行这些操作，请传播所做的更改并从服务器组的所有成员中删除导入的 Citrix Analytics 数据。在服务器组中的一个服务器上，运行以下命令：

   ```
   Publish-STFServerGroupConfiguration
   ```

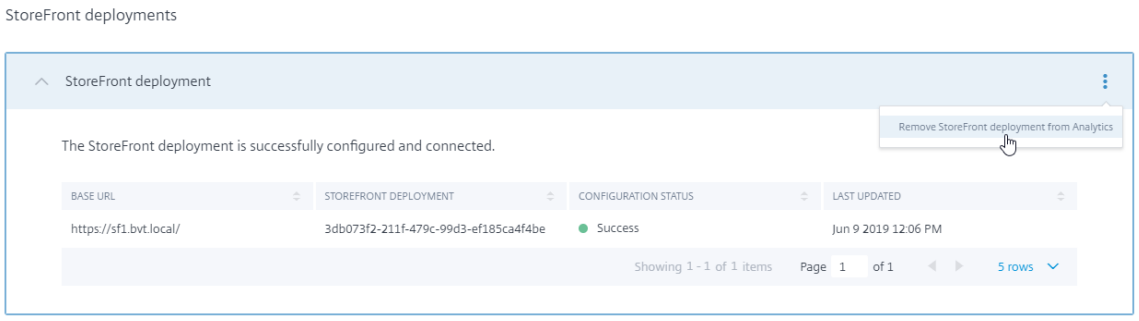

4. 在任何其他服务器组成员上，运行以下命令以确认已成功从组中的所有服务器中删除 Citrix Analytics 配置：

   ```
   Get-STFCasConfiguration
   ```

5. 使用管理员帐户登录 Citrix Cloud (`https://citrix.cloud.com/`)。
6. 选择 Citrix Cloud 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 **Citrix Cloud** 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)

```

```
16      foreach($Store in $Stores)
17      {
18
19          Write-Host "Backing up the Store web.config file for store
                $Store before making changes..." -ForegroundColor "
               Yellow"
20          Write-Host "`n"
21
22          if(!(Test-Path "$env:UserProfile\desktop$Store"))
23          {
24
25              Write-Host "Creating $env:UserProfile\desktop$Store\
                   directory for backup..." -ForegroundColor "Yellow"
26              New-Item -Path "$env:UserProfile\desktop$Store" -
                   ItemType "Directory" | Out-Null
27              Write-Host "`n"
28           }
29
30
31          Write-Host "Copying c:\inetpub\wwwroot\Citrix$Store\web.
               config to $env:UserProfile\desktop$Store..." -
               ForegroundColor "Yellow"
32          Copy-Item -Path "c:\inetpub\wwwroot\Citrix$Store\web.
               config" -Destination "$env:UserProfile\desktop$Store" -
               Force | Out-Null
33
34          if(Test-Path "$env:UserProfile\desktop$Store\web.config")
35          {
36
37              Write-Host "$env:UserProfile\desktop$Store\web.config
                   file backed up" -ForegroundColor "Green"
38           }
39
40          else
41          {
42
43              Write-Host "$env:UserProfile\desktop$Store\web.config
                   file NOT found!" -ForegroundColor "Red"
44           }
45
46          Write-Host "`n"
47
48          Write-Host "Setting the proxy server to $ProxyAddress for
               Store $Store..." -ForegroundColor "Yellow"
49          Write-Host "`n"
```



```
50
51          $StoreConfigPath = ”c:\inetpub\wwwroot\Citrix$Store\web.
                config”
52          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
53
54          if([string]::IsNullOrEmpty($ProxyFQDN))
55          {
56
57              $ProxyServer = (”HTTP://$ProxyIP”+”:”+$ProxyPort)
58           }
59
60          else
61          {
62
63              $ProxyServer = (”HTTP://$ProxyFQDN”+”:”+$ProxyPort)
64           }
65
66
67          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
68
69          # Create 3 elements
70          $SystemNet = $XMLObject.CreateNode(”element”,”system.net”,
                ””)
71          $DefaultProxy = $XMLObject.CreateNode(”element”,”
                defaultProxy”,””)
72          $Proxy = $XMLObject.CreateNode(”element”,”proxy”,””)
73          $Proxy.SetAttribute(”proxyaddress”,”$ProxyServer”)
74          $Proxy.SetAttribute(”bypassonlocal”,”true”)
75
76          # Move back up the XML tree appending new child items in
                reverse order
77          $DefaultProxy.AppendChild($Proxy)
78          $SystemNet.AppendChild($DefaultProxy)
79          $XMLObject.configuration.AppendChild($SystemNet)
80
81          # Save the modified XML document to disk
82          $XMLObject.Save($StoreConfigPath)
83
84          Write-Host ”Getting the proxy configuration for c:\inetpub
                \wwwroot\Citrix$Store...” -ForegroundColor ”Yellow”
85          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
86          $ConfiguredProxyServer = $XMLObject.configuration.'system.
                net'.defaultProxy.proxy.proxyaddress | Out-Null
87          Write-Host (”Configured proxy server for Store $Store”+”:
                ”+ $ConfiguredProxyServer) -ForegroundColor ”Green”
```

```
88          Write-Host "`n"
89       }
90
91      Write-Host "Restarting IIS..." -ForegroundColor "Yellow"
92      IISReset /RESTART
93   }
94
95
96  Set-StoreProxyServer -Stores $Stores -ProxyFQDN $ProxyFQDN -
       ProxyPort $ProxyPort
97  # OR
98  Set-StoreProxyServer -Stores $Stores -ProxyIP $ProxyIP -ProxyPort
       $ProxyPort
```

5. 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>
```

6. 按将 Citrix Analytics 数据导入到 StoreFront 部署中中所述导入 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 FQDNN 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：

```
1   <system.net>
2       <defaultProxy>
```



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

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>
```

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>
```

4. 按将 Citrix Analytics 数据导入到 StoreFront 部署中中所述导入 Citrix Analytics 数据。

升级 **StoreFront**

> 警告：
>
> 升级到 StoreFront 1912 时，部署中的所有桌面设备站点都会自动删除。如果需要保留桌面设备站点，请勿升级。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。
>
> 升级到 StoreFront 1912 CU2 时，必须在 Controller 或 StoreFront 上重新配置 TLS 密码套件的顺序，以确保 StoreFront 应用商店中的应用程序正确枚举并启动。有关详细信息，请参阅已知问题和传输层安全性 (TLS)。

升级将保留您的 StoreFront 的配置，并将用户的应用程序订阅数据保留原样，以便用户不需要订阅其所有应用程序。相比之下，卸载 StoreFront 会删除 StoreFront 和相关联的服务、站点、应用程序订阅数据（在独立服务器上）和相关联的配置。

须知

- 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。
- 不支持从现在已结束使用的旧版当前版本升级到最新的 StoreFront 当前版本。有关详细信息，请参阅CTX200356。
- 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。
- 升级到此版本的 StoreFront 时，使用经典用户体验的所有应用商店都会更新为使用统一体验。我们建议您告知用户升级引入的新体验，如统一用户体验中所述。如果您自定义了统一体验，则在升级到此版本的 StoreFront 时会保留您的自定义设置。检查自定义外观是否仍适用于新的统一体验。
- 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。

- 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。
- 关闭 StoreFront 服务器上的所有其他应用程序。
- 关闭 StoreFront 管理控制台。
- 关闭所有命令行和 PowerShell 窗口。
- 关闭所有与 StoreFront 相关的文件夹，例如 C:\inetpub\wwwroot\Citrix\Store 和 C:\inetpub\wwwroot\Citrix\Store\ 这样可以防止 Windows 资源管理器对其使用排他锁。
- 在升级服务器之前，请重新启动服务器以确保 StoreFront 文件或文件夹上没有排他锁。（重新启动资源管理器进程 - 例如通过关闭 Windows 资源管理器的所有实例 - 是不够的。
- 立即运行升级，而无需启动服务器上的任何其他程序。
- 使用管理员帐户升级服务器，在此过程中，请不要运行任何其他安装并且运行最少量的其他应用程序。

升级独立的 **StoreFront** 服务器

1. 断开用户与 StoreFront 部署的连接，以在升级过程中阻止用户访问服务器。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。
2. 通过创建 VM 快照备份服务器。
3. 导出现有 StoreFront 配置（推荐）。
4. 运行此版本的 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。

升级服务器组之前：

- 通过创建 VM 快照备份组中的所有服务器。这样，如果升级未按计划进行，您可以快速恢复到正在工作的三节点服务器组。
- 导出现有 StoreFront 配置（推荐）。仅从一台服务器导出服务器组配置。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。此备份允许您轻松构建新的服务器组。

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. 通过创建 VM 快照备份组中的所有服务器。
2. 来自服务器组中的一台服务器中的导出现有 StoreFront 配置。

3. 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。
4. 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”。
5. 通过运行此版本的 StoreFront 的安装文件来升级服务器 A。
6. 确保服务器 A 已成功升级。
7. 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。
8. 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。

   该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。
9. 检查所有服务器是否正常运行。
10. 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。

1. 通过创建 VM 快照备份组中的所有服务器。
2. 来自服务器组中的一台服务器中的导出现有 StoreFront 配置。
3. 使用管理应用商店的订阅数据中所述的 **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，这会删除订阅和配置数据。
4. 通过禁用代表服务器 C 的负载平衡器服务来禁用用户对服务器 C 的访问。这会阻止用户在升级过程中连接到服务器 C。保持表示服务器 A 和 B 的负载平衡服务处于启用状态，以便用户能够继续使用。
5. 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 现在已与服务器组孤立。
6. 使用 **Clear-STFDeployment** 将孤立服务器 C 重置为出厂默认状态
7. 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。
8. 通过运行此版本的 StoreFront 的安装文件来升级服务器 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。
9. 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。
10. 使用服务器 B 重复步骤 4、5、6 和 8（请勿重复步骤 9）。在此期间，只有服务器 A 为用户提供资源访问权限。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。
11. 使用加入现有服务器组过程将服务器 B 加入到服务器 C。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。
12. 同时为服务器 B 和 C 启用负载平衡服务，以便其能够从服务器 A 接管。

13. 禁用服务器 A 的负载平衡服务，以便将用户定向到新升级的服务器 B 和 C。
14. 使用服务器 A 重复步骤 6 和 8。
15. 使用加入现有服务器组过程将服务器 A 加入服务器组 B 和 C。这在新 StoreFront 版本（服务器 A、B 和 C）上提供了一个新的三节点服务器组。
16. 为服务器 A 启用负载平衡的服务，以便将用户定向到所有三台升级后的服务器 A、B 和 C。
    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 10）。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。

配置 StoreFront

> 注意：
>
> 在安装和升级过程中，本地管理组的成员将被复制到 CitrixStoreFrontAdministrators 组中。这使得上次安装或升级 StoreFront 时已属于本地管理员组的用户能够使用 StoreFront 管理控制台来配置 StoreFront 服务器组，并执行相关传播和复制任务。如果稍后将用户添加到本地管理员组，则必须手动将用户复制到 CitrixStoreFrontAdministrators 组中，然后才能使用 StoreFront 管理控制台来配置 StoreFront 服务器组，并执行相关传播和复制任务。如果您将当前登录的用户添加到 CitrixStoreFrontAdministrators 组中，则需要注销并重新登录才能使用 StoreFront 管理控制台。

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。Citrix 建议您向服务器组中添加的服务器不要超过 6 个。

卸载 StoreFront

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. 如果打开了 StoreFront 管理控制台，请关闭。

3. 关闭任何可能已通过其 PowerShell SDK 管理 StoreFront 的 PowerShell 会话。
4. 在 Windows 开始屏幕或 “应用程序” 屏幕中，找到并单击 **Citrix StoreFront** 磁贴。在该磁贴上单击鼠标右键，然后单击卸载。
5. 在程序和功能对话框中，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。

使用 **PowerShell** 卸载 **StoreFront**

您可以使用以下 PowerShell 来触发 StoreFront 的 MSI 窗口卸载：

1. 列出所有已安装的应用程序：

   ```
   Get-WmiObject -Class Win32_Product | Select-Object -Property Name
   ```

2. 如果列出了应用商店，则执行以下命令：

   ```
   $storefront = Get-WmiObject -Class Win32_Product | Where-Object{ $_.
   Name -eq "<Storefront_Product_Name>"}
   ```

3. 运行 `$storefront` 以确认它映射到所需产品。
4. 运行 `$storefront.uninstall()`。

创建新部署

June 29, 2021

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. 在基本 **URL** 框中指定多服务器部署中的 StoreFront 服务器或负载平衡环境的 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。
4. 单击下一步以设置身份验证服务，该服务将对 Microsoft Active Directory 验证用户的身份。

   要使用 HTTPS 来确保 StoreFront 与用户设备之间通信的安全，必须先将 Microsoft Internet Information Services (IIS) 配置为支持 HTTPS。如果没有合适的 IIS 配置，StoreFront 将使用 HTTP 进行通信。

   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。智能卡身份验证必须使用 HTTPS。可以在配置 StoreFront 后随时从 HTTP 更改为 HTTPS，只要相应的 IIS 配置已就位即可。有关详细信息，请参阅配置服务器组。

   可以随时使用 StoreFront 管理控制台中的更改基本 **URL** 任务从 HTTP 更改为 HTTPS，前提是已为 HTTPS 配置了 Microsoft Internet Information Services (IIS)。

5. 在应用商店名称页面上，指定应用商店的名称以及是否仅允许未经身份验证的（匿名）用户访问该应用商店，然后单击下一步。

   StoreFront 应用商店将桌面和应用程序聚合在一起，使其对用户可用。此时应用商店名称将显示在 Citrix Workspace 应用程序中的用户帐户下方，请选择一个向用户描述应用商店内容信息的名称。

6. 在 **Delivery Controller** 页面上，列出用于提供希望通过该应用商店获得的资源的基础结构。要向应用商店添加桌面和应用程序，请按照将 Citrix Virtual Apps and Desktops 资源添加到应用商店中中所述的相应步骤进行操作。可以将应用商店配置为提供任何 Citrix Virtual Apps and Desktops 部署组合中的资源。根据需要重复执行这些过程，以添加为该应用商店提供资源的所有部署。

7. 将所有必需的资源添加到应用商店之后，请在 **Delivery Controller** 页面中单击下一步。

8. 在远程访问页面上，指定从公用网络连接的用户是否以及如何能够访问内部资源。

   - 要将应用商店设置为对公用网络中的用户可用，请选中启用远程访问复选框。如果未选中此复选框，则只有内部网络中的本地用户能够访问该应用商店。
   - 要使仅通过该应用商店交付的资源可通过 Citrix Gateway 访问，请选择允许用户访问仅通过 **StoreFront** 交付的资源 **(**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) 通道获得内部网络中的应用商店以及所有其他资源，请选择允许用户访问内部网络中的所有资源 **(**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。

9. 如果已启用远程访问，**Citrix Gateway** 设备将列出用户可通过其访问应用商店的部署。要向此列表中添加 Citrix Gateway 部署，请按照通过 Citrix Gateway 设备提供对应用商店的远程访问中所述的相应步骤进行操作。根据需要重复执行这些过程，以添加更多部署。

10. 在 **Citrix Gateway** 设备列表中，选择用户可通过其访问应用商店的部署。如果启用通过多个部署进行访问，请指定要用于访问应用商店的默认设备。单击下一步。

11. 在身份验证方法页面上，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。您可以从以下方法中进行选择：

    - 用户名和密码：用户在访问其应用商店时将输入其凭据并进行身份验证。
    - **SAML** 身份验证：用户向身份提供程序验证身份后，即可在访问应用商店时自动登录。
    - 域直通 **†**：用户向其加入域的 Windows 计算机验证身份，即可在访问应用商店时使用其凭据自动登录。
    - 智能卡 **†**：用户在访问应用商店时使用智能卡和 PIN 进行身份验证。
    - **HTTP Basic**：用户将向 StoreFront 服务器的 IIS Web 服务器进行身份验证。
    - 通过 **Citrix Gateway** 直通：用户向 Citrix Gateway 验证身份后，即可在访问应用商店时自动登录。启用了远程访问时自动选中此方法。

> 注意：
>
> † 不会传播到应用商店的 Citrix Receiver for Web 站点的应用商店身份验证方法。使用配置 Citrix Receiver for Web 站点中所述的管理 **Receiver for Web** 站点任务为每个 Citrix Receiver for Web 站点独立配置这些身份验证方法。
>
> 本文中介绍的其他应用商店身份验证方法确实会传播到应用商店的 Citrix Receiver for Web 站点。（也就是说，在本文中为应用商店进行的选择或取消选择决定了其所有 Receiver for Web 站点使用的设置。）

12. 在配置密码验证页面上，选择 Delivery Controller 以提供密码验证，然后单击下一步。
13. 在 **XenApp Services URL** 页面上，为使用 PNAgent 访问应用程序和桌面的用户配置 XenApp Service URL。
14. 创建应用商店后，Citrix StoreFront 管理控制台中的可用选项将增多。有关详细信息，请参阅配置和管理应用商店。

现在，用户可以使用 Citrix Workspace 应用程序来访问您的应用商店，但必须为其配置该应用商店的访问详细信息。您可以通过许多方式为用户提供这些详细信息，以简化用户的配置过程。有关详细信息，请参阅用户访问选项。

或者，用户可以通过 Citrix Receiver for Web 站点访问应用商店，这使用户能够通过 Web 页面访问其桌面和应用程序。创建应用商店时，将会显示用户用于访问新应用商店的 Citrix Receiver for Web 站点的 URL。

创建新应用商店时，将默认启用 XenApp Services URL。使用运行 Citrix Desktop Lock 的已加入域的桌面设备和重用 PC 的用户，以及使用无法升级的旧版 Citrix 客户端的用户，可以使用应用商店的 XenApp Services URL 直接访问应用商店。XenApp Services URL 的格式为 http[秒]://serveraddress/Citrix/storename/PNAgent/config.xml，其中 serveraddress 是 StoreFront 部署的服务器或负载平衡环境的完全限定域名；storename 是在步骤 5 中指定的应用商店名称。

安装 StoreFront 的更多实例时，要快速向您的部署中添加更多服务器，请选择用于加入现有服务器组的选项。

将 **Citrix Virtual Apps and Desktops** 资源添加到应用商店中

要通过在 StoreFront 服务器的初始配置中创建的应用商店获得由 Citrix Virtual Apps and Desktops 提供的桌面和应用程序，请完成以下步骤。假设您已经完成本文顶部“创建新部署”过程中的第 1 步到第 6 步。

1. 在 **Delivery Controller** 页面上，列出用于提供希望通过该应用商店获得的资源的基础结构。单击添加。
2. 在“添加 Delivery Controller”对话框中，指定一个有助于识别部署的显示名称，并选择一种类型以指示希望如何通过该应用商店提供资源。“类型”默认设置为“Citrix Virtual Apps and Desktops”。XenApp 6.5 作为一种类型提供，但它已于 2018 年 6 月达到生命周期已结束状态，现在已包含在扩展支持计划中。
3. 要通过应用商店获取由 Citrix Virtual Apps and Desktops 和 XenApp 6.5 提供的桌面和应用程序，请在服务器列表中添加服务器的名称或 IP 地址。指定多台服务器以启用容错功能，并按优先级顺序列出这些条目以设置故障转移顺序。对于 Citrix Virtual Apps and Desktops 站点，请提供 Delivery Controller 的详细信息。对于 XenApp 6.5 场，列出运行 Citrix XML Service 的服务器。
4. 从传输类型列表中选择要用来与服务器通信的 StoreFront 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。
- 要通过使用传输层安全性 (TLS) 的安全 HTTP 连接发送数据，请选择 **HTTPS**。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。
- 要通过与 XenApp 6.5 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**。

> 注意：
>
> 如果使用 HTTPS 或 SSL Relay 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）。

5. 指定 StoreFront 连接服务器所用的端口。使用 HTTP 和 SSL Relay 的连接的默认端口为 80，HTTPS 连接的默认端口为 443。对于 Citrix Virtual Apps and Desktops 服务器，指定的端口必须是 Citrix XML Service 所使用的端口。
6. 如果要使用 SSL Relay 确保 StoreFront 与 XenApp 6.5 服务器之间的连接安全，请在 **SSL Relay** 端口中指定 SSL Relay 的 TCP 端口。默认端口为 443。确保将运行 SSL Relay 的所有服务器配置为监视同一端口。
7. 单击确定。可以将应用商店配置为提供任何 Citrix Virtual Apps and Desktops 部署组合中的资源。要添加更多 Citrix Virtual Desktops 站点或 Citrix Virtual Apps 场，请重复上述步骤。将需要的所有资源添加到应用商店后，返回到本文顶部“创建新部署”过程中的第 7 步。

通过 **Citrix Gateway** 设备提供对应用商店的远程访问

要配置通过 Citrix Gateway 设备提供对 StoreFront 服务器的初始配置中所创建应用商店的远程访问，请完成以下步骤。假设您已经完成本文顶部“创建新部署”过程中的步骤 1 到步骤 9。

1. 在 StoreFront 控制台“创建应用商店”对话框的远程访问页面上，单击添加。
2. 在“添加 Citrix Gateway 设备”对话框中的常规设置页面上，为 Citrix Gateway 设备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网关。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或者最靠近其所在位置的网关。
3. 对于 **Citrix Gateway URL**，请键入用于您的部署的 Citrix Gateway 虚拟服务器的“URL: 端口”组合。如果未指定端口，则使用默认 `https://` 端口 443。没有必要在 URL 中指定端口 443。

   有关创建单个完全限定的域名 (FQDN) 以在内部和外部访问应用商店的信息，请参阅创建单个完全限定的域名 (FQDN) 以在内部和外部访问应用商店。
4. 从可用选项中选择 Citrix Gateway 的用法或角色。
   - 身份验证和 **HDX** 路由： Citrix Gateway 将用于进行身份验证以及路由任何 HDX 会话。

- 仅限身份验证： Citrix Gateway 将用于身份验证，不用于任何 HDX 会话路由。
- 仅限 **HDX** 路由： Citrix Gateway 将用于 HDX 会话路由，不用于身份验证。

5. 对于所有部署，如果要通过应用商店提供由 Citrix Virtual Apps and Desktops 或 XenApp 6.5 提供的资源，请在 **Secure Ticket Authority** 页面上添加运行 STA 的服务器的 **Secure Ticket Authority (STA) URL**。添加多个 STA 的 URL 以启用容错功能，并按优先级顺序列出这些服务器以设置故障转移顺序。

   STA 托管在 Citrix Virtual Apps and Desktops 或 XenApp 6.5 服务器上，并发出会话票据以响应连接请求。这些会话票据构成了对访问 Citrix Virtual Apps and Desktops 或 XenApp 6.5 资源进行身份验证和授权的基础。使用正确的 STA URL（例如 `HTTPS://` 或`HTTP://`），具体取决于 Delivery Controller 的配置方式。STA URL 还必须与在虚拟服务器上的 Citrix Gateway 中配置的 URL 相同。

6. 要确保 Citrix Virtual Apps and Desktops 或 XenApp 6.5 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，请选择启用会话可靠性。

7. 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。StoreFront 将从两个不同的 STA 获取会话票据，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。

8. 在身份验证设置页面上，键入 Citrix Gateway 设备的虚拟服务器 **IP** 地址 (VIP)。

   使用 Citrix Gateway 虚拟服务器的专用 IP 地址，而非通过网络地址转换功能转换为专用 IP 地址的公用 IP 地址。网关通常由 StoreFront 通过其 URL 进行识别。如果使用全局服务器负载平衡 (GSLB)，则必须将 VIP 添加到每个网关中。这允许 StoreFront 识别多个网关，这些网关都使用相同的 URL（GSLB 域名）作为不同的网关。例如，可以为使用相同 URL 的应用商店配置三个网关（例如 `https://gslb.domain.com`），但每个网关都配置了唯一的 VIP，例如 10.0.0.1、10.0.0.2 和 10.0.0.3。

9. 如果要添加运行 Citrix Gateway 的设备，请从登录类型列表中选择您在设备上为 Citrix Workspace 应用程序用户配置的身份验证方法。

   - 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。

10. 如果要为 Citrix Gateway 配置 StoreFront 并希望使用智能访问，则必须键入回调 **URL**。StoreFront 会自动附加 URL 的标准部分。输入设备的内部可访问的 URL。StoreFront 连接 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。

    使用 GSLB 时，我们建议您为每个 GSLB 网关配置唯一的回调 URL。StoreFront 必须能够将每个唯一的回调 URL 解析为每个 GSLB 网关虚拟服务器配置的专用 VIP。例如，`emeagateway.domain.com`、`usgateway.domain.com` 和 `apacgateway.domain.com` 应解析为正确的网关 VIP。

11. 单击创建，将 Citrix Gateway 设备添加到远程访问设置对话框的列表中。

    有关 Citrix Gateway 设备的配置信息保存到应用商店的.cr 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。

12. 返回到本文顶部“创建新部署”过程中的步骤 10。

加入现有服务器组

June 29, 2021

StoreFront 服务器组中的服务器数量没有限制。但是，从基于模拟的容量预测来看，包含三个以上服务器的服务器组不具有优势。

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。

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：
>
> 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。

将服务器重置为出厂默认设置

December 2, 2020

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。

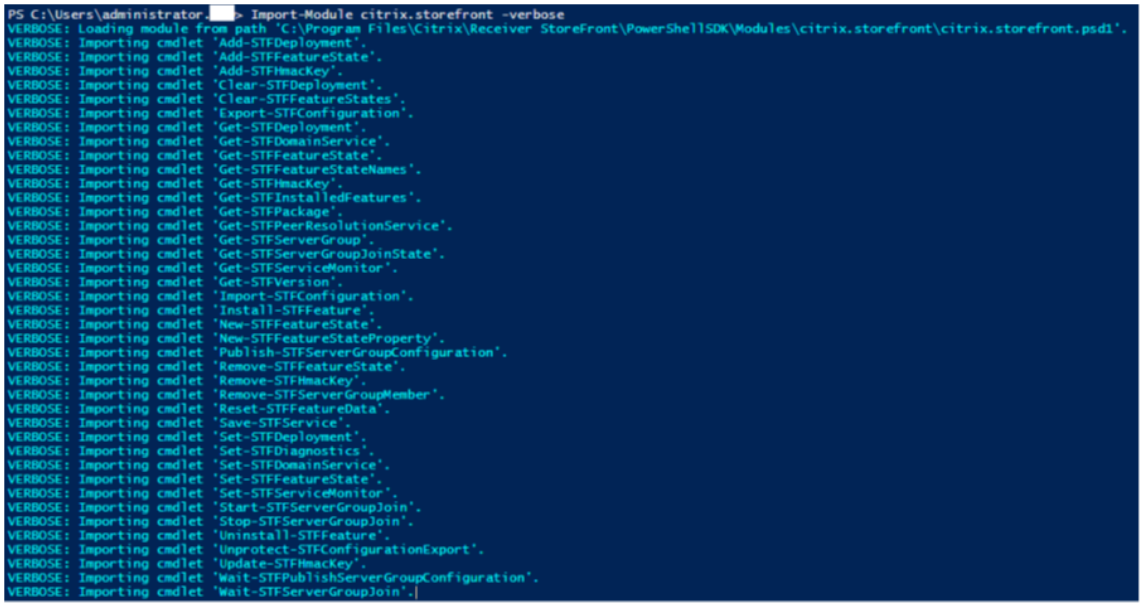
可以执行手动卸载和重新安装操作，但这更耗时，并且可能会导致其他不可预见的问题。相反，您可以运行 **Clear-STFDeployment** PowerShell cmdlet，以将 StoreFront 服务器重置为出厂默认状态。

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')
```

4. 导入 Citrix StoreFront 模块。

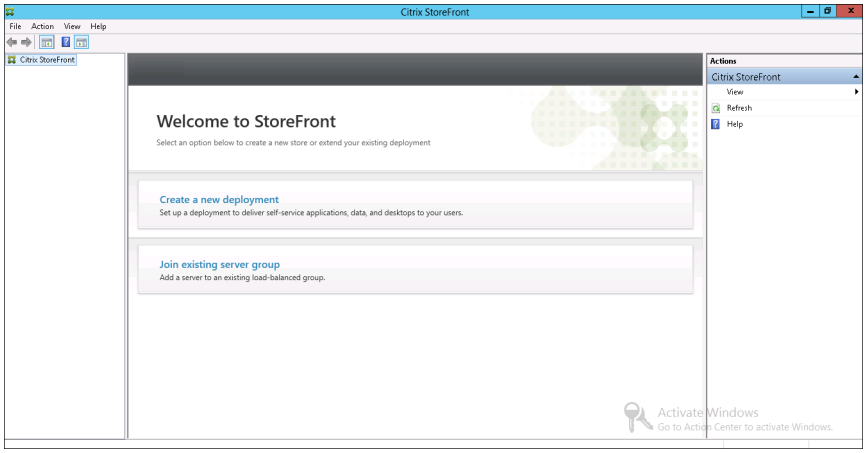
```
Import-Module citrix.storefront -verbose
```



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
```

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。



将 **Web Interface** 功能迁移至 **StoreFront**

July 27, 2020

使用 JavaScript 调整、Citrix 发布的 API 或 StoreFront 管理控制台时，许多 Web Interface 自定义设置在 StoreFront 中都具有等效设置。

此表格包含自定义概述以及如何实现这些自定义的基本信息。

文件夹位置

- 对于脚本自定义，向位于以下位置的 script.js 文件附加示例：

  C:\inetpub\wwwroot\Citrix\StoreNameWeb\custom

- 对于样式自定义，向位于以下位置的 style.css 文件附加示例：

  C:\inetpub\wwwroot\Citrix\StoreNameWeb\custom

- 对于动态内容，向位于以下位置的文本文件添加动态上下文：

  C:\inetpub\wwwroot\Citrix\StoreNameWeb\customweb

- 如果采用的是多服务器部署，可以从 StoreFront 管理控制台或通过使用 PowerShell 复制其他服务器的所有更改。

> 注意：
>
> Web Interface 允许单个用户自定义各种设置。目前，StoreFront 不具有此功能，尽管可以添加更多自定义设置以提供支持，但这不是本文讲述的重点。

Web Interface 功能	StoreFront 等效功能
使用管理控制台的自定义	
低分辨率图形布局、全分辨率图形布局、允许用户选择	不适用。StoreFront 自动检测并根据设备屏幕调整 UI。
启用搜索、禁用搜索	默认情况下启用搜索。要在桌面/**Web UI** 中禁用搜索框，请向 style.css 中添加以下样式：`.search-container { display: none; }`。要在桌面/**Web UI** 中禁用搜索框，请向 style.css 中添加以下样式：`##searchBtnPhone { display: none; }`
启用刷新	默认启用（浏览器刷新）。

Web Interface 功能	StoreFront 等效功能
启用返回上一个文件夹	默认情况下不启用。要记住当前文件夹，并在加载时返回此文件夹，请向 script.js 中添加以下内容： `CTXS.Extensions.afterDisplayHomeScreen = function (){ //check if view was saved last time CTXS.ExtensionAPI.localStorageGetItem(”view”, function (view){ if (view){ // if view was saved, change to it CTXS.ExtensionAPI.changeView(view); } if (view == ”store”){ // if view is store, see if folder was saved CTXS.ExtensionAPI.localStorageGetItem(”folder”, function(folder){ if (folder != ””){ // if folder was saved, change to it CTXS.ExtensionAPI.navigateToFolder(folder); } }); } // set up monitoring of folder CTXS.Extensions.onFolderChange = function(folder){ CTXS.ExtensionAPI.localStorageSetItem(”folder”, folder); } ; // set up monitoring of view CTXS.Extensions.onViewChange = function(newview){ // don’t retain search or appinfo views // instead, remember parent view. if ((newview != ”appinfo”)&&(newview != ”search”)){ CTXS.ExtensionAPI.localStorageSetItem(”view”, newview); } } ; }); } ;`
启用提示	由于 Citrix Workspace 应用程序面向触控和非触控设备，因此很少使用工具提示。可以通过自定义脚本添加工具提示。
图标视图、树视图、详细信息视图、列表视图、组视图、设置默认值视图、（低分辨率图形）图标视图、（低分辨率图形）列表视图、（低分辨率图形）默认值视图	Citrix Workspace 应用程序具有不同的 UI，因此这些选项不适用。可以使用 StoreFront 管理控制台配置视图。有关详细信息，请参阅为应用程序和桌面指定不同的视图。

Web Interface 功能	StoreFront 等效功能
单选项卡式 UI、选项卡式 UI，包括“应用程序”选项卡、“桌面”选项卡、“内容”选项卡、（选项卡顺序）	默认情况下，Citrix Workspace 应用程序 UI 为选项卡式，应用程序和内容位于一个选项卡内，桌面位于另一个选项卡内。同时，还有一个可选的收藏夹选项卡。
标题徽标、文本颜色、标题背景色、标题背景图像	使用 StoreFront 管理控制台可实现等效的颜色和徽标。单击 StoreFront 管理控制台的操作窗格中的 自定义 **Web** 站点外观，在显示的屏幕上进行自定义。使用样式自定义，可以设置背景图像的标题。例如 `.theme-header-bgcolor { background-image: url('spirals.png'); }`
登录前欢迎消息 (Pre-locale)（标题、文本、超链接、按钮标签）	默认情况下，没有单独的预登录屏幕。此示例脚本可添加通过单击导航的消息框： `var doneClickThrough = false; // Before web login CTXS.Extensions. beforeLogon = function (callback){ doneClickThrough = true; CTXS. ExtensionAPI.showMessage({ messageTitle: ”Welcome!”, messageText: ”Only for \<a href=” http://www.WWc.com” target=”_blank ”\>WWCo Employees”, okButtonText: ” Accept”, okAction: callback }); } ; // Before main screen (for native clients)CTXS.Extensions. beforeDisplayHomeScreen = function (callback){ if (!doneClickThrough){ CTXS.ExtensionAPI.showMessage({ messageTitle: ”Welcome!”, messageText: ”Only for WWCo Employees”, okButtonText: ”Accept”, okAction: callback }); } else { callback(); } } ;`

Web Interface 功能	StoreFront 等效功能
登录屏幕标题、登录屏幕消息、登录屏幕系统消息	登录屏幕上有四个自定义区域：屏幕的顶部和底部（标题和页脚），以及登录框本身的顶部和底部：`.customAuthHeader, .customAuthFooter .customAuthTop, .customAuthBottom { text-align: center; color: white; font-size: 16px; }` 示例脚本（静态内容）：`\$('.customAuthHeader').html("Welcome to ACME");`。示例脚本（动态内容）：`function setDynamicContent(txtFile, element){ CTXS.ExtensionAPI.proxyRequest({ url: "customweb/"+txtFile, success: function(txt){ \$(element).html(txt); } } ); } setDynamicContent("Message.txt", ".customAuthTop");`。注意：请勿在脚本中明确包含动态内容，或将其置于 **custom** 目录中，因为在此处所做的更改会强制所有客户端重新加载 UI。请将动态内容放置在 **customweb** 目录中。
应用程序屏幕欢迎消息、应用程序屏幕系统消息	请参阅上述关于 **CustomAuth** 欢迎屏幕的示例。请参阅上述关于动态内容的示例。请使用 `##customTop` 而非 `.customAuthTop` 来放置主屏幕上的内容。
页脚文本（所有屏幕）	示例脚本：`##customBottom { text-align: center; color: white; font-size: 16px; } ** Example static content using a script: **\$('\##customBottom').html("Welcome to ACME");`
没有直接等效设置的功能	
不包含标题的登录屏幕、包含标题的登录屏幕（包括消息）	StoreFront 中没有等效设置。但是，您可以创建自定义标题。请参阅上面的登录屏幕标题。
用户设置	默认情况下，没有用户设置。您可以通过 JavaScript 添加菜单和按钮。

Web Interface 功能	StoreFront 等效功能
工作区控制	管理员设置的等效功能。扩展 API 提供了其他及其重要的灵活性。请参阅 http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/receiver-customization-api.html。
深层次的自定义（代码）	
ICA 文件生成挂钩和其他调用路由自定义	等效或更好的 API。 http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-customization-sdk.html
身份验证自定义	等效或更好的 API。 http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-authentication-sdks.html
JSP/ASP 源访问	由于 UI 的呈现方式不同，因此，StoreFront 上不提供等效 API。有很多 JavaScript API 可启用 UI 自定义。

配置服务器组

June 5, 2020

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：
>
> 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**

可以通过执行更改基本 **URL** 任务修改用作部署中托管的应用商店及其他 StoreFront 服务的 URL 的根的 URL。对于多服务器部署，请指定负载平衡 URL。可以通过执行此任务随时从 HTTP 更改为 HTTPS，前提是为 HTTPS 配置了 Microsoft Internet Information Services (IIS)，并且将 HTTPS 绑定添加到默认 Web 站点。有关详细信息，请参阅保护 StoreFront 部署的安全。

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。

更改应用商店的绕行参数

> 重要：
>
> 在多服务器部署中，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。完成后，将配置更改传播到服务器组，以便更新部署中的其他服务器。

1. 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**。
3. 选择一个 Controller，单击编辑，然后单击编辑 **Delivery Controller** 屏幕上的设置。
4. 在“高级设置”中，单击设置。
5. 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）。

配置身份验证和委派

June 5, 2020

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。

方法	详细信息
配置身份验证服务	身份验证服务可对用户进行身份验证，使其能够访问 Microsoft Active Directory，从而确保用户无需重新登录即可访问自己的桌面和应用程序。
基于 XML Service 的身份验证	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 XML Service 来验证用户名和密码凭据。
适用于 XenApp 6.5 的 Kerberos 受限委派	可以通过执行配置 Kerberos 委派任务指定 StoreFront 是否使用单域 Kerberos 受限委派向 Delivery Controller 验证身份。
智能卡身份验证	为典型 StoreFront 部署中的所有组件设置智能卡身份验证。
密码过期通知时间段	如果允许 Citrix Receiver for Web 站点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。

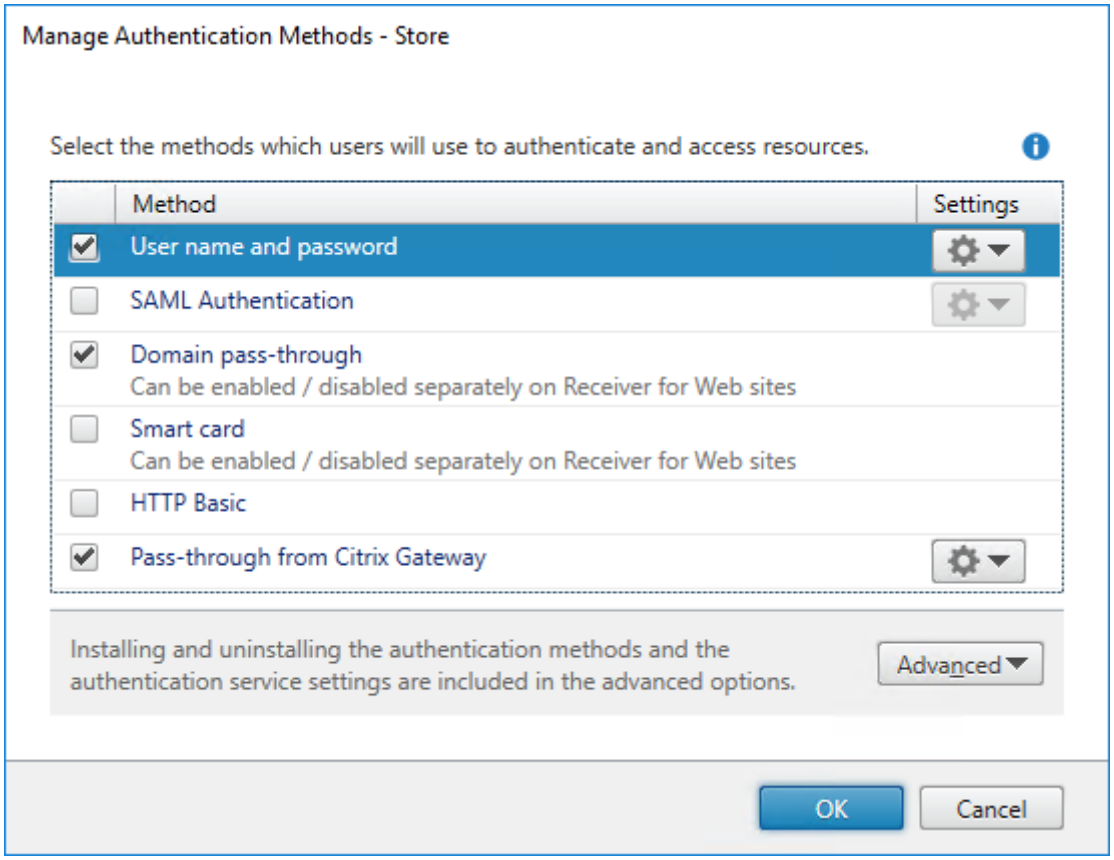
配置身份验证服务

January 27, 2021

管理身份验证方法

可以启用或禁用在创建身份验证服务时所设置的用户身份验证方法，具体操作为：在 Citrix StoreFront 管理控制台的结果窗格中选择身份验证方法，然后在操作窗格中单击 Manage Authentication Methods（管理身份验证方法）。

1. 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。
3. 指定要为用户启用的访问方法。



- 选中用户名和密码复选框可启用显式身份验证。用户在访问自己的应用商店时需要输入凭据。
- 选择 **SAML** 身份验证复选框以支持与 SAML 身份提供程序的集成。用户向身份提供程序验证身份后，即可在访问自己的应用商店时自动登录。从“设置”下拉菜单中：
  - 选择身份提供程序以配置对身份提供程序的信任。
  - 选择服务提供商以对服务提供商配置信任。身份提供程序需要此信息。
- 选中域直通以启用从用户设备直通 Active Directory 域凭据。用户向其加入域的 Windows 计算机验证身份后，即可在访问自己的应用商店时自动登录。

  要使用 Chrome 或类似的浏览器通过 Receiver for Web 站点使用域直通身份验证，必须随 WebHelper 组件一起安装 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序。默认情况下，WebHelper 随基于 Windows 的安装程序一起安装，但命令行安装需要使用 ADDLOCAL 参数进行安装。为确保用户不需要提供会话凭据，当用户设备上安装了 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序时，必须启用域直通身份验证。请参阅 适用于 Windows 的 Citrix Workspace 应用程序文档。
- 选中智能卡以启用智能卡身份验证。用户在访问应用商店时其使用智能卡和 PIN 进行身份验证。
- 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。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。

要为通过 Citrix Gateway 访问应用商店的智能卡用户启用直通身份验证，请使用“配置委派身份验证”任务。

配置可信用户域

可以通过执行“可信域”任务限制使用显式域凭据登录（直接登录或使用 Citrix Gateway 直通身份验证登录）的用户对应用商店的访问。

1. 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。
3. 在用户名和密码 **>** 设置列表中，选择配置可信域。
4. 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将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。
5. 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。
6. 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

可以通过执行管理密码选项任务来允许使用域凭据登录的 Citrix Workspace 应用程序和 Receiver for Web 站点用户更改其密码。创建身份验证服务时，默认配置会禁止 Citrix Workspace 应用程序和 Citrix Receiver for Web 站点用户更改自己的密码，即使密码已过期也是如此。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。

Citrix Workspace 应用程序和 Citrix Receiver for Web 都支持在过期时更改密码以及选择性更改密码。

使用 Citrix Workspace 应用程序或 Citrix Receiver for Web（通过 Citrix Gateway）远程访问应用商店的用户可以在密码过期时更改密码。必须启用 Citrix Gateway 选项 **Allow Password Change**（允许更改密码）（请参阅 Citrix Gateway 文档）。

如果选择了 **Allow users to change passwords**（允许用户更改密码）选项，直接访问应用商店（通过 StoreFront）的用户只能在密码过期时更改其密码，如下所示：

1. 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。
3. 在用户名和密码 **>** 设置中，选择管理密码选项。
4. 要允许用户更改其密码，请选择允许用户更改密码。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。
5. 指定使用域凭据登录的 Citrix Receiver for Web 站点用户何时可以更改其密码。
   - **Only when they expire**（仅当过期时）允许用户仅在密码已过期时更改其密码。由于密码过期而无法登录的用户将重定向到更改密码对话框。
   - **At any time**（随时），允许用户随时更改其密码。对于密码即将过期的本地用户，系统会在其登录时显示一条警告。系统只向从内部网络进行连接的用户显示密码过期警告。默认情况下，相应的 Windows 策略设置决定向用户发出通知的时间段。有关设置自定义通知时间段的详细信息，请参阅配置密码过期通知时间段。仅受 Citrix Receiver for Web 支持。

     > 注意：
     >
     > 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。

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

自助服务密码重置安全问题

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

设置自助服务密码重置时，请指定能够使用管理控制台执行密码重置和解锁帐户操作的用户。如果为 StoreFront 启用了这些功能，根据在自助服务密码重置配置控制台中配置的设置，仍可以拒绝用户执行这些任务的权限。

自助服务密码重置仅供使用 HTTPS 连接访问 StoreFront 的用户使用。这些用户不能使用 HTTP 连接访问

StoreFront，可以使用自助服务密码重置。仅当直接使用用户名和密码向 StoreFront 进行身份验证时才能使用自助服务密码重置。

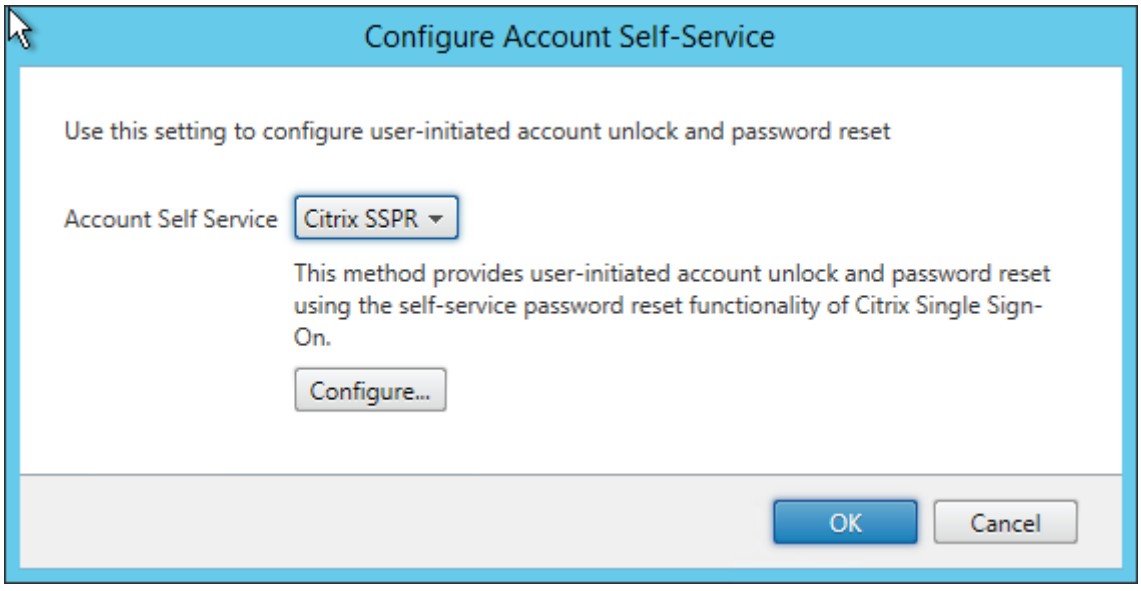
自助服务密码重置不支持 UPN 登录，例如 `username@domain.com`。

在为应用商店配置自助服务密码重置之前，必须确保：

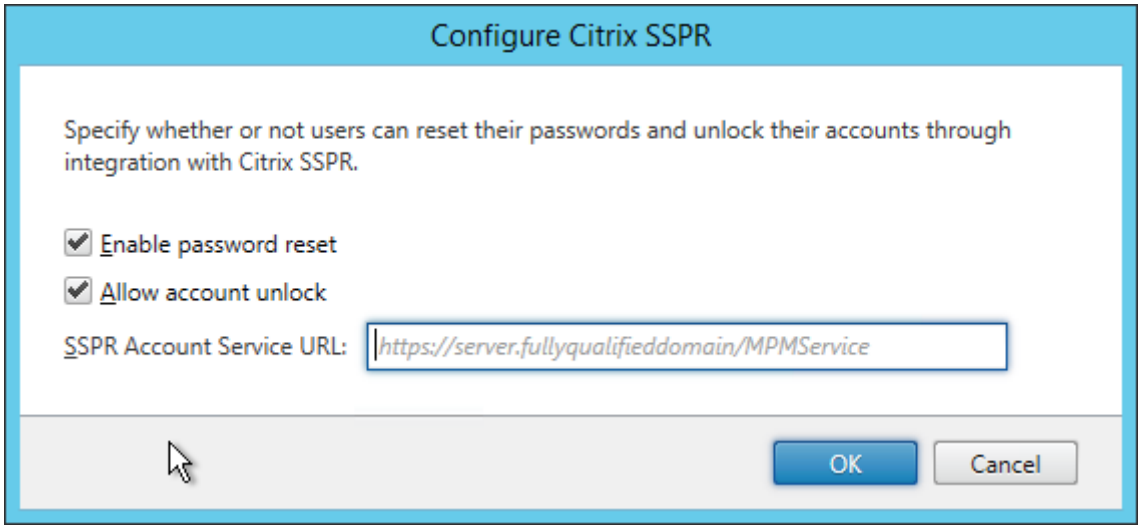
- 应用商店配置为使用用户名和密码身份验证。
- 应用商店配置为仅使用一个自助服务密码重置。如果 StoreFront 配置为使用同一域或可信域中的多个场，则必须将自助服务密码重置配置为接受来自所有这些域的凭据。
- 应用商店配置为允许用户在希望启用密码重置功能时随时更改其密码。
- 必须将 StoreFront 应用商店与 Receiver for Web 站点相关联。

必须先安装并配置自助服务密码重置才能进行使用。它在 Citrix Virtual Apps and Desktops 介质中提供。有关信息，请参阅自助服务密码重置文档。

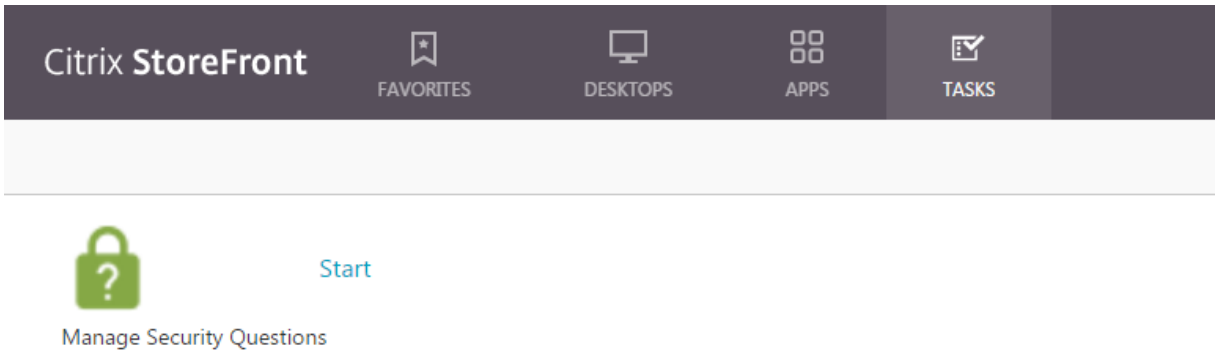
1. 通过在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点，在操作窗格中单击管理身份验证方法 **>** 用户名和密码，然后从下拉菜单中选择管理密码选项，在 StoreFront 中启用自助服务密码重置支持。
2. 选择希望用户更改密码的时间，然后单击确定。
3. 从用户名和密码下拉菜单中选择配置帐户自助服务，从下拉菜单中选择 **Citrix SSPR**，然后单击确定。
4. 指定用户是否能够通过自助服务密码重置来重置密码和解锁帐户，添加密码重置服务帐户 URL，单击确定，然后单击确定。



仅当 StoreFront 基本 URL 为 HTTPS（而非 HTTP）时此选项才可用，并且仅当您使用管理密码选项以允许用户随时更改密码之后，启用密码重置选项才可用。



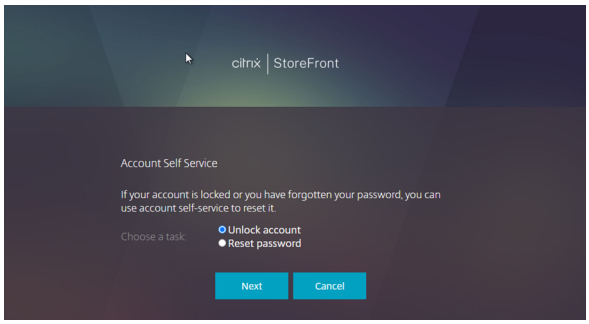
用户下次登录 Citrix Workspace 应用程序或 Citrix Receiver for Web 时，安全注册将可用。单击启动后，将显示用户必须指定回答的问题。



在 StoreFront 中配置后，Citrix Receiver for Web 登录屏幕上将显示帐户自助服务链接（在其他 Citrix Workspace 应用程序中显示为按钮）。

单击此链接会引导用户填写一系列表单，以首先选择解锁帐户或重置密码（如果两个选项均可用）。

选中一个单选按钮并单击下一步，下一个屏幕将提示您输入域和用户名（域\用户），前提是未在登录表单中输入该信息。请注意，帐户自助服务不支持 UPN 登录，例如 `username@domain.com`。



用户需要回答安全问题。如果所有答案都与用户提供的答案一致，则执行请求的操作（解锁或重置），并通知用户操作成功。

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 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。
3. 在高级下拉菜单中，选择共享身份验证服务设置。
4. 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。

将凭据验证委派给 **Citrix Gateway**

可以通过执行“配置委派身份验证”任务为通过 Citrix Gateway 访问应用商店的智能卡用户启用直通身份验证。仅当在结果窗格中启用并选择了“从 Citrix Gateway 直通”时，才能执行此项任务。

如果将凭据验证委派给 Citrix Gateway，则用户使用智能卡向 Citrix Gateway 验证身份后，即可在访问自己的应用商店时自动登录。在您启用了“从 Citrix Gateway 直通”身份验证时，此设置默认处于禁用状态，以便只有用户使用密码登录 Citrix Gateway 时才会进行直通身份验证。

基于 **XML Service** 的身份验证

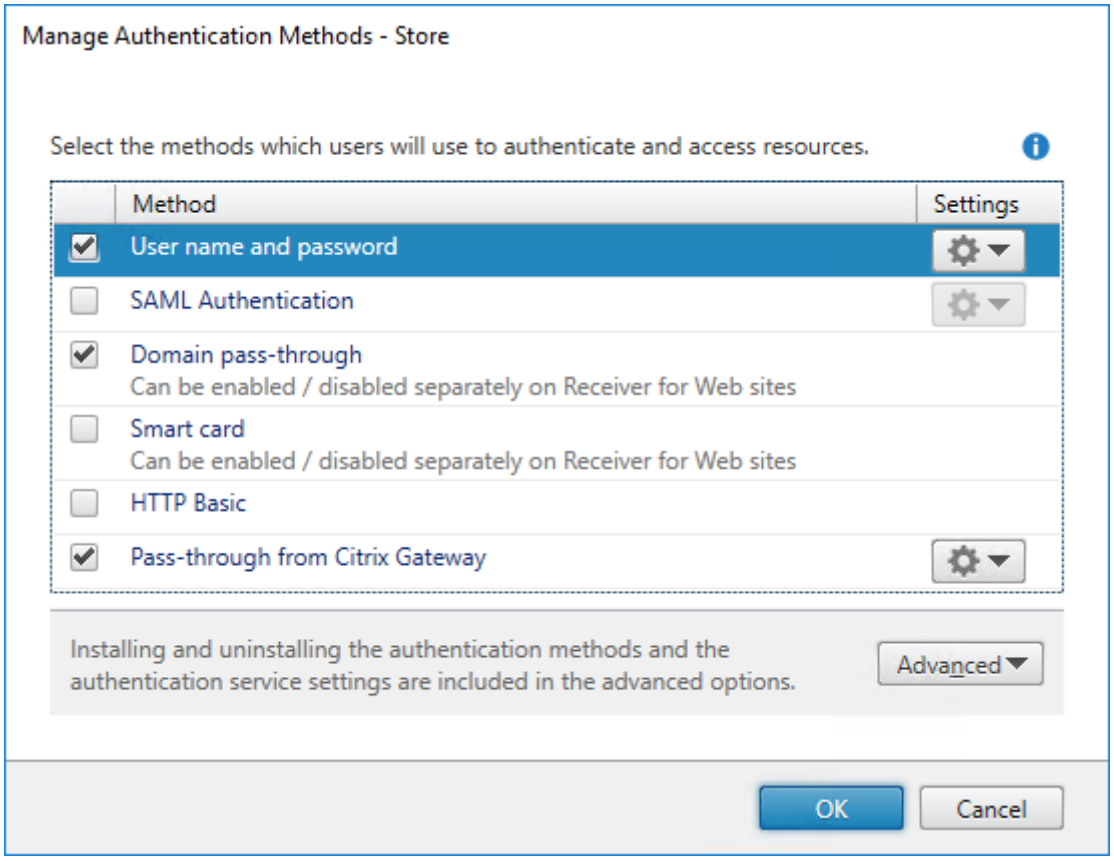
December 2, 2020

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 XML Service 来验证用户名和密码凭据。

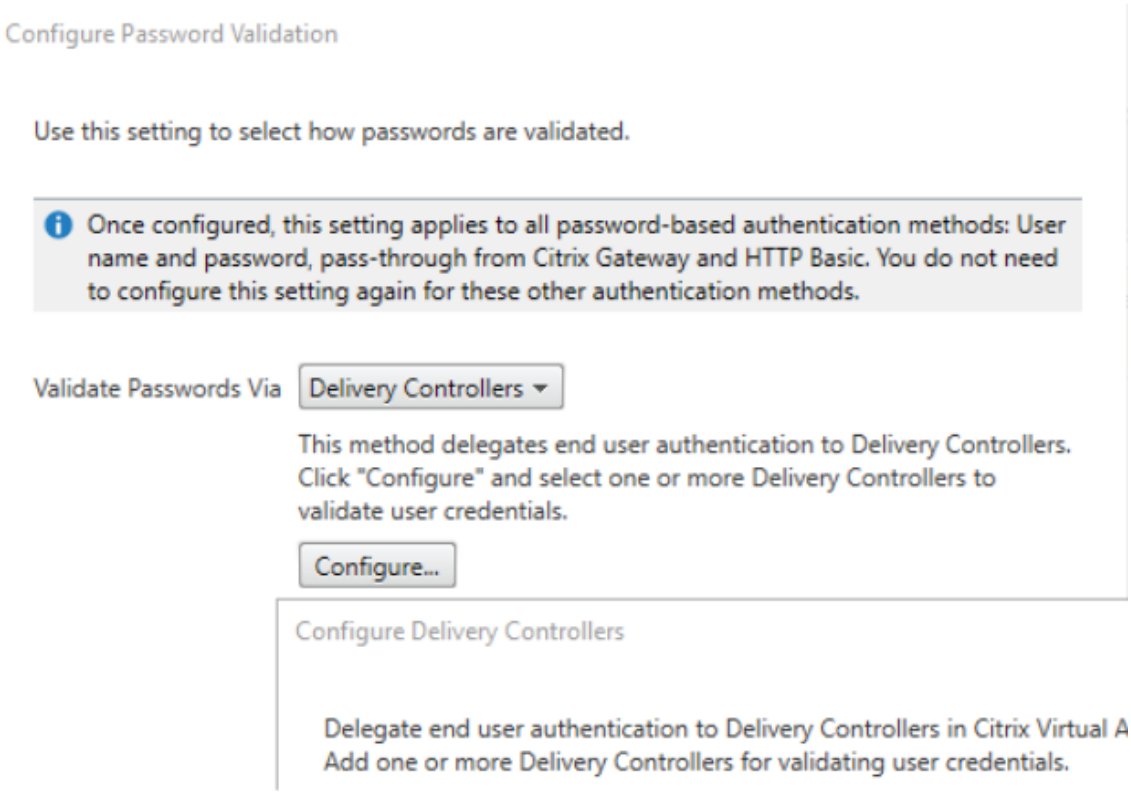
启用基于 **XML Service** 的身份验证

1. 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。

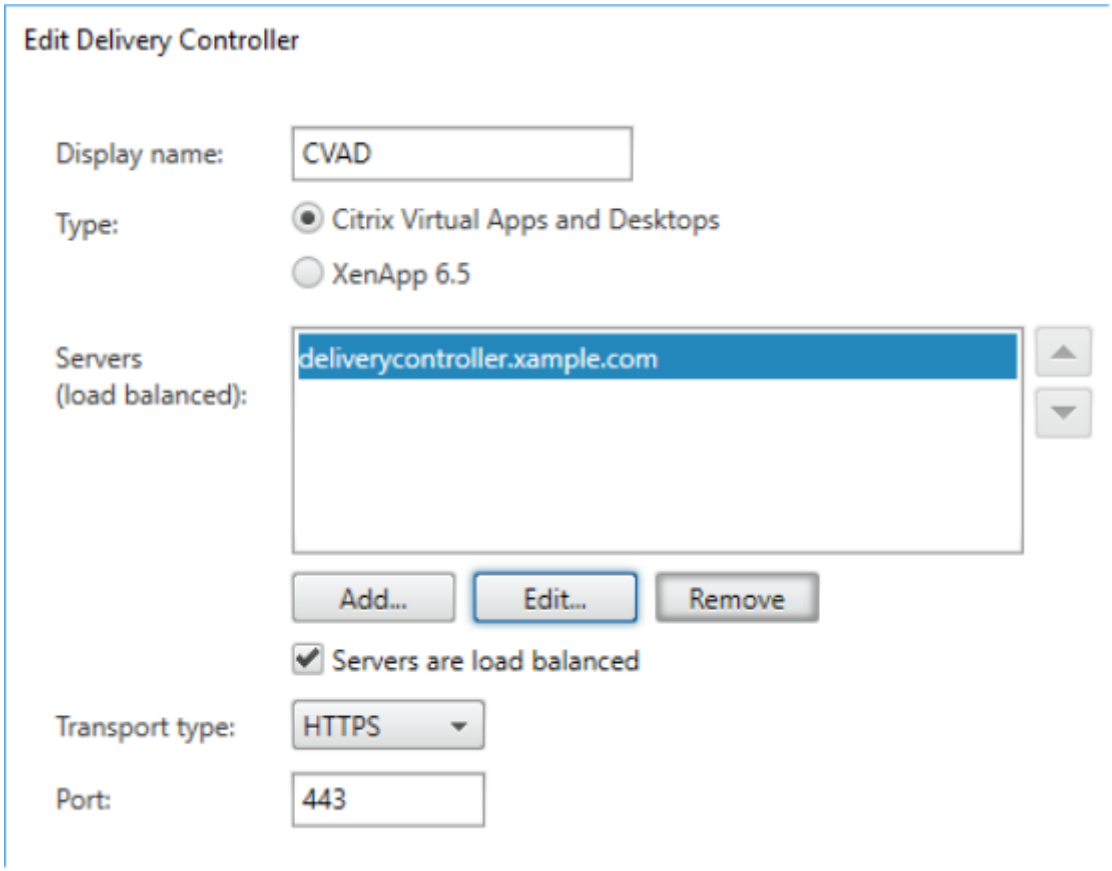
3. 在管理身份验证方法页面上，从用户名和密码 **>** 设置下拉菜单中选择配置密码验证。



4. 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）。



5. 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）。



禁用基于 **XML Service** 的身份验证

1. 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。
3. 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。
4. 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）。

为 **XenApp 6.5** 配置 **Kerberos** 约束委派

June 5, 2020

> 注意：
>
> XenApp 6.5 已达到生命周期结束 (EOL) 状态，现在已包含在扩展支持计划中。

可以通过执行配置应用商店设置 > **Kerberos** 委派任务指定 StoreFront 是否使用单域 Kerberos 约束委派向 Delivery Controller 验证身份。

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 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，然后单击“Kerberos 委派”。
3. 选择启用或禁用“使用 Kerberos 委派对 Delivery Controller 进行身份验证”，以分别启用或禁用 Kerberos 约束委派。

