StoreFront 3.15

Jun 04, 2018

StoreFront 管理从数据中心中的 XenApp、XenDesktop 服务器和 XenMobile 服务器向用户设备交付桌面和应用程序的过程。StoreFront 枚举可用桌面和应用程序，并将其汇总到应用商店中。用户可以直接通过 Citrix Receiver 访问 StoreFront 应用商店，或者通过浏览到 Citrix Receiver for Web 或桌面设备站点进行访问。用户还可以使用瘦客户端和其他兼容的最终用户设备通过 XenApp Services 站点访问 StoreFront。

StoreFront 会保留每个用户的应用程序的记录，并自动更新其设备。用户在其智能手机、平板电脑、便携式计算机和台式机之间漫游时享有一致的体验。StoreFront 是 XenApp 7.x 和 XenDesktop 7.x 的基本组件，但可以与多个版本的 XenApp 和 XenDesktop 结合使用。

从 https://www.citrix.com/downloads/storefront-web-interface/ 下载并安装 StoreFront。

StoreFront 3.15 包括多个已修复和已知的问题。

新增功能

Jun 04, 2018

StoreFront 3.15 包括以下增强功能以及多个已修复和已知的问题：

- **从 NetScaler Gateway 直通 - 对注销行为进行了小幅度的更改**。如果使用“从 NetScaler Gateway 直通”身份验证，则当用户从 Receiver for Web 站点注销时，现在会重定向到 NetScaler 注销页面。以前，用户可能会看到身份验证对话框。NetScaler 注销页面的行为取决于 NetScaler 配置。例如，重定向可能会使用户转到身份提供程序的注销页面，或转到显示简单的“注销成功”消息的页面。

我们对以下文章做了小幅度的更新：

- 系统要求（产品和平台支持变更）

已修复的问题

Jun 04, 2018

以下问题自版本 3.14 起已修复：

- 在启用了“自动启动桌面”设置的情况下，“Multiple launch prevention”（多次启动保护）选项可能不起作用。因此，后续启动相同的桌面实例的请求将失败。[#LC7430]
- 在某些应用程序的“TWIMode”设置为“关”的情况下，使用 Citrix Receiver for Chrome 时所有应用程序都将在窗口模式下启动。[#LC7558]
- 升级非默认驱动器上安装的 StoreFront 2.6 后，可能不会保留用户的应用程序订阅数据。[#LC8046]
- StoreFront 中存在两个或多个应用商店时，单击第一个或第二个应用商店中的“配置远程访问设置”可能会在最新添加的应用商店中重复该名称。[#LC8089]
- 在 StoreFront 中配置进行共享身份验证的应用商店时，尝试将新 NetScaler Gateway 设备链接到某个应用商店会导致删除已链接到该应用商店的现有 NetScaler Gateway 设备。尝试登录应用商店时，将显示以下错误消息：

  您的登录已过期。请重新登录以继续。

  此外，StoreFront 控制台还将显示重复的应用商店名称。[#LC8219]
- 使用“Import-STFConfiguration”PowerShell 命令导入具有 HTML5 配置的应用商店时，导入可能会成功完成。但是，尝试使用 Citrix Receiver for HTML5 启动应用程序将失败。[#LC8290]
- StoreFront 服务器可能会在控制台中显示空的 Receiver for Web 站点条目。在 URL 中应用商店名称的开头为文本“discovery”时会出现此问题。[#LC8320]
- 在启用了 W3C 日志记录服务的情况下，尝试更改 StoreFront 配置可能会失败并显示以下错误消息：

  保存您的更改时出错。[#LC8370]
- 此修复解决了基础组件中的网络套接字问题。[#LC8514]
- 重新启动 StoreFront MMC 控制台后，可能不会正确显示**显示 Desktop Viewer** 复选框的值。[#LC8520]
- 如果对 PNG 文件（支持透明度）执行 **Set-STFWebReceiverSiteStyle** 命令以自定义 StoreFront，PNG 文件将转换为 JPEG 文件。JPEG 文件格式可能会丢失透明度支持。[#LC8677]
- 如果执行 **Set-STFWebReceiverApplicationShortcuts** 命令以便为 Citrix Receiver for Web 站点中的应用程序快捷方式设置可信 URL，则可能会在 URL 的末尾添加正斜杠（“/”）。[#LC8761]
- 使用 **Set-STFWebReceiverSiteStyle** 命令自定义 StoreFront 时，style.css 可能会在 Custom 文件夹中错误地更改。因此，StoreFront 控制台将无法读取自定义设置。[#LC8776]
- StoreFront 服务器上可能会出现身份验证失败问题。此问题是由于 TCP 动态端口耗尽所致。[#LC8795]
- 尝试使用 **Set-STFWebReceiverSiteStyle** 命令更改 StoreFront 徽标可能会失败。[#LC8994]
- 在启用 **OverrideIcaClientname** 的情况下，尝试从远程桌面客户端建立远程会话可能会失败。未续订许可证时会出现此问题。可能会显示以下错误消息之一：

“The remote session could not be established from remote desktop client WR_XxXXxXXX because its license could not be renewed.”（无法从远程桌面客户端 WR_XxXXxXXX 建立远程会话，因为无法续订其许可证。）

或

“The remote session could not be established from remote desktop client WR_XxXXxXXX because its temporary license has expired.”（无法从远程桌面客户端 WR_XxXXxXXX 建立远程会话，因为其临时许可证已过期。）[#LC9246]

- 在 Citrix Receiver for Web 站点的任意实例的自定义文件目录中存在只读文件时，尝试升级 StoreFront 可能会失败。[#LC9252]
- 设置 XenDesktop 过程中选择已配置的站点时，默认站点可能是在 StoreFront 中创建的使用默认身份验证服务的站点。如果删除此应用商店，Citrix Receiver for Windows 的用户将无法添加任何其他应用商店，并且显示此错误消息：

  “A protocol error occurred while communicating with the Authentication Service.”（与身份验证服务通信时出现协议错误。）[#LC9404]
- 尝试登录到 StoreFront 可能会失败并显示错误**无法完成您的请求**。[#LC9521]
- 使用 StoreFront SDK 自定义特定功能以及为应用商店配置聚合时，登录可能会失败并显示错误**无法完成您的请求**。发布的应用程序的自定义图标采用最小分辨率时会出现此问题。 [#LC9561]

已知问题

Feb 26, 2018

本版本中存在以下已知问题。

- 如果在运行 .NET 4.6.1 或更早版本的服务器上禁用了 TLS 1.0，服务器组加入将不起作用。要解决此问题，请升级到 .NET 4.6.2 或更高版本。

  [# STF-687]

- 如果 StoreFront 最初是使用可执行文件从安装介质安装的，使用较高版本的完整产品安装程序时，StoreFront 将不显示为满足升级条件。解决方法：使用可执行文件从安装介质升级 StoreFront。

  [# DNA-47816]

- 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]

- 从 7.12 或更高版本的 Delivery Controller 升级过程中，会出现间歇性的（当 Windows CEIP 进程在夜间运行时会观察到）StoreFront 升级问题。显示以下错误：

  > StoreFront 无法升级，因为以下程序正在使用其中某些文件。请关闭该程序并重试。
  > 程序名称: CompatTelRunner

  要解决此问题，请按照屏幕上的说明进行操作。

  [# DNA-51341]

- 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]

第三方声明

Jun 04, 2018

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

系统要求

Jun 04, 2018

在计划进行安装时，Citrix 建议您除了服务器上安装的所有其他产品的要求以外，至少为 StoreFront 额外预留 2 GB 的 RAM 空间。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。

Citrix 已测试过，可以支持在以下平台上安装 StoreFront：

- 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。尽管服务器组最多可以包含六台服务器，但是从基于模拟的容量预测来看，包含三台以上服务器的服务器组不具有优势。一个服务器组中的所有服务器必须位于相同位置。

服务器上必须安装 Microsoft Internet Information Services (IIS) 和 Microsoft .NET Framework。如果这些必备项中的任一项已安装但未启用， StoreFront 安装程序将先启用该必备项，然后再安装产品。必须先在 Web 服务器上安装 Windows PowerShell 和 Microsoft 管理控制台（两者均为 Windows Server 的默认组件），然后才能安装 StoreFront。IIS 中 StoreFront 的相对路径在组中的所有 服务器上必须相同。

StoreFront 安装程序将添加所需的 IIS 功能。如果预安装这些功能，下面是所需功能的列表：

在所有平台上：

- 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

对于 Windows Server 2012 R2：

- Web-Asp-Net45
- Net-Wcf-Tcp-PortSharing45

在 Windows Server 2016 上
- Web-Asp-Net45
- Net-Wcf-Tcp-PortSharing45

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，必须可从企业网络内部进行访问。

- 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。
- TCP 端口 8008 仅由 Citrix Receiver for HTML5 使用，启用后，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。

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。

- XenApp 和 XenDesktop 7.18
- XenApp 和 XenDesktop 7.17
- XenApp 和 XenDesktop 7.16
- XenApp 和 XenDesktop 7.15
- XenApp 和 XenDesktop 7.14
- XenApp 和 XenDesktop 7.13
- XenApp 和 XenDesktop 7.12
- XenApp 和 XenDesktop 7.11
- XenApp 和 XenDesktop 7.9
- XenApp 和 XenDesktop 7.8
- XenApp 和 XenDesktop 7.7
- XenApp 和 XenDesktop 7.6
- XenApp 和 XenDesktop 7.5
- XenDesktop 7.1
- XenDesktop 7
- XenApp 6.5

NetScaler Gateway 要求

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

- NetScaler Gateway 12.0
- NetScaler Gateway 11.*x*
- NetScaler Gateway 10.5

Citrix Receiver for HTML5 要求

如果您计划支持用户使用在 Receiver for Web 站点上运行的 Citrix Receiver for HTML5 访问桌面和应用程序，还要满足以下要求。

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

- XenApp 和 XenDesktop 7.18
- XenApp 和 XenDesktop 7.17

- XenApp 和 XenDesktop 7.16
- XenApp 和 XenDesktop 7.15
- XenApp 和 XenDesktop 7.14
- XenApp 和 XenDesktop 7.13
- XenApp 和 XenDesktop 7.12
- XenApp 和 XenDesktop 7.11
- XenApp 和 XenDesktop 7.9
- XenApp 和 XenDesktop 7.8
- XenApp 和 XenDesktop 7.7
- XenApp 和 XenDesktop 7.6
- XenApp 和 XenDesktop 7.5
- XenDesktop 7.1
- XenDesktop 7
- XenApp 6.5 Feature Pack 2
- XenApp 6.5 Feature Pack 1 for Windows Server 2008 R2 （需要修补程序 XA650R01W2K8R2X64051，可从以下链接下载：http://support.citrix.com/article/CTX135757）

对于企业网络以外的远程用户，Citrix Receiver for HTML5 支持通过以下版本的 NetScaler Gateway 访问桌面和应用程序。

- NetScaler Gateway 12.0
- NetScaler Gateway 11.*x*

对于通过 NetScaler Gateway 连接的用户，Citrix Receiver for HTML5 支持访问以下产品所提供的桌面和应用程序。

- XenApp 和 XenDesktop 7.18
- XenApp 和 XenDesktop 7.17
- XenApp 和 XenDesktop 7.16
- XenApp 和 XenDesktop 7.15
- XenApp 和 XenDesktop 7.14
- XenApp 和 XenDesktop 7.13
- XenApp 和 XenDesktop 7.12
- XenApp 和 XenDesktop 7.11
- XenApp 和 XenDesktop 7.9
- XenApp 和 XenDesktop 7.8
- XenApp 和 XenDesktop 7.7
- XenApp 和 XenDesktop 7.6
- XenApp 和 XenDesktop 7.5
- XenDesktop 7.1
- XenDesktop 7
- XenApp 6.5

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 Receiver 用户可以通过 Citrix Receiver 访问应用商店，也可以使用 Web 浏览器登录 Citrix Receiver for Web 站点来访问应用商店。对于无法安装 Citrix Receiver 但具有兼容 HTML5 的 Web 浏览器的用户，您可以在 Citrix Receiver for Web 站点上启用 Citrix Receiver for HTML5，使这些用户可以直接在 Web 浏览器中访问桌面和应用程序。

具有未加入域的桌面设备的用户将通过自己的 Web 浏览器（已配置为访问桌面设备站点）来访问桌面。对于运行 Citrix

Desktop Lock 的已加入域的桌面设备和重用 PC 以及无法升级的旧版 Citrix 客户端，用户必须通过 XenApp Services URL 进行连接来访问应用商店。

如果要向用户交付脱机应用程序，则除了 Citrix Receiver for Windows 之外，还需要安装脱机插件。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。

假定所有用户设备都满足已安装操作系统的最低硬件要求。

启用 Citrix Receiver 的应用商店的要求

可以使用以下 Citrix Receiver 版本通过内部网络连接和 NetScaler Gateway 来访问 StoreFront 应用商店。可以使用 NetScaler Gateway 插件和/或无客户端访问通过 NetScaler Gateway 进行连接。要获得完整的 StoreFront 统一 Citrix Receiver 体验，使用的版本至少应为 Citrix Receiver for Windows 4.5。请参阅支持统一的 Citrix Receiver 体验。

- Citrix Receiver for Chrome 2.x
- Citrix Receiver for HTML5 2.x
- Citrix Receiver for Mac 12.x
- Citrix Receiver for Windows 4.x
- Citrix Receiver for Linux 13.x

通过 Citrix Receiver for Web 站点访问应用商店的要求

建议用户使用以下 Citrix Receiver、操作系统和 Web 浏览器的组合，从内部网络连接和通过 NetScaler Gateway 来访问 Citrix Receiver for Web 站点。可以使用 NetScaler Gateway 插件和无客户端访问通过 NetScaler Gateway 进行连接。

除非明确声明，否则建议使用最新版本的浏览器。

- Citrix Receiver for Windows 4.5 及更高版本，直至 Citrix Receiver for Windows 4.12
  - Windows 10（32 位和 64 位版本）
    - Microsoft Edge
    - Internet Explorer 11
    - Google Chrome
    - Mozilla Firefox
  - Windows 8.1（32 位和 64 位版本）
    - Internet Explorer 11（32 位模式）
    - Google Chrome
    - Mozilla Firefox
  - Windows 8（32 位和 64 位版本）
    - Internet Explorer 10（32 位模式）
    - Google Chrome
    - Mozilla Firefox
  - Windows 7 Service Pack 1（32 位和 64 位版本）
    - Internet Explorer 11、10、9
    - Google Chrome
    - Mozilla Firefox
  - Windows Embedded Standard 7 Service Pack 1 或 Windows Thin PC
    - Internet Explorer 11、10、9

- Citrix Receiver for Mac 12.0
  - Mac OS X 10.11 El Capitan
    - Safari 9
    - Google Chrome
    - Mozilla Firefox
  - Mac OS X 10.10 Yosemite
    - Safari 8
    - Google Chrome
    - Mozilla Firefox
  - Mac OS X 10.9 Mavericks
    - Safari 7
    - Google Chrome
    - Mozilla Firefox
- Citrix Receiver for Linux 13.x
  - Ubuntu 12.04（32 位）和 14.04 LTS（32 位）
    - Google Chrome
    - Mozilla Firefox

通过 Receiver for HTML5 访问桌面和应用程序的要求

建议用户使用以下操作系统和 Web 浏览器，通过 Receiver for Web 站点上运行的 Receiver for HTML5 访问桌面和应用程序。内部网络连接和通过 NetScaler Gateway 进行的连接均受支持。但是，对于从内部网络发起的连接，Receiver for HTML5 仅支持对特定产品提供的资源进行访问。此外，需要具有特定版本的 NetScaler Gateway 才允许从企业网络以外进行连接。有关详细信息，请参阅基础结构要求。

除非明确声明，否则建议使用最新版本的浏览器。

- 浏览器
  - Microsoft Edge
  - Internet Explorer 11
  - Safari 7
  - Google Chrome
  - Mozilla Firefox
- 操作系统
  - Windows 10（32 位和 64 位版本）
  - Windows 8.1（32 位和 64 位版本）
  - Windows 8（32 位和 64 位版本）
  - Windows 7 Service Pack 1（32 位和 64 位版本）
  - Windows Vista Service Pack 2（32 位和 64 位版本）
  - Windows Embedded XP
  - Mac OS X 10.10 Yosemite
  - Mac OS X 10.9 Mavericks
  - Mac OS X 10.8 Mountain Lion
  - Google Chrome OS 48
  - Google Chrome OS 47
  - Ubuntu 12.04（32 位）

通过桌面设备站点访问应用商店的要求

建议用户使用以下 Citrix Receiver、操作系统和 Web 浏览器的组合，从内部网络访问桌面设备站点。不支持通过 NetScaler Gateway 进行连接。

- Citrix Receiver for Windows 4.5
  - Windows 8.1（32 位和 64 位版本）
    - Internet Explorer 11（32 位模式）
  - Windows 8（32 位和 64 位版本）
    - Internet Explorer 10（32 位模式）
  - Windows 7 Service Pack 1（32 位和 64 位版本）、Windows Embedded Standard 7 Service Pack 1 或 Windows Thin PC
    - Internet Explorer 9（32 位模式）
    - Internet Explorer 8（32 位模式）
  - Windows Embedded XP
    - Internet Explorer 8（32 位模式）

通过 XenApp Services URL 访问应用商店的要求

可以使用上面列出的所有 Citrix Receiver 版本通过 XenApp Services URL 访问功能有所减少的 StoreFront 应用商店。如果支持，可以使用 NetScaler Gateway 插件和无客户端访问通过 NetScaler Gateway 进行连接。

智能卡要求

Citrix Receiver for Windows 4.X 与智能卡配合使用的要求

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 XenApp 和 XenDesktop 文档中的智能卡以及 http://www.citrix.com/ready。

通过 NetScaler Gateway 进行身份验证的要求

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 NetScaler Gateway 访问 StoreFront。

- NetScaler Gateway 12.0
- NetScaler Gateway 11.x
- NetScaler Gateway 10.5

规划 StoreFront 部署

Nov 27, 2017

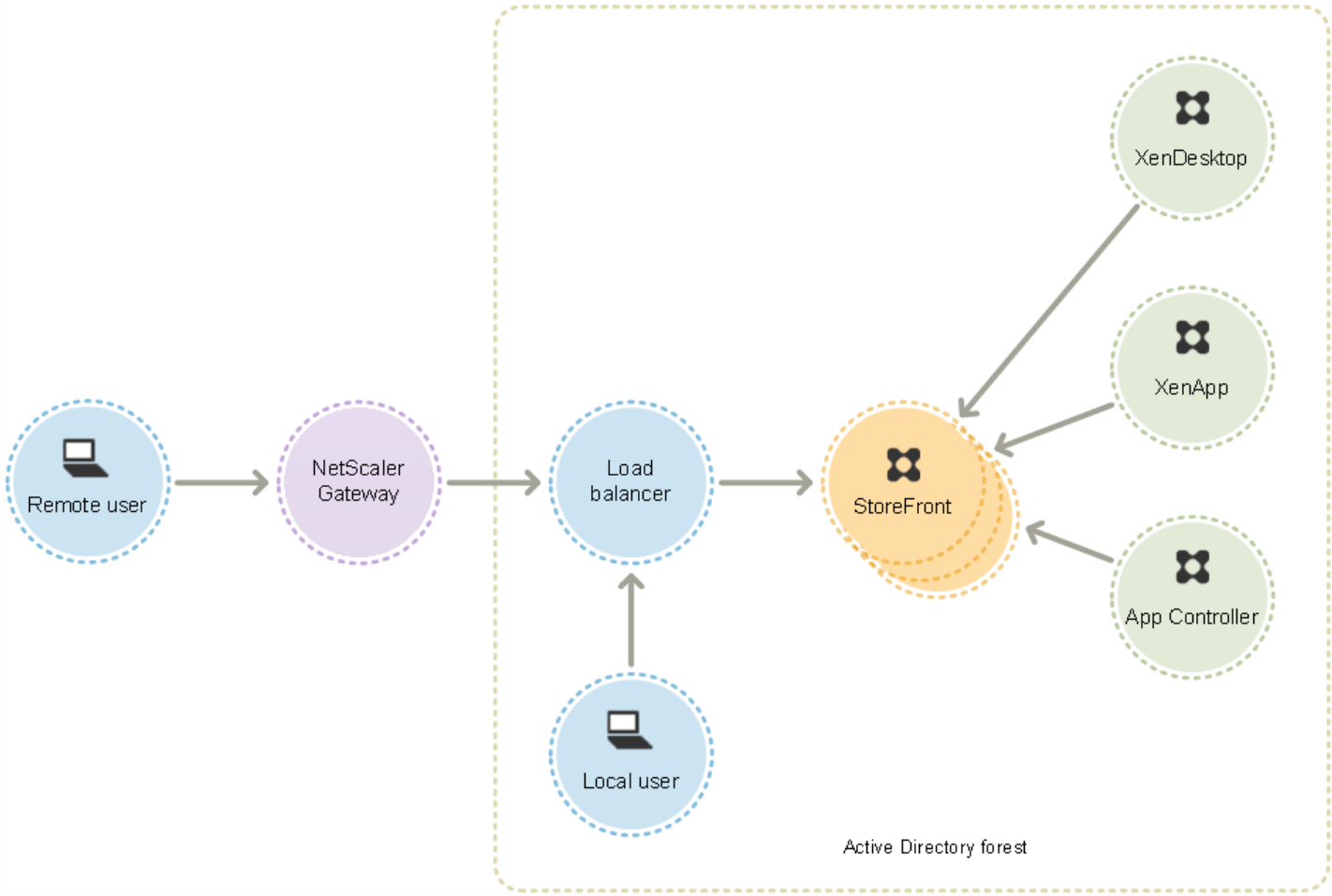
StoreFront 使用 Microsoft Internet Information Services (IIS) 上运行的 Microsoft .NET 技术提供将资源聚合在一起的企业应用商店，并使其可供用户访问。StoreFront 与 XenDesktop、XenApp 和 App Controller 部署相集成，为用户提供单一的自助访问点，以访问其桌面和应用程序。

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 XenDesktop、XenApp 和 App Controller 中的桌面和应用程序。用户通过 Citrix Receiver、Citrix Receiver for Web 站点、桌面设备站点和 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。

下图显示了典型的 StoreFront 部署。



对于多服务器部署，需要使用 NetScaler 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 NetScaler 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 http://technet.microsoft.com/zh-cn/library/hh831698.aspx。

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 XenDesktop 站点和 XenApp 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 NetScaler。

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

语法：

Set-STFWebReceiverCommunication [-WebReceiverService] [[-Loopback]] [[-LoopbackPortUsingHttp]]