配置 **StoreFront** 服务器的委派

StoreFront 未与 Citrix Virtual Apps 安装在同一计算机上时，请执行以下过程。

1. 在域控制器上，打开 MMC Active Directory Users and Computers（MMC Active Directory 用户和计算机）管理单元。
2. 在视图菜单上，单击高级功能。
3. 在左侧窗格中，单击域名下方的计算机节点，然后选择 StoreFront 服务器。
4. 在操作窗格中，单击属性。
5. 在委派选项卡上，单击仅信任此计算机来委派指定的服务和使用任意身份验证协议，然后单击添加。
6. 在添加服务对话框中，单击用户或计算机。
7. 在选择用户或计算机对话框中的输入要选择的对象名称框中，键入运行 Citrix Virtual Apps and Desktops XML Service 的服务器的名称，然后单击确定。
8. 从列表中选择 HTTP 服务类型，然后单击确定。
9. 应用更改并关闭对话框。

配置 **Citrix Virtual Apps** 服务器的委派

为每个 Citrix Virtual Apps 服务器配置 Active Directory 可信委派。

1. 在域控制器上，打开 **MMC Active Directory Users and Computers**（MMC Active Directory 用户和计算机）管理单元。
2. 在左侧窗格中，单击域名下方的计算机节点，然后选择运行 StoreFront 被配置为与之通信的 Citrix Virtual Apps and Desktops XML Service 的服务器。
3. 在操作窗格中，单击属性。
4. 在委派选项卡上，单击仅信任此计算机来委派指定的服务和使用任意身份验证协议，然后单击添加。
5. 在添加服务对话框中，单击用户或计算机。
6. 在选择用户或计算机对话框中的输入要选择的对象名称框中，键入运行 Citrix Virtual Apps and Desktops XML Service 的服务器的名称，然后单击确定。
7. 从列表中选择 HOST 服务类型，单击确定，然后单击添加。
8. 在选择用户或计算机对话框中的输入要选择的对象名称框中，键入域控制器的名称，然后单击确定。
9. 从列表中选择 **cifs** 和 **ldap** 服务类型，然后单击确定。注意：如果 ldap 服务显示两个选项，请选择一个与域控制器的 FQDN 匹配的选项。

10. 应用更改并关闭对话框。

重要注意事项

决定是否使用 Kerberos 约束委派时，请考虑以下信息。

- 要点：
  - 除非在无 Kerberos 约束委派的情况下执行直通身份验证（或智能卡 PIN 直通身份验证），否则无需 ssonsvr.exe。
- StoreFront 和 Citrix Receiver for Web 域直通：
  - 客户端上无需 ssonsvr.exe。
  - 可将 Citrix icaclient.adm 模板中的 “Local username and password”（本地用户名和密码）设置为任何内容（控制 ssonsvr.exe 功能）。
  - 需要 icaclient.adm 模板 Kerberos 设置。
  - 将 StoreFront 完全限定的域名 (FQDN) 添加到 Internet Explorer 可信站点列表中。在关于可信区域的 Internet Explorer 安全设置中，选中 “使用本地用户名” 框。
  - 客户端必须位于域中。
  - 在 StoreFront 服务器上启用域直通身份验证方法，并对 Citrix Receiver for Web 启用该方法。
- StoreFront、Citrix Receiver for Web 和提示输入 PIN 的智能卡身份验证：
  - 客户端上无需 ssonsvr.exe。
  - 已配置智能卡身份验证。
  - 可将 Citrix icaclient.adm 模板中的 “Local username and password”（本地用户名和密码）设置为任何内容（控制 ssonsvr.exe 功能）。
  - 需要 icaclient.adm 模板 Kerberos 设置。
  - 在 StoreFront 服务器上启用智能卡身份验证方法，并对 Citrix Receiver for Web 启用该方法。
  - 要确保已选择智能卡身份验证，请勿在 Internet Explorer 安全设置中针对 StoreFront 站点区域选中 “使用本地用户名” 框。
  - 客户端必须位于域中。
- Citrix Gateway、StoreFront、Citrix Receiver for Web 和提示输入 PIN 的智能卡身份验证：
  - 客户端上无需 ssonsvr.exe。
  - 已配置智能卡身份验证。
  - 可将 Citrix icaclient.adm 模板中的 “Local username and password”（本地用户名和密码）设置为任何内容（控制 ssonsvr.exe 功能）。
  - 需要 icaclient.adm 模板 Kerberos 设置。
  - 在 StoreFront 服务器上启用 Citrix Gateway 直通身份验证方法，并对 Citrix Receiver for Web 启用该方法。
  - 要确保已选择智能卡身份验证，请勿在 Internet Explorer 安全设置中针对 StoreFront 站点区域选中 “使用本地用户名” 框。
  - 客户端必须位于域中。
  - 使用 StoreFront HDX 路由配置 Citrix Gateway 的智能卡身份验证和其他虚拟服务器的启动，以通过未

经身份验证的 Citrix Gateway 虚拟服务器路由 ICA 通信。

- Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序 (AuthManager)、提示输入 PIN 的智能卡身份验证和 StoreFront：
  - 客户端上无需 ssonsvr.exe。
  - 可将 Citrix icaclient.adm 模板中的 “Local username and password”（本地用户名和密码）设置为任何内容（控制 ssonsvr.exe 功能）。
  - 需要 icaclient.adm 模板 Kerberos 设置。
  - 客户端必须位于域中。
  - 在 StoreFront 服务器上启用智能卡身份验证方法。
- Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序 (AuthManager)、Kerberos 和 StoreFront：
  - 客户端上无需 ssonsvr.exe。
  - 可将 Citrix icaclient.adm 模板中的 “Local username and password”（本地用户名和密码）设置为任何内容（控制 ssonsvr.exe 功能）。
  - 需要 icaclient.adm 模板 Kerberos 设置。
  - 在关于可信区域的 Internet Explorer 安全设置中，选中 “使用本地用户名” 框。
  - 客户端必须位于域中。
  - 在 StoreFront 服务器上启用域直通身份验证方法。
  - 确保已设置以下注册表项：

    > 小心：
    > 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。

    对于 32 位计算机：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManagerProtocols\integratedwindows
    名称：SSONCheckEnabled
    类型：REG_SZ
    值：true 或 false
    对于 64 位计算机：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\AuthManagerProtocols\inte
    名称：SSONCheckEnabled
    类型：REG_SZ
    值：true 或 false

配置智能卡身份验证

December 2, 2020

本文简要介绍了在典型 StoreFront 部署中为所有组件设置智能卡身份验证所涉及的任务。有关详细信息和按步骤的配置说明，请参阅各个产品的文档。

文档为 Citrix 环境配置智能卡介绍了如何为 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。

> 注意：
>
> 在本文中，除非另行说明，否则“Citrix Workspace 应用程序”的提及也表示受支持的 Citrix Receiver 版本。

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。
- 继续操作前，请确保正确配置了公钥基础结构。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 **Citrix Gateway**

- 在 Citrix Gateway 设备上，安装证书颁发机构颁发的签名服务器证书。有关详细信息，请参阅安装和管理证书。
- 在 Citrix Gateway 设备上，安装发布您的智能卡用户证书的证书颁发机构的根证书。有关详细信息，请参阅在 Citrix Gateway 上安装根证书。
- 为进行客户端证书身份验证创建并配置虚拟服务器。创建证书身份验证策略，指定 SubjectAltName:PrincipalName 以从证书提取用户名称。然后，将该策略绑定到虚拟服务器并配置虚拟服务器来请求客户端证书。有关详细信息，请参阅配置和绑定客户端证书身份验证策略。
- 将证书颁发机构根证书绑定到虚拟服务器。有关详细信息，请参阅将根证书添加到虚拟服务器。
- 为确保用户在已经与其资源建立连接的情况下不会再额外收到虚拟服务器要求提供凭据的提示，应创建第二个虚拟服务器。创建虚拟服务器时，请在安全套接字层 (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。

  此外，还必须将 StoreFront 配置为通过此额外的虚拟服务器将用户连接路由到相应资源。用户登录到第一个虚拟服务器，第二个虚拟服务器用于连接到用户资源。如果已经建立连接，用户无需向 Citrix Gateway 验证身份，但需要输入其 PIN 以登录其桌面和应用程序。除非您计划允许用户在遇到任何智能卡问题时回退至显式身份验证，否则可以自由选择是否配置第二个虚拟服务器来将用户连接路由到资源。
- 创建用于从 Citrix Gateway 连接到 StoreFront 的会话策略和配置文件，并将这些策略和文件绑定到相应的虚拟服务器。有关详细信息，请参阅通过 Citrix Gateway 访问 StoreFront。
- 如果将用于 StoreFront 连接的虚拟服务器配置为要求对所有通信进行客户端证书身份验证，则必须创建另一个虚拟服务器，用以为 StoreFront 提供回调 URL。此虚拟服务器仅由 StoreFront 使用，用以验证来自 Citrix

Gateway 设备的请求，因此该服务器无需供公众访问。强制进行客户端证书身份验证时，需要单独的虚拟服务器，因为 StoreFront 无法提供证书来进行身份验证。有关详细信息，请参阅创建虚拟服务器。

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。通过在 Microsoft Internet Information Services (IIS) 中获取 SSL 证书，然后将 HTTPS 绑定添加到默认 Web 站点，为 HTTPS 配置 Microsoft Internet Information Services (IIS)。有关在 IIS 中创建服务器证书的详细信息，请参阅https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831637(v=ws.11)#create-certificate-wizard。有关将 HTTPS 绑定添加到 IIS 站点的详细信息，请参阅https://docs.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/hh831632(v=ws.11)。
- 如果您要要求所有 StoreFront URL 的 HTTPS 连接都必须提供客户端证书，请在 StoreFront 服务器上配置 IIS。

  安装 StoreFront 时，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。采用此配置，智能卡用户才可以选择回退至显式身份验证，并且可以根据相应的 Windows 策略设置，允许用户删除其智能卡，而不需要重新进行身份验证。

  如果 IIS 配置为针对所有 StoreFront URL 的 HTTPS 连接均要求提供客户端证书，则智能卡用户无法通过 Citrix Gateway 进行连接，并且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。要启用此 IIS 站点配置，身份验证服务和应用商店必须位于同一服务器上，并且必须使用对所有应用商店都有效的客户端证书。此外，在此配置中，IIS 需要客户端证书才能通过 HTTPS 连接到所有 StoreFront URL；这一配置将与 Citrix Receiver for Web 客户端的身份验证相冲突。因此，应在不需要执行 Citrix Receiver for Web 客户端访问时使用此配置。
- 安装并配置 StoreFront。根据需要创建身份验证服务并添加应用商店。如果配置通过 Citrix Gateway 进行远程访问，请勿启用虚拟专用网络 (VPN) 集成。有关详细信息，请参阅安装和设置 StoreFront。
- 为内部网络中的本地用户启用针对 StoreFront 的智能卡身份验证。为通过 Citrix Gateway 访问应用商店的智能卡用户，启用 Citrix Gateway 直通身份验证方法，并确保 StoreFront 配置为将凭据验证委派给 Citrix Gateway。如果在加入域的用户设备上安装 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序时计划启用直通身份验证，请启用域直通身份验证。有关详细信息，请参阅配置身份验证服务。

  要允许通过智能卡进行 Citrix Receiver for Web 客户端身份验证，必须为每个 Citrix Receiver for Web 站点启用该身份验证方法。有关详细信息，请参阅配置 Citrix Receiver for Web 站点说明。

  如果希望智能卡用户在智能卡出现问题时能够回退到显式身份验证，请不要禁用用户名和密码身份验证方法。
- 如果计划在已加入域的用户设备上安装 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序时启用直通身份验证，请编辑应用商店的 default.ica 文件，以在用户访问其桌面和应用程序时启用用户智能卡凭据直通功能。有关详细信息，请参阅为 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序启用智能卡直通身份验证。

- 如果创建了仅用于将用户连接路由到资源的另一台 Citrix Gateway 虚拟服务器，对于向应用商店提供桌面和应用程序的部署，应配置通过此虚拟服务器对其连接进行最佳的 Citrix Gateway 路由。有关详细信息，请参阅为应用商店配置最佳 HDX 路由。
- 要使使用运行 Citrix Desktop Lock 的 PC 的用户能够使用智能卡进行身份验证，请为 XenApp Services URL 启用智能卡直通身份验证。有关详细信息，请参阅配置 XenApp Services URL 的身份验证。

配置用户设备

- 确保在所有用户设备上安装供应商的智能卡中间件。
- 对于使用重用 PC 的用户，请使用具有管理员权限的帐户安装 Receiver for Windows Enterprise。为相应应用商店配置具有 XenApp Services URL 的 Receiver for Windows。在确认可以通过智能卡登录到设备并且可以访问应用商店中的资源后，请安装 Citrix Desktop Lock。有关详细信息，请参阅安装 Desktop Lock。
- 对于所有其他用户，在用户设备上安装相应版本的 Citrix Workspace 应用程序。要为具有已加入域的设备的用户启用 Citrix Virtual Apps and Desktops 智能卡凭据直通，请使用具有管理员权限的帐户从命令提示窗口中使用 **/includeSSON** 选项安装适用于 Windows 的 Citrix Workspace 应用程序。有关详细信息，请参阅使用命令行参数。

  确保通过域策略或本地计算机策略针对智能卡身份验证配置适用于 Windows 的 Citrix Workspace 应用程序。对于域策略，请使用组策略管理控制台为您的用户帐户所属的域将适用于 Windows 的 Citrix Workspace 应用程序组策略对象模板文件 icaclient.adm 导入到域控制器中。要配置单个设备，请使用该设备上的组策略对象编辑器来配置模板。有关详细信息，请参阅智能卡。

  启用智能卡身份验证策略。要启用用户智能卡凭据直通身份验证，请选择对 PIN 使用直通身份验证。然后，要将用户智能卡凭据直通传递到 Citrix Virtual Apps and Desktops，请启用本地用户名和密码策略并选择允许对所有 ICA 连接进行直通身份验证。有关详细信息，请参阅ICA 设置参考。

  对于使用加入域的设备的用户，如果允许智能卡凭据直通传递到 Citrix Virtual Apps and Desktops，请将应用商店 URL 添加到 Internet Explorer 的 “本地 Intranet” 或 “可信站点” 区域。请确保在该区域的安全设置中选择使用当前用户名和密码自动登录。
- 如有必要，应使用适当的方式为用户提供应用商店（对于内部网络中的用户）或 Citrix Gateway 设备（对于远程用户）的详细连接信息。有关将配置信息提供给用户的详细信息，请参阅 ICA 设置参考。

为 **Receiver for Windows** 或适用于 **Windows** 的 **Citrix Workspace** 应用程序启用智能卡直通身份验证

在加入域的用户设备上安装 Receiver for Windows 时，可以启用直通身份验证。要在用户访问 Citrix Virtual Apps and Desktops 托管的桌面和应用程序时启用智能卡凭据直通功能，可以编辑应用商店的 default.ica 文件。

> 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，
> 将配置更改传播到服务器组，以便更新部署中的其他服务器。

1. 使用文本编辑器打开应用商店的 default.ica 文件，该文件通常位于 C:\inetpub\wwwroot\Citrix\storename\App_Data\ 目录中，其中 storename 为创建应用商店时为其指定的名称。
2. 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 [应用程序] 部分添加以下设置。

   ```
   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。
3. 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 [应用程序] 部分添加以下设置。

   ```
   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。

配置密码过期通知时间段

April 12, 2021

> 重要：
>
> 在多服务器部署中，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。完成后，执行将配置更改传播到服务器组操作，以便更新部署中的其他服务器。

如果您允许 Citrix Receiver for Web 站点用户随时更改其密码（如管理身份验证方法中所述），则可以配置是否在本地用户登录时提醒其密码即将过期。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。

要为所有用户设置自定义通知时段，可以编辑身份验证服务的 web.config 文件。

- 对于默认应用商店，请编辑 `C:\inetpub\wwwroot\Citrix\Authentication\web.config`
- 对于自定义应用商店，请编辑 `C:\inetpub\wwwroot\Citrix\customAuth\web.config`

1. 搜索以下显式配置：

```
1 <explicitBL authenticator="defaultDelegatedAuthenticator"
     requireAccountSIDs="true"
2   hideDomainField="true" allowUserPasswordChange="Never"
       showPasswordExpiryWarning="Windows"
3   passwordExpiryWarningPeriod="10" explicitJsonEnabled="true"
4   allowZeroLengthPassword="false">
```



```
    <domainSelection default="">
      <clear />
    </domainSelection>
    <accountPolicy allowUnlockAccount="false" allowResetPassword="
        false" />
</explicitBL>
```

2. 要禁用密码到期通知，请使用 showPasswordExpiryWarning="Never"。
3. 要设置自定义通知时段（例如，密码到期前 10 天），请使用 showPasswordExpiryWarning="Custom" 和 passwordExpiryWarningPeriod="10"。

> 注意：
>
> StoreFront 不支持 Active Directory 中的细化密码策略。

配置和管理应用商店

June 5, 2020

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
创建或删除应用商店	可以根据需要配置多个其他应用商店。
创建未经身份验证的应用商店	配置其他未经身份验证的应用商店以支持未经身份验证（匿名）的用户进行访问。
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。
向用户隐藏和公告应用商店	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。
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。
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。
高级应用商店设置	配置高级应用商店设置。

创建或删除应用商店

June 29, 2021

可以通过执行创建应用商店任务配置额外的应用商店。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。

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）。

在“应用商店名称”页面上，选择仅允许未经身份验证的用户访问此应用商店允许您创建未经身份验证的应用商店，这是匿名或未经身份验证的应用商店。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。）

> 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，
> 将配置更改传播到服务器组，以便更新部署中的其他服务器。

向应用商店添加桌面和应用程序

1. 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 管理控制台的左侧窗格中选择应用商店节点，然后在操作窗格中单击创建应用商店。
3. 在应用商店名称页面上，指定应用商店的名称，然后单击下一步。

   此时应用商店名称将显示在 Citrix Workspace 应用程序中的用户帐户下方，请选择一个向用户描述应用商店内容信息的名称。
4. 在 **Delivery Controller** 页面上，列出用于提供希望通过该应用商店获得的资源的基础结构。单击添加。
5. 在“添加 Delivery Controller”对话框中，指定一个有助于识别部署的显示名称。指定类型以指示如何提供应用商店中提供的资源。“类型”默认设置为“Citrix Virtual Apps and Desktops”。XenApp 6.5 作为一种类型提供，但它已于 2018 年 6 月达到生命周期已结束状态，现在已包含在扩展支持计划中。
6. 要通过应用商店获取由 Citrix Virtual Apps and Desktops 和 XenApp 6.5 提供的桌面和应用程序，请在服务器列表中添加服务器的名称或 IP 地址。指定多台服务器以启用容错功能，并按优先级顺序列出这些条目以设置故障转移顺序。对于 Citrix Virtual Apps and Desktops 站点，请提供 Delivery Controller 的详细信息。对于 XenApp 6.5 场，列出运行 Citrix XML Service 的服务器。
7. 从传输类型列表中选择要用来与服务器通信的 StoreFront 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。

- 要通过使用传输层安全性 (TLS) 的安全 HTTP 连接发送数据，请选择 **HTTPS**。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。
- 要通过与 XenApp 6.5 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**。

  > 注意：
  >
  > 如果使用 HTTPS 或 SSL Relay 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）。

8. 指定 StoreFront 连接服务器所用的端口。使用 HTTP 和 SSL Relay 的连接的默认端口为 80，HTTPS 连接的默认端口为 443。对于 Citrix Virtual Apps and Desktops 服务器，指定的端口必须是 Citrix XML Service 所使用的端口。
9. 如果要使用 SSL Relay 确保 StoreFront 与 XenApp 6.5 服务器之间的连接安全，请在 **SSL Relay** 端口中指定 SSL Relay 的 TCP 端口。默认端口为 443。确保将运行 SSL Relay 的所有服务器配置为监视同一端口。
10. 单击确定。可以将应用商店配置为提供任何 Citrix Virtual Apps and Desktops 部署组合中的资源。根据需要重复步骤 4 至 10，以列出为该应用商店提供资源的其他部署。将所有必需的资源添加到该应用商店中之后，单击下一步。
11. 在远程访问页面上，指定从公用网络连接的用户是否以及如何能够通过 Citrix Gateway 访问该应用商店。

    - 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。
      - 要使仅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。
12. 如果已启用远程访问，请在 **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，请指定用于访问该应用商店的默认设备。要向列表中添加其他设备，请按照通过 Citrix Gateway 提供对应用商店的远程访问中介绍的过程进行操作。
13. 在身份验证方法页面上，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。您可以从以下方法中进行选择：

    - 用户名和密码：用户在访问其应用商店时将输入其凭据并进行身份验证。
    - **SAML** 身份验证：用户向身份提供程序验证身份后，即可在访问应用商店时自动登录。

- 域直通 †：用户向其加入域的 Windows 计算机验证身份，即可在访问应用商店时使用其凭据自动登录。
- 智能卡 †：用户在访问应用商店时使用智能卡和 PIN 进行身份验证。
- **HTTP Basic**：用户将向 StoreFront 服务器的 IIS Web 服务器进行身份验证。
- 通过 **Citrix Gateway** 直通：用户向 Citrix Gateway 验证身份后，即可在访问应用商店时自动登录。启用了远程访问时自动选中此方法。

> 注意：
>
> † 不会传播到应用商店的 Citrix Receiver for Web 站点的应用商店身份验证方法。使用配置 Citrix Receiver for Web 站点中所述的管理 **Receiver for Web** 站点任务为每个 Citrix Receiver for Web 站点独立配置这些身份验证方法。
>
> 本文中介绍的其他应用商店身份验证方法确实会传播到应用商店的 Citrix Receiver for Web 站点。（也就是说，在本文中为应用商店进行的选择或取消选择决定了其所有 Receiver for Web 站点使用的设置。）

14. 在配置密码验证页面上，选择 Delivery Controller 以提供密码验证，然后单击下一步。
15. 在 **XenApp Services URL** 页面上，为使用 PNAgent 访问应用程序和桌面的用户配置该 URL，然后单击创建。
16. 创建了应用商店时，单击完成。

访问应用商店

现在，用户可以使用 Citrix Workspace 应用程序来访问您的应用商店，但必须为其配置该应用商店的访问详细信息。您可以通过许多方式为用户提供这些详细信息，以简化用户的配置过程。有关详细信息，请参阅用户访问选项。

或者，用户可以通过 Receiver for Web 站点访问应用商店，这使用户能够通过 Web 页面访问其桌面和应用程序。创建应用商店时，将会显示用户用于访问新应用商店的 Receiver for Web 站点的 URL。

创建新应用商店时，将默认启用 XenApp Services URL。使用运行 Citrix Desktop Lock 的 PC 的用户，以及使用无法升级的旧版 Citrix 客户端的用户，可以使用应用商店的 XenApp Services URL 直接访问应用商店。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 FQDN；**storename** 为在步骤 3 中指定的应用商店名称。

通过 **Citrix Gateway** 提供对应用商店的远程访问

要配置通过 Citrix Gateway 对先前过程中创建的应用商店进行远程访问，请完成以下步骤。假设您已经完成所有前面的步骤。

1. 在创建应用商店向导的远程访问页面中，单击添加。
2. 在添加 **Citrix Gateway** 设备对话框中的常规设置页面上，为 Citrix Gateway 设备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网关。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或者最靠近其所在位置的网关。

3. 对于 **Citrix Gateway URL**，请键入用于您的部署的 Citrix Gateway 虚拟服务器的“URL: 端口”组合。如果未指定端口，则使用默认 `https://` 端口 443。没有必要在 URL 中指定端口 443。

   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。

4. 从可用选项中选择 Citrix Gateway 的用法或角色。

   - 身份验证和 **HDX** 路由： Citrix Gateway 将用于进行身份验证以及路由任何 HDX 会话。
   - 仅限身份验证： Citrix Gateway 将用于身份验证，不用于任何 HDX 会话路由。
   - 仅限 **HDX** 路由： Citrix Gateway 将用于 HDX 会话路由，不用于身份验证。

5. 对于要使由 Citrix Virtual Apps and Desktops 或 XenApp 6.5 提供的资源在应用商店中可用的所有部署，请在 **Secure Ticket Authority** 页面上列出运行 STA 的服务器的 Secure Ticket Authority (STA) URL。添加多个 STA 的 URL 以启用容错功能，并按优先级顺序列出这些服务器以设置故障转移顺序。

   STA 托管在 Citrix Virtual Apps and Desktops 或 XenApp 6.5 服务器上，并发出会话票据以响应连接请求。这些会话票据构成了对访问 Citrix Virtual Apps and Desktops 或 XenApp 6.5 资源进行身份验证和授权的基础。使用正确的 STA URL（例如 `HTTPS://` 或`HTTP://`），具体取决于 Delivery Controller 的配置方式。STA URL 还必须与在虚拟服务器上的 Citrix Gateway 中配置的 URL 相同。

6. 选择设置要进行负载平衡的 Secure Ticket Authority。还可以指定时间间隔，超过此间隔后，将绕过未响应的 STA。

7. 要确保 Citrix Virtual Apps and Desktops 或 XenApp 6.5 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，请选择启用会话可靠性。

8. 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。StoreFront 将从两个不同的 STA 获取会话票据，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。

9. 在身份验证设置页面上，键入 Citrix Gateway 设备的虚拟服务器 **IP** 地址 (VIP)。

   使用 Citrix Gateway 虚拟服务器的专用 IP 地址，而非通过网络地址转换功能转换为专用 IP 地址的公用 IP 地址。网关通常由 StoreFront 通过其 URL 进行识别。如果使用全局服务器负载平衡 (GSLB)，则必须将 VIP 添加到每个网关中。这允许 StoreFront 识别多个网关，这些网关都使用相同的 URL（GSLB 域名）作为不同的网关。例如，可以为使用相同 URL 的应用商店配置三个网关（例如 `https://gslb.domain.com`），但每个网关都配置了唯一的 VIP，例如 10.0.0.1、10.0.0.2 和 10.0.0.3。

10. 如果要添加运行 Citrix Gateway 的设备，请从登录类型列表中选择您在设备上为 Citrix Workspace 应用程序用户配置的身份验证方法。

    - 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。

11. 如果要为 Citrix Gateway 配置 StoreFront 并希望使用智能访问，则必须键入回调 **URL**。StoreFront 会自动附加 URL 的标准部分。输入设备的内部可访问的 URL。StoreFront 连接 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。

    使用 GSLB 时，我们建议您为每个 GSLB 网关配置唯一的回调 URL。StoreFront 必须能够将每个唯一的回调 URL 解析为每个 GSLB 网关虚拟服务器配置的专用 VIP。例如，`emeagateway.domain.com`、`usgateway.domain.com` 和 `apacgateway.domain.com` 应解析为正确的网关 VIP。

12. 单击创建，将 Citrix Gateway 设备添加到远程访问设置对话框的列表中。

    有关 Citrix Gateway 设备的配置信息保存到应用商店的.cr 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。

删除应用商店

可以通过执行“删除应用商店”任务删除应用商店。删除应用商店时，还将删除任何关联的 Receiver for Web 站点和 XenApp Services URL。

> 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，执行将配置更改传播到服务器组操作，以便更新部署中的其他服务器。

创建未经身份验证的应用商店

June 5, 2020

可以通过执行“创建应用商店”任务配置其他未经身份验证的应用商店，以支持未经身份验证（匿名）的用户进行访问。可以根据需要创建任意数量的未经身份验证的应用商店；例如，可以为特定用户组创建未经身份验证的应用商店，或者将一组特定资源编入一组。

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。

要创建未经身份验证的应用商店，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。

> 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，

> 将配置更改传播到服务器组，以便更新部署中的其他服务器。

向应用商店添加桌面和应用程序

1. 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 管理控制台的左侧窗格中选择“应用商店”节点，然后在“操作”窗格中单击创建应用商店。
3. 在“应用商店名称”页面上，指定应用商店的名称，选择仅允许未经身份验证的 **(**匿名**)** 用户访问此应用商店，然后单击下一步。

   此时应用商店名称将显示在 Citrix Receiver 应用程序中的用户帐户下方，请选择一个向用户描述应用商店内容信息的名称。
4. 在 **Delivery Controller** 页面上，列出用于提供希望通过该应用商店获得的资源的基础结构。单击添加。
5. 在添加 **Delivery Controller** 对话框中，指定一个有助于识别部署的名称，并指示希望通过该应用商店获得的资源是否由 Citrix Virtual Apps and Desktops 提供，还是由 XenApp 6.5 提供。（请注意，XenApp 6.5 已达到生命周期结束 (EOL) 状态，现在已包含在扩展支持计划中。）分配 Delivery Controller 时，请务必仅使用支持匿名应用程序功能的 Delivery Controller。如果所配置的未经身份验证的应用商店使用不支持此功能的 Controller，可能会导致该应用商店中不提供任何匿名应用程序。

   要使 XenApp 6.5 场提供的桌面和应用程序在应用商店中可用，请将场中每个服务器的名称添加到“服务器”列表中。指定多台服务器以启用容错功能，并按优先级顺序列出这些条目以设置故障转移顺序。对于 Citrix Virtual Desktops 站点，请提供 Controller 的详细信息。对于 XenApp 6.5 场，列出运行 Citrix XML Service 的服务器。
6. 从传输类型列表中选择要用来与服务器通信的 StoreFront 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**。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。使用 HTTP 连接的默认端口为 80，使用 HTTPS 连接的默认端口为 443。对于 Citrix Virtual Apps and Desktops 服务器，指定的端口必须是 Citrix XML Service 所使用的端口。
8. 单击确定。可以将应用商店配置为提供任何 Citrix Virtual Apps and Desktops 部署组合中的资源。根据需要重复步骤 4 至 9，以列出为该应用商店提供资源的其他部署。将所有必需的资源添加到该应用商店中之后，单击创建。

您的未经身份验证的应用商店现在可供使用。要允许用户访问新应用商店，必须使用该应用商店的访问详细信息对 Citrix Workspace 应用程序进行配置。您可以通过许多方式为用户提供这些详细信息，以简化用户的配置过程。有关详细信息，请参阅
用户访问选项。

或者，用户可以通过 Receiver for Web 站点访问应用商店，这使用户能够通过 Web 页面访问其桌面和应用程序。默认情况下，使用未经身份验证的应用商店时，Citrix Receiver for Web 以包含痕迹路径的文件夹层次结构显示应用程序。创建应用商店时，将会显示用户用于访问新应用商店的 Receiver for Web 站点的 URL。

创建新应用商店时，将默认启用 XenApp Services URL。使用运行 Citrix Desktop Lock 的已加入域的桌面设备和重用 PC 的用户，以及使用无法升级的旧版 Citrix 客户端的用户，可以使用应用商店的 XenApp Services URL 直接访问应用商店。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 FQDN；storename 为在步骤 3 中指定的应用商店名称。

> 注意：
>
> 在 StoreFront 配置中，如果 *web.config* 文件已配置了参数 **LogoffAction="terminate"**，访问此未经身份验证的应用商店的 Citrix Receiver for Web 会话将不终止。通常可以在 `C:\inetpub\wwwroot\Citrix\storename\` 下找到 web.config 文件，其中 **storename** 为创建应用商店时为其指定的名称。为确保这些会话正确终止，此应用商店正在使用的 XenApp 服务器必须启用信任 XML 请求选项，如配置 Citrix XML Service 端口和信任中所示。

为用户导出应用商店预配文件

July 27, 2020

可以通过执行导出多应用商店预配文件和导出预配文件任务生成包含应用商店的连接详细信息的文件，包括为应用商店配置的任何 Citrix Gateway 部署和信标。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。用户还可以从 Receiver for Web 站点获取 Citrix Workspace 应用程序预配文件。

> 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，
> 将配置更改传播到服务器组，以便更新部署中的其他服务器。

1. 在 Windows 开始屏幕或应用程序屏幕中，找到并单击 Citrix StoreFront 磁贴。在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点。
2. 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。
3. 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

June 5, 2020

可以通过执行“隐藏应用商店”任务在用户将 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。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。要恢复对隐藏应用商店的公告，请执行“公告应用商店”任务。

> 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，
> 将配置更改传播到服务器组，以便更新部署中的其他服务器。

1. 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。
3. 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。

管理通过应用商店提供的资源

June 5, 2020

可以通过管理 **Delivery Controller** 任务来添加和删除 Citrix Virtual Apps and Desktops 所提供的应用商店资源，以及修改提供这些资源的服务器的详细信息。

> 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，
> 将配置更改传播到服务器组，以便更新部署中的其他服务器。

1. 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 **Delivery Controller**。
3. 在“管理 Delivery Controller”对话框中：
   a) 单击添加以包括应用商店中其他 Citrix Virtual Apps and Desktops 部署中的桌面和应用程序。
   b) 单击编辑以修改部署的设置。
   c) 要停止通过应用商店获得由部署提供的资源，请从 Delivery controller 列表中选择一个条目，然后单击删除。
4. 在“添加 Controller”或“编辑 Controller”对话框中，指定一个有助于识别部署的显示名称。

5. 要通过应用商店获得由 Citrix Virtual Apps and Desktops 提供的桌面和应用程序，请单击添加以输入服务器的名称或 IP 地址。指定多台服务器可实现负载平衡或故障转移，具体取决于 web.config 文件的配置方式（如对话框中所示）。默认配置负载平衡。如果配置了故障转移，请按优先级顺序列出条目以设置故障转移顺序。对于 Citrix Virtual Desktops 站点，请提供 Delivery Controller 的详细信息。对于 Citrix Virtual Apps 场，请列出运行 Citrix XML Service 的服务器。要修改服务器的名称或 IP 地址，请在“服务器”列表中选择该条目，然后单击编辑。选择列表中的一个条目并单击删除，可以停止 StoreFront 与服务器通信以枚举用户的可用资源。
6. 我们建议您选择服务器已实现负载平衡选项，以确保负载在 Citrix Virtual Apps and Desktops 站点内的所有 Delivery Controller 之间分发。StoreFront 在每次启动期间从“服务器”列表中随机选择 Delivery Controller，并在 Citrix Virtual Apps and Desktops 站点中的所有服务器之间分发负载。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 Delivery Controller 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。
7. 从传输类型列表中选择要用来与服务器通信的 StoreFront 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**。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。
   - 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**。

     > 注意：
     > 如果使用 HTTPS 或 SSL Relay 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）。
8. 指定 StoreFront 连接服务器所用的端口。使用 HTTP 和 SSL Relay 的连接的默认端口为 80，HTTPS 连接的默认端口为 443。对于 Citrix Virtual Apps and Desktops 服务器，指定的端口必须是 Citrix XML Service 所使用的端口。
9. 如果要使用 SSL Relay 确保 StoreFront 与 Citrix Virtual Apps 服务器之间的连接安全，请在 SSL Relay 端口框中指定 SSL Relay 的 TCP 端口。默认端口为 443。确保将运行 SSL Relay 的所有服务器配置为监视同一端口。
10. 单击确定。可以将应用商店配置为提供任何 Citrix Virtual Apps and Desktops 部署组合中的资源。根据需要重复步骤 3 至 9，以在 Delivery Controller 列表中添加或修改其他部署。

管理通过 **Citrix Gateway** 对应用商店的远程访问

July 27, 2020

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：
>
> 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，
> 将配置更改传播到服务器组，以便更新部署中的其他服务器。

1. 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。
3. 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。
4. 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。如果希望在列表中添加更多部署，请单击添加。否则，请继续执行步骤 14。
5. 在“常规设置”页面上，为 Citrix Gateway 设备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网关。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或者最靠近其所在位置的网关。
6. 对于 **Citrix Gateway URL**，请键入用于您的部署的 Citrix Gateway 虚拟服务器的“URL: 端口”组合。如果未指定端口，则使用默认 `https://` 端口 443。没有必要在 URL 中指定端口 443。
7. 从可用选项中选择 Citrix Gateway 的用法。
   - 身份验证和 **HDX** 路由： Citrix Gateway 将用于进行身份验证以及路由任何 HDX 会话。
   - 仅限身份验证： Citrix Gateway 将用于身份验证，不用于任何 HDX 会话路由。
   - 仅限 **HDX** 路由： Citrix Gateway 将用于 HDX 会话路由，不用于身份验证。
8. 对于所有部署，如果要通过应用商店提供由 Citrix Virtual Apps and Desktops 或 XenApp 6.5 提供的资源，请在 **Secure Ticket Authority** 页面中列出运行 STA 的服务器的 Secure Ticket Authority (STA) URL。添加多个 STA 的 URL 以启用容错功能，并按优先级顺序列出这些服务器以设置故障转移顺序。

STA 托管在 Citrix Virtual Apps and Desktops 或 XenApp 6.5 服务器上，并发出会话票据以响应连接请求。这些会话票据构成了对访问 Citrix Virtual Apps and Desktops 或 XenApp 6.5 资源进行身份验证和授权的基础。使用正确的 STA URL（例如 `HTTPS://` 或`HTTP://`），具体取决于 Delivery Controller 的配置方式。STA URL 还必须与在虚拟服务器上的 Citrix Gateway 中配置的 URL 相同。

9. 选择设置要进行负载平衡的 Secure Ticket Authority。还可以指定时间间隔，超过此间隔后，将绕过未响应的 STA。
10. 要确保 Citrix Virtual Apps and Desktops 或 XenApp 6.5 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，请选择启用会话可靠性。
11. 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。StoreFront 将从两个不同的 STA 获取会话票据，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。
12. 在身份验证设置页面上，键入 Citrix Gateway 设备的虚拟服务器 **IP** 地址 (VIP)。

    使用 Citrix Gateway 虚拟服务器的专用 IP 地址，而非通过网络地址转换功能转换为专用 IP 地址的公用 IP 地址。网关通常由 StoreFront 通过其 URL 进行识别。如果使用全局服务器负载平衡 (GSLB)，则必须将 VIP 添加到每个网关中。这允许 StoreFront 识别多个网关，这些网关都使用相同的 URL（GSLB 域名）作为不同的网关。例如，可以为使用相同 URL 的应用商店配置三个网关（例如 `https://gslb.domain.com`），但每个网关都配置了唯一的 VIP，例如 10.0.0.1、10.0.0.2 和 10.0.0.3。
13. 如果要添加运行 Citrix Gateway 的设备，请从登录类型列表中选择您在设备上为 Citrix Workspace 应用程序用户配置的身份验证方法。

    - 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。
14. 如果要为 Citrix Gateway 配置 StoreFront 并希望使用智能访问，则必须键入回调 **URL**。StoreFront 会自动附加 URL 的标准部分。输入设备的内部可访问的 URL。StoreFront 连接 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。

    使用 GSLB 时，我们建议您为每个 GSLB 网关配置唯一的回调 URL。StoreFront 必须能够将每个唯一的回调 URL 解析为每个 GSLB 网关虚拟服务器配置的专用 VIP。例如，`emeagateway.domain.com`、`usgateway.domain.com` 和 `apacgateway.domain.com` 应解析为正确的网关 VIP。
15. 单击创建，将 Citrix Gateway 设备添加到远程访问设置对话框的列表中。

    有关 Citrix Gateway 设备的配置信息保存到应用商店的.cr 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。

16. 根据需要重复步骤 4 到 13，将更多 Citrix Gateway 设备添加到 Citrix Gateway 设备列表中。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，请指定用于访问该应用商店的默认设备。
17. 单击确定保存配置并关闭“配置远程访问”对话框。

证书吊销列表 (CRL) 检查

December 2, 2020

简介

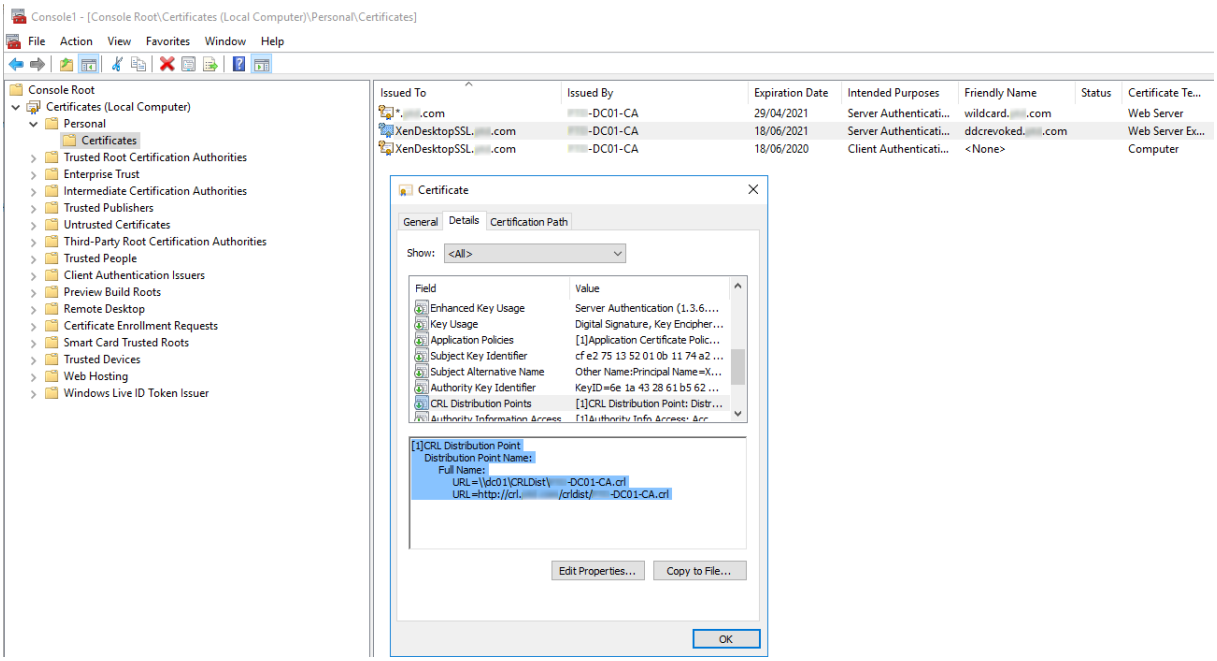
您可以将 StoreFront 配置为使用已发布的证书吊销列表 (CRL) 检查
CVAD Delivery Controller 所使用的 TLS 证书的状态。如果出现以下情况，
您可能需要吊销证书访问权限：

- 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 CRL。

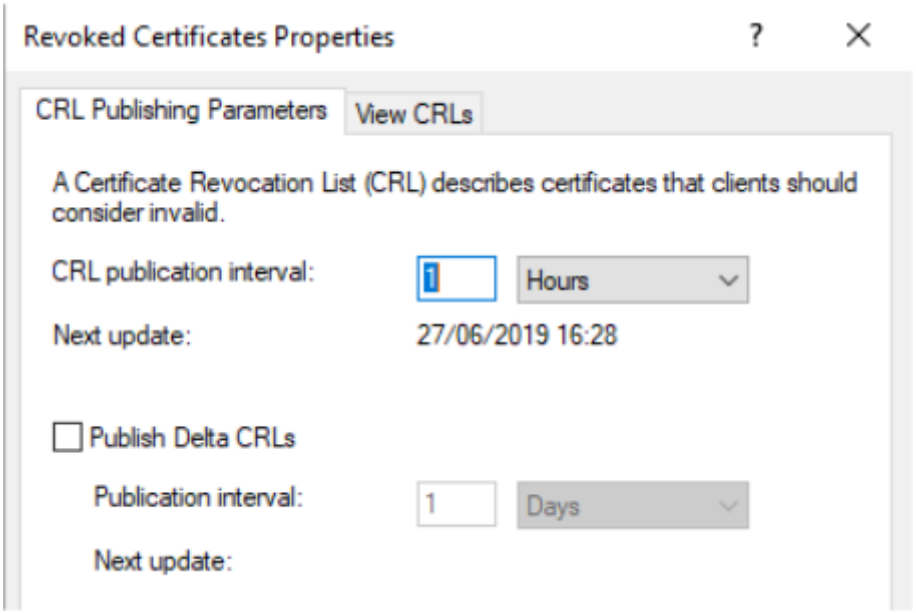
CRL 分发点 (CDP) 扩展

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 CRL 分发点
扩展的属性，以设置适合公钥基础结构的
较低 CRL 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。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，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。
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

要为存储设置证书吊销策略，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
多个存储，请对所有存储重复此过程。-CertRevocationPolicy 是
存储级别的设置，它会影响为 $StoreVirtualPath 中指定的
存储配置的所有 Delivery Controller。


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

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
```

在 **StoreFront** 服务器上使用本地导入的 **CRL**

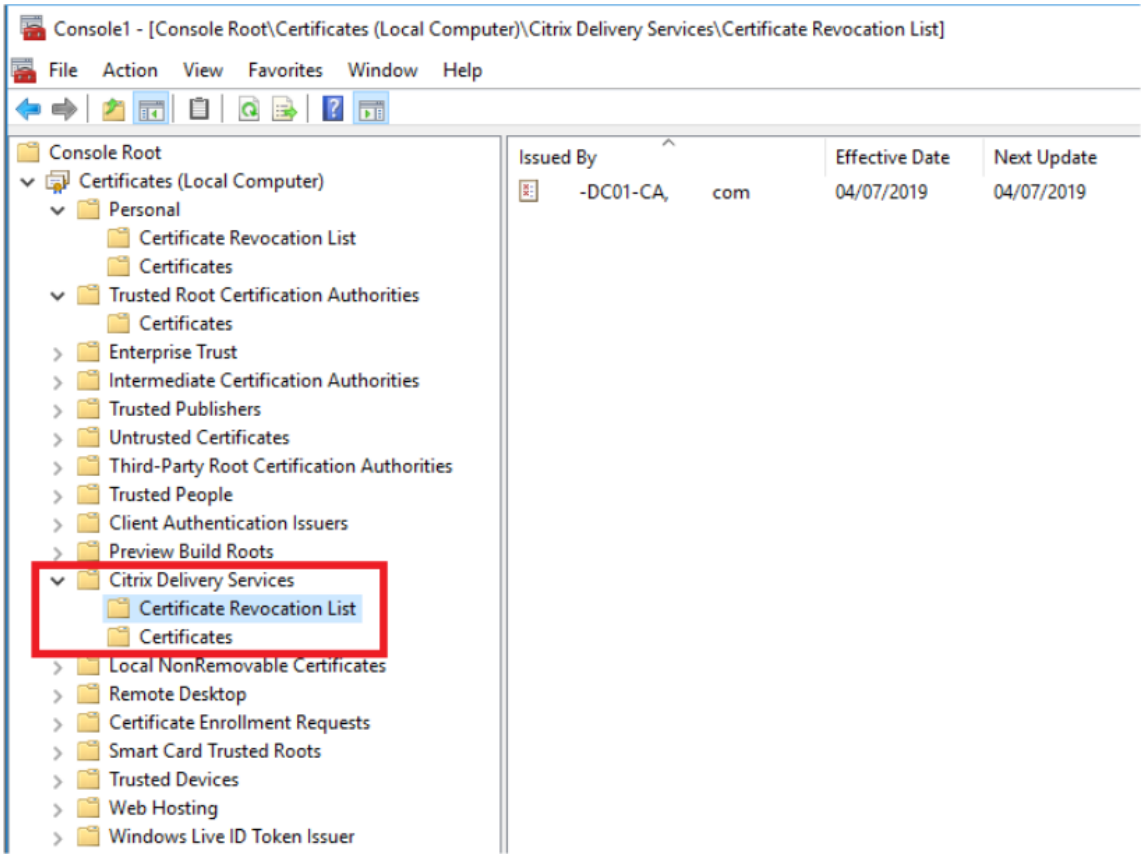
支持使用本地导入的 CRL，但 Citrix 不建议这样做，
因为：

- 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或更新的 CRL。

使用本地导入的 **CRL**

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 以委托 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。此
情况是正常的，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，
则 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 支持两种用于将存储映射到身份验证服务的
> 模型。推荐的方法是在存储和身份验证服务之间
> 进行一对一映射。在这种情况下，您必须对所有存储
> 及其各自的身份验证服务执行此部分中的步骤。
>
> 确保将证书吊销模式设置为与存储和
> 身份验证服务所用模式相同的值。或者，如果所有存储的
> 身份验证配置都相同，则可以将多个存储配
> 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。使用前面部分中所述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”
```

2. 选择要用于 XML 身份验证的存储服务、
   身份验证服务和 Delivery Controller。确保已为存储
   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
```

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

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

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
```

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**

```
无法建立 SSL 连接：在进行 SSL 连接期间发生错误
密码：拒绝访问。

此消息已由 Citrix XML Service 报告，地址为：
https://deliverycontrollerTLS.domain.com/scripts/wpnbr.dll。

无法联系指定的 Citrix XML Service，并且已从
活动服务列表中将其删除。
```

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

```
在身份验证过程中收到意外响应。

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

一般身份验证失败

ExplicitResult.State: 5

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

ActionType: LoginAttempt

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

将两个 **StoreFront** 应用商店配置为共享公用订阅数据存储

June 5, 2020

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>
```

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>
```

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。

管理应用商店的订阅数据

June 28, 2021

使用 PowerShell cmdlet 管理应用商店的订阅数据。

> 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"
```

导出订阅数据

可以使用以下 PowerShell cmdlet 将应用商店订阅数据导出为制表符分隔的.txt 文件来备份应用商店订阅数据。

```
$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"
```

有关 Restore-STFStoreSubscriptions 的详细信息，请参阅 https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/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. 导出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。

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

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

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

Subscription Datastore Size	
No of Records	Size MB
0	6.02
1000	7.02
10000	40.00
100000	219.00
200000	358.00
500000	784.00
800000	1213.02
1000000	1497.15
1300000	1919.15
1500000	2205.15
1700000	2487.15
2000000	2915.15

导入和导出**.txt** 文件的大小

Subscriptions Import/Export.txt	
No of Records	Size MB
0	0.00
1000	0.13
10000	1.30
100000	12.80
200000	25.60
500000	64.10
800000	102.00
1000000	128.00
1300000	166.00
1500000	192.00
1700000	218.00
2000000	256.00

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"
```

使用 **Microsoft SQL Server** 存储订阅数据

December 2, 2020

> 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。	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。
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。	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）

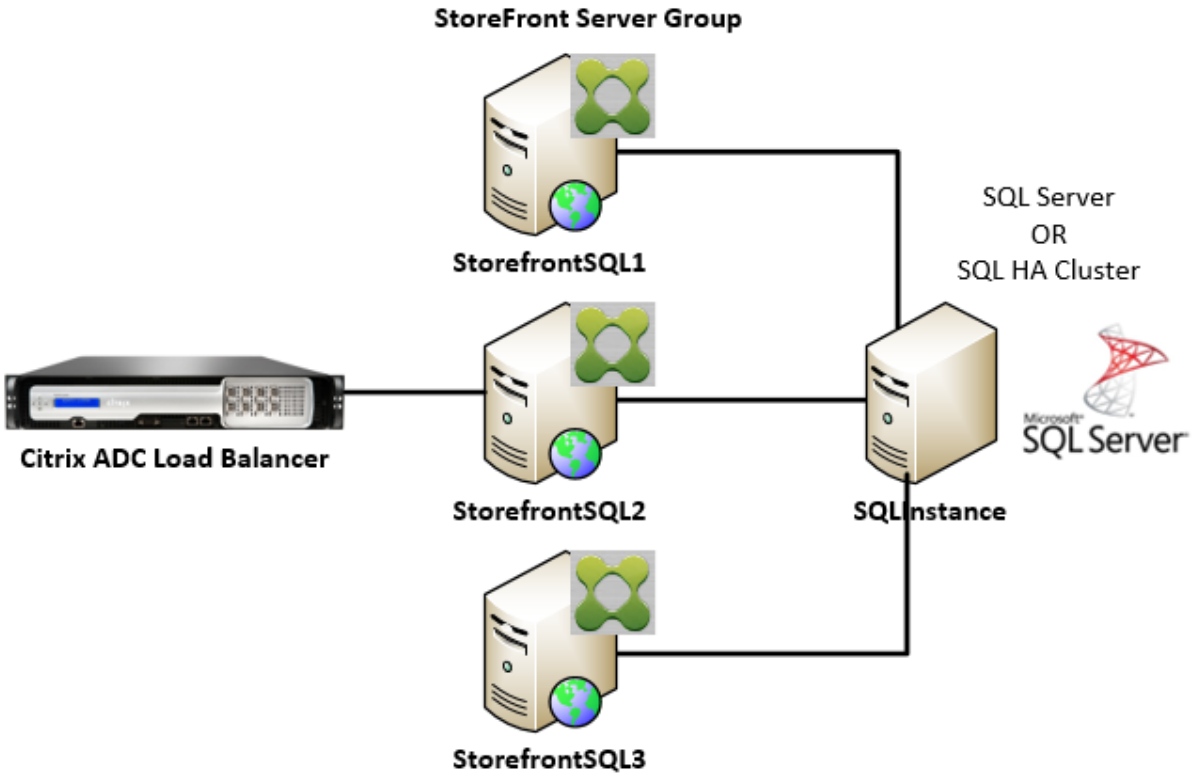
默认情况下，自版本 2.0 以来的所有 StoreFront 版本都使用平面 ESENT 数据库在服务器组成员之间存储和复制订阅数据。服务器组的每个成员都维护订阅数据库的相同副本，该副本与服务器组的所有其他成员同步。此方案不需要执行任何其他步骤即可配置。此方案适用于大多数客户，这些客户不期望经常更改 Delivery Controller 名称，或者不需要对其订阅数据执行频繁的管理任务，例如删除或更新旧用户订阅。

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）

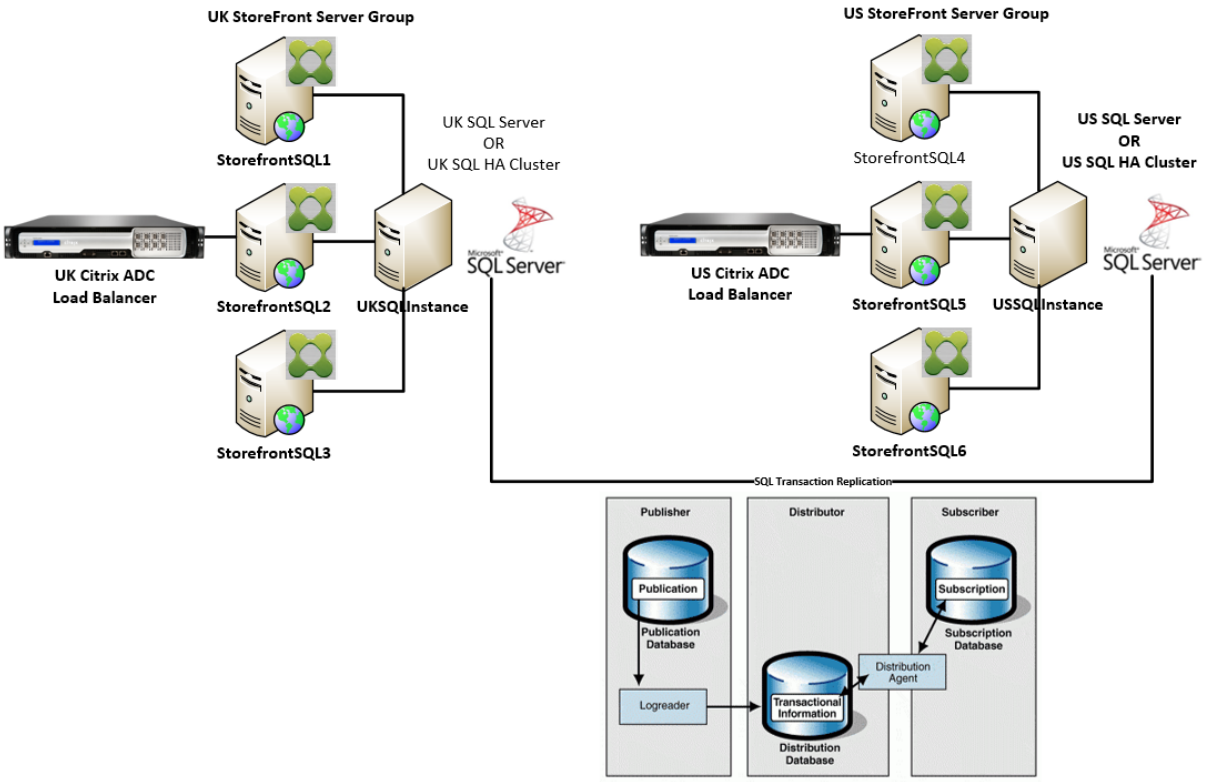
所有 StoreFront 服务器组成员连接到同一个专用的 Microsoft SQL Server 实例或 SQL 故障转移群集。此方案是最适合大型企业部署的模型，在此类部署中，Citrix 管理员希望频繁更改 Delivery Controller 名称或希望对其订阅数据执行频繁的管理任务，例如删除或更新旧用户订阅并要求高可用性。



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。

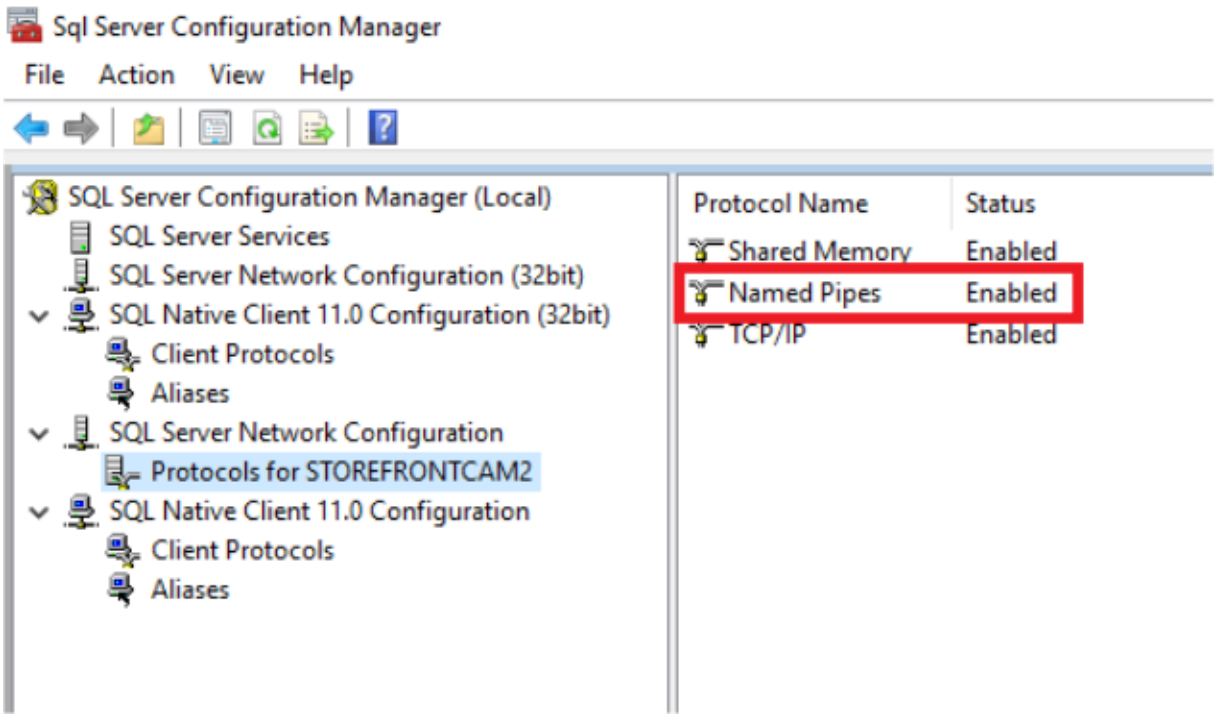
可以下载脚本 Add-LocalAppPoolAccounts.ps1 来帮助您。

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"
```

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。

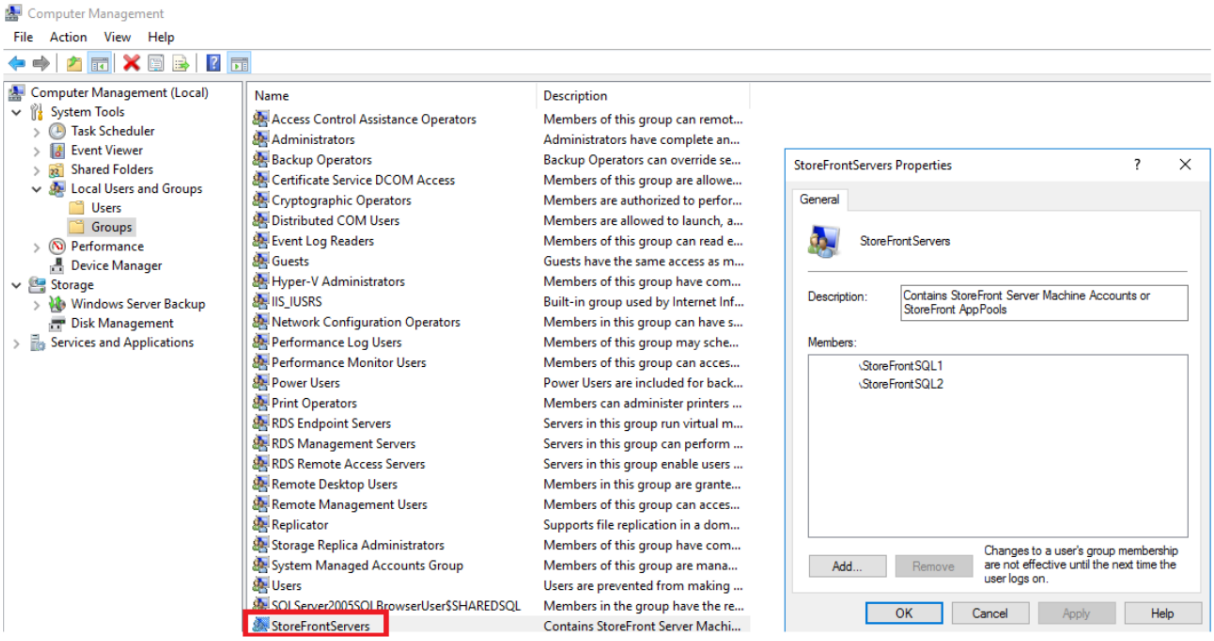


确保正确配置 Windows 防火墙规则以允许使用特定端口或动态端口建立 SQL Server 连接。请参阅 Microsoft 文档，了解如何在您的环境中执行此操作。

> 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"))
{

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

else
```

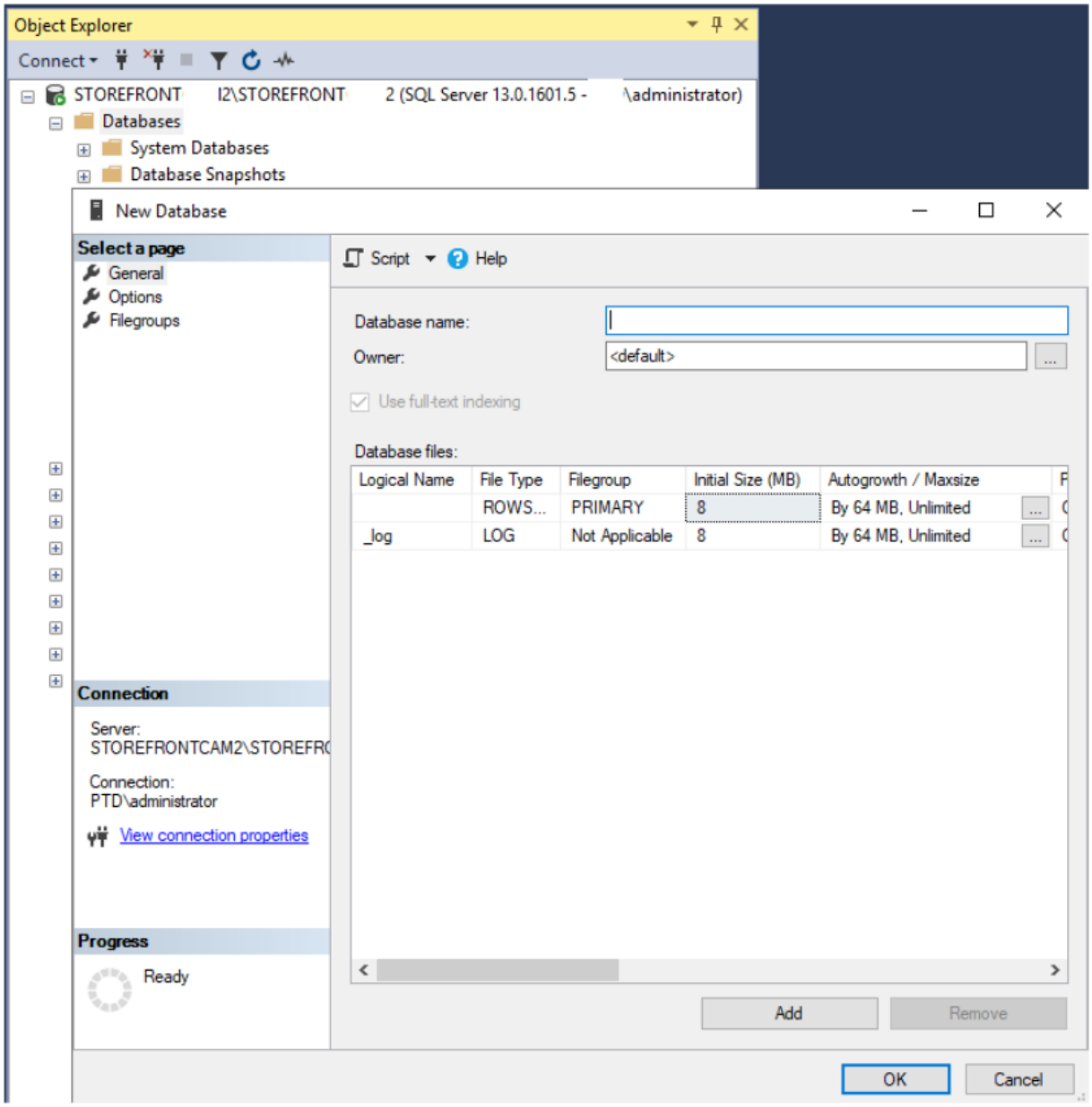


```
{

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

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

Write-Host "Adding $StoreFrontServers to $LocalGroupName local group" -
   ForegroundColor "Yellow"

foreach ($StoreFrontServer in $StoreFrontServers)
{

    $Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"
    $Computer = [ADSI]"WinNT://$Domain/$StoreFrontServer$"
    $Group.Add($Computer.Path)
 }

Write-Host "$StoreFrontServers added to $LocalGroupName" -
   ForegroundColor "Green"
 }

Add-RemoteSTFMachineAccounts -Domain "example" -StoreFrontServers @("
   StoreFrontSQL1","StoreFrontSQL2")
```

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。

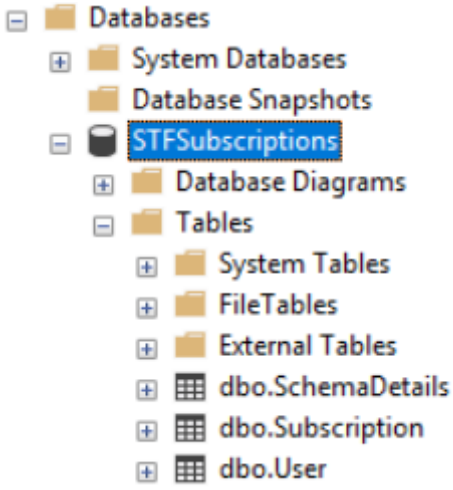
```
C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\
STFSubscriptions.mdf
```

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

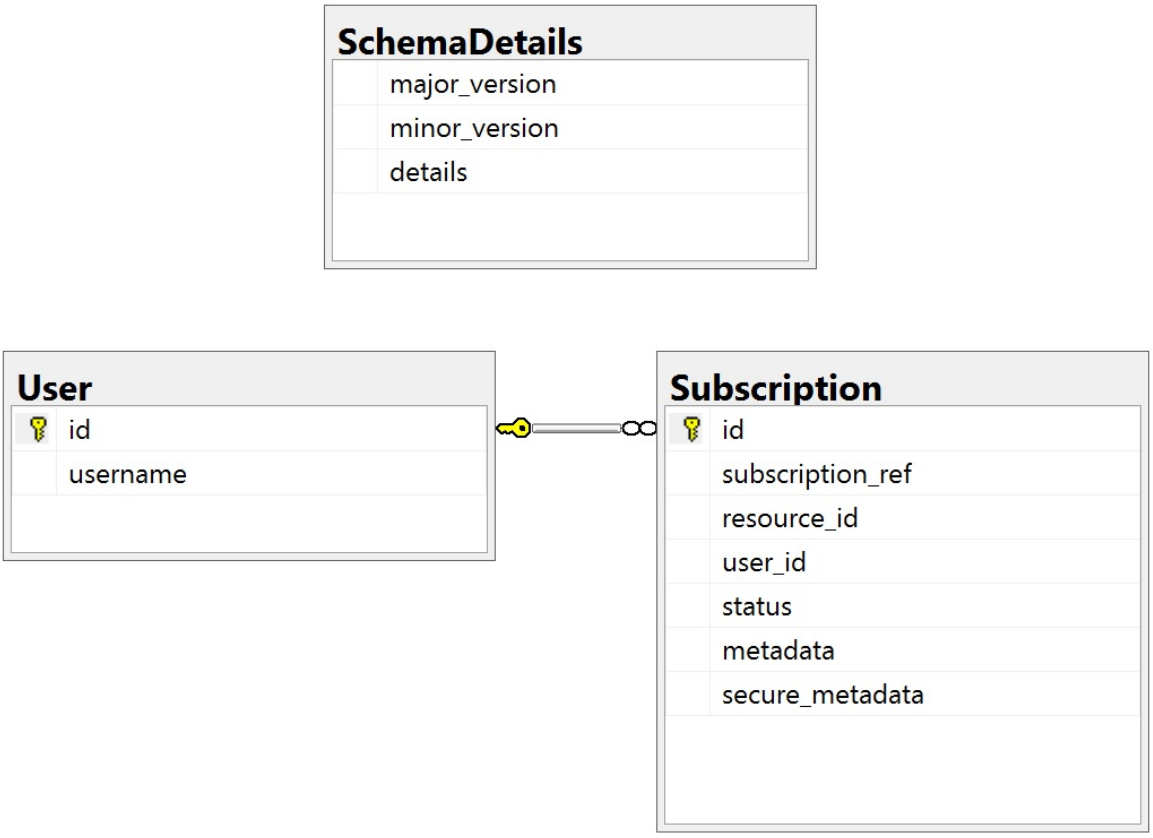

- 在脚本中设置对 SQL Server 名称的引用：

```
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
```

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"
$DBInstance = "StoreFrontInstance"
$SQLPort = "2703"
```

根据您正在使用的数据库配置配置 `$ConnectionString` 变量：


```
# For a remote database instance use the following:
$ConnectionString = "Server=$DBServer$DBInstance;Database=$DBName;
    Trusted_Connection=True;"
```

```
# For a remote database instance using a custom SQL TCP port number,
    use the following,
# taking care to use a comma `,` not a semi colon `;`:
$ConnectionString = "Server=$DBServer$DBInstance,$SQLPort;Database=
    $DBName;Trusted_Connection=True;"
```

```
# For a locally installed database instance, use the following:
$ConnectionString = "$DBLocalServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;"
```

设置 StoreFront 用于连接到订阅数据库的 SQL DB 连接字符串：

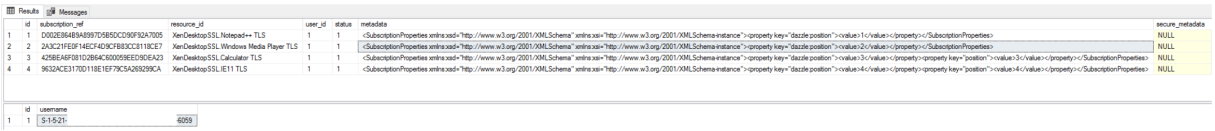
```
$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath
    $VirtualPath
Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
    ConnectionString $ConnectionString
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
```

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。

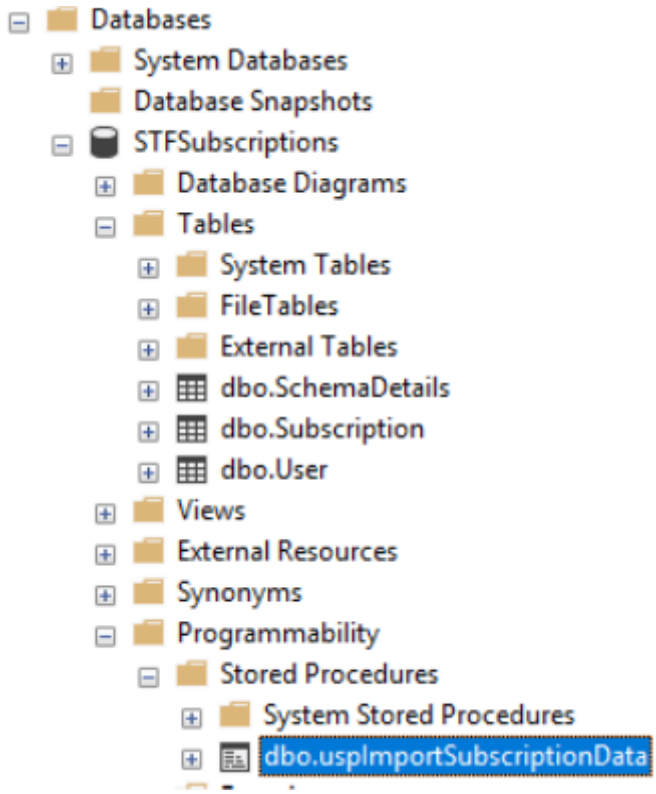
Create-ImportSubscriptionDataSP.sql 脚本将创建一个 T-SQL 存储过程以批量导入订阅数据。该将本将删除每个唯一用户的重复条目，以便将生成的 SQL 数据正确规范化并拆分为正确的表。

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。

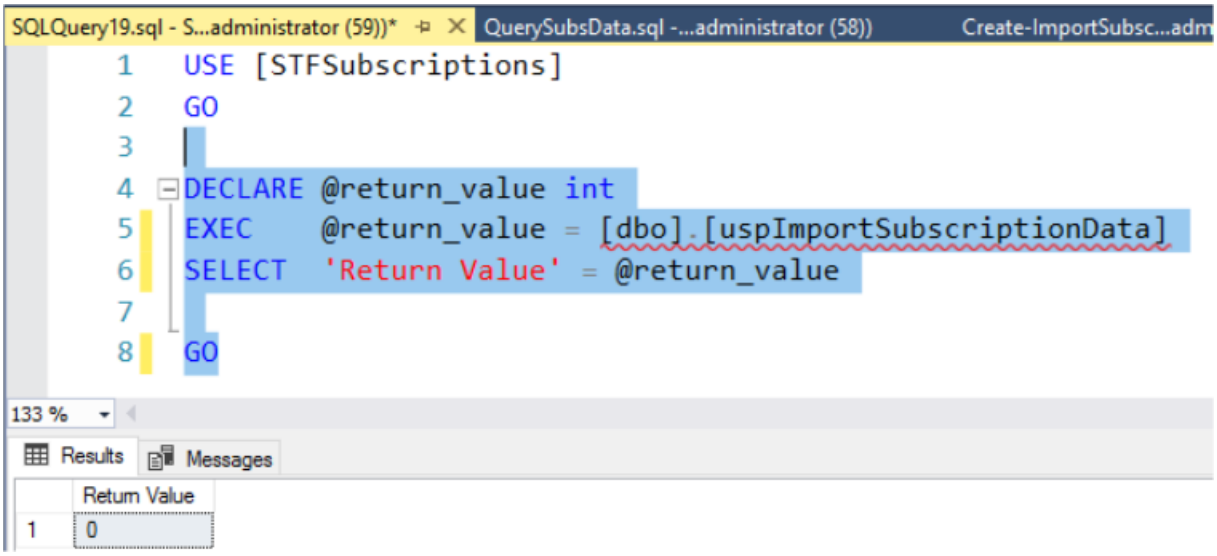
使用 SQL Server Management Studio 打开 *Create-ImportSubscriptionDataSP.sql* 文件，并在其中执行代码。此脚本将 *ImportSubscriptionDataSP* 存储过程添加到您之前创建的数据库中。

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]
```

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]
```

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]
```

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

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



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

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

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

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。

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

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

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

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

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

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

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

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

```
-- Delete ALL subscription data from a particular database and reset
    the primary key clustered index to start numbering from 0.
```

```
-- USE WITH EXTREME CARE AND NOT ON LIVE PRODUCTION DATABASES.
-- Can be useful whilst debugging data import issues to start with a
    clean database.

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

高级应用商店设置

June 29, 2021

可以使用“配置应用商店设置”中的“高级设置”页面配置高级应用商店属性。

> 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，执行将配置更改传播到服务器组操作，以便更新部署中的其他服务器。

1. 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。
3. 在配置应用商店设置页面上，选择高级设置，选择要配置的高级选项，进行所需的更改，然后单击确定。

地址解析类型

可以使用高级设置页面指定要从服务器请求的地址的类型。默认格式为 DnsPort。从高级设置上的地址解析类型下拉菜单中，选择以下选项之一：

- 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。

执行高级设置任务，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。

执行高级设置任务，选择允许重新连接会话选项，然后单击确定以启用会话重新连接。

允许特殊文件夹重定向

可以通过执行高级设置任务启用或禁用特殊文件夹重定向。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。

执行高级设置任务，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

> 注意：
>
> 此功能仅在 StoreFront 1912 LTSR CU1 及更高的受支持版本中有效。它仅用于 Citrix Virtual Apps and Desktops 服务部署中的本地主机缓存功能。
>
> 本地主机缓存需要客户部署的本地 StoreFront 作为部署的一部分。必须将注册了（或可以注册）VDA 的所有 Cloud Connector 添加到 StoreFront 作为 Delivery Controller。未添加到 StoreFront 的 Cloud Connector 无法转换为中断模式，这可能会导致用户启动失败。

要在服务中断期间确保资源（应用程序和桌面）可用性，而无需在每个区域（资源位置）中发布资源，请在每个区域的每个 StoreFront 应用商店中启用高级运行状况检查功能。

1. 在应用商店的 `web.config` 文件中，在 `farmsets` 下，添加 `advancedHealthCheck="on"`。例如：

```
<farmsets>
  <farmset name="Default" enableFileTypeAssociation="on" pooledSockets="off"
    serverCommunicationAttempts="1" communicationTimeout="30" connectionTimeout="6"
    multiFarmAuthenticationMode="ANY" backgroundHealthCheckPollingPeriod="00:01:00"
    advancedHealthCheck="on">
    <farm name="Controller12345" xmlPort="80" transport="HTTP" sslRelayPort="443"
      bypassDuration="60" allFailedBypassDuration="0" loadBalance="on"
      ticketTimeToLive="200" farmType="XenDesktop" maxServersPerRequest="0"
      zones="">
```

2. 更新文件后，手动重新启动 IIS。对其他存储重复执行 `web.config` 文件更新和 IIS 重新启动操作。

后台运行状况检查轮询期限

StoreFront 对每个 Citrix Virtual Desktops Broker 和 Citrix Virtual Apps 服务器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)。可以通过执行高级设置任务指定后台运行状况检查轮询周期，然后单击确定控制运行状况检查的频率。

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。可以通过执行高级设置任务更改默认时间，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。

可以通过执行高级设置任务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。

执行高级设置任务，选择（或取消选择）启用增强枚举选项，然后单击确定。

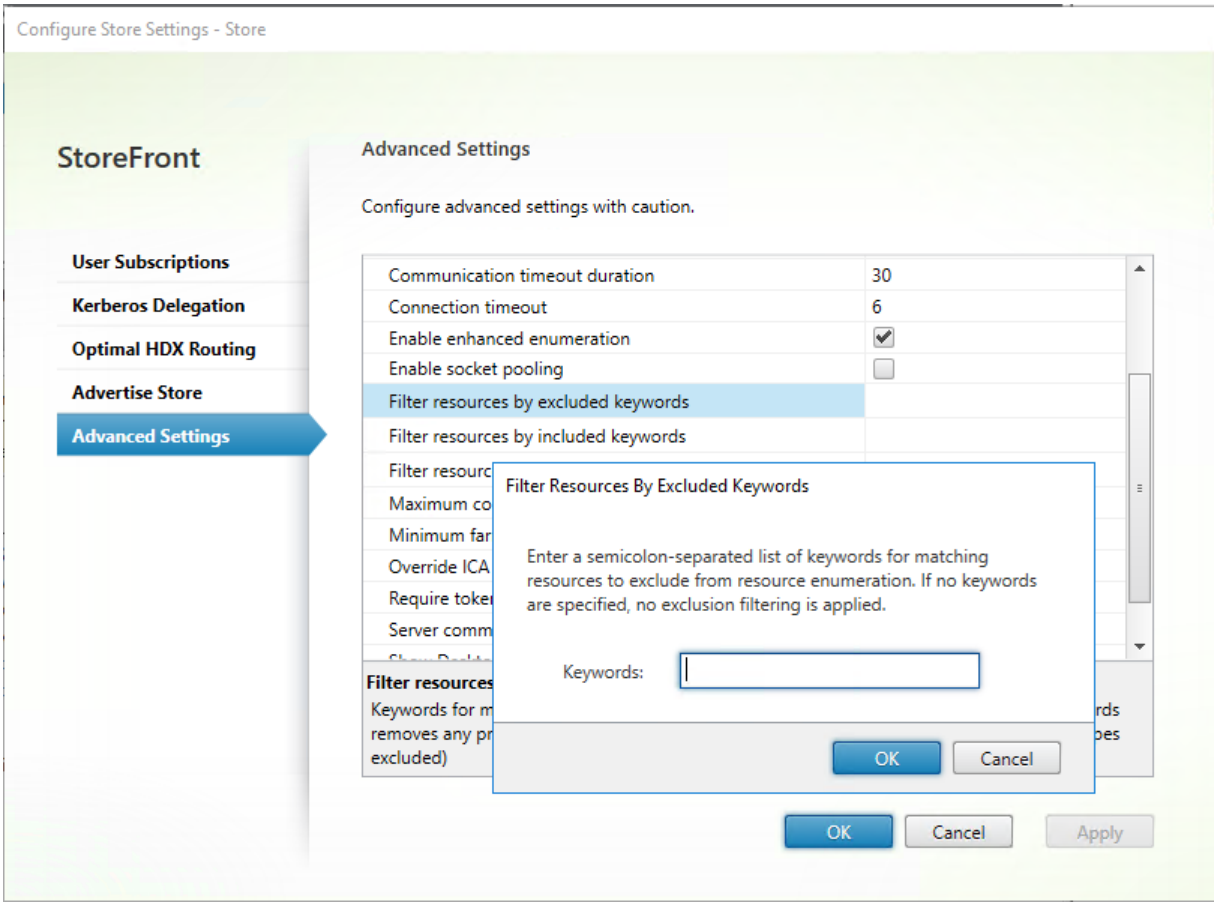
启用套接字池

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。执行高级设置任务，选择启用套接字池选项，然后单击确定以启用套接字池。

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)”。

可以通过执行高级设置任务选择过滤资源 **(**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。



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)”。

可以通过执行高级设置任务选择过滤资源 **(**按包括的关键字**)**，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。

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)”。

可以通过执行高级设置任务选择过滤资源 **(**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。

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)”。

可以通过执行高级设置任务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。

可以通过执行高级设置任务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 Citrix Receiver for Web 生成的 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”。

执行高级设置任务，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。默认值为开。

执行高级设置任务，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。

可以通过执行高级设置任务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”。

执行高级设置任务，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”。

使用高级设置任务，选择将桌面视为应用程序选项，然后单击确定。

管理 Citrix Receiver for Web 站点

July 27, 2020

Citrix Receiver for Web 站点是用作应用商店的 Web 站点。用户可以在浏览器中打开一个站点，并安全地访问通过 Citrix Virtual Apps and Desktops 为其发布的应用程序、数据和桌面。

使用 StoreFront 管理控制台执行以下 Citrix Receiver for Web 相关任务：

任务	详细信息
创建 Citrix Receiver for Web 站点	创建 Citrix Receiver for Web 站点，使用户可以通过 Web 页面访问应用商店。
配置 Citrix Receiver for Web 站点	修改 Receiver for Web 站点的设置。
统一用户体验	StoreFront 支持统一用户体验。统一体验提供集中管理的 HTML5 用户体验。
创建和管理精选应用程序	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。
配置工作区控制	工作区控制功能使应用程序能够随用户在设备之间移动。
配置适用于 HTML5 的 Citrix Workspace 应用程序对浏览器选项卡的使用	指定用户通过快捷方式使用 Citrix Receiver for HTML5 或适用于 HTML5 的 Citrix Workspace 应用程序启动资源的时间、桌面或应用程序是否会替换现有浏览器选项卡中的 Citrix Receiver for Web 站点，而不是显示在新选项卡内。
配置通信超时持续时间和重试次数	默认情况下，Citrix Receiver for Web 站点对关联应用商店的请求将在三分钟后超时。通信尝试失败一次后，应用商店将被视为不可用。可以更改默认设置。

创建 Citrix Receiver for Web 站点

June 5, 2020

创建应用商店时，将自动为其创建一个 Citrix Receiver for Web 站点。可以向现有应用商店中添加额外的 Citrix Receiver for Web 站点。

> 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，
> 将配置更改传播到服务器组，以便更新部署中的其他服务器。

1. 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。
3. 单击添加创建新 Citrix Receiver for Web 站点。键入所需的 **Web** 站点路径，然后单击下一步。
4. 选择 Citrix Receiver 体验并单击下一步。
5. 选择身份验证方法，单击创建，创建站点后，单击完成。

   此时将显示一个 URL，用户可以通过该 URL 访问 Citrix Receiver for Web 站点。有关修改 Citrix Receiver for Web 站点设置的详细信息，请参阅配置 Citrix Receiver for Web 站点。

默认情况下，当用户通过运行 Windows 或 Mac OS X 的计算机访问 Receiver for Web 站点时，此站点将尝试确定用户设备上是否已安装 Citrix Workspace 应用程序。如果检测不到 Citrix Workspace 应用程序，系统将提示用户通过 Citrix Web 站点下载并安装适合其平台的 Citrix Workspace 应用程序。有关修改此行为的详细信息，请参阅为没有安装 Citrix Workspace 应用程序的用户配置站点行为。

Receiver for Web 站点的默认配置要求用户必须安装兼容版本的 Citrix Workspace 应用程序，才能访问自己的桌面和应用程序。但是，您可以在 Citrix Receiver for Web 站点上启用适用于 HTML5 的 Citrix Workspace 应用程序，以便无法安装 Citrix Workspace 应用程序的用户仍然可以访问资源。有关详细信息，请参阅配置 Citrix Receiver for Web 站点。

配置 **Citrix Receiver for Web** 站点

June 29, 2021

可以通过执行以下任务来修改 Citrix Receiver for Web 站点的设置。某些高级设置只能通过编辑站点配置文件进行更改。有关详细信息，请参阅使用配置文件配置 Citrix Receiver for Web 站点。

> 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，
> 将配置更改传播到服务器组，以便更新部署中的其他服务器。

选择身份验证方法

可以通过执行“管理身份验证方法”任务为连接到 Citrix Receiver for Web 站点的用户分配身份验证方法。此操作允许您为每个 Receiver for Web 站点指定部分身份验证方法。

1. 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 管理控制台的左侧窗格中选择应用商店节点，然后从“应用商店”窗格中选择要修改的相关应用商店。
3. 在“应用商店”窗格中，依次单击管理 **Receiver for Web** 站点和配置，然后选择身份验证方法，指定要为用户启用的访问方法。

   > 注意：
   >
   > † 标记为 † 的 Citrix Receiver for Web 站点身份验证方法不是由应用商店的身份验证方法中的设置定义的。请为每个 Citrix Receiver for Web 站点单独配置这些身份验证方法。本文中介绍的其他身份验证方法由应用商店的身份验证方法进行定义。（也就是说，在本文中为 Citrix Receiver for Web 站点进行的选择或取消选择将替换为创建或删除应用商店中介绍的应用商店的设置。）

   - 选中用户名和密码复选框以启用显式身份验证。用户在访问自己的应用商店时需要输入凭据。
   - 选择 **SAML** 身份验证以支持与 SAML 身份提供程序的集成。用户向身份提供程序验证身份后，即可在访问自己的应用商店时自动登录。从“设置”下拉菜单中：
     - 选择身份提供程序以配置对身份提供程序的信任。
     - 选择服务提供商以对服务提供商配置信任。身份提供程序需要此信息。
   - 选中域直通 † 以启用从用户设备直通 Active Directory 域凭据。用户向其加入域的 Windows 计算机验证身份后，即可在访问自己的应用商店时自动登录。要使用此选项，在用户设备上安装 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序时，必须启用直通身份验证。

     > 注意：
     >
     > 面向 Citrix Receiver for Web 的域直通身份验证仅对使用 Internet Explorer、Microsoft Edge、Mozilla Firefox 和 Google Chrome 的 Windows 操作系统有效。

   - 选中智能卡 † 以启用智能卡身份验证。用户在访问应用商店时其使用智能卡和 PIN 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。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。
4. 选择身份验证方法后，单击确定。

   有关修改身份验证方法设置的详细信息，请参阅配置身份验证服务。

将资源快捷方式添加到其他 **Web** 站点

可以通过执行向 **Web** 站点添加快捷方式任务允许用户从内部网络上托管的可信 Web 站点快速访问桌面和应用程序。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。可信 URL 在 Citrix Receiver for Web 站点的 web.config 文件的 `<trustedUrls>` 部分中

列出。web.config 通常位于 `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。

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，然后取消选择提示快捷方式不受信任选项。

使用管理控制台添加可信 **Web** 站点

1. 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 管理控制台的左侧窗格中选择应用商店节点，然后在结果窗格中选择站点。
3. 在操作窗格中，依次单击管理 **Receiver for Web** 站点和配置，然后选择 **Web** 站点快捷方式。
4. 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。
5. 单击获取快捷方式，如果提示保存配置更改，则单击保存。
6. 登录到 Citrix Receiver for Web 站点并将所需 URL 复制到您的 Web 站点。

使用 **PowerShell** 添加可信 **Web** 站点

可以使用 https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Citrix.StoreFront.SubscriptionsStore/ 中介绍的 **Set-STFWebReceiverApplicationShortcuts** PowerShell cmdlet 添加“可信”URL。

对会话设置进行设置

1. 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** 站点和配置，然后选择会话设置。

您可以更改以下设置：

服务器通信尝试次数：Receiver for Web 尝试与应用商店服务器进行通信的次数。此尝试次数默认设置为 1。

通信超时持续时间：超过此时间后，Receiver for Web 将确定应用商店服务器不可用。此事件默认为 3 分钟。

会话超时：超过此时间后，Citrix Receiver for Web 站点上的用户会话将超时。用户会话超时后，用户可以继续使用已处于运行状态的任何桌面或应用程序，但必须重新登录才能访问 Citrix Receiver for Web 站点的各项功能，例如订阅应用程序。所有时间间隔的最小值均为 1。每个时间间隔的最大值为 1 年。默认情况下，用户会话在处于非活动状态 20 分钟后将超时。

登录超时：在此时间之后，如果没有活动，Receiver for Web 登录页面将超时。您可以为登录超时指定分钟数。默认值为 5 分钟。注意：登录超时应小于会话超时。

为应用程序和桌面指定不同的视图

可以通过执行管理 **Receiver for Web** 站点中的 **Receiver for Web** 上的应用程序和桌面视图任务来更改会话超时值。

1. 在 Windows 开始屏幕或应用程序屏幕中，找到并单击 **Citrix StoreFront** 磁贴。
2. 在左侧窗格中选择应用商店节点，在操作窗格中依次单击“管理 Receiver for Web 站点”和配置，然后选择客户端界面设置。
3. 从选择视图和默认视图下拉菜单中，选择要显示的视图。

要启用文件夹视图，请执行以下操作：

1. 在 Windows 开始屏幕或应用程序屏幕中，找到并单击 **Citrix StoreFront** 磁贴。
2. 在左侧窗格中选择应用商店节点，在操作窗格中依次单击管理 **Receiver for Web** 站点和配置。
3. 选择高级设置，然后选中启用文件夹视图。

停止向用户提供预配文件

默认情况下，Citrix Receiver for Web 站点会提供一些预配文件，以支持用户为关联的应用商店自动配置 Citrix Receiver 或 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。在本文中，除非另行说明，否则“Citrix Workspace 应用程序”的提及也表示受支持的 Citrix Receiver 版本。

可以通过执行管理 **Receiver for Web** 站点中的启用 **Receiver** 配置任务来更改会话超时值。

1. 在 Windows 开始屏幕或应用程序屏幕中，找到并单击 **Citrix StoreFront** 磁贴。
2. 在左侧窗格中选择应用商店节点，在操作窗格中依次单击管理 **Receiver for Web** 站点和配置，然后选择客户端界面设置。
3. 选择启用 **Receiver/Workspace** 应用程序配置。

为没有安装 **Citrix Workspace** 应用程序的用户配置站点行为

可以通过执行部署 **Citrix Receiver/Workspace** 应用程序任务配置当未安装 Citrix Workspace 应用程序的 Windows 或 Mac OS X 用户访问站点时 Citrix Receiver for Web 站点的行为。默认情况下，当从运行 Windows 或 Mac OS X 的计算机进行访问时，Citrix Receiver for Web 站点会自动尝试确定是否安装了 Citrix Workspace 应用程序。

如果检测不到 Citrix Workspace 应用程序，系统将提示用户下载并安装适合其平台的 Citrix Workspace 应用程序。默认下载位置为 Citrix Web 站点，但您也可以将 Citrix Workspace 应用程序安装程序复制到 StoreFront 服务器，并允许用户改为直接从 StoreFront 服务器下载这些程序的副本。

对于无法安装 Citrix Workspace 应用程序的用户，您可以在 Citrix Receiver for Web 站点上启用适用于 HTML5 的 Citrix Workspace 应用程序。适用于 HTML5 的 Citrix Workspace 应用程序使用户能够直接在 HTML5 兼容的 Web 浏览器中访问桌面和应用程序，而无需安装 Citrix Workspace 应用程序。同时支持内部网络连接和通过 Citrix Gateway 建立的连接。但是，对于从内部网络发起的连接，适用于 HTML5 的 Citrix Workspace 应用程序仅支持访

问特定产品提供的资源。此外，需要具有特定版本的 Citrix Gateway 才允许从企业网络外部建立连接。有关详细信息，请参阅基础结构要求。

对于内部网络中的本地用户，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，必须在您的 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WebSocket 策略设置。

要使 Citrix Virtual Apps and Desktops 资源在直接连接到 StoreFront 时使用适用于 HTML5 的 Citrix Workspace 应用程序成功启动，必须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。

1. 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站点。在操作窗格中，依次单击管理 **Receiver for Web** 站点和配置。
3. 选择 部署 **Citrix Citrix Receiver/Workspace** 应用程序，并指定部署选项。
    - 如果希望站点始终通过 HTML5 兼容的浏览器访问资源，而不提示用户下载和安装 Citrix Workspace 应用程序，请选择始终使用 **Receiver for HTML5**。选择此选项后，用户始终通过适用于 HTML5 的 Citrix Workspace 应用程序访问站点上的桌面和应用程序，前提是其使用 HTML5 兼容的浏览器。没有 HTML5 兼容浏览器的用户无法访问资源。禁用通过任何本地安装的 Citrix Workspace 应用程序进行访问。
    - 如果希望站点提示用户下载并安装 Citrix Workspace 应用程序，但在无法安装 Citrix Workspace 应用程序时回退到适用于 HTML5 的 Citrix Workspace 应用程序，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。通过 HTML5 兼容的浏览器访问处于禁用状态。
        - 如果选择允许用户下载 **HDX Engine (**插件**)**，Citrix Receiver for Web 将允许用户在最终用户客户端上下载并安装 Citrix Workspace 应用程序（如果 Citrix Workspace 应用程序不可用）。
        - 如果选择登录时升级插件，Citrix Receiver for Web 将在用户登录时提供用于升级 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 Citrix Receiver for Web 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。
        - 从下拉列表中选择源。

在服务器上提供 **Citrix Workspace** 应用程序安装文件

默认情况下，当用户通过运行 Windows 或 Mac OS X 的计算机访问 Citrix Receiver for Web 站点时，此站点将尝试确定用户设备上是否已安装 Citrix Workspace 应用程序。如果检测不到 Citrix Workspace 应用程序，系统将提示

用户通过 Citrix Web 站点下载并安装适合其平台的 Citrix Workspace 应用程序，或者从 StoreFront 服务器下载正确的安装程序。

1. 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站点。在操作窗格中，依次单击管理 **Receiver for Web** 站点和配置。
3. 选择部署 **Citrix Receiver/Workspace** 应用程序和 **Receiver/Workspace** 应用程序的源，然后浏览到安装文件。

登录后运行安装 **Citrix Workspace** 应用程序的提示

登录到 StoreFront 之前，Citrix Receiver for Web 将提示用户安装最新的 Citrix Workspace 应用程序（如果该应用程序尚未安装在用户的计算机上）。如果用户安装的 Citrix Workspace 应用程序可以升级，该提示可能也会显示，具体取决于配置。

可以将 Citrix Receiver for Web 配置为在登录 StoreFront 后显示该提示。

1. 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 管理控制台的左侧窗格中选择应用商店节点，然后在结果窗格中选择站点。
3. 在操作窗格中，依次单击管理 **Receiver for Web** 站点和配置。
4. 选择高级设置，然后选中登录后提示安装 **Citrix Receiver/Workspace** 应用程序。

删除 **Citrix Receiver for Web** 站点

使用操作窗格中的管理 **Receiver for Web** 站点删除 Citrix Receiver for Web 站点。如果删除站点，用户将无法再使用该 Web 页面访问应用商店。

支持统一用户体验

December 2, 2020

> 注意：
>
> StoreFront 仍是用于表示企业应用商店的名称，它将来自 Citrix Virtual Apps and Desktops 站点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。Citrix Receiver 技术现在包含在 Citrix Workspace 应用程序中。我们的产品和文档中正在实施此过渡。产品中的内容可能仍包含以前的名称，例如统一体验是指 Citrix Receiver。感谢您在此转换期间耐心等待。有关新名称的更多详细信息，请参阅 https://www.citrix.com/products/。

StoreFront 支持统一用户体验。统一体验向所有 Web 和本机 Citrix Workspace 应用程序提供集中管理的 HTML5 用户体验。此体验支持自定义和精选应用程序组管理。

使用此版本的 StoreFront 创建的应用商店使用统一体验。

使用 StoreFront 管理控制台执行以下 Citrix Receiver for Web 相关任务：

- 创建 Citrix Receiver for Web 站点。
- 更改 Citrix Receiver for Web 站点体验。
- 选择与应用商店关联的统一 Citrix Receiver for Web 站点。
- 自定义 Receiver 外观。

使用 Javascript 和 CSS 自定义 Citrix Receiver for Web 页面。

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。

> 注意：
>
> 如果使用 XenApp 6.x，在启用了统一体验的情况下，不支持设置为通过流技术推送到客户端或尽可能通过流技术进行推送，否则从服务器访问的应用程序。

创建 **Citrix Receiver for Web Web** 站点

每次创建应用商店时都会自动创建 Citrix Receiver for Web 站点。您还可以使用此过程创建其他 Receiver for Web 站点。

1. 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 **Receiver for Web** 站点 > 添加，并按照向导进行操作。

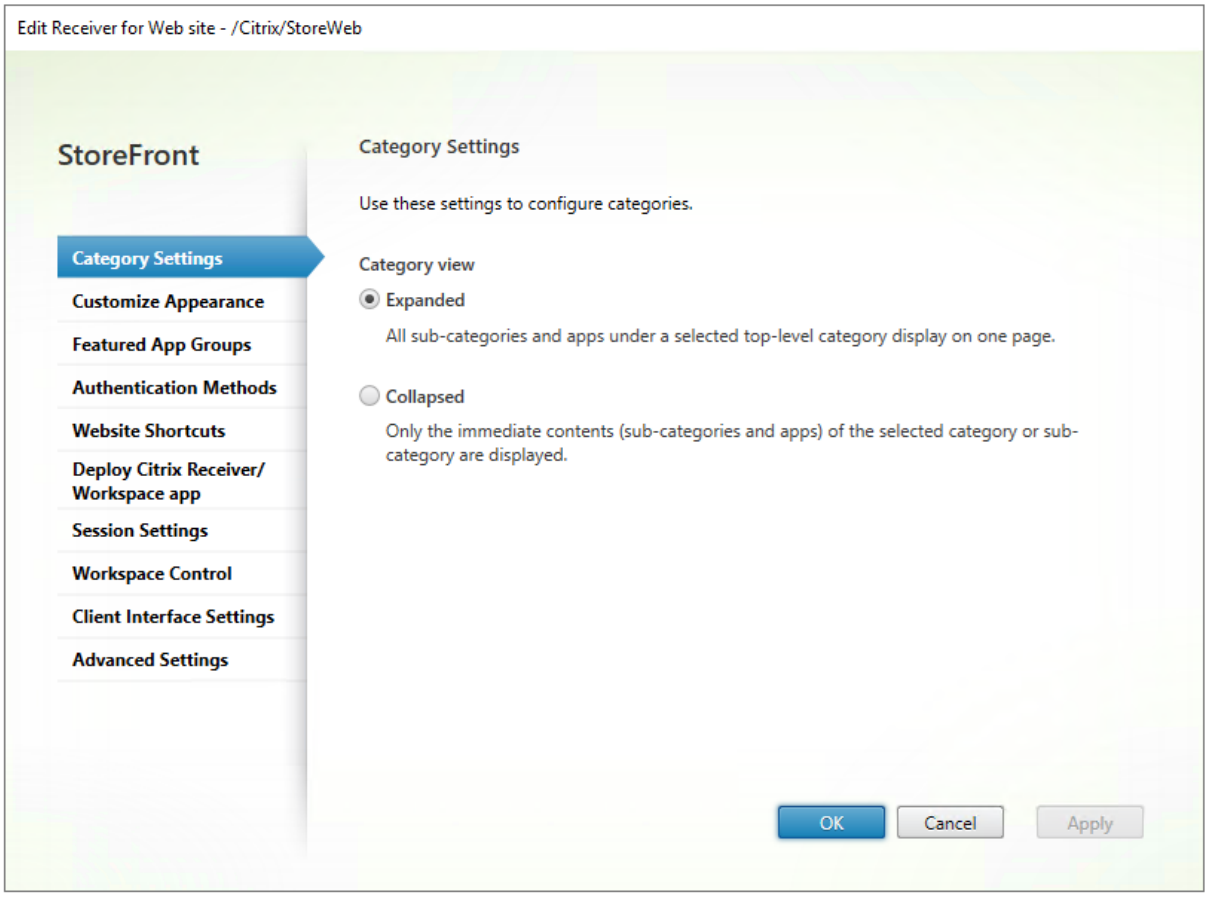
选择与应用商店关联的统一 **Citrix Receiver for Web** 站点

使用 StoreFront 创建新应用商店时，会自动创建 Citrix Receiver for Web 站点并将其与应用商店关联。Citrix Receiver for Web 站点使用统一体验。应用商店有多个 Receiver for Web 站点时，需要选择用户使用 Citrix Workspace 应用程序访问应用商店时显示哪个 Receiver for Web 站点。

1. 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. 选择用户访问此应用商店时 Citrix Workspace 应用程序客户端将显示的默认 Receiver for Web 站点。
4. 单击确定。

配置类别设置

1. 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 **Receiver for Web** 站点，选择 Receiver for Web 站点，然后单击配置。
3. 选择类别设置并进行选择以自定义登录后类别的显示方式。



选择类别视图：

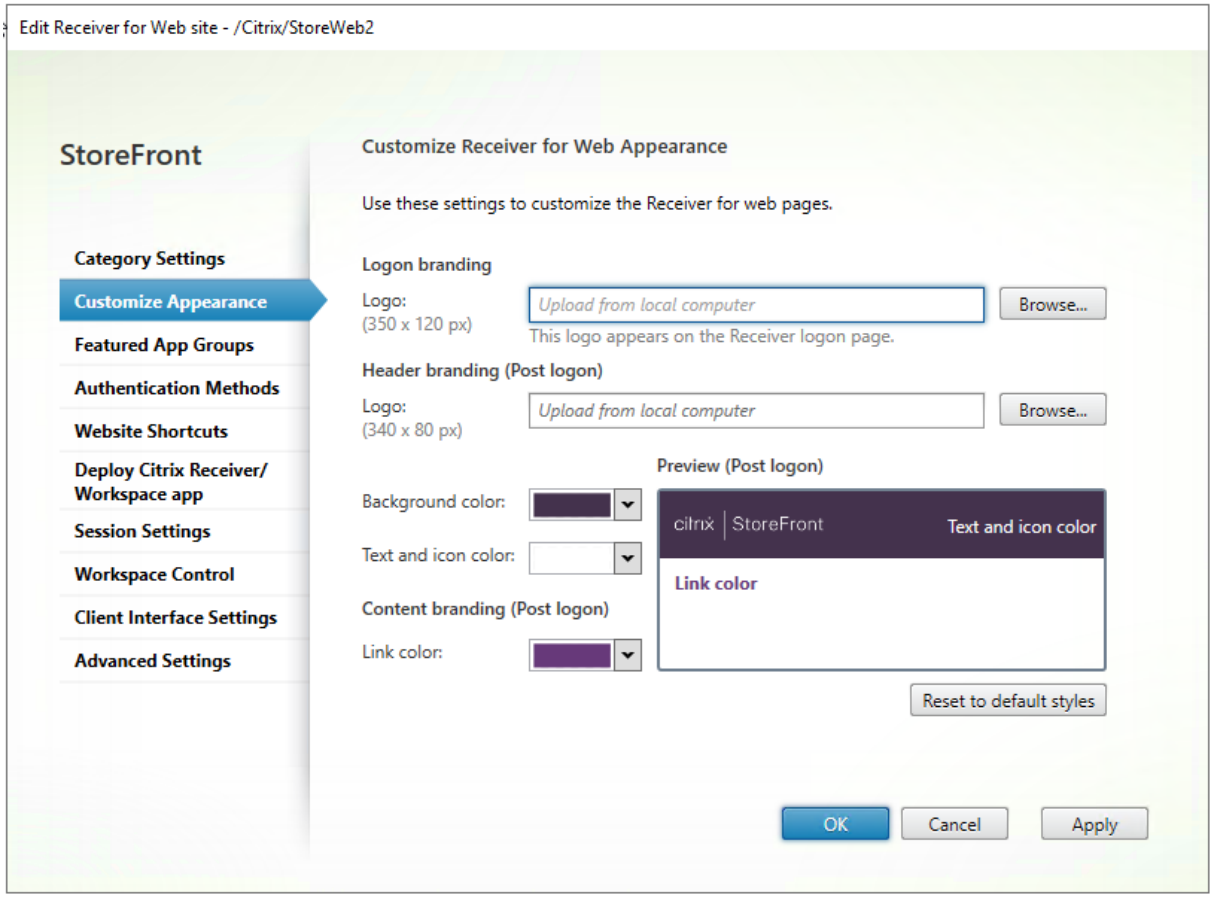
展开 -（默认值）只能选择顶层类别。所选顶层类别下的每个应用程序都可见，按子类别分组。

折叠 - 可以选择顶层类别及其子类别。只有选定类别中的应用程序可见。子类别之间的导航是通过“浏览路径记录”进行的。

统一用户体验中介绍了这些类别视图。

自定义 **Citrix Receiver** 外观

1. 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，依次单击管理 **Receiver for Web** 站点和配置。
3. 选择自定义外观并进行选择以自定义登录后 Web 站点的显示方式。



使用 **Javascript** 和 **CSS** 进一步自定义

> 注意：
>
> 在本部分中的示例中，将 Javascript 添加到 *script.js* 文件(例如在 C:\inetpub\wwwroot\Citrix\StoreWeb\custom 中)，并将 CSS 添加到同一目录中的 *style.css* 文件。

在 **Receiver for Web** 的登录页面中添加静态标头

此处“静态”意味着固定的文本，例如欢迎消息或公司名称。有关更改的内容，例如新闻消息或服务器状态，请参阅在 Receiver for Web 的登录页面中添加动态标头。

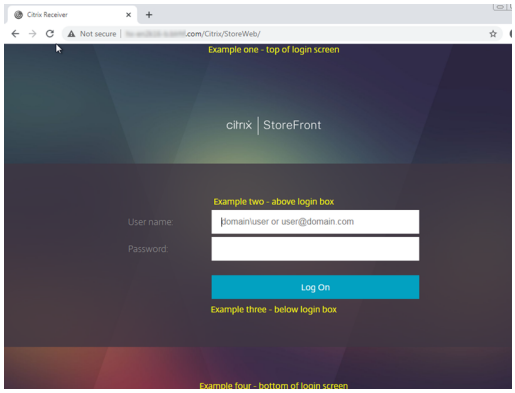
可以使用以下 javascript 行在四个位置添加静态文本：

```
1 $('.customAuthHeader').html(”Example one - top of login screen”);
2 $('.customAuthTop').html(”Example two - above login box”);
3 $('.customAuthBottom').html(”Example three - below login box”);
4 $('.customAuthFooter').html(”Example four - bottom of login screen”);
```


要使文本更加明显，请将以下样式添加到 custom.css 中：

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

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

这将显示以下结果：



要使用 HTML 格式，请将 4 行 javascript 替换为以下内容：

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

> 注意：
>
> 第四个示例行在自定义目录中需要一个名为 *logo.png* 的图像。

在 **Receiver for Web** 的登录页面中添加动态标头

此处“动态”意味着每次都加载和显示某些内容，而非缓存。Web 浏览器通常在可能时缓存内容，但 Citrix Workspace 应用程序始终缓存 UI，并始终加载以前缓存的 UI。这意味着如果您将前面的示例用于服务状态等内容，则不会得到预期的效果。

相反，您需要进行 Ajax 调用以动态加载内容并将其插入页面。为此，您需要：

1. 定义一个有用的实用程序函数，该函数从服务器上的 *\customweb* 目录中的页面获取内容，并将其添加到页面中。这相当于上面的.html 示例，并且自定义页面可以包含文本或 HTML 代码段。请使用 *\customweb* 目录，因为该目录被复制到 StoreFront 服务器组中的所有服务器（就像 \custom 目录一样），但不会下载和缓存。
2. 安排在合适的点调用此函数。过早调用该函数会导致 Citrix Workspace 应用程序中出现问题，因为脚本在配置完全加载之前运行。进行此类操作的好时机是 **beforeDisplayHomeScreen**（但如果您希望在登录页面上显示内容，然后改为使用 **beforeLogin** ）。以下代码处理这两种情况，并且适用于 Web 客户端和本机客户端。

完整的脚本如下：

```
function setDynamicContent(txtFile, element) {

   CTXS.ExtensionAPI.proxyRequest({

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


var fetchedContent=false;
function doFetchContent(callback)
{

  if(!fetchedContent) {

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

  callback();
 }


CTXS.Extensions.beforeDisplayHomeScreen = doFetchContent;
```



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

这将从 *\customweb\readme.txt* 加载内容，默认情况下包含一些不感兴趣的信息。添加您自己的文件 (*status.txt*) 并调整脚本以对其进行调用以获得更有用的结果。

在登录前或登录后显示点击浏览免责声明

以下示例已在 *script.js* 文件中作为示例提供，但需要取消注释。此代码有两个版本：第一个是在 Web 浏览器登录前完成的，第二个是在本机客户端的主 UI 之前完成的。如果您只想要登录后消息，请删除第一个函数。但是，自己使用预先登录消息不是一个好选择，因为登录流只能在 Web 浏览器上看到（而非在本机客户端上）。即使这样，当用户从 Citrix Gateway 访问时，登录流也会被隐藏。

```
var doneClickThrough = false;

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

  doneClickThrough = true;
  CTXS.ExtensionAPI.showMessage({

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

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

  if (!doneClickThrough) {

    CTXS.ExtensionAPI.showMessage({

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



```
    }
   else {

     callback();
    }

}
;
```

使点击浏览免责声明框更宽

用于 **CTXS.ExtensionAPI.showMessage()** 的消息框的样式是预先设置的。可以调整此样式使其更大，以便其他消息看起来正常。将以下示例函数添加到 script.js 中，以便在之后再次收缩样式。希望使用更大的框时，请调用 **showLargeMessage()** 而非 **CTXS.ExtensionAPI.showMessage()** 。

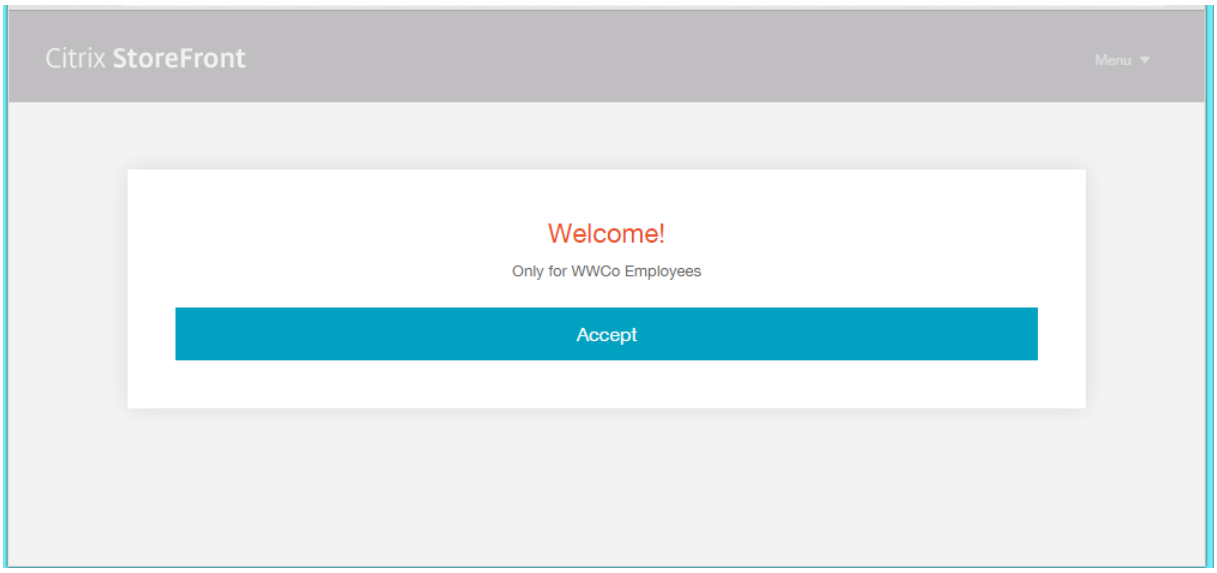
```
function mkLargeMessageExitFn(origfn)
{

  if(origfn) {

    return function() {

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

 }


function showLargeMessage(details)
{

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


显示大消息时，这会添加一个标记类。关闭框时，会在一小段延迟后删除此标记类（需要避免讨厌的“跳转”）。

添加一些 CSS 来根据此标记类的存在调整此框的大小。例如，在 custom\style.css 中尝试以下操作：

```
.largeTiles .largeMessage .messageBoxPopup
{

  width:800px;
 }
```

然后，大型 UI 上显示 messageBoxPopup 并设置了 largeMessage 标志时，宽度为 800 像素。现有代码确保其居中显示。（在移动电话等小型 UI 上，默认消息框已为全宽）。



要挤入更多文本，可以通过将以下内容添加到 custom\style.css 来减小字体大小，或者考虑添加可滚动浏览的内容。

```
.largeTiles .largeMessage .messageBoxText
{

  font-size:10px;
 }
```

使点击浏览免责声明框具有可滚动浏览的内容

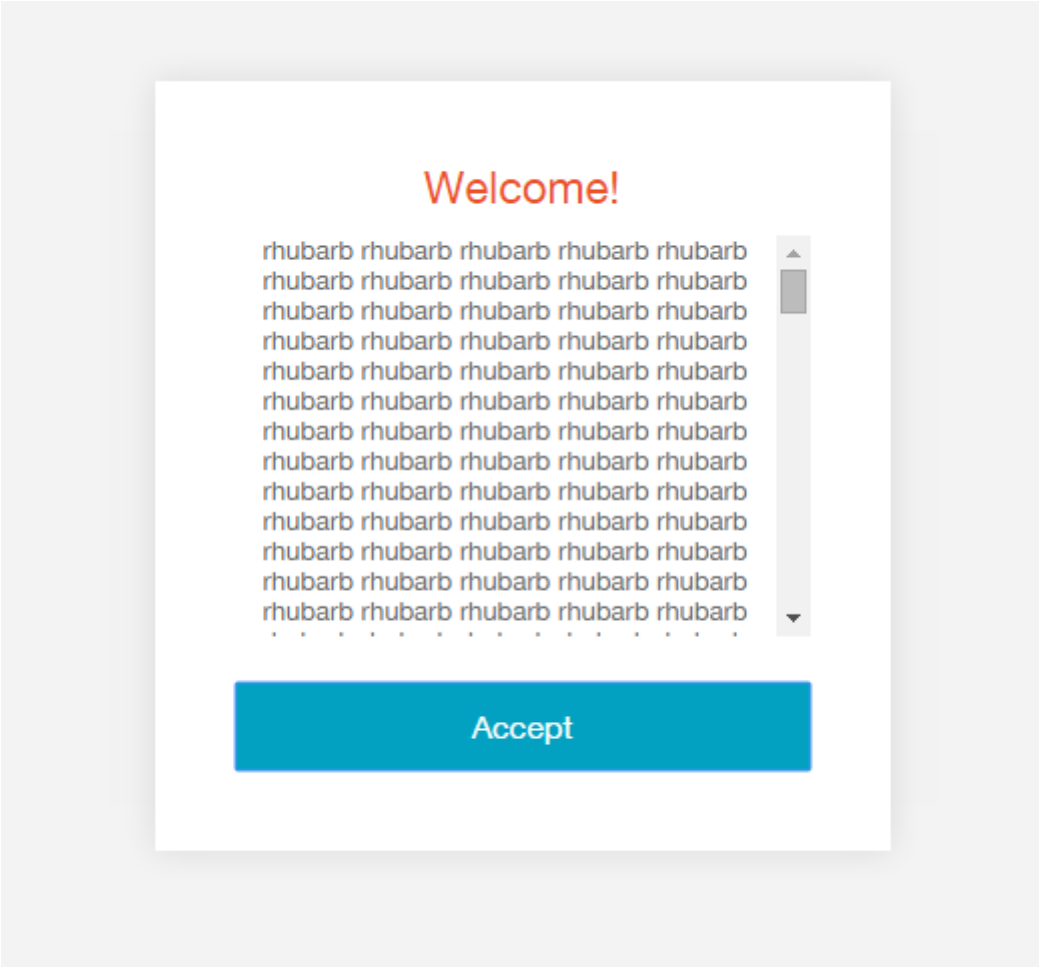
调用 **showMessage** 时，可以传递某些 HTML，而非仅仅一个字符串，以添加样式。要执行此操作，请将以前对 showMessage 的任意示例调用中的 messageText 替换为以下内容：


```
    CTXS.ExtensionAPI.showMessage({

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

然后向 style.css 中添加以下内容：

```
.disclaimer {

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

这将显示以下结果：



向每个页面添加页脚

还有专门针对此的自定义区域。可以添加下面的 Javascript 行来设置其内容：

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

定义 style.css 中的样式。设置 `position:static` 以确保滚动区域按预期工作。

```
#customBottom
{

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


> 注意：
>
> 如果使用脚本动态调整此区域的大小，则必须调用 **CTXS.ExtensionAPI.resize()** 命令以让 Citrix Workspace 应用程序知道某些内容发生了变化。

当用户转到 **“应用程序”** 选项卡时，将文件夹视图设置为默认视图

为此，请监视 “视图更改” 事件。如果 “store”（应用程序视图的内部名称）的视图发生变化，请导航到根文件夹。小心：

- 当 **onViewChange** 事件触发时，表示应用商店视图正在更改，视图尚未完成绘制。因此，如果您立即导航到该文件夹，应用商店视图的初始化代码只会撤消您的工作，因为它将在代码之后运行。为了避免这种情况，请添加 1 毫秒的延迟，以确保您的代码在当前堆栈展开后执行。
- 包含单词 “whitespace” 的三行通过在其上放置一个大型自定义区域来确保初始的 “所有应用程序”UI 脱屏绘制。这将停止 “所有应用程序” 视图在文件夹显示之前闪烁不定。

像往常一样向 script.js 中添加以下代码：

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

CTXS.Extensions.onViewChange = function(view) {

  if (view == ”store”) {

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

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

 }
 ;
```

从同时出现在特色类别中的所有应用程序中隐藏应用程序

可以使用下面的代码来实现这一点。首先记住捆绑包中的每个应用程序，然后从 “所有应用程序显示” 列表中将其删除。

```
var bundleApps = [];
```



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

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

    bundleApps.push(apps[i]);
   }

  defaultfn();
 }
 ;

CTXS.Extensions.filterAllAppsDisplay = function(allapps) {

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

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

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

   }

 }
 ;
```

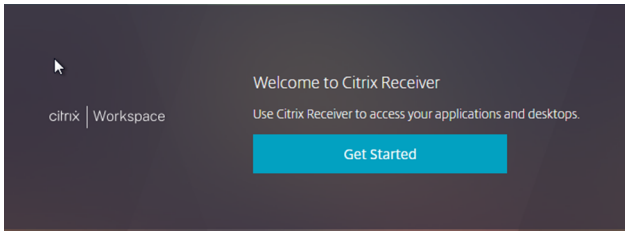
如果使用此自定义，最好将文本字符串“所有应用程序”更改为“其他应用程序”，以避免用户感到困惑。要执行此操作，请编辑自定义目录中的 *strings.en.js* 文件，然后为 **AllAppsTitle** 添加一个标记。例如，更改显示为黄色：

```
(function ($) {

  $.localization.customStringBundle(”en”, {

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


更改默认 **UI** 文本

如果您知道标签的名称，则可以更改 UI 中使用的任何文本。例如，要将 Google Chrome 上的 Receiver for Web 中使用的“安装”屏幕更改为“入门”，请按如下所示添加自定义字符串：

```
(function ($) {

  $.localization.customStringBundle(”en”, {

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



要发现要更改的标签的名称，请执行以下操作：

1. 在 StoreFront 服务器上，查看目录 C:\inetpub\wwwroot\citrix\StoreWeb\receiver\js\localization\en（假设您的应用商店名为“Store”）中的对象。
2. 在记事本中打开文件 *ctxs.strings_something.js*。
3. 查找要更改的字符串。注意：请不要直接编辑此文件，而是像对“install”示例一样在 custom 目录中创建覆盖值。

更改特色类别的背景图像

> 重要：
>
> 请勿尝试覆盖服务器上的图像。这混淆了已下载图像的任何客户端，因为这些客户端不知道图像已经改变。这也使得升级变得难以执行或不可能执行。

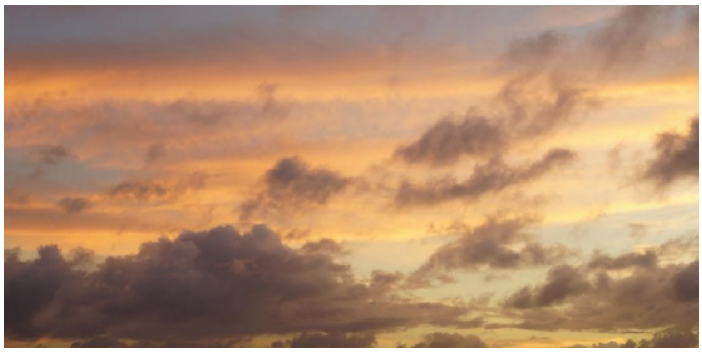
可以将自己的图像添加到 *\custom* 目录，并添加 CSS 以对其进行引用。每个特色类别（内部称为“捆绑”）使用两个图像：

- 第一个图像用作旋转木马中的磁贴。

- 第二个图像用作详细信息页面上的标题后面的背景图像。此图像将拉伸以填充屏幕的宽度，并在底部边缘添加一个 blur。

可以为每个屏幕使用不同的图像。请考虑使用相同的图像，但在详细信息页面中将其背景高度加倍，以便仅显示图像的上半部分。由于图像在详细信息页面上拉伸，因此，请使用变形后看起来很不错的图像。

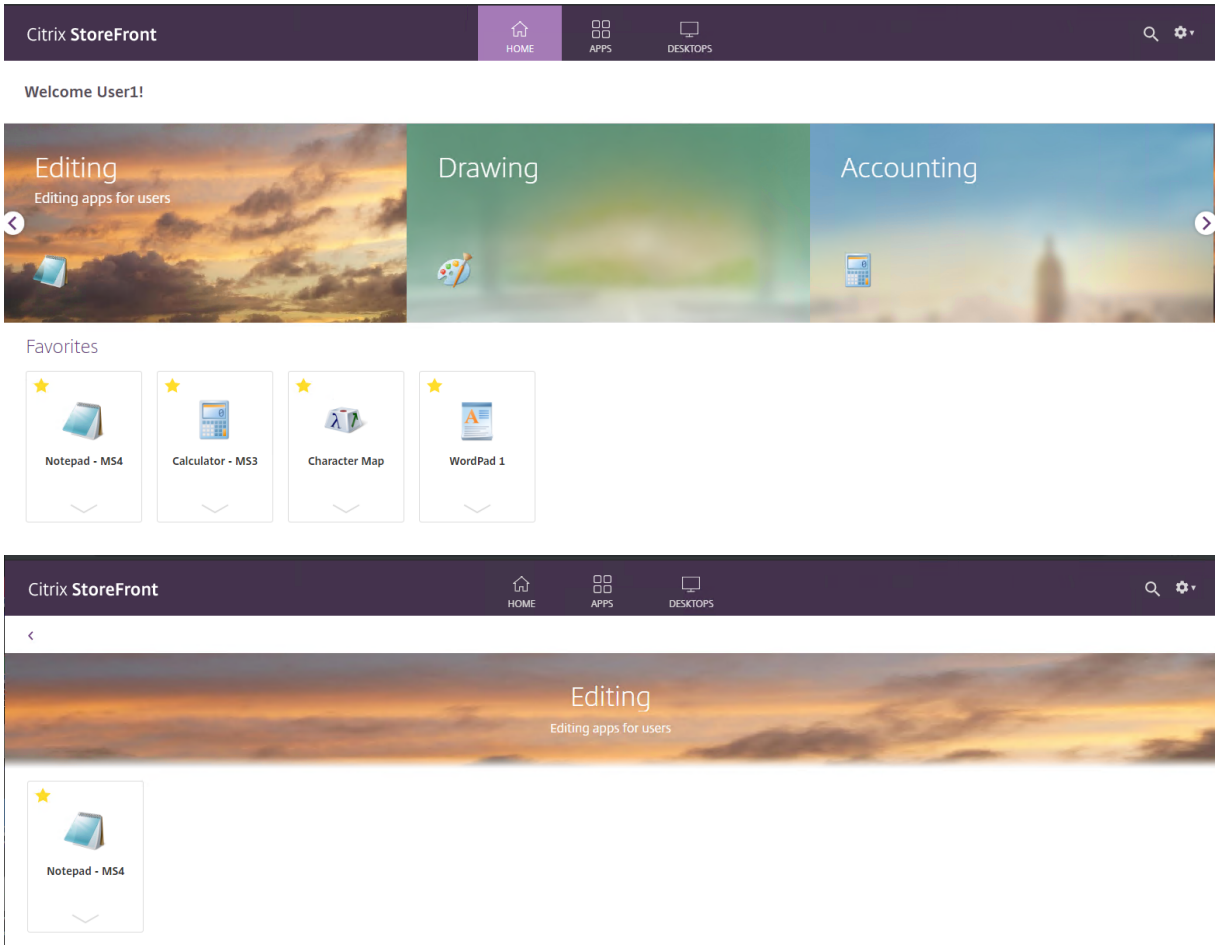
第一个捆绑包具有类 “appBundle1”，第二个具有 “appBundle2”，以此类推，直至 “appBundle8”。以下示例使用图像 “clouds.png”，您可以通过右键单击以下图像进行下载：



1. 将图像保存在 *custom* 目录中。图像需要大约 520 × 256 像素才能与其他像素保持一致（但根据需要缩放）。
2. 将以下内容添加到 style.css 中：