有效值包括：

- **On** - 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
```

请注意，必须关闭环回才能使用 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。

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 XenApp 和 XenDesktop 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。

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 NetScaler 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 NetScaler Gateway 并使用防火墙将 NetScaler Gateway 与公用和内部网络进行分隔。请确保 NetScaler Gateway 能够访问包含 StoreFront 服务器的 Active Directory 林。

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。

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 How to set up your first IIS Website（如何设置您的第一个 IIS 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。

1. Add-STFDeployment -SiteID 1 -HostBaseURL "https://www.storefront.app.com"
2. 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。

StoreFront 服务器组支持的 Citrix Receiver 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。

建议最低为每台服务器分配 4 GB 内存。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。与使用 Web Receiver 一样，使用 Citrix Receiver 时，除了本版本的 StoreFront 的基础 4 GB 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。

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：一个服务器组中的所有服务器必须位于相同的位置。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 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重试次数和通信超时持续时间和重试次数。

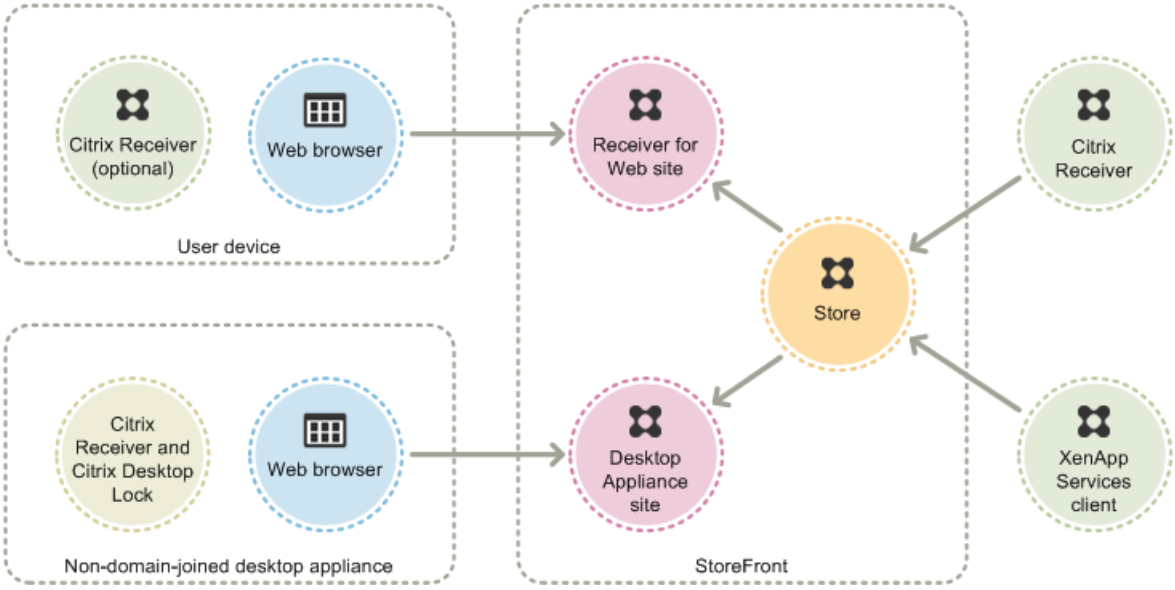
用户访问选项

Jun 04, 2018

用户可以通过四种不同的方法访问 StoreFront 应用商店。

- Citrix Receiver - 具有兼容版本 Citrix Receiver 的用户可以通过 Citrix Receiver 用户界面访问 StoreFront 应用商店。通过 Citrix Receiver 访问应用商店，可以提供最佳的用户体验和最强大的功能。
- Receiver for Web 站点 - 具有兼容 Web 浏览器的用户可以通过浏览到 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，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。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。
- 桌面设备站点 - 未加入域的桌面设备的用户可以通过设备上的 Web 浏览器（已配置为以全屏模式访问桌面设备站点）访问桌面。当您使用 Citrix Studio 为 XenDesktop 部署创建了一个新应用商店时，默认情况下将为该应用商店创建一个桌面设备站点。
- XenApp Services URL - 使用运行 Citrix Desktop Lock 的已加入域的桌面设备和重用 PC 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：



从 Citrix Receiver 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 版本，请参阅系统要求。

Citrix Receiver 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 Receiver 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 Receiver。这使 Citrix Receiver 能够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 Receiver 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 Receiver 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 文档中的*使用命令行参数配置和安装 Citrix Receiver for Windows*。

置备文件

可以为用户提供置备文件，其中包含应用商店的详细连接信息。在安装 Citrix Receiver 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 站点为用户提供的置备文件仅适用于站点所对应的单个应用商店。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，并从这些站点下载置备文件。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置备文件。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置备文件。

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 Setup URL Generator 创建包含应用商店详细连接信息的 URL。安装 Citrix Receiver 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 Receiver 中输入应用商店 URL 来创建新帐户。更多信息，请参阅 Citrix Receiver 文档。

基于电子邮件的帐户发现

首次在设备上安装 Citrix Receiver 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 站点或您内部网络所托管的 Citrix Receiver 下载页面下载了 Citrix Receiver。您可以在 Microsoft Active Directory 域名系统 (DNS) 服务器上为 NetScaler 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 Receiver 初始配置过程中输入其电子邮件地址。Citrix Receiver 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 Receiver 获得可访问应用商店的列表。

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 Receiver 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 站点或内部网络中的 Citrix Receiver 下载页面下载 Citrix Receiver，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 Receiver。如果 Citrix Receiver 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 Receiver 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 Receiver 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 Receiver 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 NetScaler Gateway 或 StoreFront 的服务位置 (SRV) 定位器资源记录。作为备用方法，也可以在名为“discoverReceiver.domain“的服务器上部署 StoreFront，其中 domain 为包含用户的电子邮件帐户的域。如果在指定域中未找到 SRV 记录，则 Citrix Receiver 将搜索名为 discoverReceiver 的计算机，以识别 StoreFront 服务器。

您必须在 NetScaler 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。要获得最佳用户体验，请安装包含使用者或使用者备用名称条目（属于 discoverReceiver.domain）的证书，其中 domain 为包含用户的电子邮件帐户的域。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 Receiver 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 NetScaler 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。在域上单击鼠标右键，并选择**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**创建纪录**。
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 NetScaler 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）的完全限定的域名 (FQDN) 和端口。
   如果环境中同时包括内部和外部 DNS 服务器，则可以在内部 DNS 服务器上添加一条指定 StoreFront 服务器 FQDN 的 SRV 记录，在外部服务器上添加另一条指定 NetScaler Gateway FQDN 的 SRV 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 NetScaler Gateway 连接信息。
7. 如果针对 NetScaler 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 NetScaler Gateway 中。

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 Receiver，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 Receiver 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 Receiver。如果检测不到 Citrix Receiver，系统将提示用户下载并安装适用于其平台的 Citrix Receiver。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 Receiver 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 和 Citrix Receiver for Mac 部署的详细信息，请参阅配置 Citrix Receiver for Web 站点。

Citrix Receiver for HTML5

Citrix Receiver for HTML5 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 Citrix Receiver for HTML5，以便无法安装 Citrix Receiver 的用户仍然能够访问其资源。使用 Citrix Receiver for HTML5，用户可以直接在兼容 HTML5 的 Web 浏览器中访问桌面和应用程序，而无需安装 Citrix Receiver。创建站点后，默认情况下将禁用 Citrix Receiver for HTML5。有关启用 Citrix Receiver for HTML5 的详细信息，请参阅 citrix-receiver-download-page-template.html。

要使用 Citrix Receiver for HTML5 访问自己的桌面和应用程序，用户必须使用兼容 HTML5 的浏览器访问 Citrix Receiver for Web 站点。有关可以与 Citrix Receiver for HTML5 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 NetScaler Gateway 连接的远程用户均可使用 Citrix Receiver for HTML5。对于来自内部网络的连接，Citrix Receiver for HTML5 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 Citrix Receiver for HTML5 作为选项，则通过 NetScaler Gateway 连接的用户将能够访问各种产品。需要将特定版本的 NetScaler Gateway 与 Citrix Receiver for HTML5 集合使用。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 Citrix Receiver for HTML5 访问 XenDesktop 和 XenApp 提供的资源。要允许使用 Citrix Receiver for HTML5 本地访问桌面和应用程序，必须在您的 XenDesktop 和 XenApp 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 Citrix Receiver for HTML5 端口。有关详细信息，请参阅 WebSockets 策略设置。

默认情况下，Citrix Receiver for HTML5 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 Citrix Receiver for HTML5 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内。您可以配置 Citrix Receiver for HTML5，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 Citrix Receiver for HTML5 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 Receiver 或者能够使用 Citrix Receiver for HTML5，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 Receiver 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，以避免出现此额外步骤。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一个快捷方式。快捷方式不能将命令行参数传递给应用程序。

要创建应用程序快捷方式，您可以使用将用于托管快捷方式的内部 Web 站点的 URL 来配置 StoreFront。用户单击 Web 站点上的应用程序快捷方式时，StoreFront 会对照您输入的 URL 列表来检查该 Web 站点，以确保请求来自可信 Web 站点。但是，对于通过 NetScaler 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受信任内部 Web 站点上的应用程序快捷方式，请将 NetScaler 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 Receiver 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 NetScaler 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 NetScaler Gateway 进行连接，则可以通过 HTTPS 连接使用 Citrix Receiver for HTML5。
- 要通过 HTTPS 连接对 Mozilla Firefox 使用 Citrix Receiver for HTML5，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。

未加入域的桌面设备的用户可以通过桌面设备站点访问其桌面。在本上下文中，未加入域表示设备没有加入包含 StoreFront 服务器的 Microsoft Active Directory 林中的域。

当您使用 Citrix Studio 为 XenDesktop 部署创建了一个新应用商店时，默认情况下将为该应用商店创建一个桌面设备站点。仅当 StoreFront 已安装并被配置为 XenDesktop 安装的一部分时才会默认创建桌面设备站点。您可以使用 Windows PowerShell 命令手动创建桌面设备站点。有关详细信息，请参阅配置桌面设备站点。

桌面设备站点可提供类似于登录到本地桌面的用户体验。桌面设备上的 Web 浏览器已配置为以全屏模式启动，并会显示桌面设备站点的登录屏幕。用户登录到站点时，默认情况下将自动启动为其配置了站点的应用商店中可供用户使用的第一个桌面（按字母顺序）。如果在一个应用商店中为用户提供了多个桌面的访问权限，则可以配置桌面设备站点以显示可用桌面，以便用户从中选择要访问的桌面。有关详细信息，请参阅配置桌面设备站点。

当用户桌面启动时，它将以全屏模式显示，因此会将 Web 浏览器遮住。用户将自动从桌面设备站点注销。当用户从桌面注销时，显示桌面设备站点登录屏幕的 Web 浏览器会再次显示出来。桌面启动时会显示一条消息，其中包含了一个链接，如果桌面无法访问，用户可以单击此链接重新启动桌面。要启用此功能，必须将交付组配置为允许用户重新启动桌面。有关详细信息，请参阅交付组。

要提供对桌面的访问，桌面设备上必须装有兼容版的 Citrix Receiver。通常，与 XenDesktop 兼容的设备供应商会将 Citrix Receiver 集成到自己的产品中。对于 Windows 设备，还必须安装 Citrix Desktop Lock，并为其配置桌面设备站点的 URL。如果使用 Internet Explorer，则必须将桌面设备站点添加到“本地 Intranet”或“可信站点”区域。有关 Citrix Desktop Lock 的详细信息，请参阅阻止用户访问本地桌面。

重要注意事项

桌面设备站点适用于内部网络中从未加入域的桌面设备访问桌面的本地用户。决定是否使用桌面设备站点向用户提供对应用商店的访问时，请考虑以下限制。

- 如果您计划部署已加入域的桌面设备和重用 PC，则不要将其配置为通过桌面设备站点访问应用商店。虽然可以为应用商店配置使用 XenApp Services URL 的 Citrix Receiver，但是，我们建议您为已加入域和未加入域的用例使用新的 Desktop Lock。有关详细信息，请参阅 Citrix Receiver Desktop Lock。
- 桌面设备站点不支持来自企业网络之外的远程用户连接。登录到 NetScaler Gateway 的用户无法访问桌面设备站点。

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 Receiver 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 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 XenDesktop 和 XenApp 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 的形式为 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 为在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 Receiver 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 Receiver 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，工作区控制对 XenApp Services URL 启用，不能进行配置或将其禁用。
- 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 XenDesktop 和 XenApp 服务器路由到域控制器。

用户身份验证

Jun 04, 2018

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 NetScaler Gateway 访问 Citrix Receiver for Web 时，NetScaler 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 用户界面选择性更改密码。选择性更改密码后，NetScaler Gateway 会话将终止，用户必须重新登录。Citrix Receiver for Linux 用户只能更改过期密码。

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 NetScaler。

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：

- 实施 Citrix 联合身份验证服务。
- 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 Microsoft 广告 FS 2016 部署和 Microsoft 广告 FS 2016 操作。
  - Microsoft AD FS v3.0 (Windows Server 2012 R2)
  - NetScaler 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 Citrix Receiver for Web。

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

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 Receiver 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 站点只支持 Internet Explorer 的域直通身份验证。在管理控制台的 Citrix Receiver for Web 站点节点中启用域直通身份验证，而且您需要在 Citrix Receiver for Windows 上配置 SSON。Citrix Receiver for HTML5 不支持域直通身份验证。要使用域直通身份验证，用户需要具有 Citrix Receiver for Windows 或适用于 Windows 的联机插件。在用户设备上安装 Citrix Receiver for Windows 或适用于 Windows 的联机插件时，必须启用直通身份验证。

用户向 NetScaler 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，NetScaler 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 Receiver 或 Citrix Receiver for Web 站点通过 NetScaler Gateway 连接到应用商店。桌面设备站点不支持通过 NetScaler Gateway 进行连接。有关配置 StoreFront 以支持 NetScaler Gateway 的详细信息，请参阅添加 NetScaler Gateway 连接。

StoreFront 支持使用针对以下 NetScaler 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的通行码登录 NetScaler Gateway，令牌代码由安全令牌（某些情况下与个人识别码组合）生成。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 NetScaler 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 NetScaler Gateway，并根据提供给 NetScaler 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 NetScaler 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 NetScaler 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 NetScaler Gateway 的用户。要为智能卡用户配置从 NetScaler Gateway 到 StoreFront 的直通身份验证，需要将凭据验证委派给 NetScaler 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 NetScaler 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 Receiver 连接到应用商店。无法安装 NetScaler 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 Receiver 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 Receiver 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 NetScaler Gateway 配置为安全远程代理。用户直接登录到 NetScaler 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 NetScaler Gateway 插件。

如果您为从 Citrix Receiver 访问应用商店的远程用户配置了为 NetScaler Gateway 执行双来源身份验证，则必须在 NetScaler 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 NetScaler 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

要为从 NetScaler Gateway 到 StoreFront 的访问启用多域身份验证，请在每个域的 NetScaler 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 NetScaler 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 NetScaler 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 NetScaler Gateway 部署支持的情况下，您可以使用 SmartAccess 并根据 NetScaler Gateway 会话策略来控制用户对 XenDesktop 和 XenApp 资源的访问。有关 SmartAccess 的详细信息，请参阅 How SmartAccess works for XenApp and XenDesktop（SmartAccess 对 XenApp 和 XenDesktop 的工作原理）。

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 Receiver、Citrix Receiver for Web、桌面设备站点和 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，同时增强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 XenDesktop 和 XenApp 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。

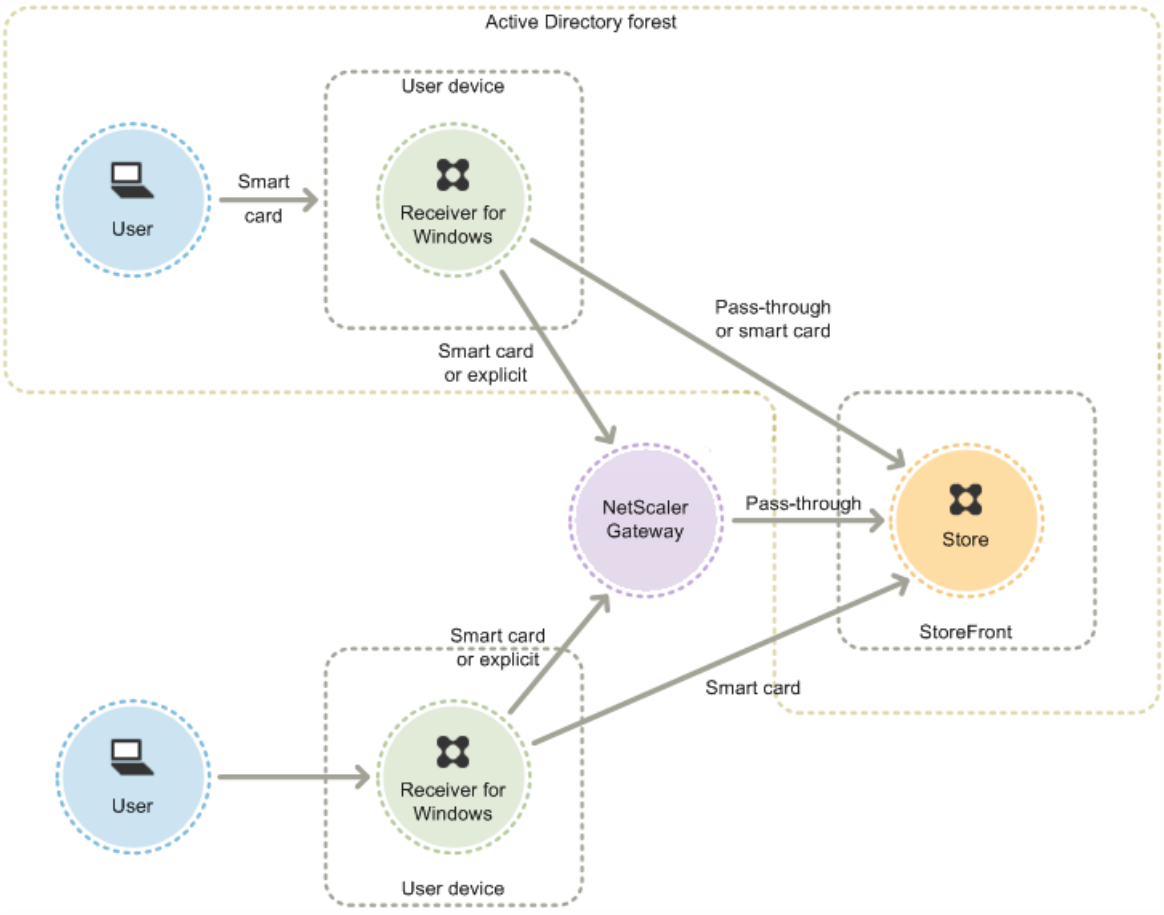
要启用智能卡身份验证，必须在包含 StoreFront 服务器的 Microsoft Active Directory 域或与 StoreFront 服务器域具有直接双向信任关系的域中配置用户的帐户。支持涉及双向信任的多林部署。

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 使用智能卡

使用运行 Citrix Receiver for Windows 的设备的用户可以使用智能卡直接进行身份验证，或通过 NetScaler 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 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，可以针对 Citrix Receiver for Windows 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 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到 Citrix Receiver for Windows，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 NetScaler 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 NetScaler Gateway 进行针对 StoreFront 的直通身份验证并将凭据验证工作委派给 NetScaler Gateway。然后，创建额外的 NetScaler 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，还必须配置为 Citrix Receiver for Windows 配置直通身份验证。

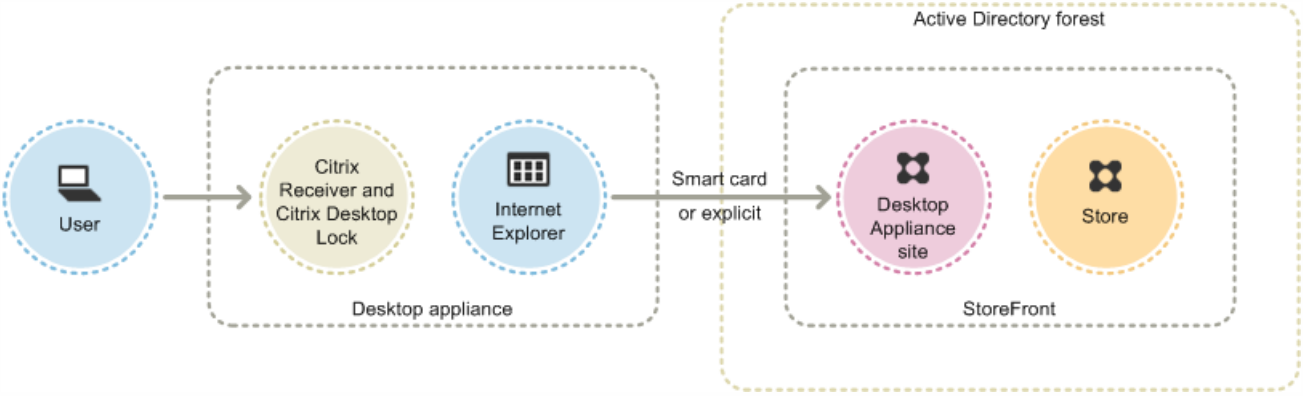
注意： 如果使用的是 Citrix Receiver for Windows 4.5 或更高版本，则可以设置第二个 vServer 并使用最佳网关路由功能，这样在启动应用程序和桌面时，不需要再显示 PIN 提示。

用户可以使用智能卡和 PIN 或使用显式凭据登录到 NetScaler 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 NetScaler Gateway 登录。可以配置从 NetScaler 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 NetScaler Gateway，这样用户就可以无提示地通过 StoreFront 的身份验证。

对桌面设备站点使用智能卡

可以将未加入域的 Windows 桌面设备配置为允许用户使用智能卡登录到桌面。设备上必须装有 Citrix Desktop Lock，并且必须使用 Internet Explorer 来访问桌面设备站点。

下图显示了如何从未加入域的桌面设备进行智能卡身份验证。



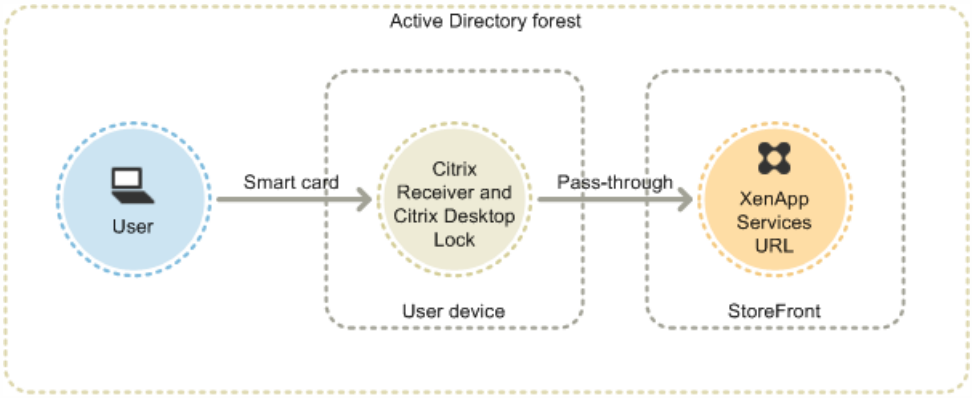
在用户访问其桌面设备时，Internet Explorer 会以全屏模式启动，显示桌面设备站点的登录屏幕。用户使用智能卡和 PIN 向站点验证身份。如果桌面设备站点已配置为支持直通身份验证，则用户在访问桌面和应用程序时将自动进行身份验证。系统不会再次提示用户输入 PIN。如果不支持直通身份验证，则用户在启动桌面或应用程序时必须再次输入 PIN。

可以允许用户在智能卡出现问题时回退至显式身份验证。为此，您需要将桌面设备站点配置为支持智能卡和显式身份验证这两种方法。在此配置中，将智能卡身份验证视为主要访问方法，以便首先提示用户输入 PIN。但是，站点也提供了一个链接，允许用户使用显式凭据进行登录。

对 XenApp Services URL 使用智能卡

已加入域的桌面设备以及运行 Citrix Desktop Lock 的重用 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，不会提示其再次输入 PIN。

对 Citrix Receiver for Web 使用智能卡

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

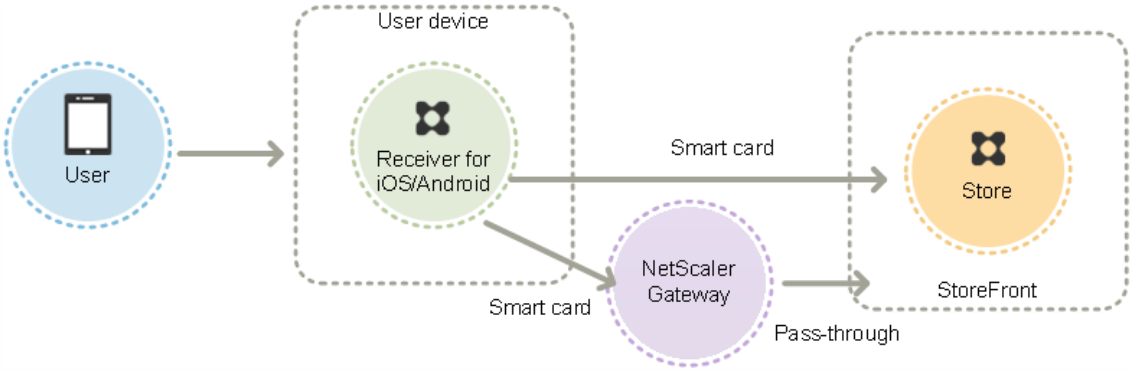
1. 在左侧面板中选择 Citrix Receiver for Web 节点。
2. 选择要使用智能卡身份验证的站点。
3. 在右侧面板中选择选择身份验证方法任务。
4. 选中弹出对话框屏幕中的“智能卡”复选框，然后单击确定。

如果为使用已加入域的设备但不通过 NetScaler Gateway 访问应用商店的 Citrix Receiver for Windows 用户启用了对 XenDesktop 和 XenApp 使用智能卡直通身份验证的支持，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并且通过 NetScaler Gateway 访问应用商店的 Citrix Receiver for Windows 用户启用了对 XenDesktop 和 XenApp 使用智能卡直通身份验证的支持，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 Citrix Receiver for iOS 和 Android 使用智能卡

使用运行 Citrix Receiver for iOS 和 Citrix Receiver for Android 的设备的用户可以使用智能卡直接进行身份验证，或通过 NetScaler 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 Receiver，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 NetScaler 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 NetScaler Gateway 进行针对 StoreFront 的直通身份验证并将凭据验证工作委派给 NetScaler Gateway。然后，创建额外的 NetScaler 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 NetScaler Gateway，具体视您为连接指定身份验证的方式而定。可以配置从 NetScaler 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 NetScaler Gateway，这样用户就可以无提示地通过 StoreFront 的身份验证。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 使用智能卡

使用运行 Citrix Receiver for Linux 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对 Linux 设备进行身份验证，Citrix Receiver for Linux 也无法获得或重用所输入的 PIN。

采用与 Citrix Receiver for Windows 相同的方式来配置智能卡的服务器端组件。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 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，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 NetScaler 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 NetScaler Gateway 进行针对 StoreFront 的直通身份验证并将凭据验证工作委派给 NetScaler Gateway。然后，创建额外的 NetScaler 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 NetScaler 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 NetScaler Gateway 登录。可以配置从 NetScaler 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 NetScaler Gateway，这样用户就可以无提示地通过 StoreFront 的身份验证。

XenApp Services 支持站点不支持 Citrix Receiver for Linux 的智能卡。

同时为服务器和 Citrix Receiver 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。使用智能卡针对 Citrix XenApp 和 XenDesktop 服务器对用户进行身份验证。
- 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

登录到 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 Receiver 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 **et-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 NetScaler 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 NetScaler 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 NetScaler Gateway 访问应用商店的 Citrix Receiver for Windows 用户启用了对 XenDesktop 和 XenApp 使用智能卡直通身份验证的支持，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并且通过 NetScaler Gateway 访问应用商店的 Citrix Receiver for Windows 用户启用了对 XenDesktop 和 XenApp 使用智能卡直通身份验证的支持，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 NetScaler 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

Feb 26, 2018

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、桌面设备站点和 XenApp Services URL 时进行配置。

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。

对于 Citrix Receiver for Web 站点以及通过 XenApp Services URL 建立的与应用商店之间的连接，工作区控制默认情况下处于启用状态。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 Receiver，或者使用 Citrix Receiver for HTML5 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 Receiver 从桌面或开始菜单本地启动的资源。

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 XenDesktop 或 XenApp 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。

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。

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。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。系统只向从内部网络进行连接的用户显示密码过期警告。有关允许用户更改密码的详细信息，请参阅配置身份验证服务。

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。

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。XenDesktop 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 Receiver 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。

在使用 XenDesktop 和 XenApp 交付应用程序时，请考虑使用以下选项来增强用户在通过您的应用商店访问其应用程序时的体验。有关交付应用程序的详细信息，请参阅创建交付组应用程序。

- 使用文件夹来组织应用程序，以便用户在浏览可用资源时能够轻松查找所需内容。在 XenDesktop 和 XenApp 中创建的文件夹将在 Citrix Receiver 中以类别形式显示。例如，您可以根据类型对应用程序进行分组，也可以为贵组织内的各种用户角色分别创建文件夹。
- 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 Receiver 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 Receiver 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中，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置备，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 中自动对所有用户可用复选框。
- 可以向用户公告 XenDesktop 应用程序，或者通过在 Citrix Receiver 的精选列表中列出常用的应用程序使其更易于查找。为此，请将字符串 KEYWORDS:Featured 附加到应用程序说明的末尾。
  注意：多个关键字之间必须用空格进行分隔；例如 KEYWORDS:Auto Featured。
- 默认情况下，Citrix Receiver for Web 站点对待 XenDesktop 和 XenApp 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，请在应用程序说明中附加字符串 **KEYWORDS:prefer="application"**，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 Receiver 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 Receiver 将为用户订阅该交付的应用程序，但不会创建快捷方式。当用户从 Citrix Receiver 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 Configure application delivery（配置应用程序交付）。

- 在 XenApp 和 XenDesktop 7.17 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 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、“XenApp 和 XenDesktop”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

Nov 27, 2017

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，请参阅设置高可用性多站点应用商店配置。

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 XenDesktop 和 XenApp 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 XenDesktop 和 XenApp 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，并为用户呈现一个图标。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 XenDesktop 和 XenApp 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，并将 KEYWORDS:Secondary 附加到其他部署中的相应资源。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。

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权限。这样，就可以通过单个应用商店为不同用户组配置不用体验。

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

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

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。

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。

如果已经为部署配置了单独的 NetScaler 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 NetScaler 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 NetScaler 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 NetScaler Gateway 进行端点分析的这种特殊情况，也可以使用最佳 NetScaler Gateway 路由。利用此配置，用户将通过 NetScaler 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 NetScaler Gateway。请注意，还必须为 NetScaler 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 Receiver 连接到 NetScaler Gateway，而不考虑用户的网络位置。

StoreFront 支持将 NetScaler 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 NetScaler Gateway 虚拟服务器的 IP 地址。

有关负载平衡的详细信息，请参阅使用 NetScaler 进行负载平衡。

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 Receiver 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

Jun 04, 2018

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 XenDesktop 和 XenApp 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 NetScaler 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 NetScaler 实现负载平衡的详细信息，请参阅使用 NetScaler 进行负载平衡。

   1. 确保在 NetScaler 设备上启用负载平衡。
   2. 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 TLS 负载平衡服务。
   3. 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。

   4. 创建虚拟服务器并将服务绑定到虚拟服务器。
   5. 在虚拟服务器上，如果您在所有平台上都安装了最新的 Citrix Receiver，并且不需要支持 Android，则可以使用 cookie 插入方法配置持久性；否则，请在源 IP 地址的基础上配置持久性。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
   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 Receiver 需要使用 HTTPS 来连接应用商店。可以在安装 StoreFront 后随时从 HTTP 更改为 HTTPS，只要相应的 IIS 配置已就位即可。

要将 IIS 配置为支持 HTTPS，请使用 StoreFront 服务器上的 Internet Information Services (IIS) 管理器控制台，创建由域证书颁发机构签名的服务器证书。然后，将 HTTPS 绑定添加到默认 Web 站点。有关在 IIS 中创建服务器证书的详细信息，请参阅 http://technet.microsoft.com/zh-cn/library/hh831637.aspx#CreateCertificate。有关将 HTTPS 绑定添加到 IIS 站点的详细信息，请参阅 http://technet.microsoft.com/zh-cn/library/hh831632.aspx#SSLBinding。

7. 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。

8. 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。

9. 使用 Citrix StoreFront 管理控制台配置服务器。

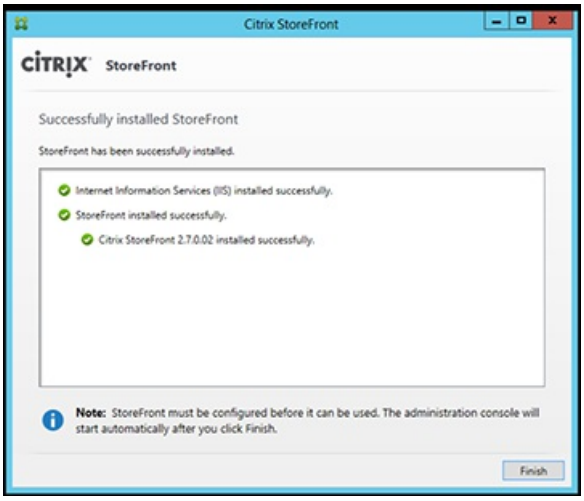
> ## Important
>
> 为避免安装 StoreFront过程中可能会出现的错误和数据丢失情况，请务必关闭所有应用程序，并且不要在目标系统中运行任何其他任务或操作。

1. 从下载页面下载安装程序。
2. 使用具有本地管理员权限的帐户登录 StoreFront 服务器。
3. 请务必在服务器上安装所需的 Microsoft .NET Framework。
4. 浏览下载的软件包，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

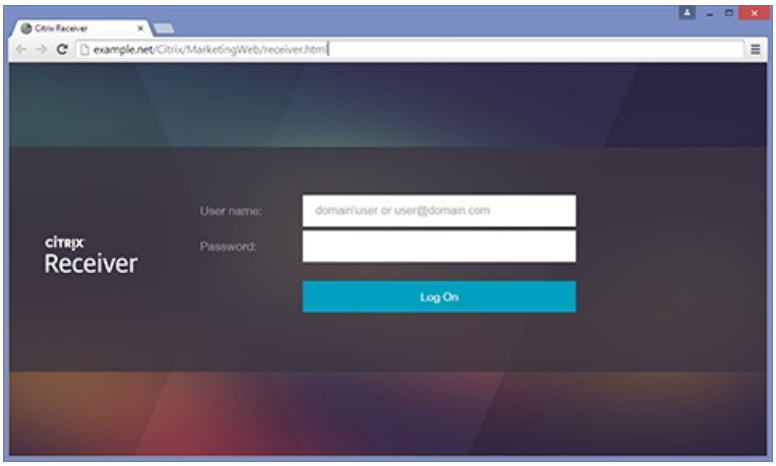
   如果尚未配置以下功能，则同时会启用这些功能。

   - .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。



9. 在 Citrix StoreFront 管理控制台中，单击创建新部署。
    1. 在**基本 URL** 框中指定 StoreFront 服务器的 URL。
    2. 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。
10. 在 **Delivery Controller** 页面上，列出用于提供希望通过应用商店获得的资源的基础结构（XenApp 或 XenDesktop Services 的详细信息）。您可以在此处输入一个“虚拟”服务器；但是不会在应用商店中显示任何应用程序。
11. 设置**传输类型**和**端口**。您可以指定 HTTP 和端口 443，然后单击**确定**。或者，也可以复制现有 Web Interface 或 StoreFront 部署中的设置。
12. 在**远程访问**页面上，选择无。如果要使用 NetScaler Gateway，请选择无 VPN 通道，然后输入网关详细信息。
13. 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/MarketingWeb/。登录后，您将在 Citrix Receiver 中访问新的用户界面。



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）：

位置：HKLM:\Software\Citrix\Telemetry\CEIP

名称：Enabled

类型：REG_DWORD

值：0 = 禁用，1 = 启用

默认情况下，“Enabled”属性隐藏在注册表中。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退出 CEIP ，则退出将应用于这两个组件。

从 StoreFront 收集的 CEIP 数据

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

数据	说明
StoreFront 版本	指示安装的 StoreFront 版本的字符串。例如，“3.8.0.0”
应用商店计数	表示部署中的应用商店数量的计数器。
服务器组中的服务器计数	表示服务器组中的服务器数量的计数器。
每个应用商店的 Delivery Controller 计数	指示可供部署中每个应用商店使用的 Delivery Controller 数量的数值列表。
启用 HTTPS	指示是否为部署启用 https 的字符串。“True”或“False”。
为 Citrix Receiver 启用经典经验	布尔值列表，指示是否为每个 Web Receiver 启用“经典体验”。对于每个 Web Receiver 为 TRUE 或 FALSE。
Citrix Receiver 的 HTML5 设置	字符串列表，指示每个 Web Receiver 的 HTML5 Receiver 设置。对于每个 Web Receiver 为“始终”、“回退”或“关”。

为 Citrix Receiver 启用工作区控制	布尔值列表，指示是否为每个 Web Receiver 启用“工作区控制”。对于每个 Web Receiver 为 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”。对于每个应用商店为“已启用”或“已禁用”。
网关计数	表示部署中配置的 NetScaler Gateway 数量的计数器。

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，请确保满足安装 StoreFront 的所有要求。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，然后将此文件复制到服务器上的临时位置。
4. 从命令提示窗口中导航到安装文件所在的文件夹，然后键入以下命令。

   CitrixStoreFront-x64.exe [-silent] [-INSTALLDIR installationlocation]
   [-WINDOWS_CLIENT filelocation\filename.exe]
   [-MAC_CLIENT filelocation\filename.dmg]

   使用 -silent 参数可对 StoreFront 以及所有必备项执行无提示安装。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。请注意，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 Receiver，系统将提示用户从 Citrix Web 站点下载和安装适合其平台的 Citrix Receiver。您可以修改此行为，以使用户从 StoreFront 服务器下载 Citrix Receiver 安装文件。有关详细信息，请参阅在服务器上提供 Citrix Receiver 安装文件。

   如果要更改此配置，请指定 -WINDOWS_CLIENT 和 -MAC_CLIENT 参数，以将 Citrix Receiver for Windows 和 Citrix Receiver for Mac 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 Citrix Receiver 安装文件的名称。Citrix Receiver for Windows 和 Citrix Receiver for Mac 安装文件位于 StoreFront 安装介质或下载软件包中。

要将现有 StoreFront 3.x 部署升级到此版本的 StoreFront，请运行此版本的 StoreFront 的安装文件。

一旦启动升级过程后，则无法将其回滚。如果升级过程中断或无法完成，则现有配置会被删除，但不会安装 StoreFront。在开始升级之前，您必须断开用户与 StoreFront 部署的连接，并且在升级过程中，还必须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。如果存在安装程序无法访问的文件，那么将无法替换这些文件，因此升级会失败，从而导致现有 StoreFront 配置被删除。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，必须将组中的所有服务器更新到已升级的版本。多服务器部署不支持同时升级，必须按顺序升级服务器。Citrix 建议您在升级之前对数据进行备份。

卸载 StoreFront 将删除身份验证服务、应用商店、用户的应用程序订阅、Citrix Receiver for Web 站点、桌面设备站点和 XenApp Services URL。这意味着如果您决定卸载 StoreFront，那么在重新安装 StoreFront 时，您必须重新创建服务、应用商店和站点。升级还使您能够保留 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。

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。

Important

开始升级之前，请执行以下操作：

- 关闭 StoreFront 服务器上的所有其他应用程序。
- 关闭所有命令行和 PowerShell 窗口。

将现有 StoreFront 3.x 升级到此版本的 StoreFront

1. 禁用通过负载平衡环境对部署的访问。禁用负载平衡的 URL 将阻止用户在升级过程中连接到部署。
2. 备份服务器组中的所有服务器。
3. 从现有服务器组中删除其中一台服务器。
4. 重新启动删除的服务器。
   请注意，可以使用局部负载平衡器在构建新服务器组的过程中对其进行检查。将可用性最大化并进一步将风险降至最低的变体涉及仅删除并升级原始服务器组中的一台服务器。然后可以基于新计算机（而非从原始服务器组中删除的计算机）构建新组。
5. 使用管理员帐户升级删除的服务器，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。
6. 检查是否已成功升级删除的服务器。
7. 从负载平衡器中删除现有服务器组中的另外一台服务器。
8. 重新启动删除的服务器，原因与步骤 1 中指出的原因相同。
9. 卸载当前安装的 StoreFront 版本并安装新版本的 StoreFront。
10. 将新安装的服务器添加到由所有升级后的服务器和全新安装的服务器组成的新服务器组，并检查其是否能够正常运行。
11. 重复步骤 3-10，直至新服务器组有足够的容量，能够接管旧服务器组的角色，将负载平衡器指向新服务器组，然后检查其是否能够正常运行。
12. 对剩余的服务器重复步骤 3-10，在每次成功升级后将每台服务器都添加到负载平衡器中。

注意

- 如果要将可用性最大化，可以在升级过程中保持对原始服务器组的访问权限，直至新服务器组可用。为此，请执行以下操作：
  1. 跳过步骤 1。
  2. 修改步骤 11，使其包括禁用使用负载平衡器访问原始服务器组的功能。从原始服务器组中导出订阅数据并将其导入到新服务器组中。启用使用负载平衡器访问新服务器组的功能。

     这样可确保用户在完成步骤 3 之后执行步骤 11 之前对订阅所做的所有更改都在新服务器组中可用。
- 可以通过以下方式进一步将可用性最大化：仅从原始服务器组中删除一台服务器并进行升级，然后使用新服务器（而非从原始服务器组中删除的服务器）构建新服务器组。新服务器组投入生产时，可以停用旧服务器。
- 在与应用商店的默认 IIS 目录**不同的**位置保存 web.config 文件的备份。请勿在（例如）C:\inetpub\wwwroot\citrix\ 中保存备份。在与应用商店的默认 IIS 目录相同的位置保存备份会干扰 StoreFront 的升级。

Citrix StoreFront 管理控制台首次启动时，会提供两个选项。

- 创建新部署。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。要添加新服务器，需要访问部署中的现有服务器。

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、桌面设备站点和 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，这意味着用户应用程序订阅的详细信息将丢失。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. 在 Windows **开始**屏幕或“应用程序”屏幕中，找到 **Citrix StoreFront** 磁贴。在该磁贴上单击鼠标右键，然后单击**卸载**。
3. 在**程序和功能**对话框中，选择 **Citrix StoreFront**，然后单击**卸载**从服务器中删除所有 StoreFront 组件。
4. 在**卸载 Citrix StoreFront** 对话框中，单击**是**。卸载完成后，单击**确定**。

创建新部署

Jun 04, 2018

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。

   可以通过在 StoreFront 管理控制台中执行更改基本 URL 任务随时从 HTTP 更改为 HTTPS，前提是为 HTTPS 配置了 Microsoft Internet Information Services (IIS)。

4. 单击下一步以设置身份验证服务，该服务可对要访问 Microsoft Active Directory 的用户进行身份验证。
   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 Receiver 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。

   可以通过在 StoreFront 管理控制台中执行**更改基本 URL** 任务随时从 HTTP 更改为 HTTPS，前提是为 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 Receiver 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 Controller 页面上，列出用于提供希望通过应用商店获得的资源的基础结构。要向应用商店中添加桌面和应用程序，请执行以下相应步骤。可以将应用商店配置为提供任何 XenDesktop 和 XenApp 部署组合中的资源。根据需要重复此过程，以添加为应用商店提供资源的所有部署。
   - 向应用商店添加 XenDesktop 和 XenApp 资源
7. 将所有必需的资源添加到应用商店之后，请在 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能够以及如何访问内部资源。
   - 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。
   - 要使该应用商店所提供的资源只能通过 NetScaler Gateway 访问，请选择**允许用户仅访问通过 StoreFront 交付的资源(无 VPN 通道)**。
   - 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)**。用户可能需要使用 NetScaler Gateway 插件建立 VPN 通道。

   如果配置通过 NetScaler Gateway 对应用商店进行远程访问，将自动启用 NetScaler Gateway 直通身份验证方法。用户向 NetScaler 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，请列出用户用于访问应用商店的 NetScaler Gateway 部署。要添加 NetScaler Gateway 部署，请执行以下相应过程。根据需要重复此过程，以添加更多的部署。
   - 通过 NetScaler Gateway 设备提供对应用商店的远程访问
10. 添加完所有 NetScaler Gateway 部署之后，请从 NetScaler Gateway 设备列表中选择用户用于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部署。单击**下一步**。

11. 在**身份验证方法**页面上，选择用户向应用商店验证身份时使用的方法，然后单击**下一步**。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，即可在访问自己的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，即可在访问自己的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 基本认证**：用户将向 StoreFront 服务器的 IIS Web 服务器进行身份验证。
- **直通 NetScaler Gateway**：用户向 NetScaler Gateway 验证身份后，即可在访问自己的应用商店时自动登录。启用了远程访问时自动选中此方法。

12. 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。

13. 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，请参阅各种管理文章。

现在，用户可以使用 Citrix Receiver 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 的形式为 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 为在步骤 5 中为应用商店指定的名称。

安装 StoreFront 的更多实例时，可以通过选择加入现有服务器组选项快速将更多服务器添加到部署中。

要通过在 StoreFront 服务器的初始配置中创建的应用商店获得由 XenDesktop 和 XenApp 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 StoreFront 控制台“创建应用商店用户界面”的 Controller 页面上，单击添加。
2. 在添加 Controller 对话框中，指定一个有助于识别部署的名称，并指示希望通过应用商店获得的资源是由 XenDesktop、XenApp 还是 XenMobile 提供。
3. 将服务器的名称或 IP 地址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 XenDesktop 站点，提供 Controller 的详细信息。对于 XenApp 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 XenDesktop 和 XenApp 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 服务器之间的安全连接发送数据，以使用 SSL Relay 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 XenDesktop 和 XenApp 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 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。

可以将应用商店配置为提供任何 XenDesktop、XenApp 和 XenMobile 部署组合中的资源。要添加更多 XenDesktop 站点或 XenApp 场，请重复执行上述过程。 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。

要配置通过 NetScaler 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“创建应用商店用户界面”的远程访问页面上，单击添加。
2. 在添加 NetScaler Gateway 设备对话框中，为设备指定便于用户识别的名称。
   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设备。例如，可以在 NetScaler 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。

3. 为设备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。
   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. 如果要添加 Access Gateway 5.0 设备，请从部署模式列表中选择设备。否则，请指定 NetScaler Gateway 设备的子网 IP 地址（如果需要）。
   子网地址是指 NetScaler 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 NetScaler 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。

5. 如果要添加运行 NetScaler Gateway 的设备，请从登录类型列表中选择之前在设备上为 Citrix Receiver 用户配置的身份验证方法。
   您所提供的有关 NetScaler Gateway 设备配置的信息将添加到应用商店的置备文件中。这使 Citrix Receiver 可以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。

6. 在回调 URL 框中填写 NetScaler 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。
   输入设备的内部可访问的 URL。StoreFront 连接 NetScaler Gateway 身份验证服务，以验证从 NetScaler Gateway 收到的请求是否来自该设备。

7. 如果要通过应用商店获得由 XenDesktop 或 XenApp 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 托管于 XenDesktop 和 XenApp 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 XenDesktop 和 XenApp 资源进行身份验证和授权的基础。

8. 如果希望 XenDesktop 和 XenApp 在 Citrix Receiver 尝试自动重新连接期间将断开的会话保持在打开状态，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 Request tickets from two STAs, where available（从两个 STA 请求票据(如果可用)）复选框。
选中 Request tickets from two STAs, where available（从两个 STA 请求票据(如果可用)）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。

9. 单击创建，将 NetScaler Gateway 部署添加到远程访问页面上的列表中。

要添加更多的部署，请重复执行上述过程。要配置通过 Access Gateway 5.0 群集远程访问应用商店，请执行通过 Access Gateway 5.0 群集提供对应用商店的远程访问中所述的步骤。添加所有 NetScaler Gateway 部署后，返回到本文顶部“创建新部署”过程中的第 10 步。

要配置通过 Access Gateway 5.0 群集提供对 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“创建应用商店用户界面”的远程访问页面上，单击添加。
2. 在添加 NetScaler Gateway 设备对话框中，为群集指定便于用户识别的名称。
   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群集。例如，可以在 NetScaler 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。

3. 输入群集的用户登录点 URL，并从版本列表中选择 5.x。
4. 从部署模式列表中，选择 Access Controller，然后单击下一步。
5. 在设备页面中，列出群集中设备的 IP 地址或完全限定的域名 (FQDN)，然后单击下一步。
6. 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。

7. 如果要通过应用商店获得由 XenDesktop 和 XenApp 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 托管于 XenDesktop 和 XenApp 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 XenDesktop 和 XenApp 资源进行身份验证和授权的基础。

8. 如果希望 XenDesktop 和 XenApp 在 Citrix Receiver 尝试自动重新连接期间将断开的会话保持在打开状态，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 Request tickets from two STAs, where available（从两个 STA 请求票据(如果可用)）复选框。
   选中 Request tickets from two STAs, where available（从两个 STA 请求票据(如果可用)）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。

9. 单击创建，将 NetScaler Gateway 部署添加到远程访问页面上的列表中。

要添加更多群集，请重复执行上述步骤。要配置通过 NetScaler Gateway 或单个 Access Gateway 5.0 设备远程访问应用商店，请执行通过 NetScaler Gateway 设备提供对应用商店的远程访问中的步骤。添加所有 NetScaler Gateway 部署后，返回到本文顶部“创建新部署”过程中的第 10 步。

加入现有服务器组

Nov 27, 2017

安装 StoreFront 前，请确保添加到组中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。尽管服务器组最多可以包含五台服务器，但是从基于模拟的容量预测来看，包含三台以上服务器的服务器组不具有优势。此外，还应确保 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。

> **Important**
>
> 向服务器组中添加新服务器时，添加的 StoreFront Service 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. 登录到要加入的 StoreFront 部署中的服务器，并打开 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，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。

如果 StoreFront 服务器是某个服务器组的成员，并且已被删除，您必须运行 Clear-DSConfiguration PowerShell cmdlet 将 StoreFront 服务器重置为出厂默认状态。 在断开连接的服务器上运行 Clear-DSConfiguration cmdlet 后，可以将该服务器重新添加到现有服务器组或其他新创建的服务器组。

1. 在用于管理整个服务器组的主 StoreFront 服务器上打开 StoreFront 管理控制台。
2. 选择左侧的 服务器组节点，然后选择其他要删除的服务器。
3. 从服务器组中删除 选定的服务器。
4. 在“操作” 窗格中，传播来自您使用的服务器的更改以断开 服务器组的其中一个成员。 任何 其他剩余的服务器组成员现在意识到服务器 已从组中删除。在您将断开连接的服务器重置为出厂 默认状态后，则无法识别该服务器不再是组的成员。
5. 在断开连接的 服务器上关闭管理控制台。
6. 将断开连接的 服务器从组中删除后在该服务器上打开一个 PowerShell 会话，并使用以下命令导入 StoreFront PowerShell 模块： `& "$Env:PROGRAMFILES\Citrix\ReceiverStoreFront\Scripts\ImportModules.ps1"`
7. 运行 Clear-DSConfiguration 命令，此命令会将 服务器重置为默认设置。
8. 打开 StoreFront 管理控制台，此时断开连接的服务器已重置， 可随时将其添加到其他服务器组。

将 Web Interface 功能迁移至 StoreFront

Nov 27, 2017

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。

- 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	
• 低图形布局 • 全图形布局 • 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。
	• 禁用。要在桌面/Web UI 中隐藏搜索框，请向 style.css 中添加以下样式：
	.search-container {
	display: none;
	}
	要在手机 UI 中隐藏搜索框，请添加：
	#searchBtnPhone {

	display: none; }
启用刷新	默认启用（浏览器刷新）。

启用返回上一个文件夹	默认情况下不启用。
	启用返回上一个文件夹 - 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 ()
	{
	// 检查上次是否保存了视图
	CTXS.ExtensionAPI.localStorageGetItem("view",
	function (view) {
	if (view) {
	// 如果保存了视图，则更改为此视图
	CTXS.ExtensionAPI.changeView(view);
	}
	if (view == "store") {
	// 如果视图是应用商店，则查看是否保存了文件夹
	CTXS.ExtensionAPI.localStorageGetItem("folder",
	function(folder) {
	if (folder != "") {
	// 如果保存了文件夹，则更改为此文件夹
	CTXS.ExtensionAPI.navigateToFolder(folder);
	}
	}
	);
	}
	// 设置文件夹监视
	CTXS.Extensions.onFolderChange = function(folder) {

	CTXS.ExtensionAPI.localStorageSetItem("folder",
	folder);
	};
	// 设置视图监视
	CTXS.Extensions.onViewChange = function(newview) {
	// 不保留搜索或应用程序信息视图
	// 而是记住父视图。
	if ((newview != "appinfo") &&
	(newview != "search")) {
	CTXS.ExtensionAPI.localStorageSetItem(
	"view", newview);
	}
	};
	});
	};

启用提示	由于 Citrix Receiver 面向触摸和非触摸设备，因此很少使用工具提示。您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 • 设置默认视图 • （低图形）图标视图 • （低图形）列表视图 （低图形）默认视图	Citrix Receiver 具有不同的 UI，因此这些选择不适用。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。
• 单选项卡 UI • 选项卡式 UI • “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 Receiver 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
• 标题背景颜色
• 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');
	
	}

• 预登录欢迎消息（预先区域设置）
  • 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;
	
	// Web 登录之前
	
	CTXS.Extensions.beforeLogon = function (callback) {
	
	doneClickThrough = true;
	
	CTXS.ExtensionAPI.showMessage({
	
	messageTitle: "Welcome!",
	
	messageText: "Only for WWCo Employees",
	
	okButtonText: "Accept",
	
	okAction: callback
	
	});
	
	};
	
	// 主屏幕之前（用于本机客户端）
	
	CTXS.Extensions.beforeDisplayHomeScreen
	
	= function (callback) {
	
	if (!doneClickThrough) {
	
	CTXS.ExtensionAPI.showMessage({
	
	messageTitle: "Welcome!",
	
	messageText: "Only for WWCo Employees",
	
	okButtonText: "Accept",
	
	okAction: callback

	});
	} else {
	callback();
	}
	};

• 登录屏幕标题
• 登录屏幕消息
• 登录屏幕系统消息
	登录屏幕上有四处用于自定义的区域。屏幕的顶部和底部（标题和页脚），以及登录框的顶部和底部。
	.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，因为在这里进行的更改会强制所有客户端重新加载 UI。请将动态内容放在 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;
	}
	使用脚本的静态内容示例：
	$('#customBottom').html("Welcome to ACME");

没有直接等效设置的功能	
• 不含标题的登录屏幕 • 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。
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 文件生成挂接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，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

Nov 27, 2017

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。

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。

可以通过执行 删除 服务器任务将服务器从多服务器 StoreFront 部署中 删除。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。

可以通过执行 传播更改任务更新多服务器 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。 系统将放弃在组内其他服务器上执行的所有更改。 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：如果更新某台服务器的配置却未将所做的更改传播到组中的其他服务器，当之后从部署中的另一台服务器传播更改时，这些更新可能会丢失。

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 Service 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，只要 Microsoft Internet Information Services (IIS) 配置为支持 HTTPS 即可。