```
.appBundle1 {

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


.bundleDetail.appBundle1 {

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

这将显示以下结果：



防止公司徽标看起来模糊不清

Receiver for Web 需要正确处理常规（“低 DPI”）屏幕和每平方英寸具有更高像素数的新高分辨率（“高 DPI”）屏幕。例如，Apple Retina 屏幕是非视网膜屏幕分辨率的两倍。在便携式计算机上，屏幕通常是 x1.5、x2 甚至 x3，其大小的“正常”像素数。由于 x2 是目前最常见的，并且差异最大，因此，Citrix Workspace 应用程序的大部分图像资源都以两种分辨率提供。正常屏幕上为 100 × 100 像素的图像，也有 200 × 200 像素的 x2 版本。

当您从 StoreFront 管理控制台上载徽标图像时，请确保其属于 x2 图像。换句话说，它们大约是常规屏幕上“空间”的宽度和高度的两倍。（在 x1 上载的图像不会放大到 x2。）常规屏幕上的“空间”为 170 × 40 像素，因此您上载的徽标图像应为 340 × 80 像素。

StoreFront 会创建徽标的副本并将其缩放到一半大小。此图像用于低 DPI 显示器。

有时，这会导致图像模糊，因为一半的图像细节已被丢弃。这是非常罕见的，因为徽标往往轮廓突出且简单。如果您的徽标遇到此问题，请使用以下解决方法：

1. 创建两个版本的徽标，一个是 x1 大小，一个是 x2 大小，并将其保存在 *\custom* 目录中。
2. 编辑 *custom\style.css*，以便其引用这两个不同的图像。这将显示如下所示的内容：


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

.logo-container {

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


.highdpi .logo-container {

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

> 注意：
>
> - 确保这些自定义样式不在“托管部分”内部。否则，这些样式会被覆盖，或者会混淆 StoreFront 管理控制台。
> - 两种样式都指定相同的背景大小。这是因为大小是以“逻辑”单位指定的，对于 x2 图像，背景大小是实际徽标宽度和高度的一半。

设置背景图像

要设置背景图像，请更新位于 `C:\inetpub\wwwroot\Citrix\<STORE>Web\custom` 下的 *Style.css*，其中 `<STORE>` 为将具有自定义设置的应用商店的名称。您指定的图像文件必须位于 `C:\inetpub\wwwroot\Citrix\<STORE>Web\media` 中。

> 注意：
>
> 统一体验专为简单的白色背景而设计。背景图像往往会分散注意力。如果添加背景图像，请尝试使用轻便的图像。如有必要，请调整任何字体，以便其继续针对此图像工作。

示例 **1**：对上载的图像的 **CSS** 引用


```
.large .storeViewSection,
.small .storeViewSection {

    background-image: url('../media/background.jpg');
    background-size: cover;
    background-repeat: no-repeat;
    background-position: center;
    background-attachment: fixed;
    {
 color:#4c9aff }
  }
```

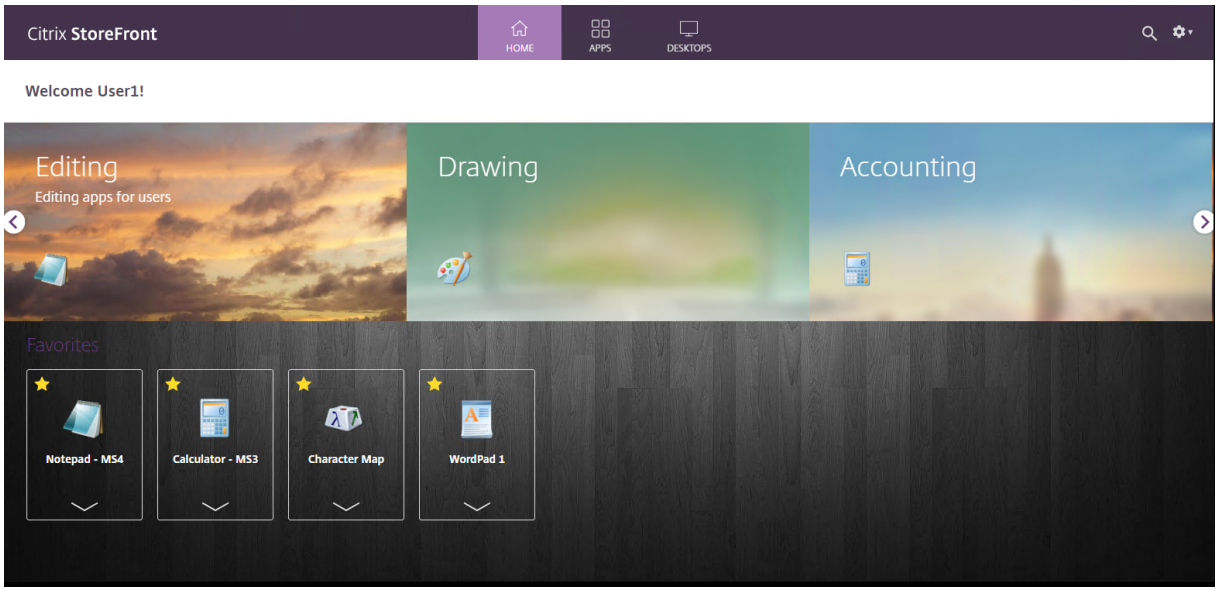
示例 **2**：对现有图像的 **CSS** 引用进行调整

```
.large .storeViewSection,
.small .storeViewSection {

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


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

    color: white;
 }


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

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


.smallTiles .applicationBundleContainer {
```

```
28
29      background-color: rgba(255, 255, 255, 0.4);
30      margin-top: 0;
31      padding-top: 14px;
32  }
```

> 注意：
>
> `background-size:cover;` 语句在某些较旧的浏览器中不起作用。

这将显示以下结果：



查找代码中的错误

有几种方法可以进行调试。请务必先尝试浏览器。这比 Citrix Workspace 应用程序中的调试自定义要容易得多。可以在页面 URL 中的? 或 # 之后添加以下参数，并且可以将多个参数连在一起。例如：

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

-errors — 通常情况下，我们尝试抑制代码中可能出现的任何错误，但您可以改为将其突出显示。出现错误时，此参数会显示一个警报框。

-debug — 此参数禁用自定义代码的任何异常处理。此参数对现代浏览器中内置的开发工具非常有用（如 Google Chrome 或 Internet Explorer 中的 F12），并且在您自己调试异常时非常有用。

-nocustom — 此参数禁用您的脚本和 CSS 自定义。如果 Citrix Workspace 应用程序无法运行，并且您希望了解该应用程序是否是由于您引入的错误所致，则此参数非常有用。

-tr — 此参数提供在单独的浏览器选项卡中跟踪 Citrix Workspace 应用程序 UI 代码，包括通过调用 **CTXS.ExtensionAPI.trace()** 添加的任何跟踪。

统一用户体验

此部分介绍统一体验的功能和外观。

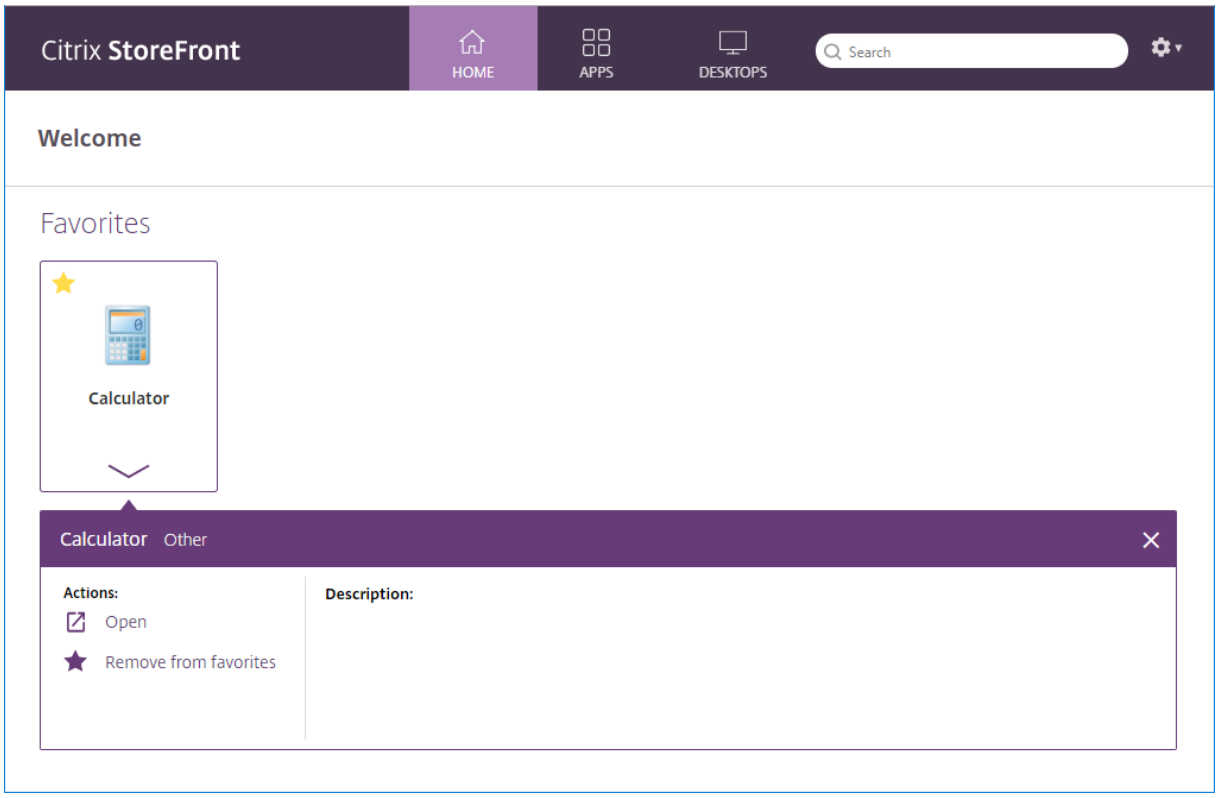
卡布局

应用商店中的应用程序以“卡片”的布局显示。您可以展开每个卡片下面的面板以显示更多详细信息和操作。

> 注意：
>
> 统一体验不允许您使用拖放功能来重新排列应用程序。

主页

主页将显示收藏夹。

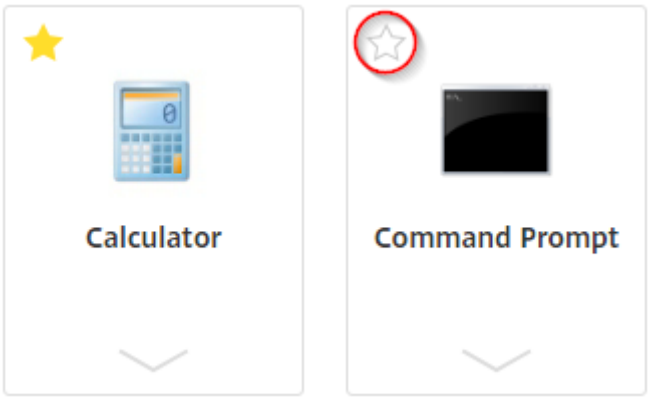


应用程序

应用程序显示已发布的应用程序。可以显示所有应用程序、喜爱的应用程序或应用程序类别。

收藏夹

单击或轻按星形可收藏某个项目：

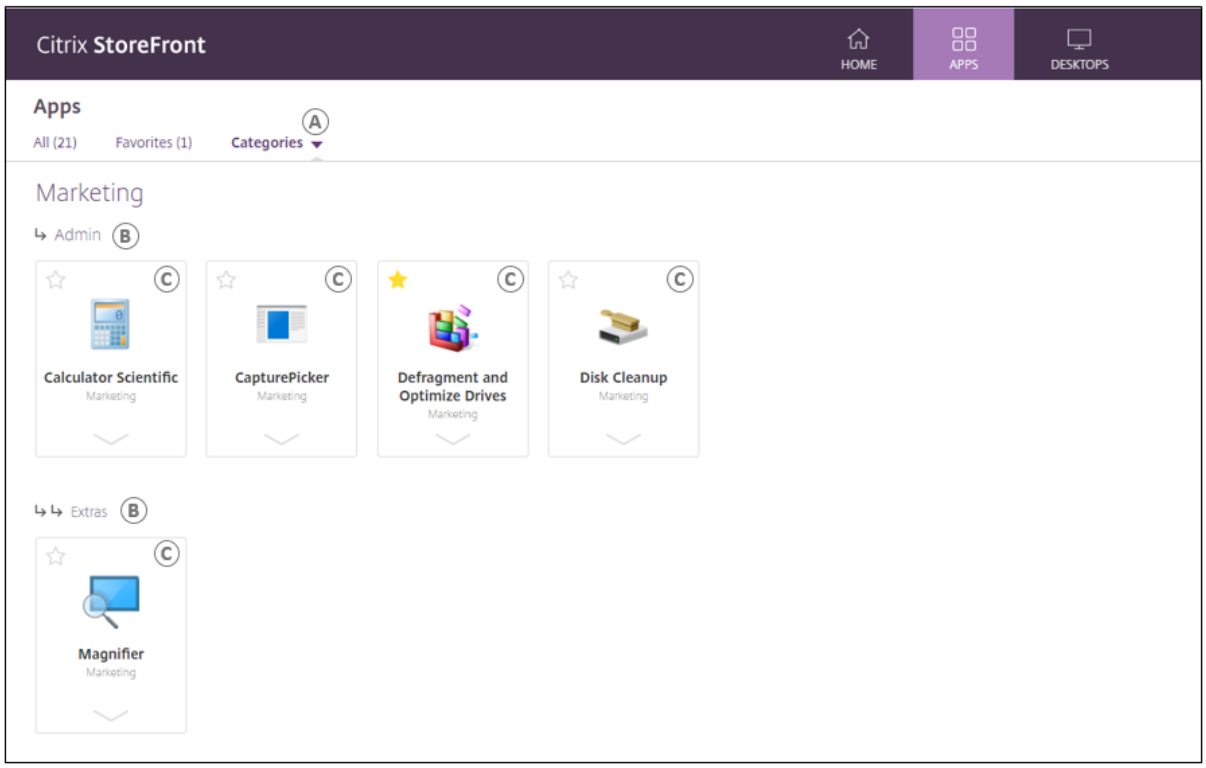


类别

可以将应用程序配置为在“展开”或“折叠”类别中显示。请参阅 配置类别设置。

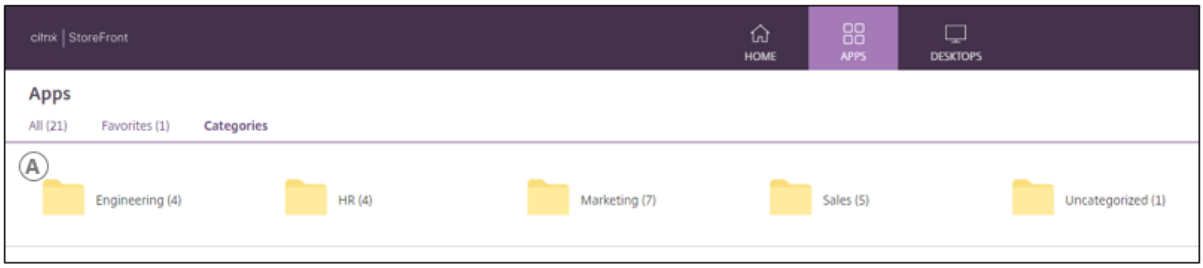
展开的类别视图

在展开的视图中，单击下拉控件 (**A**) 可查看所有顶层类别。选择子类别（例如“市场营销”）时，所有子类别 (**B**) 和所有应用程序 (**C**) 都将显示在一个页面上。

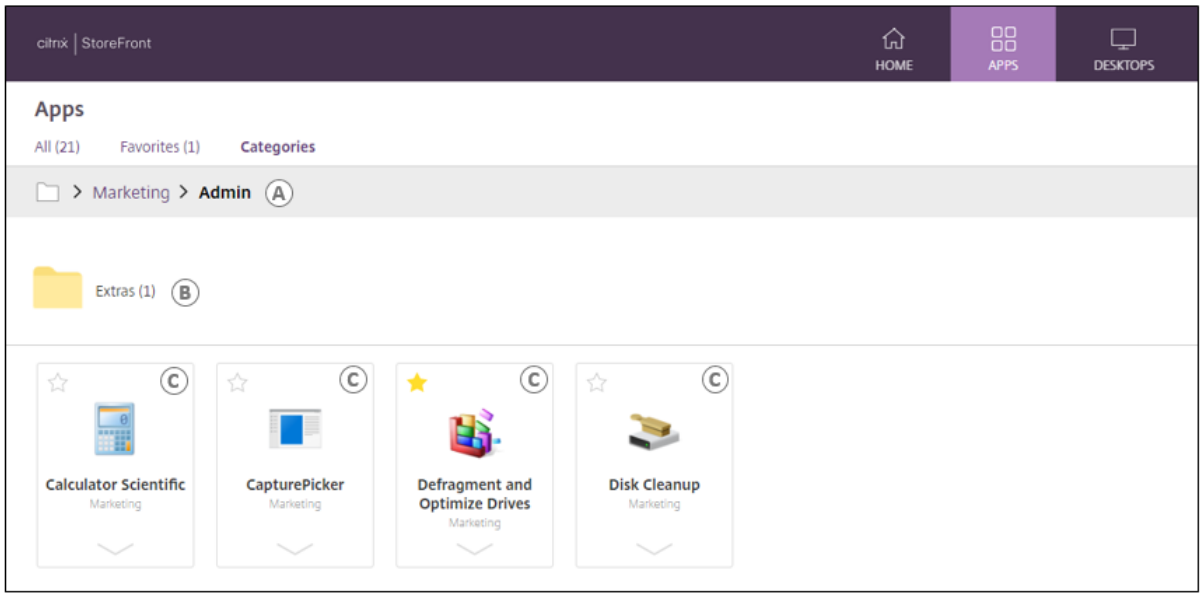


折叠的类别视图

在折叠的视图中，所有顶层类别都显示为文件夹图标 (**A**)。



选择顶层类别时，只有该级别的类别层次结构的内容才可见。选择子类别（例如“管理员”）以查看其中包含的直接子类别 (**B**) 和应用程序 (**C**)。“浏览路径记录”(**A**) 用粗体表示当前位置，允许您浏览多级类别。



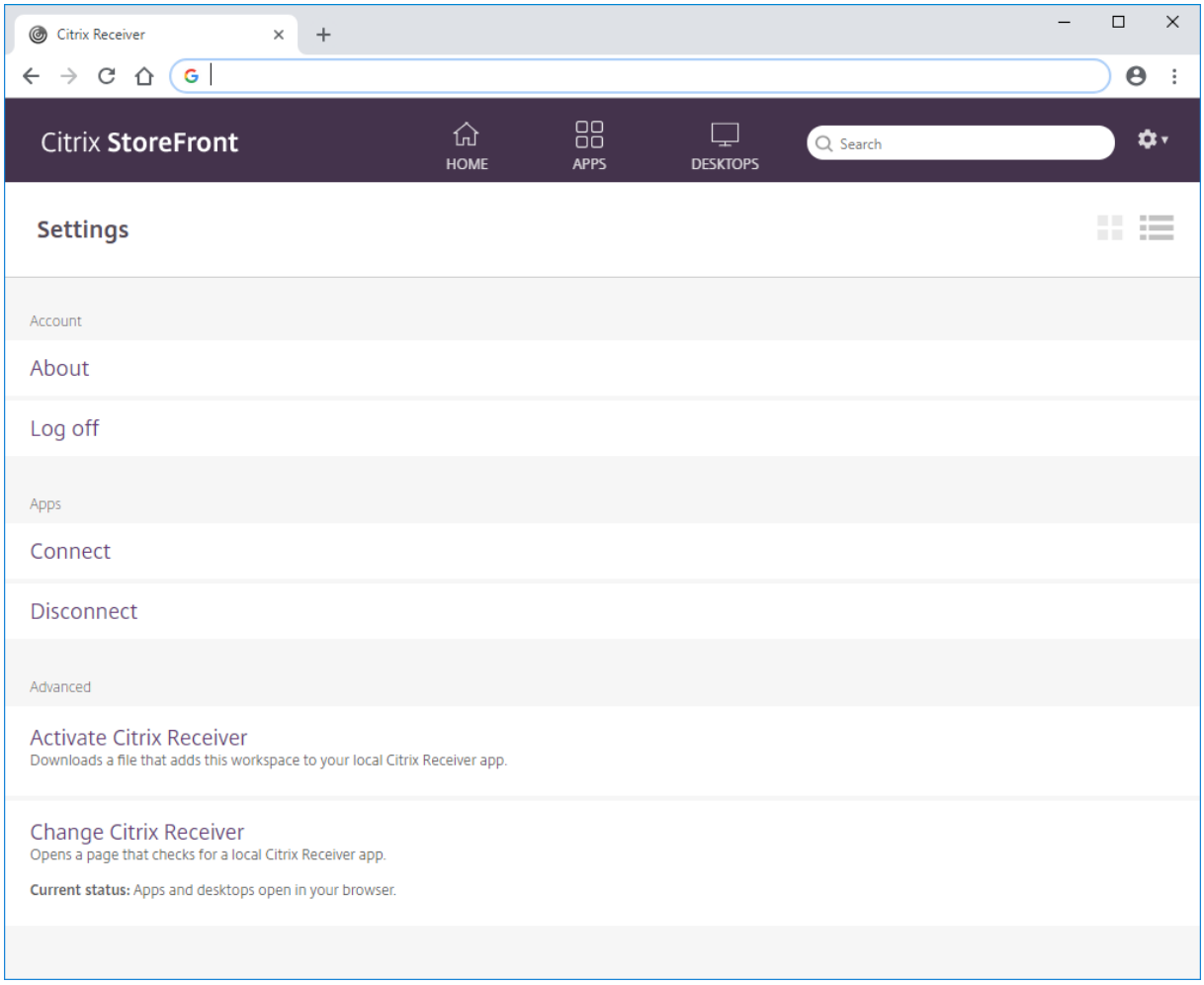
搜索

搜索所有应用程序、桌面和类别：

设置

从下拉菜单中访问设置：

该菜单显示取自 Active Directory 显示名称的用户名。如果显示名称留空（我们不建议如此操作），则将显示域和帐户名称。使用该菜单可打开“设置”页面、检查 Citrix Workspace 应用程序版本或注销。



设置分别允许您恢复任何已断开连接的会话、断开所有当前会话以及注销。以卡片或列表布局显示设置页面：

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 Receiver**。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 Receiver**。此时将打开一个用于检查本地 Citrix Workspace 应用程序的页面。此页面还允许用户在以下操作之间切换：使用本地安装的 Citrix Workspace 应用程序启动资源，或在 HTML5 浏览器中启动资源。

创建和管理精选应用程序

December 2, 2020

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。

可以通过执行精选应用程序组任务添加、编辑或删除精选应用程序组。

> 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，
> 将配置更改传播到服务器组，以便更新部署中的其他服务器。

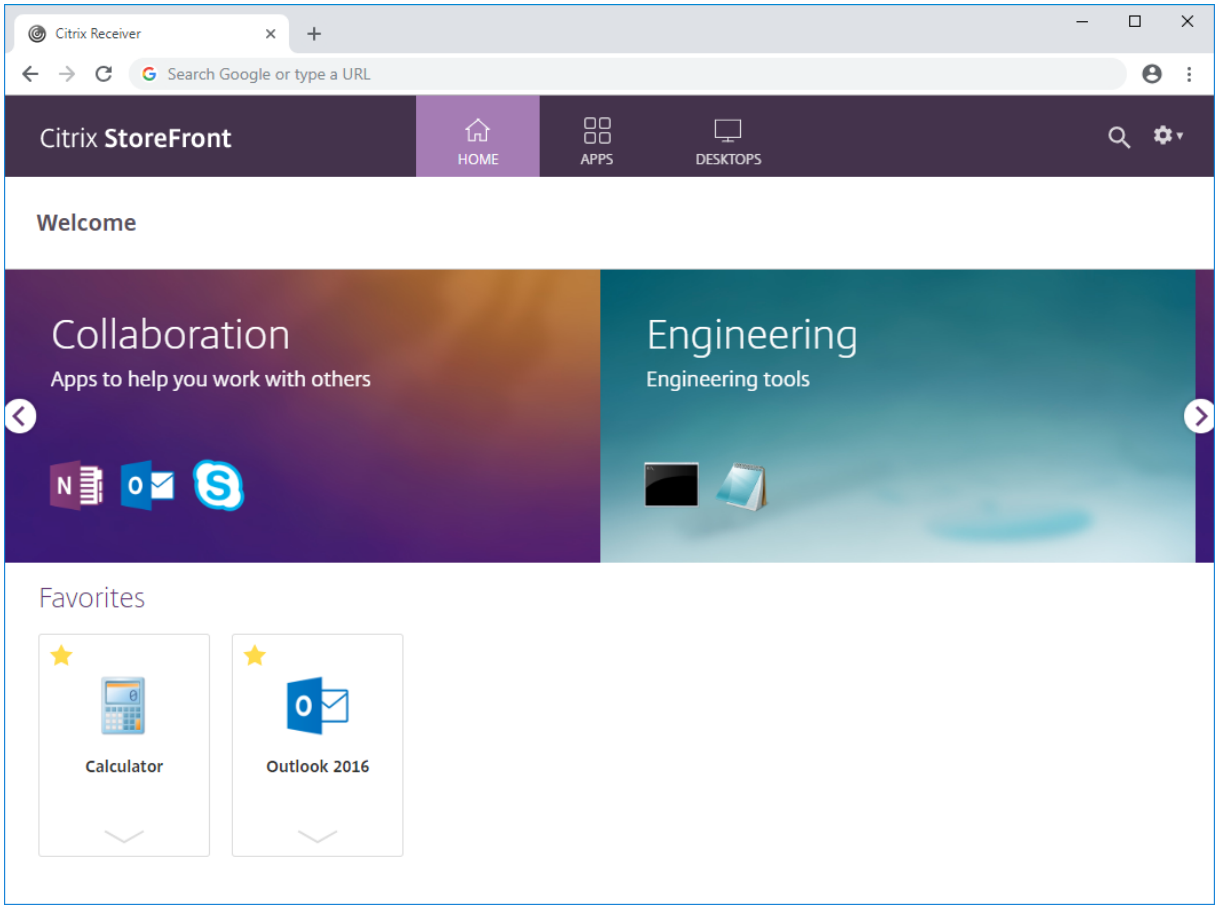
1. 在 Windows 开始屏幕或“应用程序”屏幕中，找到并单击 Citrix **StoreFront** 磁贴。
2. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店节点，然后在“操作”窗格中依次单击管理 **Receiver for Web** 站点和配置。
3. 选择精选应用程序组。
4. 在精选应用程序组对话框中，单击创建定义新的精选应用程序组。
5. 在创建精选应用程序组对话框中，指定精选应用程序组的名称、说明（可选）、背景和精选应用程序组的定义方法。您可以选择关键字、应用程序名称或应用程序类别，然后单击确定。

选项	说明
关键字	在 Studio 中定义关键字。
应用程序类别	在 Studio 中定义应用程序类别。
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。

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。



配置工作区控制

July 27, 2020

工作区控制功能使应用程序能够随用户在设备之间移动。例如，可以使医院的临床医生在不同的工作站之间移动，而无需在每个设备上重新启动自己的应用程序。默认情况下，对 Citrix Receiver for Web 站点启用工作区控制功能。要禁用或配置工作区控制功能，请编辑站点配置文件。

> 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，执行将配置更改传播到服务器组操作，以便更新部署中的其他服务器。

1. 在 Windows 开始屏幕或应用程序屏幕中，找到并单击 Citrix StoreFront 磁贴。
2. 在左侧窗格中选择应用商店，在“操作”窗格中选择管理 **Receiver for Web** 站点，然后单击配置。
3. 选择工作区控制。
4. 配置工作区控制的默认设置，其中包括：

- 启用工作区控制
- 设置会话重新连接选项
- 指定注销操作

配置适用于 **HTML5** 的 **Citrix Workspace** 应用程序对浏览器选项卡的使用

April 12, 2021

默认情况下，适用于 HTML5 的 Citrix Workspace 应用程序会在新浏览器选项卡中启动桌面和应用程序。但是，当用户通过快捷方式使用适用于 HTML5 的 Citrix Workspace 启动资源时，桌面或应用程序会替换现有浏览器选项卡中的 Citrix Receiver for Web 站点，而不是显示在新选项卡中。

> 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，执行将配置更改传播到服务器组操作，以便更新部署中的其他服务器。

1. 在 Windows 开始屏幕或应用程序屏幕中，找到并单击 Citrix StoreFront 磁贴。
2. 在左侧窗格中选择应用商店，在“操作”窗格中选择管理 **Receiver for Web** 站点，然后单击配置。
3. 选择部署 **Citrix Receiver/Workspace** 应用程序。
4. 在部署选项列表中选择始终使用 **Receiver for HTML5**，然后根据要在其中启动应用程序的选项卡，选择或取消选择在与 **Receiver for Web** 相同的选项卡中启动应用程序。

配置用户访问

December 2, 2020

配置对通过 **XenApp Services URL** 进行连接的支持

可以通过执行配置 **XenApp Services** 支持任务配置通过 XenApp Services URL 对应用商店进行访问。使用运行 Citrix Desktop Lock 的重用 PC 的用户，以及使用无法升级的旧版 Citrix 客户端的用户，可以使用应用商店的 XenApp Services URL 直接访问应用商店。创建新应用商店时，将默认启用 XenApp Services URL。

> 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，执行将配置更改传播到服务器组操作，以便更新部署中的其他服务器。

1. 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 **XenApp Services** 支持。

3. 选中或取消选中启用 **XenApp Services** 支持复选框，以允许或禁止用户通过显示的 XenApp Services URL 访问应用商店。

   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的域名，*storename* 为创建应用商店时为其指定的名称。

4. 如果启用 XenApp Services 支持，则可以选择在 StoreFront 部署中为具有 Citrix 联机插件的用户指定默认应用商店。

   指定默认应用商店后，用户可以通过 StoreFront 部署的服务器 URL 或负载平衡 URL（而非特定应用商店的 XenApp Services URL）配置 Citrix 联机插件。

禁用或启用工作区控制重新连接

工作区控制功能使应用程序能够随用户在设备之间移动。例如，可以使医院的临床医生在不同的工作站之间移动，无需在每个设备上重新启动自己的应用程序。

StoreFront 包含一项用于在适用于 Citrix Workspace 应用程序的 Store Service 中禁用工作区控制重新连接的配置。可以使用 StoreFront 控制台或 PowerShell 管理此功能。

使用 **StoreFront** 管理控制台

1. 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。
3. 选择高级设置并选中或取消选中允许重新连接会话。

使用 **PowerShell**

关闭管理控制台，然后运行以下代码段以导入 StoreFront PowerShell 模块：

```
$dsInstallProp = Get-ItemProperty `
-Path HKLM:\SOFTWARE\Citrix\DeliveryServicesManagement -Name InstallDir
$dsInstallDir = $dsInstallProp.InstallDir
& $dsInstallDir\..\Scripts\ImportModules.ps1
```

然后，使用 PowerShell 命令 **Set-DSAllowSessionReconnect** 打开或关闭工作区控制重新连接功能。

语法

```
Set-DSAllowSessionReconnect [[-SiteId] <Int64>] [[-VirtualPath] <String> ]
[[-IsAllowed] <Boolean>]
```

例如，要为 */Citrix/Store* 中的某个应用商店关闭工作区控制重新连接，请使用以下命令配置此应用商店：


```
Set-DSAllowSessionReconnect -SiteId 1 -VirtualPath /Citrix/Store -IsAllowed
 $false
```

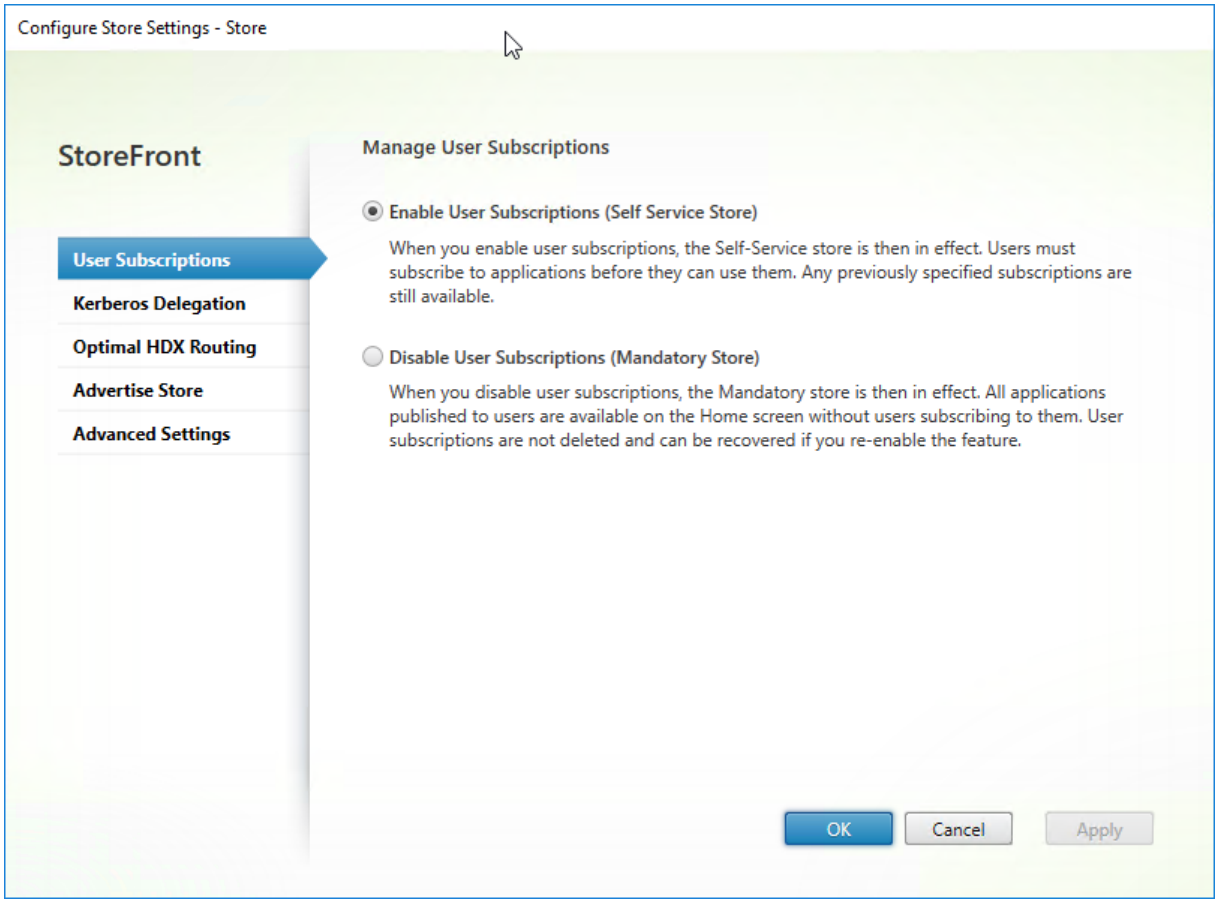
配置用户订阅

可以通过执行“用户订阅”任务选择以下选项之一：

- 要求用户在使用之前订阅应用程序（自助服务应用商店）。
- 允许用户在连接到应用商店时接收所有应用程序（强制性应用商店）。

在 StoreFront 内部禁用用户对某个应用商店的订阅还会阻止在 Citrix Workspace 应用程序中向用户显示“收藏夹”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“收藏夹”中订阅的应用程序。

1. 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 > 用户订阅以关闭或打开用户订阅功能。
3. 选择启用用户订阅 **(**自助服务应用商店**)** 以确保用户订阅应用程序以便使用。以前指定的任何订阅仍可用。
4. 选择禁用用户订阅 **(**强制性应用商店**)** 以使在用户未订阅的情况下为用户发布的所有应用程序在主屏幕上可用。其订阅不会被删除，如果您重新启用该功能，可以将其恢复。



在 StoreFront 3.5 或更高版本中，可以使用以下 PowerShell 脚本配置应用商店的用户订阅：

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath ”/citrix/<
    yourstore>”
Set-STFStoreService -StoreService $StoreObject -LockedDown $True -
    Confirm:$False
```

有关 Get-STFStoreService 的详细信息，请参阅 https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Get-STFStoreService/

将 **StoreFront** 配置为在窗口化模式下启动应用程序和桌面

June 5, 2020

无缝地启动应用程序取决于部署的 StoreFront 的可用性。如果禁用应用程序和桌面的无缝选项，请考虑在窗口化模式下启动您的资源。

下面是已发布的记事本的示例。使用的已发布应用程序的名称与 Citrix Virtual Apps and Desktops 控制台的应用程序集中显示的名称完全相同。

> 注意：
>
> 除 DesiredHRES 和 DesiredVRES 设置之外，ICA 文件中的大部分设置不区分大小写。应用窗口化的应用程序版本时，请使用浏览器名称来引用 StoreFront 服务器上 *default.ica* 文件中的应用程序。在 Delivery Controller 上使用 PowerShell 来验证应用程序的浏览器名称：
>
> ```
> >>asnp citrix*
> ```
>
> ```
> >>Get-BrokerApplication -ApplicationName
> ```

配置 StoreFront

1. 编辑 StoreFront 服务器上的 \inetpub\wwwroot\Citrix\StoreName\App_Data 目录中的 default.ica 文件。
2. 在 default.ica 文件中，找到以下行：[ApplicationServers] application=。
3. 在 application= 后创建一行并添加以下参数：

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


4. 保存该文件。

对于 Citrix Virtual Apps and Desktops 7.x 和 StoreFront 3.x 中的已发布应用程序

1. 编辑 StoreFront 服务器上的 `C:\inetpub\wwwroot\Citrix\storeWeb` 目录中的 *web.config* 文件。
2. 在 web.config 文件中，找到以下行：`showDesktopViewer=''true''`。
3. 将该值从 **True** 修改为 **False**。
4. 在客户端上或从 AD-GPMC 中，使用管理模板文件（`receiver.adm` 或 `receiver.admx\receiver.adml`，取决于操作系统）配置以下策略：
   - 计算机配置 **> Citrix** 组件 **> Citrix Receiver >** 用户体验 **>** 客户端显示设置**:** 启用
   - 无缝窗口：**False**
   - 窗口宽度：**<As per requirement>**，窗口高度：**<As per requirement>**

备注

可以将 `DeisredHRES` 和 `DesiredVRES` 设置为任何所需的分辨率，例如 800x600 或 1024x768。

如果应用程序需要以屏幕大小的百分比运行，则在设置 `TWIMode=Off` 后，添加将屏幕设置为 90% 的行 `ScreenPercent=90`。您还可以在 XenApp Services 站点中完成此操作。确保编辑该站点 (Inetpub\wwwroot\Citrix\PNAgent\conf) 的 `conf` 文件夹下的相应文件。

如果您使用 10.x 客户端并编辑 **`default`**`.ica` 或 `template.ica` 文件，则只能添加 `TWIMode=Off` 行。该行从已发布的应用程序属性获取 `HRES` 和 `VRES` 设置。否则，当用户尝试启动应用程序时会出现错误，指示 ICA 文件中条目重复。

配置通信和会话超时

April 12, 2021

配置通信超时和重试次数

默认情况下，Citrix Receiver for Web 站点对关联应用商店的请求将在三分钟后超时。通信尝试失败一次后，应用商店将被视为不可用。可以通过执行会话设置任务更改默认设置。

> 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，执行将配置更改传播到服务器组操作，以便更新部署中的其他服务器。

1. 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 管理 **Receiver for Web** 站点，然后单击配置。
3. 选择会话设置，进行更改，然后单击确定/应用保存所做的更改。

配置会话超时

如果未在 StoreFront 上正确配置会话超时，用户可能会看到以下消息：“由于不活动，您的会话已超时。”您可以重置会话超时值来延长不活动计时器，以适合用户的使用模式。

请完成以下步骤以在 StoreFront 上配置会话超时：

更改 **Citrix Receiver for Web** 的会话超时

要为通过 Citrix Receiver for Web 访问 StoreFront 应用商店的用户配置会话超时，请执行此处描述的配置。这对用户通过 Citrix Workspace 应用程序进行访问没有任何影响。

1. 在 StoreFront 上，导航到 `c:\inetpub\wwwroot\Citrix\<StoreWeb>`。
2. 在 `web.config` 文件中，找到相应的条目：`<sessionState timeout="20"/>`。
3. 将 `sessionState timeout` 更改为所需的值，以分钟为单位。

如果将 Citrix Receiver for Web 的会话超时配置为超过 **1** 小时，则还必须在身份验证服务中相应地增加令牌最长使用时间。

1. 在 StoreFront 服务器上，导航到应用商店的身份验证服务的路径。
   - 如果 Storefront 安装在自己的服务器上，并且您使用 StoreFront 管理控制台创建应用商店 `<Store>`，则此路径为 `c:\inetpub\wwwroot\Citrix\<Store>Auth`。
   - 如果 StoreFront 和 Delivery Controller 安装在同一服务器上，使用 Citrix Studio 创建 Citrix Virtual Apps and Desktops 站点时将创建默认应用商店。在这种情况下，应用商店的身份验证服务的路径为 `c:\inetpub\wwwroot\Citrix\Authentication`。
2. 在 `web.config` 文件中，找到类似以下内容的身份验证令牌生成器服务部分：

```
1 <tokenManager>
2     <services>
3     <clear />
4     <service id="9c84499f-3781-42d3-b3e0-2a12efebaa8d" displayName
          ="Authentication Token Producer">
5         <relyingParties signingId="462fc209-ecad-44a7-aacb-
              b75a11b6203a"
6         defaultLifetime="01:00:00" maxLifetime="01:00:00">
```


3. 请仅在本部分中的 <defaultLifetime="01:00:00"maxLifetime="01:00:00"> 条目中，将 maxLifetime 更改为所需的值。完整的生存期格式为 .d.hh:mm:ss[.ff]。最大生命周期内不受限制到 24 小时。

如果将 Citrix Receiver for Web 的会话超时配置为超过 **8** 小时，则还必须在 StoreWeb 中适当地增加令牌的使用时间。

1. 导航到文件系统中的 StoreWeb，默认为 c:\inetpub\wwwroot\Citrix\<Store>Web。
2. 在 web.config 文件中，找到类似以下内容的部分：

```
<citrix.deliveryservices>
  <webReceiver>
    <serverSettings>
      <authentication tokenLifeTime="08:00:00" locationURL="Authentication/GetAuthMethods">
```

3. 将 tokenLifeTime 更改为所需的值。完整的生存期格式为 .d.hh:mm:ss[.ff]。最大生命周期内不受限制到 24 小时。

更改 **Citrix Workspace** 应用程序的会话超时

要为通过 Citrix Workspace 应用程序访问 StoreFront 应用商店的用户配置会话超时，请执行此处描述的配置。这对用户通过 Receiver for Web 进行访问没有任何影响。

1. 在 StoreFront 服务器上，导航到应用商店的身份验证服务的路径。
   - 如果 Storefront 安装在自己的服务器上，并且您使用 StoreFront 管理控制台创建应用商店 <Store>，则此路径为 c:\inetpub\wwwroot\Citrix\<Store>Auth。
   - 如果 StoreFront 和 Delivery Controller 安装在同一服务器上，使用 Citrix Studio 创建 Citrix Virtual Apps and Desktops 站点时将创建默认应用商店。在这种情况下，应用商店的身份验证服务的路径为 c:\inetpub\wwwroot\Citrix\Authentication。
2. 在 web.config 文件中，找到 **Authentication Token Producer** 服务部分。

```
<service id="cfff7b1d-1cee-4241-93cd-b81aaca38856" displayName="Authentication Token Producer">
  <relyingParties signingId="8973bf5a-a523-4315-bad1-965246a66c63"
    defaultLifetime="01:00:00" maxLifetime="01:00:00">
    <add id="cfff7b1d-1cee-4241-93cd-b81aaca38856" encipherId="8973bf5a-a523-4315-bad1-965246a66c63"
      defaultLifetime="01:00:00" maxLifetime="20:00:00" />
    <add id="21d8b9df-8da9-4227-9687-e6abb5aba429" encipherId="8973bf5a-a523-4315-bad1-965246a66c63" />
    <add id="45e8ba75-ef9a-4ed4-bdc4-f454734d211f" encipherId="fc2dc08f-d5e9-4453-9a3a-621cbce14ca4" />
    <add id="59287a0b-2e19-40c9-85b4-2d21f1a2e9dd" encipherId="d83082ca-aa06-4e49-9003-2c9c81912553" />
  </relyingParties>
```

3. 将指示的 maxLifetime 更改为所需的值，以分钟为单位。完整的生存期格式为 .d.hh:mm:ss[.ff]。最大生命周期内不受限制到 24 小时。

> 注意：
>
> 在注销或会话超时后，通过 Citrix Workspace 应用程序访问 StoreFront 应用商店的用户可能会在后台看到 Citrix Virtual Apps and Desktops。但是，当他们在 StoreFront 会话超时后单击任何应用程序或桌面时，都需要再次输入凭据。StoreFront 会话超时后，任何已启动的应用程序或桌面都不会注销。

重新启动 **IIS**

运行 `iisreset` 命令以应用所做的更改。运行此命令会将用户从 Citrix Receiver for Web 中注销，并且不会影响当前 ICA 会话。

其他资源

- 安全令牌服务 API

设置高可用性多站点应用商店配置

December 2, 2020

> 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，执行将配置更改传播到服务器组操作，以便更新部署中的其他服务器。

对于从多个部署（特别是地理位置分散的部署）聚合资源的应用商店，可以在部署之间配置负载平衡和故障转移、配置到部署的用户映射以及配置特定灾难恢复部署，以提供高可用资源。如果已为部署配置了单独的 Citrix Gateway 设备，则可以为用户定义用于访问每个部署的最佳设备。

配置用户映射和聚合

在 StoreFront 管理控制台中，可以执行以下操作：

- 将用户映射到部署：根据 Active Directory 组成员身份，可以限制能够访问特定部署的用户。
- 聚合部署：可以指定哪些部署包含您要聚合的资源。聚合部署中的匹配资源将作为一个高可用资源提供给用户。
- 将区域与部署相关联：在全局负载平衡配置中通过 Citrix Gateway 进行访问时，StoreFront 在启动资源时会优先启动匹配网关区域的区域中的部署。

1. 确保为应用商店配置了要在配置中使用的所有 Citrix Virtual Apps and Desktops 部署的详细信息。有关在应用商店中添加部署的详细信息，请参阅管理通过应用商店提供的资源。
2. 在 Windows 开始屏幕或应用程序屏幕中，找到并单击 **Citrix StoreFront** 磁贴。
3. 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**。
4. 如果定义了两个或多个 Controller，请单击用户映射和多站点聚合配置 **>** 配置。
5. 单击将用户映射到 **Controller**，然后在屏幕上做出选择以指定哪些 Delivery Controller 对哪些用户可用。
6. 单击聚合资源以聚合来自多个部署的资源。聚合 Delivery Controller 时，Delivery Controller 中显示名称相同的应用程序和桌面将在 Citrix Workspace 应用程序中以单个应用程序或桌面的形式显示。

a) 要聚合 Delivery Controller，请选择多个 Controller 并单击聚合。

b) 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部署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。

7. 在“用户映射和多站点聚合配置”对话框中，单击确定。
8. 在“管理 Delivery Controller”对话框中，单击确定：

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。还可以使用 PowerShell 或者通过编辑 StoreFront 配置文件来配置 StoreFront，后者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。
- 能够定义灾难恢复部署（仅在所有其他部署都不可用时才访问的部署）。

> 警告：
>
> 通过手动编辑配置文件配置高级多站点选项后，有些任务在 Citrix StoreFront 管理控制台中将不可用，以防止错误配置。

1. 确保为应用商店配置了要在配置中使用的所有 Citrix Virtual Apps and Desktops 部署（包括灾难恢复部署）的详细信息。有关在应用商店中添加部署的详细信息，请参阅管理通过应用商店提供的资源。
2. 使用文本编辑器打开应用商店的 web.config 文件，该文件通常位于 C:\inetpub\wwwroot\Citrix\storename 目录中，其中 storename 为创建应用商店时为其指定的名称。
3. 在此文件中查找以下部分。

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

4. 指定如下所示的配置。


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

使用以下元素定义配置。

- **userFarmMapping** - 指定部署组，并定义这些部署之间的负载平衡和故障转移行为。确定用于灾难恢复的部署。在 Microsoft Active Directory 用户组与指定的部署组之间建立映射，从而控制用户对资源的访问。
- **groups** - 指定关联的映射要应用到的 Active Directory 用户组的名称和安全标识符 (SID)。必须使用域\用户

组格式输入用户组名称。虽然列出了多个组，但映射仅应用于属于所有指定组的成员的用户。要允许所有 Active Directory 用户帐户进行访问，可将组名称和 SID 设置为 **everyone**。

- **equivalentFarmSet** - 指定一组可以提供要汇聚的资源的等效部署（用于实现负载平衡或故障转移），以及可选的灾难恢复部署关联组。

  loadBalanceMode 属性决定如何向部署分配用户。将 **loadBalanceMode** 属性的值设置为 **LoadBalanced**，可以将用户随机分配给等效部署集中的部署，从而在所有可用部署之间平均分配用户。如果 **loadBalanceMode** 属性的值设置为 **Failover**，用户将按照在配置中列出的顺序连接到第一个可用部署，从而将在任意给定时间所使用的部署数量降至最低。指定聚合组的名称，以标识可提供要聚合的资源的等效部署集。此时将聚合属于同一聚合组的等效部署集所提供的资源。要指定在某个特定等效部署集中定义的部署不应与其他部署汇聚，可将聚合组名称设置为空字符串 **”“**。

  identical 属性接受值 **true** 和 **false**，并指定等效部署集中包含的所有部署是否提供完全相同的一组资源。如果部署相同，StoreFront 将仅枚举部署集中的一个主要部署中的用户资源。如果部署提供重叠但不同的资源，StoreFront 将枚举每个部署中的资源，以获取一组对用户可用的完整资源。无论部署是否相同，都会进行负载平衡（在启动时）。**identical** 属性的默认值为 **false**，即使在升级 StoreFront 以避免更改预先存在的升级后行为时设置为 **true** 也是如此。

- **primaryFarmRefs** - 指定一组等效的 Citrix Virtual Apps and Desktops 站点，其中包含的部分或全部资源匹配。输入已添加到应用商店中的部署的名称。指定的部署名称必须与您将部署添加到应用商店中时所输入的名称完全一致。

- **optimalGatewayForFarms** - 指定部署组并定义用户访问这些部署所提供的资源时所使用的最佳 Citrix Gateway 设备。用于部署的最佳设备所在的地理位置通常与该部署相同。只需要为用户访问 StoreFront 所用的设备不是最佳设备的部署定义最佳 Citrix Gateway 设备。

配置订阅同步

要配置对不同 StoreFront 部署中的应用商店中的用户订阅进行定期下拉同步，可以执行 Windows PowerShell 命令。

> 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。

创建订阅同步时请注意，已配置的 Delivery Controller 在已同步的应用商店之间必须具有相同的名称，并且 Delivery Controller 名称区分大小写。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，*XenDesktop7* 与 *Xendesktop7* 不同。

1. 使用具有本地管理员权限的帐户启动 Windows PowerShell ISE。
2. 要配置在每天的特定时间进行同步，请运行以下命令。


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

使用 **-StartTime** 指定同步计划的开始时间。使用 **(Get-Date -Format t)** 可立即启动同步计划，而指定 *10:00* 将在指定时间启动重复计划。

-RepeatMinutes 设置计划将运行的频率。例如，*30* 将每半小时运行一次计划，*180* 将每 3 小时运行一次计划。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"
   ```

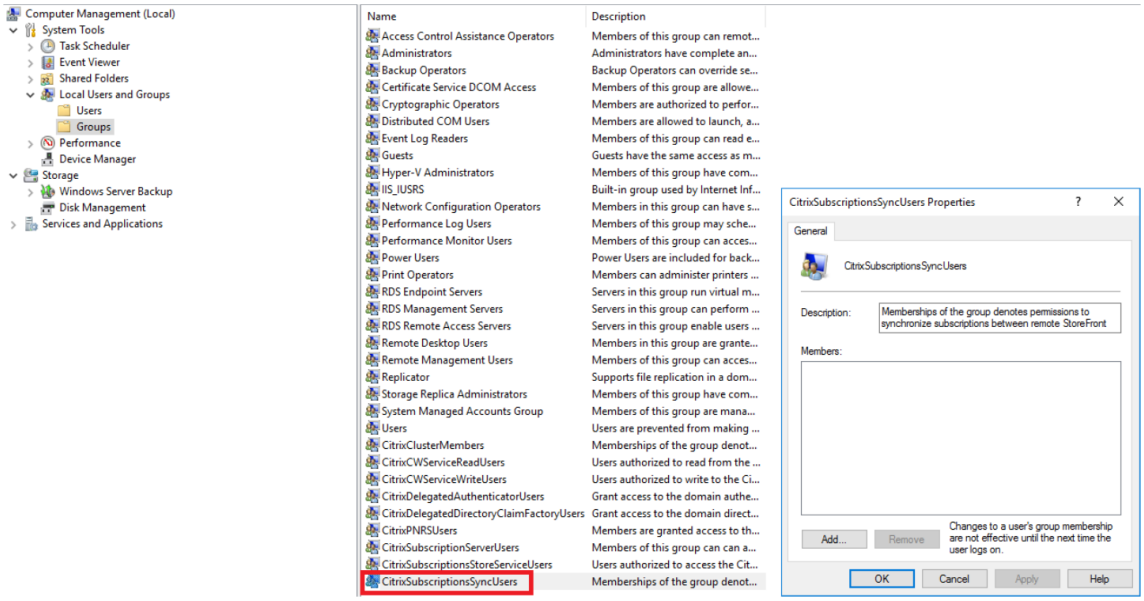
   - 在英国数据中心 StoreFront 服务器上运行，以从美国数据中心服务器提取数据：

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

   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。

```
1 Publish-STFServerGroupConfiguration
```

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。

```
1 Clear-STFSubscriptionSynchronizationSchedule
```

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。

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

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。

```
1 Clear-STFSubscriptionSynchronizationSource
```

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
```

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
```

为应用商店配置最佳 **HDX** 路由

为应用商店定义最佳网关映射时场与区域之间的区别

在 3.5 之前的 StoreFront 版本中，只能将最佳网关映射到一个或多个场。按照区域的概念，您可以根据 Citrix Virtual Apps and Desktops 控制器和已发布的资源所在的数据中心或地理位置将 Citrix Virtual Apps and Desktops 部署划分到几个区域中。Citrix Virtual Apps and Desktops Studio 中定义区域。StoreFront 与 Citrix Virtual Apps and Desktops 交互，并且在 StoreFront 中定义的所有区域都必须与在 Citrix Virtual Apps and Desktops 中定义的区域名称相匹配。

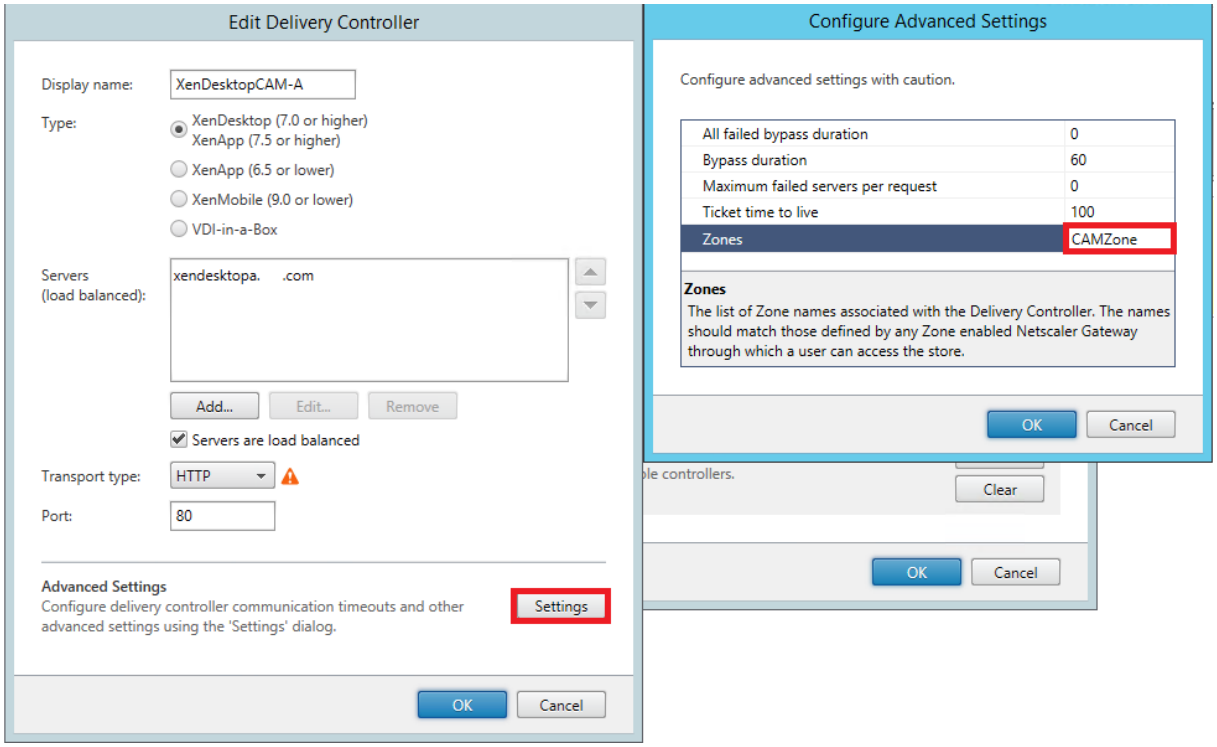
StoreFront 还允许您为所定义的区域中的所有 Delivery Controller 创建最佳网关映射。将区域映射到最佳网关与使用场创建映射基本相同，您可能已熟悉后者的操作。唯一的区别在于区域通常代表规模更大的、包含更多 Delivery Controller 的容器。不需要向最佳网关映射中添加每个 Delivery Controller。要将 Controller 放置到所需的区域中，只需使用与已在 Citrix Virtual Apps and Desktops 中定义的区域匹配的区域名称标记每个 Delivery Controller 即可。可以将一个最佳网关映射到多个区域，但您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。

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 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**。
3. 选择一个 Controller，单击编辑，然后单击编辑 **Delivery Controller** 屏幕上的设置。
4. 在区域行中，单击第二列。
5. 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 Citrix Gateway 路由，以优化从 HDX Engine 路由到使用 StoreFront 的已发布资源（例如，XenDesktop VDA 或 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。

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

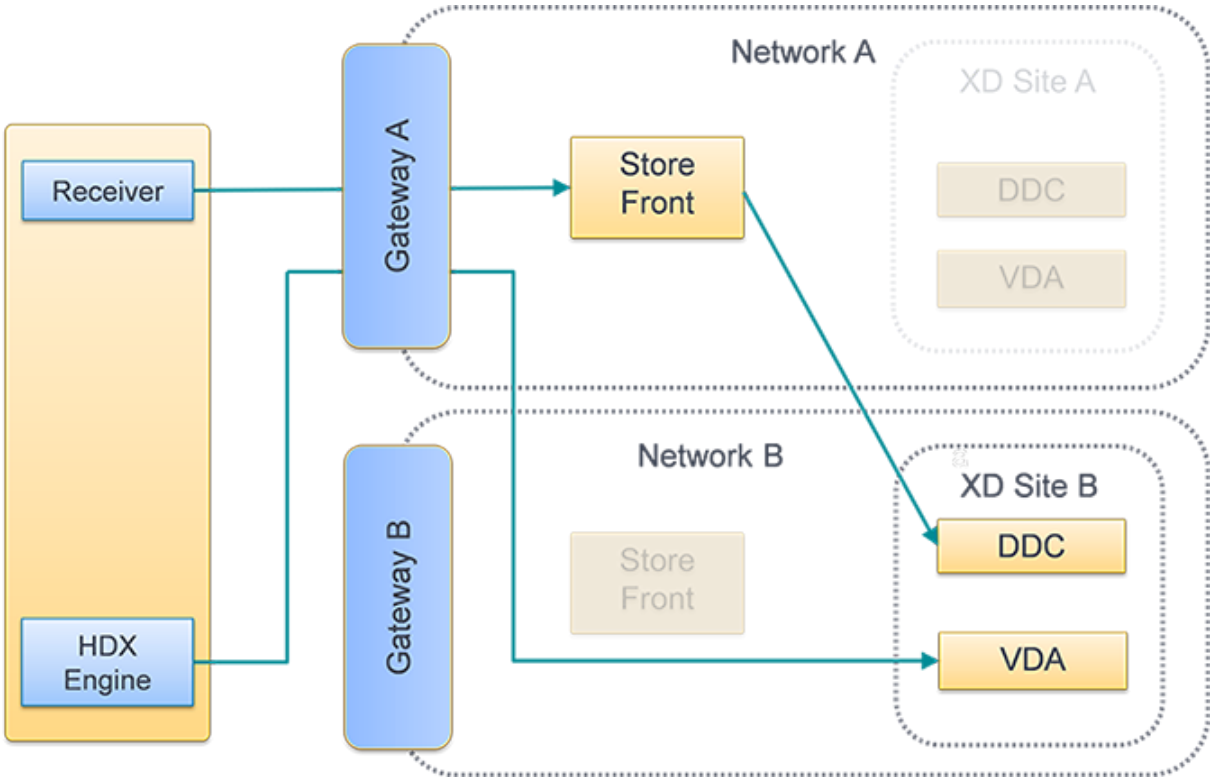
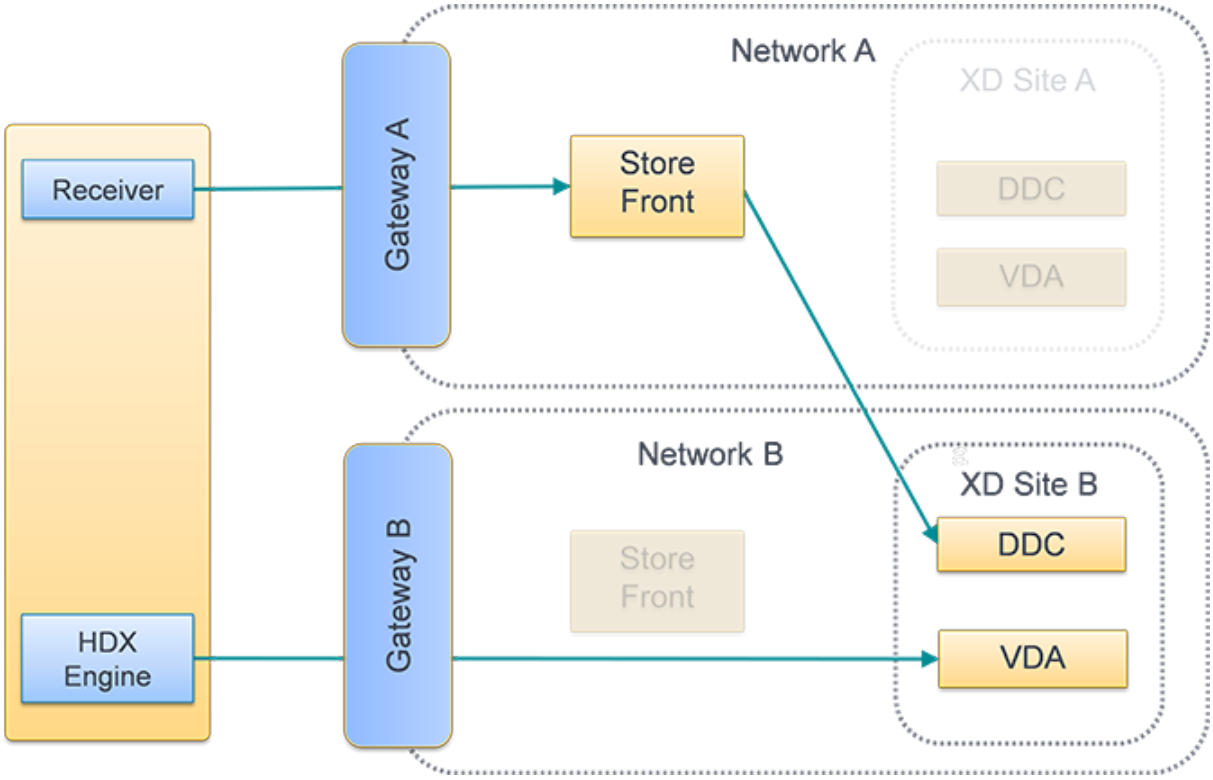