要将 IIS 配置为支持 HTTPS，请使用 StoreFront 服务器上的 Internet Information Services (IIS) 管理器控制台，创建由 Microsoft Active Directory 域证书颁发机构签名的服务器证书。 然后，将 HTTPS 绑定添加到默认 Web 站点。 有关在 IIS 中创建服务器证书的详细信息，请参阅 http://technet.microsoft.com/zh-cn/library/hh831637.aspx#CreateCertificate。 有关将 HTTPS 绑定添加到 IIS 站点的详细信息，请参阅 http://technet.microsoft.com/zh-cn/library/hh831632.aspx#SSLBinding。

为了提高某些资源提供服务器不可用时的性能，StoreFront 会临时跳过无法响应的服务器。跳过某台服务器时，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**指定减少的持续时间（以分钟为单位），如果某个特定 Delivery Controller 的所有服务器都被跳过，StoreFront 将使用该参数而非**跳过持续时间**。默认值为 0 分钟。
- **跳过持续时间**指定 StoreFront 尝试与单台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。为应用商店配置多个 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。

为**所有失败跳过的持续时间**设置的值越小，此 Delivery Controller 所提供的资源的可用性越高；但是，如果为应用商店配置了多个 Delivery Controller，并且其中一些不可用，客户端超时可能会增加。配置的场不多并且用于业务关键型 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，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**操作**窗格中单击**管理 Delivery Controller**。
3. 选择一个 Controller，单击**编辑**，然后在**编辑 Delivery Controller** 屏幕上单击**设置**。
4. 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）。
5. 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

Nov 27, 2017

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。

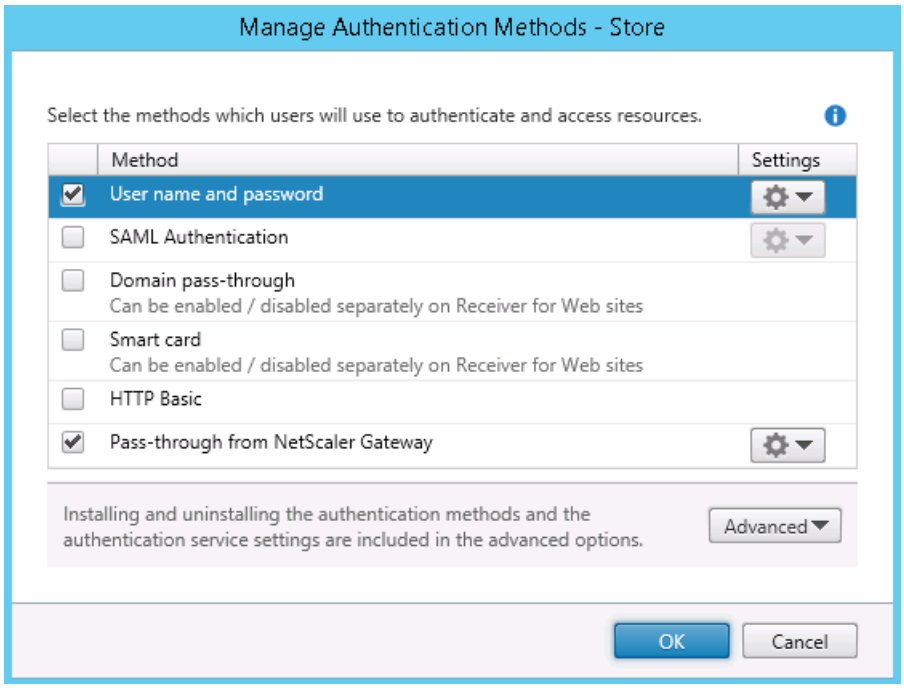
配置身份验证服务	身份验证服务可对用户进行身份验证，使其能够访问 Microsoft Active Directory，从而确保用户无需重新登录即可访问自己的桌面和应用程序。
基于 XML Service 的身份验证	如果 StoreFront 与 XenApp 或 XenDesktop 位于不同的域，并且无法设置 Active Directory 信任，则可以将 StoreFront 配置为使用 XenApp 和 XenDesktop XML Service 来验证用户名和密码凭据。
适用于 XenApp 6.5 的 Kerberos 受限委派	可以通过执行配置 Kerberos 委派任务指定 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

Nov 27, 2017

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**以对身份提供程序配置信任。
  - 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。
- 选中域直通复选框可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 时，必须启用直通身份验证。
- 选中智能卡复选框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 基本认证复选框可启用 HTTP 基本身份验证。用户将向 StoreFront 服务器的 IIS Web 服务器进行身份验证。
- 选中 NetScaler Gateway 直通复选框，以启用 NetScaler Gateway 直通身份验证。用户向 NetScaler 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 NetScaler 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 NetScaler 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(显式) > 设置**下拉菜单中，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。选择列表中的某个域并单击删除，可禁止该域中的用户帐户对应用商店进行访问。
   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桌面 Receiver 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 Receiver 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。

1. Citrix Receiver for Web 支持过期时更改密码以及选择性更改密码。所有桌面 Citrix Receiver 仅支持在过期时通过 NetScaler Gateway 修改密码。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**下拉菜单中，选择**管理密码选项**，指定在哪些情况下允许使用域凭据登录的 Citrix Receiver for Web 站点用户更改其密码。
   - 要允许用户随时更改其密码，请选择随时。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，向用户发出通知的时间段由相应的 Windows 策略设置决定。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。
   - 要允许用户只能在密码已经过期的情况下更改其密码，请选择到期时。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。支持桌面版 Citrix Receiver 和 Citrix Receiver for Web。
   - 要阻止用户更改其密码，请勿选择**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。

   如果允许 Citrix Receiver for Web 站点用户随时更改密码，请确保 StoreFront 服务器上有足够的磁盘空间，用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 Receiver	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

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对 StoreFront 进行身份验证时才能使用自助服务密码重置。

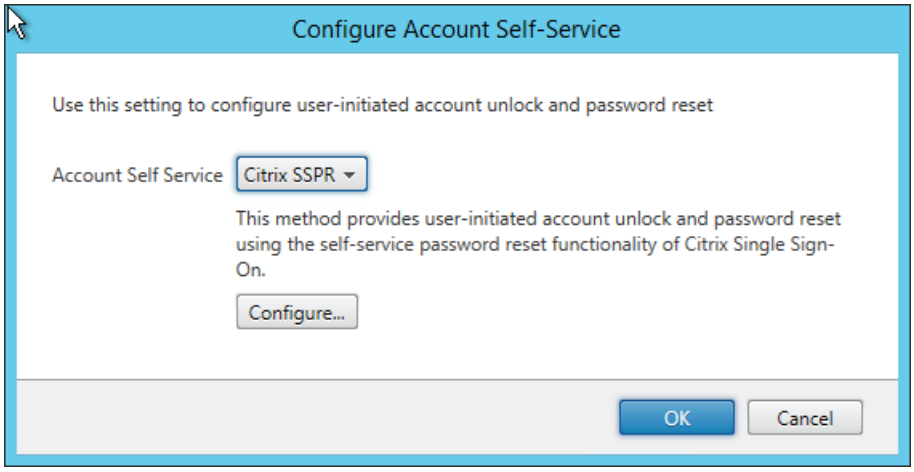
自助服务密码重置不支持 UPN 登录，例如 username@domain.com。

在为应用商店配置自助服务密码重置之前，必须确保：

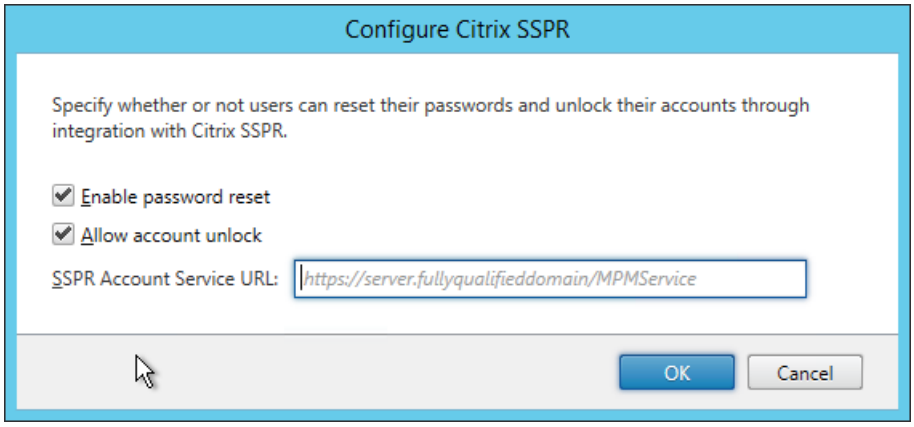
- 应用商店配置为使用用户名和密码身份验证。
- 应用商店配置为仅使用一个自助服务密码重置。如果 StoreFront 配置为使用同一域或可信域中的多个场，则必须将自助服务密码重置配置为接受来自所有这些域的凭据。
- 应用商店配置为允许用户在希望启用密码重置功能时随时更改其密码。
- 必须将 StoreFront 应用商店与 Receiver for Web 站点相关联，并且必须将该站点配置为使用统一体验。

必须先安装并配置自助服务密码重置才能进行使用。自助服务密码重置在 XenApp 和 XenDesktop 介质中提供。有关信息，请参阅自助服务密码重置文档。

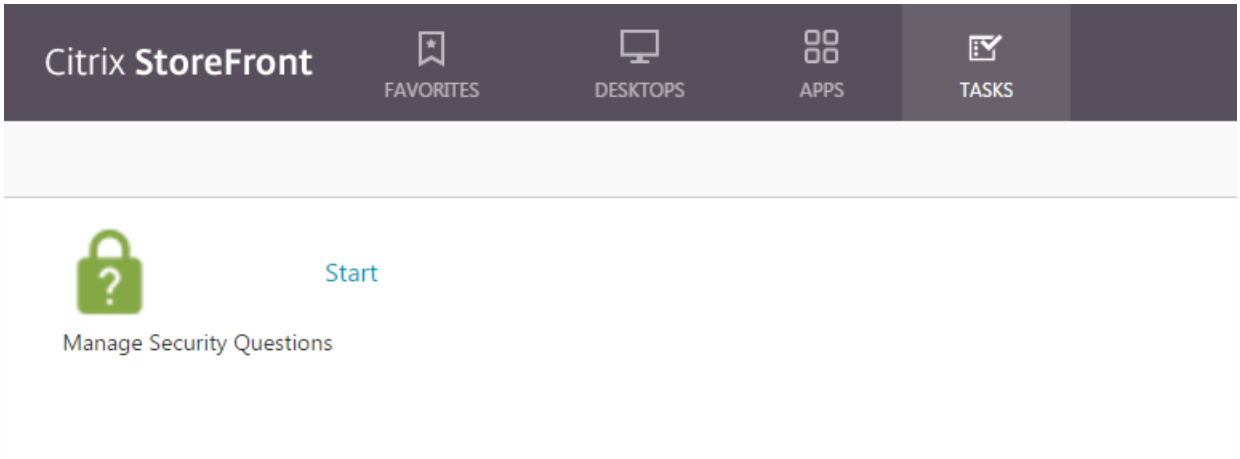
1. 通过在 Citrix StoreFront 管理控制台的左侧窗格中选择**应用商店**节点，在**操作**窗格中单击**管理身份验证方法 > 用户名和密码**，然后从下拉菜单中选择**管理密码选项**，在 StoreFront 中启用自助服务密码重置支持。
2. 选择希望用户更改密码的时间，然后单击**确定**。
3. 从**用户名和密码**下拉菜单中选择**配置帐户自助服务**，从下拉菜单中选择 **Citrix SSPR**，然后单击**确定**。
4. 指定用户是否能够通过自助服务密码重置来重置密码和解锁帐户，添加密码重置服务帐户 URL，单击**确定**，然后单击**确定**。



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。



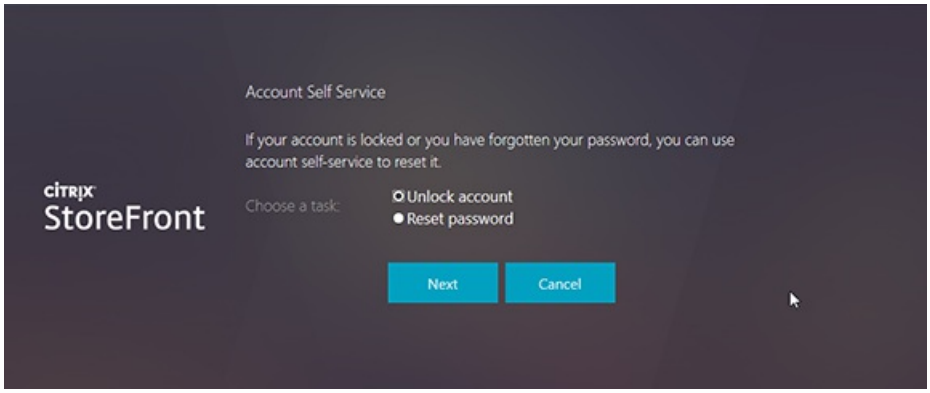
用户下次登录 Citrix Receiver 或 Citrix Receiver for Web 时，安全注册将可用。单击**启动**后，将显示用户必须指定回答的问题。



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 Receiver 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 NetScaler Gateway

可以通过执行 配置委派身份验证任务为通过 NetScaler 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 NetScaler Gateway 直通时，才能执行 此项任务。

如果 将凭据验证委派给 NetScaler Gateway ，则用户使用智能卡向 NetScaler 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 NetScaler 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 NetScaler Gateway 时才会进行直通 身份验证。

基于 XML Service 的身份验证

Nov 27, 2017

如果 StoreFront 与 XenApp 或 XenDesktop 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 XenApp 和 XenDesktop XML Service 来验证用户名和密码凭据。

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）下拉菜单中，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）。

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）下拉菜单中，选择 **Active Directory**，然后单击 **OK**（确定）。

为 XenApp 6.5 配置 Kerberos 受限委派

Nov 27, 2017

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 受限委派向 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 受限委派。

StoreFront 未与 XenApp 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 Delegation（委派）选项卡上，单击 Trust this computer for delegation to specified services only（仅信任此计算机来委派指定的服务）和 Use any authentication protocol（使用任意身份验证协议），然后单击 添加。
6. 在 Add Services（添加服务）对话框中，单击 Users or Computers（用户或计算机）。
7. 在 Select Users or Computers（选择用户或计算机）对话框中的 Enter the object names to select （输入要选择的对象名称）框中，键入运行 Citrix XML Service (XenApp) 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。

为每个 XenApp 服务器配置 Active Directory 受信委派。

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，单击域名下的**计算机**节点，然后选择运行 StoreFront 被配置为与之通信的 Citrix XML Service (XenApp) 的服务器。
3. 在**操作**窗格中，单击**属性**。
4. 在 **Delegation**（委派）选项卡上，单击 **Trust this computer for delegation to specified services only**（仅信任此计算机来委派指定的服务）和 **Use any authentication protocol**（使用任意身份验证协议），然后单击**添加**。
5. 在 **Add Services**（添加服务）对话框中，单击 **Users or Computers**（用户或计算机）。
6. 在 **Select Users or Computers**（选择用户或计算机）对话框中的 **Enter the object names to select**（输入要选择的对象名称）框中，键入运行 Citrix XML Service (XenApp) 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**输入对象名称来选择**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 受限委派时，请考虑以下信息。

- 要点：
  - 除非在无 Kerberos 受限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。在关于受信区域的 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 PIN 提示智能卡身份验证：
  - 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。
- NetScaler Gateway、StoreFront、Citrix Receiver for Web 和 PIN 提示智能卡身份验证：
  - 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 NetScaler 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 NetScaler Gateway 的智能卡身份验证和其他 vServer 的启动，以通过未经身份验证的 NetScaler Gateway vServer 路由 ICA 通信。
- Citrix Receiver for Windows (AuthManager)、提示输入 PIN 码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 (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。
  - 在关于受信区域的 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：

    警告：注册表编辑不当会导致严重问题，可能导致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\integratedwindows

    名称：SSONCheckEnabled

类型：REG_SZ
值：true 或 false

配置智能卡身份验证

Jun 04, 2018

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。

PDF

Citrix 环境的智能卡配置

This overview for configuring a Citrix deployment for smart cards uses a specific smart card type. Note that similar steps apply to smart cards from other vendors.

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 XenDesktop 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 NetScaler Gateway

- 在 NetScaler 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，请参阅安装并管理证书。
- 在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 NetScaler 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 NetScaler 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 NetScaler 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 NetScaler 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 NetScaler 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 http://technet.microsoft.com/zh-cn/library/hh831637.aspx#CreateCertificate。有关将 HTTPS 绑定添加到 IIS 站点的详细信息，请参阅 http://technet.microsoft.com/zh-cn/library/hh831632.aspx#SSLBinding。

- 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。使用此配置时，智能卡用户才能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 NetScaler 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 NetScaler 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 NetScaler Gateway 访问应用商店的智能卡用户，启用 NetScaler Gateway 直通身份验证方法，并确保 StoreFront 配置为将凭据验证委派给 NetScaler Gateway。如果在加入域的用户设备上安装 Citrix Receiver for Windows 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 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。有关详细信息，请参阅为 Citrix Receiver for Windows 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 NetScaler 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 NetScaler Gateway 路由。有关详细信息，请参阅为应用商店配置最佳 HDX 路由。
- 要允许未加入域的 Windows 桌面设备的用户使用智能卡登录到桌面，请启用桌面设备站点的智能卡身份验证。有关详细信息，请参阅配置桌面设备站点。

  为桌面设备站点配置智能卡和显式身份验证两种方法，可以使用户在智能卡出现问题时使用显式凭据进行登录。

- 对于使用运行 Citrix Desktop Lock 的已加入域的桌面设备和重用 PC 的用户，如果要允许其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。
- 如果用户使用未加入域的 Windows 桌面设备，应使用具有管理员权限的帐户安装 Receiver for Windows Enterprise。将 Internet Explorer 配置为在全屏模式下启动，并在设备开机时显示桌面设备站点。请注意，桌面设备站点 URL 区分大小写。将桌面设备站点添加到 Internet Explorer 的“本地 Intranet”或“可信站点”区域。在确认可以通过智能卡登录到桌面设备站点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。
- 如果用户使用加入域的桌面设备和重用 PC，应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 Receiver。要为具有已加入域的设备的用户启用 XenDesktop 和 XenApp 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 Receiver for Windows。有关详细信息，请参阅使用命令行参数配置和安装 Receiver for Windows。
  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 Receiver for Windows。配置域策略时，使用组策略管理控制台为用户帐户所属的域将 Receiver for Windows 组策略对象模板文件 icaclient.adm 导入域控制器中。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，请参阅使用组策略对象模板配置 Receiver。

  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 XenDesktop 和 XenApp，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 XenDesktop 和 XenApp，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 NetScaler 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 Citrix Receiver。

为 Receiver for Windows 启用使用智能卡的 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 XenDesktop 和 XenApp 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，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. 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 是创建应用商店时为其指定的名称。
2. 要为不通过 NetScaler Gateway 访问应用商店的用户启用智能卡凭据直通功能，请在 [Application] 部分添加以下设置。
   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 NetScaler Gateway 访问应用商店的用户启用智能卡凭据直通功能，请在 [Application] 部分添加以下设置。
   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

Nov 27, 2017

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。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间段，可以编辑身份验证服务的配置文件。

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，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“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，在**用户名和密码** > **设置**下拉菜单中选择**管理密码选项**，然后选中**允许用户更改密码**复选框。
4. 选择**随时...** 并在**密码过期之前提醒用户**下进行选择。

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

Nov 27, 2017

在 Citrix StoreFront 中，可以创建和管理用于将 XenApp 和 XenDesktop 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。

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置备文件	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 NetScaler Gateway 部署和信标点。
向用户隐藏和公告应用商店	在用户将 Citrix Receiver 配置为使用基于电子邮件的帐户发现或 FQDN 时阻止将应用商店呈现给用户以添加到其帐户中。
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 NetScaler 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 NetScaler Gateway 对应用商店的访问。
将 Citrix Online 应用程序与应用商店集成	选择要包含在应用商店中的 Citrix Online 应用程序，并指定用户订阅 Citrix Online 应用程序时 Citrix Receiver 执行的操作。
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

Jun 04, 2018

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。您也可以创建一个未经身份验证的应用商店，允许匿名访问或未经身份验证的访问。要创建此类型的应用商店，请参阅创建未经身份验证的应用商店说明。

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 NetScaler Gateway 对该应用商店进行远程访问（可选）。

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。

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 Receiver 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，并指示希望通过应用商店获得的资源是由 XenDesktop、XenApp 还是 AppController 提供。对于 App Controller 部署，请确保所指定的名称中不包含任何空格。
6. 如果要添加 XenDesktop 或 XenApp 服务器的详细信息，请继续执行步骤 7。要通过应用商店获得由 App Controller 管理的应用程序，请在服务器框中输入 App Controller 虚拟设备的名称或 IP 地址，并指定 StoreFront 连接 App Controller 所用的端口。默认端口为 443。继续执行步骤 11。
7. 要通过应用商店获得由 XenDesktop 或 XenApp 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 XenDesktop 站点，提供 Delivery Controller 的详细信息。对于 XenApp 场，列出运行 Citrix XML Service 的服务器。
8. 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 XenDesktop 和 XenApp 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 服务器之间的安全连接发送数据，以使用 SSL Relay 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）。
9. 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 XenDesktop 和 XenApp 服务器，指定的端口必须是 Citrix XML Service 所使用的端口。
10. 如果要使用 SSL Relay 确保 StoreFront 与 XenApp 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。
11. 单击确定。可以将应用商店配置为提供任何 XenDesktop、XenApp 和 App Controller 部署组合中的资源。根据需要重复步骤 4 至 11，以列出为该应用商店提供资源的更多部署。将所有必需的资源添加到该应用商店中之后，单击下一步。
12. 在远程访问页面上，指定从公用网络连接的用户是否能够以及如何通过 NetScaler Gateway 访问该应用商店。
    - 要将应用商店设置为对公用网络中的用户不可用，请务必不要选中**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**。
  - 要使该应用商店所提供的资源只能通过 NetScaler Gateway 访问，请选择无 VPN 通道。用户可以直接登录到 NetScaler Gateway，无需使用 NetScaler Gateway 插件。
  - 要使该应用商店和内部网络中的所有其他资源可通过 SSL 虚拟专用网络 (VPN) 通道访问，请选择完整 VPN 通道。用户需要使用 NetScaler Gateway 插件建立 VPN 通道。

  如果尚未启用 NetScaler Gateway 直通身份验证方法，则在配置对应用商店的远程访问时，将自动启用该方法。用户向 NetScaler Gateway 验证身份后，即可在访问自己的应用商店时自动登录。

13. 如果启用了远程访问，请继续执行下一个过程，以指定用户可用来访问应用商店的 NetScaler Gateway 部署。否则，在远程访问页面上，单击创建。创建完应用商店之后，单击完成。

通过 NetScaler Gateway 提供对应用商店的远程访问

要配置通过 NetScaler 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**页面上，从 **NetScaler Gateway 设备**列表中选择用户可用来访问该应用商店的部署。先前为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 12。
2. 在**添加 NetScaler Gateway 设备常规设置**对话框中，为 NetScaler Gateway 部署指定便于用户识别的名称。
   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 NetScaler 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。

3. 为部署输入虚拟服务器或用户登录点的 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 NetScaler Gateway 虚拟服务器的 FQDN。不支持对 StoreFront 和 NetScaler Gateway 虚拟服务器使用相同的 FQDN。

4. 从可用选项中选择使用 NetScaler Gateway 的选项。
   + **身份验证和 HDX 路由**：NetScaler 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**：NetScaler Gateway 将用于身份验证，不用于任何 HDX 会话路由。
   + **仅限 HDX 路由**：NetScaler Gateway 将用于 HDX 会话路由，不用于身份验证。
5. 在“Secure Ticket Authority (STA)”页面上，如果要通过应用商店获得由 XenDesktop 或 XenApp 提供的资源，请为运行 STA 的服务器列出所有 Secure Ticket Authority 页面 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 托管于 XenDesktop 和 XenApp 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 XenDesktop 和 XenApp 资源进行身份验证和授权的基础。
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. 如果希望 XenDesktop 和 XenApp 在 Citrix Receiver 尝试自动重新连接期间将断开的会话保持在打开状态，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 **Request tickets from two STAs, where available**（从两个 STA 请求票据(如果可用)）复选框。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。
8. 在“身份验证设置”页面上，选择要配置的 NetScaler Gateway 版本。
9. 指定 NetScaler Gateway 设备的 vServer IP 地址（如有需要）。vServer IP 地址是指 NetScaler 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 NetScaler Gateway 设备的映射 IP 地址。如果指定了 vServer IP 地址，则 StoreFront 使用该地址验证传入请求是否来自可信设备。
10. 从“登录类型”列表中选择在设备上为 Citrix Receiver 用户配置的身份验证方法。您所提供的有关 NetScaler Gateway 设备配

置的信息将添加到应用商店的置备文件中。这使 Citrix Receiver 可以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. 在“回调 URL”框中输入 NetScaler Gateway 身份验证服务 URL。此字段为可选字段。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 NetScaler Gateway 身份验证服务，以验证从 NetScaler Gateway 收到的请求是否来自该设备。
12. 单击“创建”，将 NetScaler Gateway 部署添加到“远程访问”页面上的列表中。根据需要重复步骤 1 至 11，将更多 NetScaler Gateway 部署添加到“NetScaler 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部署进行访问，请指定用于访问该应用商店的默认部署。
13. 否则，请在“远程访问”页面上，单击“创建”。创建完应用商店之后，单击“完成”。

现在，用户可以使用 Citrix Receiver 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。

在未加入域的服务器上为单服务器部署创建应用商店

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 Receiver 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，并指示希望通过应用商店获得的资源是由 XenDesktop、XenApp 还是 XenMobile AppController 提供。对于 App Controller 部署，请确保所指定的名称中不包含任何空格。
6. 如果要添加 XenDesktop 或 XenApp 服务器的详细信息，请继续执行步骤 7。要通过应用商店获得由 App Controller 管理的应用程序，请在服务器框中输入 App Controller 虚拟设备的名称或 IP 地址，并指定 StoreFront 连接 App Controller 所用的端口。默认端口为 443。继续执行步骤 11。
7. 要通过应用商店获得由 XenDesktop 或 XenApp 提供的桌面和应用程序，请在**服务器**框中添加服务器的名称或 IP 地址。对于 XenDesktop 站点，提供 Delivery Controller 的详细信息。对于 XenApp 场，列出运行 Citrix XML Service 的服务器。
8. 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 XenDesktop

和 XenApp 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 服务器之间的安全连接发送数据，以使用 SSL Relay 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 来确保 StoreFront 与服务器之间的连接安全，请确保在**服务器**框中指定的名称与这些服务器的证书上的名称完全匹配（包括大小写）。

9. 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 XenDesktop 和 XenApp 服务器，指定的端口必须是 Citrix XML Service 所使用的端口。
10. 如果要使用 SSL Relay 来保护 StoreFront 与 XenApp 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。
11. 单击**确定**。可以将应用商店配置为提供任何 XenDesktop、XenApp 和 App Controller 部署组合中的资源。根据需要重复步骤 4 至 11，以列出为该应用商店提供资源的更多部署。将所有必需的资源添加到该应用商店中之后，单击“下一步”。
12. 在**远程访问**页面上，指定从公用网络连接的用户是否能够以及如何通过 NetScaler Gateway 访问该应用商店。
    - 要禁止公用网络的用户访问应用商店，请选择**无**。这样，只有内部网络的本地用户才能够访问应用商店。
    - 要使该应用商店所提供的资源只能通过 NetScaler Gateway 访问，请选择**无 VPN 通道**。用户可以直接登录到 NetScaler Gateway，无需使用 NetScaler Gateway 插件。
    - 要使该应用商店和内部网络中的所有其他资源可通过 SSL 虚拟专用网络 (VPN) 通道访问，请选择**完整 VPN 通道**。用户需要使用 NetScaler Gateway 插件建立 VPN 通道。

    如果尚未启用 NetScaler Gateway 直通身份验证方法，则在配置对应用商店的远程访问时，将自动启用该方法。用户向 NetScaler Gateway 验证身份后，即可在访问自己的应用商店时自动登录。
13. 如果启用了远程访问，请继续提供通过 NetScaler Gateway 远程访问应用商店功能，以指定用户能够通过哪些 NetScaler Gateway 部署访问应用商店。否则，请在**远程访问**页面上，单击**创建**。
14. 在**配置身份验证方法**页面上，选择用户进行身份验证以及访问资源时使用的方法，然后单击**下一步**。
15. 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**。
16. 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**。

左侧的**服务器组节点**以及**操作**窗格已替换为**更改基本 URL**。唯一可用的选项为更改基本 URL，因为服务器组在未加入域的服务器中不可用。

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、桌面设备站点和 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，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。

创建未经身份验证的应用商店

Nov 27, 2017

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）的用户的访问。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 NetScaler 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，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。

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 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应用商店获得的资源的基础结构。单击添加。
5. 在添加 Controller 对话框中，指定一个有助于识别部署的名称，并指示希望通过应用商店获得的资源是由 XenApp 提供还是由 XenMobile (AppController) 提供。对于 XenMobile (AppController) 部署，请确保所指定的名称中不包含任何空格。分配 Controller 时，请务必仅使用支持匿名应用程序功能的 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。
6. 如果要添加 XenApp 服务器的详细信息，请继续执行步骤 7。要通过应用商店获得由 XenMobile (App Controller) 管理的应用程序，请在服务器框中输入 XenMobile (App Controller) 虚拟设备的名称或 IP 地址，并指定 StoreFront 连接 XenMobile (App Controller) 所用的端口。默认端口为 443。继续执行步骤 10。
7. 要通过应用商店获得由 XenApp 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 XenDesktop 站点，提供 Controller 的详细信息。对于 XenApp 场，列出运行 Citrix XML Service 的服务器。
8. 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 XenDesktop 和 XenApp 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）。
9. 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 XenDesktop 和 XenApp 服务器，指定的端口必须是 Citrix XML Service 所使用的端口。
10. 单击确定。可以将应用商店配置为提供任何 XenDesktop、XenApp 和 App Controller 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 Receiver 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，Receiver for Web 以文件夹层次结构显示应用程序并包括导航控件路径。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 的形式为 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 中为应用商店指定的名称。

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 Citirx Receiver for Web 会话将不会终止。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 XenApp 和 XenDesktop 文档中*配置 Citrix XML Service 端口和信任*中所示。

为用户导出应用商店置备文件

Nov 27, 2017

可通过导出多应用商店置备文件和导出置备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 NetScaler Gateway 部署和信标。将这些文件提供给用户，以使其能够利用应用商店的详细信息自动配置 Citrix Receiver。用户还可以从 Receiver for Web 站点获取 Citrix Receiver 置备文件。

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，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。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置备文件，请在操作窗格中单击导出多应用商店置备文件，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 将置备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

Nov 27, 2017

可以通过执行隐藏应用商店任务在用户将 Citrix Receiver 配置为使用基于电子邮件的帐户发现或 FQDN 时禁止将应用商店呈现给用户以添加到其帐户中。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 Receiver 手动配置（使用设置 URL 或置备文件）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，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**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

Nov 27, 2017

可以通过执行管理 Controller 任务添加和删除 XenDesktop、XenApp 和 App Controller 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，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，单击管理 Delivery Controller。
3. 在管理 Delivery Controller 对话框中，单击添加可将来自其他 XenDesktop、XenApp 或 App Controller 部署的桌面和应用程序加入该应用商店中。要修改部署的设置，请在 Delivery Controller 列表中选择相应条目，然后单击编辑。要停止通过应用商店获得由部署提供的资源，请从列表中选择相应条目，然后单击删除。
4. 在添加 Controller 或编辑 Controller 对话框中，指定一个便于用户识别的部署名称，并指示要通过应用商店获得的资源是由 XenDesktop、XenApp 还是 AppController 提供。对于 App Controller 部署，请确保所指定的名称中不包含任何空格。
5. 如果要添加 XenDesktop 或 XenApp 服务器的详细信息，请继续执行步骤 6。要通过应用商店获得由 App Controller 管理的应用程序，请在服务器框中输入 App Controller 虚拟设备的名称或 IP 地址，并指定 StoreFront 连接 App Controller 所用的端口。默认端口为 443。继续执行步骤 10。
6. 要通过应用商店获得由 XenDesktop 或 XenApp 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 XenDesktop 站点，提供 Delivery Controller 的详细信息。对于 XenApp 场，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相应条目并单击编辑。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。
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 XenDesktop 和 XenApp 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 服务器之间的安全连接发送数据，以使用 SSL Relay 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 XenDesktop 和 XenApp 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 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 XenDesktop、XenApp 和 App Controller 部署组合中的资源。根据需要重复步骤 3 至 10，以在 Delivery Controller 列表中添加或修改其他部署。

管理通过 NetScaler Gateway 对应用商店的远程访问

Jun 04, 2018

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 NetScaler 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 NetScaler 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，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**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 NetScaler Gateway 访问应用商店。
   - 要将应用商店设置为对公用网络中的用户不可用，请务必不要选中**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**。
     - 要使该应用商店所提供的资源只能通过 NetScaler Gateway 访问，请选择无 VPN 通道。用户可以直接登录到 NetScaler Gateway，无需使用 NetScaler Gateway 插件。
     - 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 NetScaler Gateway 插件建立 VPN 通道。

   如果尚未启用 NetScaler Gateway 直通身份验证方法，则在配置对应用商店的远程访问时，将自动启用该方法。用户向 NetScaler 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 NetScaler Gateway 设备列表中选择用户可用于访问该应用商店的部署。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 16。
5. 在 General Settings（常规设置）页面中，为 NetScaler Gateway 部署指定便于用户识别的名称。
   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 NetScaler 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。

6. 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 NetScaler Gateway 虚拟服务器的 FQDN。不支持对 StoreFront 和 NetScaler Gateway 虚拟服务器使用相同的 FQDN。

7. 如果要添加 Access Gateway 5.0 部署，请继续执行步骤 9。否则，请指定 NetScaler 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 NetScaler 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 NetScaler 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。

8. 如果要添加运行 NetScaler Gateway 的设备，请从登录类型列表中选择之前在设备上为 Citrix Receiver 用户配置的身份验证方法。
   您所提供的有关 NetScaler Gateway 设备配置的信息将添加到应用商店的置备文件中。这使 Citrix Receiver 可以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 10。

9. 要添加 Access Gateway 5.0 部署，请指示用户登录点是在独立设备中托管，还是在群集中的 Access Controller 服务器中托管。如果要添加群集，请单击下一步，然后继续执行步骤 11。
10. 如果要针对 NetScaler Gateway 或单个 Access Gateway 5.0 设备配置 StoreFront，请在回调 URL 框中填写 NetScaler 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 13。
    输入设备的内部可访问的 URL。StoreFront 连接 NetScaler Gateway 身份验证服务，以验证从 NetScaler Gateway 收到的请求是否来自该设备。
11. 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。
12. 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。
13. 对于所有部署，如果要通过应用商店获得由 XenDesktop 或 XenApp 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 托管于 XenDesktop 和 XenApp 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 XenDesktop 和 XenApp 资源进行身份验证和授权的基础。
14. 如果希望 XenDesktop 和 XenApp 在 Citrix Receiver 尝试自动重新连接期间将断开的会话保持在打开状态，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 Request tickets from two STAs, where available（从两个 STA 请求票据(如果可用)）复选框。
    选中 Request tickets from two STAs, where available（从两个 STA 请求票据(如果可用)）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。
15. 单击创建，将 NetScaler Gateway 部署添加到远程访问设置对话框的列表中。
16. 根据需要重复步骤 4 至 15，将更多 NetScaler Gateway 部署添加到 NetScaler 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部署进行访问，请指定用于访问该应用商店的默认部署。

将 Citrix Online 应用程序与应用商店集成

Nov 27, 2017

> ## 注意
>
> 自 StoreFront 3.12 起，无法在 StoreFront 管理控制台中配置此功能。如果升级到 StoreFront 3.12，则可以继续使用此功能。要更改您的配置，请使用 PowerShell cmdlet Update-DSGenericApplications。
>
> 有关在早期版本中的 StoreFront 管理控制台中配置此功能的信息，请参阅 StoreFront 3.11 的 Citrix Online 集成一文。

Update-DSGenericApplications

NAME
Update-DSGenericApplications

SYNOPSIS
更新应用商店服务的通用应用程序设置。

语法

Update-DSGenericApplications [[-StoreServiceSiteId]] [[-StoreServiceVirtualPath]] [[-GoToMeetingEnabled]] [[-GoToMeetingDeliveryOption]] [[-GoToWebinarEnabled]] [[-GoToWebinarDeliveryOption]] [[-GoToTrainingEnabled]] [[-GoToTrainingDeliveryOption]] []

说明

用于更新应用商店服务的通用 (Citrix Online) 功能的 cmdlet。

将两个 StoreFront 应用商店配置为共享公用订阅数据存储

Nov 27, 2017

从版本 2.0 开始，StoreFront 不再使用 SQL 数据库来维护其订阅数据。Citrix 使用 Windows 数据存储替换了 SQL 数据库，首次安装 StoreFront 时，无需再额外配置。安装过程会将 Windows 数据存储本地安装在每个 StoreFront 服务器上。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 NetScaler 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。

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 XenApp、 XenDesktop 和 AppC 控制器必须精确匹配； 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 文件并搜索客户端端点。 例如：

   External" authenticationMode="windows" transferMode="Streamed">

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：

   Internal" authenticationMode="windows" transferMode="Streamed">

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。

高级应用商店设置

Nov 27, 2017

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。

地址解析类型

允许应用字体平滑

允许重新连接会话

允许特殊文件夹重定向

后台运行状况检查轮询期限

通信超时期限

连接超时

启用增强枚举

启用套接字池

过滤资源(按排除的关键字)

过滤资源(按包括的关键字)

过滤资源(按类型)

并发枚举数上限

并发枚举的场数量下限

覆盖 ICA 客户端名称

要求令牌一致

服务器通信尝试次数

对旧版客户端显示 Desktop Viewer

> **Important**
>
> 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，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，做出所需的更改，然后单击**确定**。

地址解析类型

可以通过执行**高级设置**任务指定要从服务器请求的地址类型。默认格式为 DnsPort。在**高级设置**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“启用”。

可以通过执行**高级设置**任务选中**允许应用字体平滑**复选框，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“启用”。

可以通过执行**高级设置**任务选中**允许重新连接会话**复选框，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），无论操作系统如何，它们始终以相同方式显示。

可以通过执行**高级设置**任务选中或取消选中**允许特殊文件夹重定向**复选框以启用或禁用特殊文件夹重定向，然后单击**确定**。

后台运行状况检查轮询期限

StoreFront 对每个 XenDesktop Broker 和 XenApp 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

可以启用（或禁用）与 Delivery Controller 的并行通信。默认值为“启用”。

可以通过执行**高级设置**任务选中（或取消选中）**启用增强枚举**复选框，然后单击**确定**。

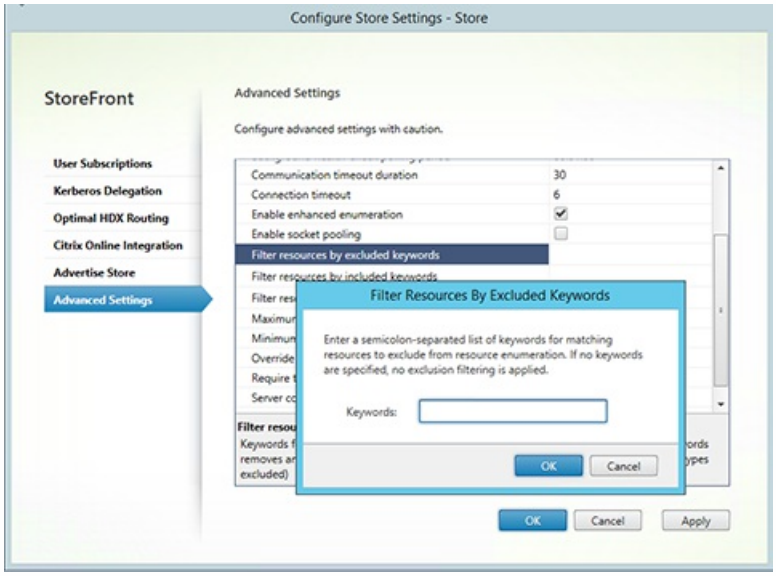
启用套接字后台打印

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。可以通过执行**高级设置**任务选中**启用套接字后台打印**复选框，然后单击**确定**以启用套接字后台打印。

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

指定发送到不同 Delivery Controller 的并发请求数上限。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

指定并行枚举之前 Delivery Controller 的数量下限。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 Receiver 将指定客户端名称。默认值为“关”。

可以通过执行**高级设置**任务选中**覆盖 ICA 客户端名称**复选框，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“启用”。

可以通过执行**高级设置**任务选中**要求令牌一致**复选框，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”。

可以通过执行**高级设置**任务选中**对旧版客户端显示 Desktop Viewer**复选框，然后单击**确定**。

管理 Citrix Receiver for Web 站点

Nov 27, 2017

利用 Citrix Receiver for Web，可以从各种设备安全轻松地访问应用程序、数据和桌面。使用 StoreFront 为 Citrix Receiver for Web 配置 Citrix Receiver for Web 应用程序选择。

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	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。
配置对统一 Citrix Receiver 体验的支持	StoreFront 同时支持经典和统一用户体验。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 Citrix Receiver for HTML5 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 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

Nov 27, 2017

可以通过执行创建 Web 站点任务添加 Receiver for Web 站点，使用户能够通过 Web 页面访问应用商店。

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，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。在“Web 站点路径”框中指定所需的 URL，然后单击**下一步**。
4. 选择 Citrix Receiver 体验并单击**下一步**。
5. 选择一种身份验证方法，单击创建，然后在站点创建完毕后单击完成。
   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 Receiver。如果检测不到 Citrix Receiver，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 Receiver。有关修改此行为的详细信息，请参阅禁用 Citrix Receiver 的检测和部署。

Receiver for Web 站点的默认配置要求用户必须安装兼容版本的 Citrix Receiver，才能访问自己的桌面和应用程序。但是，您可以在 Receiver for Web 站点上启用 Receiver for HTML5，以便无法安装 Citrix Receiver 的用户仍可以访问资源。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

Nov 27, 2017

借助 Citrix Receiver for Web 站点，用户可以通过 Web 页面访问应用商店。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，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。

选择 身份验证方法

可以通过执行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，然后从结果窗格中选择要修改的相关应用商店。
3. 在操作窗格中，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。
   - 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**以对身份提供程序配置信任。
     - 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。
   - 选中域直通复选框可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 时，必须启用直通身份验证。请注意，面向 Citrix Receiver for Web 的域直通身份验证仅对使用 Chrome、Firefox、Internet Explorer 和 Edge 的 Windows 操作系统有效。
   - 选中智能卡复选框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 NetScaler Gateway 直通复选框，以启用 NetScaler Gateway 直通身份验证。用户向 NetScaler 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来允许用户从内部网络上托管的 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。

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，然后从结果窗格中选择站点。
3. 在**操作**窗格中，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的域名，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。

设置会话 超时

默认情况下，Citrix Receiver for Web 站点上的用户会话在处于非活动状态 20 分钟后超时。会话超时后，用户可以继续使用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 站点功能，例如订阅应用程序。

可以通过执行管理 Receiver for Web 站点中的**会话超时**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**窗格中单击**管理 Receiver for Web 站点**和**配置**，然后选择**会话设置**。可以为**会话超时**指定分钟和小时。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。

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**窗格中单击“管理 Receiver for Web 站点”和**配置**，然后选择**会话设置**。
3. 在**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**窗格中单击**管理 Receiver for Web 站点**，然后单击**继续**。
3. 选择**高级设置**，然后选中**启用文件夹视图**。

停止向用户提供置备文件

默认情况下，Citrix Receiver for Web 站点会提供一些置备文件，以支持用户为关联的应用商店自动配置 Citrix Receiver。这些置备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 NetScaler Gateway 部署和信标点的详细信息。

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**窗格中单击**管理 Receiver for Web 站点**和**配置**，然后选择**会话设置**。
3. 选择**启用 Receiver 配置**。

为没有 安装 Citrix Receiver 的用户配置站点行为

可以通过执行**部署 Citrix Receiver** 任务配置当未安装 Citrix Receiver 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 Receiver。

如果检测不到 Citrix Receiver，系统将提示用户下载并安装适用于其平台的 Citrix Receiver。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。

对于无法安装 Citrix Receiver 的用户，可以在 Citrix Receiver for Web 站点上启用 Citrix Receiver for HTML5。Citrix Receiver for HTML5 允许用户直接在与 HTML5 兼容的 Web 浏览器中访问桌面和应用程序，而无需安装 Citrix Receiver。内部网络连接和通过 NetScaler Gateway 进行的连接均受支持。但是，对于从内部网络发起的连接，Citrix Receiver for HTML5 仅支持对特定产品提供的资源进行访问。此外，需要具有特定版本的 NetScaler Gateway 才允许从企业网络以外进行连接。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 Citrix Receiver for HTML5 访问 XenDesktop 和 XenApp 提供的资源。要允许使用 Citrix Receiver for HTML5 本地访问桌面和应用程序，必须在您的 XenDesktop 和 XenApp 服务器上启用“ICA WebSockets 连接”策略。XenDesktop 和 XenApp 对 Citrix Receiver for HTML5 连接使用端口 8008。确保防火墙和其他网络设备允许访问此端口。有关详细信息，请参阅 WebSockets 策略设置。

只能在 HTTP 连接上通过 Internet Explorer 使用 Citrix Receiver for HTML5。要通过 HTTPS 连接对 Mozilla Firefox 使用 Citrix Receiver for HTML5，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**。

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，单击**管理 Receiver for Web 站点**和**配置**。
3. 选择**部署 Citrix Receiver** 并制定在用户设备上检测不到 Citrix Receiver 时 Citrix Receiver for Web 站点的响应。

- 如果希望站点提示用户下载并安装适合其平台的 Citrix Receiver，请选择**本地安装**。用户必须安装 Citrix Receiver 才能通过该站点访问桌面和应用程序。
  - 如果选择 **Allow users to download HDX engine (plug in)**（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下载并安装 Citrix Receiver（如果 Citrix Receiver 不可用）。
  - 如果选择 **Upgrade plug-in at logon**（登录时升级插件），Citrix Receiver for Web 将在用户登录时升级 Citrix Receiver 客户端。要启用此功能，请确保 StoreFront 服务器上存在可用的 Citrix Receiver 文件。
  - 从下拉菜单中选择源。
- 如果希望站点提示用户下载并安装 Citrix Receiver，但在无法安装 Citrix Receiver 时回退到 Citrix Receiver for HTML5，请选择**如果本地 Receiver 不可用，则使用 Receiver for HTML5**。对于未安装 Citrix Receiver 的用户，每当他们登录站点时，都会提示其下载并安装 Citrix Receiver。
- 如果希望站点允许通过 Citrix Receiver for HTML5 访问资源，而不提示用户下载并安装 Citrix Receiver，请选择**始终使用 Receiver for HTML5**。选择该选项后，用户将始终通过 Citrix Receiver for HTML5 访问该站点上的桌面和应用程序，前提是用户使用与 HTML5 兼容的浏览器。未使用 HTML5 兼容浏览器的用户必须在本机安装 Citrix Receiver。

在服务器上提供 Citrix Receiver 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 Receiver。如果检测不到 Citrix Receiver，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 Receiver。

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，单击**管理 Receiver for Web 站点**和**配置**。
3. 选择**部署 Citrix Receiver** 和 **Receiver 的源**，然后浏览到安装文件。

登录后运行安装 Citrix Receiver 的提示

登录 StoreFront 之前，如果尚未在用户的计算机上安装 Citrix Receiver（适用于 Internet Explorer、Firefox 和 Safari 用户），或者用户首次访问站点时（适用于 Chrome 用户），Citrix Receiver for Web 会提示用户安装最新的 Citrix Receiver。如果可以升级 Citrix Receiver 的安装，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，然后从结果窗格中选择站点。
3. 在**操作**窗格中，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**。

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。

支持统一的 Citrix Receiver 体验

Nov 27, 2017

StoreFront 同时支持**经典**和**统一**用户体验。利用经典体验，每个 Citrix Receiver 平台负责提供自己的用户体验。新的统一体验向所有 Web 和本机 Citrix Receiver 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。

默认情况下，使用此版本的 StoreFront 创建的应用商店使用统一体验，但是升级的 Citrix 默认情况下保留经典体验。要支持统一体验，必须将 StoreFront 应用商店与 Receiver for Web 站点关联起来，并且必须将此站点配置为使用统一体验。

重要：如果将 Receiver for Web 站点添加到受限制的区域中，则不支持统一体验。如果必须将 Receiver for Web 站点添加到"受限制的区域"中，请将您的应用商店配置为使用经典体验。

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。
- 选择与该应用商店关联的统一 Citrix Receiver for Web 站点。
- 自定义 Receiver 外观。

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。

> ### 注意
>
> 如果使用 XenApp 6.x，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**的应用程序不支持启用统一体验。

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 Web 站点 > 添加，并按照向导进行操作。

更改 Citrix Receiver 体验

您可以选择 Citrix Receiver for Web Web 站点是提供**经典**体验还是**统一**体验。请注意，启用经典体验会禁用高级自定义和精选应用程序组管理功能。

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，在中间窗格中选择要更改的应用商店，然后在操作窗格中单击**管理 Receiver for Web 站点**，然后单击**配置**。
3. 选择 **Receiver 体验**，然后选择**禁用经典体验**或**启用经典体验**。

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，会自动创建采用统一模式的 Citrix Receiver for Web 站点并将其与应用商店关联。但是，如果从 StoreFront 早期版本升级，将默认采用经典体验。

要选择 Citrix Receiver for Web 站点以便为应用商店提供统一体验，必须至少创建一个禁用经典体验的 Citrix Receiver for Web 站点。

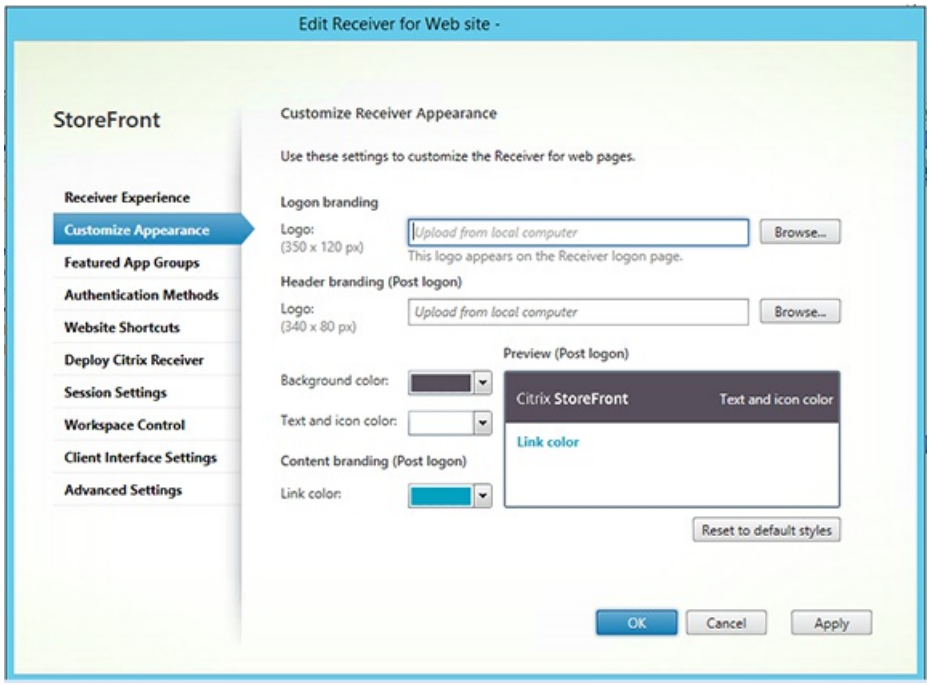
1. 在 Windows **开始**屏幕或**应用程序**屏幕中，找到并单击 **Citrix StoreFront** 磁贴。
2. 在 Citrix StoreFront 管理控制台的左侧窗格中选择**应用商店**节点，在中间窗格中选择一个应用商店，然后在**操作**窗格中单击**配置统一外观**。只有支持统一体验（禁用经典体验）的 Web 站点才可以设置为应用商店的默认值。如果您未创建 Citrix Receiver for Web Web 站点，则会显示一条消息，其中包含指向“创建新 Receiver for Web Web 站点”的消息。您还可以将现有 Receiver for Web 站点更改为 Receiver for Web Web 站点。请参阅更改 Citrix Receiver 体验。
3. 创建 Citrix Receiver for Web 时，为此应用商店选择**配置统一体验**，然后选择特定的 Web 站点。

> **Important**
>
> 如果您在 Receiver for Web 站点上将统一体验更改为经典体验，这可能会影响本机 Citrix Receiver 客户端。在此 Receiver for Web 站点上将体验更改回统一体验不会将本机 Citrix Receiver 客户端的体验更新为统一体验。必须在管理控制台上的“应用商店”节点中重置统一体验。

自定义 Citrix Receiver 外观

您的 Citrix Receiver for Web Web 站点必须禁用经典 Citrix Receiver 体验，才能自定义 Citrix Receiver 的外观。

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“操作”窗格中单击**管理 Receiver for Web 站点**和**配置**。
3. 选择 **Receiver 体验** > **禁用经典体验**。
4. 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。



创建和管理精选应用程序

Nov 27, 2017

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，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。

请注意，仅当禁用了经典体验时此功能才可用。

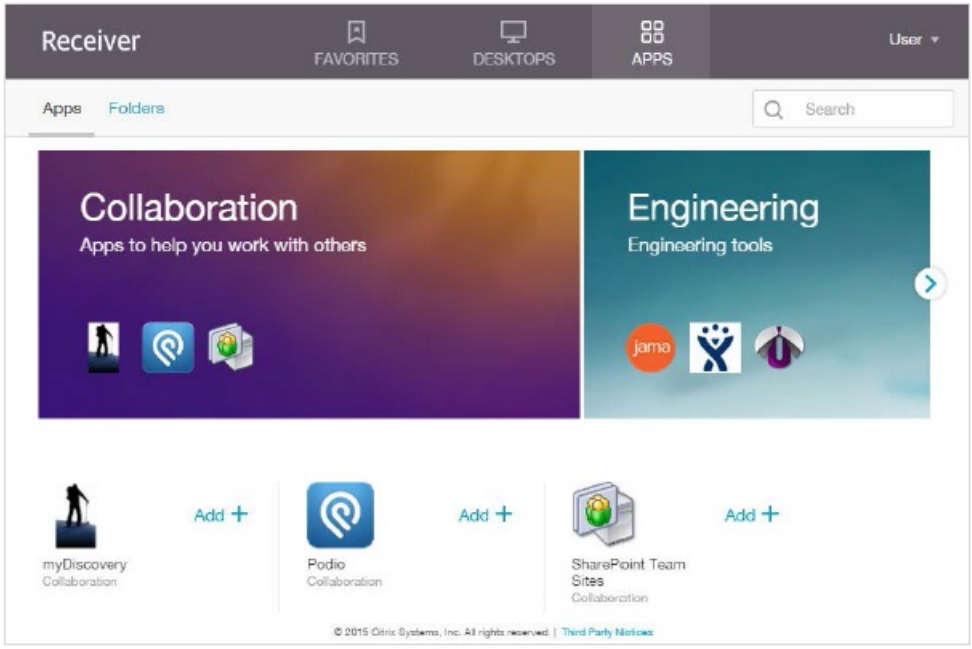
1. 在 Windows **开始**屏幕或“应用程序”屏幕中，找到并单击 Citrix **StoreFront** 磁贴。
2. 在 Citrix StoreFront 管理控制台的左侧窗格中选择“应用商店”节点，然后在“操作”窗格中单击**管理 Receiver Web 站点**和**配置**。
3. 选择**精选应用程序组**。
4. 在**精选应用程序组**对话框中，单击**创建**定义新的精选应用程序组。
5. 在**创建精选应用程序组**对话框中，指定精选应用程序组的名称、说明（可选）、背景和定义此精选应用程序组方法。您可以选择关键字、应用程序名称或应用程序类别，然后单击**确定**。

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 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

Nov 27, 2017

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，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 Citrix Receiver for HTML5 对浏览器选项卡的使用

Nov 27, 2017

默认情况下，Citrix Receiver for HTML5 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 Citrix Receiver for HTML5 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，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**。
4. 从**部署选项**下拉菜单中选择**始终使用 HTML 5 Receiver**，然后根据启动应用程序要使用的选项卡，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**。

配置通信超时持续时间和重试次数

Nov 27, 2017

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，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，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。

配置用户访问

Nov 27, 2017

本文包含以下信息：

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

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。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，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 XenApp Services 支持**。
3. 选中或清除**启用 XenApp Services 支持**复选框，以分别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 的形式为 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* 为在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。

为所有 Citrix Receiver 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 包含一项用于在所有 Citrix Receiver 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**，然后选中或取消选中**允许重新连接会话**。

使用 PowerShell

确保关闭管理控制台。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** 启用或关闭工作区控制重新连接功能。

语法

```
Set-DSAllowSessionReconnect [[-SiteId] ] [[-VirtualPath] ] `
[[-IsAllowed] ]
```

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
```

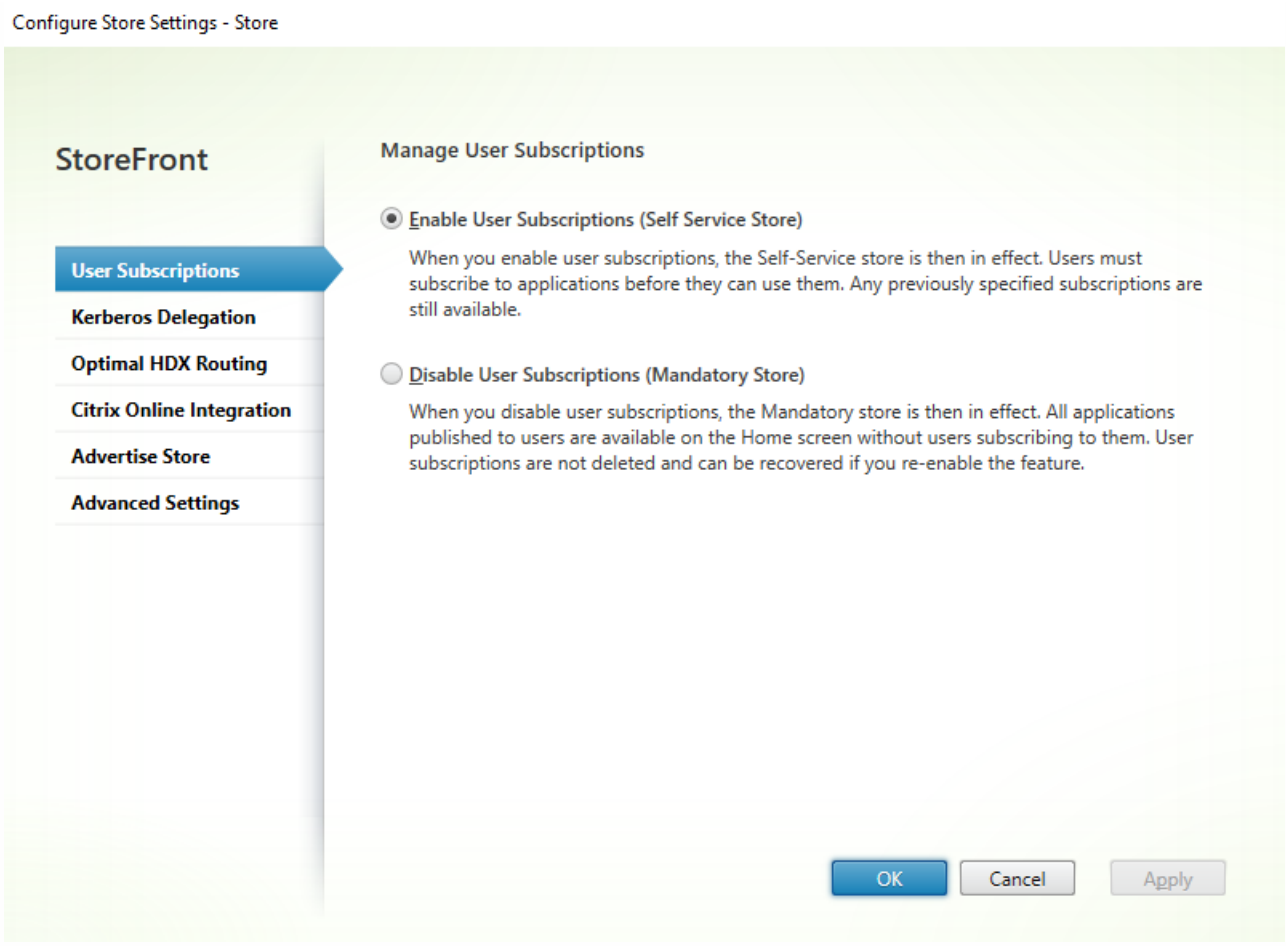
配置用户订阅

使用“用户订阅”任务可选择以下选项之一：

- 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 Receiver 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**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/"

Set-STFStoreService -StoreService $StoreObject -LockedDown $True -Confirm:$False
```

有关 Get-STFStoreService 的详细信息，请参阅 https://citrix.github.io/storefront-sdk/Citrix.StoreFront.Stores/Get-STFStoreService/

管理应用商店的订阅数据

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 控制台管理 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. 在每个 StoreFront 服务器上查找订阅应用商店文件夹：
   C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_
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。

Code 复制

```
function Remove-SubscriptionData

{

    [CmdletBinding()]

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

    $SubsService = "Citrix Subscriptions Store"

    # Path to Subscription Data in StoreFront version 2.6 or higher

    $SubsPath = "C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_$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 获取制表符分隔的 .txt 文件格式的应用商店订阅数据的备份。

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

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

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

还原订阅数据

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

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

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

有关 Restore-STFStoreSubscriptions 的详细信息，请参阅 https://citrix.github.io/storefront-sdk/Citrix.StoreFront.SubscriptionsStore/Restore-STFStoreSubscriptions/#restore-stfstoresubscriptions

还原单个 StoreFront 服务器上的数据

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

还原 StoreFront 服务器组中的数据

要将订阅数据还原到服务器组，需要执行以下操作。

包含三台 StoreFront 服务器的示例服务器组部署。

StoreFrontA

StoreFrontB

StoreFrontC

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

```
Code 复制

$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://citrix.github.io/storefront-sdk/Citrix.StoreFront.SubscriptionsStore/Import-STFStoreSubscriptions/#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：

…

这些值按如下所示进行定义：

- <*user-identifier*> - 必需项。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*> - 必需项。标识所订阅资源的字符序列。
- <*subscription-id*> - 必需项。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*> - 必需项。订阅的状态：已订阅或已取消订阅。
- <*property-name*> 和 <*property-value*> - 必需项。零或多个 和 值对的序列。它们表示与 StoreFront 客户端（通常为 Citrix Receiver）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

Code 复制

```
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"
```

设置高可用性多站点应用商店配置

Nov 27, 2017

在本文中：

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 NetScaler Gateway 设备，则可以为用户定义用于访问每个部署的最佳设备。

自 StoreFront 3.5 起，StoreFront 管理控制台支持常见的多站点场景。Citrix 建议您在满足要求时使用该管理控制台。

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 组成员关系，可以限制能够访问特定部署的用户。
- **聚合部署**：可以指定哪些部署具有您要聚合的资源。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 NetScaler Gateway 进行访问时，StoreFront 在启动资源时会优先启动与网关区域匹配的区域中的部署。

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. 确保为应用商店配置了要在配置中使用的所有 XenDesktop 和 XenApp 部署的详细信息。有关将部署添加到应用商店的详细信息，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**，选择 Controller，然后单击**聚合**以指定是否聚合 Delivery Controller。如果启用了 Delivery Controller 的聚合，这些 Delivery Controller 中显示名称相同的应用程序和桌面将在 Citrix Receiver 中以单个应用程序/桌面的形式显示。
7. 选中一个或两个**聚合 Controller 设置**复选框，然后单击**确定**。

    Controller 发布相同的资源 - 选中时，StoreFront 将仅枚举聚合集中的其中一个 Controller 中的资源。取消选中时，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）。选中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。取消选中时，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。

高级配置

虽然您可以通过 StoreFront 管理控制台配置多个常见的多站点和高可用性操作，但是，您仍然能够使用配置文件通过与较旧版本的 StoreFront 相同的方式配置 StoreFront。

使用 PowerShell 或者通过编辑 StoreFront 配置文件获取的额外功能：

- 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。

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. 确保为应用商店配置了要在配置中使用的所有 XenDesktop 和 XenApp 部署（包括灾难恢复部署）的详细信息。有关将部署添加到应用商店的详细信息，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。

4. 指定如下所示的配置。

```
...

aggregationGroup="aggregationgroupname">

...
```

...

...

...

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中的部署，从而在所有可用部署中平均分配用户。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聚合，可将聚合组名称设置为空字符串 **""**。

  identical 属性接受值 **true** 和 **false**，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 XenDesktop 或 XenApp 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 NetScaler 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 NetScaler 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应用程序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。
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。
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。

1. 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键入以下命令以导入 StoreFront 模块。
   ```
   Import-Module "installationlocation\Management\Cmdlets\UtilsModule.psm1"
   Import-Module "installationlocation\Management\Cmdlets\
    SubscriptionSyncModule.psm1"
   ```
   其中 installationlocation 是 StoreFront 的安装目录，通常为 C:\Program Files\Citrix\Receiver StoreFront\。

2. 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。
   ```
   Add-DSSubscriptionsRemoteSyncCluster -clusterName deploymentname
    -clusterAddress deploymentaddress
   ```
   其中 deploymentname 为一个帮助用户识别远程部署的名称，deploymentaddress 为远程部署的 StoreFront 服务器或负载平衡的服务器组的外部可访问地址。

3. 要指定与用户应用程序订阅同步的远程应用商店，请键入以下命令。
   ```
   Add-DSSubscriptionsRemoteSyncStore -clusterName deploymentname
    -storeName storename
   ```
   其中 deploymentname 为在上一步中为远程部署定义的名称，storename 为在创建本地应用商店和远程应用商店时为其指定的名称。要在应用商店之间同步应用程序订阅，两个应用商店在各自的 StoreFront 部署中所具有的名称必须相同。

4. 要配置在每天的特定时间进行同步，请键入以下命令。
   ```
   Add-DSSubscriptionsSyncSchedule -scheduleName
    synchronizationname -startTime hh:mm
   ```
   其中 synchronizationname 为一个帮助用户识别要创建的计划的名称。使用 -startTime 设置可指定每天在两个应用商店之间进行订阅同步的时间。可配置进一步的时间表来指定一天内其他的同步时间。

5. 或者，要配置按特定时间间隔定期同步，请键入以下命令。
   ```
   Add-DSSubscriptionsSyncReoccuringSchedule -scheduleName
    synchronizationname -startTime hh:mm:ss -repeatMinutes interval
   ```
   其中 synchronizationname 为一个帮助用户识别要创建的计划的名称。使用 -startTime 设置可指定每天启动循环计划的时间。对于 interval，则用于指定同步之间的间隔时间（分钟）。

6. 将远程部署中每个 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。
   这样，一旦您在远程部署上配置同步计划，远程部署中的服务器即可访问本地部署上的订阅应用商店服务。
   CitrixSubscriptionSyncUsers 组是您在步骤 1 中导入订阅同步模块时创建的。有关修改本地用户组的详细信息，请参阅 http://technet.microsoft.com/zh-cn/library/cc772524.aspx。

7. 如果本地 StoreFront 部署中包含多台服务器，请使用 Citrix StoreFront 管理控制台将配置更改传播到组中的其他服务器。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。

8. 对远程 StoreFront 部署重复步骤 1 到 7，以配置从远程部署到本地部署的互补订阅同步计划。
   为 StoreFront 部署配置同步计划时，请确保计划不会导致出现各个部署尝试同时进行同步的情况。

9. 要开始同步应用商店间的用户应用程序订阅，请在本地和远程部署上重新启动订阅应用商店服务。在每个部署中的主服务器上的 Windows PowerShell 命令提示窗口中，键入以下命令。
   Restart-DSSubscriptionsStoreSubscriptionService
10. 要删除现有订阅同步计划，请键入以下命令。然后，将配置更改传播到部署中的其他 StoreFront 服务器，并重新启动订阅应用商店服务。
    Remove-DSSubscriptionsSchedule -scheduleName synchronizationname
    其中 synchronizationname 是您在创建计划时为其指定的名称。

11. 要列出当前为 StoreFront 部署配置的订阅同步计划，请键入以下命令。
    Get-DSSubscriptionsSyncScheduleSummary

为应用商店配置最佳 HDX 路由

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。

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 XenApp 或 XenDesktop 控制器和已发布的资源所在的数据中心或地理位置将 XenApp 7.8 或 XenDesktop 7.8 部署划分到几个区域中。在 XenApp 或 XenDesktop 7.8 Studio 中定义区域。StoreFront 现在与 XenApp 7.8 和 XenDesktop 7.8 交互操作，在 StoreFront 中定义的所有区域都必须与在 XenApp 和 XenDesktop 中定义的区域名称相匹配。

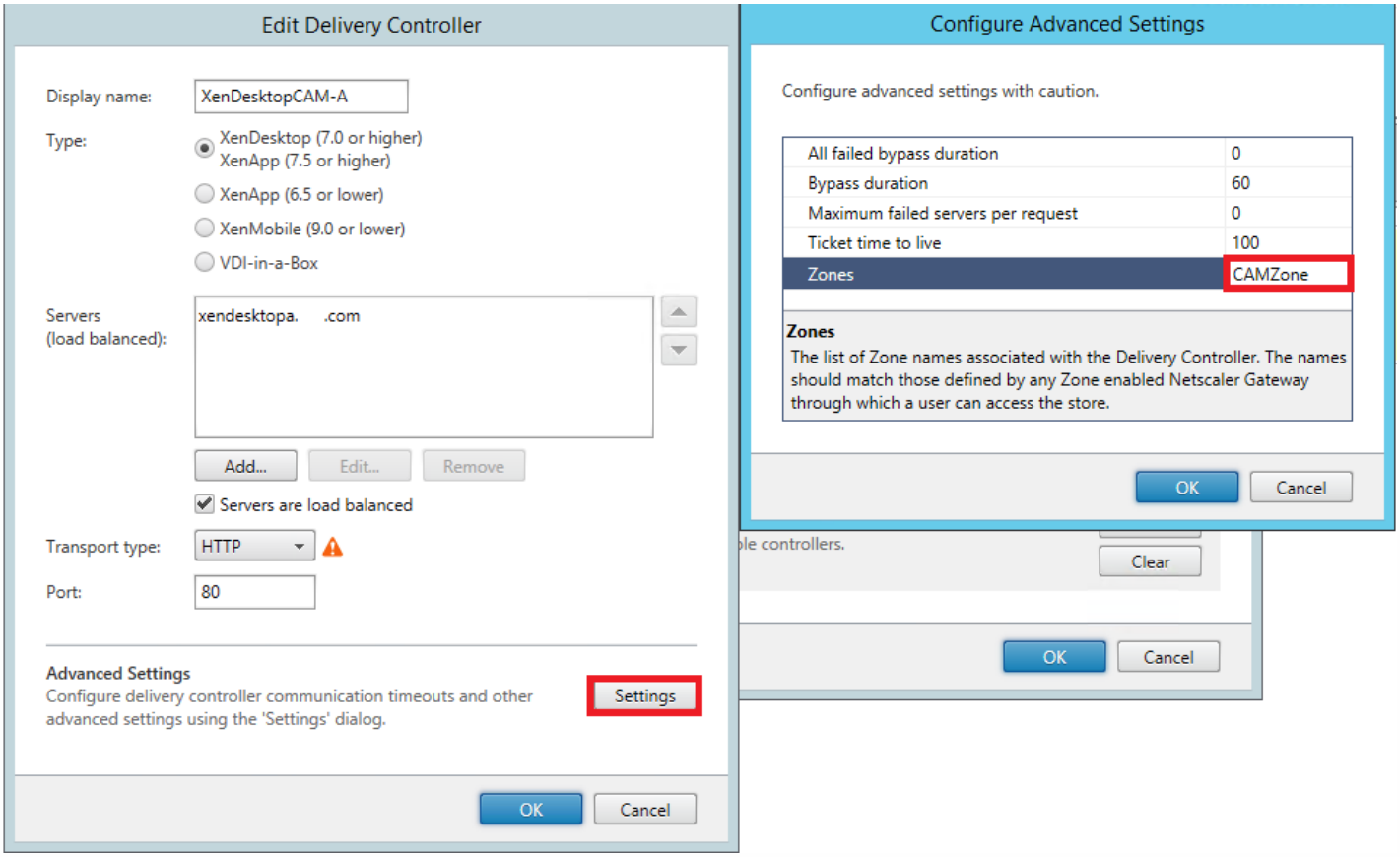
本版本的 StoreFront 还允许您为所定义的区域中的所有 Delivery Controller 创建最佳网关映射。将区域映射到最佳网关与使用场创建映射基本相同，您可能已熟悉后一种操作。唯一的区别在于区域通常代表规模更大的、包含更多 Delivery Controller 的容器。不需要向最佳网关映射中添加每个 Delivery Controller。要将 Controller 放置到所需的区域中，只需使用与已在 XenApp 或 XenDesktop 中定义的区域匹配的区域名称标记每个 Delivery Controller 即可。可以将一个最佳网关映射到多个区域，但您通常应使用一个区域。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 NetScaler 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**，然后在**编辑 Delivery Controller** 屏幕上单击**设置**。
4. 在**区域**行中的第二列中单击。
5. 单击 **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 NetScaler 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 XenApp 或 XenDesktop 发布的应用程序）的 ICA 连接处理。通常，一个站点的最佳网关布置在同一地理位置。

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 NetScaler 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	-> 本地 UK 应用程序和桌面
	–> 仅用于 UK 故障转移的 US 应用程序和桌面
1 x US 网关 -> 1 x US StoreFront	-> 本地 US 应用程序和桌面
	–> 仅用于 US 故障转移的 UK 应用程序和桌面

UK 网关使用 UK StoreFront 提供对 UK 托管资源（如应用程序和桌面）的远程访问。

UK StoreFront 同时定义了基于 UK 和基于 US 的 NetScaler Gateway，并在其 Delivery Controller 列表中包含 UK 和 US 场。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。

在没有最佳网关路由的情况下，所有 ICA 启动将通过创建启动请求的 UK 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：只能为一个站点和每个 StoreFront 应用商店映射一个最佳网关。

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

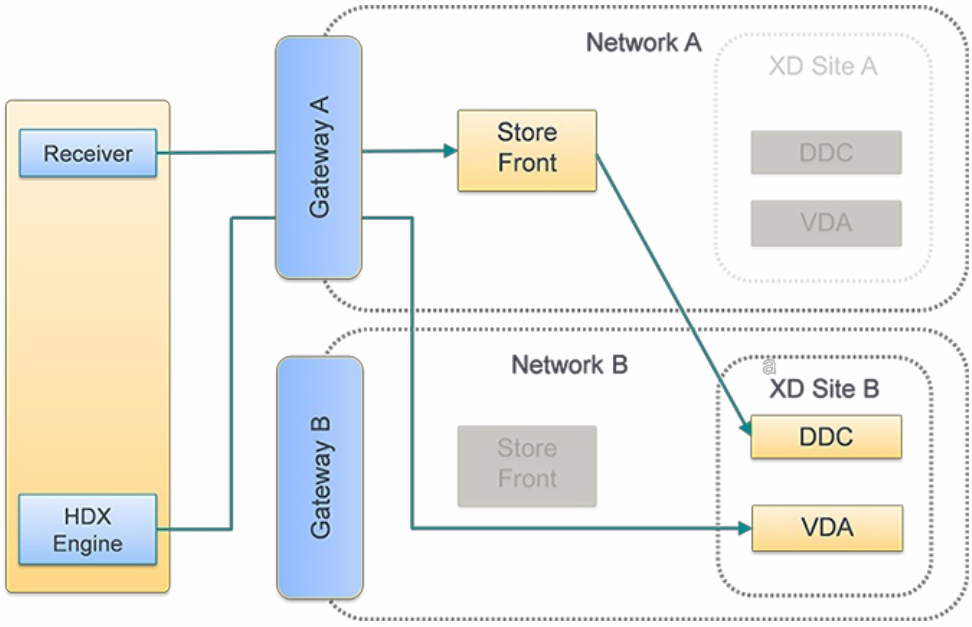
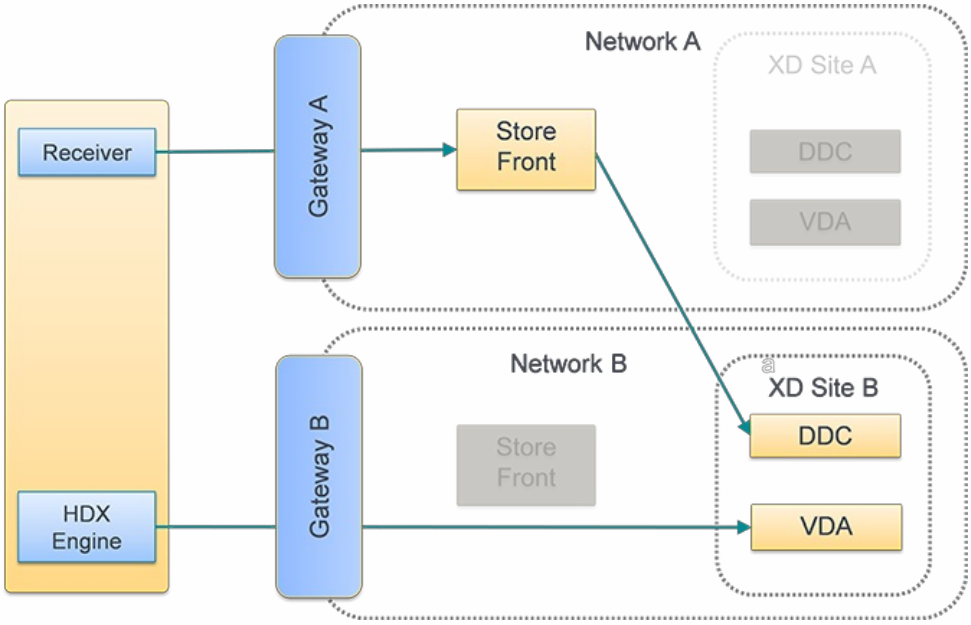


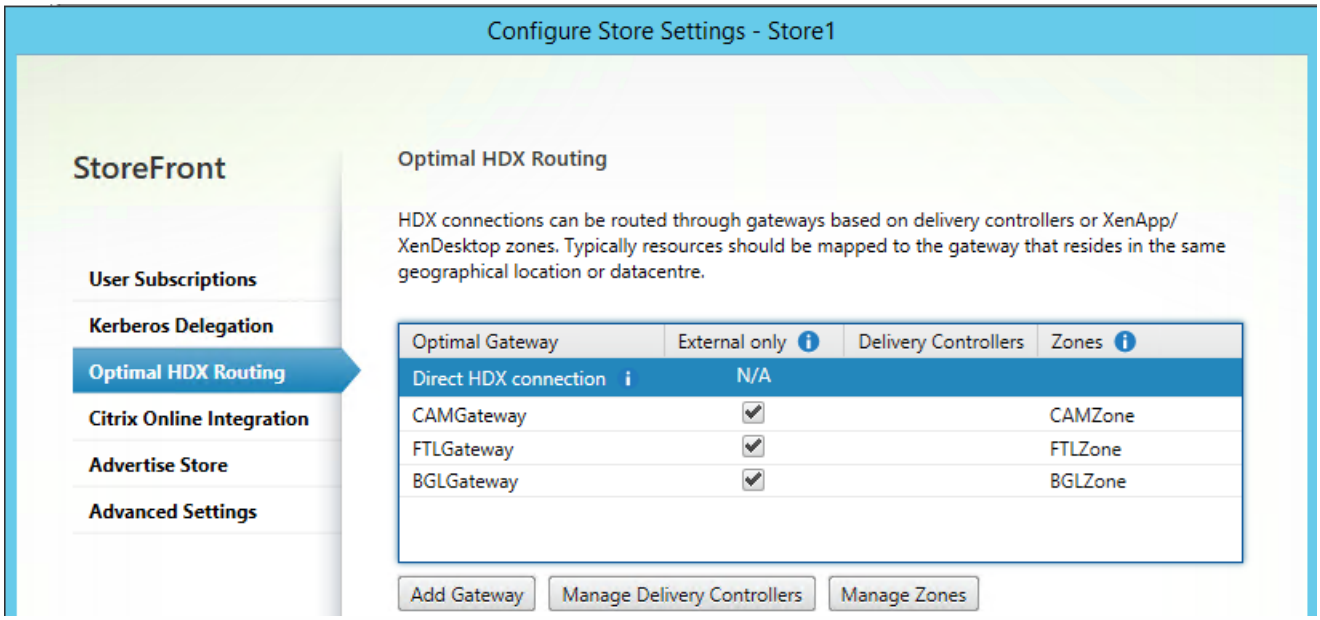
图 2. 最佳网关路由



使用 Citrix StoreFront 管理控制台

为部署配置单独的 NetScaler Gateway 设备之后，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，该复选框将与 **-enabledOnDirectAccess = false** 等效，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 NetScaler Gateway”屏幕。

1. 在**常规设置**屏幕上，填写“显示名称”、“NetScaler 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 NetScaler 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 NetScaler Gateway 进行远程访问。
2. 在 **Secure Ticket Authority (STA)** 屏幕上，填写显示的选项。STA 托管于 XenDesktop 和 XenApp 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 XenDesktop 和 XenApp 资源进行身份验证和授权的基础。
3. 在**身份验证设置**屏幕上，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 NetScaler Gateway 路由

PowerShell API 参数

Parameter	Description
-SiteId (整型)	IIS 中的站点 ID。对于默认安装 StoreFront 的 IIS 中的站点，通常为 1。
-ResourcesVirtualPath (字符串)	要进行配置以具有最佳网关映射场的应用商店的路径。 示例："/Citrix/Store"
-GatewayName (字符串)	为识别 StoreFront 中的 NetScaler Gateway 而提供的名称。 示例 1：ExternalGateway 示例 2：InternalGateway
-Hostnames (字符串数组)	指定最佳 NetScaler Gateway 设备的完全限定的域名 (FQDN) 和端口。 示例 1：gateway.example.com，用于标准 vServer 端口 443。 示例 2：gateway.example.com:500，用于非标准 vServer 端口 500。
-Farms (字符串数组)	指定一组（通常位于同一个位置）共享通用最佳 NetScaler Gateway 设备的 XenDesktop、XenApp 和 App Controller 部署。场可以包含提供已发布资源的单个 Delivery Controller 或多个 Delivery Controller。 可以在 StoreFront 中的 Delivery Controller 下配置一个 XenDesktop 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 (字符串数组)	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 (字符串数组)	指定运行 Secure Ticket Authority (STA) 的 XenDesktop 或 XenApp 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 (布尔型)	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 (布尔型)	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 (布尔型)	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 (布尔型)	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 NetScaler 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。

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** 创建或覆盖适用于场的最佳网关映射。

```
& "$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 创建或覆盖适用于场的最佳网关映射。

```
& "$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 的适用于场的所有最佳网关。

```
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"
```

为场配置直接 HDX 连接

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

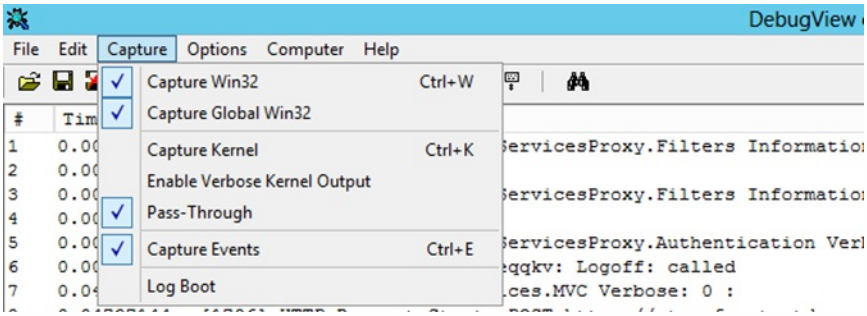
1. 通过运行以下命令，使用 PowerShell 在所有服务器组节点上启用 StoreFront 跟踪：

   ```
   & "$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

     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。

     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

     Farm1 配置为不使用网关。所有网关都不用于启动。

与 NetScaler Gateway 和 NetScaler 集成

Nov 27, 2017

将 NetScaler 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 NetScaler 提供负载平衡。

计划网关和服务器证书的使用

将 StoreFront 与 NetScaler Gateway 和 NetScaler 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 - 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 XenApp 和 XenDesktop 7.x 控制器，它们提供同等资源。
- 准备硬件保护的私钥存储。网关和服务器（包括一些 NetScaler 型号）可以将私钥安全地存储在硬件安全模块 (HSM) 或可信平台模块 (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 NetScaler Gateway 实施 GSLB，这可能要求 GSLB 中的每个网关具有一个相同的证书，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 End-To-End Encryption with XenApp and XenDesktop（XenApp 和 XenDesktop 的端到端加密）以及 XenApp 和 XenDesktop 的安全一节。

添加 NetScaler Gateway 连接

Jun 04, 2018

可以通过执行添加 NetScaler Gateway 设备任务添加用户用于访问应用商店的 NetScaler Gateway 部署。配置通过 NetScaler Gateway 对应用商店进行远程访问之前，必须启用 NetScaler Gateway 直通身份验证方法。有关为 StoreFront 配置 NetScaler 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，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“操作”窗格中单击管理 NetScaler Gateway。
3. 单击**添加**和常规设置，为 NetScaler Gateway 部署指定便于用户识别的名称。
   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 NetScaler 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 NetScaler Gateway 虚拟服务器的 FQDN。不支持对 StoreFront 和 NetScaler 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 NetScaler 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 NetScaler 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 NetScaler 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 NetScaler Gateway 的设备，请从登录类型列表中选择之前在设备上为 Citrix Receiver 用户配置的身份验证方法。
   您所提供的有关 NetScaler Gateway 设备配置的信息将添加到应用商店的置备文件中。这使 Citrix Receiver 可以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 NetScaler Gateway 或单个 Access Gateway 5.0 设备配置 StoreFront，请在回调 URL 框中填写 NetScaler 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 NetScaler Gateway 身份验证服务，以验证从 NetScaler 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 XenDesktop 或 XenApp 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 托管于 XenDesktop 和 XenApp 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 XenDesktop 和 XenApp 资源进行身份验证和授权的基础。

12. 如果希望 XenDesktop 和 XenApp 在 Citrix Receiver 尝试自动重新连接期间将断开的会话保持在打开状态，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 Request tickets from two STAs, where available（从两个 STA 请求票据(如果可用)）复选框。
    选中 Request tickets from two STAs, where available（从两个 STA 请求票据(如果可用)）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. 单击创建以添加 NetScaler Gateway 部署的详细信息。添加完部署之后，请单击完成。
    有关更新部署详细信息的详细说明，请参阅配置 NetScaler Gateway 连接设置。

要提供通过 NetScaler Gateway 对应用商店的访问，必须配置一个内部信号点和至少两个外部信标点。Citrix Receiver 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 作为内部信号点。使用所添加的第一个 NetScaler 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。有关更改信标点的详细信息，请参阅配置信标点。

要允许用户通过 NetScaler 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 NetScaler Gateway

Nov 27, 2017

NetScaler 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 NetScaler Gateway，以便正确配置 NetScaler 和 StoreFront 使其能够配合使用。

要求

- 要将多个网关 vServer 导出为 ZIP 文件，需要 NetScaler 11.1.51.21 或更高版本。**注意**：NetScaler 只能导出使用 XenApp 和 XenDesktop 向导创建的网关 vServer。
- DNS 必须能够解析且 StoreFront 必须能够联系 NetScaler 生成 ZIP 文件中的 GatewayConfig.json 文件中的所有 STA (Secure Ticket Authority) 服务器 URL。
- NetScaler 生成 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。NetScaler 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 vServer 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。

    或者

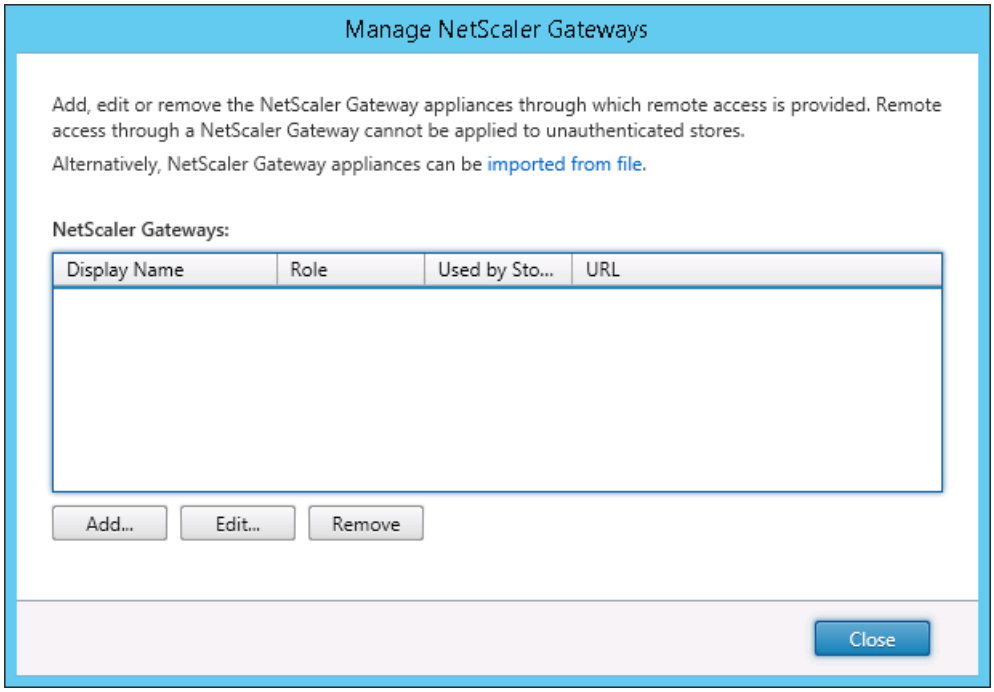
    如果您在您的环境中使用不同的外部和内部 DNS 命名空间，回调 URL 和端口组合可能与网关 URL 和端口组合不同。如果您的网关位于 DMZ 中并使用 URL，而 StoreFront 位于您的公司专用网络中并使用 URL，则您可以使用回调 URL 指回 DMZ 中网关 vServer。

使用控制台导入 NetScaler Gateway

可以通过导入 NetScaler 配置文件来导入一个或多个 NetScaler Gateway 设备。

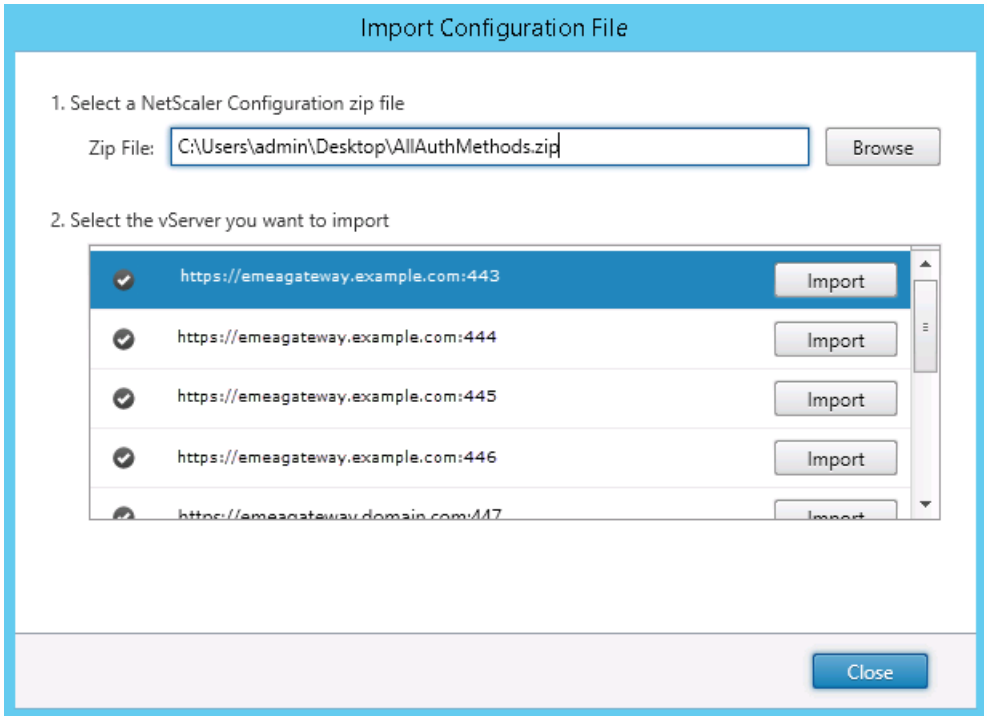
> **Important**
>
> Citrix 不支持手动编辑从 NetScaler 中导出的配置文件。

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 NetScaler Gateway**。
2. 在“管理 NetScaler Gateway”屏幕中，单击**从文件中导入**链接。



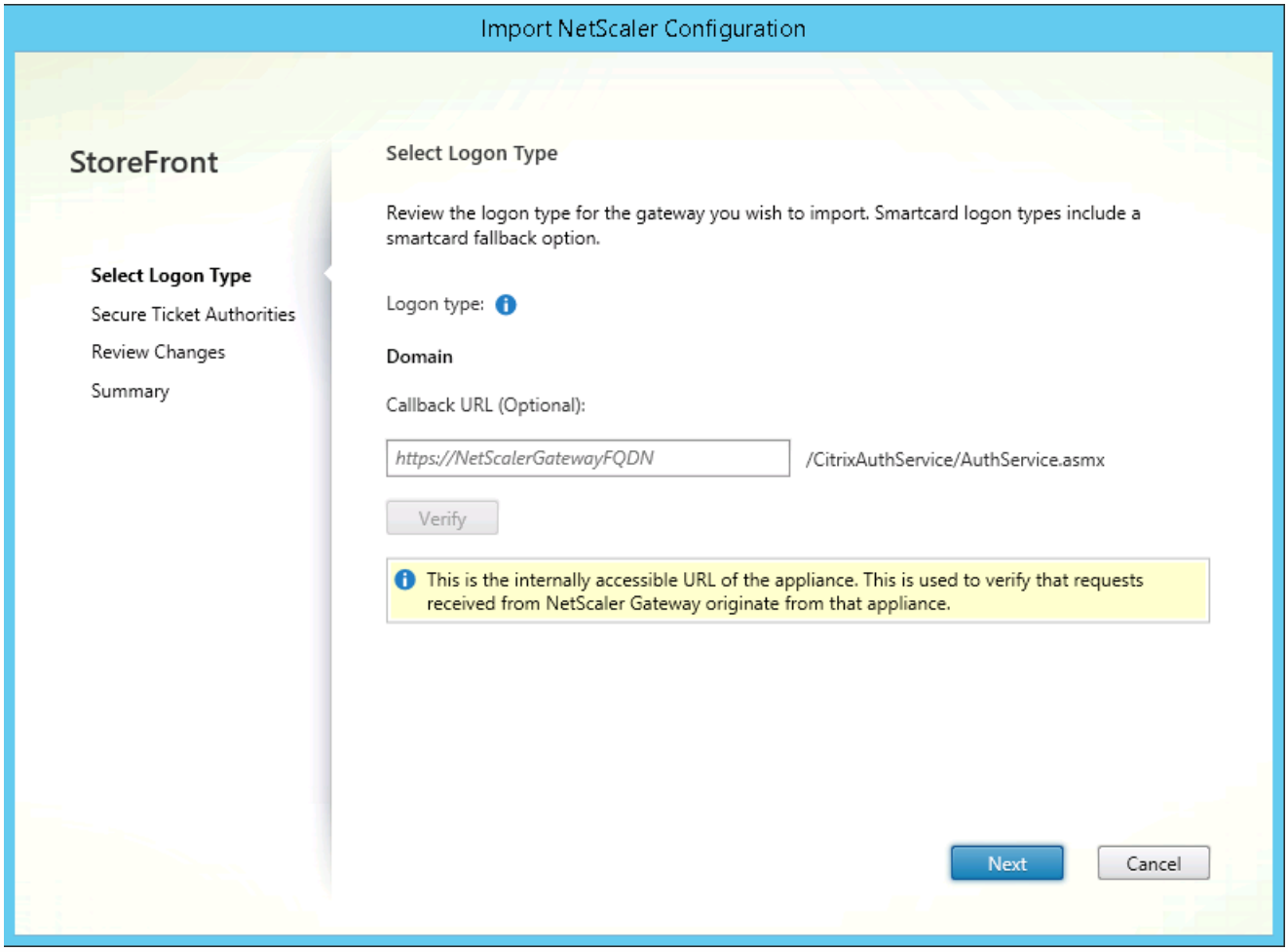
3. 浏览到 NetScaler 配置 ZIP 文件。

4. 将显示所选 ZIP 文件中的网关 vServer 列表。请选择您要导入的网关虚拟 vServer 并单击**导入**。如果重复导入某个 vServer，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，指定一个回调 URL。登录类型是在 NetScaler Gateway 设备上为 Citrix Receiver 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