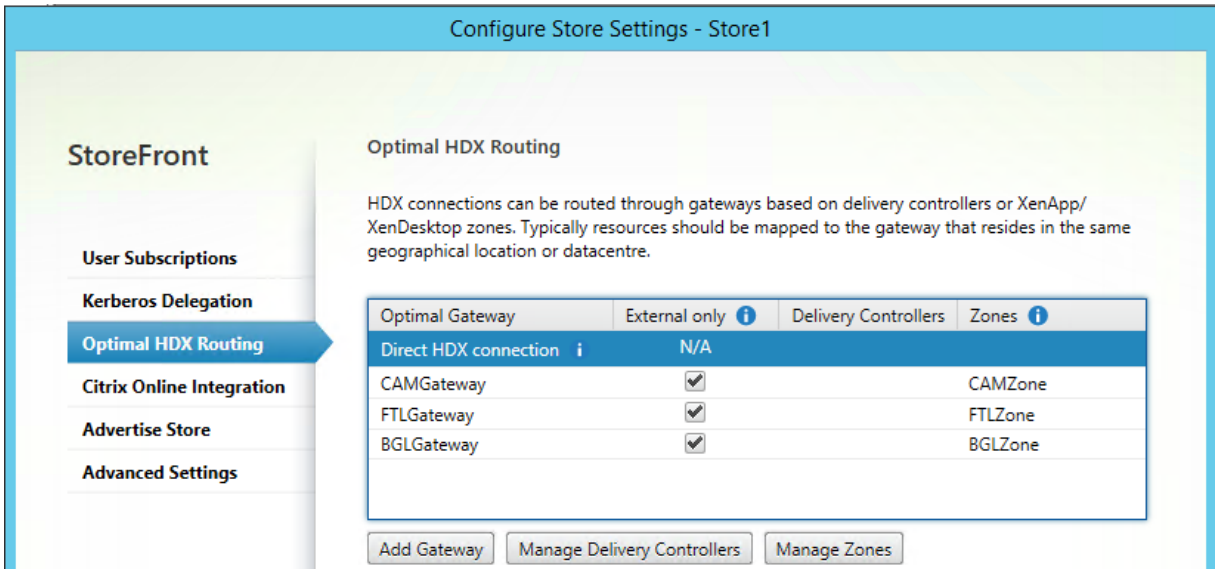
图 2. 最佳网关路由



使用 **Citrix StoreFront** 管理控制台

为部署配置了单独的 Citrix Gateway 设备后，可以为用户定义用于访问每个部署的最佳设备。

1. 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。
3. 在设置 > 最佳 **HDX** 路由页面上，选择一个网关。
4. 如果选中了仅限外部复选框，则相当于设置了 **-enabledOnDirectAccess = false**，并且“直接 HDX 连接”与对场或区域使用 **Set-DSFarmsWithNullOptimalGateway** 等效。



添加新网关

之前的过程中的其中一个选项为添加网关。选择添加网关后，将显示“添加 Citrix Gateway”屏幕。

1. 在常规设置屏幕上，填写“显示名称”、“Citrix Gateway URL”和“使用情况”或“角色”设置，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。
2. 在 **Secure Ticket Authority (STA)** 屏幕上，填写显示的选项。STA 托管在 Citrix Virtual Apps and Desktops 服务器上，并发出会话票据以响应连接请求。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。
3. 在身份验证设置屏幕中，输入用于指定远程用户如何提供身份验证凭据的设置。

使用 **PowerShell** 为应用商店配置最佳 **Citrix Gateway** 路由

PowerShell API 参数

-SiteId (Int) - IIS 中的站点 ID。对于默认安装 StoreFront 的 IIS 中的站点，通常为 1。

-ResourcesVirtualPath (String) - 要进行配置以具有场到最佳网关映射的应用商店的路径。

示例：”/Citrix/Store”

-GatewayName (String) - 为识别 StoreFront 中的 Citrix Gateway 提供的名称。

示例 1：ExternalGateway

示例 2：InternalGateway

-Hostnames (String Array) - 指定最佳 Citrix Gateway 设备的完全限定的域名 (FQDN) 和端口。

标准虚拟服务器端口 443 的示例 1：`gateway.example.com`

非标准虚拟服务器端口 500 的示例 2：`gateway.example.com:500`

-Farms (String Array) - 指定一组（通常位于同一个位置）共享通用最佳 Citrix Gateway 设备的 Citrix Virtual Apps and Desktops 部署。一个场可以包含一个或多个提供已发布资源的 Delivery Controller。

可以在 StoreFront 中的 Delivery Controller 下配置一个 Citrix Virtual Desktops 站点 “XenDesktop”。它表示为一个场。这样可以在其故障转移列表中包含多个 Delivery Controller。

示例：”XenDesktop”

`XenDesktop-A.example.com`

`XenDesktop-B.example.com`

`XenDesktop-C.example.com`

-Zones (String Array) - 指定一个或多个包含多个 Delivery Controller 的数据中心。这要求您标记包含要将 Delivery Controller 对象分配到的相应区域的 StoreFront 中的对象。

-staUrls (String Array) - 指定运行 Secure Ticket Authority (STA) 的 Citrix Virtual Apps and Desktops 服务器的 URL。如果使用多个场，则使用逗号分隔的列表列出每个场上的 STA 服务器：

示　　例：`http://xenapp-a.example.com/scripts/ctxsta.dll,http://xendesktop-a.example.com/scripts/ctxsta.dll`

-StasUseLoadBalancing (Boolean) - 设置为 **true**：从所有 STA 随机获取会话票据，在所有 STA 之间平均分发请求。设置为 **false**：用户将按照在配置中列出的顺序连接到第一个可用 STA，从而将在任意给定时间所使用的 STA 数量降至最低。

-StasBypassDuration — 设置在请求失败后将 STA 视为不可用的时间期限，单位为小时、分钟和秒。

示例：02:00:00

-EnableSessionReliability (Boolean) - 设置为 **true**：在 Receiver 自动尝试重新连接时，保持断开连接的会话处于打开状态。如果配置了多个 STA 并希望确保会话始终具有可靠性，可将 useTwoTickets 属性的值设置为 **true**，以便能够从两个不同的 STA 获取会话票据，以防其中一个 STA 在会话期间不可用。

-UseTwoTickets (Boolean) - 设置为 **true**：从两个不同的 STA 获取会话票据，以防其中一个 STA 在会话期间不可用。设置为 **false**：仅使用一个 STA 服务器。

-EnabledOnDirectAccess (Boolean) - 设置为 **true**：确保当内部网络上的本地用户直接登录 StoreFront 时，仍通过为场定义的最佳设备路由与其资源的连接。设置为 **false**：不通过场的最佳设备路由与资源的连接，除非用户通过 Citrix Gateway 访问 StoreFront。

PowerShell 脚本跨多个行时（如下所示），每个行都必须以续行符 (‘) 结尾。

> 提示：
>
> Citrix 建议您将所有代码示例都复制到 Windows PowerShell 集成脚本环境 (ISE)，以便在运行前使用格式检查器验证 Powershell 代码。

为场配置最佳网关

> 注意：
>
> 通过旧 PowerShell cmdlet **Set-DSOptimalGatewayForFarms** 配置最佳 HDX 路由不起作用。
>
> 要解决此问题，请执行以下操作：
>
> 1. 请使用 **Add-DSGlobalV10Gateway** 命令为全局网关配置希望用于最佳 HDX 路由的设置，并为身份验证设置提供默认值。
> 2. 使用 **Add-DSStoreOptimalGateway** 命令可添加最佳网关配置。
>
> 示例：
>
> ```
> Add-DSGlobalV10Gateway -Id 2eba0524-af40-421e-9c5f-a1ccca80715f -Name
> LondonGateway -Address ”http://example”-Logon Domain -SecureTicketAuthorityUrls
>  @(”http://staurl1”, ”http://staurl2”)
> Add-DSStoreOptimalGateway -SiteId 1 -VirtualPath /Citrix/Store1 -GatewayId
>  2eba0524-af40-421e-9c5f-a1ccca80715f -Farms @(”Controller”)-EnabledOnDirectAccess
>  $true
> ```

示例

为应用商店 **Internal** 创建或覆盖“场的最佳网关”映射。

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

Set-DSOptimalGatewayForFarms -SiteId 1 `

-ResourcesVirtualPath /Citrix/Internal `
-GatewayName ”gateway1” `
-Hostnames ”gateway1.example.com:500” `
-Farms ”XenApp”,”XenDesktop” `
-StaUrls ”https://xenapp.example.com/scripts/ctxsta.dll”,”https://xendesktop.example.com/scripts/ctxsta.dll” `
-StasUseLoadBalancing:$false `
-StasBypassDuration 02:00:00 `
-EnableSessionReliability:$false `
-UseTwoTickets:$false `
-EnabledOnDirectAccess:$true
```

为区域配置最佳网关

示例

为应用商店 **CAMZone** 创建或覆盖 “场的最佳网关” 映射。

```
**& "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\ImportModules
    .ps1" **

\*\*Set-DSOptimalGatewayForFarms -SiteId 1 `\*\*

**-ResourcesVirtualPath /Citrix/Internal `
-GatewayName "gateway1" `
-Hostnames "gateway1.example.com:500" `
-Zones "CAMZone" `
-StaUrls "https://xenapp.example.com/scripts/ctxsta.dll","https://
    xendesktop.example.com/scripts/ctxsta.dll" `
-StasUseLoadBalancing:$false `
-StasBypassDuration 02:00:00 `
-EnableSessionReliability:$false `
-UseTwoTickets:$false `
-EnabledOnDirectAccess:$true   **
```

示例

此脚本将返回应用商店 **Internal** 的所有 “场的最佳网关” 映射。

```
Get-DSOptimalGatewayForFarms -SiteId 1 -ResourcesVirtualPath "/Citrix/
Internal"
```

示例

删除应用商店 **Internal** 的场映射的所有最佳网关。

```
Remove-DSOptimalGatewayForFarms -SiteId 1 -ResourcesVirtualPath "/Citrix/
Internal"
Configure direct HDX connections for farms
```

示例

此脚本阻止所有 ICA 启动通过应用商店 **Internal** 的指定场列表的网关传递。

```
Set-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath /Citrix/
Store -Farms "Farm1","Farm2"
```


示例

此脚本返回为阻止 ICA 启动通过应用商店 **Internal** 的网关进行传递而配置的所有场。

```
Get-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath "/Citrix/
Internal"
```

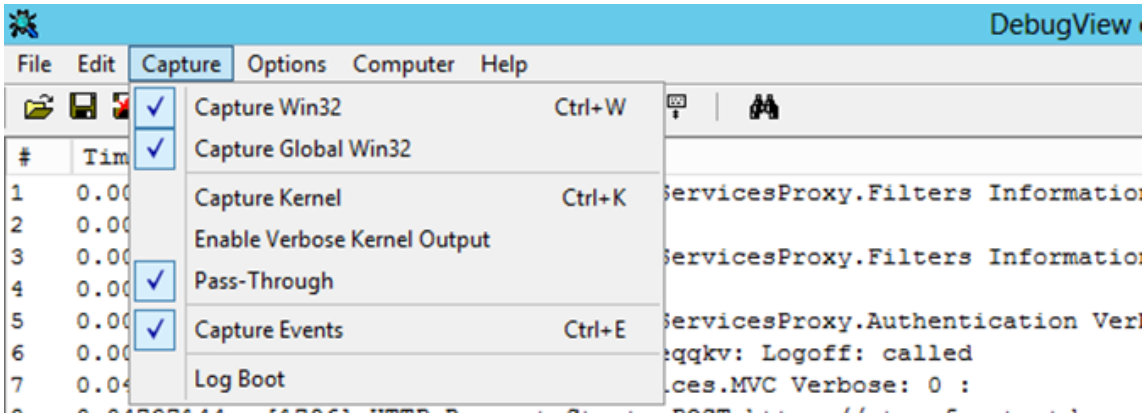
确定 StoreFront 是否正在使用适用于场的最佳网关映射

1. 通过运行以下命令，使用 PowerShell 在所有服务器组节点上启用 StoreFront 跟踪：

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

#Traces output is to c:\Program Files\Citrix\Receiver Storefront\
    admin\trace\
Set-DSTraceLevel -All -TraceLevel Verbose
```

2. 在 StoreFront 服务器的桌面上打开 Debug View 工具。如果正在使用 StoreFront 服务器组，可能必须在所有节点上执行此操作，以确保从接收启动请求的节点获取跟踪。

3. 启用 Capture Global Win32 事件。



4. 将跟踪输出另存为.log 文件，然后使用记事本打开此文件。搜索以下示例场景中显示的日志条目。

5. 之后请关闭跟踪，因为跟踪会占用 StoreFront 服务器上的大量磁盘空间。

```
Set-DSTraceLevel -All -TraceLevel Off
```

经过测试的最佳网关场景

```
- 外部客户端登录 **Gateway1**。启动通过场 **Farm2** 的指定最佳网关 **
    Gateway2** 定向。
```



```
`Set-DSOptimalGatewayForFarms -onDirectAccess=false`

将 Farm2 配置为使用最佳网关 Gateway2。

在禁用直接访问时，Farm2 具有最佳网关。

最佳网关 Gateway2 将用于启动。

- 内部客户端使用 StoreFront 登录。启动通过场 Farm1 的指定最佳网关 Gateway1 定向。

`Set-DSOptimalGatewayForFarms -onDirectAccess=true`

无需动态识别网关。直接连接 StoreFront。

将 Farm1 配置为使用最佳网关 Gateway1。

启用直接访问时，Farm1 具有最佳网关。

最佳网关 Gateway1 将用于启动。

- 内部客户端使用 Gateway1 登录。Farm1 上的资源启动不可以通过任何网关传递，直接连接 StoreFront。

`Set-DSFarmsWithNullOptimalGateway`

需要动态识别网关：Gateway1

将 Farm1 配置为不使用网关。所有网关都不用于启动。
```

与 **Citrix Gateway** 和 **Citrix ADC** 集成

June 5, 2020

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。

计划网关和服务器证书的使用

将 StoreFront 与 Citrix Gateway 和 Citrix ADC 相集成要求对网关和服务器证书的使用进行计划。应考虑您的部署中哪些 Citrix 组件将需要服务器证书：

- 计划从外部证书颁发机构获取用于面向 Internet 的服务器和网关的证书。客户端设备可能不会自动信任由内部证书颁发机构签名的证书。
- 准备外部和内部服务器名称。许多组织都有供内部和外部使用的单独命名空间，例如 `example.com`（外部）和 `example.net`（内部）。通过使用者备用名称 (SAN) 扩展，一个证书可以包含这两种名称。一般情况下，建议不要使用该选项。如果向 IANA 注册顶级域 (TLD)，公共证书颁发机构只会颁发一个证书。在这种情况下，不能使用一些常用内部服务器名称（如 example.local），且外部名称和内部名称仍需要单独的证书。
- 应尽可能为外部服务器和内部服务器使用单独的证书。网关可以支持多个证书，这需要将不同的证书绑定到每个接口。
- 应避免在面向 Internet 的服务器与非面向 Internet 的服务器之间共享证书。这些证书很可能不同，即与您的内部证书颁发机构所颁发的证书有不同的有效期和不同吊销策略。
- 只应在同等服务之间共享“通配符”证书。应避免在不同类型的服务器（例如 StoreFront 服务器和其他种类的服务器）之间共享证书。应避免在不同的管理控制下的服务器或具有不同的安全策略的服务器之间共享证书。下面是提供同等服务的服务器典型示例：
  - 一组 StoreFront 服务器和在它们之间执行负载平衡的服务器。
  - GSLB 中一组面向 Internet 的网关。
  - 一组 Citrix Virtual Apps and Desktops 控制器，它们提供同等的资源。
- 准备硬件保护的私钥存储。网关和服务器（包括一些 Citrix ADC 型号）可以将私钥安全地存储在硬件安全模块 (HSM) 或受信任的平台模块 (TPM) 中。出于安全考虑，这些配置通常不用于支持共享证书及其私钥，请查阅组件相关文档。如果通过 Citrix Gateway 实施 GSLB，这可能要求 GSLB 中的每个网关具有相同的证书，并且证书中包含您要使用的所有 FQDN。

有关保护 Citrix 部署的详细信息，请参阅白皮书使用 Citrix Virtual Apps and Desktops 进行端到端加密以及 Citrix Virtual Apps and Desktops 的安全部分。

在 **Citrix Gateway VIP** 上禁用身份验证后，配置 **StoreFront** 登录

在 Citrix Gateway VIP 上禁用身份验证后，登录到 StoreFront。此过程适用于以下两种方案：
内部网络。应用程序从远处位置启动失败，因为如果将 X-Citrix-Gateway 标题传递到 StoreFront，则在 Citrix Gateway 上禁用身份验证时无法使用 STA。
Citrix Receiver for Web。如果未在 Citrix Gateway VIP 上启用身份验证，Receiver 客户端将不进行身份验证。

在 **StoreFront** 服务器上所做的更改

1. 禁用要求令牌一致字段：

   - StoreFront 3.0
     a) 编辑应用商店 Web 站点的 `web.config` 文件。例如，如果 StoreFront 应用商店名称为 `NoAuth`，则 StoreFront 服务器中的 `web.config` 文件的路径为 **inetpub\wwwroot\Citrix\NoAuth**。

   a) 在 `web.config` 文件中找到以下行并将值从 True 更改为 False。
   之前
   ```
   <resourcesGateways requireTokenConsistency="true">
   ```


之后

```
<resourcesGateways requireTokenConsistency="false">
```

> 注意：
>
> 在 StoreFront 3.x 上，要求令牌一致是 GUI 中的一个复选框。有关详细信息，请参阅高级应用商店设置。

b) 保存 `web.config` 文件，然后重新启动 IIS 服务。

2. 打开 **Citrix StoreFront** 管理控制台。
3. 单击针对 Web 的管理 **Receiver for Web** 站点。
4. 选择相应的 Citrix Receiver for Web 站点，单击配置，然后选择身份验证方法。
5. 请务必取消选中从 **Citrix Gateway** 直通选项。

> 注意：
>
> 假定在 StoreFront 服务器上设置了 Citrix Gateway 和 “启用远程访问”。

在 **Citrix Gateway** 上所做的更改

1. 打开 Citrix Gateway 虚拟服务器。
2. 单击身份验证选项卡并确保清除启用身份验证复选框。
3. 将相应的会话策略绑定到 Citrix Gateway 虚拟服务器。
4. 测试连接。

添加 **Citrix Gateway** 连接

June 5, 2020

可以通过执行 “添加 Citrix Gateway 设备” 任务添加用户访问您的应用商店时所用的 Citrix Gateway 部署。配置通过 Citrix Gateway 对应用商店进行远程访问之前，必须启用 Citrix Gateway 直通身份验证方法。有关为 StoreFront 配置 Citrix Gateway 的详细信息，请参阅使用 WebFront 与 StoreFront 集成。

> 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，
> 将配置更改传播到服务器组，以便更新部署中的其他服务器。

1. 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**。
3. 单击添加和“常规设置”，为 Citrix Gateway 部署指定便于用户识别的显示名称。

   用户将在 Citrix Receiver 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。
4. 为部署输入虚拟服务器或用户登录点（对于 Access Gateway 5.0）的 URL。指定部署中使用的产品版本。

   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。
5. 如果要添加 Access Gateway 5.0 部署，请继续执行步骤 7。否则，请指定 Citrix Gateway 设备的子网 IP 地址（如果需要）。Access Gateway 9.3 设备要求必须指定子网 IP 地址，但对版本更高的产品而言，此地址是可选项。

   子网地址是指 Citrix Gateway 用来表示正与内部网络中的服务器进行通信的用户设备的 IP 地址。此地址也可以是 Citrix Gateway 设备的映射 IP 地址。如果指定了子网 IP 地址，则 StoreFront 使用该地址验证传入请求是否来自可信设备。
6. 如果要添加运行 Citrix Gateway 的设备，请从登录类型列表中选择您在设备上为 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。

   - 如果需要用户输入其 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。继续执行步骤 8。
7. 要添加 Access Gateway 5.0 部署，请指示用户登录点是否在独立设备中托管。如果要添加群集，请单击“下一步”，然后继续执行步骤 9。
8. 如果要针对 Citrix Gateway 或单个 Access Gateway 5.0 设备配置 StoreFront，请在“回调 URL”框中填写 Citrix Gateway 身份验证服务 URL。StoreFront 会自动附加 URL 的标准部分。单击下一步，继续执行步骤 11。

   输入设备的内部可访问的 URL。StoreFront 连接 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。
9. 要针对 Access Gateway 5.0 群集配置 StoreFront，请在设备页面上列出该群集中设备的 IP 地址或 FQDN，然后单击下一步。

10. 在启用无提示身份验证页面上，列出在 Access Controller 服务器上运行的身份验证服务的 URL。添加多台服务器的 URL 以启用容错功能，并按优先级顺序列出这些服务器以设置故障转移顺序。单击下一步。

    StoreFront 使用身份验证服务对远程用户进行身份验证，以使用户无需在访问应用商店时重新输入凭据。

11. 对于所有部署，如果要通过应用商店获得由 Citrix Virtual Apps and Desktops 提供的资源，请在 Secure Ticket Authority (STA) 页面中列出运行 STA 的服务器的 URL。添加多个 STA 的 URL 以启用容错功能，并按优先级顺序列出这些服务器以设置故障转移顺序。

    STA 托管在 Citrix Virtual Apps and Desktops 服务器上，并发出会话票据以响应连接请求。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。

12. 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。

13. 单击创建添加 Citrix Gateway 部署的详细信息。添加了部署后，单击完成。

    有关更新部署详细信息的详细说明，请参阅配置 Citrix Gateway 连接设置。

要提供通过 Citrix Gateway 对应用商店的访问，必须配置一个内部信标点和至少两个外部信标点。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。默认情况下，StoreFront 使用部署的服务器 URL 或负载平衡的 URL 作为内部信标点。使用所添加的第一个 Citrix Gateway 部署的 Citrix Web 站点和虚拟服务器或用户登录点（对于 Access Gateway 5.0）URL 作为外部信标点。有关更改信号点的详细信息，请参阅配置信标点。

要允许用户通过 Citrix Gateway 访问应用商店，请确保为这些应用商店配置远程用户访问。

导入 **Citrix Gateway**

December 2, 2020

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

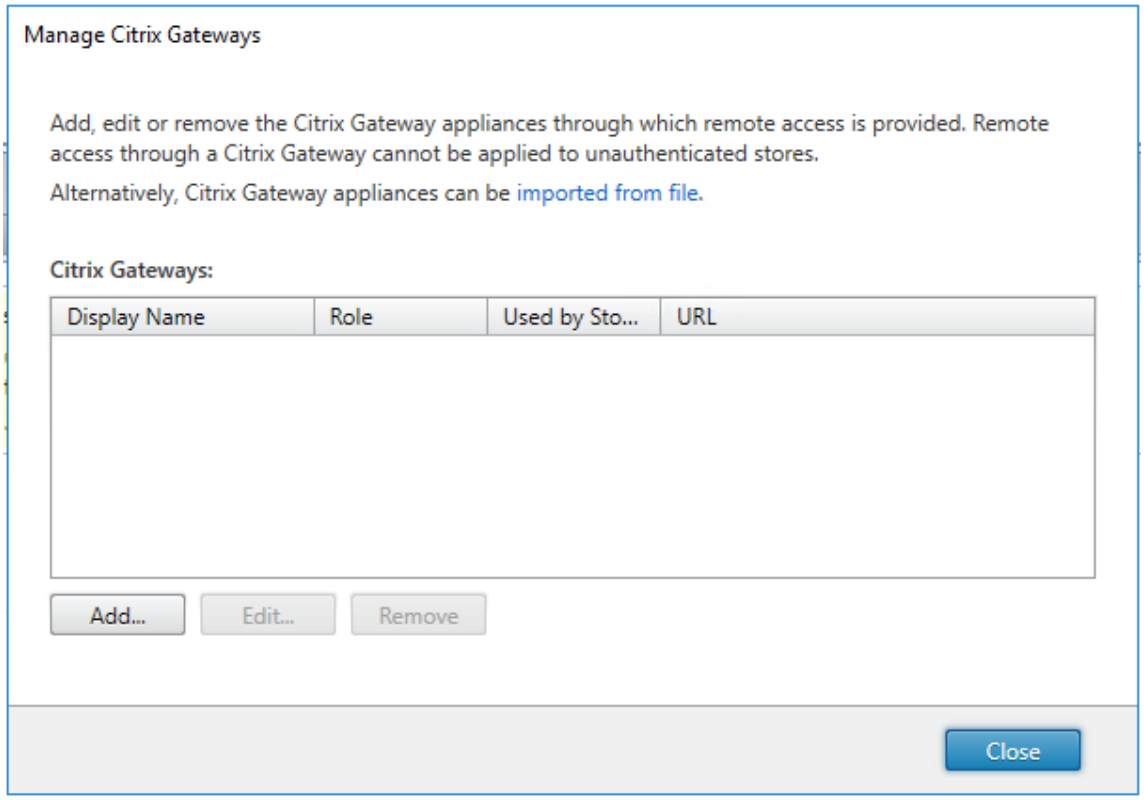
  如果您在您的环境中使用不同的外部和内部 DNS 命名空间，回调 URL 和端口组合可能与网关 URL 和端口组合不同。如果您的网关位于 DMZ 中并使用 <example.com> URL，而 StoreFront 位于您的企业专用网络中并使用 <example.local> URL，则您可以使用 <example.local> 回调 URL 指回 DMZ 中网关虚拟服务器。

使用控制台导入 **Citrix Gateway**

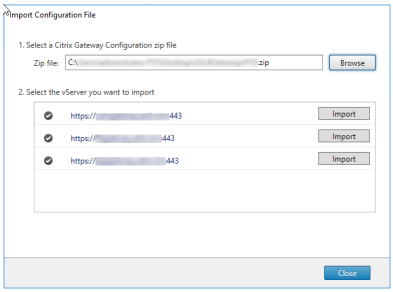
可以使用相同的导入文件导入一个或多个 Citrix Gateway 虚拟服务器配置。如果您有来自不同 Citrix ADC 设备的多个网关虚拟服务器，则必须使用多个导入文件。

> 重要：
>
> Citrix 不支持手动编辑从 Citrix Gateway 导出的配置文件。

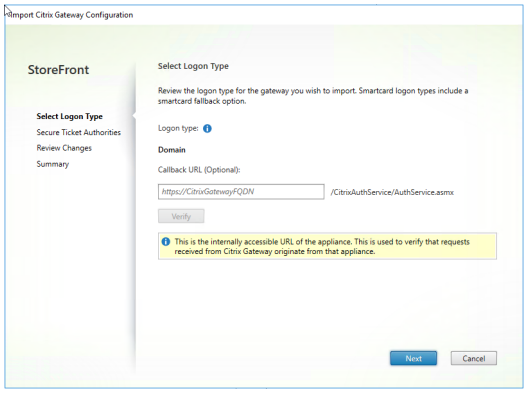
1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店，然后在操作窗格中单击管理 **Citrix Gateway**。
2. 在 “管理 Citrix Gateway” 屏幕中，单击从文件中导入链接。



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。

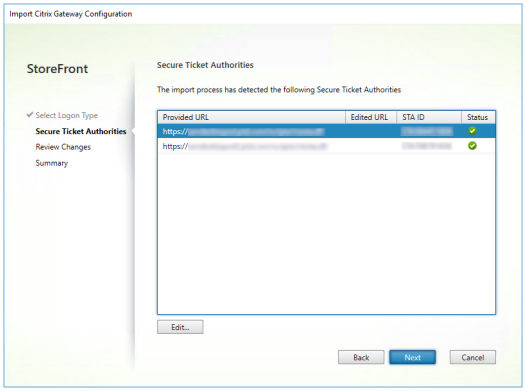


控制台中的登录类型	**JSON** 文件中的 **LogonType**	需要回调 **URL**
域	域	否
域和安全令牌	DomainAndRSA	否
安全令牌	RSA	是
智能卡 - 不回退	智能卡	是
智能卡 - 域	SmartCardDomain	是
智能卡 - 域和安全令牌	SmartCardDomainAndRSA	是
智能卡 - 安全令牌	SmartCardRSA	是
智能卡 - SMS 身份验证	SmartCardSMS	是
SMS 身份验证	SMS	是

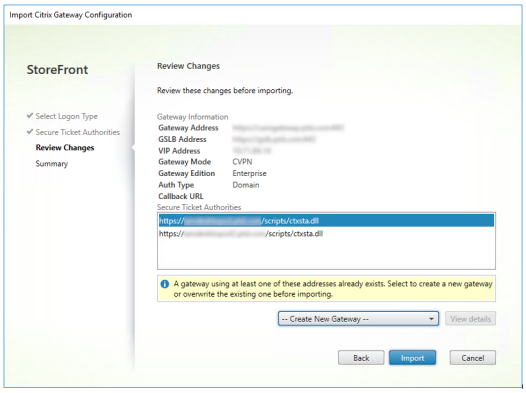
如果需要回调 URL，StoreFront 将基于在 ZIP 文件中找到的网关 URL 自动填充“回调 URL”。可以将此更改为指回正确的 Citrix Gateway VIP 的任何有效的 URL。对于 GSLB 网关，您导入的每个网关都需要唯一的回调 URL。

要使用智能访问，则需要回调 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"
```

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 }


GatewayMode             : CVPN
CallbackUrl             :
GslbAddressUri          : https://gslb.example.com/
AddressUri              : https://emeagateway.example.com/
Address                 : https://emeagateway.example.com:444
GslbAddress             : https://gslb.example.com:443
VipAddress              : 10.0.0.2
Stas                    : {
STA298854503, STA909374257 }

StaLoadBalance          : True
CertificateThumbprints  : {
F549AFAA29EBF61E8709F2316B3981AD503AF387 }

GatewayAuthType         : DomainAndRSA
GatewayEdition          : Enterprise
ReceiverForWebSites     : {
Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
    ReceiverForWebSite }


GatewayMode             : CVPN
CallbackUrl             : https://emeagateway.example.com:445
GslbAddressUri          : https://gslb.example.com/
AddressUri              : https://emeagateway.example.com/
Address                 : https://emeagateway.example.com:445
GslbAddress             : https://gslb.example.com:443
VipAddress              : 10.0.0.2
Stas                    : {
STA298854503, STA909374257 }

StaLoadBalance          : True
CertificateThumbprints  : {
F549AFAA29EBF61E8709F2316B3981AD503AF387 }

GatewayAuthType         :SmartCard
```



```
60  GatewayEdition          : Enterprise
61  ReceiverForWebSites     : {
62  Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
        ReceiverForWebSite }
```

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。

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

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。

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

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。

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



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

Import-STFNetScalerConfiguration 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。

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

配置 Citrix Gateway 连接设置

June 5, 2020

执行以下任务可更新用户访问您的应用商店时所用的 Citrix Gateway 部署的详细信息。有关为 StoreFront 配置 Citrix Gateway 的详细信息，请参阅使用 WebFront 与 StoreFront 集成。

如果对 Citrix Gateway 部署进行任何更改，应确保通过这些部署访问应用商店的用户将修改后的连接信息更新到 Citrix Workspace 应用程序中。如果为应用商店配置了 Citrix Receiver for Web 站点，则用户可以从该站点获取更新的 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，
将配置更改传播到服务器组，以便更新部署中的其他服务器。

更改常规 **Citrix Gateway** 设置

可以通过执行“更改常规设置”任务修改向用户显示的 Citrix Gateway 部署名称，并将对虚拟服务器或用户登录点 URL 以及 Citrix Gateway 基础结构部署模式所做的更改更新到 StoreFront 中。

1. 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 管理控制台的左侧窗格中选择“应用商店”，然后单击“管理 Citrix Gateway”。
3. 为 Citrix Gateway 部署指定便于用户识别的名称。

   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。
4. 为部署输入虚拟服务器或用户登录点（对于 Access Gateway 5.0）的 URL。指定部署中使用的产品版本。

   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。
5. 如果部署运行的是 Access Gateway 5.0，请继续执行步骤 7。否则，请指定 Citrix Gateway 设备的子网 IP 地址（如果需要）。

   子网地址是指 Citrix Gateway 用来表示正与内部网络中的服务器进行通信的用户设备的 IP 地址。此地址也可以是 Citrix Gateway 设备的映射 IP 地址。如果指定了子网 IP 地址，则 StoreFront 使用该地址验证传入请求是否来自可信设备。
6. 如果您的设备运行 Citrix Gateway，请从登录类型列表中选择您在设备上为 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。

   - 如果需要用户输入其 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。
7. 如果部署由 Citrix Gateway 或单个 Access Gateway 5.0 设备组成，则在回调 URL 框中填写 Citrix Gateway 身份验证服务 URL。StoreFront 会自动附加 URL 的标准部分。

输入设备的内部可访问的 URL。StoreFront 连接 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。

管理 **Access Gateway 5.0** 设备

可以通过执行“管理设备”任务在 StoreFront 中添加、编辑或删除 Access Gateway 5.0 群集中设备的 IP 地址或 FQDN。

通过 **Access Controller** 启用静默用户身份验证

可以通过执行“启用无提示身份验证”任务为 Access Gateway 5.0 群集 Access Controller 服务器上运行的身份验证服务添加、编辑或删除 URL。请输入多个服务器的 URL 以启用容错功能，并按优先级顺序列出这些服务器以设置故障转移顺序。StoreFront 使用身份验证服务对远程用户进行身份验证，以使用户无需在访问应用商店时重新输入凭据。

管理 **Secure Ticket Authority**

可以通过执行“Secure Ticket Authority”任务更新 StoreFront 从中获取用户会话票据的 Secure Ticket Authorities (STA) 列表，以及配置会话可靠性。STA 托管在 Citrix Virtual Apps and Desktops 服务器上，并发出会话票据以响应连接请求。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。

1. 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 管理控制台的左侧窗格中选择应用商店节点，在结果窗格中选择一个 Citrix Gateway 部署。在操作窗格中，单击“管理 Citrix Gateway”。
3. 单击添加输入运行 STA 的服务器的 URL。指定多个 STA 的 URL 以启用容错功能，并按优先级顺序列出这些服务器以设置故障转移顺序。要修改 URL，请在 Secure Ticket Authority URLs 列表中选择相应的条目，然后单击编辑。从列表中选择一个 URL 并单击删除，可阻止 StoreFront 从该 STA 中获取会话票据。
4. 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。

删除 **Citrix Gateway** 部署

在操作窗格中，可以通过执行管理 **Citrix Gateway** 中的“删除任务”从 StoreFront 中删除 Citrix Gateway 部署的详细信息。删除 Citrix Gateway 部署后，用户将无法通过该部署访问应用商店。

使用 **Citrix ADC** 设备进行负载平衡

December 2, 2020

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。本文提供关于以下内容的详细信息：如何将 Citrix ADC 设备配置为在服务器组中的 StoreFront 节点之间对来自 Citrix Workspace 应用程序和 Citrix Receiver for Web 的传入请求进行负载平衡。本文还介绍了如何配置 StoreFront 监视器以便与 Citrix ADC 设备配合使用。

本部分内容中的示例已在以下环境中进行了测试：

- 单服务器组中包含四个 Windows Server 2012 R2 StoreFront 3.x 节点。
- 配置一个 Citrix ADC 设备 12.1 负载平衡器用于最少连接和 CookieInsert“粘滞” 负载平衡。
- 一个安装了 Citrix Workspace 应用程序的 Windows 10 测试客户端。

打算使用 **HTTPS** 的情况下负载平衡部署的服务器证书要求

查看计划网关和服务器证书的使用部分。

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。

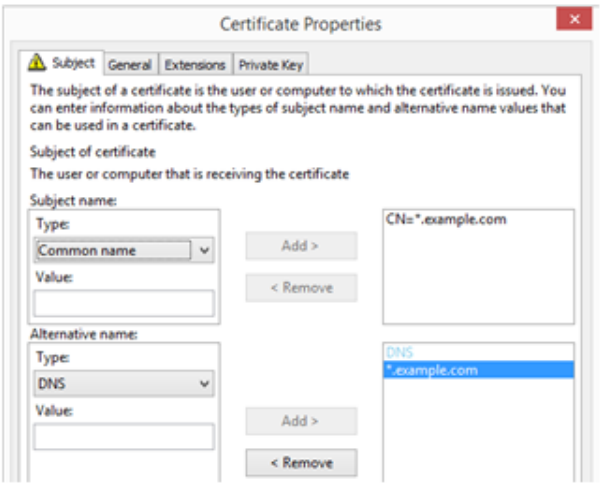
- 选项 **1**：在 Citrix ADC 设备负载平衡虚拟服务器和 StoreFront 服务器组节点上均使用 **.example.com* 通配符证书。这样可以简化配置，将来无需替换证书即可以添加其他 StoreFront 服务器。
- 选项 **2**：在 Citrix ADC 设备负载平衡虚拟服务器和 StoreFront 服务器组节点上均使用包含使用者可选名称 (SAN) 的证书。证书中包含匹配所有 StoreFront 服务器完全限定域名 (FQDN) 的其他 SAN 为可选，但是建议采用，因为这样可以在 StoreFront 部署中提供更大的灵活性。包含用于基于电子邮件的发现 discoverReceiver.example.com 的 SAN。

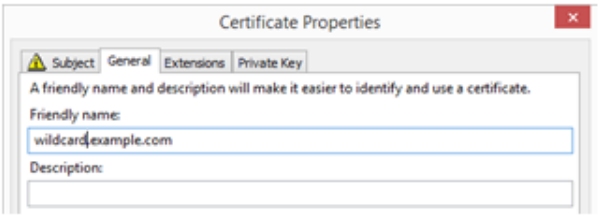
有关基于电子邮件的发现配置的详细信息，请参阅 http://blogs.citrix.com/2013/04/01/configuring-email-based-account-discovery-for-citrix-receiver/。

> 注意：
>
> 导出与证书关联的私钥不可行时，请使用两个单独的证书：一个在 Citrix ADC 设备负载平衡虚拟服务器上使用，另一个证书在 StoreFront 服务器组节点上使用。两个证书都必须包含使用者备用名称。

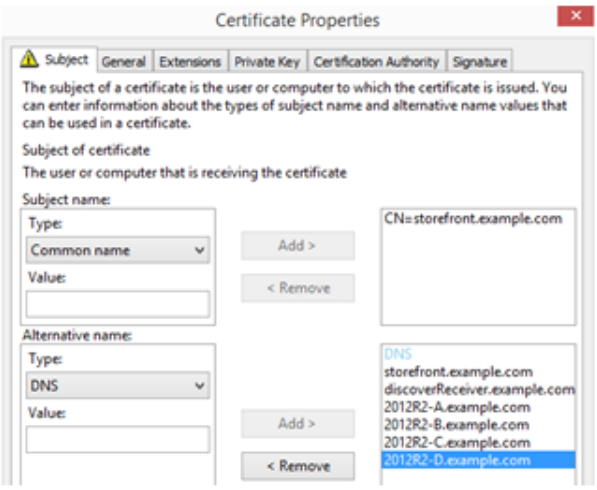
Example Web server certificates

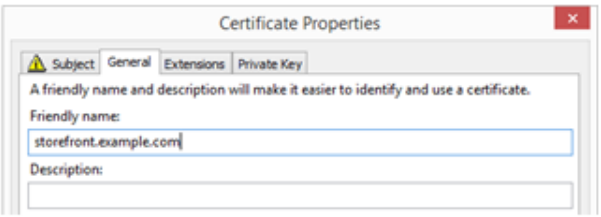
Option 1: Wildcard certificate



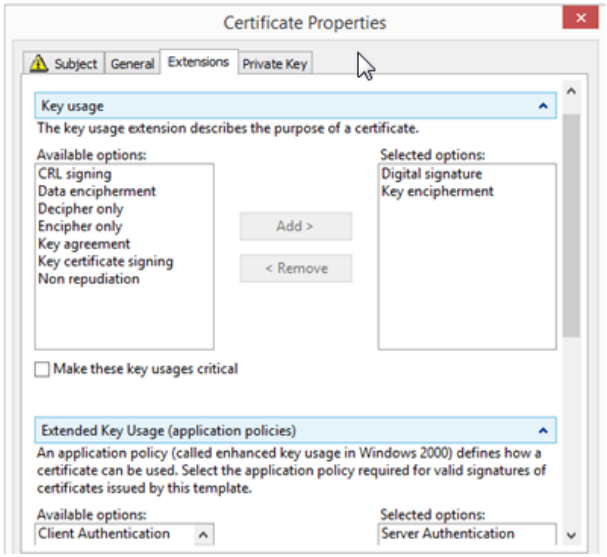


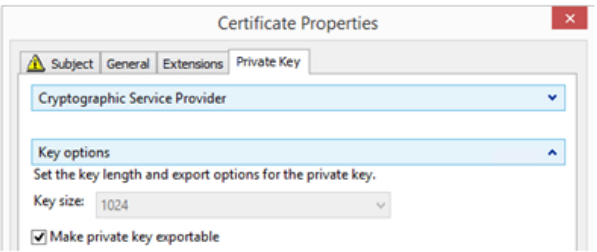
Option 2: SAN certificate with every StoreFront server





Common Properties





为 **Citrix ADC** 设备负载平衡器和所有 **StoreFront** 服务器创建服务器证书

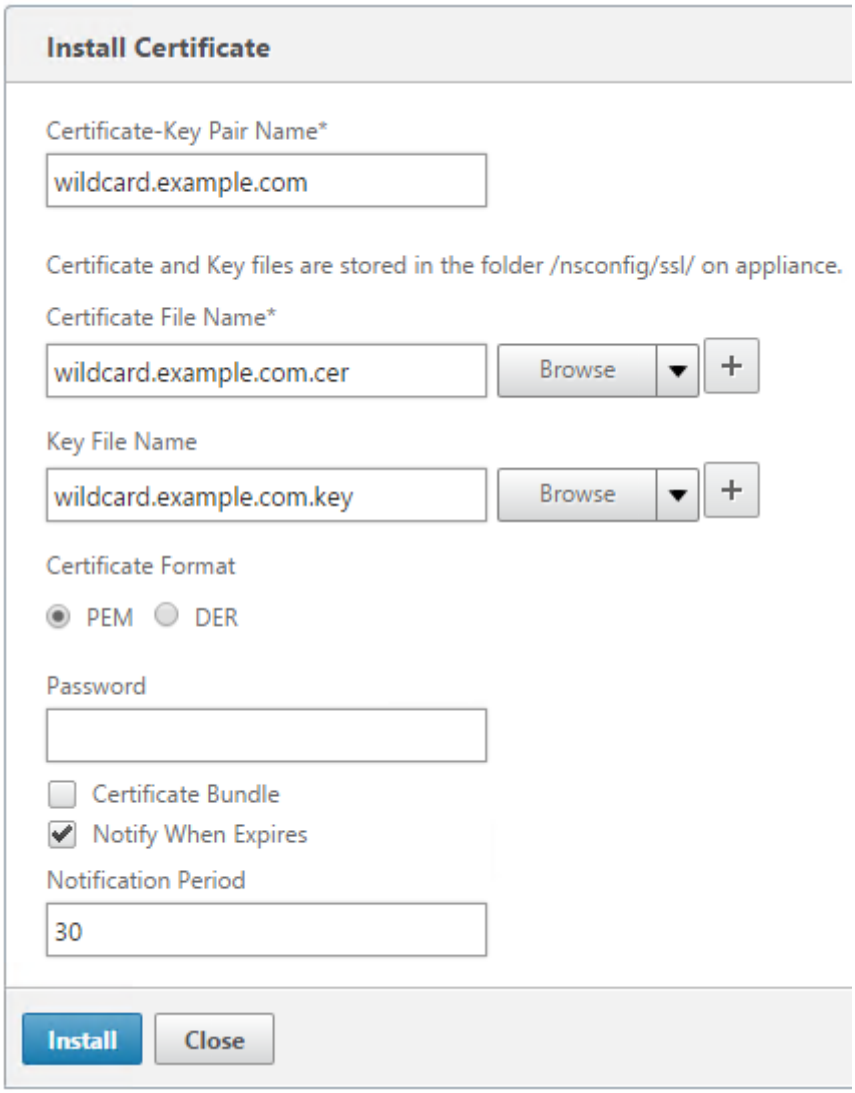
将 **Windows** 证书颁发机构颁发的证书导入 **Citrix ADC** 设备

- WinSCP 是极其有用的第三方免费工具，可将文件从 Windows 计算机移动到 Citrix ADC 设备文件系统。将要导入的证书复制到 Citrix ADC 设备文件系统内的 */nsconfig/ssl/* 文件夹。
- 您也可以在 Citrix ADC 设备上使用 OpenSSL 工具从 *PKCS12/PFX* 文件提取证书和密钥，以便以 Citrix ADC 可以使用的 PEM 格式创建两个单独的.CER 和.KEY X.509 文件。

1. 将 PFX 文件复制到 Citrix ADC 设备或 VPX 上的 */nsconfig/ssl* 中。
2. 打开 Citrix ADC 设备命令行界面 (CLI)。
3. 键入 **Shell** 以退出 Citrix ADC 设备 CLI 并切换到 FreeBSD shell。
4. 使用 `cd /nsconfig/ssl/` 更改目录。
5. 运行 `openssl pkcs12 -in <imported cert file>.pfx -nokeys -out <certfilename>.cer`，并在出现提示时输入 PFX 密码。
6. 运行 `openssl pkcs12 -in <imported cert file>.pfx -nocerts -out <keyfilename>.key`，并在出现提示时输入 PFX 密码，然后设置私钥 PEM 密码以保护.KEY 文件。
7. 运行 `ls -al` 以检查是否已在 `/nsconfig/ssl/` 内成功创建.CER 和.KEY 文件。
8. 键入 **Exit** 以返回到 Citrix ADC 设备 CLI。

导入服务器证书后在 **Citrix ADC** 设备上进行配置

1. 登录到 Citrix ADC 设备管理 GUI。
2. 选择 **Traffic Management**（流量管理）**> SSL > SSL Certificates**（**SSL** 证书），然后单击 **Install**（安装）。
3. 在 “Install Certificate”（安装证书）窗口中，输入证书和私钥对名称。
    - 在 Citrix ADC 设备文件系统上，选择 /nsconfig/ssl/ 下面的.cer 证书文件。
    - 从同一位置选择包含私钥的.key 文件。



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)。

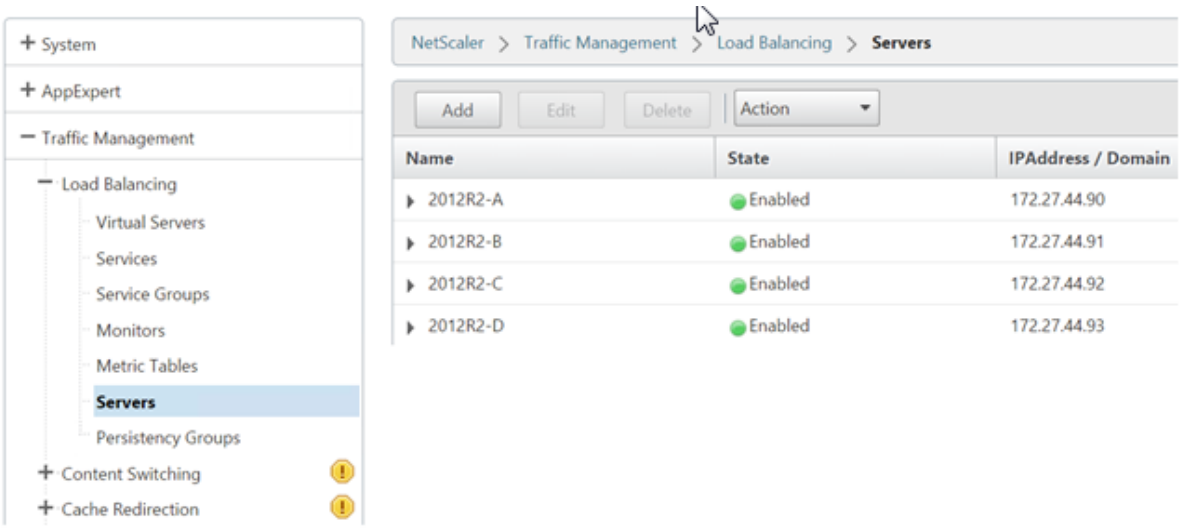
方案 **1**：在客户端与 **Citrix ADC** 设备负载平衡器以及负载平衡器与多个 **StoreFront 3.x** 服务器之间建立端到端 **HTTPS 443** 安全连接

此方案使用修改后的 StoreFront 监视器并使用端口 443。

将单个 **StoreFront** 服务器节点添加到 **Citrix ADC** 设备负载平衡器

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）**> Servers**（服务器）**> Add**（添加），分别添加要进行负载平衡的四个 StoreFront 节点。

   示例 = 4 个名为 2012R2-A 到 2012R2-D 的 2012R2 StoreFront 节点。
3. 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。

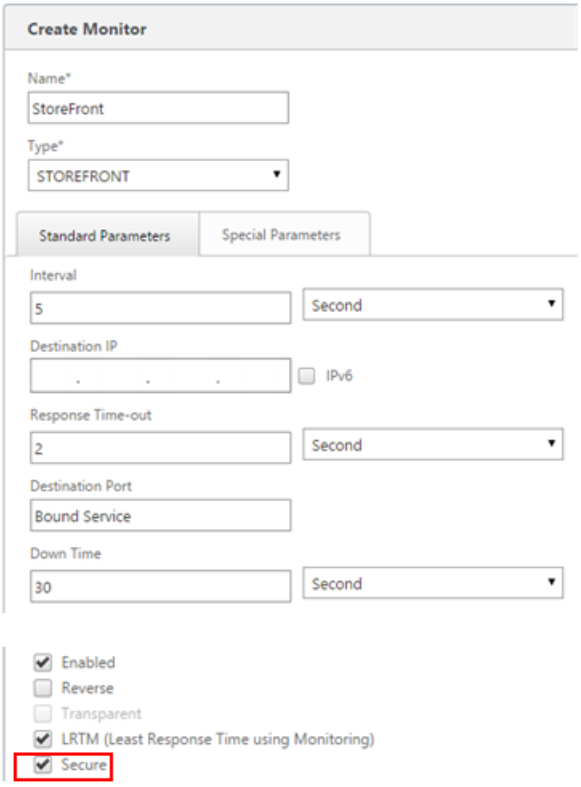


定义一个 **StoreFront** 监视器，用于检查服务器组中所有 **StoreFront** 节点的状态

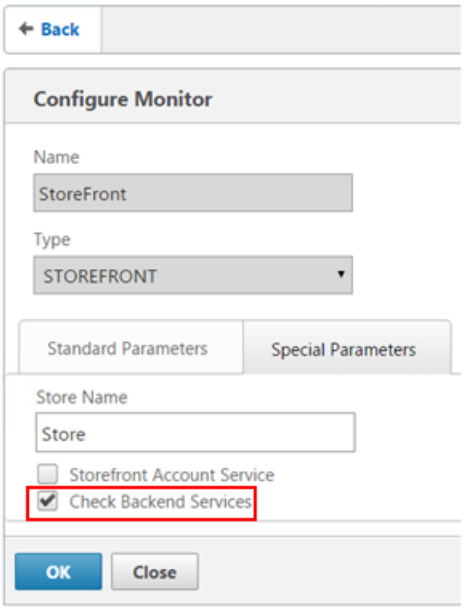
1. 登录到 Citrix ADC 管理 GUI。
2. 选择 **Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Monitors**（监视器）**> Add**（添加），添加名为 *StoreFront* 的新监视器，并接受所有默认设置。
3. 从 **Type**（类型）下拉菜单中，选择 **StoreFront**。
4. 如果在负载平衡虚拟服务器与 StoreFront 之间使用 HTTPS 连接，请确保选中 **Secure**（安全）选项；否则，请让此选项保留未选中状态。
5. 在特殊参数选项卡中，键入应用商店名称。
6. 在特殊参数选项卡中，选择检查后端服务选项。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

Standard Parameters Tab

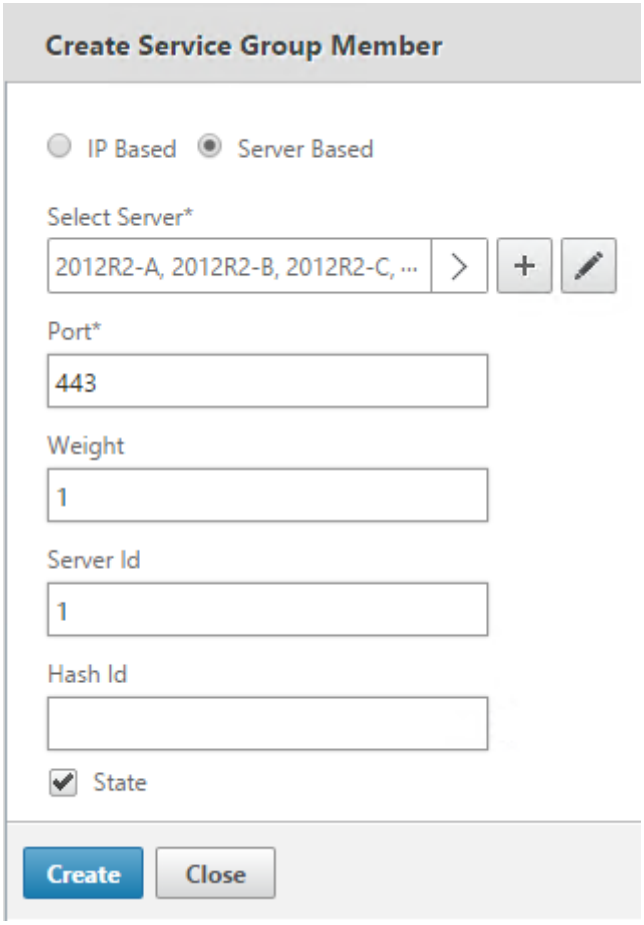


Special Parameters Tab

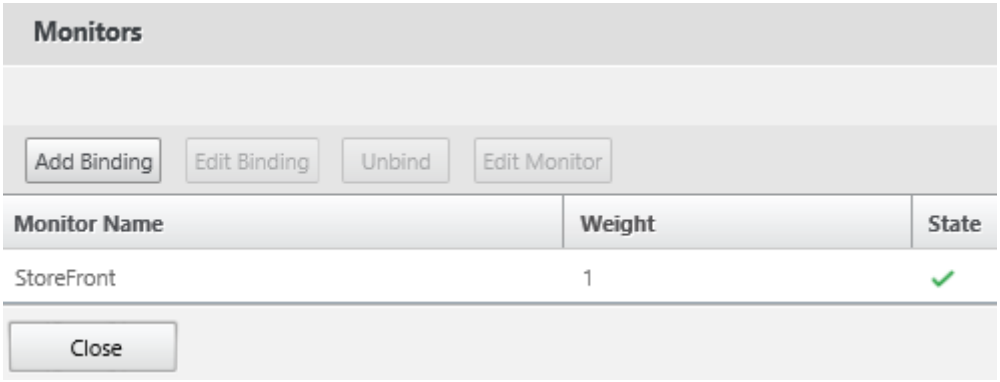


创建包含所有 **StoreFront** 服务器的 **HTTPS 443** 服务组

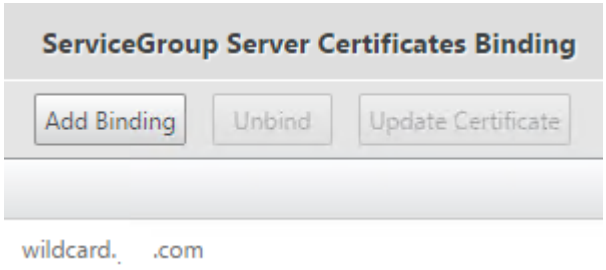
1. 在服务组内，选择右侧的 **Members**（成员）选项，然后添加您之前在“Servers”（服务器）部分定义的所有 StoreFront 服务器节点。
2. 设置 TLS 端口，并在添加时为每个节点指定一个唯一的服务器 ID。



3. 在 **Monitors**（监视器）选项卡上，选择之前创建的 StoreFront 监视器。

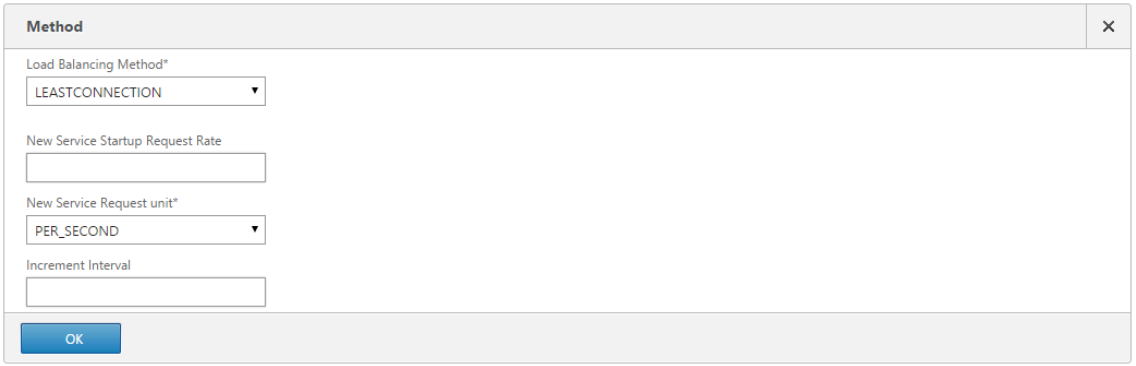


4. 在证书选项卡上，绑定之前导入的服务器证书。
5. 绑定用于为之前导入的服务器证书进行签名的 CA 证书，以及可能属于 PKI 信任链的任何其他 CA。

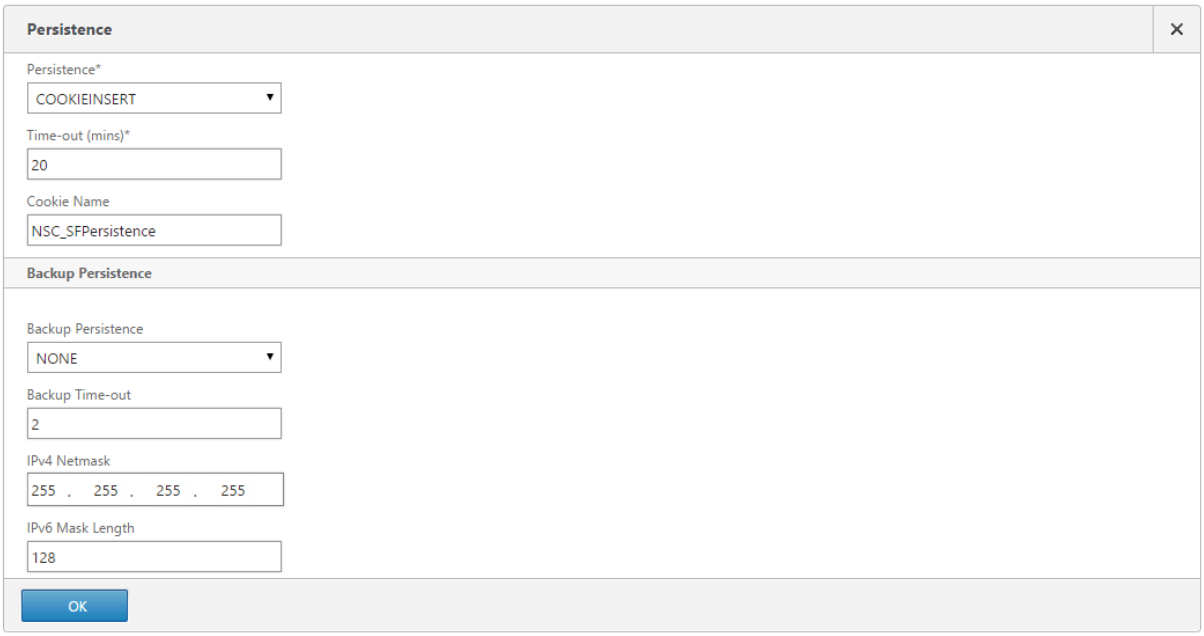


创建用于用户流量的负载平衡虚拟服务器

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. 选择虚拟服务器采用的负载平衡方法。StoreFront 负载平衡的常用选项为 **round robin**（轮询）或 **least connection**（最少连接）。



4. 将您之前创建的服务组绑定到负载平衡虚拟服务器。
5. 将之前绑定到服务组的同一服务器和 CA 证书绑定到负载平衡虚拟服务器。
6. 在负载平衡虚拟服务器菜单中，选择右侧的 **Persistence**（持久性），将持久性方法设置为 **COOKIEINSERT**。
7. 为该 Cookie 命名。例如，**NSC_SFPersistence**，这样可以在调试时使其在 Fiddler 跟踪中易于识别。
8. 将备份持久性设置为 **NONE**（无）。



方案 **2**：**HTTPS** 终止 **-** 客户端与 **NetScaler** 负载平衡器之间进行 **HTTPS 443** 通信，**Citrix ADC** 负载平衡器与其后方的 **StoreFront 3.x** 服务器之间进行 **HTTP 80** 连接

此方案使用默认的 StoreFront 监视器并使用端口 8000。

将单个 **StoreFront** 服务器添加到 **Citrix ADC** 负载平衡器

1. 登录到 Citrix ADC 管理 GUI。
2. 选择 **Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Servers**（服务器）**> Add**（添加），分别添加要进行负载平衡的四个 StoreFront 服务器。示例：4 个 2012R2 StoreFront 服务器，分别命名为 2012R2-A 至 2012R2–D。3.
3. 使用基于 IP 的服务器配置，并输入每个 StoreFront 服务器的服务器 IP 地址。

定义一个 **HTTP 8000 StoreFront** 监视器，用于检查服务器组中所有 **StoreFront** 服务器的状态

1. 登录到 Citrix ADC 管理 GUI。
2. 选择 **Traffic Management**（流量管理）**> Monitors**（监视器）**> Add**（添加），添加名为 StoreFront 的新监视器。
3. 为新监视器添加一个名称并接受所有默认设置。
4. 在类型列表中选择 **StoreFront**。
5. 在特殊参数选项卡中，键入应用商店名称。
6. 在目标端口中键入 8000。这样可以与在每个 StoreFront 服务器上创建的默认监视器实例相匹配。
7. 在特殊参数选项卡中，选择检查后端服务选项。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 服务器上的 Windows 服务监视 StoreFront 服务，探测操作会返回正在运行的所有

StoreFront 服务的状态。

创建包含所有 **StoreFront** 服务器的 **HTTP 80** 服务组

1. 在服务组内，选择右侧的 **Members**（成员）选项，然后添加您之前在“Servers”（服务器）部分定义的所有 StoreFront 服务器节点。
2. 将 HTTP 端口设置为 80，并在添加服务器时为每台服务器分配一个唯一的服务器 ID。
3. 在 **Monitors**（监视器）选项卡上，选择之前创建的 StoreFront 监视器。

创建用于用户流量的 **HTTPS** 终止负载平衡虚拟服务器

1. 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。
2. 选择虚拟服务器将使用的负载平衡方法。StoreFront 负载平衡的常用选项为“round robin”（轮询）或“least connection”（最少连接）。
3. 将您之前创建的服务组绑定到负载平衡虚拟服务器。
4. 将之前绑定到服务组的同一服务器和 CA 证书绑定到负载平衡虚拟服务器。

   > 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）。

5. 在负载平衡虚拟服务器菜单中，选择右侧的 **Persistence**（持久性），将持久性方法设置为 **COOKIEINSERT**。
6. 为该 Cookie 命名。例如，**NSC_SFPersistence**，这样可以在调试时使其在 Fiddler 跟踪中易于识别。
7. 将备份持久性设置为 **NONE**（无）。