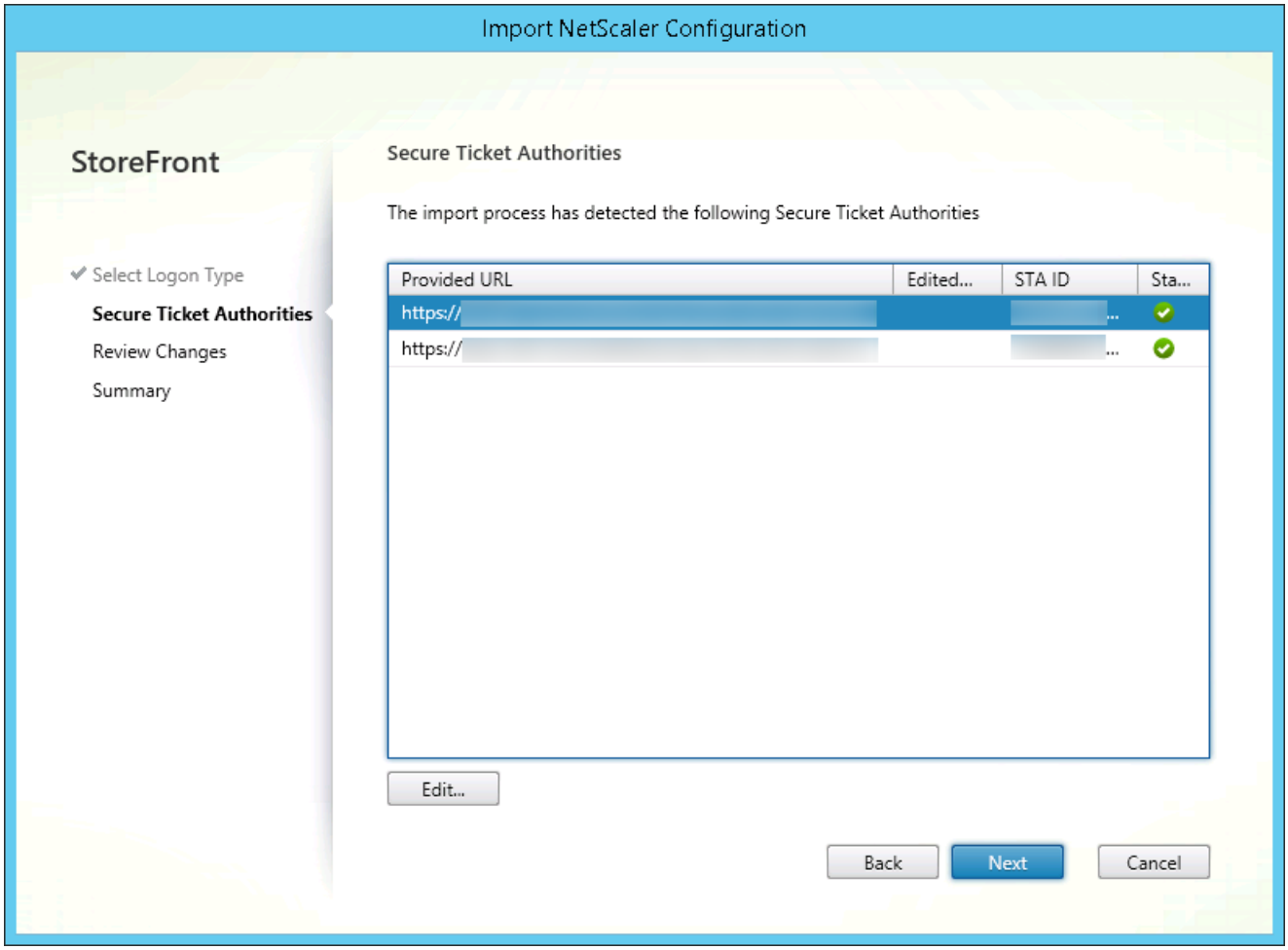
SMS 身份验证	短信	是

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 NetScaler Gateway vServer IP 的任何有效的 URL。

如果您要使用智能访问，则需要回调 URL。

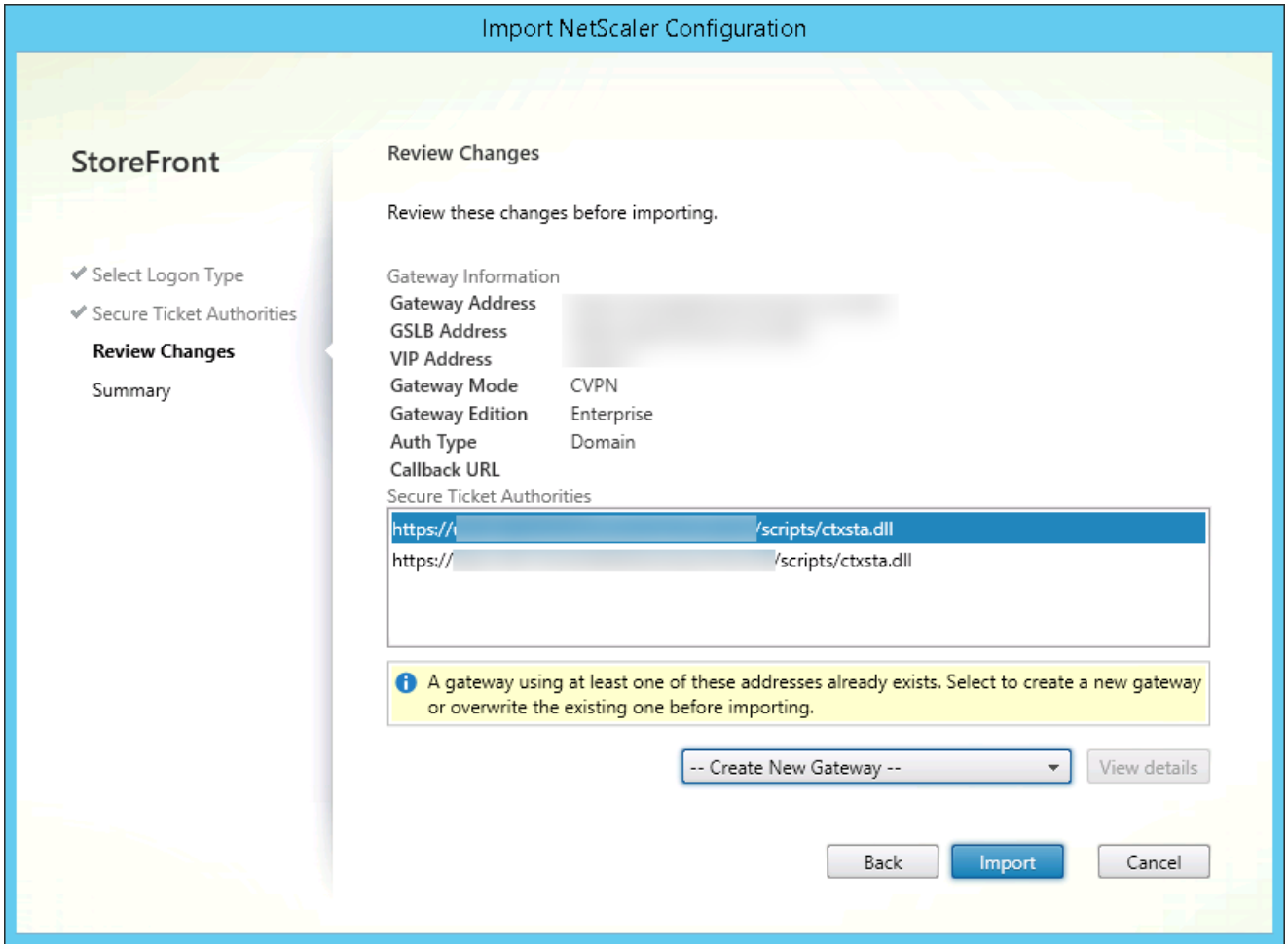
6. 单击**下一步**。

7. StoreFront 使用 DNS 联系 ZIP 文件中列出的所有 STA (Secure Ticket Authorities) 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，则 StoreFront 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 vServer 配置，请重复上面的步骤。

> **注意**
>
> 应用商店的默认网关是本机 Citrix Receiver 尝试通过其连接的网关，除非它们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本机 Citrix Receiver 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 NetScaler Gateway

Read-STFNetScalerConfiguration

- 将 ZIP 文件复制到当前登录的 StoreFront 管理员的桌面。
- 将 NetScaler 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。

命令 复制

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$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。

命令 复制

```
$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

GatewayEdition         : Enterprise

ReceiverForWebSites    : {Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite}
```

Import-STFNetScalerConfiguration（不指定 CallbackURL）

将 ZIP 文件复制到当前登录的 StoreFront 管理员的桌面。 将 NetScaler 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。

命令 复制

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$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。

命令 复制

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -Confirm:$False
```

Import-STFNetScalerConfiguration（指定自己的 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。

命令 复制

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.c

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.c

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.c
```

Import-STFNetScalerConfiguration 会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。

命令 复制

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://e

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://e

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://e
```

配置 NetScaler Gateway 连接设置

Jun 04, 2018

执行以下任务可更新用户访问您的应用商店时所用的 NetScaler Gateway 部署的详细信息。有关为 StoreFront 配置 NetScaler Gateway 的详细信息，请参阅使用 WebFront 与 StoreFront 集成。

如果对 NetScaler 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 Receiver 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中获取更新过的 Citrix Receiver 置备文件。否则，可以为应用商店导出置备文件，并将此文件设置为对用户可用。

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，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。

更改常规 NetScaler 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 NetScaler Gateway 部署名称，并将对虚拟服务器或用户登录点 URL 以及 NetScaler 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节点，然后单击管理 NetScaler Gateway。
3. 为 NetScaler Gateway 部署指定便于用户识别的名称。
   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 NetScaler 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 NetScaler Gateway 虚拟服务器的 FQDN。不支持对 StoreFront 和 NetScaler Gateway 虚拟服务器使用相同的 FQDN。

5. 如果您的部署运行的是 Access Gateway 5.0，请继续执行步骤 7。否则，请指定 NetScaler Gateway 设备的子网 IP 地址（如果需要）。
   子网地址是指 NetScaler 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 NetScaler 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. 如果设备运行的是 NetScaler Gateway，请从登录类型列表中选择在设备上为 Citrix Receiver 用户配置的身份验证方法。
   您所提供的有关 NetScaler Gateway 设备配置的信息将添加到应用商店的置备文件中。这使 Citrix Receiver 可以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 NetScaler Gateway 或单个 Access Gateway 5.0 设备组成，则在回调 URL 框中填写 NetScaler 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 NetScaler Gateway 身份验证服务，以验证从 NetScaler Gateway 收到的

请求是否来自该设备。

管理 Access Gateway 5.0 设备

使用 管理 设备任务可在 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

使用 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。 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 托管于 XenDesktop 和 XenApp 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 XenDesktop 和 XenApp 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 NetScaler Gateway 部署。在操作窗格中，单击管理 NetScaler 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. 如果希望 XenDesktop 和 XenApp 在 Citrix Receiver 尝试自动重新连接期间将断开的会话保持在打开状态，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 Request tickets from two STAs, where available（从两个 STA 请求票据(如果可用)）复选框。
   选中 Request tickets from two STAs, where available（从两个 STA 请求票据(如果可用)）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 NetScaler Gateway 部署

在**操作**窗格中，可以通过执行管理 NetScaler Gateway 中的**删除**任务从 StoreFront 中删除 NetScaler Gateway 部署的详细信息。删除 NetScaler Gateway 部署后，用户将无法通过该部署访问应用商店。

使用 NetScaler 进行负载平衡

Nov 27, 2017

本文包含使用 NetScaler 对两台及更多 StoreFront 服务器进行负载平衡所需的信息。

配置 StoreFront 服务器组和 NetScaler 负载平衡

为 NetScaler 负载平衡器和 StoreFront 服务器创建服务器证书

创建负载平衡 vServer 以实现服务器组之间的订阅同步

配置用于负载平衡的 StoreFront 服务器组

Citrix 服务监视器

NetScaler Gateway 与负载平衡 vServers 位于同一 NetScaler 设备上

使用 NetScaler 对 StoreFront 服务器组进行负载平衡时的环回选项

配置 StoreFront 服务器组和 NetScaler 负载平衡

规划要进行负载平衡的 StoreFront 部署

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 服务器组的方法指南。本文提供关于以下内容的详细信息：如何将 NetScaler 设备配置为在服务器组中的所有 StoreFront 节点之间对来自 Citrix Receiver/Citrix Receiver for Web 的传入请求进行负载平衡，以及如何配置与 NetScaler 或第三方负载平衡器结合使用的新 StoreFront 监视器。

对于负载平衡配置示例，请参阅下面的“方案 1”和“方案 2”部分。

通过以下环境进行测试

- 单服务器组中包含四个 Windows Server 2012 R2 StoreFront 3.0 节点。
- 配置一个 NetScaler 10.5 负载平衡器用于最少连接和 CookieInsert“粘滞”负载平衡。
- 一个安装了 Fiddler 4.0 和 Citrix Receiver for Windows 4.3 的 Windows 8.1 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

请查看计划网关和服务器证书的使用一节。

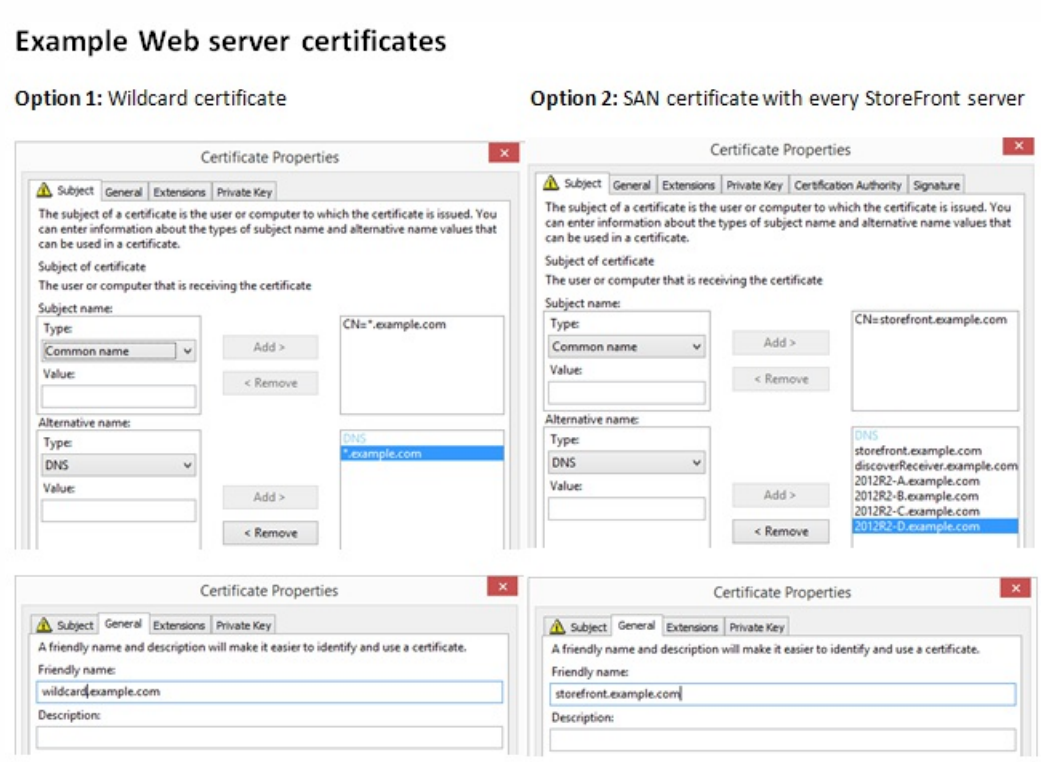
从商业证书颁发机构购买证书或通过您的企业 CA 颁发证书之前，请考虑以下选项。

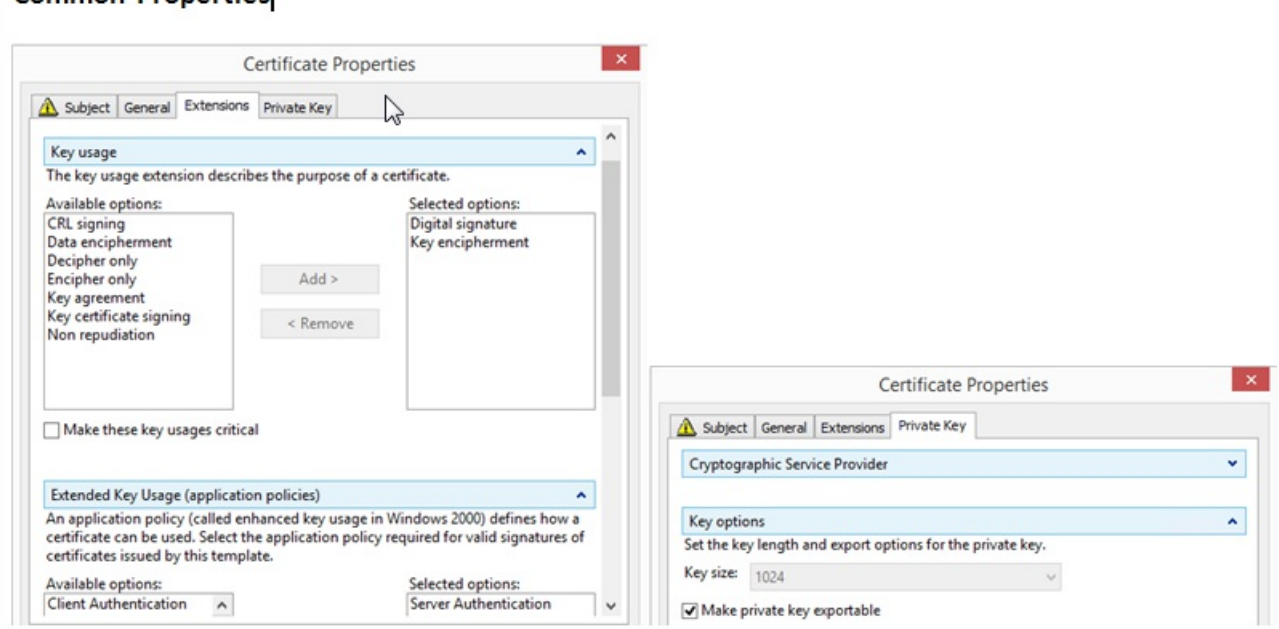
- **选项 1**：在 NetScaler 负载平衡 vServer 和 StoreFront 服务器组节点上均使用 *.example.com 通配符证书。这样可以简化配置，将来无需替换证书即可以添加其他 StoreFront 服务器。
- **选项 2**：在 NetScaler 负载平衡 vServer 和 StoreFront 服务器组节点上均使用包含使用者备用名称的证书。证书中包含匹配所有 StoreFront 服务器完全限定域名 (FQDN) 的其他 SAN 为可选，但是建议采用，因为这样可以在 StoreFront 部署中提供更大的灵活性。包含用于基于电子邮件发现 discoverReceiver.example.com 的 SAN。

    有关基于电子邮件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 NetScaler 负载平衡 vServer 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。





为 NetScaler 负载平衡器和所有 StoreFront 服务器创建服务器证书

使用 OpenSSL 将 Windows CA 颁发的证书导入到 NetScaler 设备

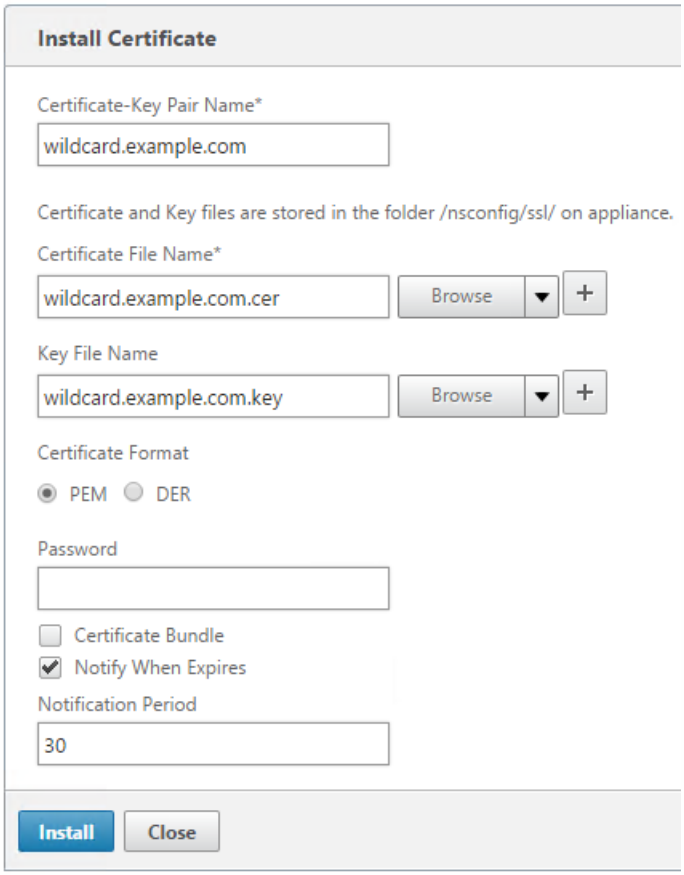
- WinSCP 是非常有用的第三方免费工具，可将文件从 Windows 计算机移动到 NetScaler 文件系统。将要导入的证书复制到 NetScaler 文件系统内的 **/nsconfig/ssl/** 文件夹。
- 您也可以使用 NetScaler 上的 OpenSSL 工具从 **PKCS12/PFX** 文件提取证书和密钥，以便以 NetScaler 可以使用的 PEM 格式创建两个单独的 .CER 和 .KEY X.509 文件。

1. 将 PFX 文件复制到 NetScaler 设备或 VPX 上的 **/nsconfig/ssl/** 中。

2. 打开 NetScaler 命令行接口 (CLI)。
3. 键入 **Shell** 以退出 NetScaler CLI 并切换到 FreeBSD shell。
4. 使用 **cd /nsconfig/ssl/** 更改目录。
5. 运行 **openssl pkcs12 -in <导入的证书文件>.pfx -nokeys -out <证书文件名>.cer**，并在出现提示时输入 PFX 密码。
6. 运行 **openssl pkcs12 -in <导入的证书文件>.pfx -nocerts -out <密钥文件名>.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 NetScaler CLI。

导入服务器证书后在 NetScaler 上进行配置

1. 登录 NetScaler 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 NetScaler 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 NetScaler 负载平衡器的 StoreFront 服务器组。

示例 - **storefront.example.com** 解析为负载平衡 vServer 虚拟 IP (VIP)。

方案 1：在客户端与 NetScaler 负载平衡器以及负载平衡器与两个或更多个

StoreFront 3.0 服务器之间建立端到端的 HTPPS 443 安全连接。

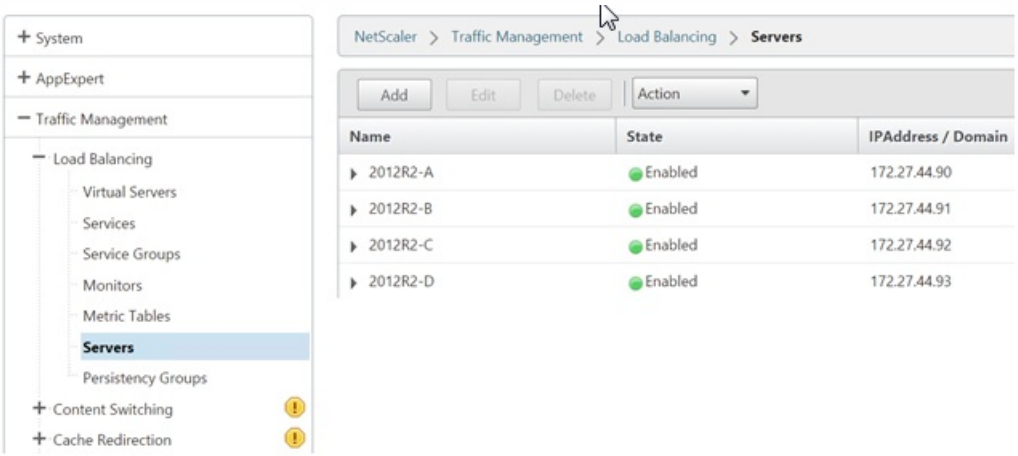
此方案使用修改后的 StoreFront 监视器并使用端口 443。

将单个 StoreFront 服务器节点添加到 NetScaler 负载平衡器

1. 登录 NetScaler 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 2012R2 StoreFront 节点，分别命名为 2012R2-A 至 2012R2–D

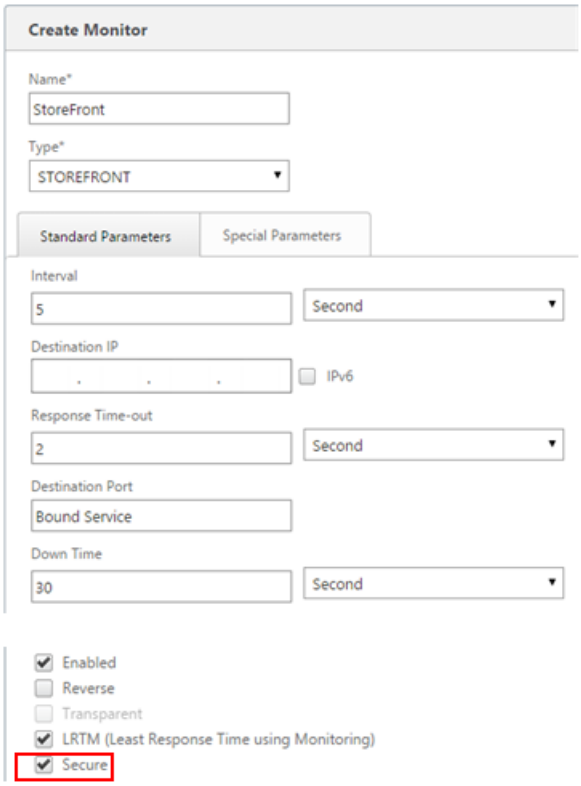
3. 使用基于 IP 的服务器配置，并输入每个 StoreFront 节点的服务器 IP 地址。



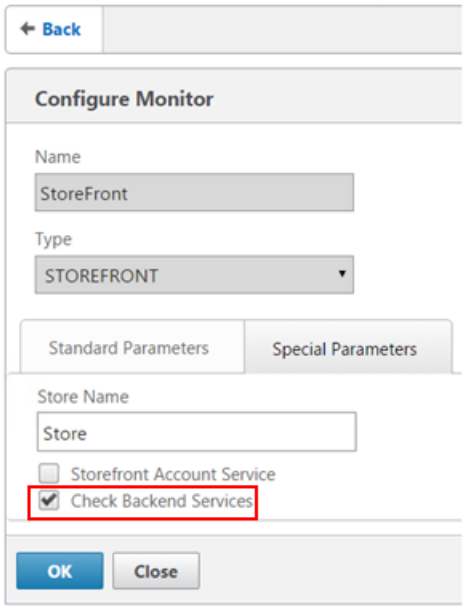
定义一个 StoreFront 监视器，用于检查服务器组中所有 StoreFront 节点的状态。

1. 登录 NetScaler 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，选择 **StoreFront**。
4. 如果在负载平衡 vServer 与 StoreFront 之间使用 HTTPS 连接，请确保选中**安全**复选框；否则，请将此选项保持在禁用状态。
5. 在“Special Parameters”（特殊参数）选项卡下面，指定应用商店的名称。
6. 选中“Special Parameters”（特殊参数）选项卡下面的 **Check Backend Services**（检查后端服务）复选框。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 Service，探测操作会返回正在运行的所有 StoreFront Service 的状态。

Standard Parameters Tab



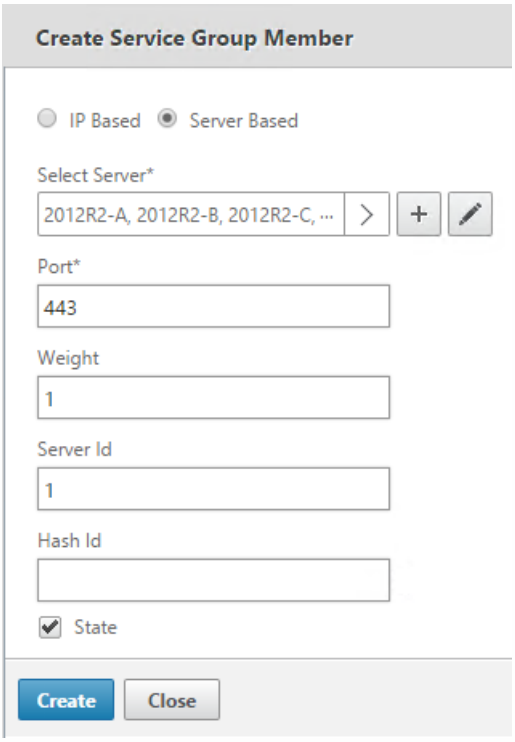
Special Parameters Tab



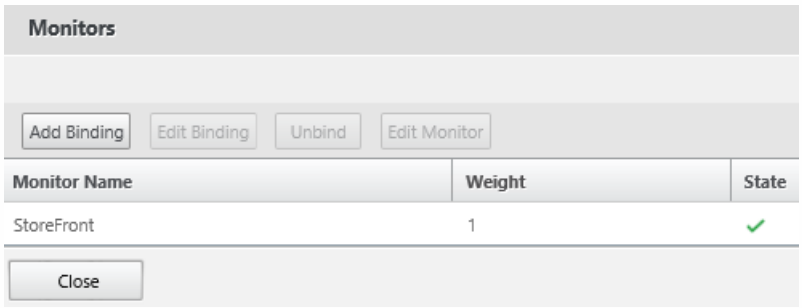
创建包含所有 StoreFront 服务器的 HTTPS 443 服务组

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 SSL 端口，并在添加节点时为每个节点分配一个唯一的服务器 ID。

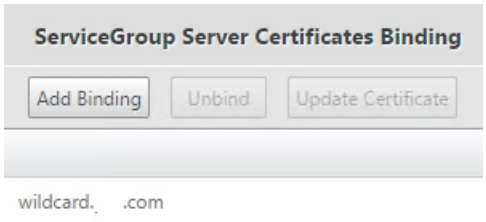


3. 在“Monitors”（监视器）选项卡上，选择之前创建的 StoreFront 监视器。



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。

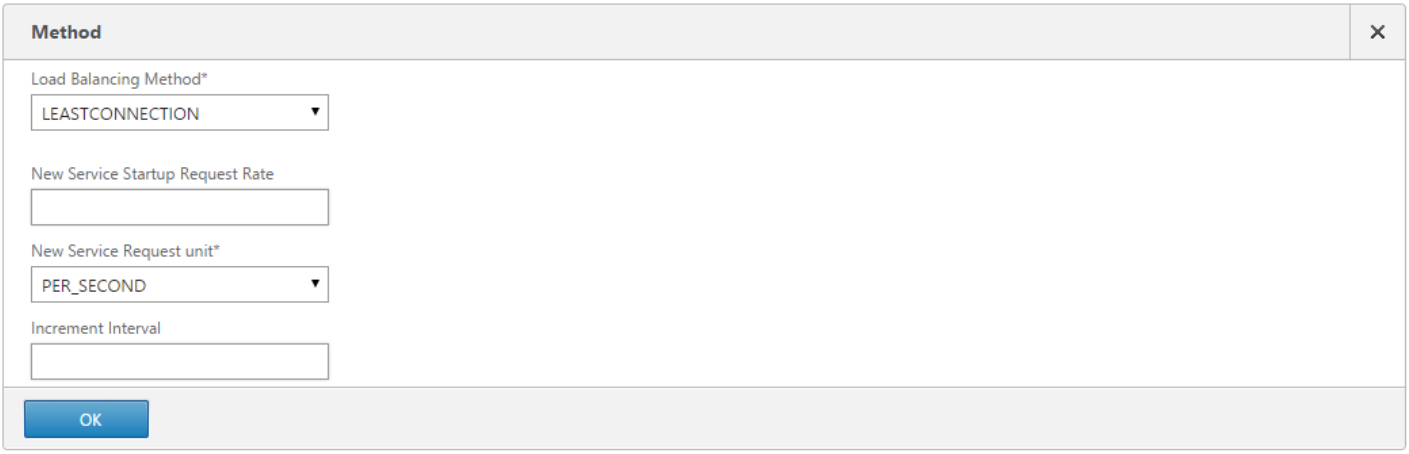


创建用于用户流量的负载平衡 vServer

1. 登录 NetScaler 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 vServer。

3. 选择 vServer 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）。



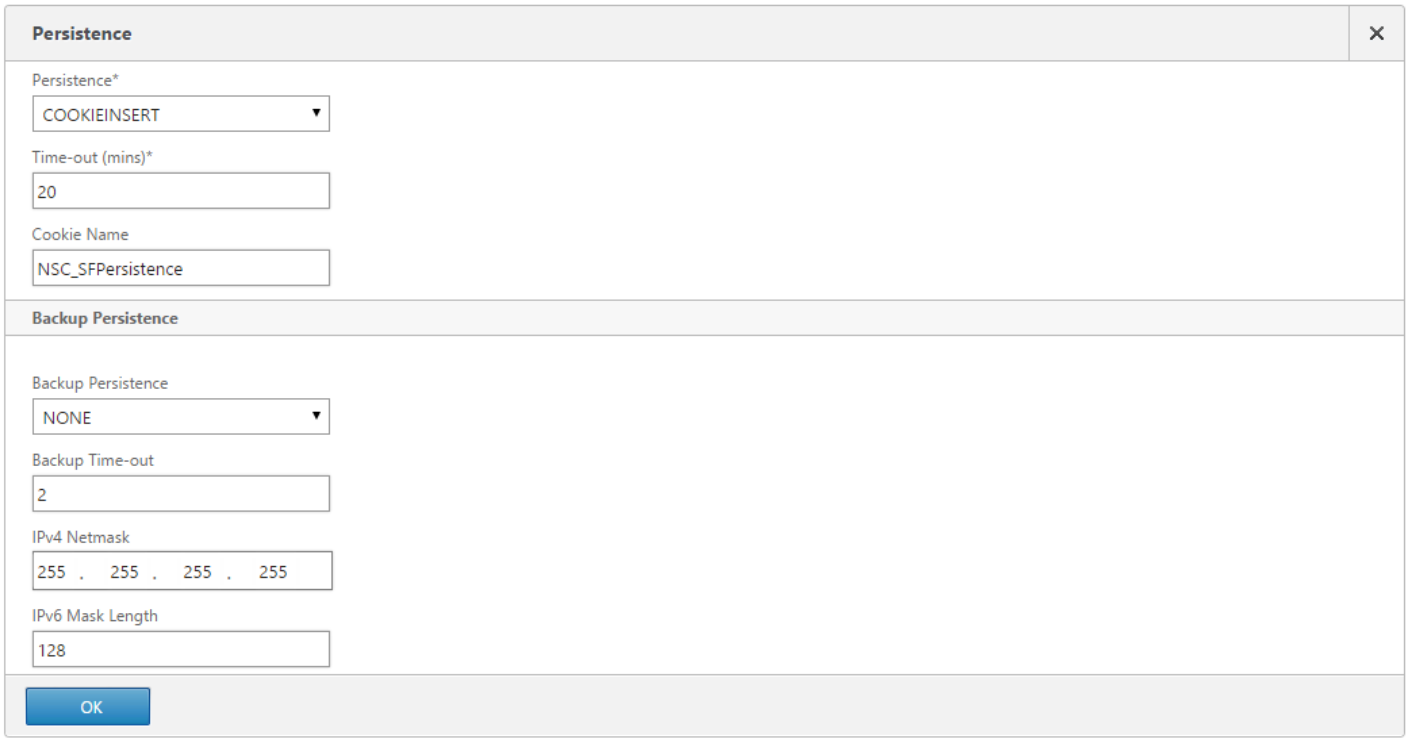
4. 将您之前创建的**服务组**绑定到负载平衡 vServer。

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 vServer。

6. 在负载平衡 vServer 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，负载平衡器与其后方的 StoreFront 3.0 服务器之间进行 HTTP 80 连接。

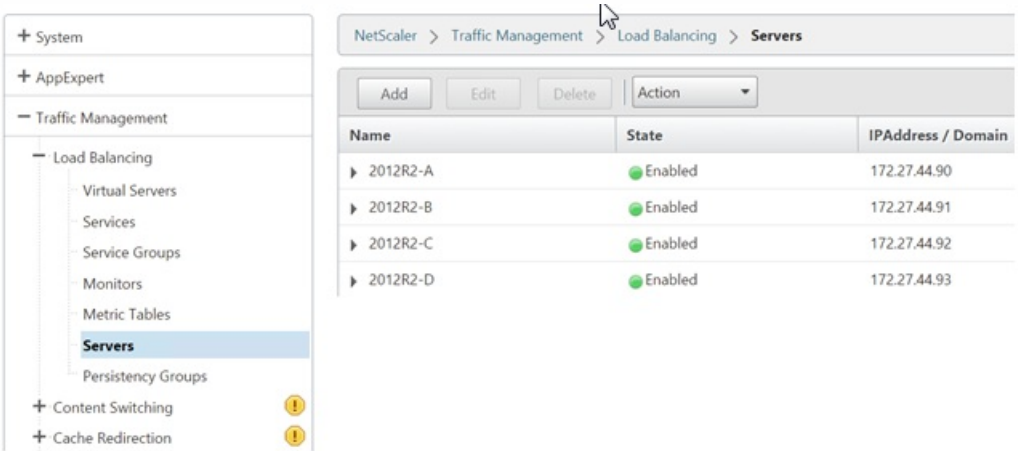
此方案使用默认的 StoreFront 监视器并使用端口 8000。

将单个 StoreFront 服务器添加到 NetScaler 负载平衡器

1. 登录 NetScaler 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. 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 NetScaler 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. 从下拉菜单中选择 **Type**（类型）为 **StoreFront**。
5. 在“Special Parameters”（特殊参数）选项卡下面，指定应用商店的名称。
6. 在目标端口中输入 **8000**，此端口匹配在各个 StoreFront 服务器上创建的默认监视器实例。
7. 勾选“Special Parameters”（特殊参数）选项卡下面的 **Check Backend Services**（检查后端服务）复选框。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 Service，探测操作会返回正在运行的所有 StoreFront Service 的状态。

创建包含所有 StoreFront 服务器的 HTTP 80 服务组

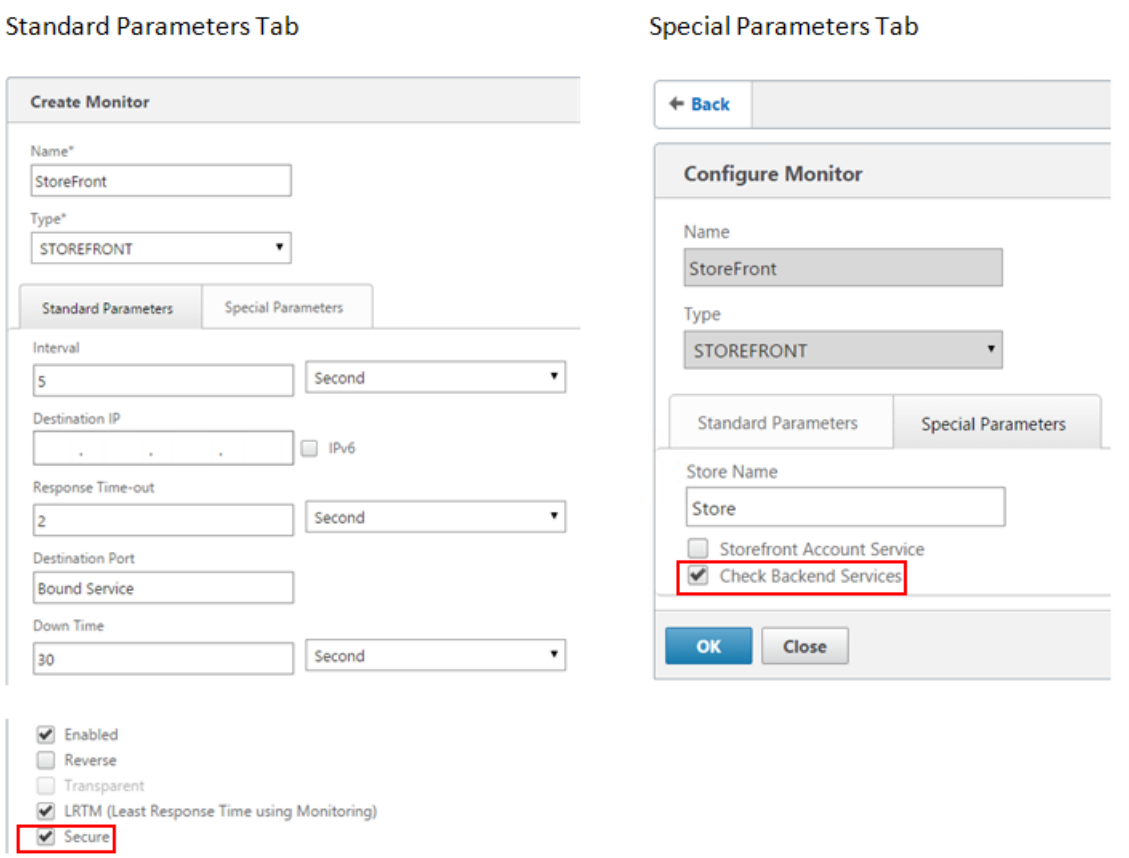
1. 在服务组内，选择右侧的“Members”（成员）选项，然后添加您之前在“Servers”（服务器）部分定义的所有 StoreFront 服务器节点。
2. 将 HTTP 端口设置为 80，并在添加服务器时为每台服务器分配一个唯一的服务器 ID。
3. 在“Monitors”（监视器）选项卡上，选择之前创建的 StoreFront 监视器。

创建用于用户流量的 HTTPS 终止负载平衡 vServer

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 vServer。
2. 选择 vServer 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 vServer。
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 vServer。

   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 vServer 菜单中，选择 **Persistence**（持久性），并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 vServer 以实现服务器组之间的订阅同步

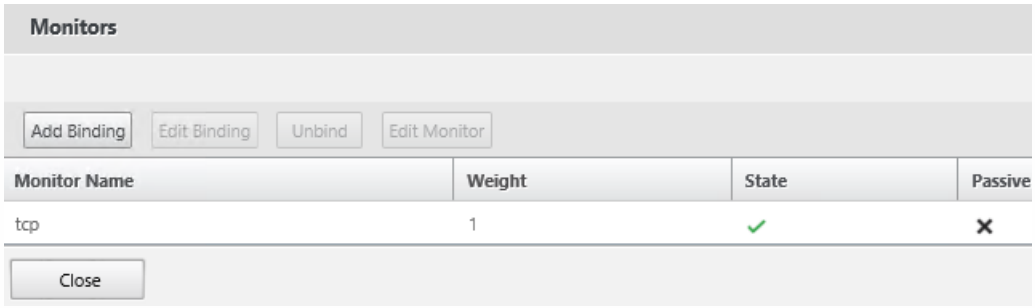
创建负载平衡 vServer 之前的注意事项：

- **选项 1**：创建单个 vServer：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 vServer 对：一个用于对用户流量进行负载平衡以执行已发布应用程序和桌面的 ICA 启动，另一个用于对订阅日期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 vServer 将失败。要为此服务提供高可用性，请在部署中的每个 NetScaler 上创建第二个 vServer，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 vServer 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。

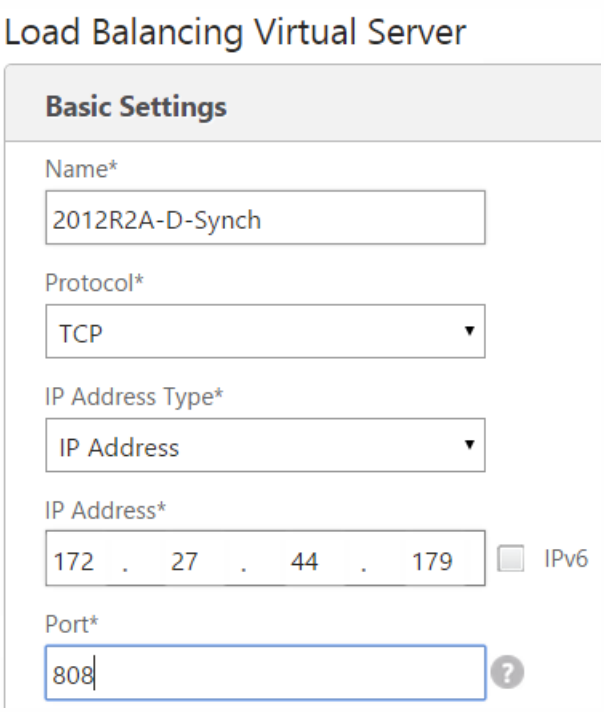
配置用于订阅同步的服务器组

1. 登录 NetScaler 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 **Monitors**（监视器）选项卡上，选择 TCP 监视器。



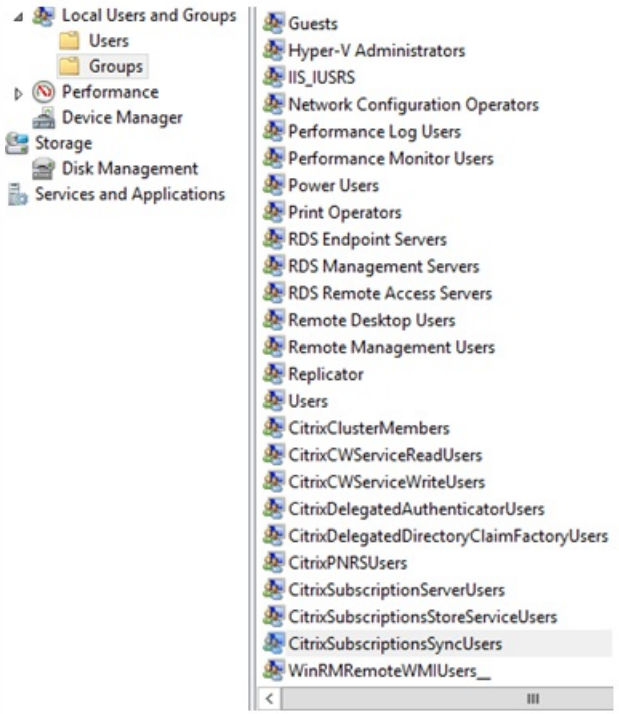
创建负载平衡 vServer 以实现服务器组之间的订阅同步

1. 登录 NetScaler 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** 作为端口号，请勿使用 **443**。



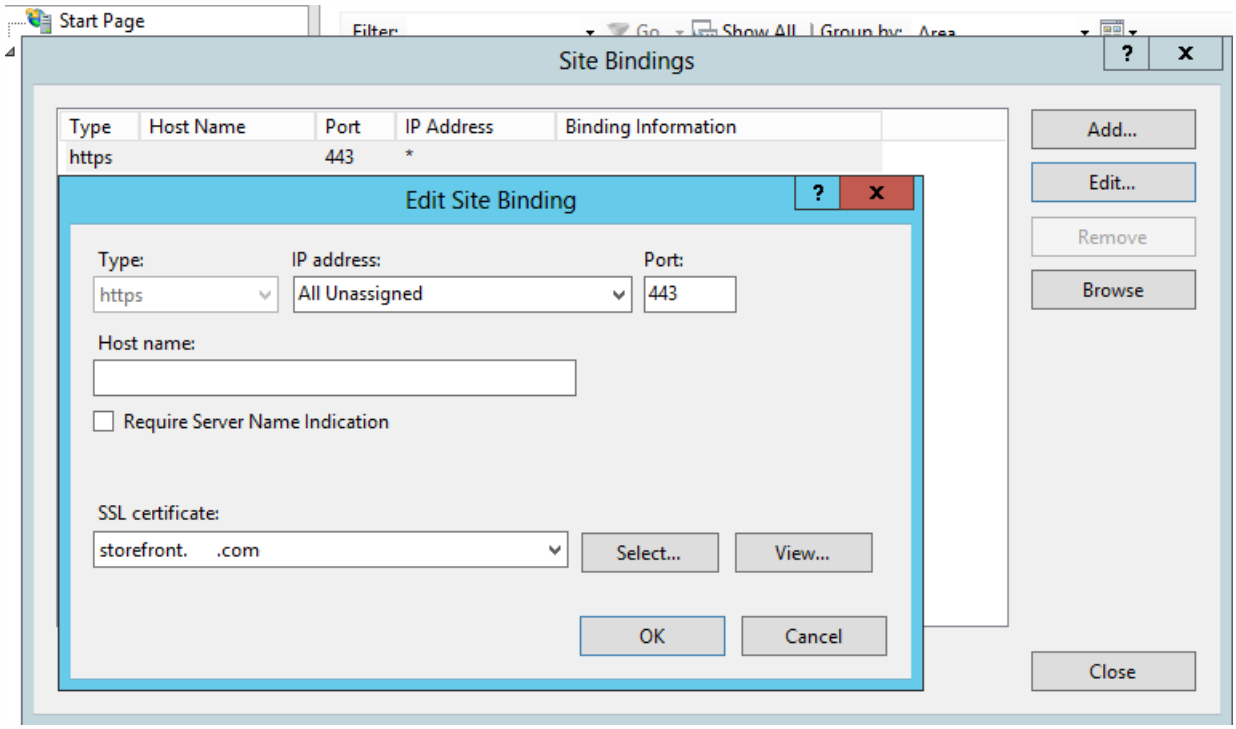
CitrixSubscriptionsSyncUsers 中的成员身份

位置 A 处的 **StoreFront 服务器 A** 要向另一个位置的 **服务器 B** 请求与获取订阅数据，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获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。



配置用于负载平衡的 StoreFront 服务器组

1. 将部署在 NetScaler 负载平衡 vServer 上的相同证书和私钥导入到服务器组的每个 StoreFront 节点上。
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。

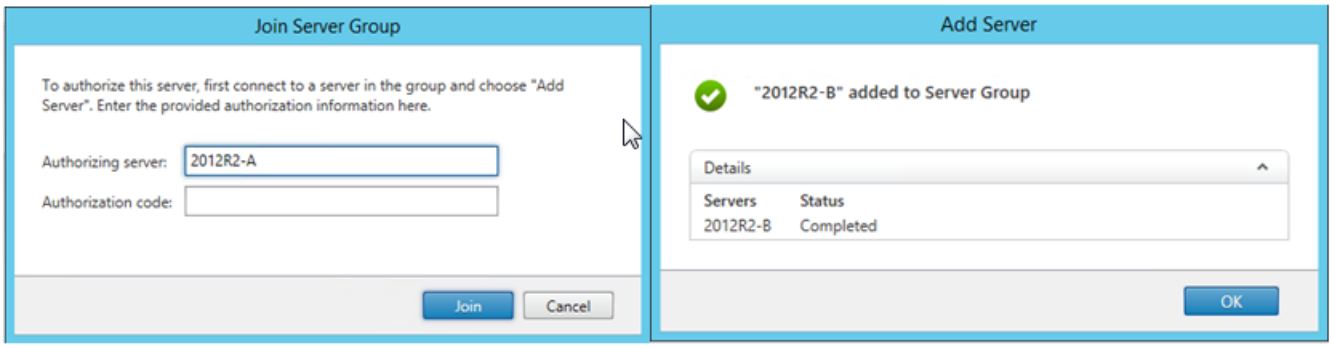


3. 在服务器组中的每个节点上安装 StoreFront。
4. 安装 StoreFront 期间，将主节点上的主机基 URL 设置为服务器组的所有成员使用的共享 FQDN。必须使用将负载平衡 FQDN 作为常用名称 (CN) 或使用者备用名称 (SAN) 包含在内的证书。

请参阅为 NetScaler 负载平衡器和 StoreFront 服务器创建服务器证书。

5. 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。

6. 选择**服务器组 > 添加服务器 > 复制加入服务器的授权代码**。



7. 将主节点的配置传播到组中的所有其他服务器组节点。

8. 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 服务监视器

要启用对 StoreFront 借以执行正确操作的 Windows 服务的运行状态进行外部监视，请使用 **Citrix 服务监视器** 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（如 NetScaler）从外部确定的 StoreFront 服务器部署的相对运行状态。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：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，请使用三个 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

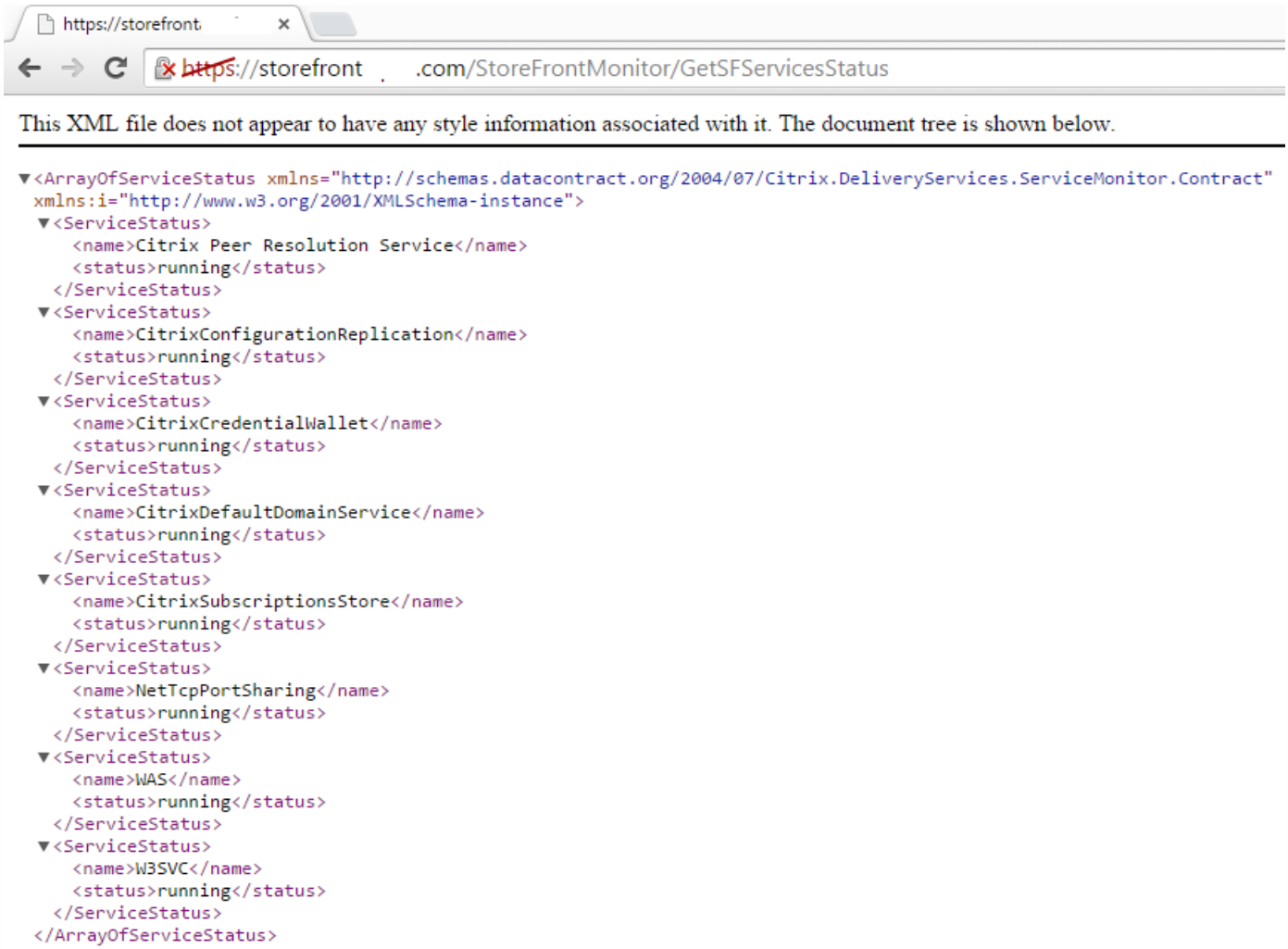
1. 打开主 StoreFront 服务器上的 PowerShell 集成脚本环境 (ISE)，然后运行以下命令以将默认监视器更改为 HTTPS 443。

```
$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 Service 状态的 XML 摘要。

https://:443/StoreFrontMonitor/GetSFServicesStatus

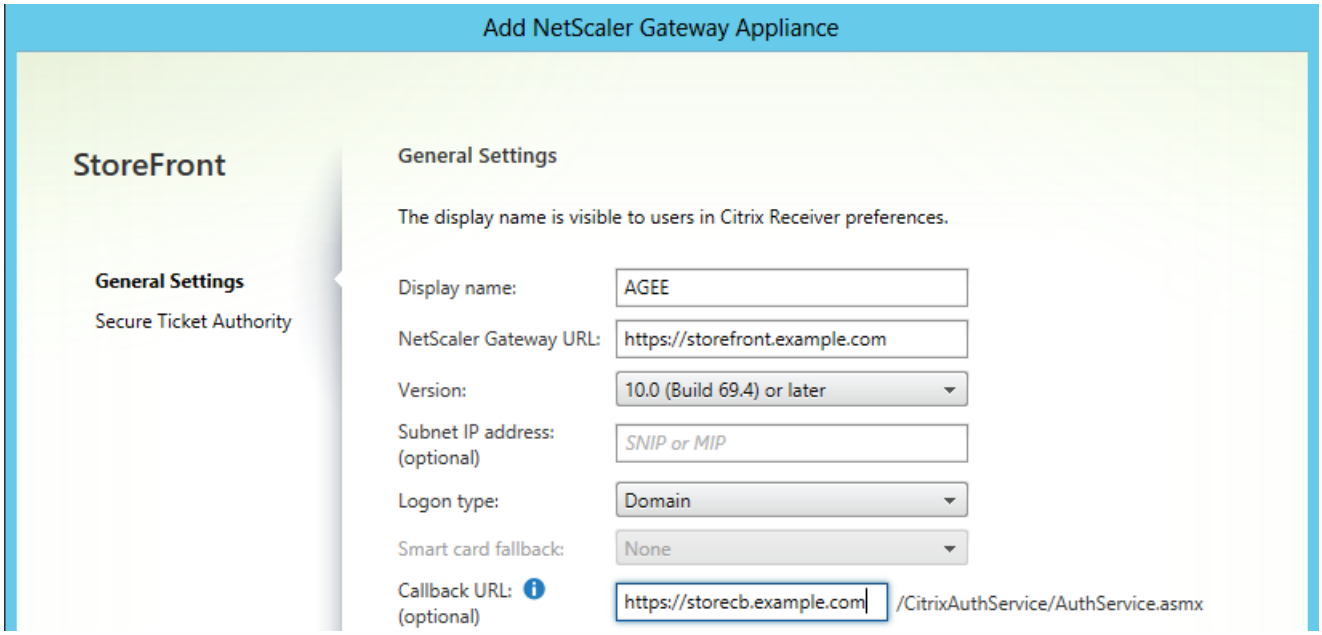


NetScaler Gateway 与负载平衡 vServers 位于同一 NetScaler 设备上

如果在同一个 NetScaler 设备上配置了 NetScaler Gateway vServer 和负载平衡 vServer，内部域用户尝试直接（而不是通过 NetScaler Gateway vServer）访问 StoreFront 负载平衡主机基 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 NetScaler Gateway 的子网 IP 地址 (SNIP) 相关联，StoreFront 会假定最终用户已经在 NetScaler Gateway 经过身份验证。这样会触发 StoreFront 尝试使用 AGBasic 协议执行 NetScaler Gateway 静默身份验证，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，以便使用用户名和密码身份验证而非 AGBasic。

在 StoreFront 服务器组上配置 NetScaler Gateway



使用 NetScaler 对 StoreFront 服务器组进行负载平衡时的环回选项

在之前的 StoreFront 版本中（如 2.6 或更低版本），Citrix 建议手动修改每个 StoreFront 服务器上的主机文件，以将负载平衡器的完全限定的域名 (FQDN) 映射到特定 StoreFront 服务器的环回地址或 IP 地址。这样可确保 Receiver for Web 始终与负载平衡部署中的同一服务器上的 StoreFront Service 进行通信。这是必需操作，因为 HTTP 会话是在 Receiver for Web 与身份验证服务之间的显式登录过程中创建的，并且 Receiver for Web 使用基本 FQDN 与 StoreFront Service 进行通信。如果基本 FQDN 解析为负载平衡器，负载平衡器可能会将流量发送到组中的其他 StoreFront 服务器，从而导致身份验证失败。此过程不会绕过负载平衡器，但 Receiver for Web 尝试访问与自身驻留在同一服务器上的应用商店服务时除外。

可以使用 PowerShell 设置环回选项。启用环回将无需在服务器组的每个 StoreFront 服务器上创建主机文件条目。

Receiver for Web web.config 文件示例：

PowerShell 命令示例：

& "c:\program files\Citrix\receiver storefront\scripts\ImportModules.ps1"

Set-DSLoopback -SiteId 1 -VirtualPath "/Citrix/StoreWeb" -Loopback "OnUsingHttp" -LoopbackPortUsingHttp 81

-Loopback 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 SSL-terminating 负载平衡器，则不使用此值。
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 SSL terminating 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。如果将环回设置为“On”，Fiddler 之类的工具无法捕获 Receiver for Web 与 StoreFront Service 之间的流量。

为同一 NetScaler Gateway 配置两个 URL

Nov 27, 2017

在 StoreFront 中，可以从 StoreFront 管理控制台的“管理 NetScaler Gateway”> “添加”或“编辑”来添加单个 NetScaler Gateway URL。也可以在“管理 NetScaler Gateway”>“从文件中导入”中添加公用 NetScaler 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 NetScaler Gateway 管理：

1. **GSLB 和多个 NetScaler Gateway**。可使用 GSLB 和多个 NetScaler 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 NetScaler Gateway**。可使用同一 NetScaler 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。如果您是初次了解 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 NetScaler 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 NetScaler 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。

使用两个网关 URL 时的部署注意事项

> **Important**
>
> 使用 -gslburl 参数配置第二个网关 URL 之前，Citrix 建议查看具有哪些服务器证书以及您的组织如何执行 DNS 解析。要在您的 NetScaler 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 从公司网络外部和内部访问已发布资源，或考虑是否接受两个不同的 URL，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。

或者

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

- **一组 XenApp 和 XenDesktop 7.x Delivery Controller 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 *.xendesktop.example.net。

  或者

  专门签名 SAN 服务器证书应包含具有四个 Controller 的 XenDesktop 站点所需的所有服务器 FQDN。

  XD1A. xendesktop.example.net

  XD1B. xendesktop.example.net

  XD2A. xendesktop.example.net

  XD2B. xendesktop.example.net

- **使用拆分 DNS 在内部和外部访问 NetScaler Gateway 的示例服务器证书**

  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 网关的示例服务器证书**

  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

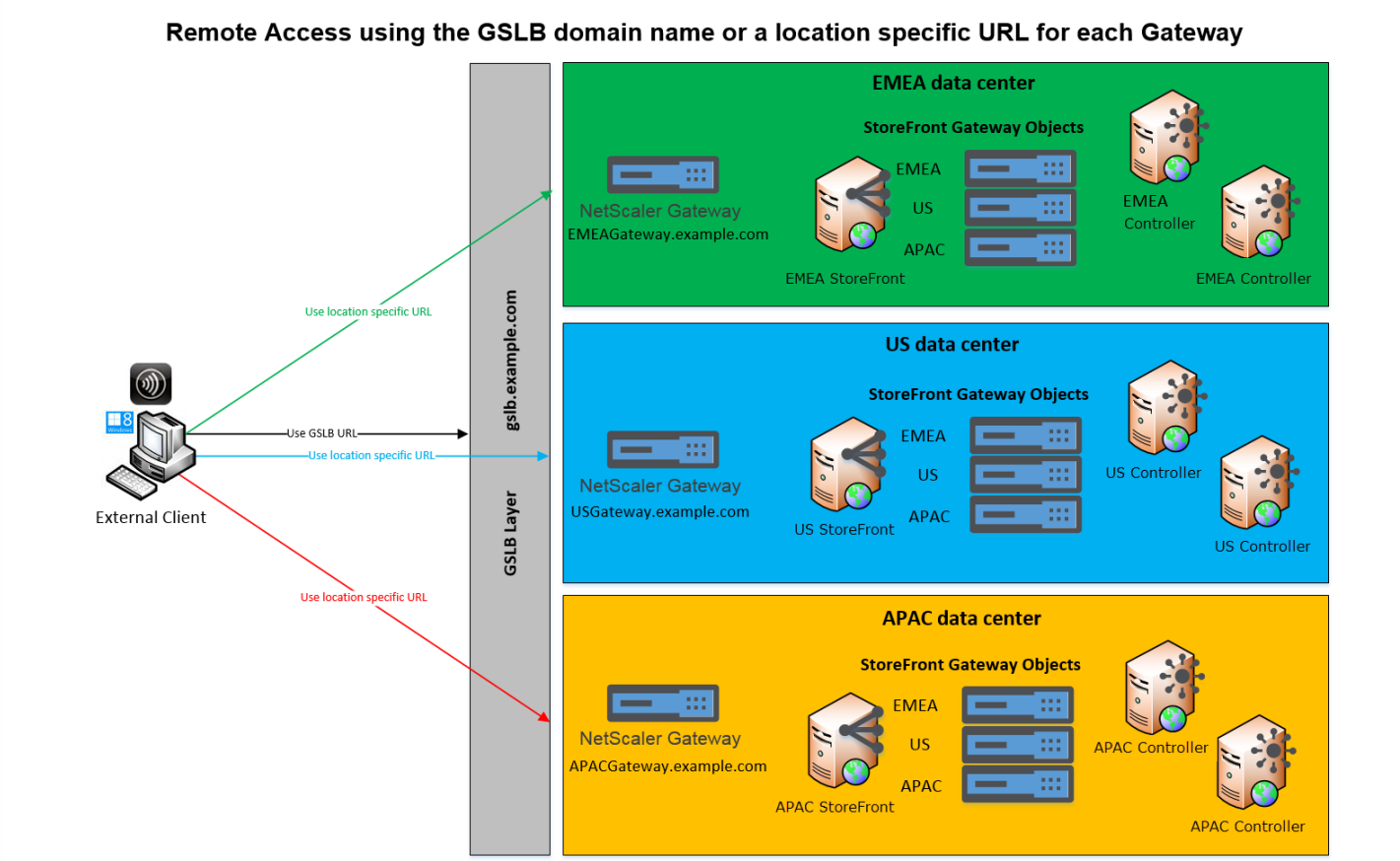
  usgateway.example.com

  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：GSLB 和多个 NetScaler Gateway

管理员可使用 GSLB 和多个 NetScaler 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。

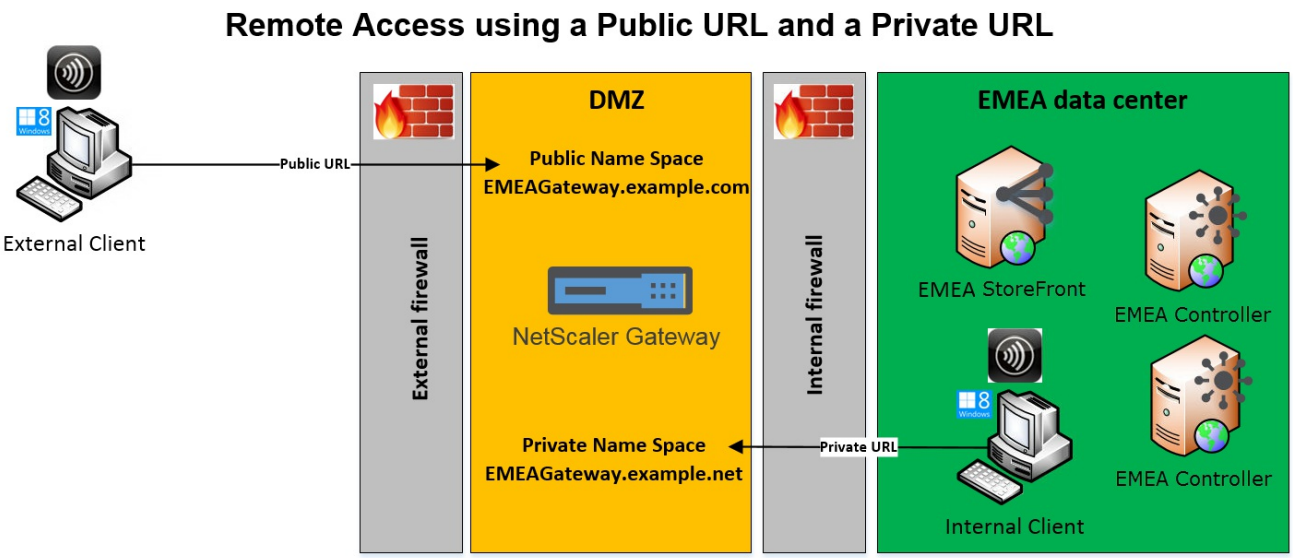


在此示例中：

- 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 NetScaler 上配置每个 GSLB 服务都表示一个网关 VPN vServer。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 NetScaler Gateway vServer。
- GSLB NetScaler 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 XenApp 和 XenDesktop 控制器失败，它们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 #2：使用公用 URL 或专用 URL 的单个 NetScaler Gateway

管理员可使用同一 NetScaler 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 NetScaler Gateway，即使客户端是内部的也是如此。
- NetScaler 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 NetScaler 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：

命令 复制

```
Add-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://emeagateway.example.com" -GSLBurl "https://gslb.example.cor

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-STFRoamingGatway** 之后可以通过 $EMEAGateway 传输以更新 StoreFront 配置并删除 GSLBurl。

命令 复制

```
$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:

命令 复制

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:

命令 复制

```
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：

命令 复制

```
$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 或内部 URL 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

用例 #2：漫游 web.config 文件中的网关

针对委派表单身份验证 (DFA) 配置 NetScaler 和 StoreFront

Nov 27, 2017

可扩展的身份验证为基于 NetScaler 和 StoreFront 表单的身份验证扩展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 NetScaler 和 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，NetScaler 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。

安装建议

- 要确保 NetScaler 和 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，NetScaler 将 StoreFront 服务器证书的发行方作为可信证书颁发机构。

StoreFront 群集安装注意事项

- 将第三方身份验证插件安装在所有节点上，然后再将其联合到一起。
- 在一个节点上配置所有委派表单身份验证相关设置，然后将更改传播到其他节点。 请参阅“启用委派表单身份验证”。

启用委派表单身份验证

因为 StoreFront 中没有用于设置 Citrix 预共享密钥设置的 GUI，所以请使用 PowerShell 控制台安装委派表单身份验证。

1. 安装委派表单身份验证。默认情况下其并未安装，您需要使用 PowerShell 控制台进行安装。

```
PS C:\Users\administrator.PTD.000> cd 'C:\Program Files\Citrix\Receiver StoreFront\Scripts'
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> & .\ImportModules.ps1
Adding snapins
Importing modules
Loading 'C:\Program Files\Citrix\Receiver StoreFront\\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'
Loading 'C:\Program Files\Citrix\Receiver StoreFront\\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'

PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Install-DSDFAServer
Id                          : bf694fbc-ae0a-4d56-8749-c945559e897a
ClassType                   : e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc
FrameworkController         : Citrix.DeliveryServices.Framework.FileBased.FrameworkController
ParentInstance              : 8dd182c7-f970-466c-ad4c-27a5980f716c
RootInstance                : 5d0cdc75-1dee-4df7-8069-7375d79634b3
TenantId                    : 860e9401-39c8-4f2c-928d-34251102b840
Data                        : {}
ReadOnlyData                : {[Name, DelegatedFormsServer], [Cmdlet, Add-DSWebFeature], [Snapin, Citrix.DeliverySer
                              vices.Web.Commands], [Tenant, 860e9401-39c8-4f2c-928d-34251102b840]}
ParameterData               : {[FeatureClassId, e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc], [ParentInstanceId, 8dd182c7-f
                              970-466c-ad4c-27a5980f716c], [TenantId, 860e9401-39c8-4f2c-928d-34251102b840]}
AdditionalInstanceDependencies : {b1e48ef0-b9e5-4697-af9b-0910062aa2a3}
IsDeployed                  : True
FeatureClass                : Citrix.DeliveryServices.Framework.Feature.FeatureClass
```