创建负载平衡虚拟服务器以实现服务器组之间的订阅同步

创建负载平衡虚拟服务器之前的注意事项：

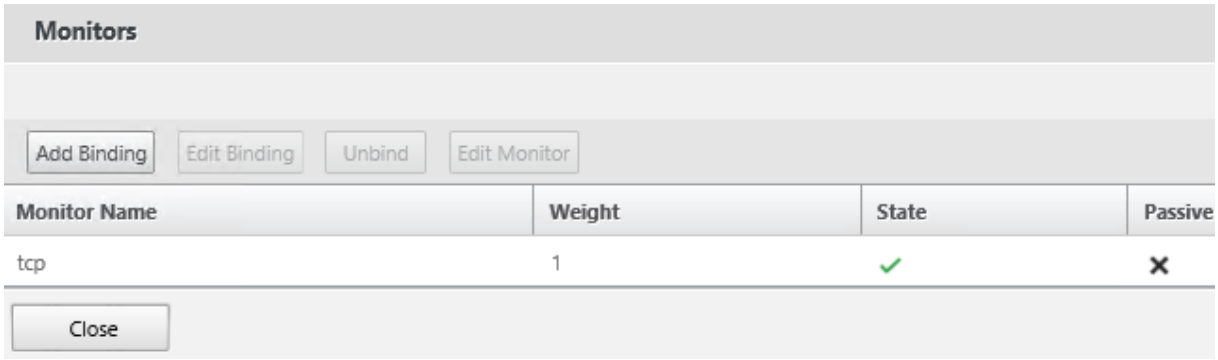
- 选项 **1**：创建单个虚拟服务器：仅对用户流量进行负载平衡。如果仅对已发布应用程序和桌面执行 ICA 启动，此选项即可满足要求。（强制，通常可满足所有需求。）
- 选项 **2**：创建虚拟服务器对：一个用于对用户流量进行负载平衡以对已发布的应用程序和桌面执行 ICA 启动，另一个用于对订阅数据同步操作进行负载平衡。（仅当在大型多站点部署中的两个或更多个进行负载平衡的 StoreFront 服务器组之间传播订阅数据时需要。）

如果多站点部署包含两个或更多个位于不同地理位置的 StoreFront 服务器组，您可以根据重复计划采用提取策略在它们之间复制订阅数据。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。配置复制计划时，请指定与订阅同步虚拟服务器虚拟 IP 地址匹配的服务器组地址。确保服务器组地址是该位置上服务器组的负载平衡器的 FQDN。

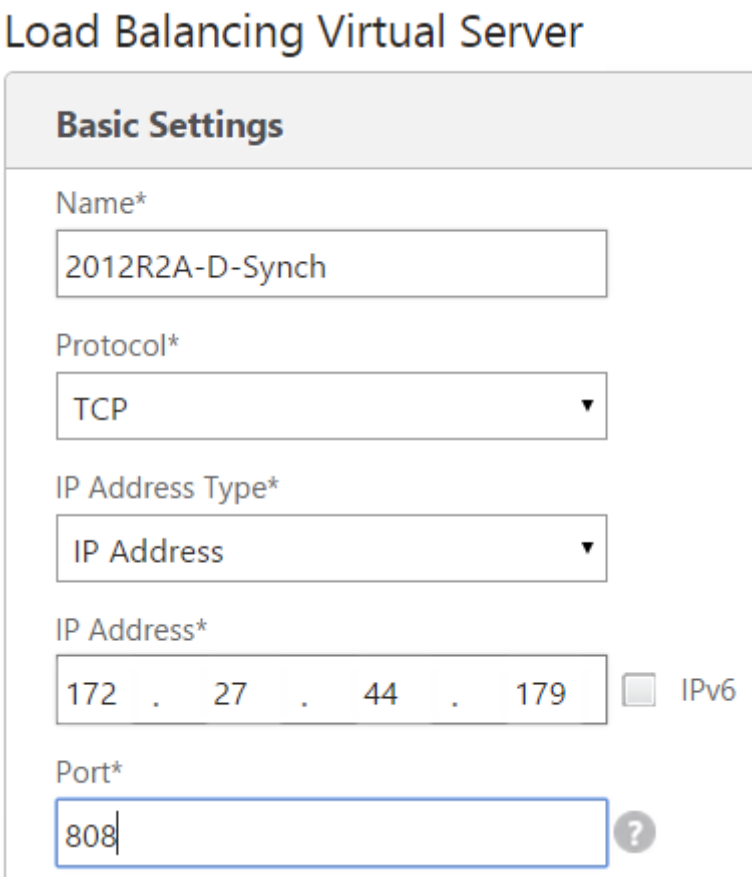
配置用于订阅同步的服务组

1. 登录到 Citrix ADC 设备管理 GUI。
2. 选择 **Traffic Management**（流量管理）**> Service Groups**（服务组）**> Add**（添加），添加新服务器组。
3. 将协议更改为 **TCP**。
4. 在服务组内，选择右侧的 **Members**（成员）选项，然后添加您之前在“Servers”（服务器）部分定义的所有 StoreFront 服务器节点。
5. 在监视器选项卡上，选择 TCP 监视器。



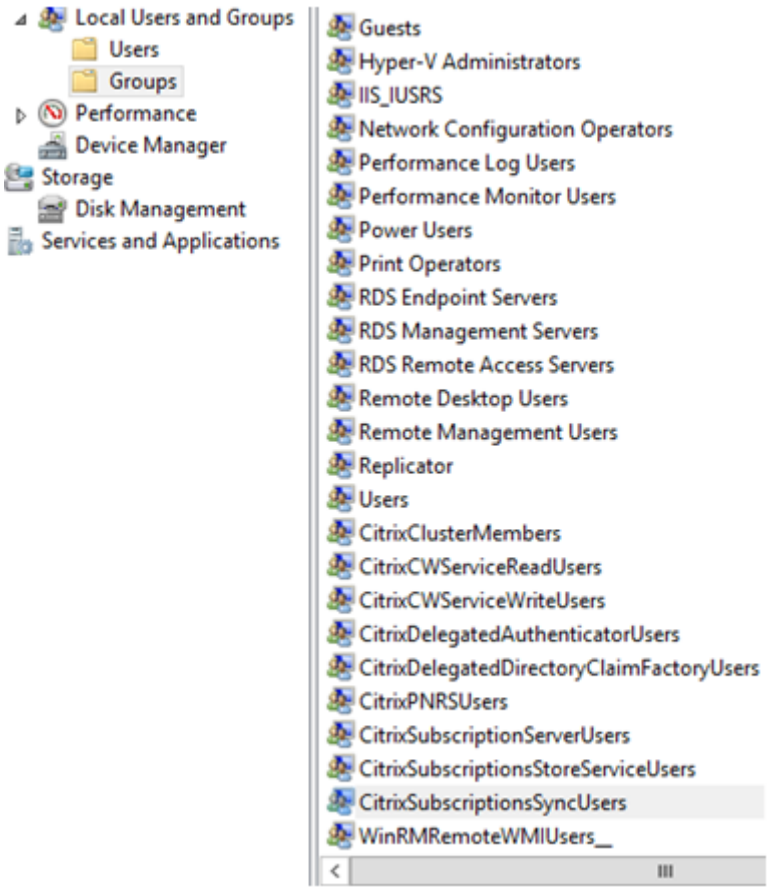
创建负载平衡虚拟服务器以实现服务器组之间的订阅同步

1. 登录到 Citrix ADC 设备管理 GUI。
2. 选择 **Traffic Management**（流量管理）**> Service Groups**（服务组）**> Add**（添加），添加新服务器组。
3. 将负载平衡方法设置为 **round robin**（轮询）。
4. 将协议更改为 **TCP**。
5. 输入 **808** 而非 **443** 作为端口号。



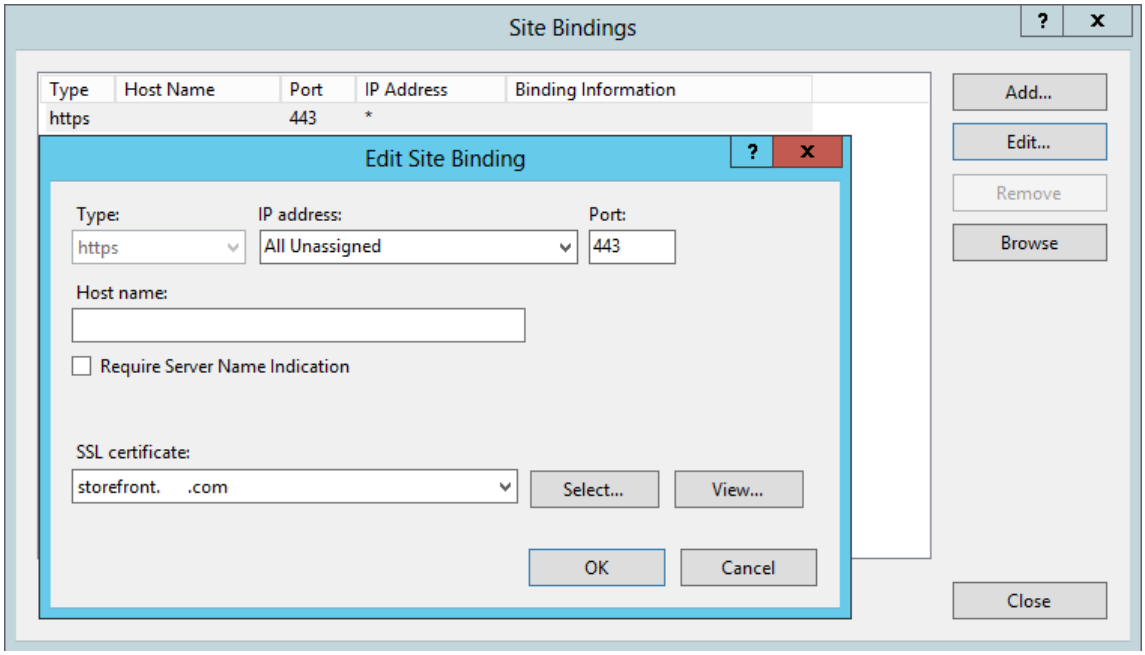
CitrixSubscriptionsSyncUsers 中的成员身份

为使位置 **A** 处的 **StoreFront** 服务器 **A** 可以向另一个位置的服务器 **B** 请求与提取订阅数据，服务器 A 必须是服务器 B 上的 **CitrixSubscriptionsSyncUsers** 本地安全组的成员。**CitrixSubscriptionsSyncUsers** 本地组包含获得授权可从特定服务器提取订阅数据的所有远程 StoreFront 服务器的访问控制列表。为实现双向订阅同步，服务器 B 也必须是服务器 A 上的 **CitrixSubscriptionsSyncUsers** 安全组的成员，才能从中提取订阅数据。



方案 **1**：在 **Citrix ADC** 与 **StoreFront** 之间使用 **HTTPS** 配置 **StoreFront** 服务器组

1. 将部署在 Citrix ADC 设备负载平衡虚拟服务器上的相同证书和私钥导入服务器组的每个 StoreFront 节点。
2. 在每个 StoreFront 节点上的 IIS 中创建 HTTPS 绑定，然后绑定之前导入其中的证书。

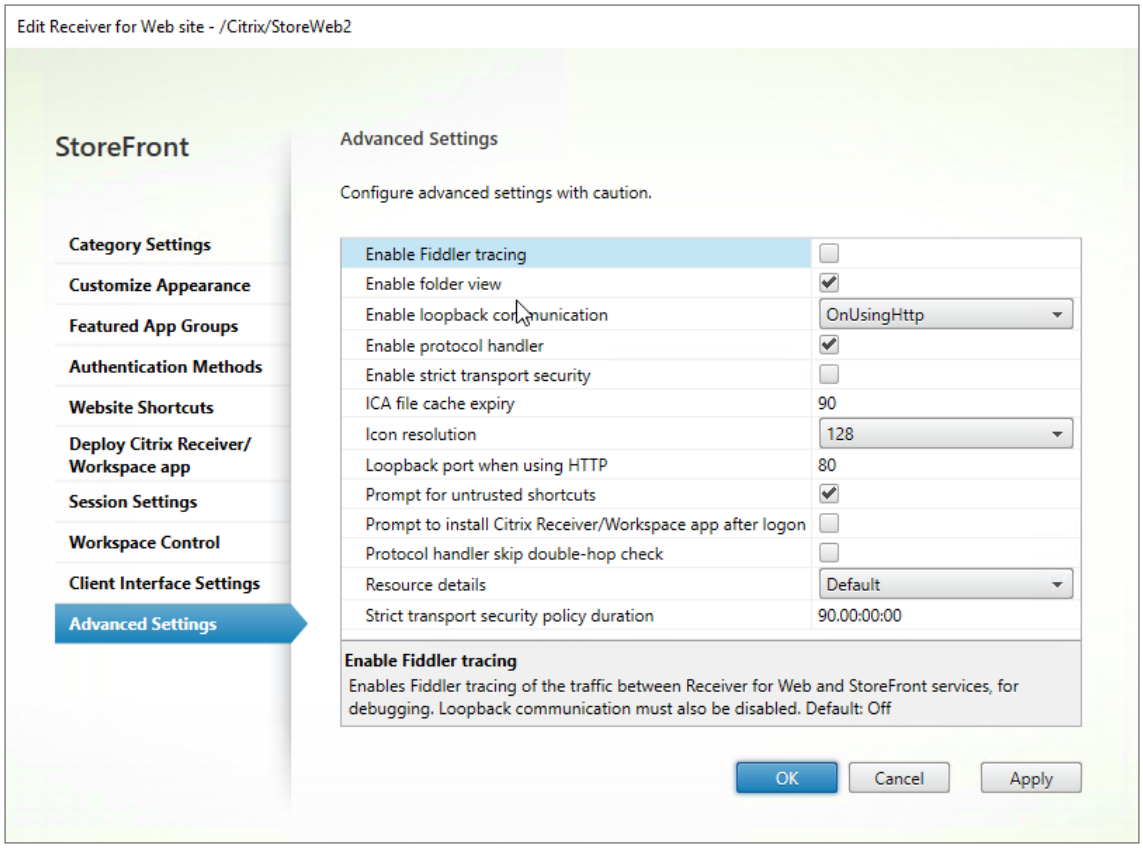


3. 如果在 Citrix ADC 负载平衡器与 StoreFront 之间使用 HTTPS，则必须使用将负载平衡 FQDN 作为公用名 (CN) 或使用者可选名称 (SAN) 包含在内的证书。

   请参阅 为 Citrix ADC 设备负载平衡器和 StoreFront 服务器创建服务器证书。

方案 **2**：在 **Citrix ADC** 与 **StoreFront** 之间使用 **HTTP** 配置 **StoreFront** 服务器组

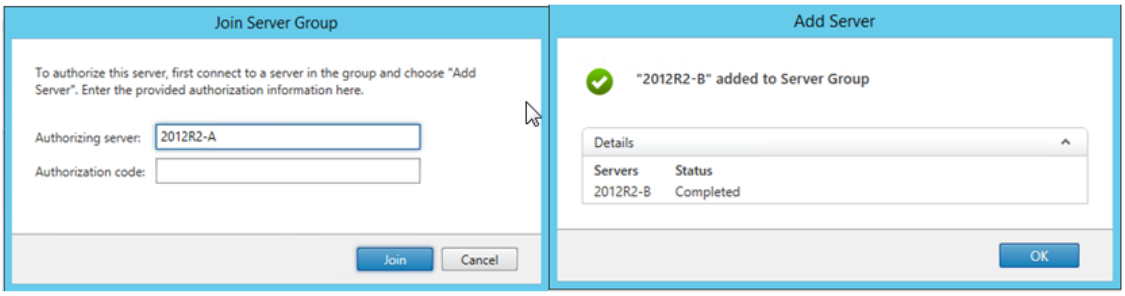
1. 从每个 StoreFront 节点中删除 IIS 中的 HTTPS 绑定（如果已存在）。
2. 确保 HTTP 绑定在 IIS 中存在，并且设置为使用端口 80。
3. 将 Receiver for Web 中的环回设置配置为 **OnUsingHTTP** 和端口 **80**。此步骤对于确保本机 Citrix Workspace 应用程序与 Receiver for Web 之间的客户端检测成功至关重要。



方案 **1** 和方案 **2** 的常用步骤

1. 在服务器组中的每个节点上安装 StoreFront。
2. 安装 StoreFront 期间，将主节点上的主机基本 URL 设置为服务器组的所有成员使用的共享 FQDN。这应始终为 `https://storefrontlb.domain.com`（适用于方案 1 和 2），并且必须与 Citrix ADC 负载平衡虚拟服务器的 FQDN 匹配。

   请参阅为 Citrix ADC 设备负载平衡器和 StoreFront 服务器创建服务器证书。
3. 完成初始 StoreFront 配置后，相继将每个节点加入使用主节点的服务器组。
4. 选择服务器组 **>** 添加服务器 **>** 复制加入的服务器的授权代码。



5. 将主节点的配置传播到组中的所有其他服务器组节点。

6. 使用可以联系和解析负载平衡器的共享 FQDN 的客户端来测试负载平衡服务器组。

Citrix Service Monitor

要对 StoreFront 正常运行所依赖的 Windows 服务的运行状态进行外部监视，请使用 **Citrix Service Monitor** Windows 服务。此服务独立于其他服务，可以监视并报告其他关键 StoreFront Service 的故障。监视器启用由其他 Citrix 组件（例如 Citrix ADC 设备）从外部确定的 StoreFront 服务器部署的相对运行状况。第三方软件可以利用 StoreFront 监视器的 XML 响应来监视关键 StoreFront Service 的运行状况。

部署 StoreFront 后，将创建使用 HTTP 和端口 8000 的默认监视器。

> 注意：
>
> 一个 StoreFront 部署中只能存在一个监视器实例。

要对现有默认监视器进行更改，如将协议和端口号改为 HTTPS 443，请使用 PowerShell cmdlet 查看或重新配置 StoreFront 监视器服务 URL。

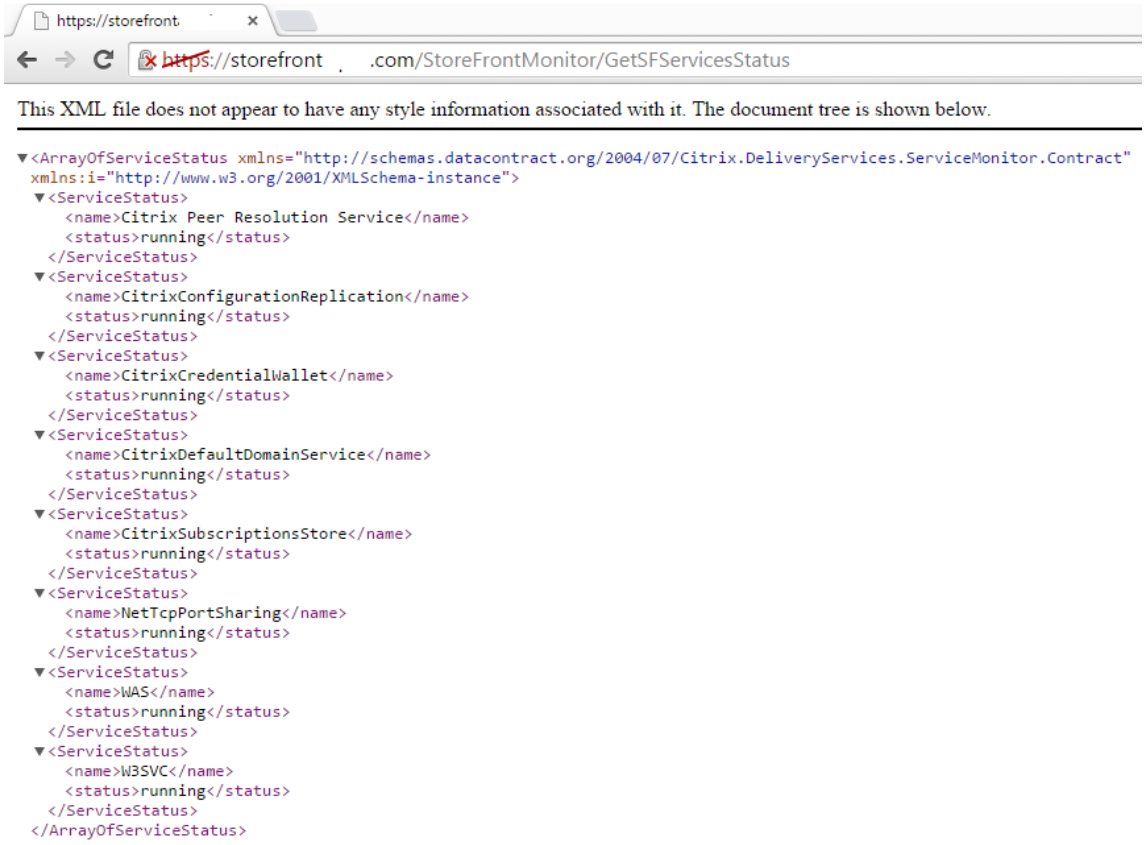
删除默认服务监视器，将其替换为使用 **HTTPS** 和端口 **443** 的监视器

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监视器更改为 HTTPS 443。

```
$ServiceUrl = ”https://localhost:443/StorefrontMonitor”
Set-STFServiceMonitor -ServiceUrl $ServiceUrl
Get-STFServiceMonitor
```

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. 要快速测试新监视器，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。浏览器应该会返回每个 StoreFront 服务状态的 XML 摘要。

   `https://<loadbalancingFQDN>:443/StoreFrontMonitor/GetSFServicesStatus`

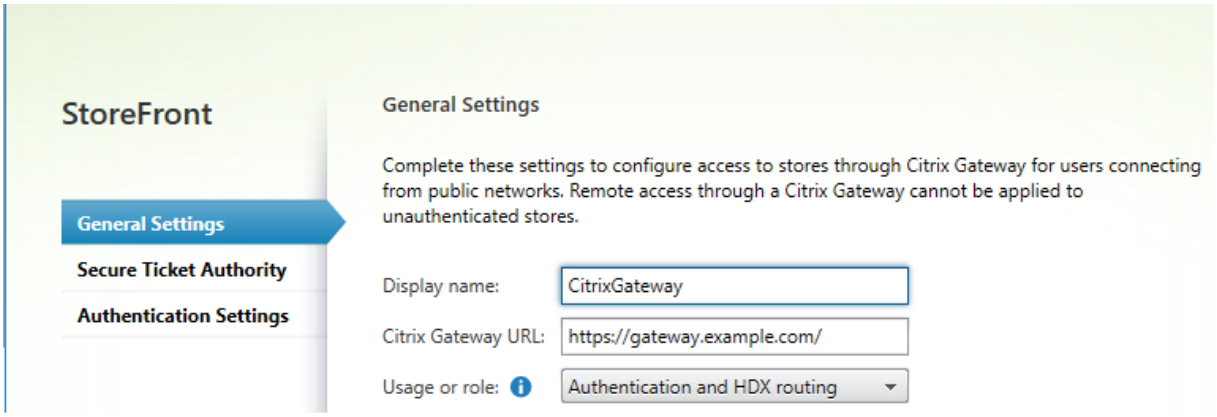


Citrix Gateway 与负载平衡虚拟服务器位于相同的 **Citrix ADC** 设备上

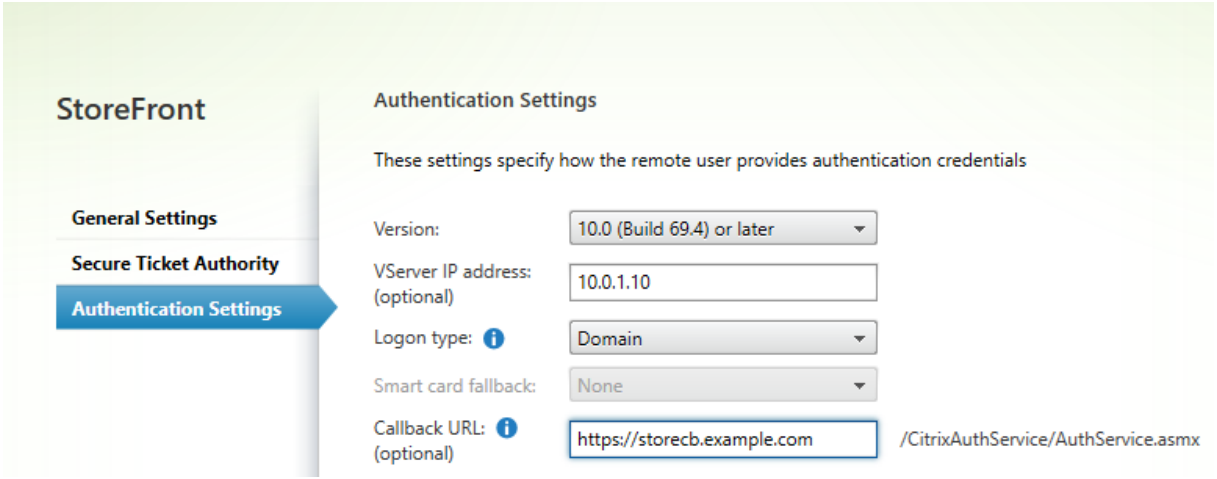
如果在同一个 Citrix ADC 设备上配置了 Citrix Gateway 虚拟服务器和负载平衡虚拟服务器，内部域用户尝试直接（而不是通过 Citrix Gateway 虚拟服务器）访问 StoreFront 负载平衡主机基本 URL 时可能会遇到问题。

在此情况下，由于 StoreFront 将传入用户的源 IP 地址与 Citrix Gateway 子网 IP 地址 (SNIP) 相关联，StoreFront 会假定最终用户已经在 Citrix Gateway 经过身份验证。这样会触发 StoreFront 尝试使用 AGBasic 协议执行 Citrix Gateway 无提示身份验证，而不是实际提示用户使用其域凭据进行登录。为避免出现此问题，请省略如下所示的 SNIP 地址或者输入 VIP，以便使用用户名和密码身份验证而非 AGBasic 登录协议。

在 **Storefront** 服务器组上配置 **Citrix Gateway**



输入 Citrix Gateway VIP 到“虚拟服务器 IP 地址”字段中。如果负载平衡虚拟服务器驻留在同一个 Citrix ADC 设备上，请勿将 SNIP 用于 Citrix Gateway。



使用 **Citrix ADC** 设备对 **StoreFront** 服务器组进行负载平衡时的环回选项

可以使用 PowerShell 设置环回选项。

Receiver for Web web.config 文件示例

```
<communication attempts="2" timeout="00:01:00" loopback="On"
    loopbackPortUsingHttp="80">
```

PowerShell 命令示例

```
& "c:\program files\Citrix\receiver storefront\scripts\ImportModules.
    ps1"
```



```
2 Set-DSLoopback -SiteId 1 -VirtualPath ”/Citrix/StoreWeb” -Loopback ”
    OnUsingHttp” -LoopbackPortUsingHttp 81
```

-Loopback 参数可以采用三个值：

值	上下文
On - 将 URL 的主机更改为 127.0.0.1。架构和端口（如果指定）不更改。	如果使用 TLS 终止负载平衡器，则不能使用。
OnUsingHttp - 将主机更改为 127.0.0.1，将架构更改为 HTTP 并修改为 **loopbackPortUsingHttp** 属性配置的端口值。	仅当负载平衡器为 TLS 终止时才能使用。负载平衡器与 StoreFront 服务器之间的通信使用 HTTP。可以使用 -loopbackPortUsingHttp 属性显式配置 HTTP 端口。
Off - 请求中的 URL 不进行任何修改。	用于故障排除。如果环回设置为 **On**，Fiddler 之类的工具无法捕获 Receiver for Web 与 StoreFront 服务之间的流量。

为同一 **Citrix Gateway** 配置两个 **URL**

December 2, 2020

在 StoreFront 中，可以从 StoreFront 管理控制台的管理 **Citrix Gateway >** 添加或编辑来添加单个 Citrix Gateway URL。也可以在管理 **Citrix Gateway >** 从文件中导入中添加公用 Citrix Gateway URL 和 GSLB（全局服务器负载平衡）URL。

本文介绍了如何使用 PowerShell cmdlet 和 StoreFront PowerShell SDK 来使用可选参数 -gslburl 以设置网关的 GslbLocation 属性。在以下用例中，此功能简化了在 StoreFront 中进行的 Citrix Gateway 管理：

1. **GSLB** 和多个 **Citrix Gateway**。可使用 GSLB 和多个 Citrix Gateway 对与大型全球 Citrix 部署中两个或更多位置的已发布资源的远程连接进行负载平衡。
2. 使用公用 **URL** 或专用 **URL** 的单个 **Citrix Gateway**。可使用同一 Citrix Gateway 在外部使用公用 URL 进行访问以及在内部使用专用 URL 进行访问。

这是一项高级功能和主题。如果您是初次了解 StoreFront 网关和全局服务器负载平衡 (GSLB) 概念，请参阅本文结尾处的相关信息链接。

此功能具有以下优点：

- 支持单个网关对象有两个同时使用的 URL。
- 用户可以在两个不同的 URL 之间切换来访问 Citrix Gateway，无需管理员重新配置 StoreFront 网关对象来匹配用户要使用的网关 URL。

- 使用多个 GSLB 网关时用于验证 StoreFront 网关配置的设置和测试时间缩短。
- 在 DMZ 内部的 StoreFront 中使用相同的 Citrix Gateway 对象进行外部和内部访问。
- 支持两个 URL 进行最佳网关路由。有关最佳网关路由的详细信息，请参阅设置高可用性多站点应用商店配置。

使用两个网关 **URL** 时的部署注意事项

- StoreFront 管理控制台中显示每个网关的 gatewayURL FQDN。每个网关的 GSLBURL 属性仅通过使用 PowerShell cmdlet 可见。
- 本机 Citrix Receiver 和 Citrix Workspace 应用程序使用 gatewayURL 进行身份验证。
- gatewayURL 包含在用于使用应用商店和网关信息配置 Citrix Receiver 和 Citrix Workspace 应用程序的预配文件 (receiver.cr) 中的位置标记中。
- 使用提供的 Powershell 修改应用商店和漫游 web.config 文件。请勿手动执行此操作。

> 重要：
>
> 使用 -gslburl 参数配置第二个网关 URL 之前，请检查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。有关服务器证书的详细信息，请参阅计划网关和服务器证书的使用。

DNS

- 拆分 **DNS**。大型企业使用拆分 DNS 很常见。拆分 DNS 涉及使用不同的命名空间和不同的 DNS 服务器进行公用和专用 DNS 解析。请检查您的现有 DNS 基础结构是否支持这一点。
- 用于对已发布的资源进行外部和内部访问的单个 **URL**。决定是否要使用相同的 URL 从企业网络外部和内部访问已发布的资源，或考虑是否接受两个不同的 URL，例如 `example.com` 和 `example.net`。

服务器证书示例

本节包含使用两个网关 URL 时的示例服务器证书部署。

负载平衡的 **StoreFront** 部署的示例服务器证书

专门签名的通配符服务器证书应包含 FQDN *.storefront.example.net。

或

专门签名的 SAN 服务器证书应包含对三个 StoreFront 服务器进行负载平衡所需的所有 FQDN。

```
loadbalancer.storefront.example.net
server1.storefront.example.net
server2.storefront.example.net
server3.storefront.example.net
```


设置 StoreFront 服务器组的主机基本 URL，该 URL 要成为共享的 FQDN，它解析为负载平衡器 IP 地址：

```
loadbalancer.storefront.example.net
```

使用拆分 **DNS** 在外部和内部访问的 **Citrix Gateway** 的服务器证书示例

用于外部和内部访问的公开签名的 SAN 服务器证书应包含外部和内部 FQDN。

```
gateway.example.com
gateway.example.net
```

在外部访问的所有 **GSLB** 网关的服务器证书示例

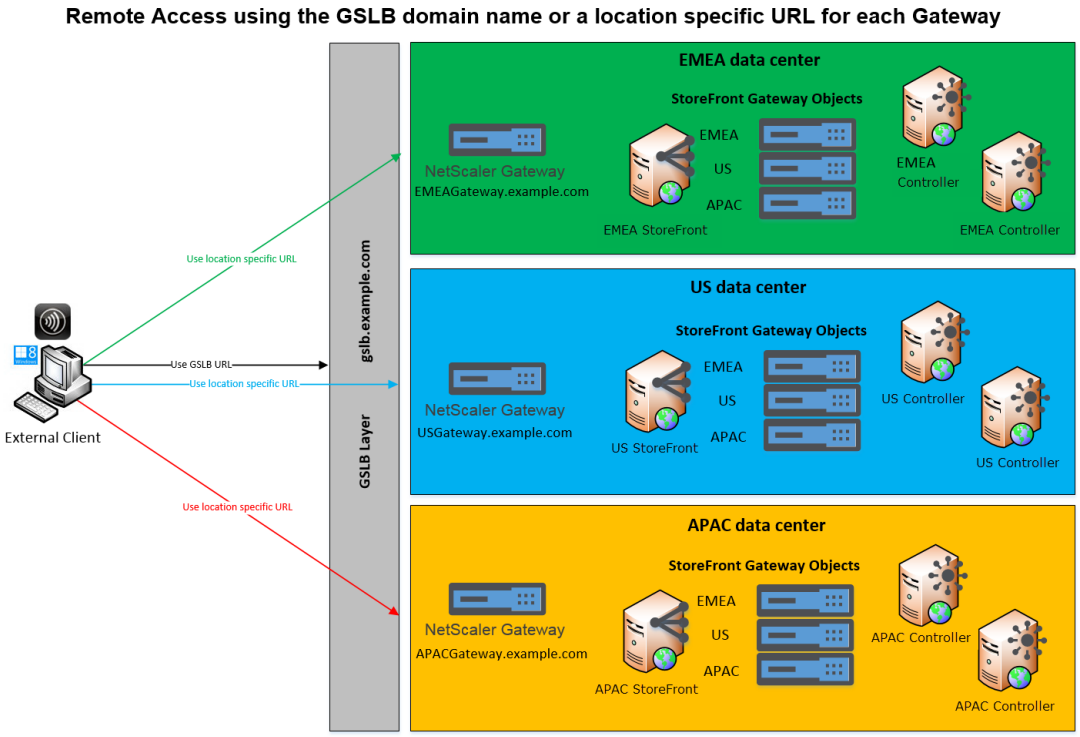
用于通过 GSLB 进行外部访问的公开签名的 SAN 服务器证书应包含 FQDN。

```
gslbdomain.example.com
emeagateway.example.com
usgateway.example.com
apacgateway.example.com
```

这允许用户使用 GSLB 访问最近的网关，或使用网关的唯一 FQDN 在其所选项的位置中选取网关。

用例 #1：Receiver for Web：GSLB 和多个 Citrix Gateway

管理员可使用 GSLB 和多个 Citrix Gateway 对与大型全球 Citrix 部署中两个或更多位置的已发布资源的远程连接进行负载平衡。



在此示例中：

- 每个位置或数据中心至少包含一个网关、一个或多个 StoreFront 服务器、一个或多个 XenApp 和 XenDesktop 控制器，才能在该位置提供已发布的资源。全球部署中的 GSLB Citrix ADC 设备上配置每个 GSLB 服务都表示一个网关 VPN 虚拟服务器。部署中的所有 StoreFront 服务器都必须配置为包含组成 GSLB 层的所有 Citrix Gateway 虚拟服务器。GSLB Citrix Gateway 在主动/主动模式下使用，但如果一个位置的网络连接、DNS、网关、StoreFront 服务器或 Citrix Virtual Apps and Desktops 控制器出现故障，这些网关还可以提供故障转移。如果 GSLB 服务不可用，用户会被自动定向到另一个网关。
- 进行远程连接时，根据配置的 GSLB 负载平衡算法（如往返时间 (RTT) 或静态临近度），外部客户端会被定向到最近的网关。
- 每个网关的唯一 URL 允许用户通过选择要使用的网关的位置特定的 URL 来手动选择要从其启动资源的数据中心。
- GSLB 或 DNS 委派未按预期发挥作用时，可以绕过 GSLB。用户可以使用数据中心的位置特定的 URL 继续访问任何数据中心的远程资源，直到所有 GSLB 相关问题得到解决。

用例 #1：Receiver for Web 和 Citrix Receiver 或 Citrix Workspace 应用程序：GSLB 和多个 Citrix Gateway

网关属性

要将 GSLB 与本机 Citrix Receiver 或 Citrix Workspace 应用程序结合使用，请使用 **Add-STFRoamingGateway**（创建）或 **Set-STFRoamingGateway**（修改）指定以下属性：

-GatewayUrl — 设置为所有 GSLB 网关的共享 FQDN

-GSLBurl — 设置为每个网关的唯一网关 FQDN

> 注意：
>
> 这可能看似违背常理，但对此 Web 用例没有影响。它确保本机 Citrix Receiver 或 Citrix Workspace 应用程序通过访问终端节点 `https://storefront.domain.com/citrix/<storename>/discovery` 在发现文档中接收 GSLB 使用的共享 FQDN。它还确保由 StoreFront 的导出预配文件命令导出的预配文件 (receiver.cr) 包含共享 GSLB FQDN。

示例预配文件

使用 `-GatewayUrl https://gslb.domain.com` 的示例文件 1。这允许本机 Citrix Receiver 或 Citrix Workspace 应用程序使用 GSLB 连接到网关。

```
<?xml version="1.0" encoding="utf-8"?>
<Services version="1.0"
    xmlns="http://www.citrix.com/ServiceRecord">
    <Service type="store">
        <SRID>167659780</SRID>
        <Name>Store</Name>
        <Address>https://storefront.domain.com/Citrix/Store/discovery</Address>
        <Gateways>
            <Gateway Name="EMEAGateway" Default="true" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
            <Gateway Name="USGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
            <Gateway Name="APACGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
        </Gateways>
        <Beacons>
            <Internal>
                <Beacon>https://storefront.domain.com/</Beacon>
            </Internal>
            <External>
                <Beacon>https://emeagateway.domain.com</Beacon>
                <Beacon>https://usgateway.domain.com</Beacon>
                <Beacon>https://apacgateway.domain.com</Beacon>
                <Beacon>http://gslb.domain.com</Beacon>
            </External>
        </Beacons>
    </Service>
</Services>
```

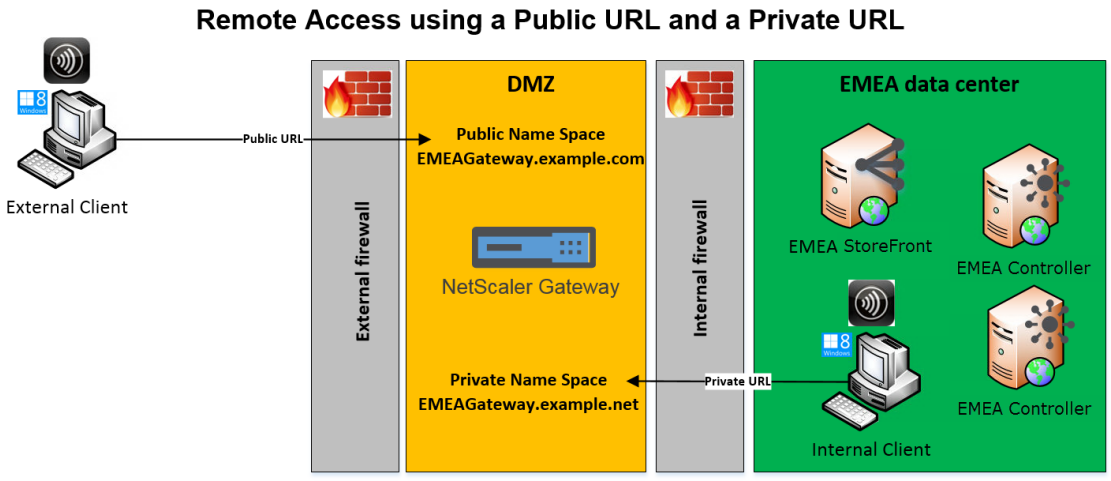
使用 `-GatewayUrl https://emeagateway.domain.com, https://usgateway.domain.com and https://apacgateway.domain.com` 的示例文件 2。这允许本机 Citrix Receiver 或 Citrix Workspace 应用程序使用唯一的 URL 连接到网关。


```
<?xml version="1.0" encoding="utf-8"?>
<Services version="1.0"
    xmlns="http://www.citrix.com/ServiceRecord">
    <Service type="store">
        <SRID>167659780</SRID>
        <Name>Store</Name>
        <Address>https://storefront.domain.com/Citrix/Store/discovery</Address>
        <Gateways>
            <Gateway Name="EMEAGateway" Default="true" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://emeagateway.domain.com/</Location>
            </Gateway>
            <Gateway Name="USGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://ftlgateway.domain.com/</Location>
            </Gateway>
            <Gateway Name="APACGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://bglgateway.domain.com/</Location>
            </Gateway>
        </Gateways>
        <Beacons>
            <Internal>
                <Beacon>https://storefront.domain.com/</Beacon>
            </Internal>
            <External>
                <Beacon>https://emeagateway.domain.com</Beacon>
                <Beacon>https://usgateway.domain.com</Beacon>
                <Beacon>https://apacgateway.domain.com</Beacon>
                <Beacon>http://gslb.domain.com</Beacon>
            </External>
        </Beacons>
    </Service>
</Services>
```

共享 FQDN 由本机 Citrix Receiver 和 Citrix Workspace 应用程序用来进行身份验证。

用例 #2：使用公用 URL 或专用 URL 的单个 Citrix Gateway

管理员可使用同一 Citrix Gateway 在外部使用公用 URL 进行访问以及在内部使用专用 URL 进行访问。



在此示例中：

- 管理员希望对已发布资源和 HDX 启动通信的所有访问都通过 Citrix Gateway，即使客户端是内部的也是如此。
- Citrix Gateway 位于 DMZ 中。
- 有两种不同的网络路由通过 DMZ 任一端的两个防火墙到达 Citrix Gateway。
- 面向公众的外部命名空间不同于内部命名空间。

PowerShell cmdlet 示例

可使用 PowerShell cmdlet **Add-STFRoamingGateway** 和 **Set-STFRoamingGateway** 并带参数 -gslburl 对 StoreFront 网关对象设置 **GslbLocation** 属性。例如：

```
Add-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://
    emeagateway.example.com" -GSLBurl "https://gslb.example.com" -
    SubnetIPAddress "10.0.0.1" -CallbackUrl "https://emeagateway.example
    .com" -LogonType "DomainAndRSA" -SmartCardFallbackLogonType "None" -
    Version "Version10_0_69_4" -SecureTicketAuthorityUrls "https://emea-
    controller.example.com/scripts/ctxsta.dll,https://us-controller.
    example.com/scripts/ctxsta.dll,https://apac-controller.example.com/
    scripts/ctxsta.dll"
Set-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://
    emeagateway.example.com" -GSLBurl "https://gslb.example.com"
Get-STFRoamingGateway -Name "EMEAGateway" (returns just the EMEA
    gateway object)
Or
Get-STFRoamingGateway (returns all gateway object configured in
    StoreFront)
```

对于用例 #1，可以通过将 **GslbLocation** 设置为 NULL 从 EMEAGateway 中删除 GSLBurl。以下 PowerShell 将修改内存中存储的网关对象 $EMEAGateway。**Set-STFRoamingGateway** 之后可以通过 $EMEAGateway 传输以更新 StoreFront 配置并删除 GSLBurl。

```
$EMEAGateway = Get-STFRoamingGateway
$EMEAGateway.GslbLocation = $Null
Set-STFRoamingGateway -Gateway $EMEAGateway
```

对于用例 #1，使用 **Get-STFRoamingGateway** 返回以下网关：

```
Name: EMEAGateway
Location: https://emeagateway.example.com/ (Unique URL for the EMEA
    Gateway)
GslbLocation: https://gslb.example.com/ (GSLB URL for all three
    gateways)

Name: USGateway
Location: https://USgateway.example.com/ (Unique URL for the US Gateway
    )
```



```
GslbLocation: https://gslb.example.com/ (GSLB URL for all three
    gateways)

Name: APACGateway
Location: https://APACgateway.example.com/ (Unique URL for the APAC
    Gateway)
GslbLocation:  https://gslb.example.com/ (GSLB URL for all three
    gateways)
```

对于用例 #2，使用 **Get-STFRoamingGateway** 返回以下网关：

```
Name: EMEAGateway
Location: https://emeagateway.example.com/ (Public URL for the Gateway)
GslbLocation: https://emeagateway.example.net/ (Private URL for the
    Gateway)
```

对于用例 #1，使用 **Get-STFStoreRegisteredOptimalLaunchGateway** 返回最佳网关路由：

```
$StoreObject = Get-STFStoreService -SiteId 1 -VirtualPath "/Citrix/<
    YourStore>"

Get-STFStoreRegisteredOptimalLaunchGateway -StoreService $StoreObject

Hostnames:       {
 emeagateway.example.com, gslb.example.com }

Hostnames:       {
 usgateway.example.com, gslb.example.com }

Hostnames:       {
 apacgateway.example.com, gslb.example.com }
```

每个网关的 **GSLB URL** 或内部 **URL** 都存储在漫游服务 **web.config** 文件中

StoreFront 不在 StoreFront 管理控制台中显示每个网关的 GSLB URL 和 URL，但可以通过打开 StoreFront 服务器上 C:\inetpub\wwwroot\Citrix\Roaming\web.config 中的漫游服务 Web.Config 文件位置来查看所有 GSLB 网关的已配置 GSLBLocation 路径。

用例 **#1**：漫游 **web.config** 文件中的网关


```
<gateway id="cca13269-18c1-10fd-a0df-7931b3897aa8" name="EMEAGateway"
    default="false" edition="Enterprise" version="Version10_0_69_1" auth
    ="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.1" rwmode
    ="NONE" deployment="Appliance" callbackurl=https://emeagateway.
    example.com/CitrixAuthService/AuthService.asmx sessionreliability="
    true" requesttickettwosta="false" stasUseLoadBalancing="false"
    stasBypassDuration="01:00:00">
<location path="https://emeagateway.example.com/" /><gslbLocation path=
    "https://gslb.example.com/" /><clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.com/scripts/ctxsta.dll"
     />
<location path="https://us-controller.example.com/scripts/ctxsta.dll"
    />
<location path="https://apac-controller.example.com/scripts/ctxsta.dll"
     />
</secureticketauthorityurls>
</gateway>

<gateway id="b8ec720c-d85e-1889-8188-1cf08a2cf762" name="USGateway"
    default="false" edition="Enterprise" version="Version10_0_69_1" auth
    ="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.2" rwmode
    ="NONE" deployment="Appliance" callbackurl="https://usgateway.
    example.com/CitrixAuthService/AuthService.asmx" sessionreliability="
    true" requesttickettwosta="false" stasUseLoadBalancing="false"
    stasBypassDuration="01:00:00"><location path="https://usgateway.
    example.com/" /><gslbLocation path="https://gslb.example.com/" /><
    clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.com/scripts/ctxsta.dll"
     />
<location path="https://us-controller.example.com/scripts/ctxsta.dll"
```

```
    />
<location path="https://apac-controller.example.com/scripts/ctxsta.dll"
    />
</secureticketauthorityurls>
</gateway>

<gateway id="c57117b5-e111-1eed-9117-a1ffa1c8100e" name="APACGateway"
    default="false" edition="Enterprise" version="Version10_0_69_1" auth
    ="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.3" rwmode
    ="NONE" deployment="Appliance" callbackurl="https://apacgateway.
    example.com/CitrixAuthService/AuthService.asmx" sessionreliability="
    true" requesttickettwosta="false" stasUseLoadBalancing="false"
    stasBypassDuration="01:00:00"><location path="https://apacGateway.
    example.com/" /><gslbLocation path="https://gslb.example.com/" /><
    clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.com/scripts/ctxsta.dll"
    />
<location path="https://us-controller.example.com/scripts/ctxsta.dll"
    />
<location path="https://apac-controller.example.com/scripts/ctxsta.dll"
    />
</secureticketauthorityurls>
</gateway>
```

用例 **#2**：漫游 **web.config** 文件中的网关

```
<gateway id="cca13269-18c1-10fd-a0df-7931b3897aa8" name="EMEAGateway"
    default="false" edition="Enterprise" version="Version10_0_69_1" auth
    ="Domain" smartcardfallback="None" ipaddress="10.0.0.1" rwmode="NONE
    " deployment="Appliance" callbackurl="https://emeagateway.example.
    com/CitrixAuthService/AuthService.asmx" sessionreliability="true"
    requesttickettwosta="false" stasUseLoadBalancing="false"
    stasBypassDuration="01:00:00">
<location path="https://emeagateway.example.com/" />
<gslbLocation path=" https://emeagateway.example.net/" />
<clusternodes>
```

```
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.net/scripts/ctxsta.dll"
    />
</secureticketauthorityurls>
</gateway>
```

相关信息

参阅开发人员文档中的 Citrix StoreFront SDK PowerShell 模块。

针对委派表单身份验证 (DFA) 配置 Citrix ADC 和 StoreFront

June 5, 2020

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-27
    a5980f716c
RootInstance                    : 5d0cdc75-1dee-4df7-8069-7375
    d79634b3
TenantId                        : 860e9401-39c8-4f2c-928d-34251102
    b840
Data                            : {
  }

ReadOnlyData                    : {
 [Name, DelegatedFormsServer], [Cmdlet, Add-DSWebFeature], [Snapin
    , Citrix.DeliverySer
                                  vices.Web.Commands], [Tenant, 860
                                      e9401-39c8-4f2c-928d-34251102
                                      b840] }

ParameterData                   : {
 [FeatureClassId, e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc], [
```

```
      ParentInstanceId, 8dd182c7-f
24                                970-466c-ad4c-27a5980f716c], [
                                     TenantId, 860e9401-39c8-4f2c
                                     -928d-34251102b840] }
25
26 AdditionalInstanceDependencies : {
27  b1e48ef0-b9e5-4697-af9b-0910062aa2a3 }
28
29 IsDeployed                     : True
30 FeatureClass                   : Citrix.DeliveryServices.Framework
      .Feature.FeatureClass
```

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。

```
1 PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Add-
     DSCitrixPSKTrustedClient -clientId netscaler.fqdn.com -
     passphrase secret
```

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。

```
1  <example connectorURL="http://Example.connector.url:8080/adapters-
      sf-aaconnector-webapp">
2     <routeTable order="1000">
3       <routes>
4         <route name="StartExampleAuthentication" url="Example-
             Bridge-Forms/Start">
5           <defaults>
6             <add param="controller" value="
                 ExplicitFormsAuthentication" />
7             <add param="action" value="AuthenticateStart" />
8             <add param="postbackAction" value="Authenticate" />
9             <add param="cancelAction" value="CancelAuthenticate"
                  />
10            <add param="conversationFactory" value="
                 ExampleBridgeAuthentication" />
11            <add param="changePasswordAction" value="
                 StartChangePassword" />
12            <add param="changePasswordController" value="
                 ChangePassword" />
```



```
13                <add param="protocol" value="CustomForms" />
14              </defaults>
15            </route>
```

4. 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。

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Set-
   DSDFAProperty -ConversationFactory ExampleBridgeAuthentication
```

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

December 2, 2020

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

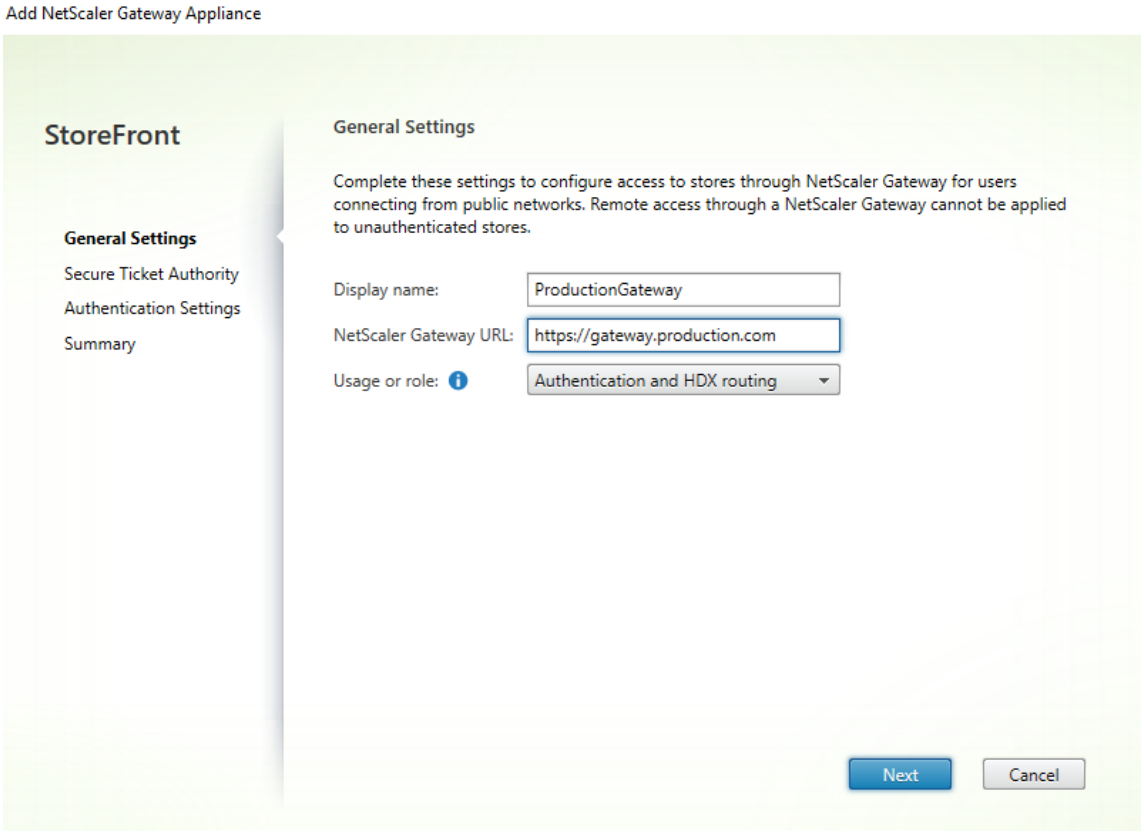
此示例中的 `development.com` 域的设置方式如下所示：

- 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。

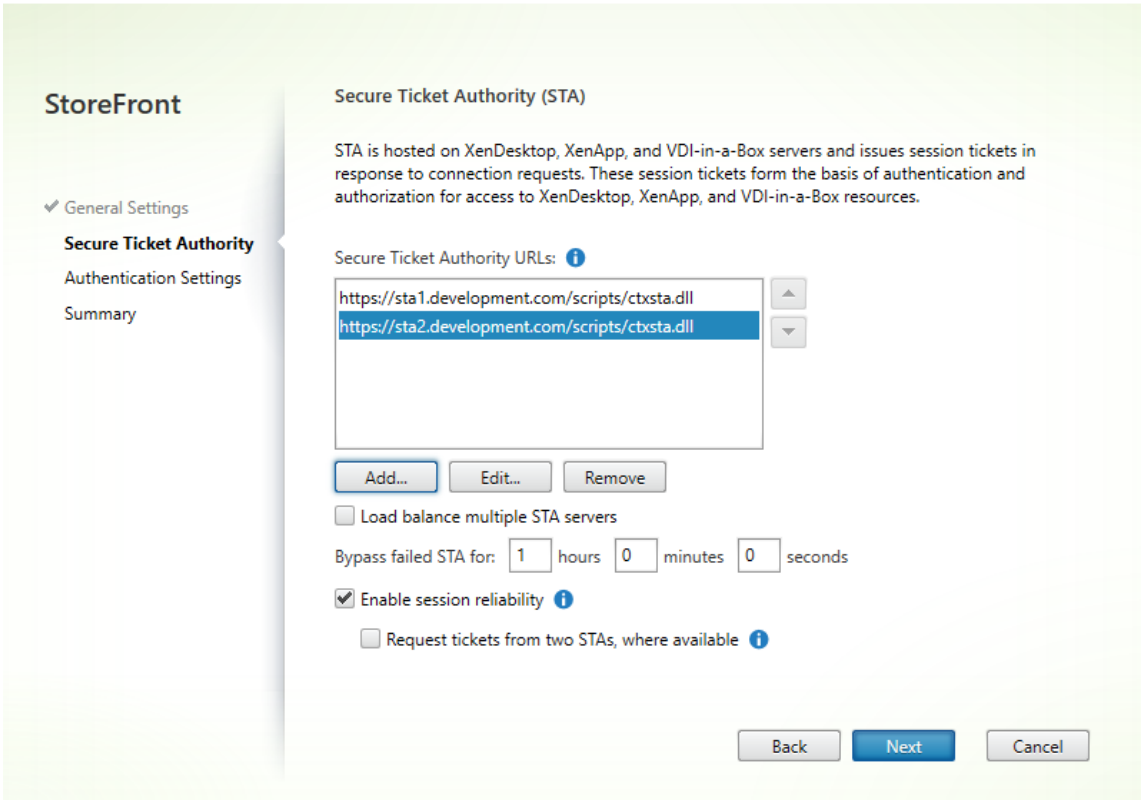
为应用商店配置 **Citrix Gateway**

要为应用商店配置 Citrix Gateway，请执行以下操作：

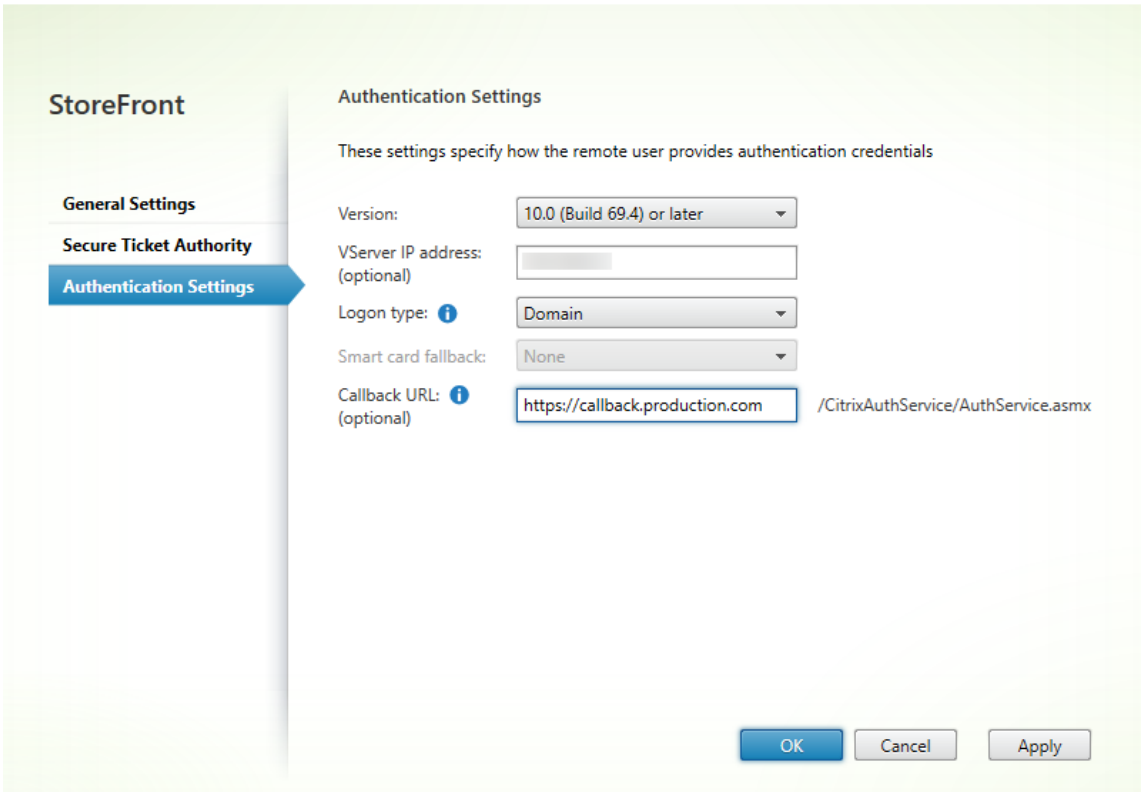
1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择应用商店，然后在操作窗格中单击管理 **Citrix Gateway**。
2. 在“管理 Citrix Gateway”屏幕中，单击添加。
3. 完成“常规设置”、“Secure Ticket Authority”和“身份验证”步骤。



Add NetScaler Gateway Appliance



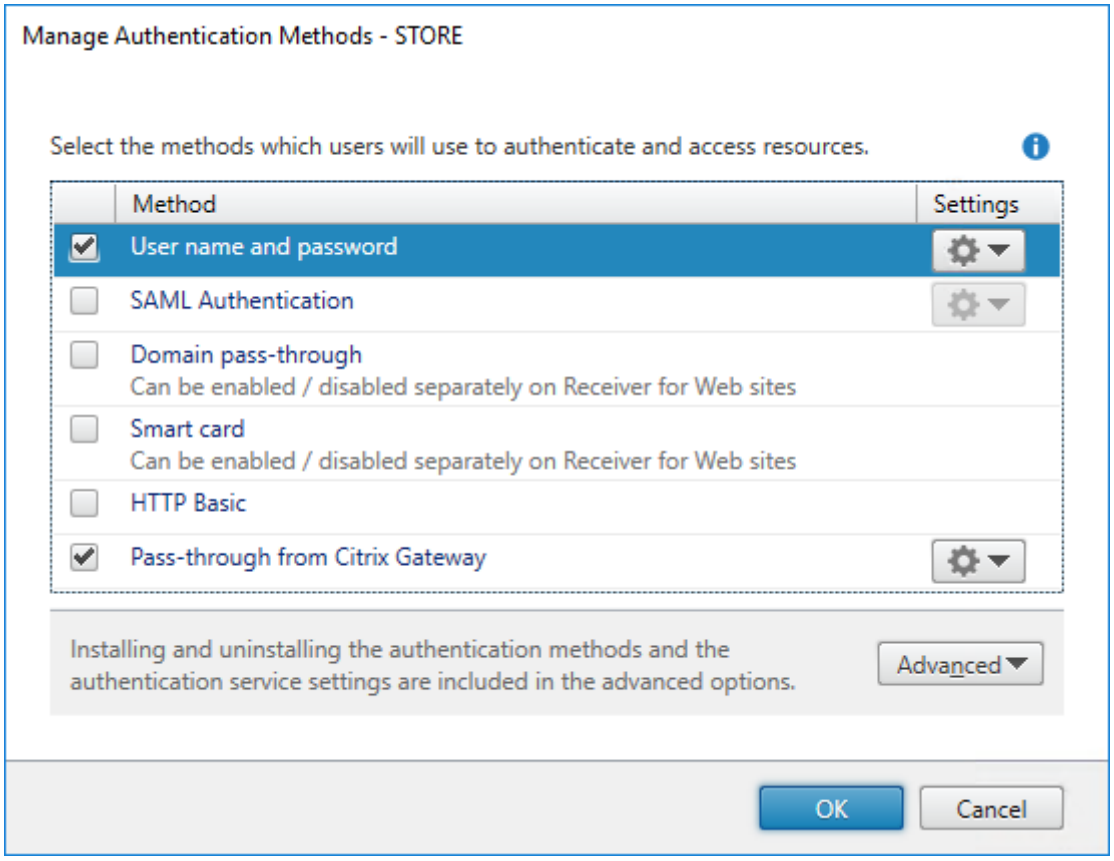
Edit NetScaler Gateway appliance - ProductionGateway