2. 添加 Citrix 受信客户端。配置 StoreFront 和 NetScaler 之间的共享秘密密钥（暗码）。您的暗码和客户端 ID 必须与在 NetScaler 中配置的相同。

```
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。

4. 在 PowerShell 中，设置委派表单身份验证对话工厂。本例中设置为 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

Nov 27, 2017

某些组织配置了一些策略，这些策略不允许您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 NetScaler 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 NetScaler Gateway 进行身份验证”不受支持。对于本机桌面或移动 Citrix Receiver，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：

- NetScaler 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：

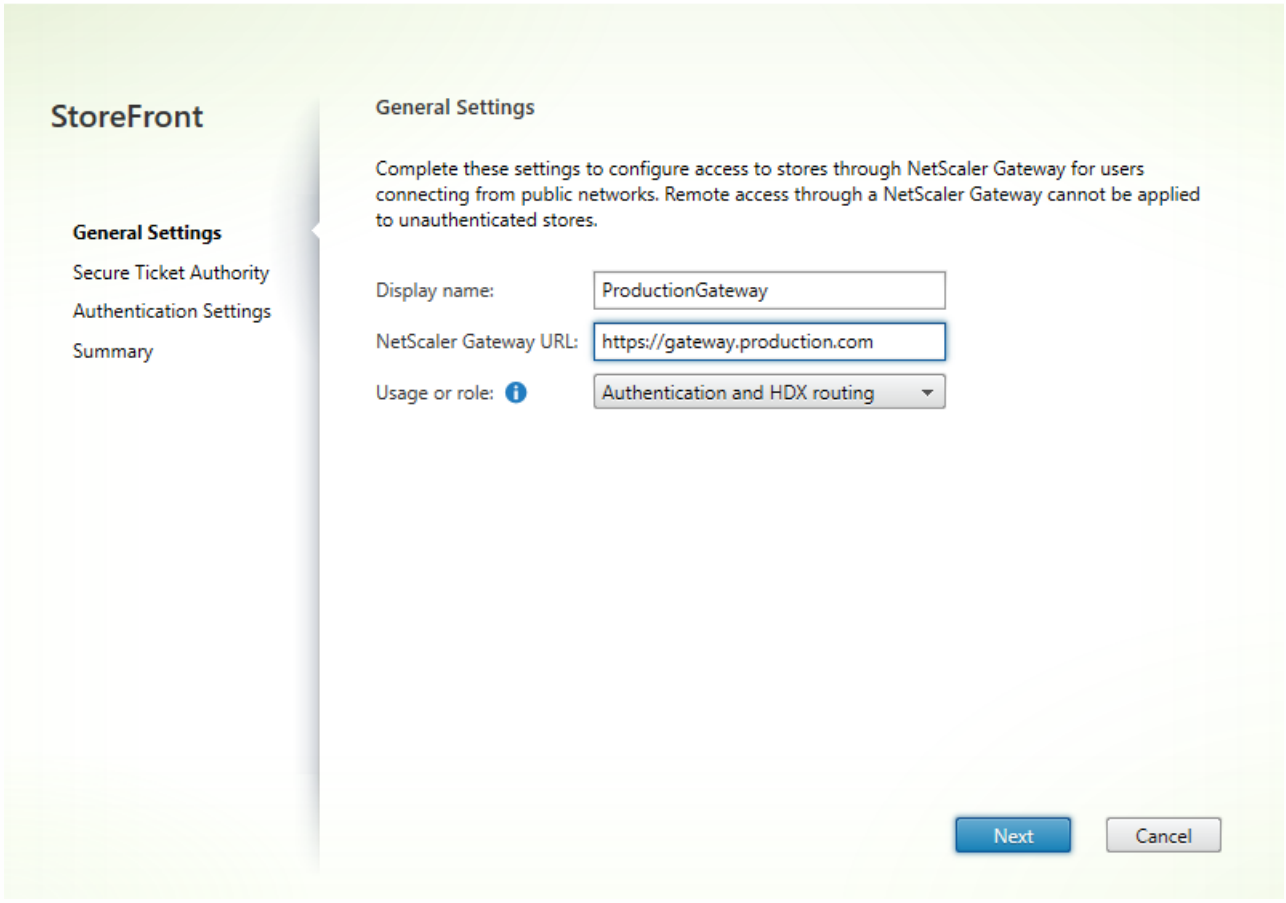
- StoreFront、XenApp 和 XenDesktop 7.0 或更高版本以及 VDA 都位于 development.com 域中。
- 对 Citrix Receiver for Web 站点进行的身份验证使用 development\testuser1 帐户和密码进行。
- 这两个域之间不存在信任关系。

为应用商店配置 NetScaler Gateway

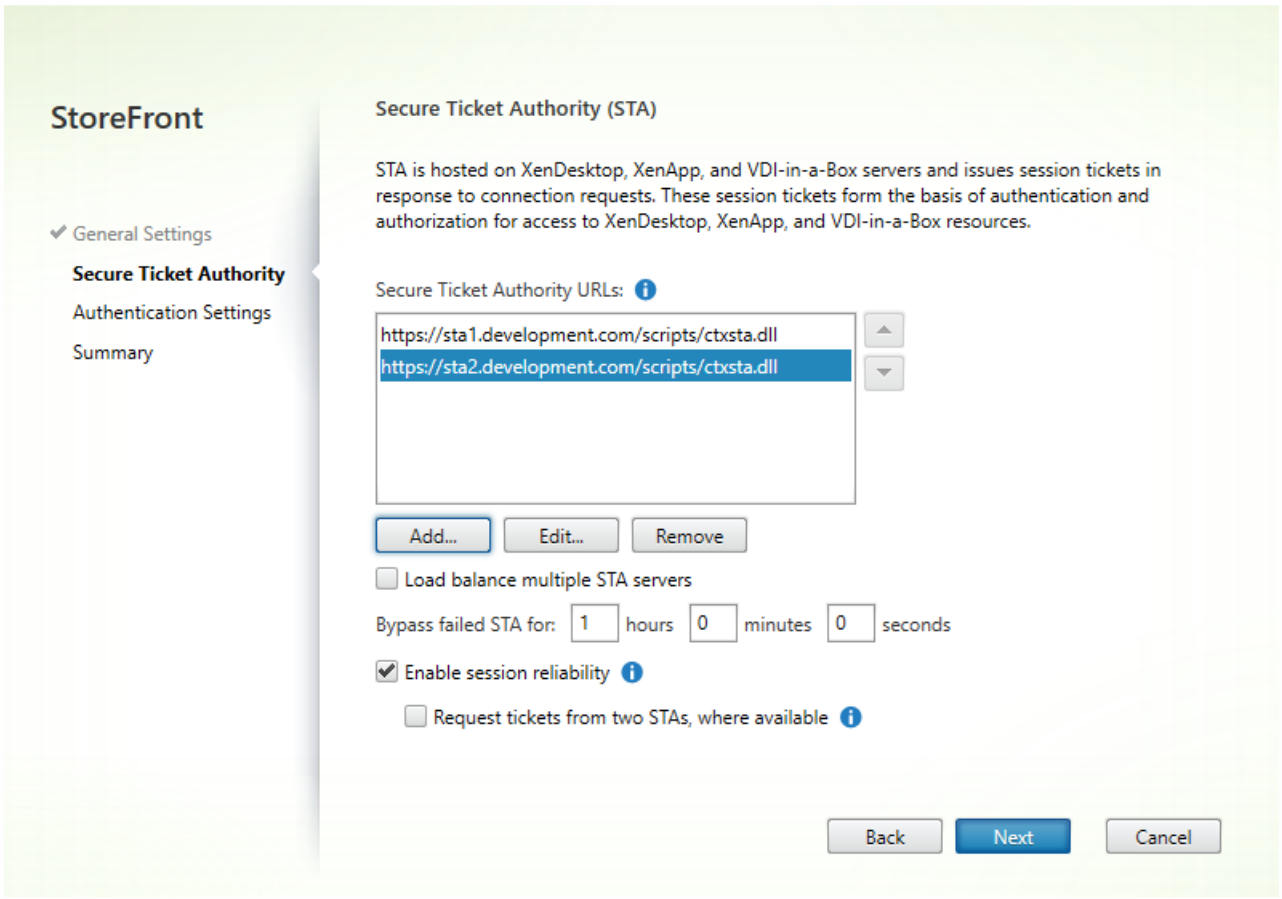
要为应用商店配置 NetScaler Gateway，请执行以下操作：

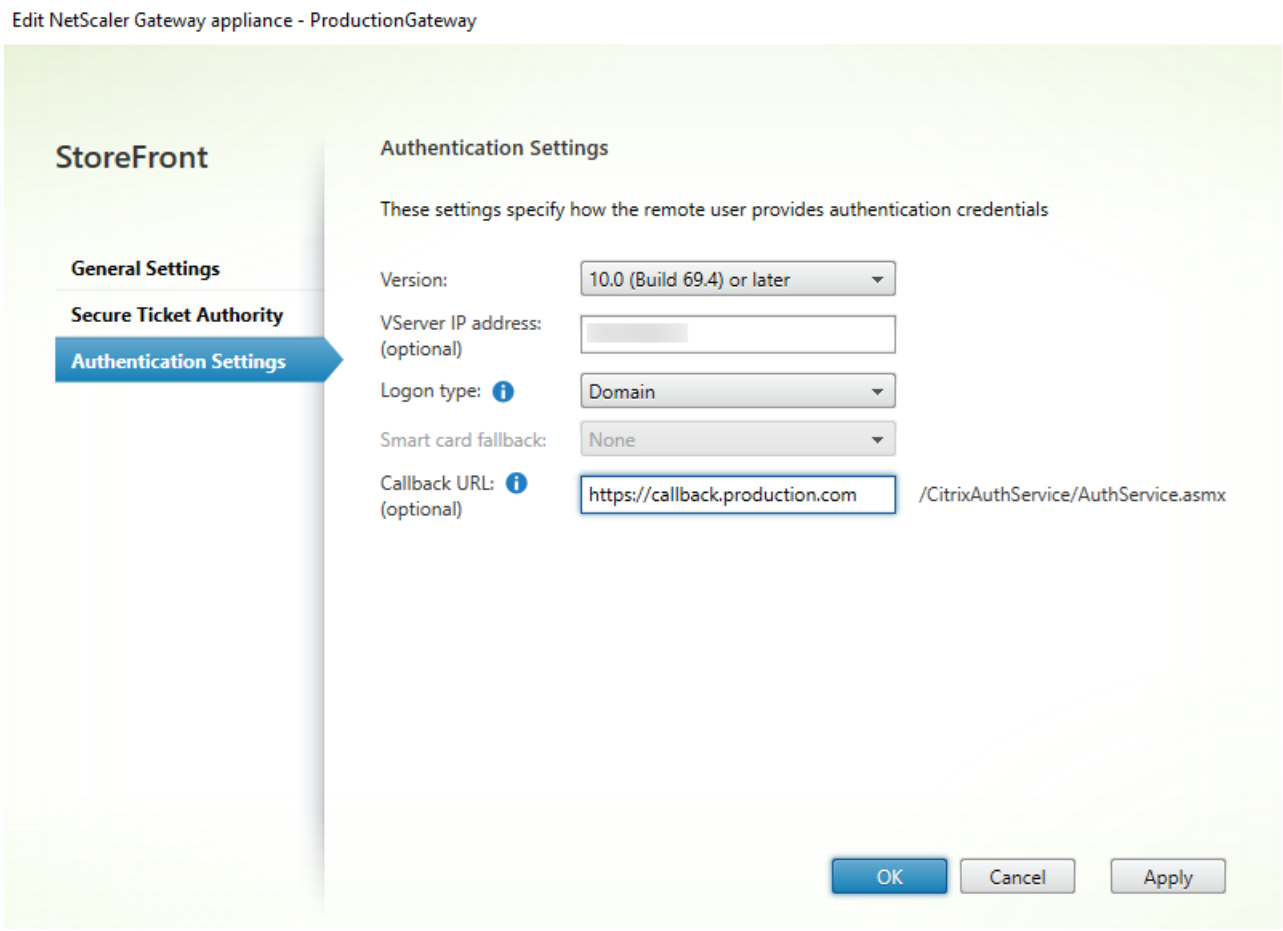
1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择**应用商店**，然后在**操作**窗格中单击**管理 NetScaler Gateway**。
2. 在“管理 NetScaler Gateway”屏幕中，单击**添加**按钮。
3. 完成“常规设置”、“Secure Ticket Authority”和“身份验证”步骤。

Add NetScaler Gateway Appliance



Add NetScaler Gateway Appliance



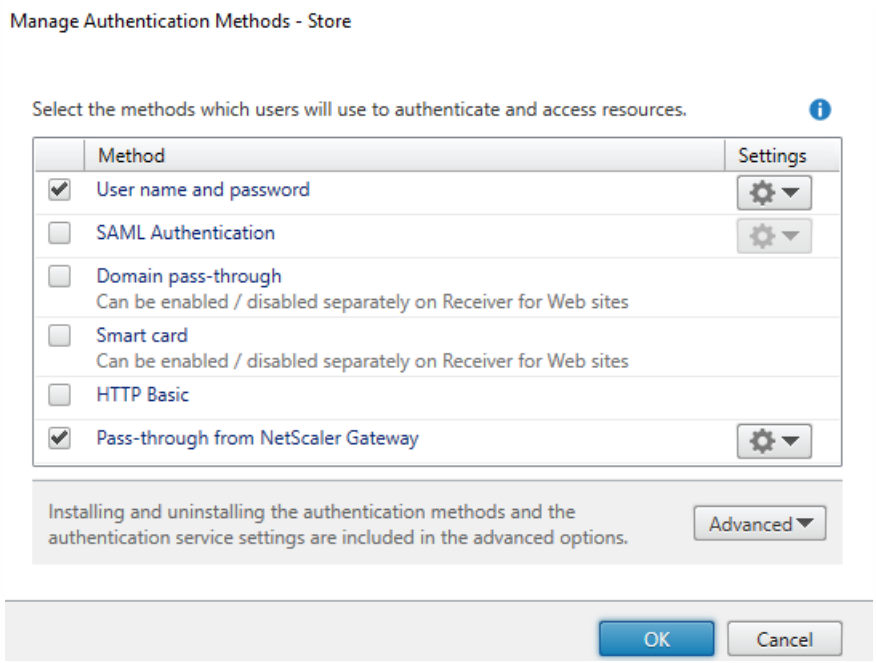


注意

可能需要添加 DNS 条件转发器，以便这两个域中正在使用的 DNS 服务器可以解析另一个服务器上的 FQDN。NetScaler 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 NetScaler Gateway vServer 的虚拟 IP (VIP)。

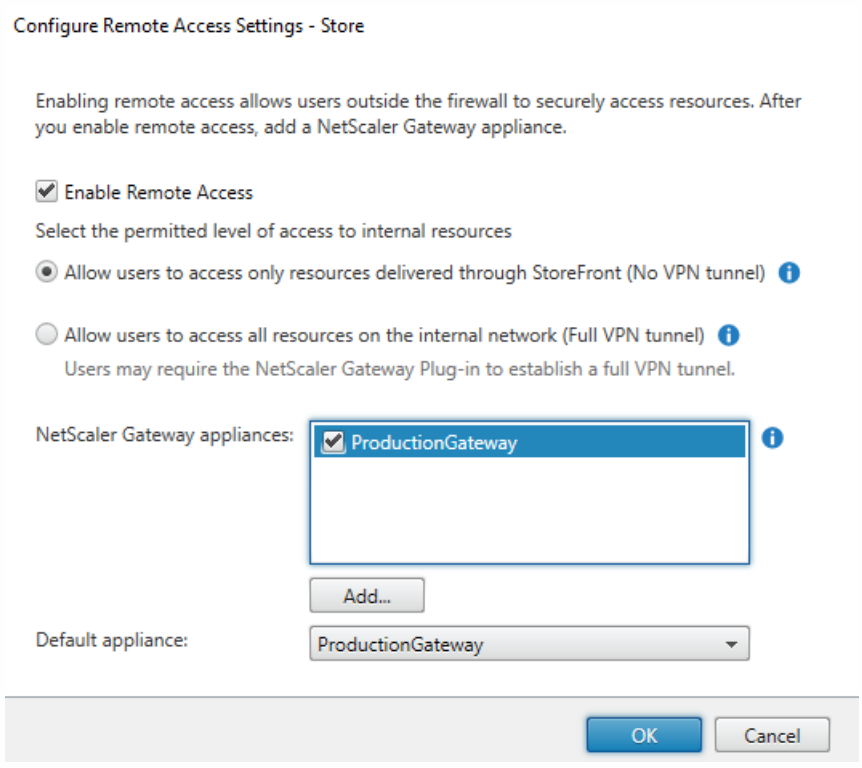
启用从 NetScaler Gateway 直通

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 NetScaler 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

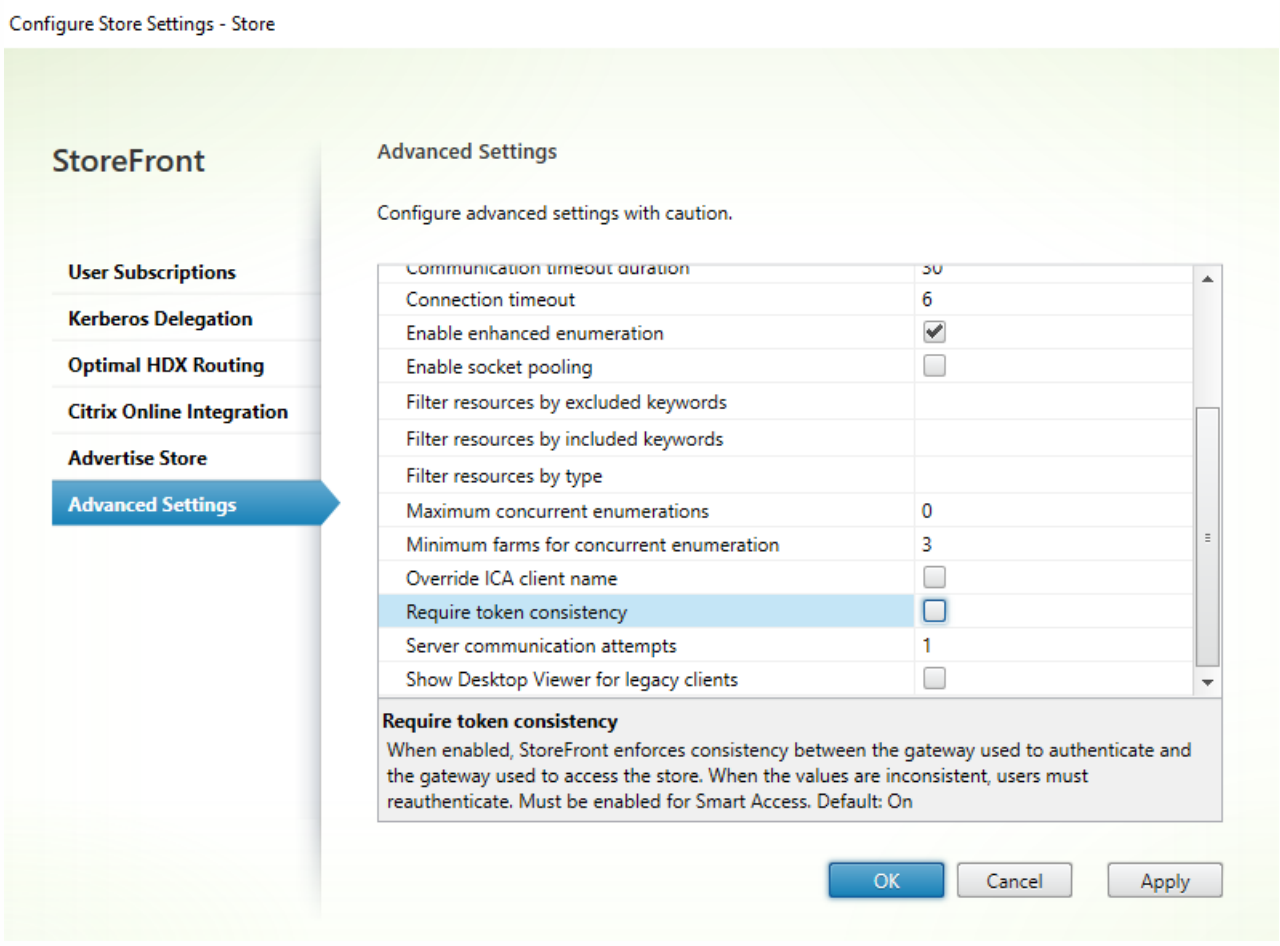
1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择**应用商店**节点，然后在结果窗格中选择一个应用商店。在**操作**窗格中，单击**配置远程访问设置**。
2. 选择**启用远程访问**。
3. 请确保您已在自己的应用商店中注册 NetScaler Gateway。如果未注册 NetScaler Gateway，STA 票证将不起作用。



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

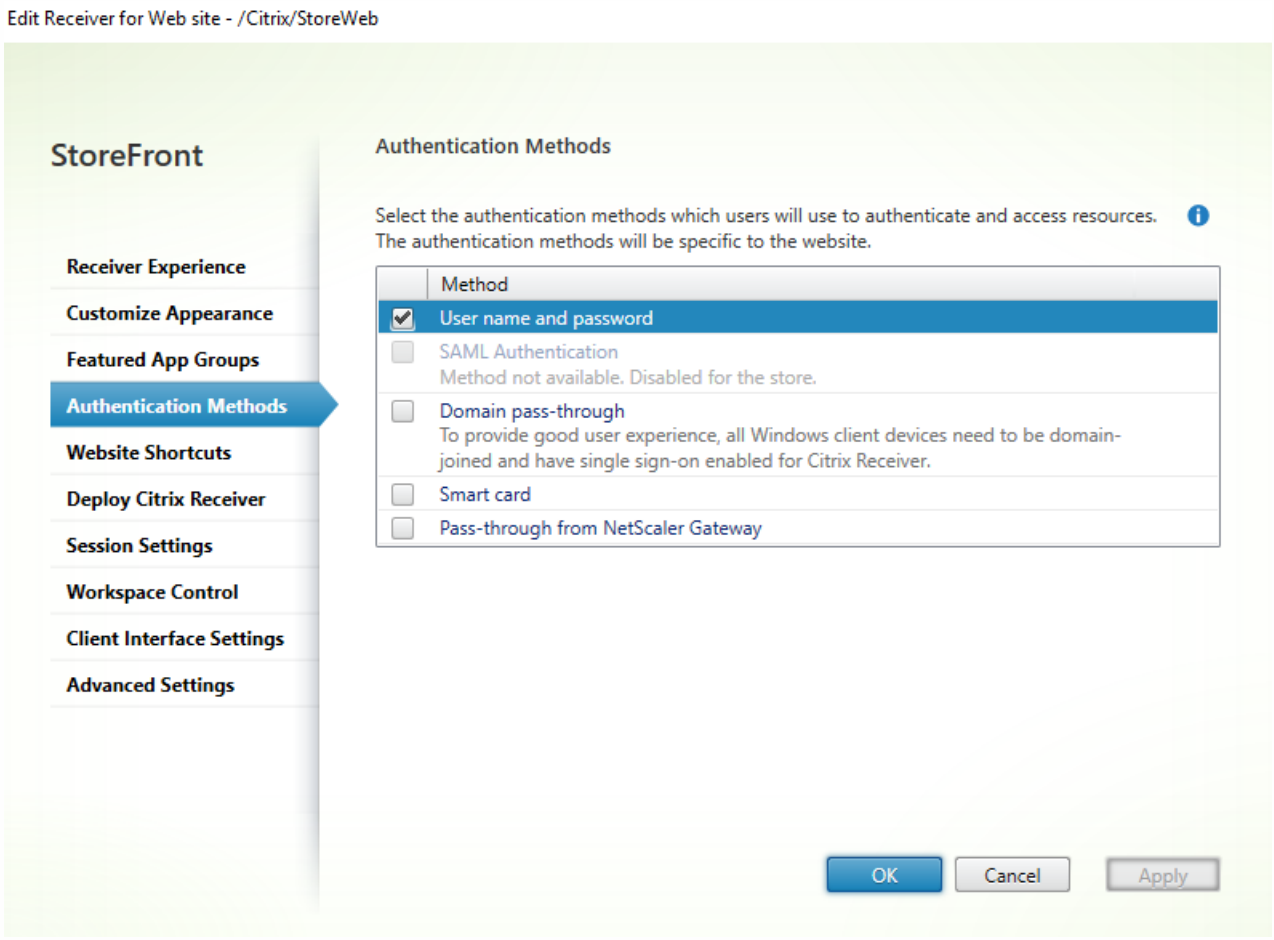
“要求令牌一致”设置默认处于选中状态。如果禁用此设置，用于 NetScaler 端点分析 (EPA) 的 SmartAccess 功能将停止运行。有关 SmartAccess 的详细信息，请参阅 CTX138110。

对 Receiver for Web 站点禁用从 NetScaler Gateway 直通

Important

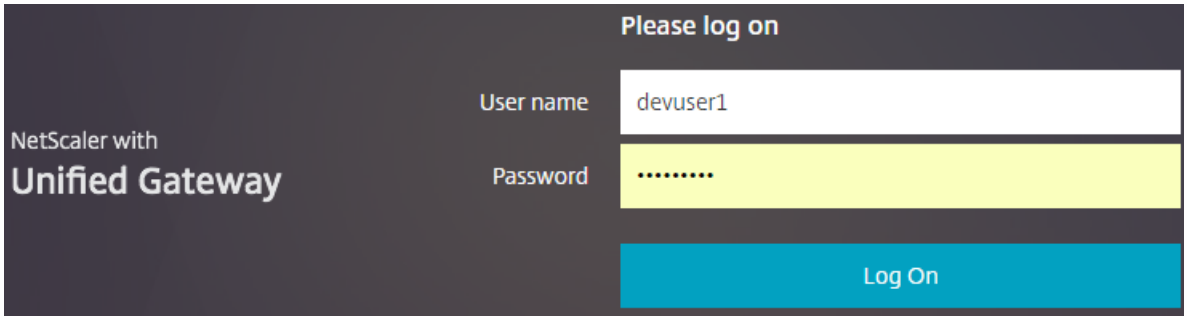
禁用从 NetScaler Gateway 直通将阻止 Receiver for Web 尝试使用 production.com 域中不正确的凭据从 NetScaler 通过。禁用从 NetScaler Gateway 直通会导致 Receiver for Web 提示用户输入凭据。这些凭据与用于通过 Netscaler Gateway 登录的凭据不同。

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“身份验证方法”中，取消选中“从 NetScaler Gateway 直通”复选框。
5. 单击**确定**。

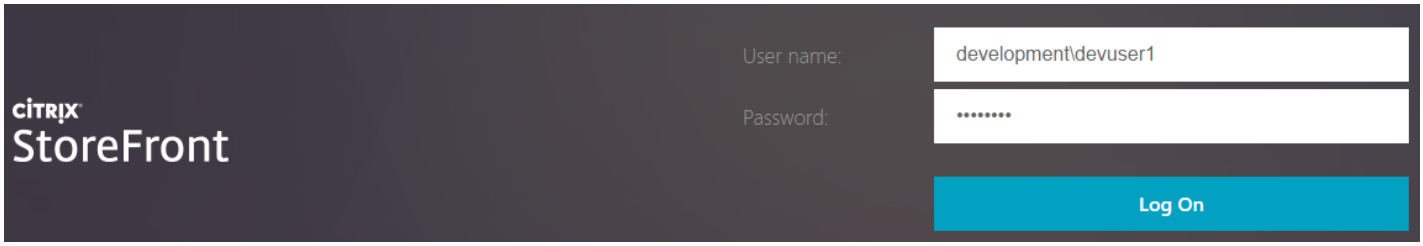


使用 production.com 用户和凭据登录网关

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。

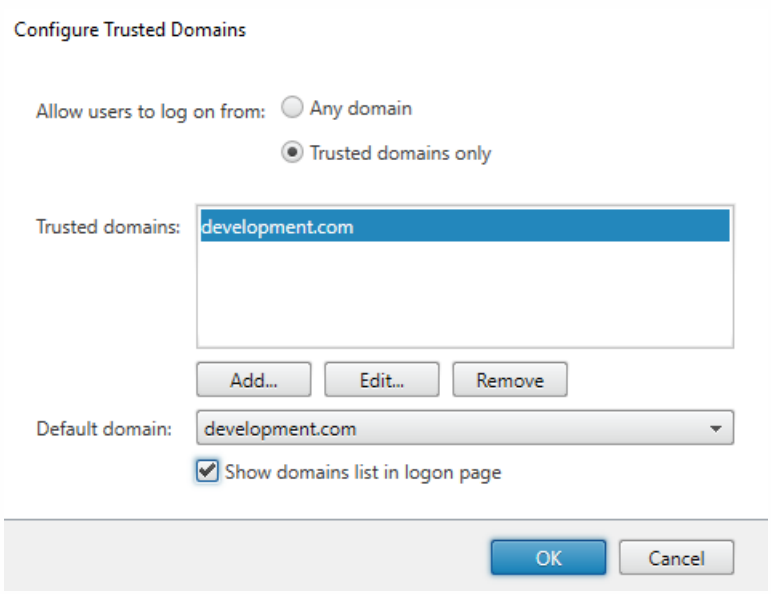


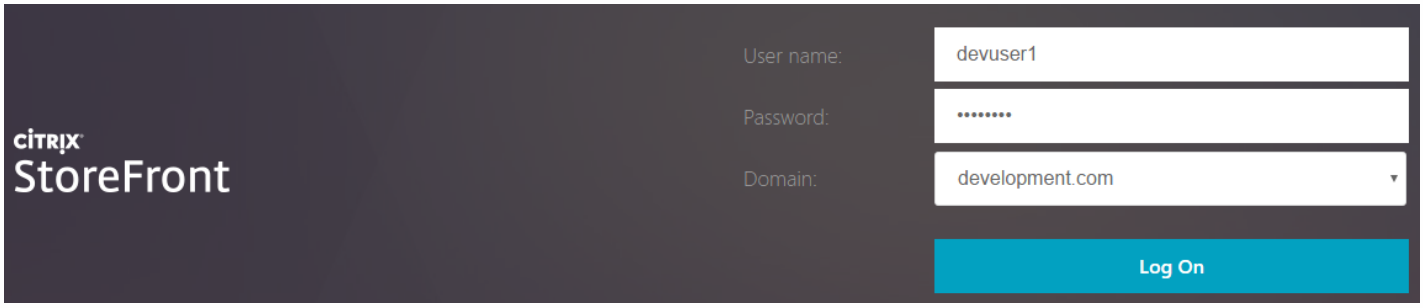
在 StoreFront 中添加可信域下拉列表（可选）

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 NetScaler 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 NetScaler 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**添加 development.com 作为可信域，然后选中**在登录页面中显示域列表**复选框。
4. 单击**确定**。



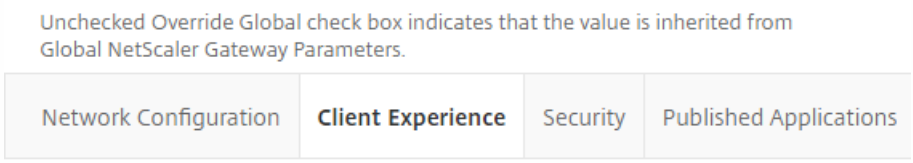


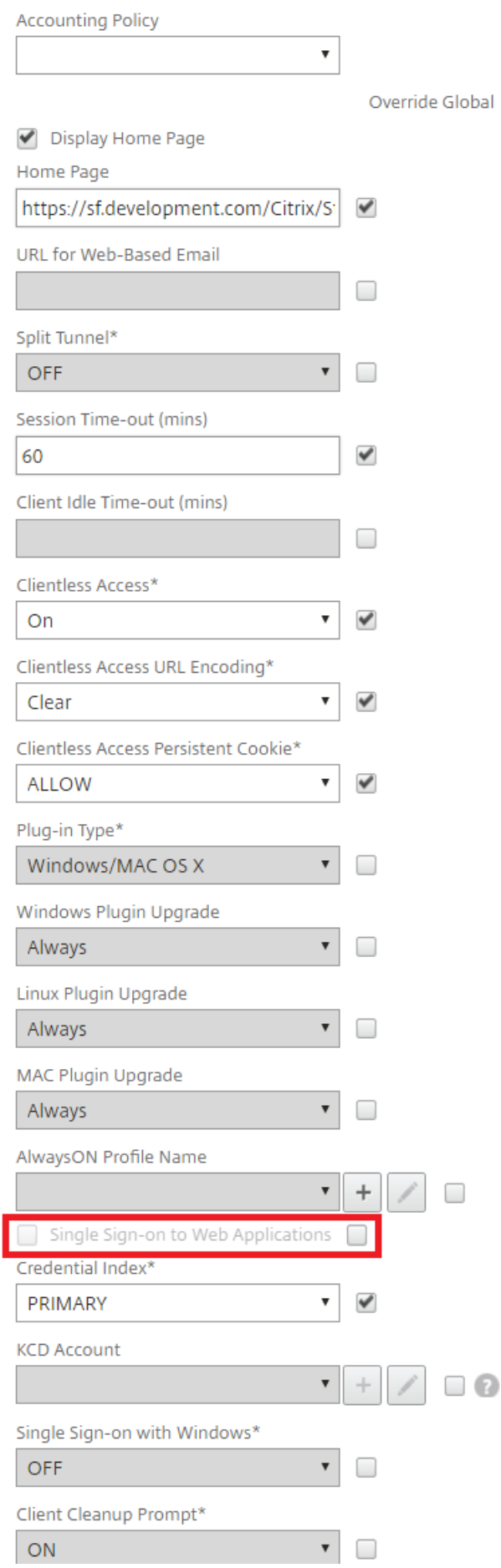
注意

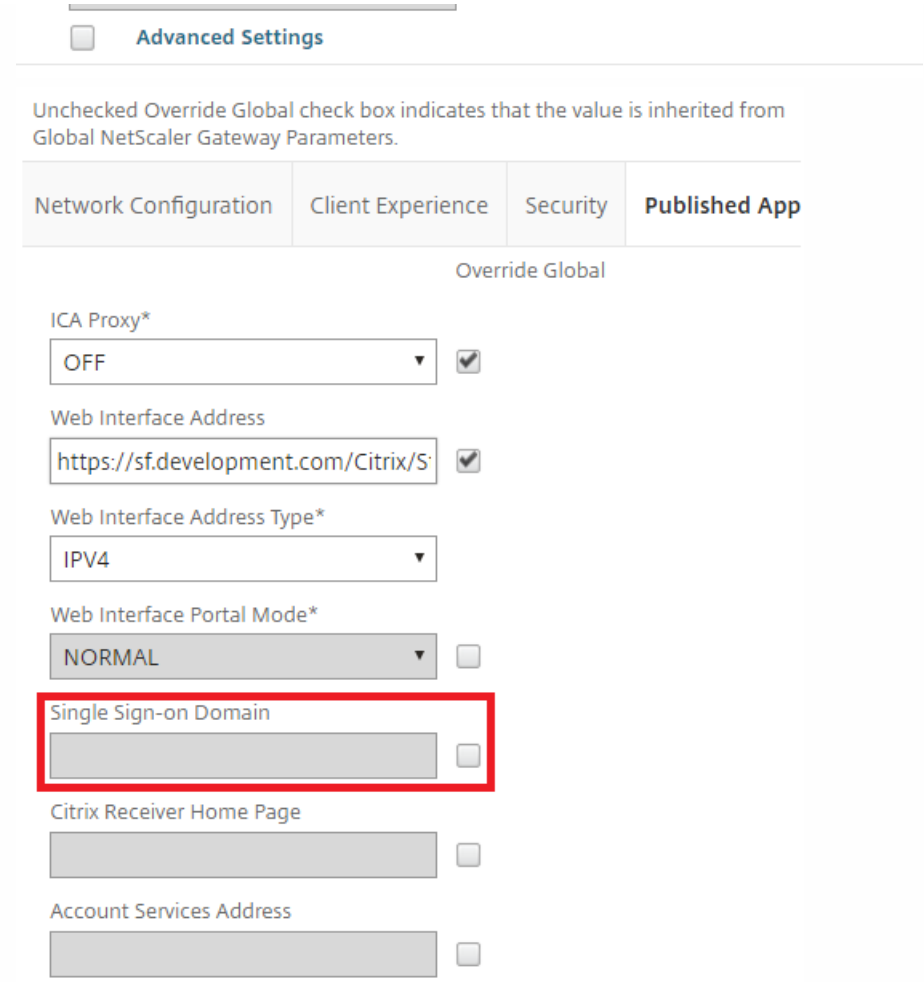
不建议在此身份验证场景中使用浏览器密码缓存。如果用户为两个不同的域帐户设置了不同的密码，密码缓存会导致体验较差。

NetScaler 无客户端 VPN (CVPN) 会话操作策略

- 如果在您的 NetScaler 会话策略中启用了“单点登录到 Web 应用程序”，NetScaler 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 NetScaler 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 NetScaler 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

Nov 27, 2017

可以通过执行管理信标任务指定内部网络之内和之外要用作信标点的 URL。Citrix Receiver 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 Receiver。这可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 Receiver 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，但位于公司网络外部。因此，用户必须通过 NetScaler Gateway 连接桌面和应用程序。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 NetScaler 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 NetScaler 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 Receiver 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中获取更新过的 Citrix Receiver 置备文件。否则，可以为应用商店导出置备文件，并将此文件设置为对用户可用。

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，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。
   - 要对您的 StoreFront 部署使用服务器 URL 或负载平衡的 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。选择列表中的一个 URL，然后单击删除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 Receiver 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。

高级配置

Nov 27, 2017

StoreFront 允许可以使用 StoreFront 控制台、PowerShell、证书属性或配置文件配置的高级选项。

配置桌面设备站点	创建、删除和修改桌面设备站点。
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	通过 NetScaler 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。
配置资源过滤	根据资源类型和关键字过滤枚举资源。

配置桌面设备站点

Nov 27, 2017

以下任务说明了如何创建、删除和修改桌面设备站点。要创建或删除站点，请执行 Windows PowerShell 命令。通过编辑站点配置文件，可更改桌面设备站点设置。

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，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：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。

创建或 删除桌面设备站点

通过每个桌面设备站点只能访问一个应用商店。 您可以创建一个应用商店，将希望通过未加入域的桌面设备提供给用户的所有资源包含在内。 也可以创建单独的应用商店，每个应用商店具有一个桌面设备站点，并对用户的桌面设备进行配置，使其连接到合适的站点。

1. 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键入以下命令以导入 StoreFront 模块。
   & "installationlocation\Scripts\ImportModules.ps1"
   其中 installationlocation 是 StoreFront 的安装目录，通常为 C:\Program Files\Citrix\Receiver StoreFront\。

2. 要创建 新的桌面设备站点，请键入以下命令。
   Install-DSDesktopAppliance -FriendlyName sitename -SiteId iisid
   -VirtualPath sitepath -UseHttps {$False | $True}
   -StoreUrl storeaddress [-EnableMultiDesktop {$False | $True}]
   [-EnableExplicit {$True | $False}] [-EnableSmartCard {$False | $True}]
   [-EnableEmbeddedSmartCardSSO {$False | $True}]
   其中 sitename 是方便用户识别桌面设备站点的名称。 对于 iisid，请指定托管 StoreFront 的 Microsoft Internet Information Services (IIS) 站点的数字 ID，该值可从 Internet Information Services (IIS) 管理器控制台获取。 将 sitepath 替换为应在 IIS 中创建的站点的相对路径，例如 /Citrix/DesktopAppliance。 请注意，桌面设备站点 URL 区分大小写。

   通过将 -UseHttps 设为适当值来指示是否将 StoreFront 配置为使用 HTTPS。

   要指定 Desktop Appliance Connector 站点使用的应用商店服务的绝对 URL，请使用 StoreUrl storeaddress。 此值针对管理控制台中的“应用商店”摘要显示。

   默认情况下，当用户登录到桌面设备站点时，用户可用的第一个桌面将自动启动。 要配置新的桌面设备站点以支持用户在多个桌面（如果可用）之间进行选择，请将 -EnableMultiDesktop 设为 $True。

   默认情况下，为新站点启用显式身份验证。 可通过将 -EnableExplicit 参数设为 $False，禁用显式身份验证。 通过将 -EnableSmartCard 设为 $True 可启用智能卡身份验证。要启用使用智能卡的直通身份验证，必须同时将 -EnableSmartCard 和 -EnableEmbeddedSmartCardSSO 设为 $True。 如果您启用显式身份验证和智能卡身份验证或使用智能卡的直通身份验证，则会在用户初次登录时提示用户使用智能卡登录，但如果他们在使用智能卡时遇到问题，则会退回到显式身份验证。

   通过可选参数配置的设置在桌面设备站点创建之后还可通过编辑站点配置文件进行修改。

   示例：

   在默认 IIS Web 站点中的虚拟路径 /Citrix/DesktopAppliance1 下创建一个 Desktop Appliance Connector 站点。

```
Install-DSDesktopAppliance `

-FriendlyName DesktopAppliance1 `

-SiteId 1 `

-VirtualPath /Citrix/DesktopAppliance1 `

-UseHttps $false `

-StoreUrl https://serverName/Citrix/Store `

-EnableMultiDesktop $true `

-EnableExplicit $true `

-EnableSmartCard $true `

-EnableEmbeddedSmartCardSSO $false
```

3. 要删除 现有的桌面设备站点，请键入以下命令。
   Remove-DSDesktopAppliance -SiteId iisid -VirtualPath sitepath
   其中 iisid 为托管 StoreFront 的 IIS 站点的数字 ID 号， sitepath 为 IIS 中桌面设备站点的相对路径，例如，/Citrix/DesktopAppliance。

4. 要列出 StoreFront 部署中当前可用的桌面设备站点， 请键入以下命令。
   Get-DSDesktopAppliancesSummary

配置 用户身份验证

桌面设备站点支持显式身份验证、智能卡身份验证以及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。如果您启用显式身份验证和智能卡身份验证或使用智能卡的直通身份验证，则默认会在用户初次登录时提示用户使用智能卡登录。 如果用户使用智能卡时遇到问题，将向其提供选项以输入显式凭据。 如果将 IIS 配置为与所有 StoreFront URL 进行 HTTPS 连接都需要客户端证书，那么即使用户无法使用智能卡，也无法退回到显式身份验证。 要为桌面设备站点配置身份验证方法，请编辑站点配置文件。

1. 使用文本 编辑器打开桌面设备站点的 web.config 文件，该文件 通常位于 C:\inetpub\wwwroot\Citrix\storenameDesktopAppliance 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。
3. 将 enabled 属性的 值更改为 false，为站点禁用显式身份验证。
4. 在此文件中 查找以下元素。

5. 将 enabled 属性的 值设为 true 以启用智能卡身份验证。要启用使用 智能卡的直通身份验证，必须将 useEmbeddedSmartcardSso 属性的值也设为 true。使用 embeddedSmartcardSsoPinTimeout 属性以小时、分钟和秒为单位 设置 PIN 输入屏幕超时前显示的 时间。 当 PIN 输入屏幕超时时，用户将返回到登录屏幕，且必须先 移除然后再重新插入智能卡才可再次访问 PIN 输入屏幕。默认情况下， 超时时间段设为 20 秒。

支持用户 在多个桌面之间进行选择

默认情况下，当用户登录到桌面设备站点时，在为其配置站点的应用商店中对用户可用的第一个桌面（按字母顺序）会自动启动。 如果在一个应用商店中为用户提供了多个桌面的访问权限，则可以配置桌面设备站点以显示可用桌面，以便用户从中选择要访问的桌面。 要更改这些设置，请编辑站点配置文件。

1. 使用文本 编辑器打开桌面设备站点的 web.config 文件，该文件 通常位于 C:\inetpub\wwwroot\Citrix\storenameDesktopAppliance 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。
3. 将 showMultiDesktop 属性的 值更改为 true，使用户在登录到 桌面设备站点时能够查看应用商店中的所有可用桌面 并从中选择。

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

Nov 27, 2017

注意：要将此 功能与本地桌面版 Receiver 结合使用，需要使用以下版本。

- Windows Receiver 4.2
- MAC Receiver 11.9

您可以通过 NetScaler 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。

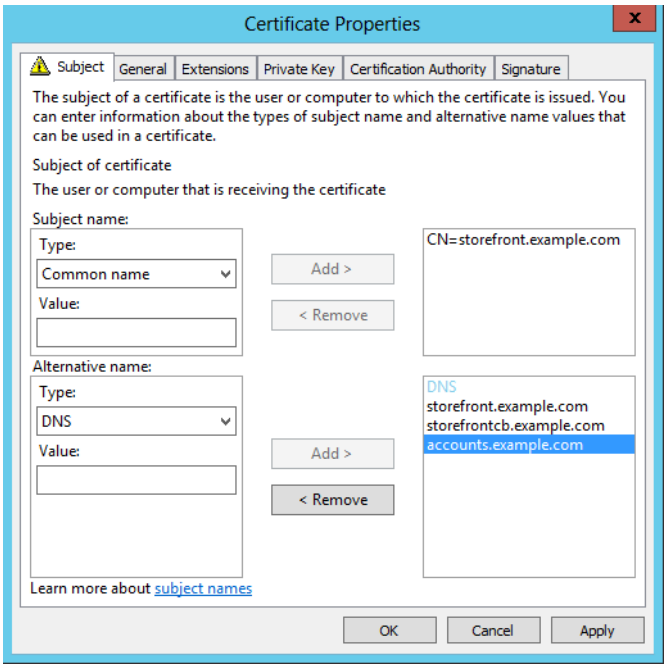
本机 Receiver 的 StoreFront 信标

Citrix Receiver 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 Receiver。这可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。有关配置信标点的信息，请参阅配置信标点。

配置 NetScaler Gateway vServer 和 SSL 证书

外部客户端试图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 NetScaler Gateway vServer IP。确保 SSL 证书的 Common Name（公用名）和 Subject Alternative Name（使用者备用名称）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) 签署网关证书，任何外部客户端都将自动信任绑定到网关 vServer 的证书。如果使用的是第三方根 CA（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 NetScaler Gateway 和 StoreFront 服务器，请考虑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。



NetScaler Gateway vServer 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 字段中作为使用者备用名称 (SAN)。
2. 确保私钥可导出，以便证书和密钥能够导入到 NetScaler Gateway 中。
3. 确保已将“默认身份验证”设置为“允许”。
4. 使用第三方 CA（如 Verisign）或组织的企业根 CA 签署证书。

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) 签署 NetScaler Gateway vServer SSL 证书

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 NetScaler Gateway vServer 的证书由受信第三方签署，外部客户端可能无需将任何根 CA 证书复制到其受信根 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，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 NetScaler Gateway vServer。
- 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 证书复制到其受信根 CA 存储中。如果在安装了本机 Receiver 的情况下使用便携式设备（如 iPhone 和 iPad），请在这些设备上创建安全配置文件。

将根证书导入到便携式设备中

- iOS 设备可以使用电子邮件附件导入 .CER x.509 证书文件，因为通常不可以访问 iOS 设备的本地存储。
- Android 设备需要相同的 .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

确保您组织 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 NetScaler Gateway vServer 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 所颁发的证书导入到 NetScaler 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 NetScaler Gateway 文件系统。将要导入的证书复制到 NetScaler Gateway 文件系统内的 /nsconfig/ssl/ 文件夹。您可以使用 NetScaler Gateway 上的 OpenSSL 工具从 PKCS12/PFX 文件提取证书和密钥，以便以 NetScaler 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 NetScaler Gateway 设备或 VPX 上的 /nsconfig/ssl 中。

2. 打开 NetScaler Gateway 命令行界面。
3. 要切换到 FreeBSD shell，请键入 Shell 以退出 NetScaler 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. 要返回到 NetScaler Gateway 命令行接口，请键入 Exit。

本地 Windows/Mac Receiver 网关会话策略

REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS

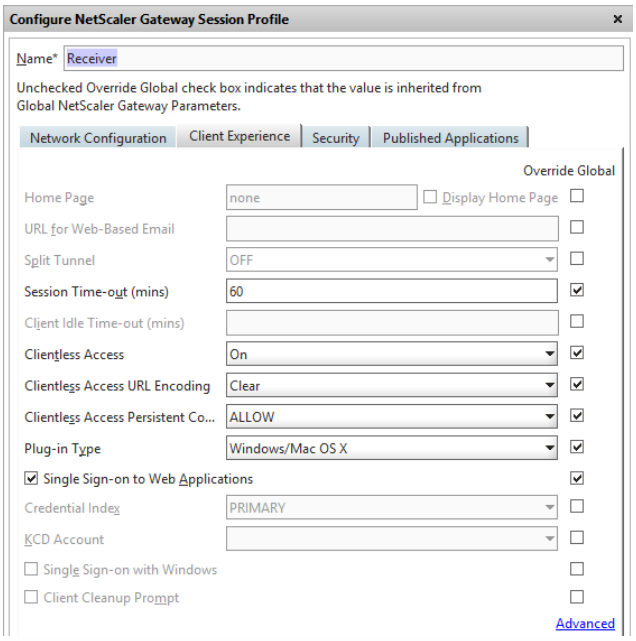
Receiver for Web 网关会话策略

REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS

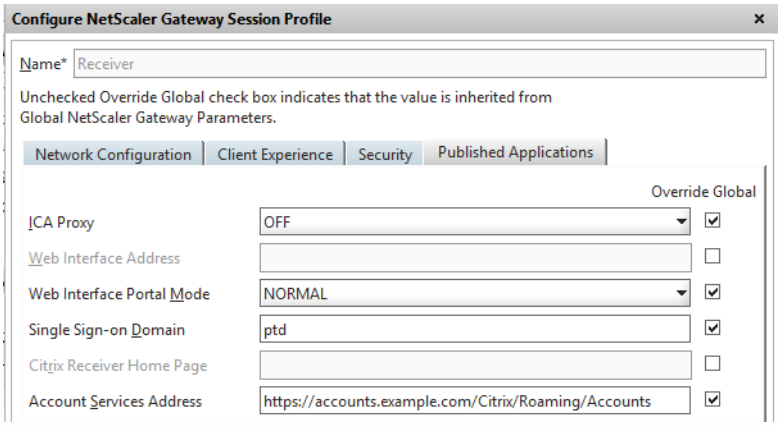
cVPN 和智能访问设置

如果使用 SmartAccess，请在 NetScaler Gateway vServer 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

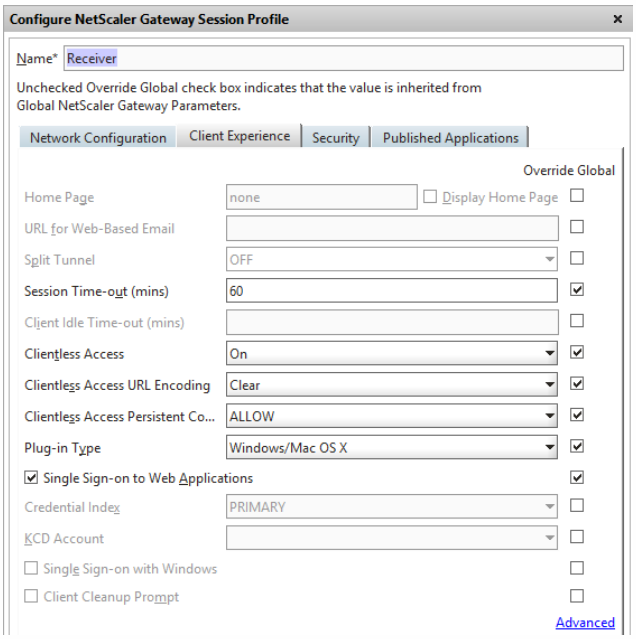


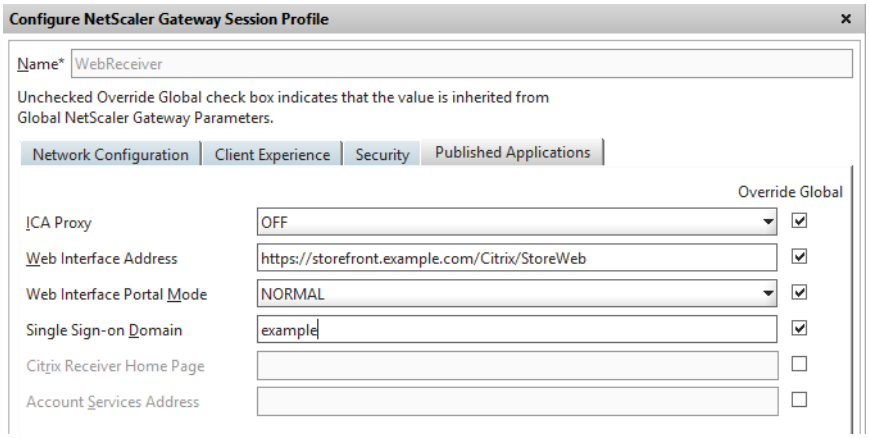
将会话配置文件帐户服务 URL 配置为 https://accounts.example.com/Citrix/Roaming/Accounts，而非 https://storefront.example.com/Citrix/Roaming/Accounts。



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

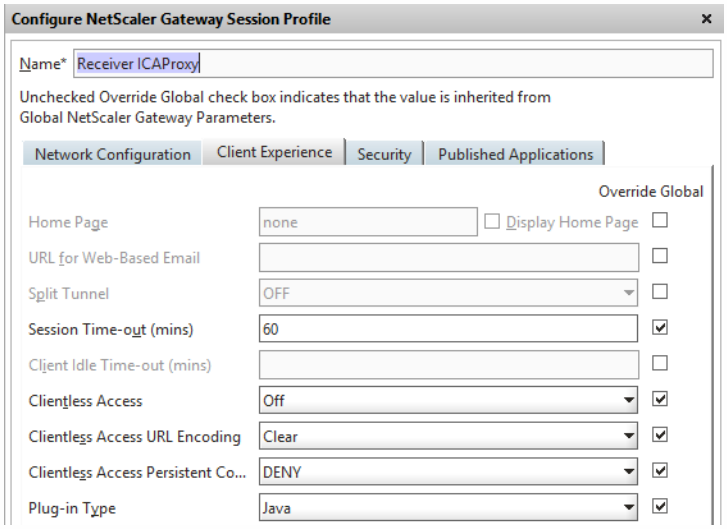


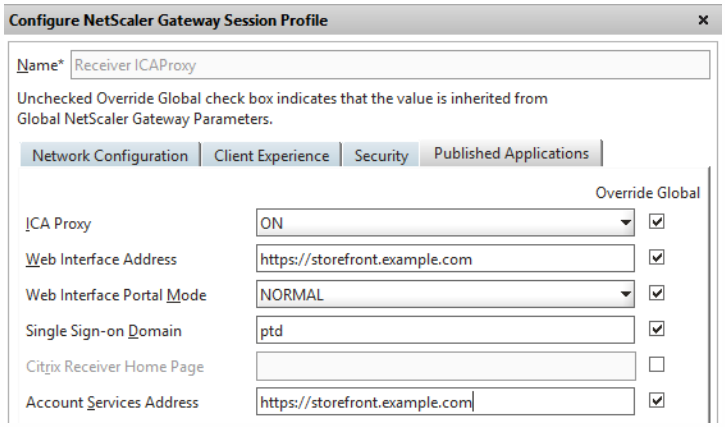


ICA 代理和基本模式设置

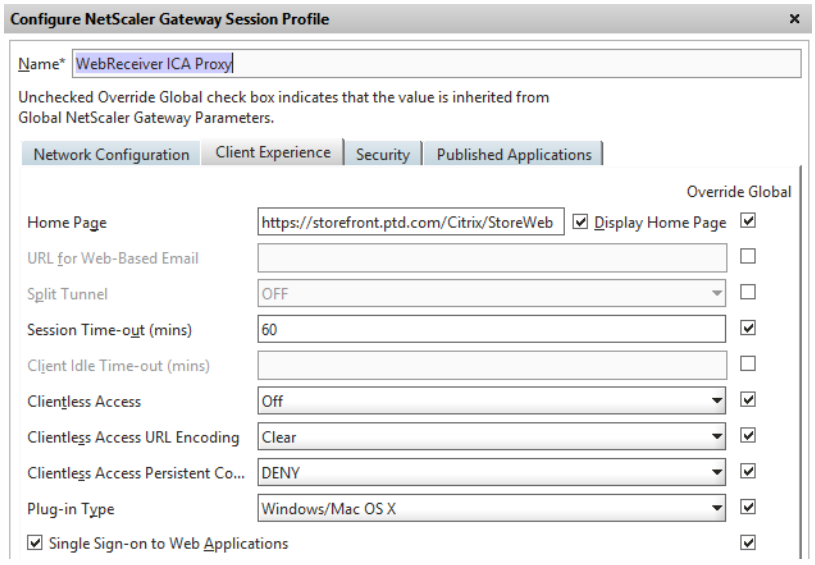
如果使用 ICA 代理，请在 NetScaler Gateway vServer 属性页面上启用基本模式。只需使用 NetScaler 平台许可证。

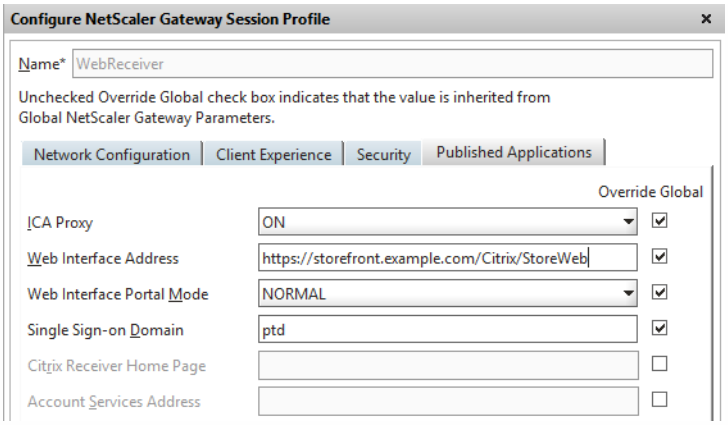
Receiver 配置文件





Receiver for Web 配置文件





配置 StoreFront 服务器主机基本 URL、网关和 SSL 证书

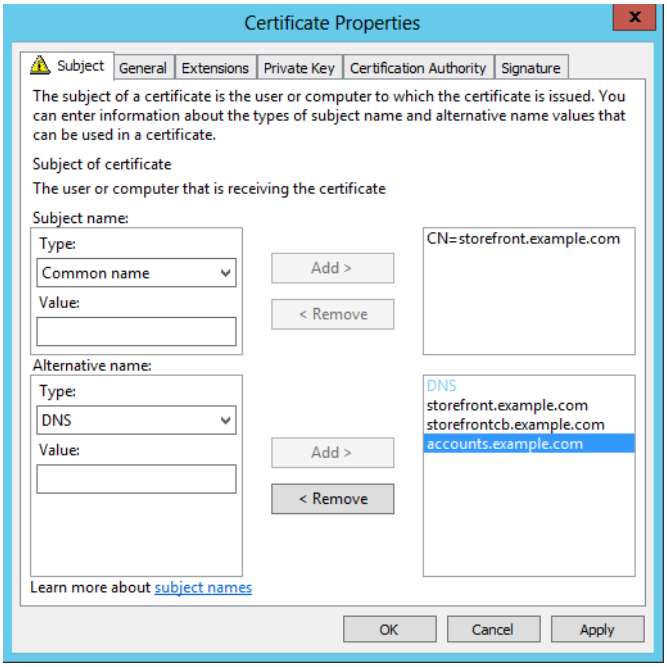
解析到 NetScaler Gateway vServer 的同一共享 FQDN 还应直接解析到 StoreFront 负载平衡器（如果已创建 StoreFront 群集）或托管应用商店的单个 StoreFront IP。

内部 DNS：创建三个 DNS A 记录。

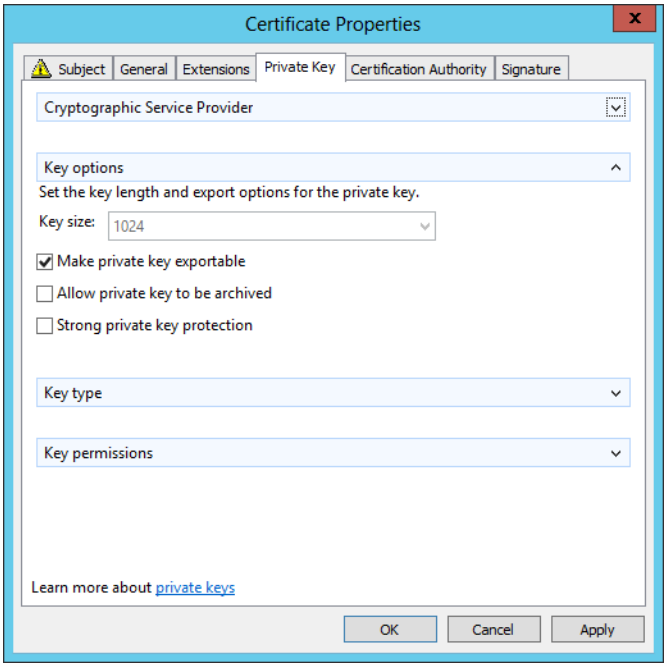
- storefront.example.com 应解析到 storefront 负载平衡器或单个 StoreFront 服务器 IP。
- 如果 DMZ 和企业本地网络之间存在防火墙，则 storefrontcb.example.com 应解析为网关 vServer VIP 以允许此情况。
- accounts.example.com — 作为 storefront.example.com 的 DNS 别名创建。它也解析到 StoreFront 群集的负载平衡器 IP 或单个 StoreFront 服务器 IP。

StoreFront 服务器示例证书：storefront.example.com

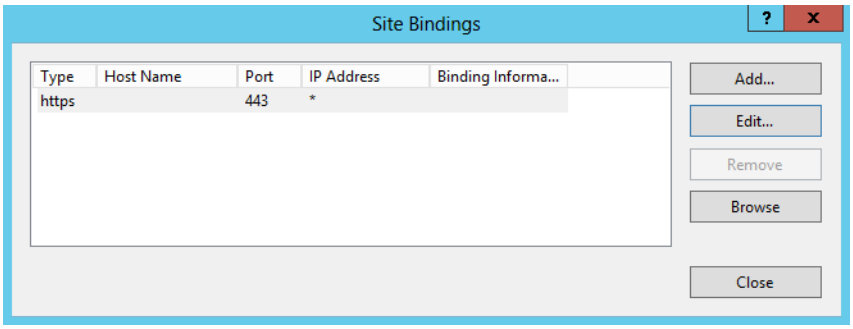
1. 安装 StoreFront 之前，为 StoreFront 服务器或服务器组创建恰当的证书。
2. 将共享 FQDN 添加到“Common name”（公用名）和 DNS 字段中。确保这与绑定到之前创建的 NetScaler Gateway vServer 的 SSL 证书中所使用的 FQDN 相匹配，或使用绑定到 NetScaler Gateway vServer 的相同证书。
3. 将帐户别名 (accounts.example.com) 作为另一个 SAN 添加到证书中。请注意，SAN 中使用的帐户别名是在先前过程（**本机 Receiver Gateway 会话策略和配置文件**）的 NetScaler Gateway 会话配置文件中使用的帐户别名。



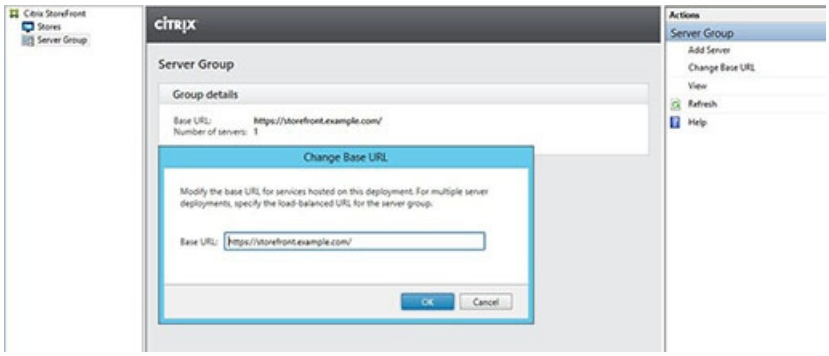
4. 确保私钥可导出，以便证书能够转移到其他服务器或多个 StoreFront 服务器组节点。



5. 使用第三方 CA（例如 VeriSign）、您的企业根 CA 或中间 CA 签署证书。
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（如 NetScaler LB vServer），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。



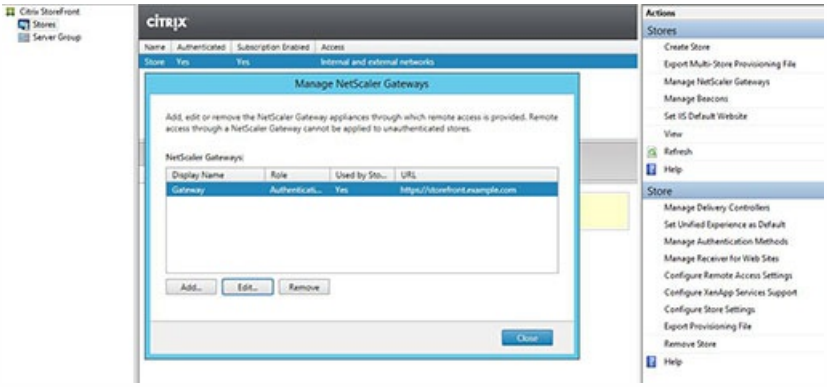
9. 在 StoreFront 服务器上配置主机基本 URL，以匹配已经选择的共享 FQDN。
   注意 ：StoreFront 始终自动选择证书内 SAN 列表中的最后一个使用者备用名称。这只是对 StoreFront 管理员有所帮助的建议主机基本 URL，通常都是正确的。如果它作为 SAN 存在于证书内，则可手动将其设置为任何有效的 HTTPS://<FQDN>。示例：https://storefront.example.com



在 StoreFront 服务器上配置 Gateway：storefront.example.com

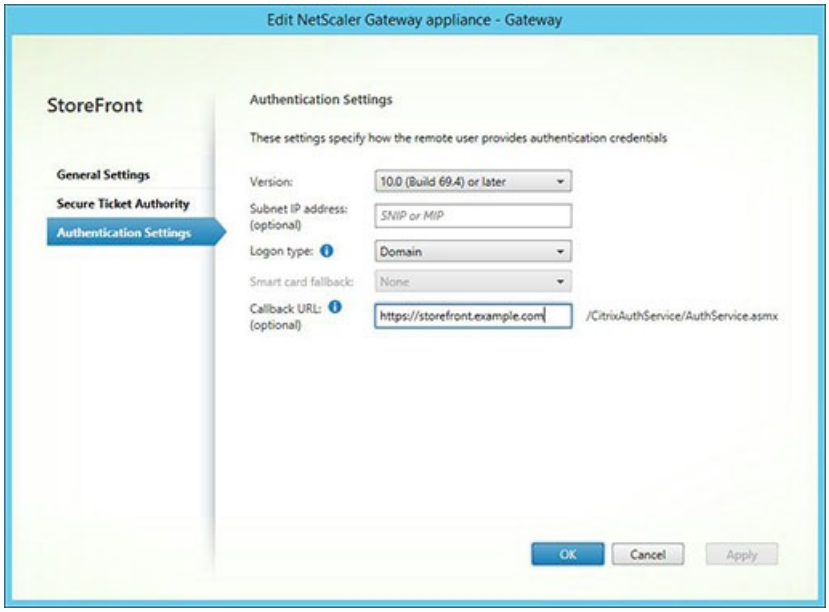
1. 在**应用商店**节点中，单击**操作**窗格中的**管理 NetScaler Gateway**。

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 **NetScaler Gateway URL** 字段中键入共享 FQDN。

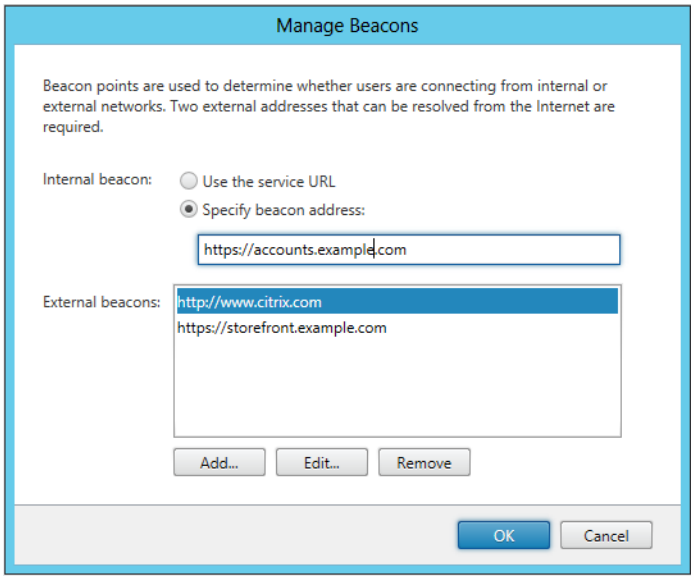
4. 选择**身份验证设置**选项卡，然后在**回调 URL** 字段中键入回调 FQDN。



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 NetScaler Gateway vServer 所共享的外部信标 (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。



8. 请注意，如果希望使用 FQDN 来支持发现，请遵循以下步骤。如果置备文件配置足够，或者仅使用 Receiver for Web，则可跳过以下步骤。

将附加 条目添加到 C:\inetpub\wwwroot\Citrix\Authentication\web.config 中。身份验证 web.config 文件中有两个 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 。

9. 搜索 字符串。找到以下条目并添加以**粗体**显示的行，然后保存并关闭 web.config 文件。

.....

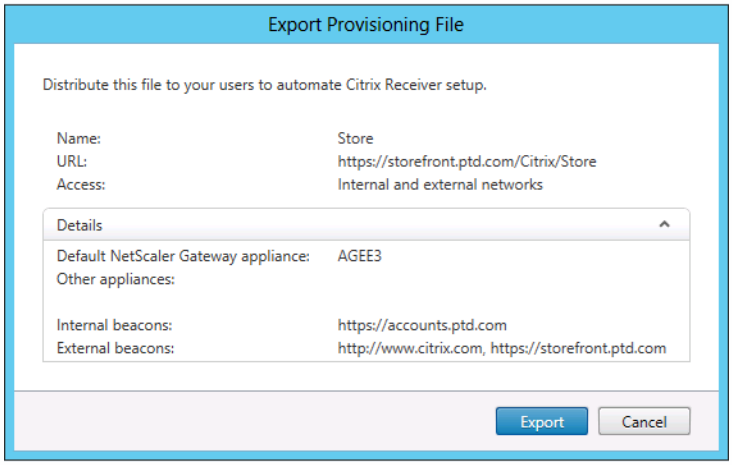
.....

9. 在 **C:\inetpub\wwwroot\Citrix\Roaming\web.config** 中，找到以下条目并添加以**粗体**显示的行，然后保存并关闭 web.config 文件。

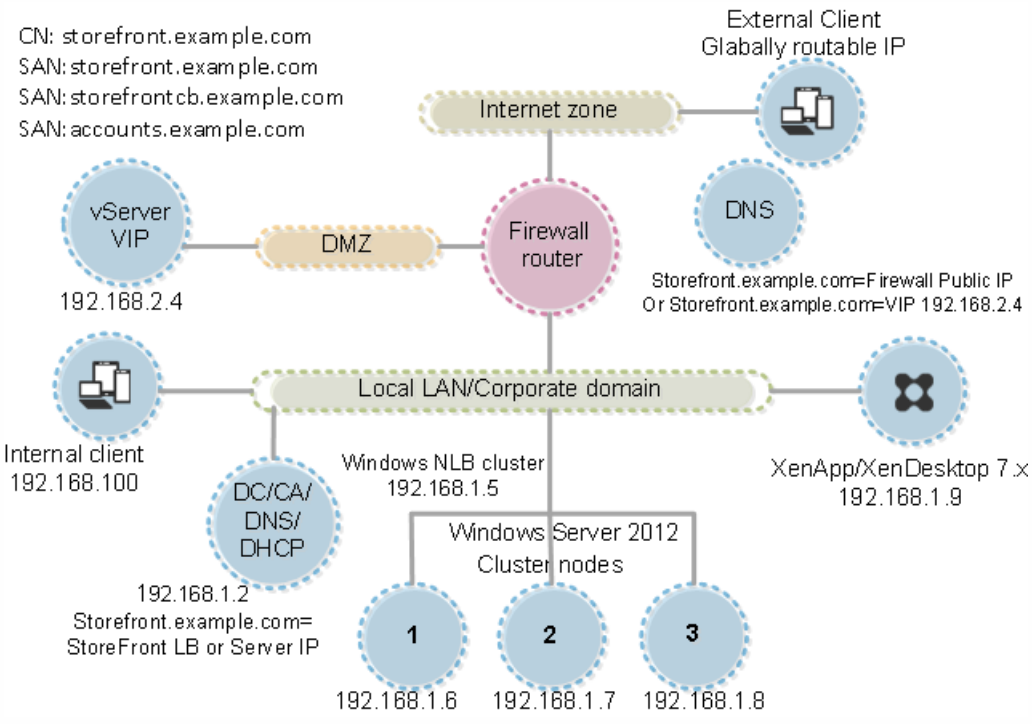
.....

.....

或者，也可以导出应用商店的本机 receiver .CR 置备文件。这样，您在首次使用本机 Receiver 时便不必进行配置。将此文件分发给所有 Windows 和 MAC Receiver 客户端。



如果客户端上已安装 Receiver，则会识别 .CR 文件类型，双击置备文件会将其自动导入。



配置资源过滤

Nov 27, 2017

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应用商店自定义 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“应用商店自定义 SDK”。

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 XenDesktop 或 XenApp 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
- 必需

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

Nov 27, 2017

可以使用配置文件为不能通过 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 Receiver 登录对话框
- 阻止 Receiver for Windows 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

Nov 27, 2017

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。

启用 ICA 文件签名服务

禁用文件类型关联

自定义 Citrix Receiver 登录对话框

阻止 Citrix Receiver for Windows 缓存密码和用户名

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 Receiver 版本能够验证文件是否来自受信任的来源。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，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 Receiver 中启用 ICA 文件签名服务的详细信息，请参阅 ICA 文件签名服务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。

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. 确保要用于对 ICA 文件进行签名的证书在 StoreFront 服务器上的 Citrix 交付服务证书存储中可用，而在当前用户的证书存储中不可用。
2. 使用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 是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。

   ...

4. 将要用于进行签名的证书的详细信息包含在此文件中，如下所示。

   certificateid" thumb="certificatethumbprint" />

   ...

   其中 certificateid 是用于在应用商店配置文件中标识证书的值，certificatethumbprint 是哈希算法生成的证书数据的摘要（或指纹）。

5. 在此文件中查找以下元素。

6. 将 enabled 属性的值更改为 True，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 "certificatethumbprint"

   Add-DSCertificateKeyReadAccess -certificate $certificates[0] -accountName “IIS APPPOOL\Citrix Delivery Services Resources”
   ```

   其中 certificatethumbprint 是通过哈希算法生成的证书数据的摘要。

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。

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. 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 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。

3. 将 enableFileTypeAssociation 属性的值更改为 off，为应用商店禁用文件类型关联。

自定义 Citrix Receiver 登录对话框

Citrix Receiver 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 Citrix Receiver 登录对话框中的标题文本，可以编辑身份验证服务的文件。

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，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. 使用文本编辑器打开身份验证服务的 UsernamePassword.tfrm 文件，该文件通常位于 C:\inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\ 目录中。
2. 在该文件中找到以下行。
   @* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
3. 如下所示，删除前导和后导前导 @* 及后导 @*，取消语句的注释状态。
   @Heading("ExplicitAuth:AuthenticateHeadingText")
   Citrix Receiver 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身份验证服务的 ExplicitAuth.resx 文件，该文件通常位于 C:\inetpub\wwwroot\Citrix\Authentication\App_Data\resources\ 目录中。
5. 在此文件中找到以下元素。编辑 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 Citrix Receiver 登录对话框中看到的主题文本。

   My Company Name

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

阻止 Citrix Receiver for Windows 缓存密码和用户名

默认情况下，Citrix Receiver for Windows 会在用户登录 StoreFront 应用商店时存储其密码。要阻止 Citrix Receiver for Windows（但 Citrix Receiver for Windows Enterprise 除外）缓存用户的密码，请编辑用于身份验证服务的文件。

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，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. 使用文本编辑器打开 inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\UsernamePassword.tfrm 文件。
2. 在此文件中找到以下行。
   @SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey: "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked: ControlValue("SaveCredentials"))
3. 注释掉如下所示语句。

   Citrix Receiver for Windows 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**
>
> 注册表编辑器如果使用不当，会导致可能需要重新安装操作系统的严重问题。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

Nov 27, 2017

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。

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。

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. 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 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。

3. 将 showDesktopsView 和 showAppsView 属性的值更改为 false，以分别阻止将桌面和应用程序显示给用户（即使站点提供这些内容也是如此）。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。

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，无论工作区控制如何配置，该用户的应用程序均不会重新连接。

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”

默认情况下，Citrix Receiver for Web 为未经身份验证（未经身份验证的用户的访问）和强制性（用户无需订阅，便可在“首页”屏幕中使用所有已发布的应用程序）应用商店显示“我的应用程序文件夹视图”。此视图以文件夹层次结构显示应用程序，并包括导航控件路径。

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. 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 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。

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

Nov 27, 2017

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
- .gif
- .htm
- .html
- ica
- .ico
- .jpg
- .js
- .png
- .svg
- .txt
- .xml

如果为 Citrix Receiver for Web 启用了 Citrix Receiver 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 Citrix Receiver for HTML5，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

请求过滤

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：

- ISAPI 过滤器
- ISAPI 扩展
- CGI 程序
- FastCGI 程序

> ## Important
>
> - 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

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。

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。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

StoreFront 安装将向“管理员”安全组中添加以下服务：

- Citrix Configuration Replication (NT SERVICE\CitrixConfigurationReplication)
- Citrix Cluster Join (NT SERVICE\CitrixClusterService)

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

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 Receiver 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。要获得最佳用户体验，请安装包含使用者或使用者备用名称条目（属于 **discoverReceiver.domain**，其中 domain 为包含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 Receiver 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 Receiver 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 Service 和 Citrix Subscriptions Store Service 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 \Scripts 下的文件夹中存储了多个 PowerShell 脚本 (.ps1)。默认 StoreFront 安装不使用这些脚本。这些脚本简化了不经常执行的特定任务的配置步骤。这些脚本已签名，允许 StoreFront 支持 PowerShell 执行策略。我们建议使用 **AllSigned** 策略。（**限制**策略不受支持，因为这会阻止执行 PowerShell 脚本。）StoreFront 不会更改 PowerShell 执行策略。

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

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 XenApp 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 XenApp 组件。

Citrix 建议使用 NetScaler 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 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 Receiver 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。

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。

导出和导入 StoreFront 配置

Nov 27, 2017

可以导出 StoreFront 部署的完整配置。这包括单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，导出的配置备份将以单个 .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。

导出和导入 StoreFront 配置时的注意事项

用于加密和解密 StoreFront 备份的 PowerShell 凭据对象

PowerShell cmdlet

配置导出和导入示例

导出和导入 StoreFront 配置时的注意事项

- 是要使用备份存档中包含的主机基本 URL，还是指定要在导入服务器上使用的新的主机基本 URL？
- 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，请使用包含所选项的密码的 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。

用于加密和解密 StoreFront 备份的 PowerShell 凭据对象

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，此示例代码仅获取当前登录的 Windows 用户。

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential($User,$Password)
```

PowerShell cmdlet

Export-STFConfiguration

参数	说明
-TargetFolder (字符串)	备份存档的导出路径。 示例："$env:userprofile\desktop\"
-Credential（PSCredential 对象）	在导出时指定凭据对象以创建加密的 .ctxzip 备份存档。 PowerShell 凭据对象应包含用于加密和解密的密码。请勿同时使用 **-Credential** 和 **-NoEncryption** 参数。 示例：$CredObject
-NoEncryption（开关）	指定备份存档应采用未加密的 .zip 形式。 请勿同时使用 **-NoEncryption** 与 **-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。

> ## Important
>
> 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（反之亦然）。

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://.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："$env:userprofile\desktop\backup.ctxzip"
-OutputFolder (字符串)	创建加密备份存档 (.ctxzip) 的取消加密副本 (.zip) 的路径。最初的加密备份副本将保留，以便重复使用。请勿指定已取消加密副本的文件名和文件扩展名。 示例："$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 SDK 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：

```
$SDKModules = 'C:\Program Files\Citrix\Receiver StoreFront\PowerShellSDK\Modules\Citrix.StoreFront'
Import-Module "$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
Import-Module "$SDKModules.SubscriptionsStore\Citrix.StoreFront.SubscriptionsStore.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。

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -zipFileName "backup" -NoEncryption
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.zip"
```

创建服务器 A 上现有配置的加密备份并将其还原到相同的部署。

```
# Create a PowerShell Credential Object
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential($User,$Password)
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -zipFileName "backup" -Credential $CredObject
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject
```

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
```

备份服务器 A 上的现有配置并将其还原到服务器 B 上的新出厂默认安装

服务器 B 是新部署，但是计划与服务器 A 同时存在。应指定 **-HostBaseURL** 参数。服务器 B 也是一个新的出厂默认 StoreFront 安装。

1. 创建一个 PowerShell 凭据对象并导出一份加密的服务器 A 配置。
2. 在服务器 B 上创建一个 PowerShell 凭据对象，使用的密码与加密备份时使用的密码相同。
3. 使用 **-HostBaseURL** 参数，解密服务器 A 配置并将其导入到服务器 B 上。

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject -
HostBaseURL "https://serverB.example.com
```

备份服务器 A 上的现有配置并使用此备份覆盖服务器 B 上的现有部署

服务器 B 是配置过时的现有部署。使用服务器 A 配置更新服务器 B。服务器 B 计划与服务器 A 同时存在。指定 **-HostBaseURL** 参数。

1. 创建一个 PowerShell 凭据对象并导出一份加密的服务器 A 配置。
2. 在服务器 B 上创建一个 PowerShell 凭据对象，使用的密码与加密备份时使用的密码相同。
3. 使用 **-HostBaseURL** 参数，解密服务器 A 配置并将其导入到服务器 B 上。

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" –Credential $CredObject -
```

HostBaseURL "https://serverB.example.com"

使用相同的主机基本 URL 创建现有部署的克隆，例如在升级到新服务器操作系统和停用过时的 StoreFront 部署时。

2012R2 服务器 B 是新部署，计划取代过时的 2008R2 服务器 A。应使用备份存档中的 HostBaseURL。请勿在导入时使用 **-HostBaseURL** 参数。服务器 B 也是一个新的出厂默认 StoreFront 安装。

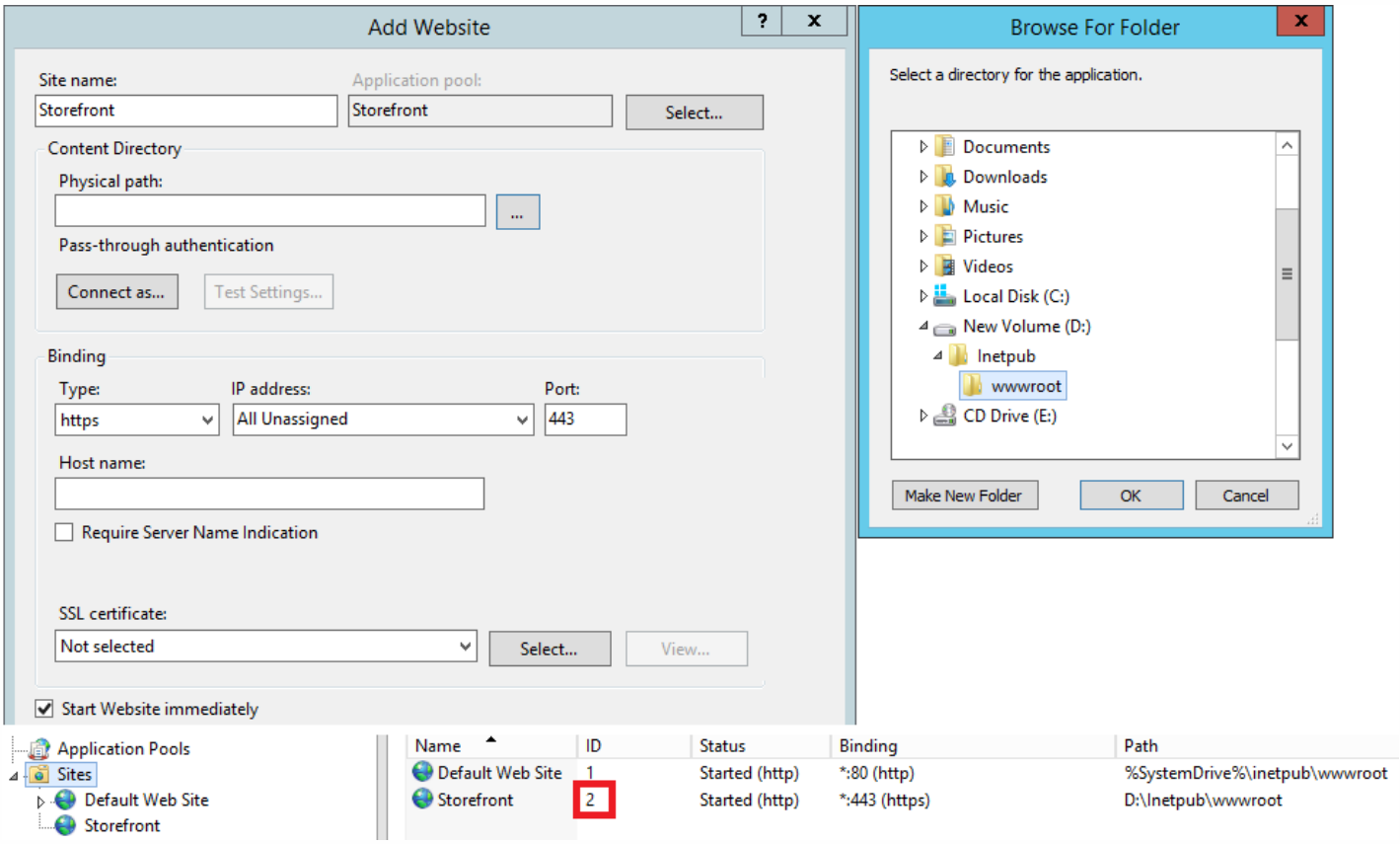
1. 创建一个 PowerShell 凭据对象并导出 2008R2 服务器 A 配置的加密副本。
2. 在 2012R2 服务器 B 上创建一个 PowerShell 凭据对象，使用的密码与加密备份时使用的密码相同。
3. 解密 2008R2 服务器 A 配置并将其导入到 2012R2 服务器 B 上，无需使用 **-HostBaseURL** 参数。

Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject

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，但应该使用大于 1 的 IIS SiteID。

名为 StoreFront 的新 Web 站点已经在 IIS 内配置，此站点使用 **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. 创建一个 PowerShell 凭据对象并导出一份加密的服务器 A 配置。
2. 在服务器 B 上，使用名为 **StoreFront** 的新 Web 站点配置 IIS，此站点也使用 **SiteID 2**。
3. 在服务器 B 上创建一个 PowerShell 凭据对象，使用的密码与加密备份时使用的密码相同。

4. 使用 **-HostBaseURL** 参数，解密服务器 A 配置并将其导入到服务器 B 上。使用备份中包含的站点 ID，并且该 ID 必须与要在其中导入 StoreFront 配置的目标 Web 站点的 ID 相匹配。

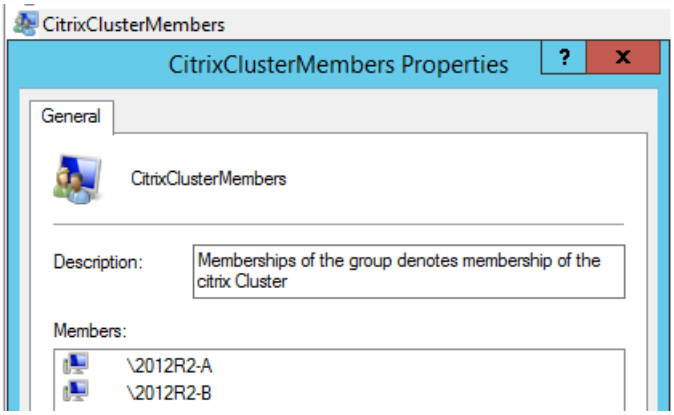
```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject -
HostBaseURL "https://serverB.example.com"
```

服务器组场景

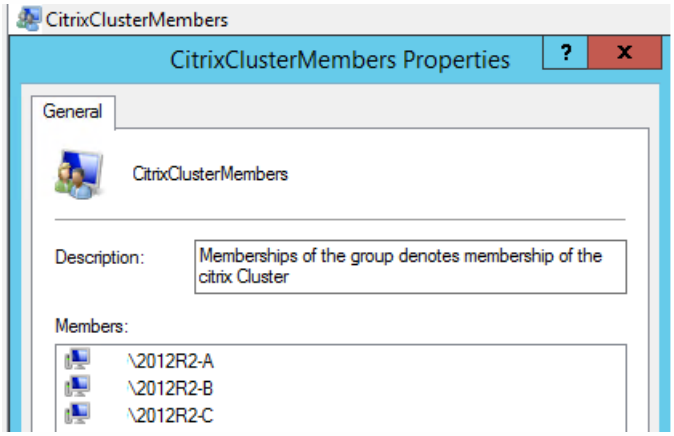
场景 1：备份现有服务器组配置，然后将其还原到相同的服务器组部署中。

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，因此，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 配置未发生变化。即使导入了仅包含两个初始服务器组节点的旧备份，但也必须维护三台服务器的当前 CitrixClusterMembership。在导入过程中，将保留当前的群集成员关系，然后在配置成功导入到主服务器上之后执行写回。如果在执行初始备份之后，从服务器组删除服务器组节点，导入还会保留当前的 CitrixClusterMembership。

1. 从 2012R2-A 中导出服务器组 1 配置，该服务器是用于管理整个服务器组的主服务器。



2. 然后将另一台服务器 2012R2-C 添加到现有服务器组中。



3. 必须将服务器组的配置还原到之前的某个已知工作状态。StoreFront 在导入过程中将备份三台服务器的当前 CitrixClusterMembership，并在导入成功后进行还原。

4. 将服务器组 1 配置重新导入到 2012R2-A 节点上。

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject
```

5. 将新导入的配置传播到整个服务器组，从而使所有服务器在导入后具有一致的配置。

场景 2：备份服务器组 1 的现有配置，使用此备份在另一个出厂默认安装上创建新的服务器组。然后，可以将其他新服务器组成员添加到新的主服务器。

创建包含两个新服务器（2012R2-C 和 2012R2-D）的服务器组 2。服务器组 2 配置将基于现有部署（即服务器组 1）的配置，服务器组 1 也包含两台服务器 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" -Credential $CredObject -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 应用到服务器组 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.ctxzip" -Credential $CredObject -HostBaseURL "https://servergroup2.example.com"

StoreFront SDK

Nov 27, 2017

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** - 本版本提供高级别 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，实现了配置部署（包括应用商店、身份验证方法、Citrix Receiver for Web 和统一的 Citrix Receiver 站点）以及通过 NetScaler 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。

> ### Important
>
> 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，type:
   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
<示例：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：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。
<示例：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：创建包含桌面设备站点的部署>	脚本：创建配置了桌面设备站点的简单部署。

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，Citrix 建议您按照本文档中所述的步骤进行操作，而不要复制粘贴示例脚本。

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"
)
# 导入 StoreFront 模块。要求使用 3.0 版之前的 PowerShell，这些版本不支持自动加载
Import-Module Citrix.StoreFront
Import-Module Citrix.StoreFront.Stores
Import-Module Citrix.StoreFront.Authentication
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。

```
# 根据应用商店确定要使用的身份验证和 Receiver 虚拟路径
$authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"
$receiverVirtualPath = "$($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。

```
# 确定部署是否已存在
$existingDeployment = Get-STFDeployment
if(-not $existingDeployment)
```

```
{
    # 安装所需的 StoreFront 组件
    Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -Confirm:$false
}
elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)
{
    # 部署存在，但配置为所需的主机基本 URL
    Write-Output "A deployment has already been created with the specified hostbase url on this server and will be used."
}
else
{
    Write-Error "A deployment has already been created on this server with a different host base url."
}
```

- 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。

```
# 确定指定虚拟路径下是否存在身份验证服务
$authentication = Get-STFAuthenticationService -VirtualPath $authenticationVirtualPath
if(-not $authentication)
{
    # 添加使用附加了 Auth 的应用商店的 IIS 路径的身份验证服务
    $authentication = Add-STFAuthenticationService $authenticationVirtualPath
}
else
{
    Write-Output "An Authentication service already exists at the specified virtual path and will be used."
}
```

- 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。

```
# 确定指定虚拟路径下是否存在身份验证服务
$authentication = Get-STFAuthenticationService -VirtualPath $authenticationVirtualPath
```

```
if(-not $authentication)
{
    # 添加使用附加了 Auth 的应用商店的 IIS 路径的身份验证服务
    $authentication = Add-STFAuthenticationService $authenticationVirtualPath
}
else
{
    Write-Output "An Authentication service already exists at the specified virtual path and will be used."
}
```

- 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）。

```
# 确定指定虚拟路径下是否存在应用商店服务
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
if(-not $store)
{
# 添加使用新身份验证服务且配置为发布来自所提供的服务器的资源的应用商店
$store = Add-STFStoreService -VirtualPath $StoreVirtualPath -AuthenticationService $authentication -
FarmName $Farmtype -FarmType $Farmtype -Servers $FarmServers -LoadBalance $LoadbalanceServers `
    -Port $Port -SSLRelayPort $SSLRelayPort -TransportType $TransportType
}
else
{
    Write-Output "A Store service already exists at the specified virtual path and will be used. Farm and servers will
be appended to this store."
    # 获取在应用商店中配置的场数量
    $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.Count
    # 将场附加到具有唯一名称的应用商店
    Add-STFStoreFarm -StoreService $store -FarmName "Controller$($farmCount + 1)" -FarmType $Farmtype -
Servers $FarmServers -LoadBalance $LoadbalanceServers -Port $Port `
    -SSLRelayPort $SSLRelayPort -TransportType $TransportType
```

```
}
```

- 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。

```
# 确定指定虚拟路径下是否存在 Receiver 服务
$receiver = Get-STFWebReceiverService -VirtualPath $receiverVirtualPath
if(-not $receiver)
{
   # 添加一个 Receiver for Web 站点，以便用户能够访问应用商店中已发布的应用程序和桌面
   $receiver = Add-STFWebReceiverService -VirtualPath $receiverVirtualPath -StoreService $store
}
else
{
   Write-Output "A Web Receiver service already exists at the specified virtual path and will be used."
}
```

- 为应用商店启用 XenApp 服务，以便较旧的 Citrix Receiver 客户端能够连接到已发布的应用程序。

```
# 确定是否为应用商店服务配置了 PNA
$storePnaSettings = Get-STFStorePna -StoreService $store
if(-not $storePnaSettings.PnaEnabled)
{
  # 在应用商店上启用 XenApp Services 并将其设为此服务器的默认服务
  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，Citrix 建议您按照本文档中所述的步骤进行操作，而不要复制粘贴示例脚本。

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]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP",
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$GatewaySTAUrls,
    [string]$GatewaySubnetIP,
    [Parameter(Mandatory=$true)]
    [string]$GatewayName
)
Set-StrictMode - 版本 2.0

# 任何故障都属于终止故障。
$ErrorActionPreference = 'Stop'
```

```
$ReportErrorShowStackTrace = $true

$ReportErrorShowInnerException = $true

# 导入 StoreFront 模块。要求使用 3.0 版之前的 PowerShell，这些版本不支持自动加载

Import-Module Citrix.StoreFront

Import-Module Citrix.StoreFront.Stores

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。

```
# 通过调用简单部署示例创建简单部署

$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition -Parent

$scriptPath = Join-Path $scriptDirectory "SimpleDeployment.ps1"

& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers $FarmServers -StoreVirtualPath
$StoreVirtualPath -Farmtype $Farmtype `

  -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。

```
# 根据应用商店确定身份验证和 Receiver 站点

$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 NetScaler 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。

```
# 从支持的协议中获取 Citrix Receiver for Web CitrixAGBasic 和 ExplicitForms 身份验证方法。

# 包括演示目的，因为协议名称可以直接使用（如果已知）

$receiverMethods = Get-STFWebReceiverAuthenticationMethodsAvailable | Where-Object { $_ -match "Explicit" -or
$_ -match "CitrixAG" }

# 在 Receiver for Web 中启用 CitrixAGBasic（进行远程访问时需要启用）

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。

```
# 从安装的协议中获取 CitrixAGBasic 身份验证方法。

# 包括演示目的，因为协议名称可以直接使用（如果已知）
```

```
$citrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-Object { $_ -match "CitrixAGBasic" }

# 在身份验证服务中启用 CitrixAGBasic（进行远程访问时需要启用）

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。

```
# 添加用于远程访问新应用商店的新网关

Add-STFRoamingGateway -Name "NetScaler10x" -LogonType Domain -Version Version10_0_69_4 -GatewayUrl $GatewayUrl '

-CallbackUrl $GatewayCallbackUrl -SecureTicketAuthorityUrls $GatewaySTAUrls

# 从配置中获取新网关（如果 -PassThru 作为一个参数提供，则 Add-STFRoamingGateway 将返回新网关）

$gateway = Get-STFRoamingGateway -Name $GatewayName

# 如果提供了网关子网，请在网关对象上设置该子网

if($GatewaySubnetIP)

{

   Set-STFRoamingGateway -Gateway $gateway -SubnetIPAddress $GatewaySubnetIP

}

# 在新应用商店中注册网关

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，Citrix 建议您按照本文档中所述的步骤进行操作，而不要复制粘贴示例脚本。

了解脚本

本部分内容介绍由 StoreFront 生成的脚本的各部分的作用。这将有助于您自定义自己的脚本。

- 请设置错误处理要求并导入所需的 StoreFront 模块。在较新的 PowerShell 版本中，不需要导入。

```
Param(

   [Parameter(Mandatory=$true)]

   [Uri]$HostbaseUrl,

   [long]$SiteId = 1,
```



```
    [string]$Farmtype = "XenDesktop",
    [Parameter(Mandatory=$true)]
    [string[]]$FarmServers,
    [string]$StoreVirtualPath = "/Citrix/Store",
    [bool]$LoadbalanceServers = $false,
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP",
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$GatewaySTAUrls,
    [string]$GatewaySubnetIP,
    [Parameter(Mandatory=$true)]
    [string]$GatewayName,
    [Parameter(Mandatory=$true)]
    [Uri]$OptimalGatewayUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$OptimalGatewaySTAUrls,
    [Parameter(Mandatory=$true)]
    [string]$OptimalGatewayName
)
Set-StrictMode - 版本 2.0
# 任何故障都属于终止故障。
$ErrorActionPreference = 'Stop'
```

```
$ReportErrorShowStackTrace = $true

$ReportErrorShowInnerException = $true

# 导入 StoreFront 模块。要求使用 3.0 版之前的 PowerShell，这些版本不支持自动加载

Import-Module Citrix.StoreFront

Import-Module Citrix.StoreFront.Stores

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。

```
# 创建远程访问部署

$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition -Parent

$scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.ps1"

& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers $FarmServers -StoreVirtualPath
$StoreVirtualPath -Farmtype $Farmtype `

  -LoadbalanceServers $LoadbalanceServers -Port $Port  -SSLRelayPort $SSLRelayPort -TransportType
$TransportType `

  -GatewayUrl $GatewayUrl -GatewayCallbackUrl $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -
GatewayName $GatewayName
```

- 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。

```
# 添加用于通过远程 HDX 访问桌面和应用程序的新网关

$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。

```
# 获取通过 SimpleDeployment.ps1 配置的应用商店

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

# 在新应用商店中注册该网关以针对所有场（当前仅有一个场）启动

$farmNames = @($store.FarmsConfiguration.Farms | foreach { $_.FarmName })

Register-STFStoreOptimalLaunchGateway -Gateway $gateway -StoreService $store -FarmName $farmNames
```

示例：创建包含桌面设备站点的部署

以下示例在简单部署示例基础之上构建，用于添加包含桌面设备站点的部署。

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，Citrix 建议您按照本文档中所述的步骤进行操作，而不要复制粘贴示例脚本。

了解脚本

本部分内容介绍由 StoreFront 生成的脚本的各部分的作用。这将有助于您自定义自己的脚本。

- 请设置错误处理要求并导入所需的 StoreFront 模块。在较新的 PowerShell 版本中，不需要导入。

```
Param(
  [Parameter(Mandatory=$true)]
  [Uri]$HostbaseUrl,
  [long]$SiteId = 1,
  [string]$Farmtype = "XenDesktop",
  [Parameter(Mandatory=$true)]
  [string[]]$FarmServers,
  [string]$StoreVirtualPath = "/Citrix/Store",
  [bool]$LoadbalanceServers = $false,
  [int]$Port = 80,
  [int]$SSLRelayPort = 443,
  [ValidateSet("HTTP","HTTPS","SSL")]
  [string]$TransportType = "HTTP",
  [Parameter(Mandatory=$true)]
  [Uri]$GatewayUrl,
  [Parameter(Mandatory=$true)]
  [Uri]$GatewayCallbackUrl,
  [Parameter(Mandatory=$true)]
  [string[]]$GatewaySTAUrls,
  [string]$GatewaySubnetIP,
  [Parameter(Mandatory=$true)]
  [string]$GatewayName,
  [Parameter(Mandatory=$true)]
  [Uri]$OptimalGatewayUrl,
```

```
    [Parameter(Mandatory=$true)]
    [string[]]$OptimalGatewaySTAUrls,
    [Parameter(Mandatory=$true)]
    [string]$OptimalGatewayName
)
Set-StrictMode - 版本 2.0
# 任何故障都属于终止故障。
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
# 导入 StoreFront 模块。要求使用 3.0 版之前的 PowerShell，这些版本不支持自动加载
Import-Module Citrix.StoreFront
Import-Module Citrix.StoreFront.Stores
Import-Module Citrix.StoreFront.Roaming
```

- 根据 $StoreVirtualPath 的桌面设备路径自动创建该路径。

```
$desktopApplianceVirtualPath = "$($StoreIISPath.TrimEnd('/'))Appliance"
```

- 调用到简单部署脚本中以配置包含所需服务的默认部署。

```
# 创建远程访问部署
$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition -Parent
$scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.ps1"
& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers $FarmServers -StoreVirtualPath
$StoreVirtualPath -Farmtype $Farmtype `
  -LoadbalanceServers $LoadbalanceServers -Port $Port  -SSLRelayPort $SSLRelayPort -TransportType
$TransportType `
  -GatewayUrl $GatewayUrl -GatewayCallbackUrl $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -
GatewayName $GatewayName
```

- 获取要用于桌面设备站点的应用商店服务。使用 **Add-STFDesktopApplianceService** cmdlet 可添加包含多桌面并且使用显式用户名和密码身份验证的新站点。

```
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
# 使用通过应用商店服务发布的桌面创建新桌面设备站点
```

```
Add-STFDesktopApplianceService -VirtualPath $desktopApplianceVirtualPath -StoreService $store -EnableExplicit
```

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 管理控制台中配置 SAML 身份验证（请参阅配置身份验证服务），也可以使用以下 PowerShell cmdlet 配置 SAML 身份验证：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:///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：

命令 复制

```
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/FederationMeta



# 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
```

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。

命令 复制

```
# 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"
```

示例输出

命令 复制

```
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

Nov 27, 2017

安装或卸载 StoreFront 时，StoreFront 安装程序将在 C:\Windows\Temp\ 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，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。

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。
   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，指出将禁止在后面记录相同的日志条目。 限制时间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，指出将不再禁止记录重复的日志条目。

启用 跟踪

警告：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. 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键入以下命令并重新启动服务器以启用跟踪。

   ```
   Add-PSSnapin Citrix.DeliveryServices.Framework.Commands

   Set-DSTraceLevel -All -TraceLevel Verbose
   ```

   -TraceLevel 的允许值为（以不断增加的追踪详细级别）：Off、Error、Warning、Info、Verbose。
   StoreFront 自动捕获“错误”跟踪消息。潜在生成的大量数据可能会使跟踪显著影响 StoreFront 的性能，因此，除非故障排除明确要求，否则建议不要使用 Info 或 Verbose 级别。

   Set-DSTraceLevel cmdlet 的可选参数包括：

-FileCount：指定跟踪文件的数量（默认 = 3）
-FileSizeKb：指定每个跟踪文件的最大大小（默认 = 1000）
-ConfigFile ：-All 的备选参数，允许上载特定配置文件，而不是上载所有文件。例如，-ConfigFile 值为 c:\inetpub\wwwroot\Citrix\\web.config 时将为名为 的应用商店设置跟踪。

2. 要禁用跟踪，请键入以下命令并重新启动服务器。

```
Add-PSSnapin Citrix.DeliveryServices.Framework.Commands

Set-DSTraceLevel -All -TraceLevel Off
```

启用跟踪后，跟踪信息将写入到 StoreFront 安装目录 \Admin\Trace\ 中，该目录位于 C:\Program Files\Citrix\Receiver StoreFront\。