> 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)。

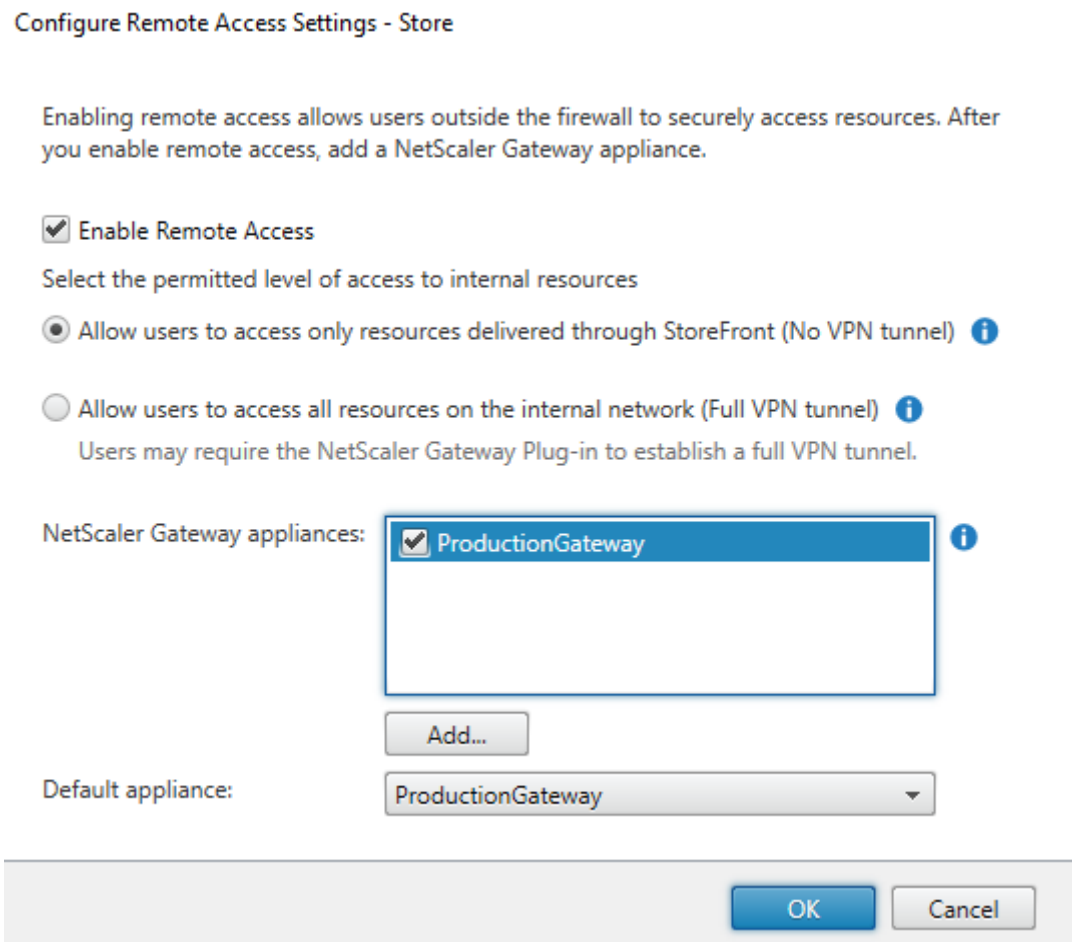
启用从 **Citrix Gateway** 直通

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。



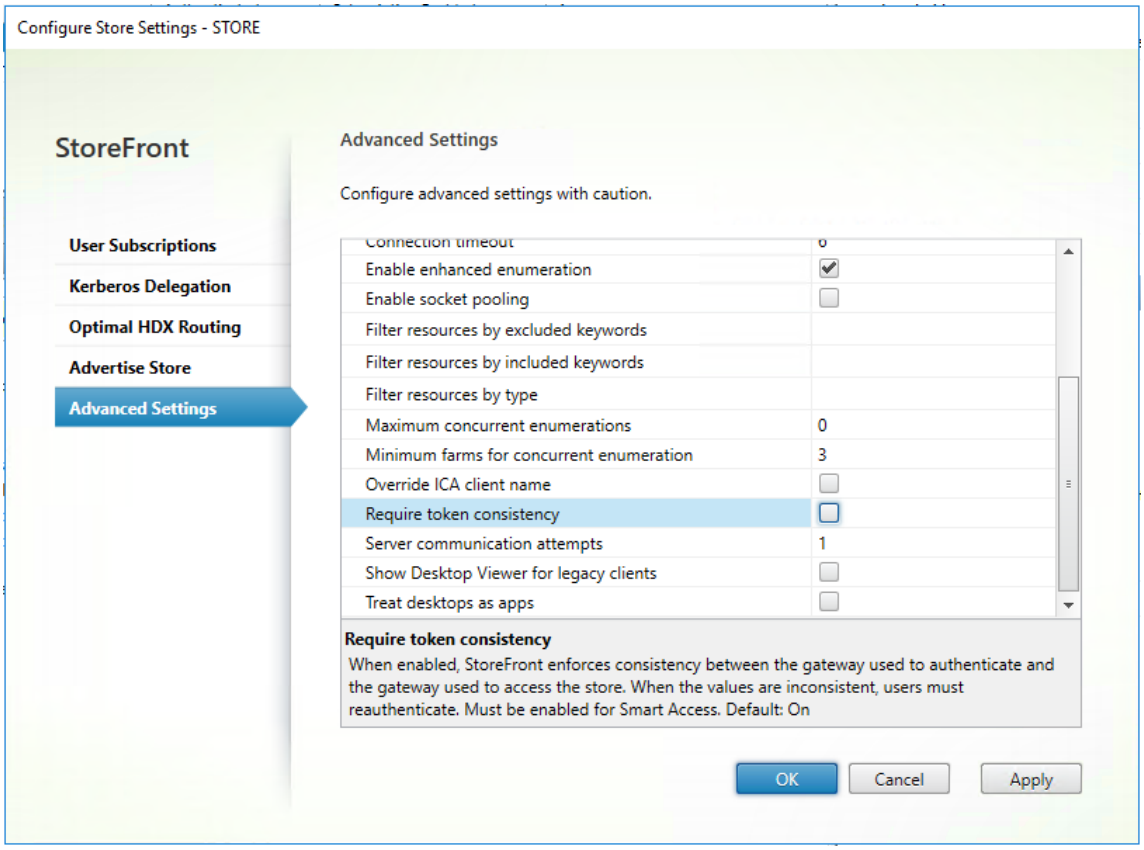
配置应用商店以便使用网关进行远程访问

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。

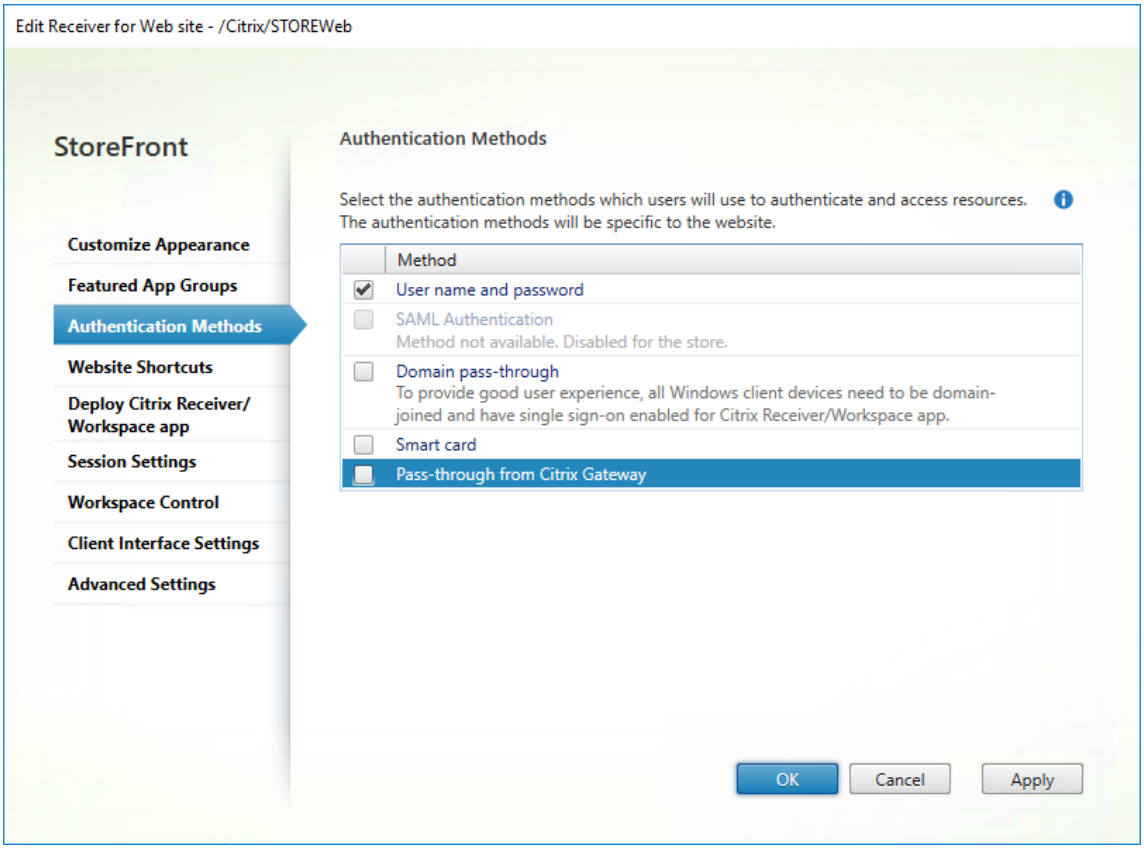


> 注意：
>
> “要求令牌一致”设置默认处于选中状态。如果禁用此设置，用于 Citrix ADC 端点分析 (EPA) 的 SmartAccess 功能将停止运行。有关 SmartAccess 的详细信息，请参阅 CTX138110。

对 **Receiver for Web** 站点禁用从 **Citrix Gateway** 直通

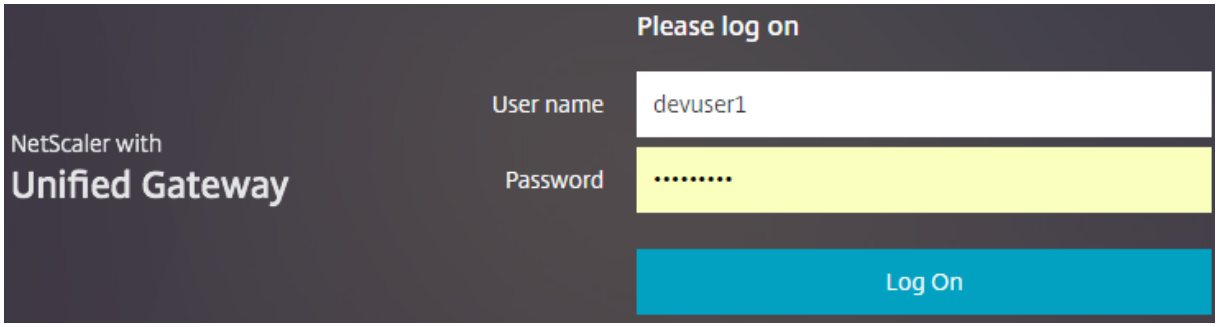
> 重要：
>
> 禁用从 Citrix Gateway 直通将阻止 Receiver for Web 尝试使用 `production.com` 域中不正确的凭据从 Citrix ADC 设备通过。禁用从 Citrix Gateway 直通会导致 Receiver for Web 提示用户输入凭据。这些凭据与用于通过 Citrix Gateway 登录的凭据不同。

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。

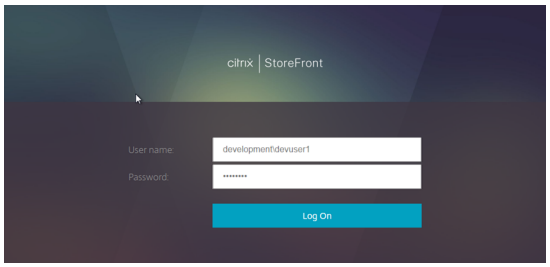


使用 **production.com** 用户和凭据登录网关

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。

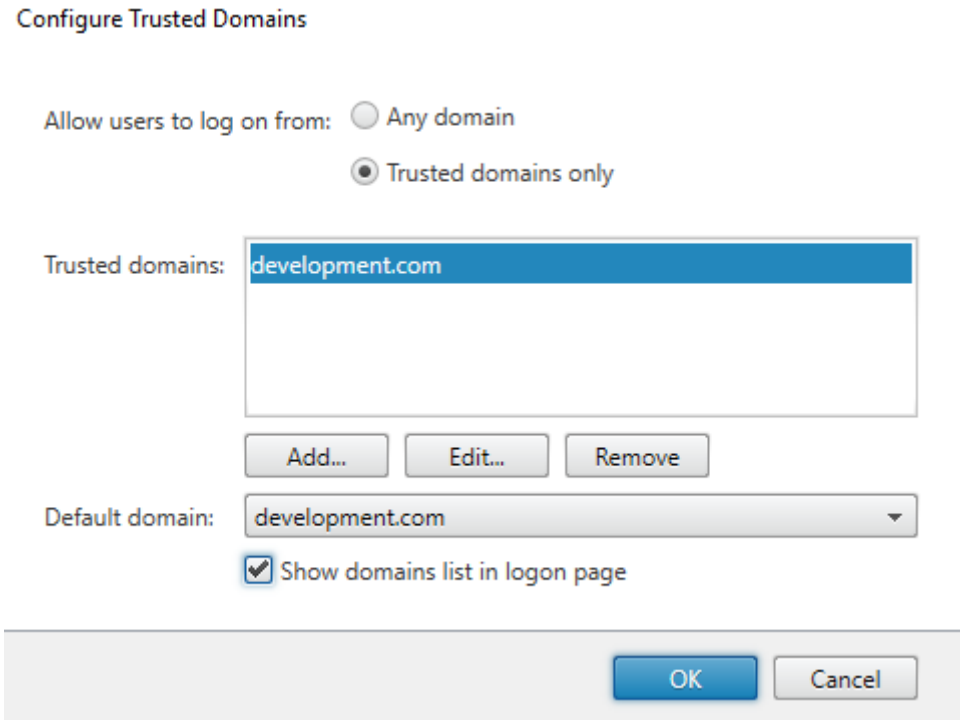


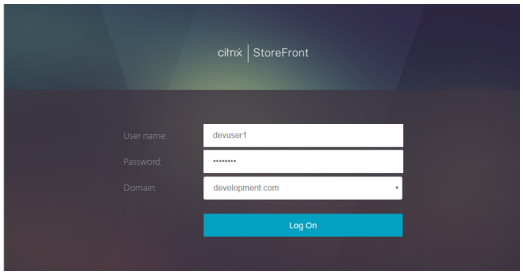
在 **StoreFront** 中添加可信域下拉列表（可选）

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。

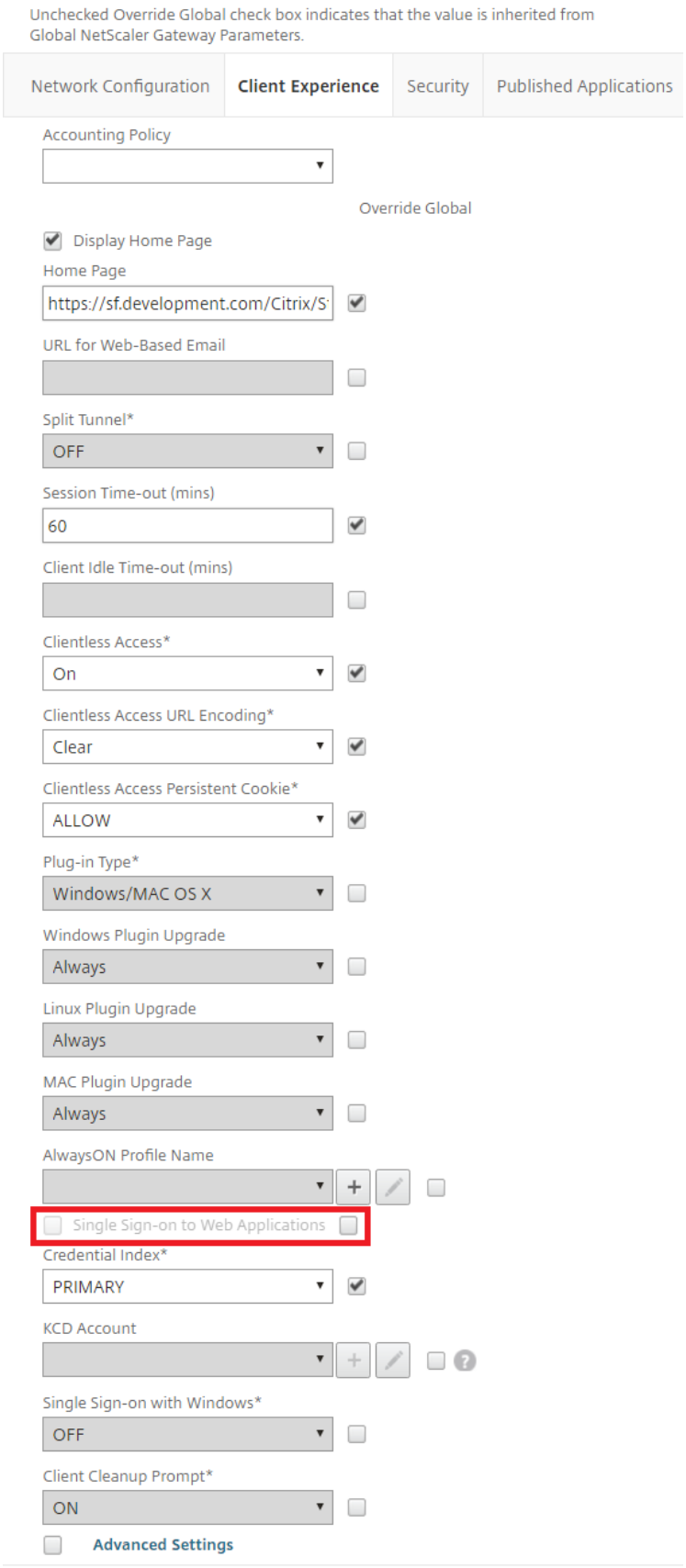


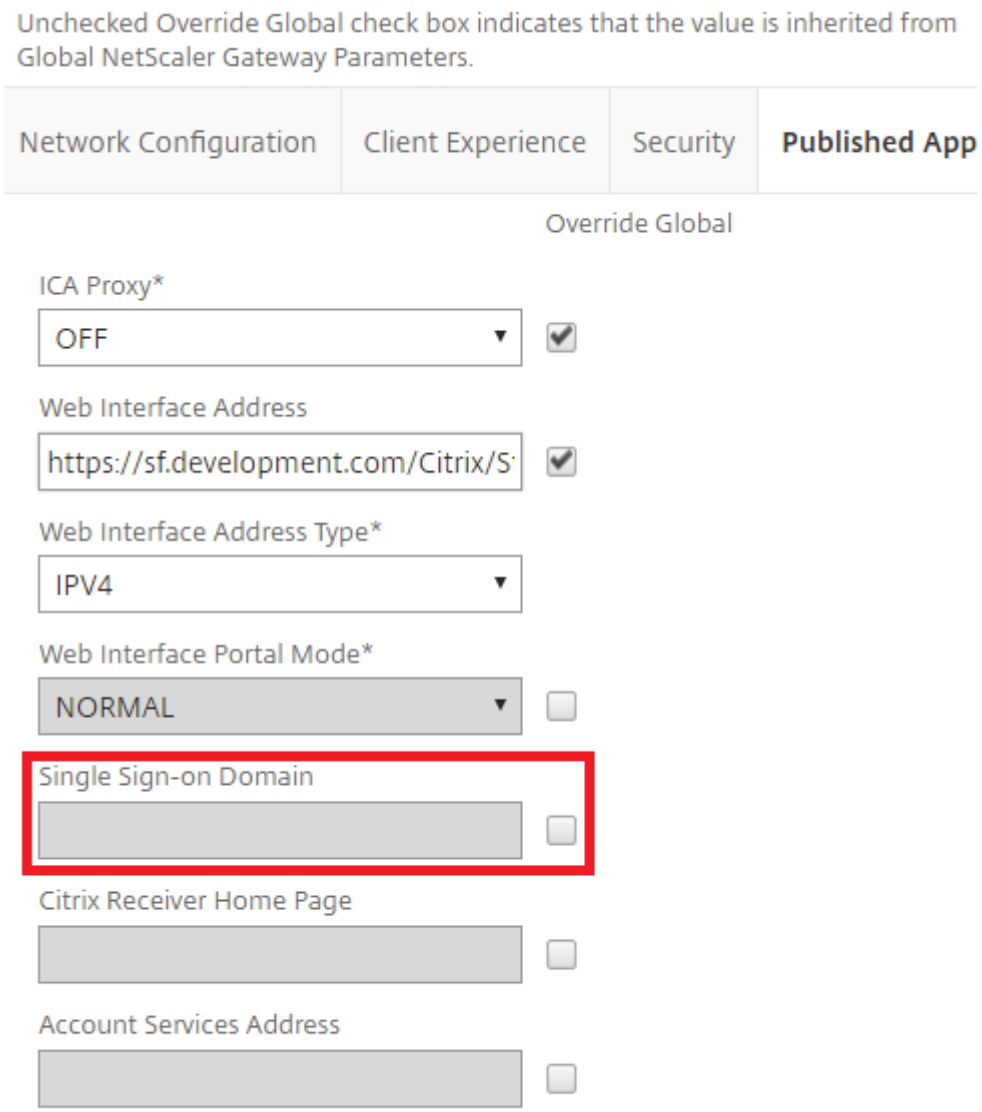


> 注意：
>
> 不建议在此身份验证场景中使用浏览器密码缓存。如果用户为两个不同的域帐户设置了不同的密码，密码缓存会导致体验较差。

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

June 5, 2020

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 使用部署的服务器 URL 或负载平衡的 URL 作为内部信标点。使用所添加的第一个 Citrix Gateway 部署的 Citrix Web 站点和虚拟服务器或用户登录点（对于 Access Gateway 5.0）URL 作为外部信标点。

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。如果为应用商店配置了 Receiver for Web 站点，则用户可以从该站点获取更新的 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，
> 将配置更改传播到服务器组，以便更新部署中的其他服务器。

1. 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。
3. 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。
4. 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性外部信标点，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。

创建单个完全限定的域名 (FQDN) 以在内部和外部访问应用商店

December 2, 2020

您可以通过 Citrix Gateway 提供对企业网络资源和 Internet 资源的访问权限，并通过为内部和外部漫游客户端创建单个 FQDN 来简化用户体验。

创建单个 FQDN 对配置任一本机 Receiver 的用户很有帮助。无论当前连接到的是内部网络还是公用网络，他们只需记住单个 URL 即可。

Citrix Workspace 应用程序的 StoreFront 信标

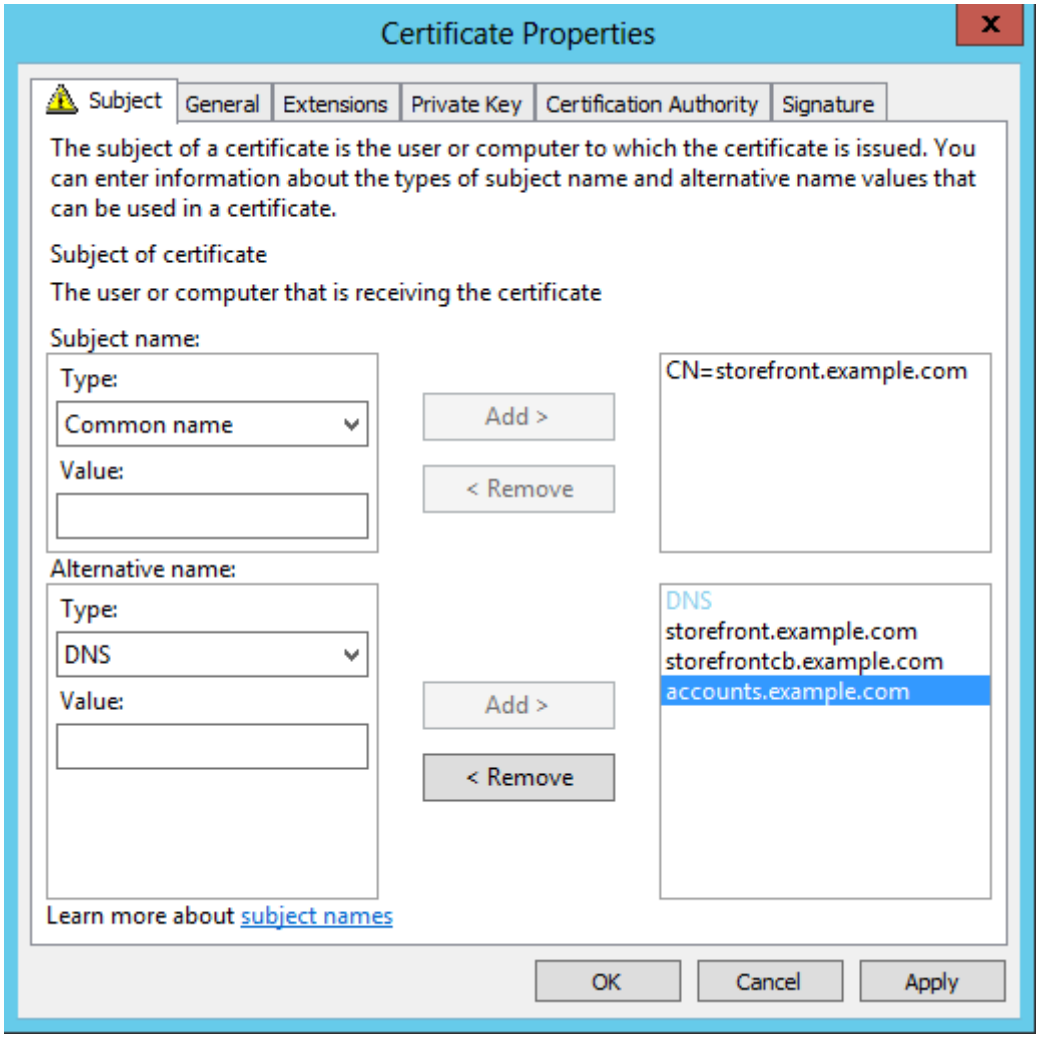
Citrix Workspace 应用程序尝试联系信标点并根据响应来确定用户是连接到本地网络还是公用网络。用户访问桌面或应用程序时，位置信息将传递给提供资源的服务器，以便能够将相应的连接详细信息返回给 Citrix Workspace 应用程序。这样可以确保在用户访问桌面或应用程序时不会收到重新登录提示。有关配置信号点的信息，请参阅配置信标点。

> 注意：
>
> 在本文中，除非另行说明，否则 “Citrix Workspace 应用程序” 的提及也适用于受支持的 Citrix Receiver 版本。

配置 Citrix Gateway 虚拟服务器和 SSL 证书

外部客户端尝试从企业网络外部访问资源时，共享 FQDN 解析到 DMZ 中的外部防火墙路由器接口 IP 或 Citrix Gateway 虚拟服务器 IP。确保 SSL 证书的 “Common Name”（公用名）和 “Subject Alternative Name”（使用者可选名称）字段包含用于在外部访问应用商店的共享 FQDN。通过使用第三方根 CA（例如 Verisign）代替企业证书颁发机构 (CA) 对网关证书进行签名，任何外部客户端都将自动信任绑定到网关虚拟服务器的证书。如果您使用第三方根 CA（例如 Verisign），则无需将任何其他根 CA 证书导入到外部客户端上。

要将具有共享 FQDN 公用名的单个证书部署到 Citrix Gateway 和 StoreFront 服务器，请考虑您是否希望支持远程发现。如果是，请确保证书遵循使用者可选名称的规范。



Citrix Gateway 虚拟服务器示例证书：**`storefront.example.com`**

1. 确保共享 FQDN、回调 URL 以及帐户别名 URL 包含在 DNS 字段中作为使用者可选名称 (SAN)。
2. 确保私钥可导出，以便证书和密钥能够导入到 Citrix Gateway 中。
3. 确保已将“默认授权”设置为“允许”。
4. 使用第三方 CA（例如 Verisign）或组织的企业根 CA 对证书进行签名。

两节点服务器组示例 **SAN**

`storefront.example.com`（必选）

`storefrontcb.example.com`（必选）

`accounts.example.com`（必选）

`storefrontserver1.example.com`（可选）

`storefrontserver2.example.com`（可选）

使用证书颁发机构 **(CA)** 对 **Citrix Gateway** 虚拟服务器 **SSL** 证书进行签名

根据您的要求，有两个选项可用于选择 CA 签名证书的类型。

- 选项 1 - 第三方 CA 签名证书：如果绑定到 Citrix Gateway 虚拟服务器的证书由可信第三方签署，外部客户端可能无需将任何根 CA 证书复制到其可信根 CA 证书存储中。Windows 客户端附带最常见签署机构的根 CA 证书。可以使用的第三方商业 CA 的示例包括 DigiCert、Thawte 和 Verisign。请注意，诸如 iPad、iPhone 以及 Android 平板电脑和手机之类的移动设备可能仍需将根 CA 复制到设备上，这样才能信任 Citrix Gateway 虚拟服务器。
- 选项 2 - 企业根 CA 签名证书：如果选择此选项，每个外部客户端都需将企业根 CA 证书复制到其可信根 CA 存储中。如果使用安装了本机 Receiver 的便携式设备（例如 iPhone 和 iPad），请在这些设备上创建安全配置文件。

将根证书导入便携式设备

- iOS 设备可以使用电子邮件附件导入.CER x.509 证书文件，因为通常无法访问 iOS 设备的本地存储。
- Android 设备也需要使用相同的.CER x.509 格式。可从设备本地存储或电子邮件附件导入证书。

外部 **DNS**：**storefront.example.com**

确保贵组织的 Internet 服务提供商所提供的 DNS 解析解析到 DMZ 外边缘上防火墙路由器面向外部的 IP，或者解析到 Citrix Gateway 虚拟服务器 VIP。

拆分视图 **DNS**

- 如果正确配置了拆分视图 DNS，DNS 请求的源地址应将客户端发送到正确的 DNS A 记录。
- 客户端在公共网络与企业网络之间漫游时，其 IP 应发生变化。客户端查询 storefront.example.com 时应收到正确的 A 记录，具体取决于其当前连接到的网络。

将 **Windows CA** 颁发的证书导入 **Citrix Gateway**

WinSCP 是极其有用的第三方免费工具，可将文件从 Windows 计算机移动到 Citrix Gateway 文件系统。将要导入的证书复制到 Citrix Gateway 文件系统内的 /nsconfig/ssl/ 文件夹。可以在 Citrix Gateway 上使用 OpenSSL 工具从 PKCS12/PFX 文件提取证书和密码，以便以 Citrix Gateway 可以使用的 PEM 格式创建两个单独的.CER 和.KEY X.509 文件

1. 将 PFX 文件复制到 Citrix Gateway 设备或 VPX 上的 /nsconfig/ssl 中。
2. 打开 Citrix Gateway 命令行界面。
3. 要切换到 FreeBSD shell，请键入 **Shell** 以退出 Citrix Gateway 命令行接口。
4. 要更改目录，请使用 `cd /nsconfig/ssl`

5. 运行`openssl pkcs12 -in <imported cert file>.pfx -nokeys -out <certfilename>.cer`，并在出现提示时输入 PFX 密码。
6. 运行`openssl pkcs12 -in <imported cert file>.pfx -nocerts -out <keyfilename>.key`
7. 出现提示时输入 PFX 密码，然后设置私钥 PEM 暗码以保护.KEY 文件。
8. 要确保已在 /nsconfig/ssl/ 内成功创建.CER 和.KEY 文件，请运行 `ls -al`。
9. 要返回 Citrix Gateway 命令行接口，请键入 Exit。

Citrix Receiver for Windows 或 **Citrix Receiver for Mac**、**Citrix Gateway** 会话策略

REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS

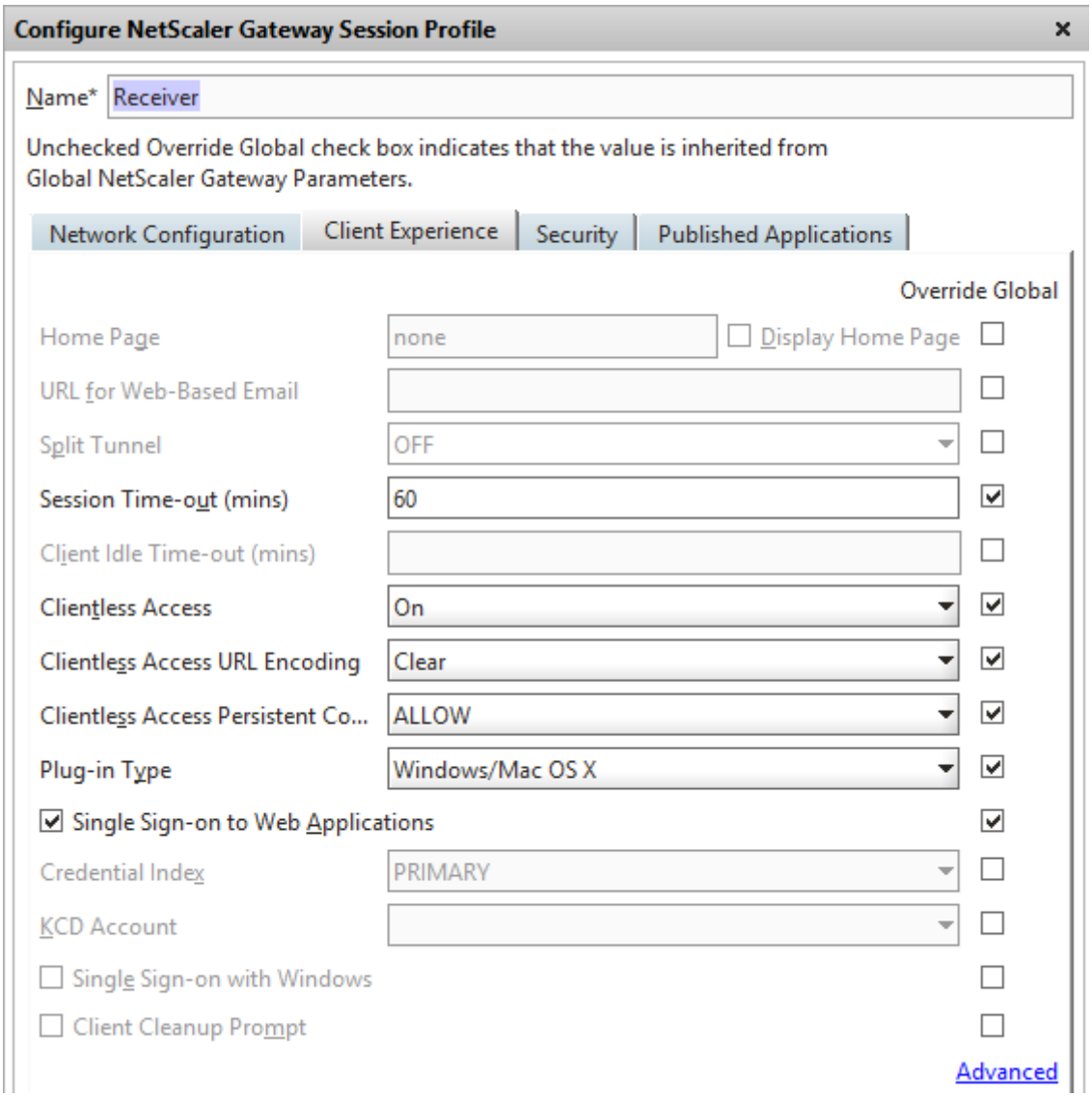
Receiver for Web 网关会话策略

REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS

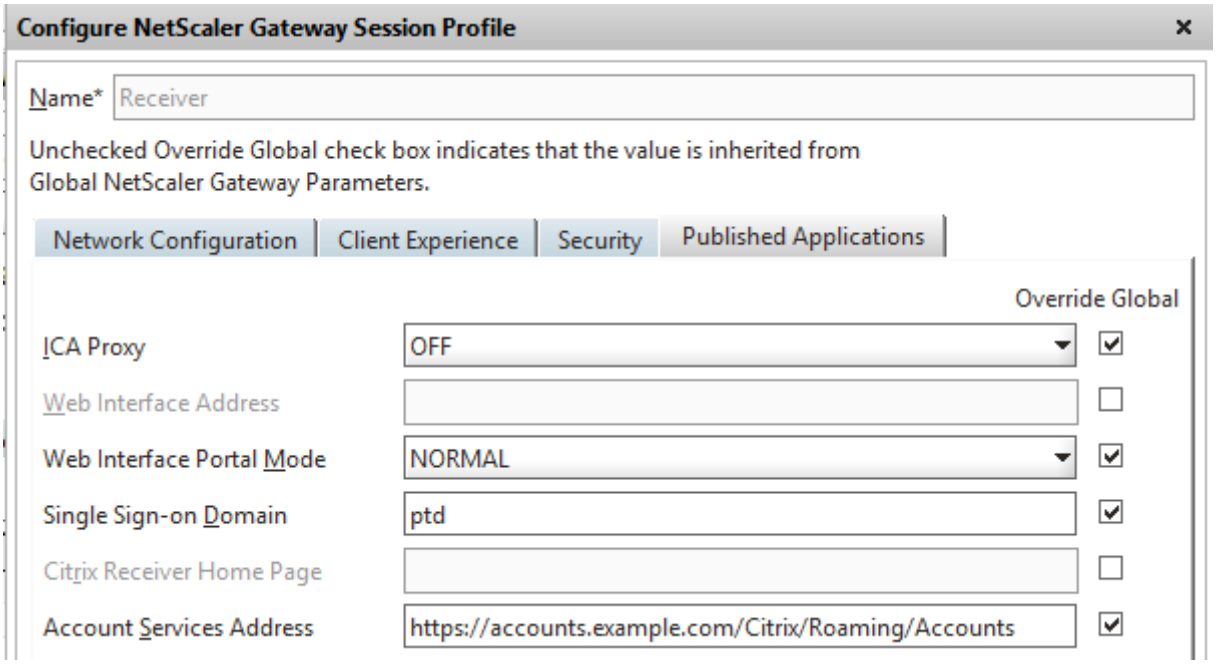
cVPN 和智能访问设置

如果使用 SmartAccess，请在 Citrix Gateway 虚拟服务器属性页面上启用智能访问模式。访问远程资源的每个并发用户都需要使用通用许可证。

Receiver 配置文件

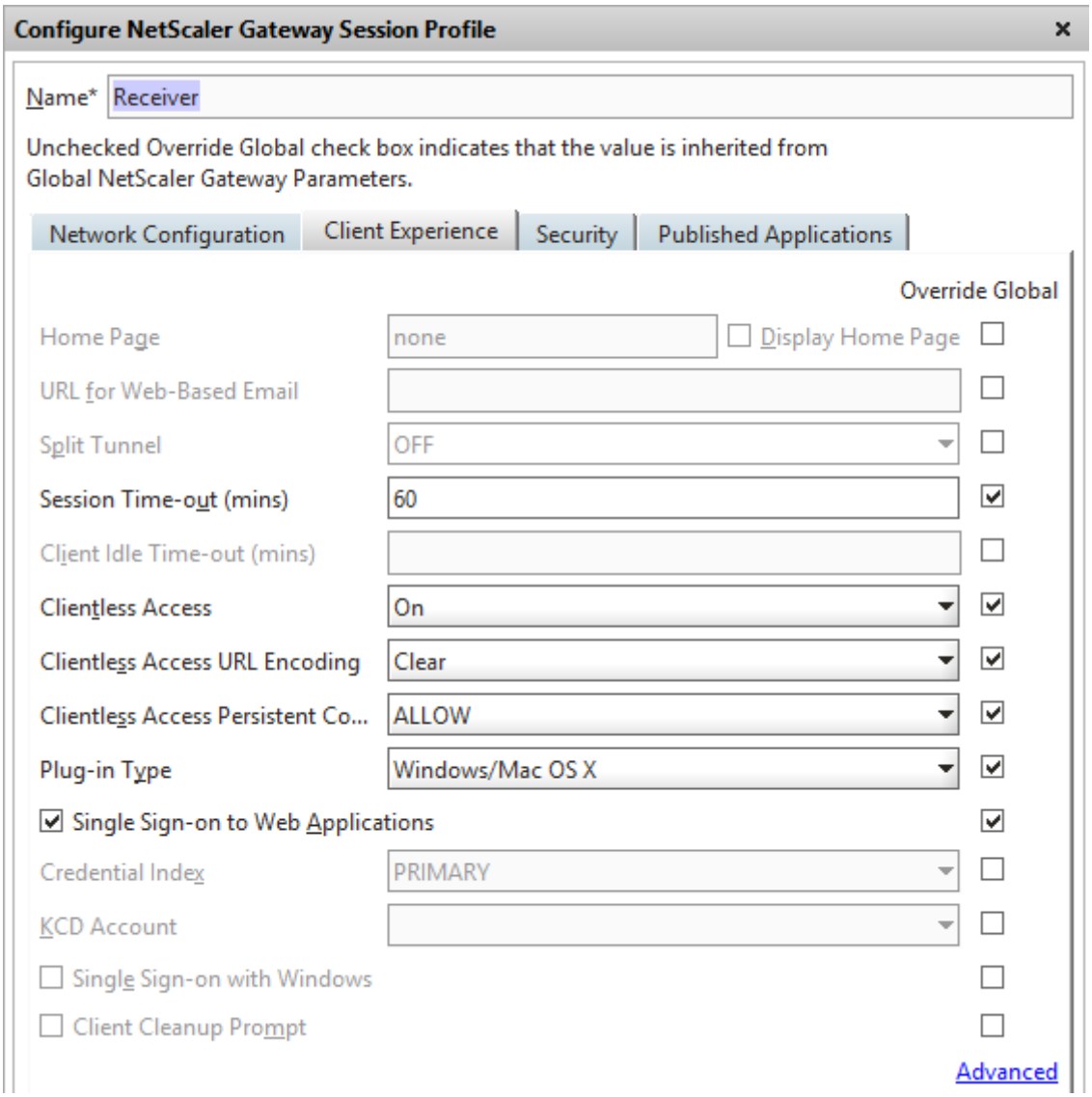


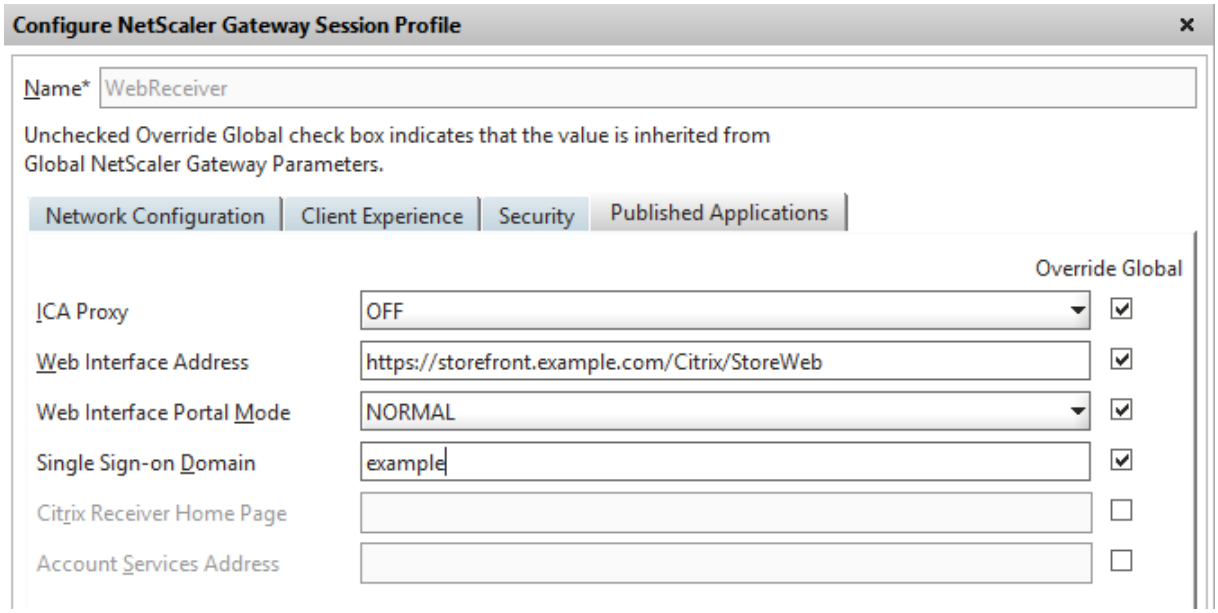
将会话配置文件帐户服务 URL 配置为 `https://accounts.example.com/Citrix/Roaming/Accounts`，而不是 `https://storefront.example.com/Citrix/Roaming/Accounts`。



此外，请在 StoreFront 服务器上的身份验证和漫游 web.config 文件中添加此 URL 作为附加 <allowedAudiences>。有关详细信息，请参阅下面的“配置 StoreFront 服务器主机基本 URL、网关和 SSL 证书”部分。

Receiver for Web 配置文件

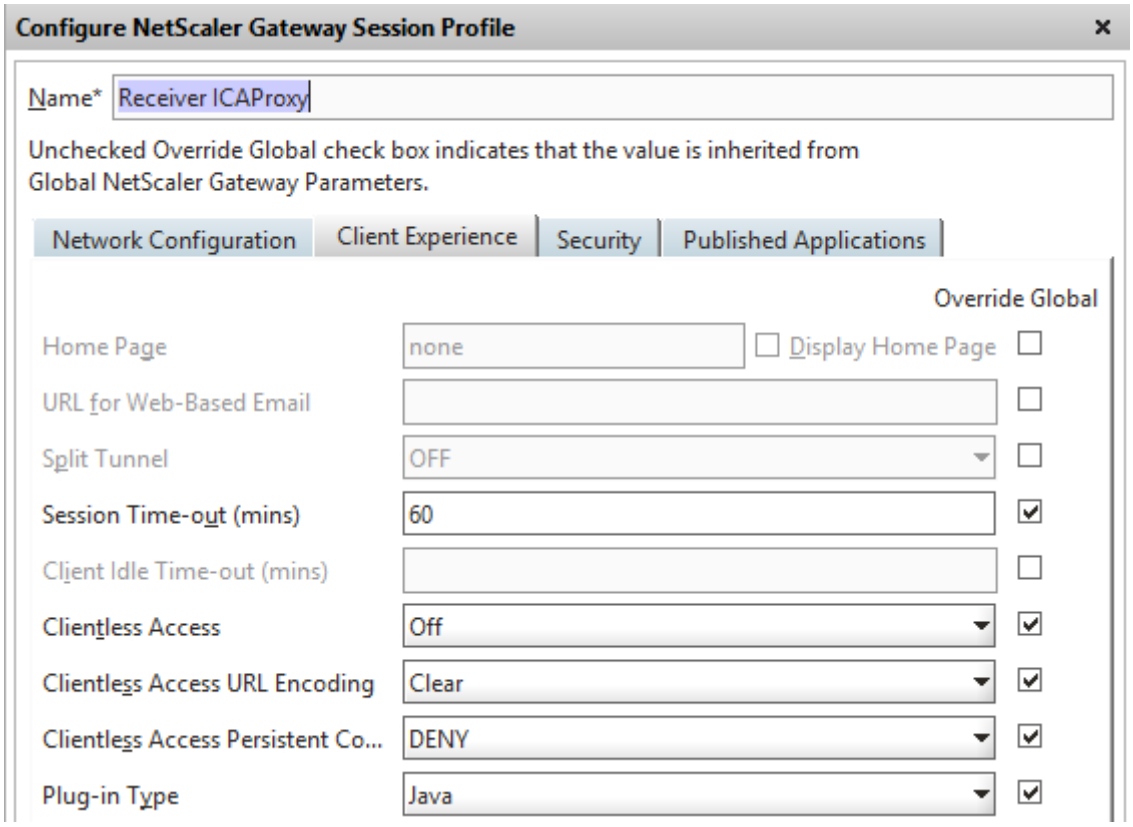


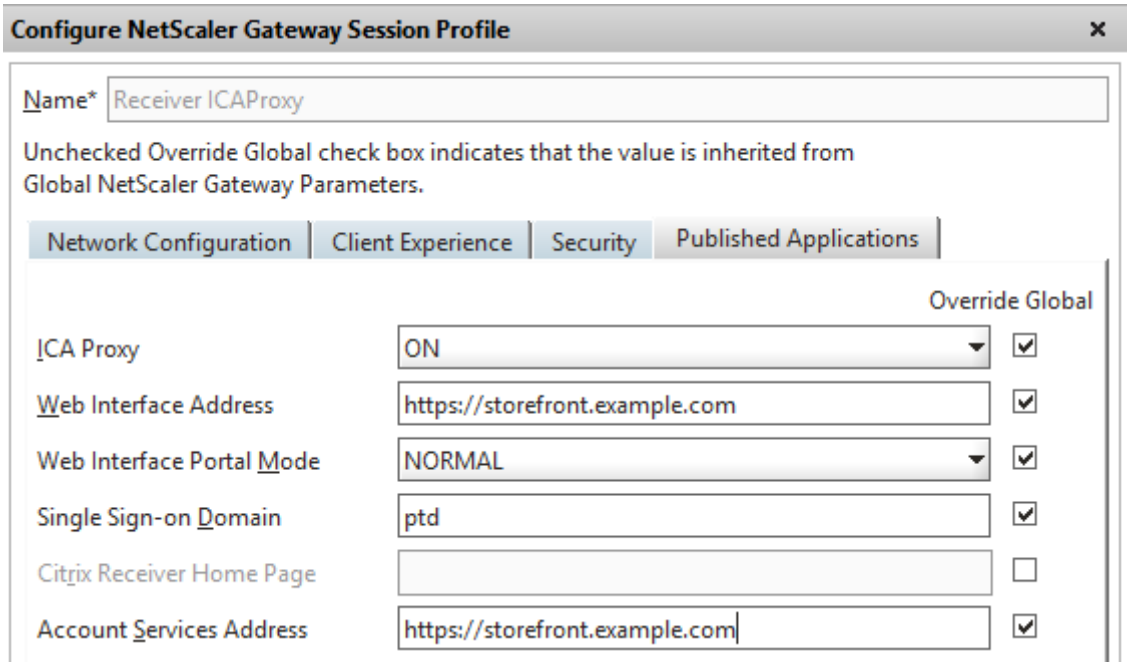


ICA 代理和基本模式设置

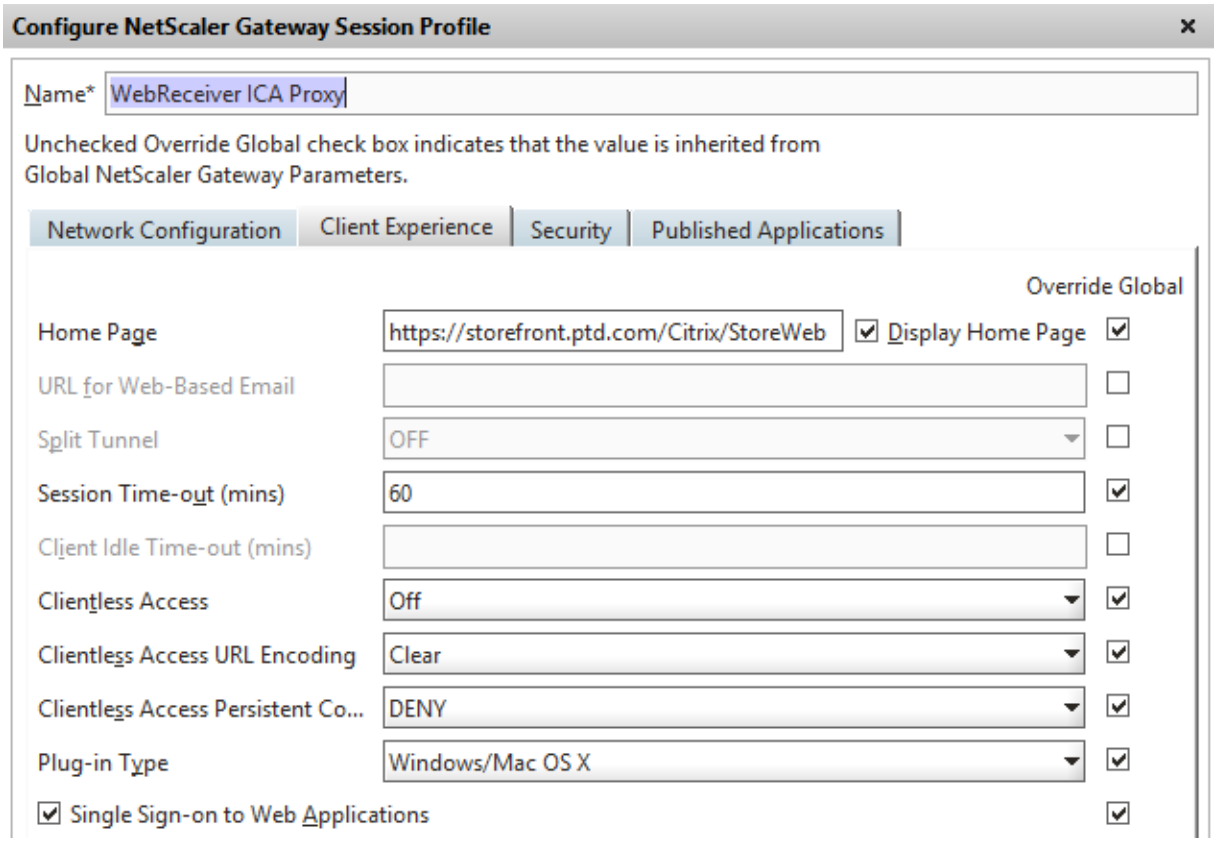
如果使用 ICA 代理，请在 Citrix Gateway 虚拟服务器属性页面上启用基本模式。只需使用 Citrix ADC 平台许可证。

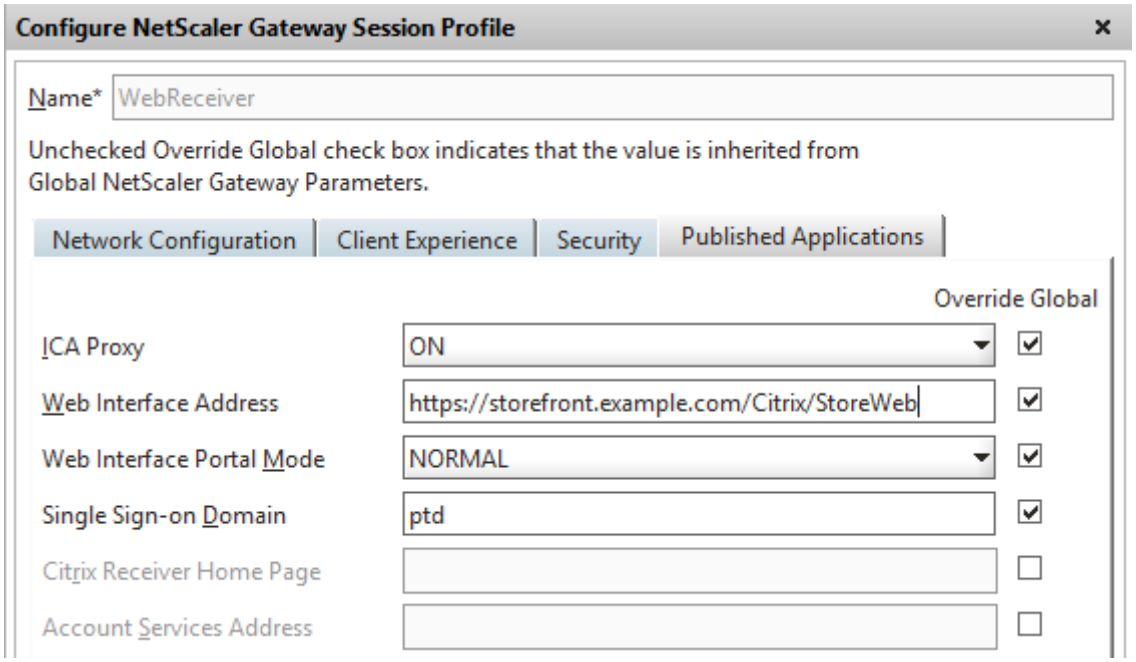
Receiver 配置文件





Receiver for Web 配置文件





配置 **StoreFront** 服务器主机基本 **URL**、网关和 **SSL** 证书

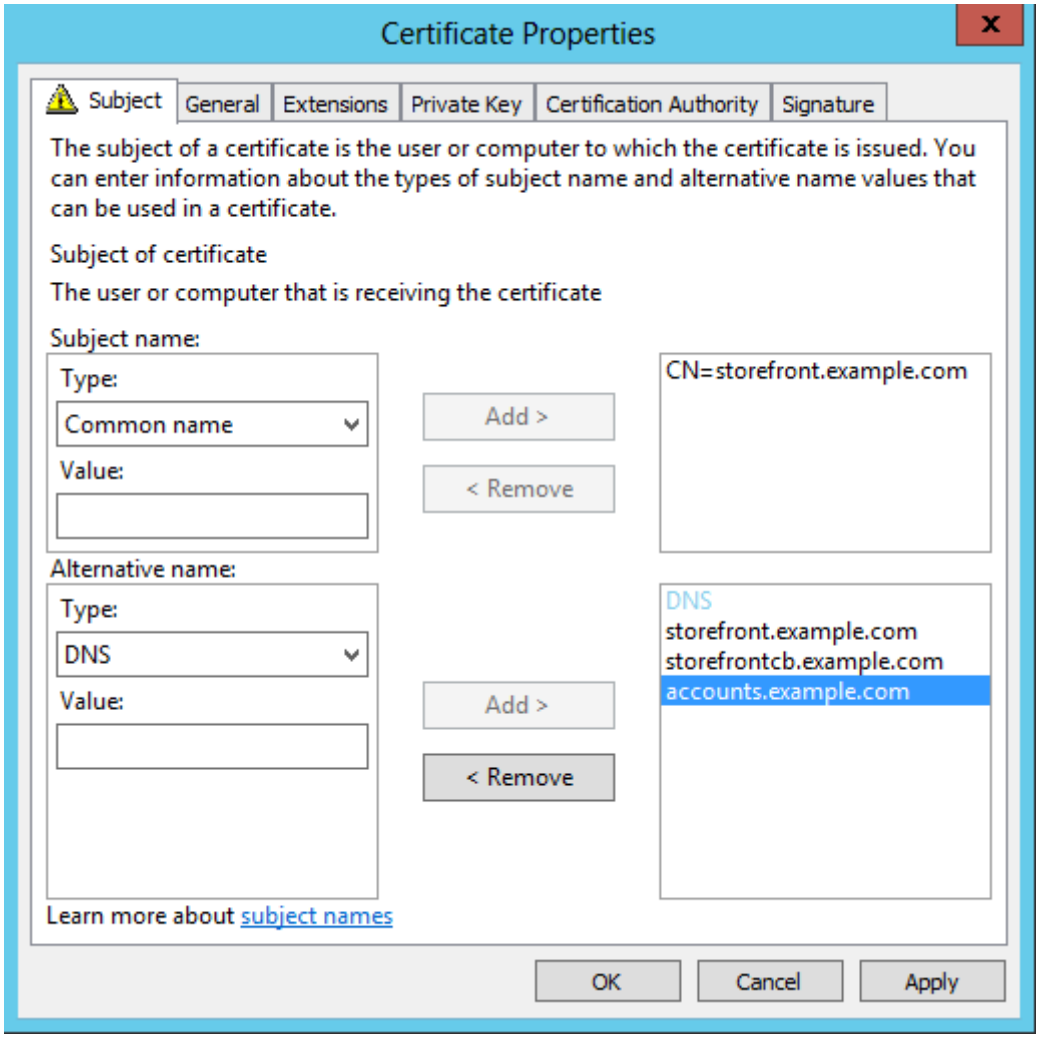
解析到 Citrix Gateway 虚拟服务器的同一共享 FQDN 还应直接解析到 StoreFront 负载平衡器（如果已创建 StoreFront 群集）或托管应用商店的单个 StoreFront IP。

内部 **DNS**：创建三个 **DNS A** 记录

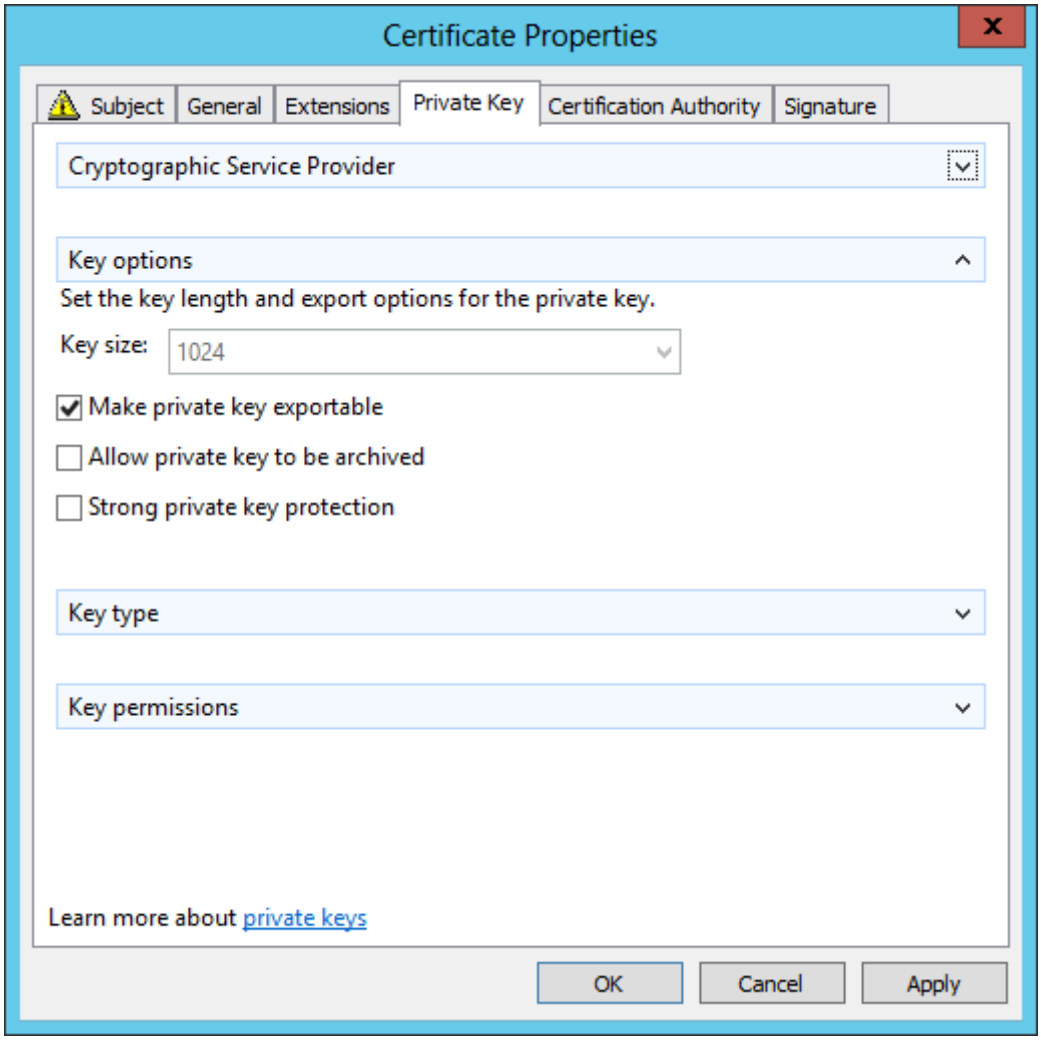
- storefront.example.com 应解析为 StoreFront 负载平衡器或单个 StoreFront 服务器 IP。
- 如果 DMZ 和企业本地网络之间存在防火墙，则 storefrontcb.example.com 应解析为网关虚拟服务器 VIP 以允许此情况。
- accounts.example.com — 作为 storefront.example.com 的 DNS 别名创建。它也解析到 StoreFront 群集的负载平衡器 IP 或单个 StoreFront 服务器 IP。

StoreFront 服务器示例证书：**storefront.example.com**

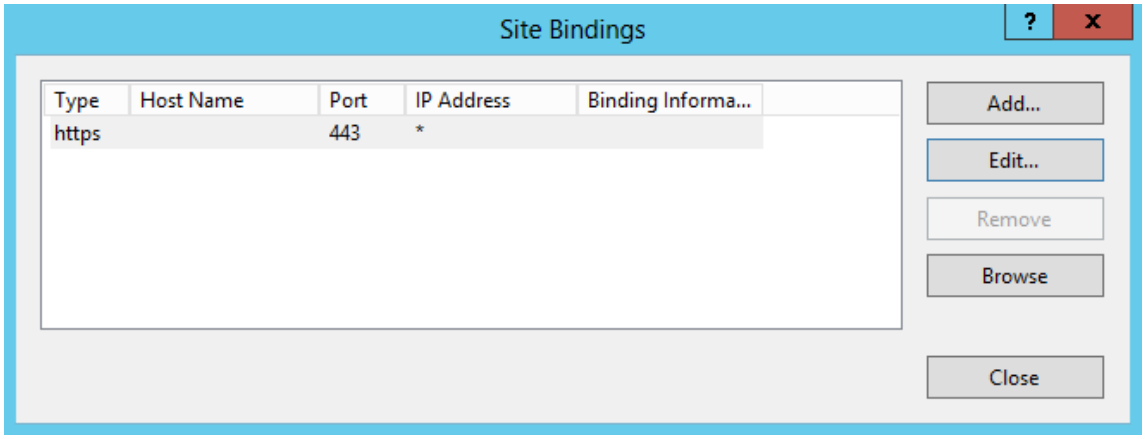
1. 安装 StoreFront 之前，为 StoreFront 服务器或服务器组创建恰当的证书。
2. 将共享 FQDN 添加到 “Common name”（公用名）和 DNS 字段中。确保这与绑定到之前创建的 Citrix Gateway 虚拟服务器的 SSL 证书中所使用的 FQDN 相匹配，或使用绑定到 Citrix Gateway 虚拟服务器的相同证书。
3. 将帐户的别名 (`accounts.example.com`) 作为另一个 SAN 添加到证书中。请注意，SAN 中使用的帐户别名是在先前过程（本机 **Receiver Gateway** 会话策略和配置文件）的 Citrix Gateway 会话配置文件中使用的帐户别名。



4. 确保私钥可导出，以便证书能够转移到其他服务器或多个 StoreFront 服务器组节点。



5. 使用第三方 CA（例如 Verisign）、企业根 CA 或中间 CA 对证书进行签名。
6. 以 PFX 格式导出证书（包括私钥）。
7. 将证书和私钥导入到 StoreFront 服务器中。如果要部署 Windows NLB StoreFront 群集，请将证书导入到每个节点中。如果使用的是备用负载平衡器（例如 Citrix ADC 负载平衡虚拟服务器），请改为在其中导入证书。
8. 在 StoreFront 服务器的 IIS 中创建 HTTPS 绑定，并将导入的 SSL 证书绑定到其上。



9. 在 StoreFront 服务器上配置主机基本 URL，以匹配已经选择的共享 FQDN。

   > 注意：
   >
   > StoreFront 始终自动选择证书内 SAN 列表中的最后一个使用者可选名称。这只是对 StoreFront 管理员有所帮助的建议主机基本 URL，通常都是正确的。如果它作为 SAN 存在于证书内，则可手动将其设置为任何有效的 `HTTPS://<FQDN>`。示例：`https://storefront.example.com`。

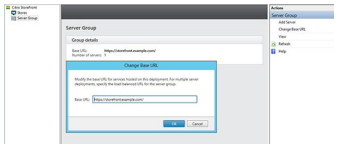
将服务器基本 **URL** 从 **HTTP** 更改为 **HTTPS**

在 Citrix StoreFront 上配置单服务器部署或服务器组部署时，主机基本 URL 选项可用。此选项适用于在没有服务器证书的情况下已安装和配置 Citrix StoreFront 的客户。安装该证书后，请确保 StoreFront 及其服务使用安全连接继续操作。

> 注意：
>
> IT 管理员必须先在 Citrix StoreFront 服务器上生成服务器证书并进行安装，然后再运行此过程。此外，还需要通过 HTTPS (443) 创建 IIS 绑定以确保任何新连接的安全。

完成以下步骤以在 StoreFront 3.x 上更改基本 URL：

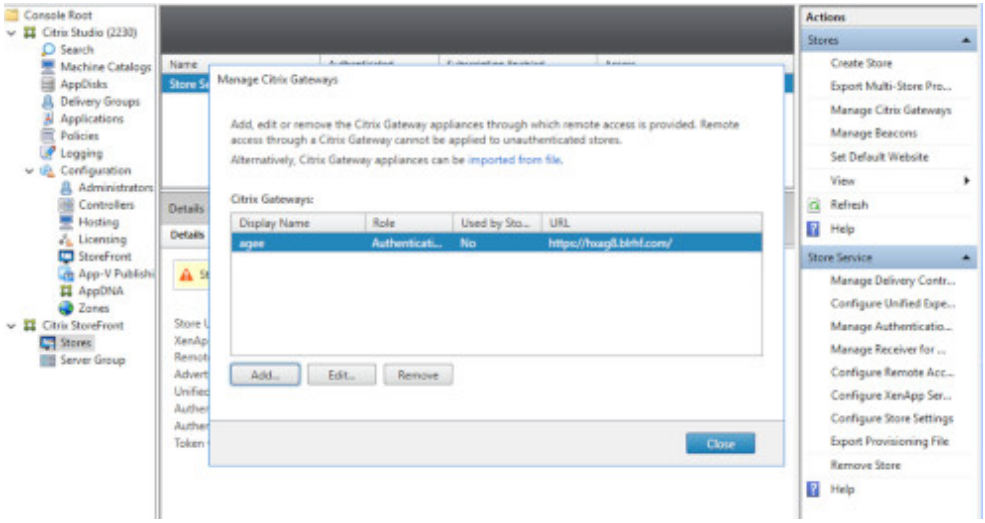
1. 在 StoreFront 中，单击左侧面板中的服务器组。
2. 在右侧面板中单击更改基本 **URL** 。
3. 键入基本 URL 并单击确定。



在 **StoreFront** 服务器上配置网关：**storefront.example.com**

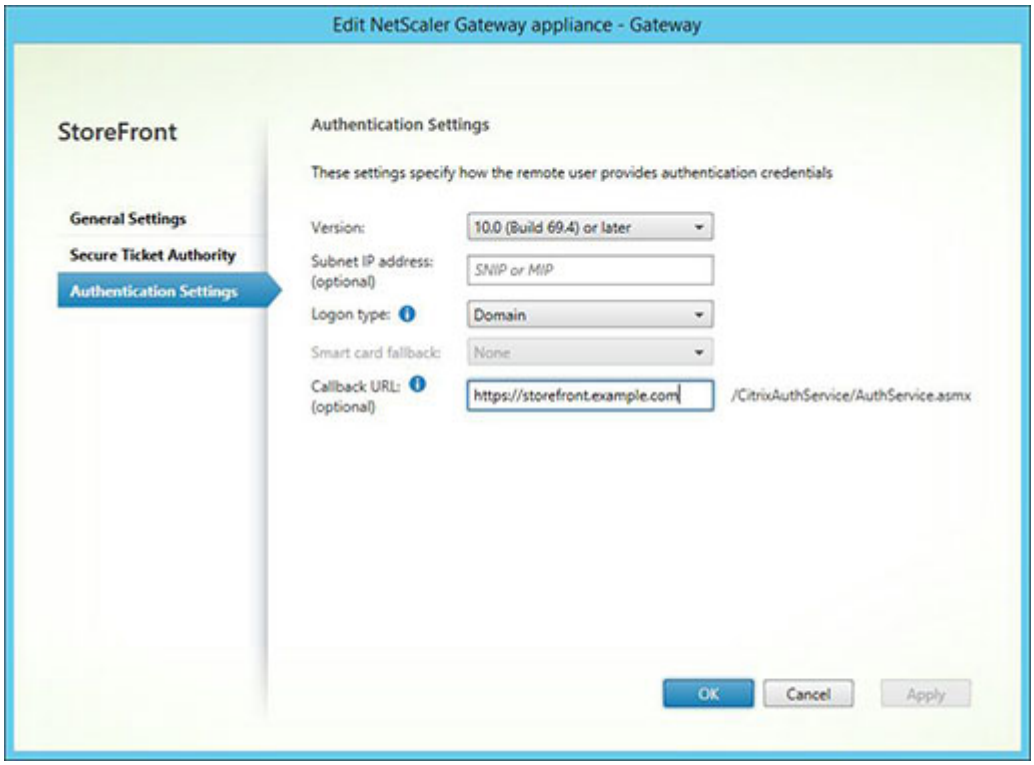
1. 在应用商店节点中，单击操作窗格中的管理 **Citrix Gateway**。

2. 从列表中选择网关，然后单击编辑。



3. 在常规设置页面上的 **Citrix Gateway URL** 字段中键入共享 FQDN。

4. 选择身份验证设置选项卡，然后在回调 **URL** 字段中键入回调 FQDN。

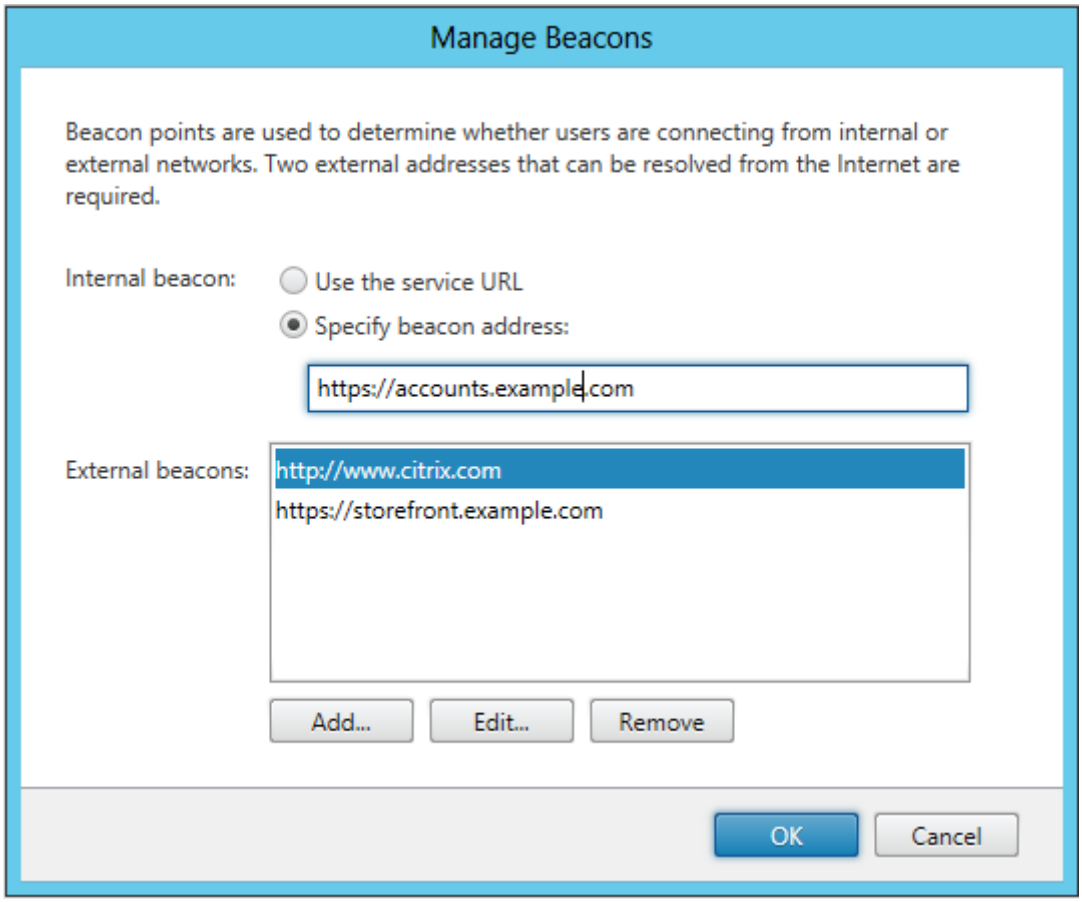


5. 选择 **Secure Ticket Authority** 选项卡，确保 Secure Ticket Authority (STA) 服务器与已在应用商店节点中配置的 Delivery Controller 列表匹配。

6. 为应用商店启用远程访问。

7. 手动将内部信标设置为帐户别名 (accounts.example.com)，不得从网关外部对其进行解析。此 FQDN 必须有别于 StoreFront 主机基本 URL 和 Citrix Gateway 虚拟服务器共享的外部信标 (storefront.example.com)。

请勿使用共享 FQDN，因为这会导致内部和外部信标相同。



支持使用多个不同的 **FQDN** 进行发现

要允许 Citrix Workspace 应用程序使用多个 FQDN 发现应用商店，请执行以下步骤。如果预配文件配置足够，或者仅使用 Receiver for Web，则可跳过以下步骤。

将附加 <allowedAudiences> 条目添加到 *C:\inetpub\wwwroot\Citrix\Authentication\web.config* 中。此文件中有两个 <allowedAudiences> 条目。仅身份验证令牌生成器文件中的第一个条目需要添加附加 <allowedAudience> 条目。

1. 在 <service id> 部分中，找到 <allowedAudiences> 字符串。为 audience="https://accounts.example.com/" 添加一行，如下所示。保存，然后关闭 web.config 文件。

```
1 <service id="abd6f54b-7d1c-4a1b-a8d7-14804e6c8c64" displayName="
     Authentication Token Producer">
2 ...
3 <allowedAudiences>
4 <add name="https-storefront.example.com" audience="https://
     storefront.example.com/" />
```

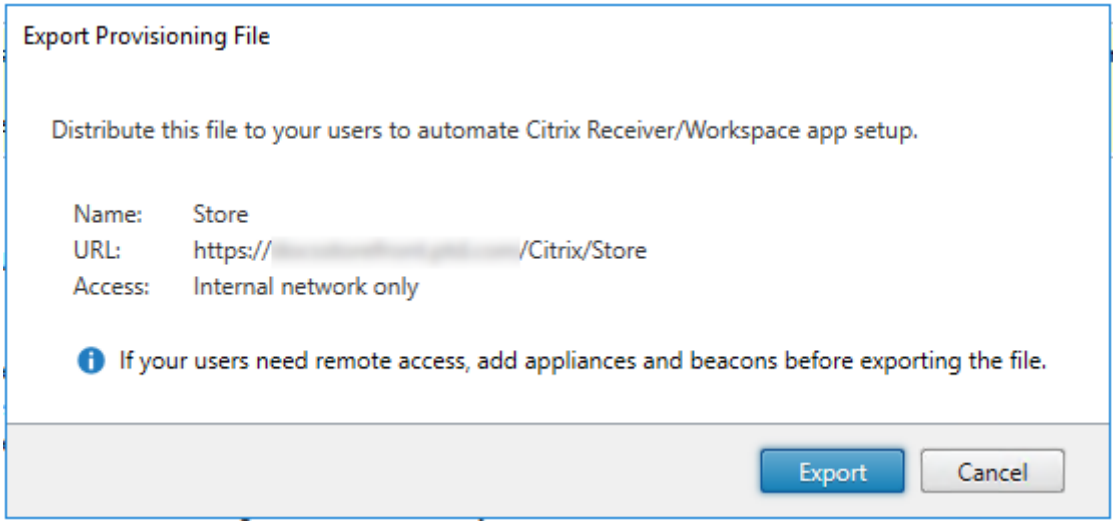


```
<add name="https-accounts.example.com" audience="https://accounts.
    example.com/" />
</allowedAudiences>
```

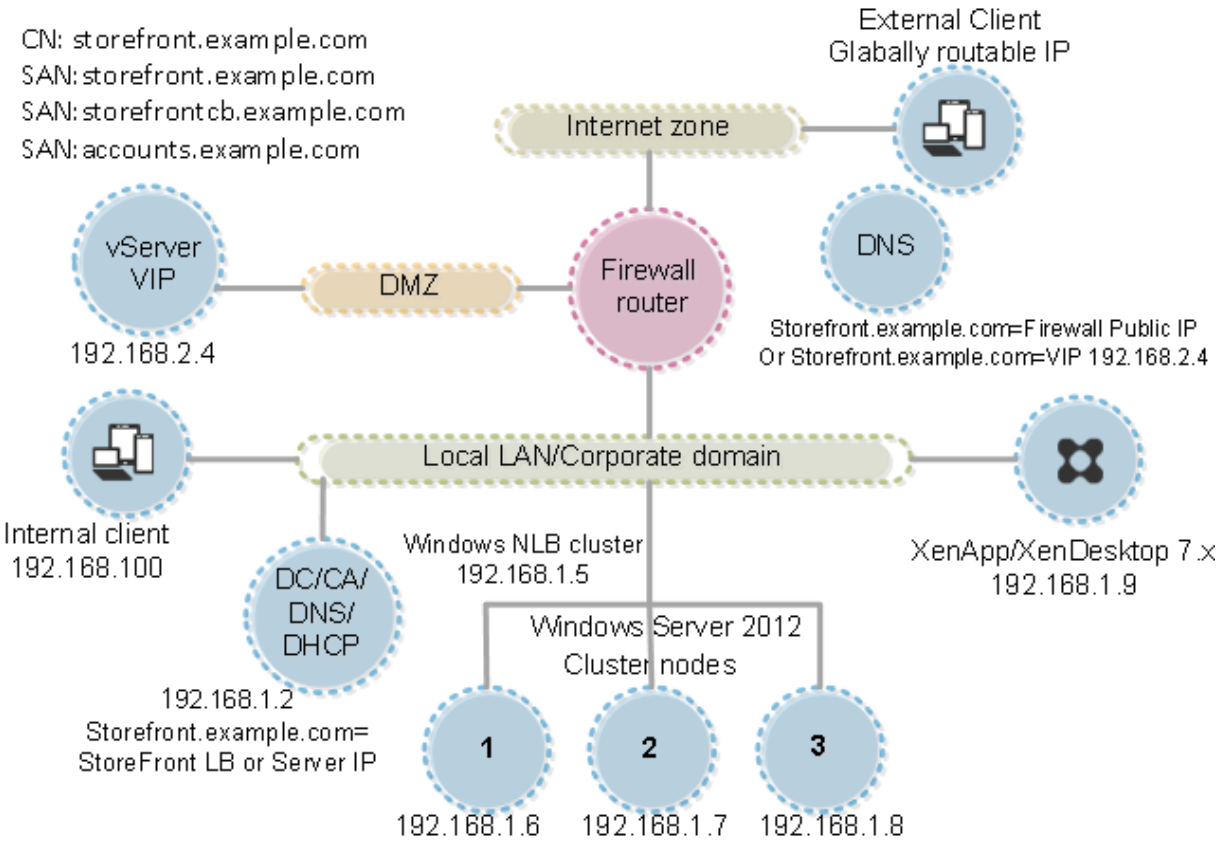
2. 在 *C:\inetpub\wwwroot\Citrix\Roaming\web.config* 中，找到 <tokenManager> 部分并为 `audience ="https://accounts.example.com/"` 添加一行，如下所示。保存，然后关闭 web.config 文件。

```
<tokenManager>
<services>
<clear />
...
</trustedIssuers>
<allowedAudiences>
<add name="https-storefront.example.com" audience="https://
    storefront.example.com/" />
<add name="https-accounts.example.com" audience="https://accounts.
    example.com/" />
</allowedAudiences>
</service>
</services>
</tokenManager>
```

或者，可以导出应用商店的本机 Receiver .CR 预配文件。这样，您在首次使用 Citrix Workspace 应用程序时便不必进行配置。请将此文件分发给所有 Windows 和 MAC Citrix Workspace 应用程序客户端。



如果客户端上已安装 Citrix Workspace 应用程序，则会识别.CR 文件类型，双击预配文件将开始导入。



高级配置

June 5, 2020

可以使用 StoreFront 控制台、PowerShell、证书属性或配置文件配置下面的高级选项。

任务	详细信息
配置资源筛选	根据资源类型和关键字筛选枚举资源。

配置资源筛选

June 29, 2021

本主题说明了如何根据资源类型和关键字过滤枚举资源。可以将此类型的过滤与 Store Customization SDK 提供的更加高级的自定义结合使用。借助此 SDK，您可以控制向用户显示的应用程序和桌面、修改访问条件以及调整启动参数。有关详细信息，请参阅 Citrix StoreFront SDK PowerShell 模块。

> 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。

配置过滤

使用在 StoresModule 中定义的 PowerShell cmdlet 配置过滤器。使用以下 PowerShell 代码段可加载所需的模块：

```
$dsInstallProp = Get-ItemProperty `
 -Path HKLM:\SOFTWARE\Citrix\DeliveryServicesManagement -Name
    InstallDir
$dsInstallDir = $dsInstallProp.InstallDir
& $dsInstallDir..\Scripts\ImportModules.ps1
```

按类型过滤

使用此过滤器可按资源类型过滤资源枚举。此过滤器属于内含过滤器，表示将从资源枚举结果中删除不属于指定类型的任何资源。使用以下 cmdlet：

Set-DSResourceFilterType：根据资源类型设置枚举过滤。

Get-DSResourceFilterType：获取允许 StoreFront 在枚举中返回的资源类型列表。

注意：请先应用资源类型，然后再应用关键字。

按关键字过滤

使用此过滤器可根据关键字过滤资源，例如从 Citrix Virtual Apps and Desktops 派生的资源。关键字是根据相应资源的说明字段中的标记生成的。

此过滤器可以在内含或独占模式下运行，但不能同时在这两种模式下运行。内含过滤器允许资源的枚举与所配置的关键字匹配，并从枚举中删除不匹配的资源。独占过滤器从枚举中删除与所配置的关键字匹配的资源。使用以下 cmdlet：

Set-DSResourceFilterKeyword：根据资源关键字设置枚举过滤。

Get-DSResourceFilterKeyword：获取过滤器关键字的列表。

以下关键字属于保留关键字，不能用于过滤：

- 自动
- 强制

有关关键字的详细信息，请参阅优化用户体验和配置应用程序交付。

示例

以下命令将过滤设置为从枚举中排除工作流资源：

```
Set-DSResourceFilterKeyword -SiteId 1 -VirtualPath "/Citrix/Store" -
    ExcludeKeywords @("WFS")
```

以下示例将允许的资源类型设置为仅限应用程序：

```
Set-DSResourceFilterType -SiteId 1 -VirtualPath "/Citrix/Store" -
    IncludeTypes @("Applications")
```

使用配置文件进行配置

June 5, 2020

可以使用配置文件为无法通过 Citrix StoreFront 管理控制台设置的 Citrix StoreFront 和 Citrix Receiver for Web 配置其他设置。

可以配置的 Citrix StoreFront 设置包括：

- 启用 ICA 文件签名服务
- 禁用文件类型关联
- 自定义 Citrix Workspace 应用程序登录对话框
- 阻止适用于 Windows 的 Citrix Workspace 应用程序缓存密码和用户名

可以配置的 Citrix Receiver for Web 设置包括：

- 资源对用户的显示方式
- 禁用“我的应用程序文件夹视图”

使用配置文件配置 **StoreFront**

June 29, 2021

本文介绍了不能使用 Citrix StoreFront 管理控制台执行的其他配置任务。

> 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，
> 将配置更改传播到服务器组，以便更新部署中的其他服务器。

启用 **ICA** 文件签名服务

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 Receiver，由 Citrix Receiver 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 Citrix Workspace 应用程序中启用 ICA 文件签名的详细信息，请参阅 ICA 文件签名可阻止启动来自不可信服务器的应用程序或桌面。

> 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。

   通过启动 MMC.exe 控制台、添加证书管理单元\ 本地计算机、展开证书存储节点、找到“Citrix 交付服务”，然后导入证书来执行此操作。

2. 使用文本编辑器打开应用商店的 web.config 文件，该文件通常位于 C:\inetpub\wwwroot\Citrix\storename\ 目录中，其中 storename 为创建应用商店时为其指定的名称。

3. 在此文件中查找以下部分。

```
1 <certificateManager>
2     <certificates>
```



```
        <clear />
        <add ... />
        ...
    </certificates>
</certificateManager>
```

4. 包含要用于签名的证书的详细信息。

```
<certificateManager>
    <certificates>
        <clear />
        <add id="certificateid" thumb="certificatethumbprint" />
        <add ... />
    ...
    </certificates>
</certificateManager>
```

其中，**certificateid** 是帮助您在存储配置文件中识别证书的值，**certificatethumbprint** 是哈希算法生成的证书数据的摘要（或指纹）。**certificateID** 可以是您选择的任何数字，前提是未将其用于任何其他证书。

5. 在此文件中查找以下元素。

```
<icaFileSigning enabled="False" certificateId="" hashAlgorithm="
    sha1" />
```

6. 将 enabled 属性的值更改为 True 可为应用商店启用 ICA 文件签名服务。将 **certificateId** 属性的值设置为用来标识证书的 ID，即步骤 4 中的 **certificateid**。
7. 如果要使用除 SHA-1 之外的其他哈希算法，请根据需要将 hashAgorithm 属性的值设置为 sha256、sha384 或 sha512。
8. 使用具有本地管理员权限的帐户启动 Windows PowerShell，并在命令提示窗口中键入以下命令，以允许应用商店访问私钥。

```
Add-PSSnapin Citrix.DeliveryServices.Framework.Commands
$certificate = Get-DSCertificate "Certificate_thumbprint_ID"
Add-DSCertificateKeyReadAccess -certificate $certificate[0] -
    accountName "IIS APPPOOL\Citrix Delivery Services Resources"
```

其中，`Certificate_thumbprint_ID` 是通过哈希算法生成的证书数据的摘要（或指纹）。

> 注意：
>
> 如果 `$certificate` 值为空，请改用以下命令：
>
> ‘‘‘
>
> Add-PSSnapin Citrix.DeliveryServices.Framework.Commands
> $certificate = Get-Item ‘Cert:\LocalMachine\Citrix Delivery Services\Certificate_thumbprint_ID’
> Add-DSCertificateKeyReadAccess -certificate $certificate[0] -accountName “IIS APP-POOL\Citrix Delivery Services Resources”

禁用文件类型关联

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。要禁用文件类型关联，请编辑应用商店配置文件。

1. 使用文本编辑器打开应用商店的 web.config 文件，该文件通常位于 C:\inetpub\wwwroot\Citrix\storename\ 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。

```
<farmset ... enableFileTypeAssociation=”on” ... >
```

3. 将 enableFileTypeAssociation 属性的值更改为 off，为应用商店禁用文件类型关联。

配置资源对用户的显示方式

如果桌面和应用程序在某个应用商店中均可用，则将默认显示单独的桌面视图和应用程序视图。用户在访问应用商店时将先看到桌面视图。如果只有一个桌面可供用户使用，则无论应用程序是否在应用商店中也可用，该桌面都会在用户登录应用商店时自动启动。要更改这些设置，请编辑 StoreWeb 的配置文件。

1. 使用文本编辑器打开 Citrix Receiver for Web 站点的 `web.config` 文件，此文件通常位于 `C:\inetpub\wwwroot\Citrix\<storename>Web\` 目录中，其中 storename 是创建应用应用商店时为其指定的名称。
2. 在此文件中查找以下元素。

```
<uiViews showDesktopsView=”true” showAppsView=”true” defaultView=”desktops” />
```

3. 将 **showDesktopsView** 和 **showAppsView** 属性的值更改为 false，以分别阻止向用户显示桌面和应用程序（即使它们在应用商店中可用也是此）。如果同时启用了桌面视图和应用程序视图，请将 defaultView 属性的值设置为 apps，以便在用户访问应用商店时先显示应用程序视图。

4. 在此文件中查找以下元素。

```
<userInterface ... autoLaunchDesktop="true">
```

5. 将 **autoLaunchDesktop** 属性的值更改为 **false**，以便在用户访问应用商店且只有一个桌面可供该用户使用时，阻止 StoreFront 自动启动该桌面。

   如果 **autoLaunchDesktop** 属性设置为 **true**，并且只能使用一个桌面的用户访问应用商店时，则无论工作区控制配置如何，该用户的应用程序都不会重新连接。

自定义 **Citrix Workspace** 应用程序登录对话框

用户登录应用商店时，默认情况下，登录对话框中将不显示标题文本。可以显示默认文本“请登录”或编写自己的自定义消息。要显示和自定义登录对话框中的标题文本，请编辑身份验证服务的文件。

1. 使用文本编辑器打开用于身份验证服务的 UsernamePassword.tfrm 文件，该文件通常位于 C:\inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\ 目录中。
2. 在此文件中查找以下行。

```
@* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
```

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")
```

   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\Authentication\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>
```

   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。要阻止 Citrix Receiver for Windows 或适用于 Windows 的 Citrix Workspace 应用程序（但 Citrix Receiver for Windows Enterprise 除外）缓存用户的密码，请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\Authentication\App_Data\Templates\UsernamePassword.tfr
2. 在此文件中查找以下行。

```
@SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey:
    "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked:
    ControlValue("SaveCredentials"))
```

3. 按如下所示，注释掉语句。

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

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。此设置不适用于 Citrix Receiver for Windows Enterprise。

> 警告：
>
> 注册表编辑器使用不当可能导致严重问题，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。请确保在编辑注册表之前进行备份。

默认情况下，Citrix Receiver for Windows 自动填充上次输入的用户名。要禁止填充用户名字段，请编辑用户设备上的注册表：

1. 创建 REG_SZ 值 HKLM\SOFTWARE\Citrix\AuthManager\RememberUsername。
2. 将其值设置为 “false”。

使用配置文件配置 **Citrix Receiver for Web** 站点

June 5, 2020

本主题介绍无法通过 Citrix StoreFront 管理控制台执行的其他 Citrix Receiver for Web 站点配置任务。

> 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，
> 将配置更改传播到服务器组，以便更新部署中的其他服务器。

配置资源对用户的显示方式

如果某个 Citrix Receiver for Web 站点同时提供桌面和应用程序，则默认情况下将分别显示桌面视图和应用程序视图。用户登录该站点后，将首先看到桌面视图。如果只有一个桌面可供用户使用，则无论站点是否还提供应用程序，该桌面都会在用户登录站点时自动启动。要更改这些设置，请编辑站点配置文件。

1. 使用文本编辑器打开 Citrix Receiver for Web 站点的 web.config 文件，此文件通常位于 C:\inetpub\wwwroot\Citrix\storenameWeb\ 目录中，其中 storename 是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。

```
1 <uiViews showDesktopsView="true" showAppsView="true" defaultView="
    desktops" />
```

3. 将 **showDesktopsView** 和 **showAppsView** 属性的值更改为 false，以分别阻止向用户显示桌面和应用程序（即使站点提供这些桌面和应用程序也是如此）。如果同时启用了桌面视图和应用程序视图，请将 defaultView 属性的值设置为 apps，以便在用户登录站点时首先显示应用程序视图。
4. 在此文件中查找以下元素。

```
1 <userInterface ... autoLaunchDesktop="true">
```

5. 将 **autoLaunchDesktop** 属性的值更改为 **false**，以便在用户登录站点并且只有一个桌面可供该用户使用时，阻止 Citrix Receiver for Web 站点自动启动该桌面。

   如果 **autoLaunchDesktop** 属性设置为 **true**，则当只有一个桌面可用的用户登录时，用户的应用程序不会重新连接，而无论工作区控制配置如何设置。

> 注意：
>
> 要使 Citrix Receiver for Web 站点能够自动启动桌面，通过 Internet Explorer 访问该站点的用户必须将该站点添加到“本地 Intranet”或“可信站点”区域中。

禁用“我的应用程序文件夹视图”

1. 使用文本编辑器打开 Citrix Receiver for Web 站点的 web.config 文件，此文件通常位于 C:\inetpub\wwwroot\Citrix\storenameWeb\ 目录中，其中 storename 是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。

```
<userInterface enableAppsFolderView=”true”>
```

3. 将 **enableAppsFolderView** 属性的值更改为 **false**，以禁用 Citrix Receiver for Web 的“我的应用程序文件夹视图”。

保护 **StoreFront** 部署的安全

June 29, 2021

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。

配置 **Microsoft Internet Information Services (IIS)**

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

可以不允许使用未列出的文件扩展名。

StoreFront 要求在请求筛选中使用以下文件扩展名：

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

- .xml

如果为 Citrix Receiver for Web 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

MIME 类型

可以删除与以下文件类型对应的 MIME 类型：

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

请求筛选

StoreFront 要求在请求筛选中使用以下 HTTP 谓词。可以不允许使用未列出的谓词。

- GET
- POST
- HEAD

其他 **Microsoft IIS** 设置

StoreFront 不需要以下各项：

- CGI 程序
- FastCGI 程序

> 重要：
>
> - 请勿配置 IIS 授权规则。StoreFront 直接支持身份验证，并且不使用或不支持 IIS 身份验证。
> - 请勿在 StoreFront 站点的“SSL Settings”（SSL 设置）中选择 **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。必须选择“使用 cookie”设置。请勿选择“无 cookie/使用 URI”设置。
> - StoreFront 要求完全信任。请勿将全局.NET 信任级别设置为“高”或更低。

> - StoreFront 不支持为每个站点使用独立的应用程序池。请勿修改这些站点设置。但是，可以设置应用程序池空闲超时以及应用程序池使用的虚拟内存量。

配置用户权限

> 注意：
>
> 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，将向其应用程序池授予登录权限作为服务登录以及权限为进程调整内存配额、生成安全审核和替换一个进程级令牌。这是创建应用程序池时的常规安装行为。应用程序池为 Citrix 配置 Api、Citrix Delivery Services 资源、Citrix Delivery Services 身份验证和 Citrix Receiver for Web。

您不需要更改这些用户权限。这些权限不会被 StoreFront 使用，并且自动禁用。

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)

如果为 XenApp 6.5 配置了 StoreFront Kerberos 约束委派，这将创建 Citrix StoreFront 协议转换服务 (NT SERVICE\SYSTEM)。此服务需要一项的权限通常不会被授予 Windows 服务。

配置服务设置

在上文“配置用户权限”部分中列出的 StoreFront Windows 服务配置为以 NETWORK SERVICE 身份登录；请勿更改此配置。Citrix StoreFront 协议转换服务以 SYSTEM 身份登录；请勿更改此配置。

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。

请勿使用权限较少的域帐户替换这些虚拟帐户。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
- CitrixPNRSUsers
- CitrixStoreFrontPTServiceUsers
- CitrixSubscriptionServerUsers
- CitrixSubscriptionsStoreServiceUsers
- CitrixSubscriptionsSyncUsers
- CitrixStoreFrontAdministrators（从 StoreFront 1912 LTSR CU1 起）

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 文件签名服务，StoreFront 还可以使用证书对 ICA 文件进行数字签名。

要为第一次在设备上安装 Citrix Workspace 应用程序的用户启用基于电子邮件的帐户发现，您必须在 StoreFront 服务器上安装有效的服务器证书。指向根证书的完整链也必须有效。为获得最佳用户体验，请安装具有 **discoverReceiver.domain** 的“使用者”或“使用者备用名称”条目的证书，其中 domain 为包含您的用户的电子邮件帐户的 Microsoft Active Directory 域。虽然您可以为包含用户的电子邮件帐户的域使用通配符证书，但是必须首先确保贵公司的安全策略允许部署此类证书。也可以使用用户电子邮件帐户所属域的其他证书，但是当 Citrix Workspace 应用程序第一次连接到 StoreFront 服务器时，用户将看到一个证书警告对话框。基于电子邮件的帐户发现不能与任何其他证书身份验证一起使用。有关详细信息，请参阅配置基于电子邮件的帐户发现。

如果您的用户通过将应用商店 URL 直接输入 Citrix Workspace 应用程序来配置其帐户，并且不使用基于电子邮件的帐户发现，那么 StoreFront 服务器上的证书只需对于该服务器有效，并且具有指向根证书的有效链。

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` 中的文件夹中安装了各种 PowerShell 脚本 (.ps1)。默认 StoreFront 安装不使用这些脚本，但是您可以用来简化特定和罕见的配置任务。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，因为它会阻止 PowerShell 脚本运行。）StoreFront 不会更改 PowerShell 执行策略。

向“可信发布者”存储中添加代码签名证书，因为 StoreFront 不会自动添加。如果未添加证书，则在启用打开脚本执行策略设置并设置仅允许签名脚本时，StoreFront 管理控制台管理单元不会加载。

如果在 PowerShell 会话中运行脚本，则当 PowerShell 脚本在设置了 **AllSigned** 执行策略中的始终运行选项的情况下运行时，Windows 会自动在“可信发布者”存储中添加代码签名证书。(如果选择永不运行选项，证书将添加到“不受信任的证书”存储中，并且 StoreFront PowerShell 脚本不会运行。)

一旦将代码签名证书添加到“可信发布者”存储中，Windows 将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。

StoreFront 通信

在生产环境中，Citrix 建议使用 Internet 协议安全性 (IPsec) 或 HTTPS 协议来确保在 StoreFront 与您服务器之间传输的数据的安全。IPsec 是 Internet 协议的一组标准扩展，可提供经过身份验证和加密的通信，并且可以实现数据完整性和重播保护功能。由于 IPsec 是一个网络层协议集，因此无需任何修改即可将其用于更高级别的协议。HTTPS 使用安全套接字层 (SSL) 和传输层安全性 (TLS) 协议来提供强大的数据加密。

可使用 SSL Relay 来确保 StoreFront 和 Citrix Virtual Apps 服务器之间数据通信的安全。SSL Relay 是执行主机身份验证和数据加密的默认 Citrix Virtual Apps 组件。

Citrix 建议您在托管 StoreFront 的 Web 服务器中禁用 TLS 1.0 和 1.1 支持。您应该通过组策略对象执行此操作，这些对象会在 StoreFront 服务器上创建必需的注册表设置以禁用 TLS 1.0 和 TLS 1.1 等旧协议。另请参阅 Microsoft TLS/SSL 设置 参考主题。

Citrix 建议使用 Citrix Gateway 和 HTTPS 来确保 StoreFront 与用户设备之间的通信安全。要使用 HTTPS，StoreFront 要求将托管身份验证服务和相关联的应用商店的 Microsoft Internet Information Services (IIS) 实例

配置为支持 HTTPS。如果没有合适的 IIS 配置，StoreFront 将使用 HTTP 进行通信。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。

Storefront 不支持 ECDSA（椭圆曲线 DSA）证书。

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 文件签名服务

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 文件签名服务。

用户更改密码

可以允许使用 Active Directory 域凭据登录的 Receiver for Web 站点用户随时或仅当到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 Receiver for Web 站点用户更改自己的密码，即使密码已到期也是如此。有关详细信息，请参阅优化用户体验。

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

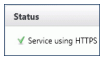
要使用 HTTPS 来确保 StoreFront 与用户设备之间通信的安全，必须先将 Microsoft Internet Information Services (IIS) 配置为支持 HTTPS。如果在未首先安装和配置 SSL 证书的情况下安装和配置 Citrix StoreFront，StoreFront 将使用 HTTP 进行通信。

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。

示例：

将基本 **URL** 更改为 **HTTPS** 之前：

将基本 **URL** 更改为 **HTTPS** 之后：



1. 在 StoreFront 服务器上将 Microsoft Internet Information Services (IIS) 配置为 HTTPS

a) 使用 Internet Information Services (IIS) 管理器控制台，导入由 Microsoft Active Directory 域证书颁发机构签名的 SSL 服务器证书。
b) 通过 HTTPS (443) 向默认 Web 站点添加 IIS 绑定。

有关详细说明，请参阅 CTX200292。

2. 在 Citrix StoreFront 管理控制台中，在左侧窗格中选择服务器组。
3. 在“操作”窗格中，选择更改基本 **URL**。
4. 键入基本 URL 并单击确定。

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 Citrix Receiver for 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。

其他安全信息

> 注意：
>
> 此信息可能会随时更改，恕不另行通知。

安全扫描

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。

解释安全扫描报告时，请注意以下事项：

- StoreFront 中的 HTML 页面可能不包括点击劫持保护（通过内容安全策略或 X-Frame-Options 响应头）。但是，这些 HTML 页面仅包含静态内容，因此点击劫持攻击不相关。
- Microsoft IIS 的版本和 ASP.NET 的使用在 HTTP 标头中可见。但是，此信息在 StoreFront 本身的存在中显而易见，因为它依赖于这些技术。
- 启动应用程序和桌面时，StoreFront 使用令牌来防止跨站点请求伪造 (CSRF)。此令牌在响应中作为 cookie 发送，而不被标记为 “Secure” 或 “HttpOnly”。稍后在请求中发送时，令牌将包含在 URL 的查询字符串中。但是，StoreFront 不依赖于此机制来验证 HTTP 请求。
- StoreFront 使用开源组件 jQuery。使用的一个版本是 jQuery 1.3.2。根据 jQuery 开源项目，在 jQuery 1.12.0 中进行了更改，以减轻特定形式的跨域请求的潜在漏洞。这种更改不是对 jQuery 本身漏洞的缓解；它是对应用程序逻辑潜在误用的缓解。NetScaler 和 StoreFront 共享的 Receiver for Web 功能中的相关 Citrix 应用程序逻辑不使用这种特定形式的跨域请求，不受此漏洞的影响，并且未从此缓解中受益。

出于兼容性原因，此缓解后来在 jQuery 1.12.3 中已删除。由于 Citrix 应用程序逻辑没有从此缓解中受益，因此，此删除在使用 jQuery 1.12.4 的 NetScaler 和 StoreFront 各版本中不会产生重大影响。

CSRF 令牌使用情况

客户端向 StoreFront 服务器发出的某些 GET 请求包括放置在 URL 查询参数中的 CSRF 令牌。已审查有关此问题的客户报告以了解安全影响。尽管这种行为不是可直接利用的安全问题，但它不被视为最佳做法。这是因为它允许将令牌保留在（例如）浏览器历史记录中或代理服务器等中间设备的日志中。

作为深入防御的措施，您可以在 StoreFront 服务器上使用以下 PowerShell 脚本禁用针对特定的已识别的 GET 请求端点的 CSRF 令牌使用情况：

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

如果执行此操作，还必须从所使用的任何基于 WebAPI 的自定义项中的 URL 中删除 CSRF 令牌。

导出和导入 **StoreFront** 配置

July 5, 2021

> 注意：
>
> 只能导入与目标 StoreFront 安装相同的 StoreFront 版本的 StoreFront 配置。这包括 CU 版本。例如，您可以在 StoreFront 版本 1912 LTSR 与 1912 LTSR 之间的导出和导入配置，或者在版本 1912 LTSR CU1 与 1912 LTSR CU1 之间导出和导入配置，但不能在版本 1912 LTSR CU1 与 1912 LTSR CU2 之间导出和导入配置。

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（例如将托管操作系统从 2008R2 升级到 2019）期间移动 StoreFront。

- 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

安装和配置各种 StoreFront 组件时自动安装的 Citrix StoreFront SDK 中提供了以下 cmdlet。有关详细信息，请参阅 StoreFront SDK一文。

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：
>
> 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)	备份存档的导出路径。示例：`$env:userprofile\desktop\`
-Credential（PSCredential 对象）	使用此参数将创建加密备份存档的未加密副本。指定包含解密密码的 PowerShell 凭据对象。示例：`$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：`$env:userprofile\\desktop\\backup.ctxzip`
-OutputFolder (字符串)	创建加密备份存档 (.ctxzip) 的取消加密副本 (.zip) 的路径。最初的加密备份副本将保留，以便重复使用。请勿指定取消加密副本的文件名和文件扩展名。示例：`$env:userprofile\desktop\`
-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。

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
```

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
```

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"
```

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
```

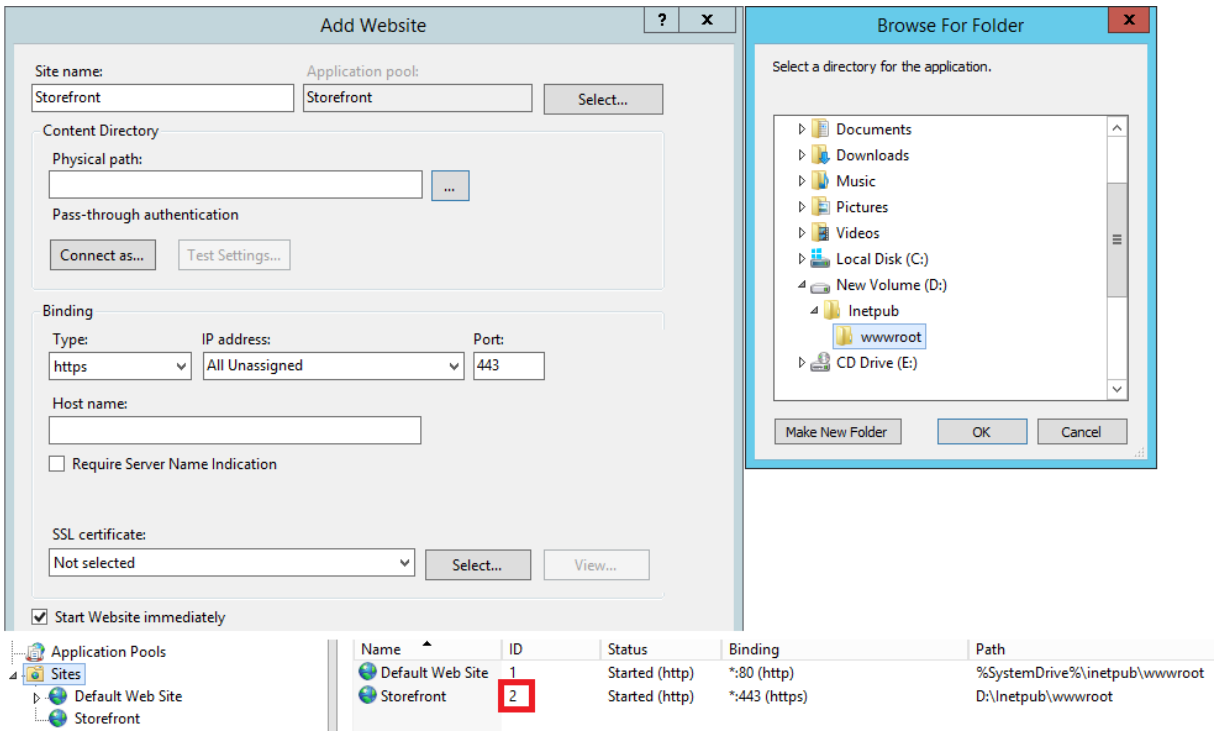
将 backup.zip 文件复制到服务器 B 的桌面。

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://serverB.example.com"
```

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。

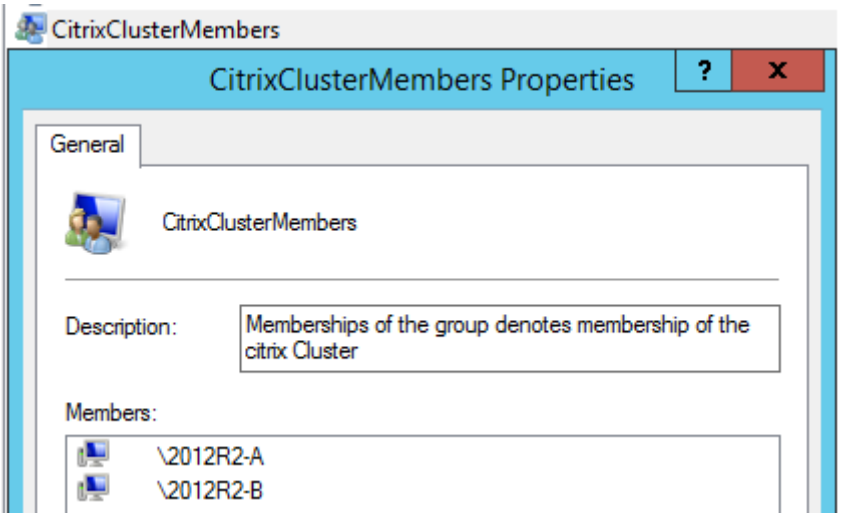

```
Import-STFConfiguration -configurationZip ”$env:userprofile\desktop\
backup.ctxzip”-HostBaseURL ”https://serverB.example.com”
```

服务器组场景

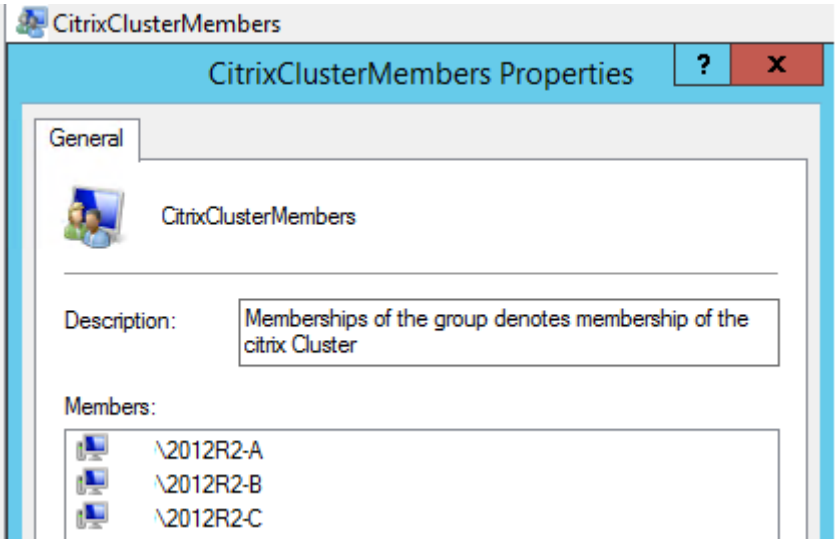
场景 **1**：备份现有服务器组配置，然后将其还原到相同的服务器组部署中

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。



1. 然后将另一台服务器 2012R2-C 添加到现有服务器组中。



1. 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。
2. 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"
   ```

3. 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"
   ```

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
"
```

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)
```

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
```

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"
```


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
```

StoreFront SDK

June 5, 2020

Citrix StoreFront 提供基于多个 Microsoft Windows PowerShell 3.0 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。

有关 SDK 参考，请参阅 StoreFront SDK。

StoreFront 3.0 与最新的 StoreFront SDK 之间的主要区别

- 高级别 **SDK** 示例 - 此版本提供高级别 SDK 脚本，使您能够轻松快速地编写脚本和自动执行 StoreFront 部署。可以定制高级别示例以满足您的特定要求，这样您能够通过运行一个脚本创建新部署。
- 新的低级别 **SDK** - Citrix 提供记录的低级别 StoreFront SDK，实现了部署的配置（包括应用商店、身份验证方法、Citrix Receiver for Web 和统一 Citrix Receiver 站点）以及通过 Citrix Gateway 进行远程访问。
- 向后兼容性 - StoreFront 3.6 仍然包含 StoreFront 3.0 及更早的 API，这样可以逐步将现有脚本转换到新 SDK。

> 重要：
>
> 在可行的情况下，会维护与 StoreFront 3.0 的向后兼容。但是，Citrix 建议您在编写新脚本时，使用新的 **Citrix.StoreFront.*** 模块，因为 StoreFront 3.0 SDK 已弃用，最终将被删除。

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. 在 PowerShell 3.0 中启动 shell。

   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。

示例	说明
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"
    )
```



```
16      # Import StoreFront modules. Required for versions of
            PowerShell earlier than 3.0 that do not support
            autoloading
17      Import-Module Citrix.StoreFront
18      Import-Module Citrix.StoreFront.Stores
19      Import-Module Citrix.StoreFront.Authentication
20      Import-Module Citrix.StoreFront.WebReceiver
```

- 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”。

```
1   # Determine the Authentication and Receiver virtual path to use
        based of the Store
2   $authenticationVirtualPath = ”$($StoreIISPath.TrimEnd('/'))Auth”
3   $receiverVirtualPath = ”$($StoreVirtualPath.TrimEnd('/'))Web”
```

- 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。

```
1   # Determine if the deployment already exists
2   $existingDeployment = Get-STFDeployment
3   if(-not $existingDeployment)
4   {
5
6       # Install the required StoreFront components
7       Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -
            Confirm:$false
8    }
9
10  elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)
11  {
12
13      # The deployment exists but it is configured to the desired
            hostbase url
14      Write-Output ”A deployment has already been created with the
            specified hostbase url on this server and will be used.”
15   }
16
17  else
18  {
19
```

```
20      Write-Error "A deployment has already been created on this
            server with a different host base url."
21   }
```

- 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   }
```

- 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 `
```



```
8           -Port $Port -SSLRelayPort $SSLRelayPort -TransportType
               $TransportType
9    }
10
11  else
12  {
13
14      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."
15      # Get the number of farms configured in the store
16      $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.
           Count
17      # Append the farm to the store with a unique name
18      Add-STFStoreFarm -StoreService $store -FarmName "Controller$(
           $farmCount + 1)" -FarmType $Farmtype -Servers $FarmServers
            -LoadBalance $LoadbalanceServers -Port $Port `
19          -SSLRelayPort $SSLRelayPort -TransportType $TransportType
20   }
```

- 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。

```
1   # Determine if the receiver service at the specified virtual path
        exists
2   $receiver = Get-STFWebReceiverService -VirtualPath
       $receiverVirtualPath
3   if(-not $receiver)
4   {
5
6       # Add a Receiver for Web site so users can access the
           applications and desktops in the published in the Store
7       $receiver = Add-STFWebReceiverService -VirtualPath
           $receiverVirtualPath -StoreService $store
8    }
9
10  else
11  {
12
13      Write-Output "A Web Receiver service already exists at the
           specified virtual path and will be used."
14   }
```

- 为应用商店启用 XenApp 服务，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)
{

# Enable XenApp services on the store and make it the default for
    this server
Enable-STFStorePna -StoreService $store -AllowUserPasswordChange
   -DefaultPnaService
 }
```

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。

```
Param(
    [Parameter(Mandatory=$true)]
    [Uri]$HostbaseUrl,
    [Parameter(Mandatory=$true)]
    [long]$SiteId = 1,
    [string]$Farmtype = ”XenDesktop”,
    [Parameter(Mandatory=$true)]
    [string[]]$FarmServers,
    [string]$StoreVirtualPath = ”/Citrix/Store”,
    [bool]$LoadbalanceServers = $false,
    [int]$Port = 80,
    [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
```

- 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
```

- 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
```



```
$authentication = Get-STFAuthenticationService -StoreService $store
$receiverForWeb = Get-STFWebReceiverService -StoreService $store
```

- 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。

```
# Get the Citrix Receiver for Web CitrixAGBasic and ExplicitForms authentication method from the supported protocols
# Included for demonstration purposes as the protocol name can be used directly if known
$receiverMethods = Get-STFWebReceiverAuthenticationMethodsAvailable | Where-Object { $_ -match "Explicit" -or $_ -match "CitrixAG" }

# Enable CitrixAGBasic in Receiver for Web (required for remote access)
Set-STFWebReceiverService $receiverForWeb -AuthenticationMethods $receiverMethods
```

- 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
```

- 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
```

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,
```



```
8       [string]$StoreVirtualPath = "/Citrix/Store",
9       [bool]$LoadbalanceServers = $false,
10      [int]$Port = 80,
11      [int]$SSLRelayPort = 443,
12      [ValidateSet("HTTP","HTTPS","SSL")]
13      [string]$TransportType = "HTTP",
14      [Parameter(Mandatory=$true)]
15      [Uri]$GatewayUrl,
16      [Parameter(Mandatory=$true)]
17      [Uri]$GatewayCallbackUrl,
18      [Parameter(Mandatory=$true)]
19      [string[]]$GatewaySTAUrls,
20      [string]$GatewaySubnetIP,
21      [Parameter(Mandatory=$true)]
22      [string]$GatewayName,
23      [Parameter(Mandatory=$true)]
24      [Uri]$OptimalGatewayUrl,
25      [Parameter(Mandatory=$true)]
26      [string[]]$OptimalGatewaySTAUrls,
27      [Parameter(Mandatory=$true)]
28      [string]$OptimalGatewayName
29  )
30  Set-StrictMode -Version 2.0
31  # Any failure is a terminating failure.
32  $ErrorActionPreference = 'Stop'
33  $ReportErrorShowStackTrace = $true
34  $ReportErrorShowInnerException = $true
35  # Import StoreFront modules. Required for versions of PowerShell
        earlier than 3.0 that do not support autoloading
36  Import-Module Citrix.StoreFront
37  Import-Module Citrix.StoreFront.Stores
38  Import-Module Citrix.StoreFront.Roaming
```

- 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。

```
1  # Create a remote access deployment
2  $scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
       Definition -Parent
3  $scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.
       ps1"
4  & $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
       FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
       Farmtype $Farmtype `
```



```
    -LoadbalanceServers $LoadbalanceServers -Port $Port  -
        SSLRelayPort $SSLRelayPort -TransportType $TransportType `
    -GatewayUrl $GatewayUrl -GatewayCallbackUrl
        $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -
        GatewayName $GatewayName
```

- 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
```

- 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
```

示例：在身份提供程序与服务提供商 **(StoreFront)** 之间交换元数据以进行 **SAML** 身份验证

可以在 StoreFront 管理控制台中或使用下面的 PowerShell cmdlet 配置 SAML 身份验证（请参阅配置身份验证服务）：

- Export-STFSamlEncryptionCertificate
- Export-STFSamlSigningCertificate
- Import-STFSamlEncryptionCertificate
- Import-STFSamlSigningCertificate
- New-STFSamlEncryptionCertificate
- New-STFSamlIdPCertificate
- New-STFSamlSigningCertificate

可以使用 cmdlet **Update-STFSamlIdPFromMetadata** 在身份提供程序与服务提供商之间交换元数据（标识符、证书、端点或其他配置），在此情况下为 StoreFront。

对于具有专用身份验证服务且名为 “Store” 的 StoreFront 应用商店，元数据端点将为：

```
https://<storefront host>/Citrix/StoreAuth/SamlForms/ServiceProvider/
Metadata
```

如果您的身份提供程序支持元数据导入，那么您可以将其指向上面的 URL。注意：这必须通过 HTTPS 执行。

要让 StoreFront 使用来自身份提供程序的元数据，可以使用以下 PowerShell：

```
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"
```

示例：为 **SAML** 身份验证列出指定应用商店的元数据和 **ACS** 端点

可以使用以下脚本列出指定应用商店的元数据和 ACS (Assertion Consumer Service) 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:
Service Provider ID: $spId
Assertion Consumer Service: $acs
Metadata: $md
Test Page: $samlTest"
```

输出示例：

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

StoreFront 故障排除

December 2, 2020

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。

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。

Citrix StoreFront 管理控制台将自动记录跟踪信息。默认情况下，对其他操作的跟踪功能处于禁用状态，必须手动启用。Windows PowerShell 命令创建的日志存储在 StoreFront 安装的 \Admin\logs\ 目录中，通常位于 C:\Program Files\Citrix\Receiver StoreFront。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。

> 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，
> 将配置更改传播到服务器组，以便更新部署中的其他服务器。

对身份验证失败进行故障排除

StoreFront 使用 LogonUser API (https://docs.microsoft.com/en-us/windows/desktop/api/winbase/nf-winbase-logonusera) 来记录基于密码的身份验证失败，当登录因用户名或密码不正确而失败时，该 API 将返回错误 1326。有关详细信息，请参阅https://docs.microsoft.com/en-us/windows/desktop/debug/system-error-codes--1300-1699-。

您可以监视事件 ID 4625 的安全审核日志，如 https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625 中所述。子状态指示身份验证尝试出现的问题。

配置日志限制

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">
   ```

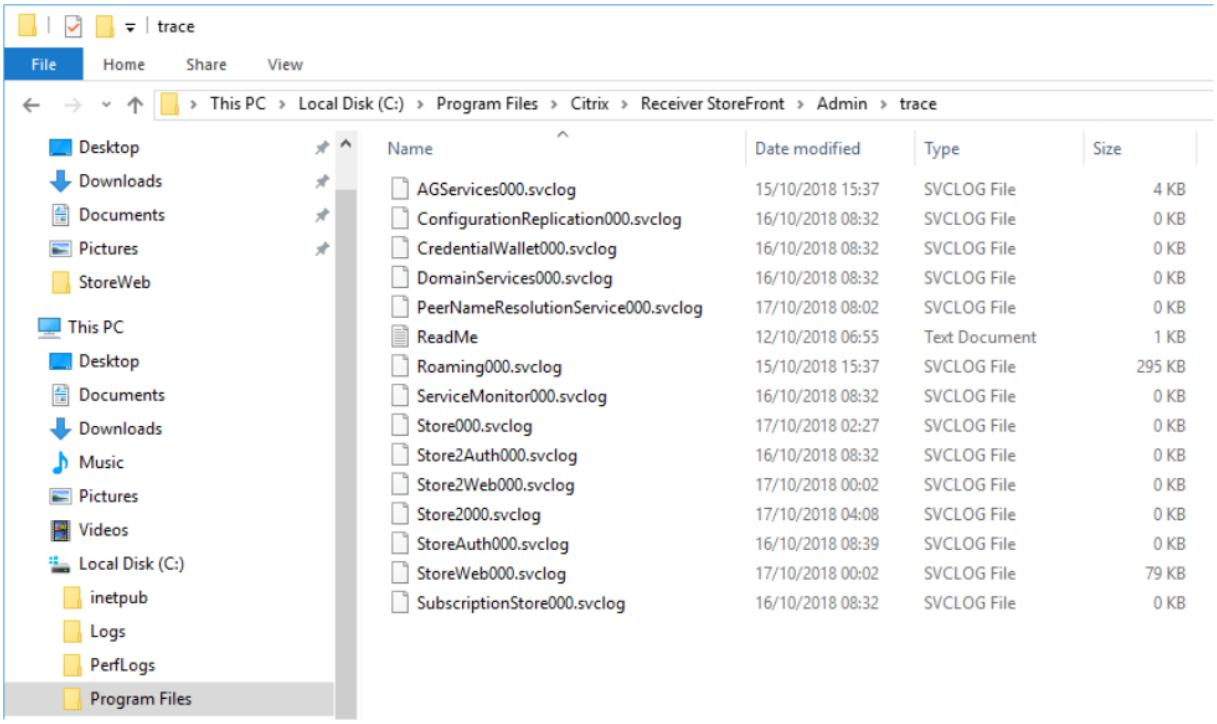
   在 StoreFront 的配置中，重复日志条目数默认限制为每分钟 10 条。
3. 更改 duplicateInterval 属性的值，以小时、分钟和秒为单位设置监视重复日志条目的时间段。使用 duplicateLimit 属性设置必须在指定时间间隔内记录的重复条目数，以便触发日志限制。

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。

对调试启用跟踪

> 重要：
>
> 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 控制台的所有实例。

将跟踪输出发送到 c:\Program Files\Citrix\Receiver StoreFront\admin\trace



> 注意：
>
> 运行 `Get-Help Set-STFDiagnostics -detailed` 以获取 Powershell 帮助以及有关如何使用 Set-STFDiagnostics cmdlet 的说明。

使用具有本地管理员权限的帐户启动 Windows PowerShell，然后在命令提示窗口中指定以下必需参数以启用或禁用跟踪。

- **-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。

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：

```
1 Set-STFDiagnostics -All -TraceLevel ”Verbose” -confirm:$False
```


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
```

有关设置 Set-STFDiagnostics cmdlet 的详细信息，请参阅 StoreFront PowerShell SDK 文档。

启用 **launch.ica** 文件的日志记录

将信息保存在客户端计算机的 launch.ica 文件中，以对多个问题进行故障排除。launch.ica 文件由 Citrix Web Interface 或 Citrix StoreFront 服务器生成。

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
   ```

其他资源

> 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。

对 **StoreFront** 升级问题进行故障排除

使用以下步骤对 StoreFront 升级问题进行故障排除。

尝试升级之前

1. 确认您有所有 StoreFront 服务器的备份。
2. 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。
3. 验证您仅从受支持的 StoreFront 版本升级到当前版本。
4. 如果 StoreFront 服务器是 StoreFront 服务器组的一部分，则必须按顺序升级组中的所有服务器。不支持同时升级 StoreFront 服务器组。
5. 删除 *C:\inetpub\wwwroot\citrix* 或其子目录中的任何 *thumbs.db* 文件。显示隐藏的文件以完成此步骤：文件夹选项 **>** 查看，选择选项显示隐藏的文件、文件夹和驱动器，并清除选项隐藏受保护的操作系统文件 **(**推荐**)**。
6. 在开始执行升级过程之前，请禁用防病毒软件。
7. 确认正在升级的服务器已从任何负载平衡器中删除，并且没有连接的活动用户会话。
8. 请在执行升级之前重新启动 StoreFront 服务器。
9. 手动停止以下服务：
    - CitrixConfigurationReplication
    - CitrixCredentialWallet
    - CitrixDefaultDomainService
    - CitrixPeerResolutionService
    - CitrixSubscriptionsStore
10. 确保 StoreFront 管理控制台已关闭。

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。

4. 检查安装日志文件中是否存在以下错误：

    无法设置进程执行策略：因对 PowerShell 模块进行签名的证书不受信任所致。要查看证书是否不受信任，请提取 CitrixStoreFront-x64.exe，然后对其中一个 PowerShell 文件使用上下文命令属性 **>** 数字签名 **>** 详细信息 **>** 查看证书 **>** 证书路径。

手动删除 **StoreFront**

> 警告：
>
> 手动删除 StoreFront 会清除所有现有信息。

要手动删除 StoreFront，请执行以下操作：

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

您现在可以重新安装 StoreFront。

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States